TD11 : Groupe symplectique, groupe orthogonal, groupe unitaire.

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

Exercice 1 : $\star$
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 $\theta_1,\dots,\theta_t \in \mathbb{R}\setminus\pi\mathbb{Z}$, tels que

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

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 1.

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 $P(u) = P_1(u)\circ\dots\circ P_r(u) = 0$, 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 2 : $\star\star$

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 $\varepsilon \in \mathbb{F}_q^\times \backslash \mathbb{F}_q^{\times 2}$. 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 2.

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 3 : ⋆⋆

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 3.

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 1 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 4 : ⋆⋆
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 4.

a) C'est exactement le même raisonnement que la question a) de l'exercice 3 : 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 3 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 5 : ⋆⋆
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 5. 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 $B + {}^tB + 2^n B^t B = 0$. 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 ${}^tAA = A^tA = I_3$. 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 6 : ⋆⋆

Soit K un corps de caractéristique différente de 2 et soient $\alpha, \beta \in K^*$. On note $(1, i, j, k)$ la base canonique de K^4, et on note $\mathbf{H}_{\alpha,\beta}$ l'unique structure de K-algèbre sur K^4 définie par

$$1 \text{ est le neutre pour la multiplication, } i^2 = \alpha\,,\ j^2 = \beta,\ ij = -ji = k\,.$$

a) Définir la norme réduite $N : \mathbf{H}_{\alpha,\beta} \to K$ et la conjugaison $\mathbf{H}_{\alpha,\beta} \to \mathbf{H}_{\alpha,\beta}$.

b) Montrer que si K est algébriquement clos, alors $\mathbf{H}_{\alpha,\beta}$ est isomorphe à $\mathrm{Mat}_2(K)$.

c) Montrer que $\mathbf{H}_{\alpha,\beta}$ est une algèbre à division (i.e. un "corps non commutatif") si et seulement si N est une forme anisotrope sur le K-espace vectoriel $\mathbf{H}_{\alpha,\beta}$.

d) Montrer que si $K = \mathbb{F}_q$, alors $\mathbf{H}_{\alpha,\beta}$ n'est pas intègre.

e) Soient $\alpha', \beta' \in K^*$. Montrer que les K-algèbres $\mathbf{H}_{\alpha,\beta}$ et $\mathbf{H}_{\alpha',\beta'}$ sont isomorphes si et seulement si les normes N et N' associées sont des formes quadratiques isométriques.

Solution de l'exercice 6.

a) Par analogie avec les quaternions de Hamilton, on définit le conjugué d'un élément $z = a + bi + cj + dk$ par $\overline{z} := a - bi - cj - dk$. De même, on définit la norme d'un élément $z = a + bi + cj + dk$ par $N(z) := z\overline{z} = a^2 - \alpha b^2 - \beta c^2 + \alpha\beta d^2$.

b) Soient $a, b \in K^*$ des racines carrées respectives de α et β (ces racines existent car K est algèbriquement clos). Le morphisme de K-algèbres $\mathbf{H}_{\alpha,\beta} \to \mathrm{Mat}_2(K)$ défini par $i \mapsto \begin{pmatrix} a & 0 \\ 0 & -a \end{pmatrix}$ et $j \mapsto \begin{pmatrix} 0 & b \\ b & 0 \end{pmatrix}$ est l'isomorphisme voulu.

c) Il est clair que N est une forme quadratique sur le K-espace vectoriel $\mathbf{H}_{\alpha,\beta}$.
Supposons que $\mathbf{H}_{\alpha,\beta}$ soit une algèbre à division. Soient $z \in \mathbf{H}_{\alpha,\beta} \setminus \{0\}$ et z' un inverse de z. On a alors $N(z)N(z') = N(zz') = N(1) = 1$ et donc $N(z) \neq 0$. Par conséquent, la forme quadratique N est anisotrope.
Réciproquement, si N est anisotrope, alors pour tout élément $z \in \mathbf{H}_{\alpha,\beta} \setminus \{0\}$, l'élément $N(z)^{-1}\overline{z}$ fournit un inverse de z, donc $\mathbf{H}_{\alpha,\beta}$ est une algèbre à division.

d) On sait que sur un corps fini, une forme quadratique de dimension ≥ 3 est isotrope. Par conséquent, la norme N est isotrope sur $\mathbf{H}_{\alpha,\beta}$, donc il existe $z \in \mathbf{H}_{\alpha,\beta} \setminus \{0\}$ tel que $z\overline{z} = N(z) = 0$, donc $\mathbf{H}_{\alpha,\beta}$ n'est pas intègre.

e) Soit $\varphi : \mathbf{H}_{\alpha,\beta} \xrightarrow{\sim} \mathbf{H}_{\alpha',\beta'}$ un isomorphisme de K-algèbres. Comme le centre de ces algèbres est réduit à K, on a nécessairement $\varphi(K) = K$. On note $\mathbf{P}_{\alpha,\beta} \subset \mathbf{H}_{\alpha,\beta}$ le sous-espace vectoriel des quaternions purs. Pour tout $z \in \mathbf{H}_{\alpha,\beta} \setminus \{0\}$, on a $z \in \mathbf{P}_{\alpha,\beta}$ si et seulement si $z \notin K$ et $z^2 \in K$ si et seulement si $\varphi(z) \notin K$ et $\varphi(z)^2 \in K$ si et seulement si $\varphi(z) \in \mathbf{P}_{\alpha',\beta'}$. Donc $\varphi_{|\mathbf{P}_{\alpha,\beta}}$ induit un isomorphisme $\mathbf{P}_{\alpha,\beta} \to \mathbf{P}_{\alpha',\beta'}$. Montrons maintenant que φ préserve la conjugaison : soit $z \in \mathbf{H}_{\alpha,\beta}$. Alors z s'écrit $z = z_0 + p$ avec $z_0 \in K$ et $p \in \mathbf{P}_{\alpha,\beta}$. On a donc $\varphi(\overline{z}) = \varphi(z_0 - p) = \varphi(z_0) - \varphi(p)$ et $\varphi(z) = \varphi(z_0) + \varphi(p)$. Or on a vu que $\varphi(z_0) \in K$ et $\varphi(p) \in \mathbf{P}_{\alpha',\beta'}$, donc les formules précédentes assurent que $\varphi(\overline{z}) = \overline{\varphi(z)}$. On en déduit que pour tout $z \in \mathbf{H}_{\alpha,\beta}$,

$$N'(\varphi(z)) = \varphi(z)\overline{\varphi(z)} = \varphi(z)\varphi(\overline{z}) = \varphi(z\overline{z}) = z\overline{z} = N(z)$$

car $z\overline{z} \in K$ et φ est un morphisme de K-algèbres.
Cela assure que les formes quadratiques N et N' sont isométriques via φ.
Réciproquement, supposons qu'il existe une isométrie (linéaire) $f : (\mathbf{H}_{\alpha,\beta}, N) \to (\mathbf{H}_{\alpha',\beta'}, N')$. Le théorème de Witt (appliqué à l'orthogonal d'un vecteur de norme 1) assure que l'on peut supposer que f envoie $\mathbf{P}_{\alpha,\beta}$ sur $\mathbf{P}_{\alpha',\beta'}$. On a alors $f(i)^2 = -N'(f(i)) = -N(i) = i^2 = \alpha$, et de même $f(j)^2 = \beta$. De plus, comme i et j sont orthogonaux pour N, $f(i)$ et $f(j)$ sont orthogonaux pour N' : ainsi on a $f(i)f(j) + f(j)f(i) = 0$. Cela implique que la sous-K-algèbre de $\mathbf{H}_{\alpha',\beta'}$ engendrée par $f(i)$ et $f(j)$ est isomorphe à $\mathbf{H}_{\alpha,\beta}$, donc par égalité des dimensions, que $\mathbf{H}_{\alpha',\beta'}$ est isomorphe comme K-algèbre à $\mathbf{H}_{\alpha,\beta}$.

Exercice 7 : $\star\star\star$
Soient K un corps de caractéristique $\neq 2$, $\alpha, \beta \in K^*$. On note $\mathbf{H} := \mathbf{H}_{\alpha,\beta}$ (voir l'exercice 6 pour la définition) et $\mathbf{H}^\times := \{x \in \mathbf{H} : N(x) \neq 0\}$.
Pour tout $q \in \mathbf{H}^\times$ et $x \in \mathbf{H}$, on note $S_q(x) := qxq^{-1}$. On rappelle que l'on dispose de la norme N sur $\mathbf{H}$ qui est une forme quadratique.

a) Montrer que pour tout $q \in \mathbf{H}^\times$ et tout $x \in \mathbf{H}$, $N(S_q(x)) = N(x)$.

b) Montrer que pour tout $q \in \mathbf{H}^\times$, $S_{q|_K} = \mathrm{id}_K$ et $S_q(\mathbf{P}) = \mathbf{P}$, où $\mathbf{P} := \mathrm{vect}(i, j, k) \subset \mathbf{H}$ désigne l'espace des quaternions purs.

c) En déduire un morphisme de groupes $s : \mathbf{H}^\times \to \mathrm{O}(\mathbf{P}, N)$ et montrer que son noyau est K^*.

d) Montrer que pour tout $p \in \mathbf{P}^\times := \mathbf{P} \cap \mathbf{H}^\times$, $s(p)$ est le renversement d'axe p. En déduire que $s(\mathbf{H}^\times) = \mathrm{SO}(\mathbf{P}, N)$.

e) En déduire un isomorphisme $\mathbf{H}^\times / K^* \cong \mathrm{SO}(\mathbf{P}, N)$.

f) On suppose $\alpha = \beta = 1$. Montrer que N est une forme isométrique à la forme quadratique $(x, y, z) \mapsto x^2 - y^2 - z^2$ sur K^3. Montrer que $\mathrm{PGL}_2(K) \cong \mathrm{SO}_3(K, N)$ et $\mathrm{PSL}_2(K) \cong \Omega_3(K, N) := D(\mathrm{O}_3(K, N))$.

g) Montrer que pour tout $u \in \mathrm{SO}(\mathbf{H}, N)$, il existe $a, b \in \mathbf{H}^\times$ tels que $u(x) = axb$ pour tout $x \in \mathbf{H}$. Montrer en outre que $N(a)N(b) = 1$.

h) Montrer que pour tout $u \in \mathrm{O}(\mathbf{H}, N) \setminus \mathrm{SO}(\mathbf{H}, N)$, il existe $a, b \in \mathbf{H}^\times$ tels que $u(x) = a\overline{x}b$ pour tout $x \in \mathbf{H}$.

i) Notons $U := \{(a, b) \in \mathbf{H}^\times \times \mathbf{H}^\times : N(a) = N(b)\}$. Construire un morphisme de groupes surjectif $S : U \to \mathrm{SO}(\mathbf{H}, N)$ et calculer son noyau.

j) On suppose $\alpha = \beta = 1$. Montrer que N est une forme hyperbolique sur $\mathrm{Mat}_2(K)$ et que les groupes $\mathrm{P}\Omega_4(K, N) := \mathrm{P}(\mathrm{D}(\mathrm{O}_4(K, N)))$ et $\mathrm{PSL}_2(K) \times \mathrm{PSL}_2(K)$ sont isomorphes.

Solution de l'exercice 7.

a) C'est clair puisque la norme est multiplicative et $N(1) = 1$.

b) Par définition, K est contenu dans le centre de $\mathbf{H}$, ce qui assure que $S_{q|_K} = \mathrm{id}_K$. En outre, on a toujours l'équivalence, pour un $x \in \mathbf{H} \setminus \{0\}$, $x \in \mathbf{P}$ si et seulement si $x \notin K$ et $x^2 \in K$. Cette caractérisation (ou un calcul direct) assure que $S_q(\mathbf{P}) = \mathbf{P}$.

c) Les questions a) et b) assurent que si l'on pose $s(q) := S_{q|_{\mathbf{P}}}$ pour tout $q \in \mathbf{H}^\times$, on définit ainsi un élément $s(q) \in \mathrm{O}(\mathbf{P}, N)$. Or il est clair que $s(1) = \mathrm{id}_{\mathbf{P}}$ et $s(qq') = s(q)s(q')$, donc on a bien défini un morphisme de groupes $s : \mathbf{H}^\times \to \mathrm{O}(\mathbf{P}, N)$. Calculons son noyau : un élément de $\mathbf{H}$ commutant avec tous les éléments de $\mathbf{P}$ commute avec tous les éléments de $\mathbf{H}$, donc est dans K. Par conséquent, $\mathrm{Ker}(s) = K \cap \mathbf{H}^\times = K^*$.

d) Soit σ la réflexion orthogonale d'axe p. Alors on sait que pour tout $x \in \mathbb{P}$, $\sigma(x) = x - 2\frac{\langle x,p\rangle}{N(p)}p = x - \frac{x\overline{p}+p\overline{x}}{p\overline{p}}p$. Or pour tout $x \in \mathbb{P}$, on a $\overline{x} = -x$, donc $\sigma(x) = \frac{pxp}{N(p)}$, donc le renversement d'axe p est donné par $x \mapsto -\sigma(x) = -\frac{pxp}{N(p)} = pxp^{-1} = s(p)$, d'où le résultat.

En particulier, $s(p)$ est un renversement pour tout $p \in \mathbf{P}^\times$, donc $\det(s(p)) = 1$ pour tout $p \in \mathbf{P}^\times$.

Soit alors $z \in \mathbf{H}^\times$. On sait que tout élément de $\mathrm{O}(\mathbf{P}, N)$ est produit de reflexions orthogonales, donc il existe $q_1, \ldots, q_r \in \mathbf{P}^\times$ tels que $s(z)$ est la composée des reflexions orthogonales d'axe $q_1, \ldots, q_r$. Donc $s(z) = (-1)^r s(q_1) \circ \cdots \circ s(q_r)$. Supposons que $s(z) \notin \mathrm{SO}(\mathbf{P}, N)$. Alors r est impair, et pour tout $x \in \mathbf{P}$, on a $zxz^{-1} = -q_1 \ldots q_r x (q_1 \ldots q_r)^{-1}$. En notant $q := q_1 \ldots q_r$, on en déduit que pour tout $x \in \mathbf{H}$, $\overline{x} = (z^{-1}q)x(z^{-1}q)^{-1}$. Ceci est contradictoire puisque $x \mapsto \overline{x}$ est un anti-automorphisme alors que $x \mapsto (z^{-1}q)x(z^{-1}q)^{-1}$ est un automorphisme. Par conséquent, $s(z) \in \mathrm{SO}(\mathbf{P}, N)$.

On a donc montré que $s(\mathbf{H}^\times) \subset \mathrm{SO}(\mathbf{P}, N)$. Enfin, tout élément de $\mathrm{SO}(\mathbf{P}, N)$ est produit de renversements, et les renversements sont dans l'image de s (et même dans $s(\mathbf{P}^\times)$), donc $s(\mathbf{H}^\times) = \mathrm{SO}(\mathbf{P}, N)$.

e) C'est la conjonction des questions c) et d).

f) Pour tout $q = xi + yj + zk \in \mathbf{P}$, on a $N(q) = -x^2 - y^2 + z^2$, d'où la description de la classe d'isométrie de N. En outre, en adaptant la question b) de l'exercice 6, on voit facilement que dans le cas présent, on a un isomorphisme de K-algèbres $\mathbf{H} \cong \mathrm{Mat}_2(K)$, et donc un isomorphisme de groupes $\mathbf{H}^\times/K^* \cong \mathrm{PGL}_2(K)$. Par conséquent, la question e) fournit un isomorphisme $\mathrm{PGL}_2(K) \xrightarrow{\sim} \mathrm{SO}_3(K, N)$, et le calcul du groupe dérivé de $\mathrm{GL}_2(K)$ assure que cet isomorphisme induit l'isomorphisme suivant entre les sous-groupes dérivés :

$$\mathrm{PSL}_2(K) \xrightarrow{\sim} \Omega_3(K, N)\,.$$

g) et h) Comme à la question d), on voit facilement que pour tout $q \in \mathbf{H}^\times$, la reflexion orthogonale de droite Kq est donnée par la formule suivante : $x \mapsto \frac{-q\overline{x}q}{N(q)}$. Or tout élément de $\mathrm{SO}(\mathbf{H}, N)$ (resp. $\mathrm{O}(\mathbf{H}, N) \setminus \mathrm{SO}(\mathbf{H}, N)$) est produit d'un nombre pair (resp. impair) de reflexions orthogonales. On en déduit donc les deux formules souhaitées, en composant un nombre pair (resp. impair) de reflexions données par des formules du type $x \mapsto \frac{-q\overline{x}q}{N(q)}$, pour certains $q \in \mathbf{H}^\times$. La condition $N(a)N(b) = 1$ dans la question g) s'obtient en écrivant que $N(u(x)) = N(x)$ pour tout x.

i) Pour $(a, b) \in U$, on définit $S_{a,b} : \mathbf{H} \to \mathbf{H}$ par $S_{a,b}(q) := aqb^{-1}$. Il est clair que pour tout $(a, b) \in U$, $S_{a,b} \in \mathrm{O}(\mathbf{H}, N)$, et que l'on définit ainsi un morphisme de groupes $S : U \to \mathrm{O}(\mathbf{H}, N)$. Soit $(a, b) \in U$. Supposons que $S_{a,b} \notin \mathrm{SO}(\mathbf{H}, N)$. Alors la question h) assure qu'il existe

$c, d \in \mathbf{H}^\times$ tels que pour tout $x \in H$, on ait $S_{a,b}(x) = c\overline{x}d$. On en déduit que pour tout $x \in \mathbf{H}$, on a $c^{-1}axb^{-1}d^{-1} = \overline{x}$, relation qui implique que pour tout $x \in \mathbf{H}$, $c^{-1}axa^{-1}c = \overline{x}$, ce qui aboutit à une contradiction comme à la question d). Donc S est à valeur dans $\mathrm{SO}(\mathbf{H}, N)$. La question g) assure que l'image du morphisme de groupes S contient $\mathrm{SO}(\mathbf{H}, N)$, donc S est un bien un morphisme de groupes surjectif $\mathbf{H}^\times \to \mathrm{SO}(\mathbf{H}, N)$. Son noyau est constitué de l'ensemble des $(a, b) \in U$ tels que $axb^{-1} = x$ pour tout $x \in \mathbf{H}$, i.e. l'ensemble des $(a, b) \in U$ tels que $a = b$ (prendre $x = 1$) et a commute avec tous les éléments de $\mathbf{H}$. Donc $\mathrm{Ker}(S) = \{(\lambda, \lambda) : \lambda \in K^*\}$.

j) On voit que dans ce cas, pour tout $q = x + yi + zj + tk \in \mathbf{H}$, on a $N(q) = x^2 - y^2 - z^2 + t^2$. Donc $(\mathbf{H}, N)$ est bien somme de deux plans hyperboliques. Comme à la question f), on sait que l'on a un isomorphisme de K-algèbres $\mathbf{H} \xrightarrow{\sim} \mathrm{Mat}_2(K)$. Cet isomorphisme induit des isomorphismes de groupes $\mathbf{H}^\times \xrightarrow{\sim} \mathrm{GL}_2(K)$ et $U \xrightarrow{\sim} \{(A, B) \in \mathrm{GL}_2(K) \times \mathrm{GL}_2(K) : \det(A) = \det(B)\}$. Donc $D(U) \cong \mathrm{SL}_2(K) \times \mathrm{SL}_2(K)$ puisque $D(\mathrm{GL}_2(K)) = \mathrm{SL}_2(K)$. On en déduit via la question i) que S induit un isomorphisme $(\mathrm{SL}_2(K) \times \mathrm{SL}_2(K))/\{\pm I_2\} \xrightarrow{\sim} \Omega_4(K, N)$. En quotientant ces deux groupes par leur centre, on obtient finalement un isomorphisme

$$\mathrm{PSL}_2(K) \times \mathrm{PSL}_2(K) \xrightarrow{\sim} \mathrm{P}\Omega_4(K, N)\,.$$

Exercice 8 : $\star\star\star$

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 8.

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 2), 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 $\mathrm{P}\Omega_3(K) \cong \mathrm{PSL}_2(K)$. On remarquera que ce résultat est un cas particulier de l'exercice 7, question f).

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 2) : 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 $|K| > 3$, ce qui est un cas particulier de la question j) de l'exercice 7.

vii) On a vu que $\mathrm{SO}_4^+(\mathbb{F}_3) \cong (\mathrm{SL}_2(\mathbb{F}_3) \times \mathrm{SL}_2(\mathbb{F}_3)) \rtimes \mathbb{F}_3^*/\mathbb{F}_3^*$. 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, on en déduit que $\Omega_4^+(\mathbb{F}_3) \cong (\mathbf{H}_8 \times \mathbf{H}_8)/\{\pm 1\}$, donc $\mathrm{P}\Omega_4^+(\mathbb{F}_3) \cong (\mathbb{Z}/2\mathbb{Z})^4$.

Exercice 9 : $\star\star\star$

Soit K un corps de caractéristique $\neq 2$, V un K-espace vectoriel de dimension n et q une forme quadratique sur V.

a) On note $I(q)$ l'idéal bilatère de $T(V)$ engendré par les éléments de la forme $v\otimes v - q(v)$ pour $v \in V$. On pose $C(q) := T(V)/I(q)$. Montrer que $C(q)$ est une K-algèbre, canoniquement isomorphe à $\bigwedge V$ comme K-espace vectoriel, et admettant une décomposition $C(q) = C(q)^+ \oplus C(q)^-$ définie par le degré des éléments de $T(V)$.

b) Vérifier $C(q)^+$ est une sous-algèbre de $C(q)$.

c) Montrer que $\dim_K C(q) = 2^n$ et donner une base de $C(q)$ comme K-espace vectoriel.

d) Montrer que V se plonge naturellement dans $C(q)$.

e) Calculer $C(q)$ lorsque $K = \mathbb{R}$, $\dim_{\mathbb{R}}(V) \leq 2$. Généraliser au cas où K est quelconque et $\dim_K(V) \leq 1$.

f) Calculer le centre de $C(q)$.

g) On note $\alpha := \mathrm{id}_{C(q)^+} \oplus -\mathrm{id}_{C(q)^-} \in \mathrm{GL}_K(C(q))$ et pour tout $x \in C(q)^\times$, $\rho_x \in \mathrm{End}_K(C(q))$ défini par $\rho_x : z \mapsto \alpha(x) z x^{-1}$. Montrer que cela définit un morphisme de groupes $\rho : C(q)^\times \to \mathrm{GL}_K(C(q))$.

h) On note $\Gamma(V,q) := \{x \in C(q)^\times : \rho_x(V) \subset V\}$. Montrer que $\Gamma(V,q)$ contient les vecteurs non isotropes de (V,q).

i) On suppose q non dégénérée. Montrer que $\mathrm{Ker}(\rho) = K^*$.

j) Montrer qu'il existe un unique $t \in \mathrm{GL}_K(C(q))$ tel que $t_{|V} = \mathrm{id}_V$ et $t(xy) = t(y)t(x)$ pour tout $x, y \in C(q)$.

k) Pour tout $x \in C(q)$, on pose $\overline{x} := t(\alpha(x))$. Montrer que la formule $N(x) := x\overline{x}$ définit une application $N : C(q) \to C(q)$ induisant un morphisme de groupes $N : \Gamma(V,q) \to K^*$.

l) On suppose q non dégénérée. Montrer que $\mathrm{Im}\,(\rho) = \mathrm{O}(V,q)$.

m) On suppose q non dégénérée. Montrer que l'on dispose d'un morphisme naturel $\theta : \mathrm{O}(V,q) \to K^*/(K^*)^2$.

n) On suppose q non dégénérée et isotrope. Montrer que $\theta : \mathrm{SO}(V,q) \to K^*/(K^*)^2$ est surjectif.

o) On suppose q non dégénérée. On note $\mathrm{Pin}(V,q) := \mathrm{Ker}(N) = \{g \in \Gamma(V,q) : N(g) = 1\}$ et $\mathrm{Spin}(V,q) := \{g \in \mathrm{Pin}(V,q) : \det(\rho(g)) = 1\}$. Montrer que l'on a des suites exactes de groupes :

$$1 \to \{\pm 1\} \to \mathrm{Pin}(V,q) \xrightarrow{\rho} \mathrm{O}(V,q) \xrightarrow{\theta} K^*/(K^*)^2$$

et

$$1 \to \{\pm 1\} \to \mathrm{Spin}(V,q) \xrightarrow{\rho} \mathrm{SO}(V,q) \xrightarrow{\theta} K^*/(K^*)^2\,.$$

p) On suppose $K = \mathbb{R}$ et q non dégénérée et non définie. Montrer que $\theta : \mathrm{SO}(V,q) \to K^*/(K^*)^2$ est surjective.

q) Montrer les isomorphismes suivants : $\mathrm{Spin}_2(\mathbb{C}) \cong \mathbb{C}^*$, $\mathrm{Spin}_3(\mathbb{C}) \cong \mathrm{SL}_2(\mathbb{C})$, $\mathrm{Spin}_4(\mathbb{C}) \cong \mathrm{SL}_2(\mathbb{C}) \times \mathrm{SL}_2(\mathbb{C})$, $\mathrm{Spin}_5(\mathbb{C}) \cong \mathrm{Sp}_4(\mathbb{C})$, $\mathrm{Spin}_6(\mathbb{C}) \cong \mathrm{SL}_4(\mathbb{C})$, ainsi que $\mathrm{Spin}_2(\mathbb{R}) \cong \mathrm{U}_1(\mathbb{C})$, $\mathrm{Spin}_3(\mathbb{R}) \cong \mathrm{SU}_2(\mathbb{C})$, $\mathrm{Spin}_4(\mathbb{R}) \cong \mathrm{SU}_2(\mathbb{C}) \times \mathrm{SU}_2(\mathbb{C})$.

Solution de l'exercice 9.

a) Il est clair que $C(q)$ est naturellement une K-algèbre. Remarquons que contrairement à $\bigwedge(V)$ ou $S(V)$, l'algèbre $C(q)$ n'est en général pas naturellement $\mathbb{Z}$-graduée, puisque l'idéal $I(q)$ n'est pas homogène. On peut écrire un isomorphisme canonique de K-espaces vectoriels $C(q) \xrightarrow{\sim} \bigwedge V$ en toute caractéristique, mais cela demande quelques vérifications un peu longues. On donnera une autre version de cet isomorphisme (moins canonique) à la question c). La K-algèbre $T(V)$ est munie d'une décomposition en somme directe $T(V) = T(V)^+ \oplus T(V)^-$, où $T(V)^+$ (resp. $T(V)^-$) est le sous-espace vectoriel formé des éléments de degré pair (resp. impair). Or l'idéal $I(q)$ est engendré par des éléments de degré pair, donc cet idéal admet lui aussi une décomposition $I(q) = I(q)^+ \oplus I(q)^-$, où $I(q)^\pm := I(q) \cap T(q)^\pm$. Il est alors clair que le quotient $C(q) = T(V)/I(q)$ admet lui aussi une décomposition (en somme directe de sous-K-espaces vectoriels) de la forme $C(q) = C(q)^+ \oplus C(q)^-$, où $C(q)^+$ (resp. $C(q)^-$) est l'image de $T(V)^+$ (resp. $T(V)^-$) dans $C(q)$.

b) Comme $T(V)^+$ est une sous-K-algèbre de $T(V)$, on en déduit immédiatement que $C(q)^+$ est une sous-K-algèbre de $C(q)$. Remarquons également que $C(q)^-$ n'est pas une sous-algèbre de $C(q)$, mais que $C(q)^-$ est stable par multiplication par un élément de $C(q)^+$. On dit que $C(q)$ est une K-algèbre $\mathbb{Z}/2\mathbb{Z}$-graduée.

c) Soit $e_1, \dots, e_n$ une base de V. Par définition de $C(q)$, on a la relation suivante : pour tous $v, w \in C(q)$, $v \cdot w + w \cdot v = 2b(v, w)$. Par conséquent, tout produit $e_{i_1} \cdot \dots \cdot e_{i_r}$ peut se réécrire sous la forme d'une combinaison linéaire de produits $e_{j_1} \cdot \dots \cdot e_{j_s}$ avec $j_1 < \dots < j_s$. On en déduit donc que la famille $(e_{i_1} \cdot \dots \cdot e_{i_r})_{1 \leq i_1 < \dots < i_r \leq n}$ est une famille génératrice de $C(q)$ comme K-espace vectoriel. Donc $\dim_K C(q) \leq 2^n$.

Montrons que c'est une égalité. Pour cela, on démontre le fait suivant : si (V, q) et (V', q') sont deux espaces quadratiques, alors on a un isomorphisme canonique de K-algèbres graduées $C(q \oplus^\perp q') = C(q) \otimes^{\mathrm{su}} C(q')$. En effet, on dispose d'une application linéaire $\varphi : V \oplus V' \to C(V) \otimes C(q')$ définie par $\varphi(v \oplus v') := v \otimes 1 + 1 \otimes v'$. Or on a la relations suivante : pour tout $(v, v') \in V \times V'$, on a $\varphi(v \oplus v')^2 = q(v) + q(v') = (q \oplus^\perp q')(v \oplus v')$, donc la définition de $C(q \oplus^\perp q')$ assure que l'application φ se prolonge en un morphisme de K-algèbres graduées

$$\overline{\varphi} : C(q \oplus^\perp q') \to C(q) \otimes C(q') \,.$$

Réciproquement, les inclusions de V et V' dans $V \oplus V'$ assurent l'existence de morphismes de K-algèbres graduées $C(q), C(q') \to C(q \oplus^\perp q')$, dont on déduit (ce qui demande un petit calcul) un morphisme de K algèbres graduées $\psi : C(q) \otimes^{\mathrm{su}} C(q') \to C(q \oplus^\perp q')$. Il est alors immédiat de constater que ψ est la réciproque de $\overline{\varphi}$, ce qui conclut la preuve du fait énoncé plus haut.

Remarquons au passage que pour la calcul de la dimension et d'une base (voir ci-dessous), on a seulement besoin de la surjectivité de $\overline{\varphi}$, laquelle est évidente puisque les éléments $x \otimes 1$ et $1 \otimes x$, avec $x \in V$, $x' \in V'$, engendrent $C(q) \otimes^{\mathrm{su}} C(q')$ comme K-algèbre, et ces éléments sont clairement dans l'image de $\overline{\varphi}$.

Pour finir le calcul de la dimension, on raisonne par récurrence sur la dimension n de V. Si $n = 1$, on a $v = K$ et $q(x) = ax^2$ pour un certain $a \in K$. Si $a = 0$, on a $C(q) = \bigwedge K = K \oplus K$ qui est bien de dimension 2, et si $a \neq 0$, on voit que $T(K) \cong K[X]$ et il est évident que $C(q)$ est l'idéal de $K[X]$ engendré par $(X^2 - a)$, donc $C(q) \cong K[X]/(X^2 - a)$, qui est bien de dimension 2 sur K. Si $n > 1$, on a de nouveau deux cas : soit $q = 0$ et $C(q) \cong \bigwedge V$, auquel cas $\dim_K C(q) = 2^n$, soit $q \neq 0$, il existe $v \in V$ tel que $q(v) \neq 0$, et $V = Kv \oplus^\perp (Kv)^\perp$, donc $C(q) \cong C(q_{|Kv}) \otimes C(q_{|(Kv)^\perp})$, et l'hypothèse de récurrence assure que $\dim_K C(q) = 2.2^{n-1} = 2^n$.

Finalement, $\dim_K C(q) = 2^n$, et la famille génératrice précédente formée des $(e_{i_1} \cdot \dots \cdot e_{i_r})_{1 \leq i_1 < \dots < i_r \leq n}$ est bien une base de $C(q)$.

Remarque : il est désormais facile d'exhiber un isomorphisme de K-espaces vectoriels entre $C(q)$ et $\bigwedge V$: il suffit de faire correspondre la base $(e_{i_1} \wedge \dots \wedge e_{i_r})$ de $\bigwedge V$ avec la base $(e_{i_1} \cdot \dots \cdot e_{i_r})$ de $C(q)$...

d) On dispose du morphisme naturel $V \to T(V) \to C(q)$. On a montré à la question précédente que si (e_i) est une base de V, alors les images des vecteurs e_i dans $C(q)$ forment une famille libre. Cela assure que le morphisme naturel $V \to C(q)$ est bien injectif.

e) — On suppose d'abord $K = \mathbb{R}$. Si $n = 0$, il est clair que $C(q) \cong \mathbb{R}$. Si $n = 1$, on a montré à la question précédente que deux cas se présentaient : soit $q = 0$, et $C(q) \cong \bigwedge \mathbb{R} \cong K[X]/(X^2)$, soit $q \neq 0$ (disons $q(x) = ax^2$) et $C(q) \cong \mathbb{R}[X]/(X^2 - a)$; dans ce dernier cas, on a deux possibilités : si $a > 0$, alors $C(q) \cong \mathbb{R}^2$, et si $a > 0$, $C(q) \cong \mathbb{C}$. Enfin, si $n = 2$, limitons-nous aux formes quadratiques non dégénérées : il y a trois cas (trois signatures possibles). Si $\mathrm{sign}(q) = (2, 0)$, alors $C(q) \cong \mathrm{Mat}_2(\mathbb{R})$. Si $\mathrm{sign}(q) = (1, 1)$, alors $C(q) \cong \mathrm{Mat}_2(\mathbb{R})$. Si $\mathrm{sign}(q) = (0, 2)$, alors $C(q) \cong \mathbf{H}$, où $\mathbf{H}$ est l'algèbre des quaternions de Hamilton.

— Désormais, K est un corps quelconque. Si $n = 0$, on a $C(q) \cong K$. Si $n = 1$, on a trois possibilités : si on note $q(x) = ax^2$, soit $a = 0$ et alors $C(q) \cong \bigwedge K \cong K[X]/(X^2)$, soit $a \in (K^*)^2$ et alors $C(q) \cong K^2$, soit $a \notin (K^*)^2$ et alors $C(q) \cong K[X]/(X^2 - a) \cong K(\sqrt{(a)})$ est un corps qui est une extension quadratique de K.

f) On note $Z(q)$ le centre de l'algèbre $C(q)$. On fixe une base orthogonale (e_i) de V. Pour toute partie $I = \{i_1, \dots, i_r\} \subset \{1, \dots, n\}$, avec $i_1 < \cdots < i_r$, on note $e_I := e_{i_1} \cdot \cdots \cdot e_{i_r}$. Alors pour tout tel I et tout $j \in \{1, \dots, n\}$, on a

$$e_I \cdot e_j = \varepsilon_{I,j} e_j \cdot e_I \,,$$

où $\varepsilon_{I,j} := (-1)^{|I|}$ si $j \notin I$ et $\varepsilon_{I,j} := -(-1)^{|I|}$ si $j \in I$. Soit alors $x = \sum_I x_I e_I \in C(q)$. On a clairement $a \in Z(q)$ si et seulement si $e_j \cdot x = x \cdot e_j$ pour tout $1 \leq j \leq n$. Soit alors $j \in \{1, \dots, n\}$. En utilisant les relations de commutation susmentionnées, on obtient la caractérisation suivante : $x \cdot e_j = e_j \cdot x$ si et seulement si $x_I = 0$ pour tout I tel que ($|I|$ est pair et $j \in I$) ou ($|I|$ est impair et $j \notin I$). En faisant varier j dans $\{1, \dots, n\}$, on en déduit la dichotomie suivante :
— si n est pair : $x \in Z(q)$ si et seulement si $x_I = 0$ pour tout $I \neq \emptyset$. Donc $Z(q) = K e_\emptyset \cong K$.
— si n est impair : $x \in Z(q)$ si et seulement si $x_I = 0$ pour tout $I \neq \emptyset$ et $I \neq \{1, \dots, n\}$. Donc $Z(q) = K e_\emptyset \oplus K e_{\{1,\dots,n\}} \cong K^2$.

g) Tout d'abord, pour tout $x \in C(q)^\times$, l'application $\rho_x : C(q) \to C(q)$ est bien linéaire, et elle est inversible d'inverse $\rho_{x^{-1}}$. Donc $x \mapsto \rho_x$ définit bien une application $\rho : C(q)^\times \to \mathrm{GL}_K(C(q))$. On voit facilement que c'est un morphisme de groupes en montrant que pour tout $x, y \in C(q)$, on a $\alpha(x \cdot y) = \alpha(x) \cdot \alpha(y)$.

h) Voir cours 2015, proposition III.6.4.

i) Voir cours 2015, proposition III.6.5.

j) On définit $C'(q)$ comme la K-algèbre opposée à $C(q) : C'(q) = C(q)$ comme K-espace vectoriel, et la multiplication $\cdot'$ sur $C'(q)$ est définie par $a \cdot' b := b \cdot a$. Alors l'application naturelle $i : V \to C'(q)$ est une application linéaire telle que $i(x)^2 = q(x)$, donc par définition de $C(q)$, l'application i se prolonge en un morphisme de K-algèbres $i : C(q) \to C'(q)$ En composant ce morphisme avec l'identification $C'(q) \xrightarrow{\sim} C(q)$, on obtient une application linéaire $t : C(q) \to C(q)$ telle que $t_{|_V} = \mathrm{id}_V$ et $t(x \cdot y)t(y) \cdot t(x)$. L'unicité de t résulte de la propriété universelle de $C(q)$ qui découle de sa définition. Et l'unicité implique que t est une involution.

k) voir cours 2015, proposition III.6.6.

l) voir cours 2015, proposition III.6.7.

m) voir cours 2015, proposition III.6.8.

n) La forme q étant non dégénérée et isotrope, elle représente tous les éléments de K, i.e. l'application $q : V \to K$ est surjective. Par conséquent, soit $\lambda \in K^*$, il existe $v \in V$ tel que $q(v) = -\lambda$. Alors la question h) assure que $v \in \Gamma(V, q)$, et la définition de N assure que $N(v) = v \cdot (-v) = -q(v) = \lambda$. Mais $\rho(v)$ est une reflexion, donc $\rho(v) \in \mathrm{O}(V, q) \setminus \mathrm{SO}(V, q)$. Il suffit de multiplier v par un vecteur $v' \in V$ tel que $q(v') = -1$ (qui existe) pour obtenir un élément $x := v \cdot v' \in \Gamma(V, q)$ tel que $N(x) = \lambda$ et $\det(\rho(x)) = \det(\rho(v)) \det(\rho(v')) = (-1)(-1) = 1$, donc l'élément $\rho(x) \in \mathrm{SO}(V, q)$ vérifie que $\theta(\rho(x))$ est la classe de $N(x) = \lambda$ dans $K^*/(K^*)^2$. D'où la surjectivité souhaitée.

o) Le morphisme $\mathrm{Pin}(V, q) \to \mathrm{O}(V, q)$ est la composée de l'inclusion $\mathrm{Pin}(V, q) \subset \Gamma(V, q)$ avec le morphisme $\rho : \Gamma(V, q) \to \mathrm{O}(V, q)$. Par conséquent, le noyau de $\mathrm{Pin}(V, q) \to \mathrm{O}(V, q)$ est exactement

$$\mathrm{Ker}(\rho) \cap \mathrm{Pin}(V, q) = X^* \cap \mathrm{Pin}(V, q) = \{x \in K^* : N(x) = 1\} = \{x \in K^* : x^2 = 1\} = \{\pm 1\} \,.$$

Cela assure que la suite suivante (dont les morphismes sont les morphismes naturels)

$$1 \to \{\pm 1\} \to \mathrm{Pin}(V, q) \xrightarrow{\rho} \mathrm{O}(V, q)$$

est exacte. En outre, soit $y \in \mathrm{Ker}(\theta : \mathrm{O}(V, q) \to K^*/(K^*)^2)$: par surjectivité de ρ (voir question k)), il existe $x \in \Gamma(V, q)$ tel que $\rho(x) = y$. Alors par construction de θ (voir question m)), on a $\theta(y) = N(x) \bmod (K^*)^2$. Comme $\theta(y) = 1 \in K^*/(K^*)^2$, il existe $t \in K^*$ tel que $N(x) = t^2$. Alors on a $\rho(t^{-1}x) = \rho(x) = y$ car $K^* = \mathrm{Ker}(\rho)$ et $N(t^{-1}x) = 1 \in K^*$, donc $t^{-1}x \in \mathrm{Pin}(V, q)$.

On a donc montré que $y = \rho(t^{-1}x) \in \rho(\mathrm{Pin}(V,q))$, donc $\mathrm{Ker}(\theta) \subset \rho(\mathrm{Pin}(V,q))$. L'inclusion inverse étant évidente, cela termine la preuve de l'exactitude de la suite

$$1 \to \{\pm 1\} \to \mathrm{Pin}(V,q) \xrightarrow{\rho} \mathrm{O}(V,q) \xrightarrow{\theta} K^*/(K^*)^2\,.$$

La seconde suite exacte se déduit immédiatement de celle-ci, en remarquant que $\mathrm{Spin}(V,q) = \mathrm{Pin}(V,q) \cap \rho^{-1}(\mathrm{SO}(V,q))$.

p) C'est une conséquence directe de la question n).

q) Les détails sont laissés au lecteur courageux...

Exercice 10 :
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 $x_0 := (1,\dots,1) \in V$.

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 10.

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 2). 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 11 : $\star\star\star$
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 11.

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.

Exercice 12 :
Déterminer les groupes unitaires, orthogonaux et symplectiques en dimension 1 et 2.

Solution de l'exercice 12. Voir cours.

Exercice 13 : $\star\star\star$
Soient p un nombre premier impair, $f \geq 1$ et $q = p^f$. Soit b la forme sur $(\mathbb{F}_{q^2})^3 \times (\mathbb{F}_{q^2})^3$ définie par $b(u, v) = u_1v_3^q + u_2v_2^q + u_3v_1^q$

a) Déterminer l'ensemble Δ des droites isotropes de b. Quel est le cardinal de Δ ?

b) Notons (e_1, e_2, e_3) la base canonique de $(\mathbb{F}_{q^2})^3$. On définit aussi les éléments $t_{\alpha,\beta}$ et $h_{\gamma,\delta}$ de $\mathrm{PU}_3(\mathbb{F}_{q^2})$ correspondant respectivement aux matrices

$$\begin{pmatrix} 1 & -\beta^q & \alpha \\ 0 & 1 & \beta \\ 0 & 0 & 1 \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} \gamma & 0 & 0 \\ 0 & \delta & 0 \\ 0 & 0 & \gamma^{-q} \end{pmatrix}$$

avec les conditions $\delta^{1+q} = 1$, $\gamma \neq 0$, $\alpha + \alpha^q + \beta^{1+q} = 0$. Déterminer le stabilisateur de e_1 dans $\mathrm{PU}_3(\mathbb{F}_{q^2})$ et montrer que $T := \{t_{\alpha,\beta} \mid \alpha + \alpha^q + \beta^{1+q} = 0\}$ en est un sous-groupe distingué.

c) Montrer que l'action de $\mathrm{PSU}_3(\mathbb{F}_{q^2})$ sur Δ est 2-transitive.

d) Calculer le sous-groupe dérivé T_{e_1} de T.

e) On appelle transvection unitaire de $(\mathbb{F}_{q^2})^3$ toute transvection de $(\mathbb{F}_{q^2})^3$ préservant la forme b. Montrer que $u \in \mathrm{U}_3(\mathbb{F}_{q^2})$ est une transvection unitaire si et seulement si il existe $\alpha \in \mathbb{F}_{q^2}$ vérifiant $\alpha + \alpha^q = 0$ et $a \in (\mathbb{F}_{q^2})^3$ isotrope tels que pour tout $x \in (\mathbb{F}_{q^2})^3$, on ait $u(x) = x + \alpha b(a,x)a$ (on dit que u est une transvection unitaire de vecteur a).

f) Pour tout vecteur isotrope a, montrer que l'ensemble T_a des transvections unitaires de vecteur a forme un sous-groupe abélien distingué dans le stabilisateur de a sous $\mathrm{SU}_3(\mathbb{F}_{q^2})$.

g) Montrer que toute transvection unitaire est un commutateur dans $\mathrm{SU}_3(\mathbb{F}_{q^2})$.

h) Montrer que le sous-groupe de $\mathrm{SU}_3(\mathbb{F}_{q^2})$ engendré par les transvections unitaires agit transitivement sur $\{x \in (\mathbb{F}_{q^2})^3 : b(x,x) = 1\}$.

i) Montrer que $\mathrm{SU}_3(\mathbb{F}_{q^2})$ est engendré par les transvections unitaires.

j) Montrer que $\mathrm{PSU}_3(\mathbb{F}_{q^2})$ est un groupe simple.

Solution de l'exercice 13.

a) Un petit calcul montre que les droites isotropes sont $ke_1 = k(1,0,0)$ et les $k(\alpha,\beta,1)$ avec $\alpha + \alpha^q + \beta^{1+q} = 0$. Le nombre de solutions de cette équation est $q^2 \cdot q = q^3$ (car l'application $\mathbb{F}_{q^2} \to \mathbb{F}_q$ définie par $x \mapsto x^{1+q}$ est surjective et l'application $\begin{array}{ccc} \mathbb{F}_{q^2} & \to & \mathbb{F}_q \\ x & \mapsto & x + x^q \end{array}$ est $\mathbb{F}_q$-linéaire).
Le cardinal de Δ est donc $q^3 + 1$.

b) On vérifie d'abord que les $t_{\alpha,\beta}$ et $h_{\gamma,\delta}$ stabilisent bien ke_1. Notons respectivement T et H les sous-groupes de $\mathrm{PU}_3(\mathbb{F}_{q^2})$ engendrés par les $t_{\alpha,\beta}$ et les $h_{\gamma,\delta}$: ils forment un produit semi-direct $T \rtimes H$ (la vérification est laissée au lecteur).
L'image réciproque de $T \rtimes H$ dans $\mathrm{U}_3(\mathbb{F}_{q^2})$ est de cardinal $q^3 \cdot (q^2-1)(q+1)$. De plus, l'action de $\mathrm{U}_3(\mathbb{F}_{q^2})$ sur Δ étant transitive, on a

$$|\mathrm{Stab}_{\mathrm{U}_3}(ke_1)| = |\mathrm{U}_3(\mathbb{F}_{q^2})| \cdot |\Delta|^{-1} = q^3(q^2-1)(q+1)\,.$$

Ceci montre que le stabilisateur de ke_1 dans $\mathrm{PU}_3(\mathbb{F}_{q^2})$ est exactement le groupe $T \rtimes H$.

c) Un petit calcul montre que l'action de $T \subset \mathrm{PSU}_3(\mathbb{F}_{q^2})$ est transitive sur $\Delta \setminus \{ke_1\}$. Or $\mathrm{SU}_3(\mathbb{F}_{q^2})$ agit transitivement sur Δ, donc on en déduit facilement que $\mathrm{PSU}_3(\mathbb{F}_q^2)$ agit 2 fois transitivement sur Δ.

d) On calcule que $t_{\alpha,\beta} \cdot t_{\alpha',\beta'} = t_{\alpha+\alpha'-\beta^q\beta',\beta+\beta'}$. Donc $[t_{\alpha,\beta}, t_{\alpha',\beta'}] = t_{\beta\beta'^q-\beta'\beta^q,0}$. On en déduit que $T_{e_1} := D(T)$ est le groupe formé des matrices

$$\begin{pmatrix} 1 & 0 & \alpha \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

avec $\alpha \in \mathbb{F}_{q^2}$ tel que $\alpha^q = -\alpha$. C'est le groupe des transvections unitaires de T.

e) Soit $u \in \mathrm{U}_3(\mathbb{F}_{q^2})$ une transvection de vecteur $a \in (\mathbb{F}_{q^2})^3$. Alors il existe une forme linéaire f non nulle telle que pour tout $x \in (\mathbb{F}_{q^2})^3$, $u(x) = x + f(x)a$, avec $f(a) = 0$. Puisque u est unitaire, on a, pour tous $x, y \in (\mathbb{F}_{q^2})^3$, $b(u(x), u(y)) = b(x,y)$, i.e.

$$\overline{b(a,x)}f(y) + b(a,y)\overline{f(x)} + b(a,a)f(y)\overline{f(x)} = 0\,.$$

Donc en prenant $y = a$ et x quelconque, on voit que $b(a,a) = 0$ (car $f \neq 0$). Et en choisissant x tel que $b(a,x) = 1$, en posant $\alpha := -\overline{f(x)}$, on obtient que pour tout y, $f(y) = \alpha b(a,y)$. En outre, pour y tel que $b(a,y) = 1$, on constate que $\alpha + \overline{\alpha} = 0$.
Par conséquent, pour toute transvection unitaire u de $(\mathbb{F}_{q^2})^3$, il existe un vecteur isotrope a et $\alpha \in \mathbb{F}_{q^2}$ tel que $\alpha + \overline{\alpha} = 0$ de sorte que pour tout $x \in (\mathbb{F}_{q^2})^3$,

$$u(x) = x + \alpha b(a,x)a\,.$$

Réciproquement, il est clair qu'une telle donnée définit une transvection unitaire.

f) On peut toujours compléter le vecteur isotrope a en un plan hyperbolique de base hyperbolique (a, c). Ensuite, on complète la famille (a, c) en une base (a, b, c) de $(\mathbb{F}_{q^2})^3$ avec un vecteur b orthogonal à a et c et de norme 1. On est alors ramené via ce changement de bases aux calculs des questions a),b),c),d). D'où le résultat souhaité.

g) Cela résulte des questions e), f), et des calculs de commutateurs de la question d).

h) Soient x et y deux vecteurs tels que $b(x, x) = b(y, y) = 1$. Si la restriction de b au sous-espace engendré par x et y est non dégénérée, alors un calcul dans $\mathrm{SU}_2(\mathbb{F}_{q^2}) \cong \mathrm{SL}_2(\mathbb{F}_q)$ assure le résultat. Si b restreinte à $\mathrm{vect}(x, y)$ est dégénérée, on peut trouver z tel que les plans $\mathrm{vect}(x, z)$ et $\mathrm{vect}(y, z)$ soient non dégénérés (prendre par exemple un vecteur isotrope $z \notin \mathrm{vect}(x, y)$, non orthogonal à x, ni à y). Alors on conclut par le cas précédent en composant deux transvections unitaires.

i) Pour tout x tel que $b(x, x) = 1$, le stabilisateur de x dans $\mathrm{SU}_3(\mathbb{F}_{q^2})$ est isomorphe à $\mathrm{SU}(x^\perp, b) \cong \mathrm{SU}_2(\mathbb{F}_{q^2})$. Or $\mathrm{SU}_2(\mathbb{F}_{q^2})$ est engendré par les transvections unitaires, donc la question h) assure que $\mathrm{SU}_3(\mathbb{F}_{q^2})$ est engendré par les transvections unitaires.

j) La question c) assure que le groupe $\mathrm{PSU}_3(\mathbb{F}_{q^2})$ agit primitivement sur Δ. Pour tout $d \in \Delta$, on pose T_d l'image de T_a dans $\mathrm{PSU}_3(\mathbb{F}_{q^2})$, où a est un vecteur directeur de d. La question f) assure que pour tout $d \in \Delta$, T_d est un sous-groupe abélien de $\mathrm{PSU}_3(\mathbb{F}_{q^2})$, distingué dans le stabilisateur de d. Et la question i) assure que $\mathrm{PSU}_3(\mathbb{F}_{q^2})$ est engendré par la réunion des T_d, $d \in \Delta$. Par conséquent, le théorème d'Iwasawa assure que tout sous-groupe distingué de $\mathrm{PSU}_3(\mathbb{F}_{q^2})$ agissant non trivialement sur Δ contient $D(\mathrm{PSU}_3(\mathbb{F}_{q^2}))$. Or les questions g) et i) assurent que $D(\mathrm{PSU}_3(\mathbb{F}_{q^2})) = \mathrm{PSU}_3(\mathbb{F}_{q^2})$, donc cela démontre que le groupe $\mathrm{PSU}_3(\mathbb{F}_{q^2})$ est un groupe simple.

Exercice 14 : $\star\star\star$

Soient p un nombre premier impair, $r \geq 1$ et $q = p^r$.

a) On note $V_1, V_2 := (\mathbb{F}_{q^2})^2$, et (e_i, f_i) la base canonique de V_i. On munit $V := V_1 \otimes_{\mathbb{F}_{q^2}} V_2$ de la forme bilinéaire symétrique b définie par $b(v_1 \otimes v_2, v_1' \otimes v_2') := b_1(v_1, v_1')b_2(v_2, v_2')$, où b_i est la forme bilinéaire alternée sur V_i telle que $b_i((1, 0), (0, 1)) = 1$. On pose enfin

$$V' := \mathrm{Vect}_{\mathbb{F}_p}\{e_1 \otimes e_2, f_1 \otimes f_2, \lambda e_1 \otimes f_2 + \overline{\lambda} f_1 \otimes e_2 : \lambda \in \mathbb{F}_{q^2}\} \subset V\,.$$

i) Montrer que $\dim_{\mathbb{F}_p} V' = 4$.

ii) Construire un morphisme de groupes $\mathrm{SL}_2(\mathbb{F}_{q^2}) \to \mathrm{O}(V', b)$.

iii) En déduire un isomorphisme de groupes $\mathrm{P}\Omega_4^-(\mathbb{F}_q) \cong \mathrm{PSL}_2(\mathbb{F}_{q^2})$.

b) On note (e_i) la base canonique de $\mathbb{F}_q^4$ et on note $W := \bigwedge^2(\mathbb{F}_q^4)$.

i) Quelle est la dimension de W comme $\mathbb{F}_q$-espace vectoriel ?

ii) Montrer que W est muni d'une forme bilinéaire symétrique non dégénérée naturelle f telle que pour tout $\sigma : \{1, 2, 3, 4\} \to \{1, 2, 3, 4\}$, $f(e_{\sigma(1)} \wedge e_{\sigma(2)}, e_{\sigma(3)} \wedge e_{\sigma(4)}) = \varepsilon(\sigma)$, avec par convention $\varepsilon(\sigma) = 0$ si σ n'est pas bijective.

iii) Montrer que $\mathrm{GL}_4(\mathbb{F}_q)$ agit naturellement sur W.

iv) Construire un morphisme de groupes $\mathrm{SL}_4(\mathbb{F}_q) \to \mathrm{O}(W, f)$.

v) En déduire un isomorphisme $\mathrm{P}\Omega_6^+(\mathbb{F}_q) \cong \mathrm{PSL}_4(\mathbb{F}_q)$.

c) On note (e_1, e_2, e_3, e_4) une base orthonormée pour la forme sesquilinéaire naturelle sur $X := (\mathbb{F}_{q^2})^4$, et $X' \subset \bigwedge^2 X$ le sous-$\mathbb{F}_q$-espace vectoriel engendré par les vecteurs $\lambda e_{\sigma(1)} \wedge e_{\sigma(2)} + \overline{\lambda} e_{\sigma(3)} \wedge e_{\sigma(4)}$, pour tout $\sigma \in \mathfrak{A}_4$ et $\lambda \in \mathbb{F}_{q^2}$.

i) Montrer que $\dim_{\mathbb{F}_q} X' = 6$.

ii) Montrer que X' est muni d'une forme bilinéaire symétrique f telle que pour tout $\sigma \in \mathfrak{A}_4$, $\lambda, \mu \in \mathbb{F}_{q^2}$,

$$f(\lambda e_{\sigma(1)} \wedge e_{\sigma(2)} + \overline{\lambda} e_{\sigma(3)} \wedge e_{\sigma(4)}, \mu e_{\sigma(1)} \wedge e_{\sigma(2)} + \overline{\mu} e_{\sigma(3)} \wedge e_{\sigma(4)}) = \lambda\overline{\mu} + \overline{\lambda}\mu\,.$$

iii) Construire un morphisme de groupes $\mathrm{SU}_4(\mathbb{F}_{q^2}) \to \mathrm{O}(X', f)$.

iv) En déduire un isomorphisme de groupes $\mathrm{P}\Omega_6^-(\mathbb{F}_q) \cong \mathrm{PSU}_4(\mathbb{F}_{q^2})$.

Solution de l'exercice 14.

a) i) On fixe un élément $\varepsilon \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. On vérifie facilement que V' est un $\mathbb{F}_p$-espace vectoriel de dimension 4, dont une base est $e_1 \otimes e_2, f_1 \otimes f_2, e_1 \otimes f_2 + f_1 \otimes e_2, \varepsilon e_1 \otimes f_2 + \overline{\varepsilon} f_1 \otimes e_2$.

ii) On considère la représentation de $\mathrm{SL}_2(\mathbb{F}_{q^2})$ sur V définie par l'action diagonale $g \cdot (v_1 \otimes v_2) := g(v_1) \otimes \overline{g}(v_2)$. Montrons que le sous-$\mathbb{F}_p$-espace vectoriel $V' \subset V$ est stable par cette action. Comme $\mathrm{SL}_2(\mathbb{F}_{q^2})$ est engendré par les transvections, il suffit de montrer que V' est stable par les transvections. Pour cela, il suffit de considérer l'élément $g = \begin{pmatrix} 1 & 0 \\ \lambda & 1 \end{pmatrix}$ (dans la base (e_i, f_i) de V_i), avec $\lambda \in \mathbb{F}_{q^2}$. On a alors

$$g \cdot (e_1 \wedge e_2) = (e_1 + \lambda f_1) \otimes (e_2 + \overline{\lambda} f_2) = e_1 \otimes e_2 + (\lambda f_1 \otimes e_2 + \overline{\lambda} e_1 \otimes f_2) + \lambda\overline{\lambda} f_1 \otimes f_2 \in V'$$

car $\lambda\overline{\lambda} \in \mathbb{F}_q$. De même,

$$g \cdot (f_1 \otimes f_2) = f_1 \otimes f_2 \in V' \,,$$

et

$$g \cdot (\varepsilon e_1 \otimes f_2 + \overline{\varepsilon} f_1 \otimes e_2) = (\varepsilon\lambda + \overline{\varepsilon}\overline{\lambda}) f_1 \otimes f_2 + (\varepsilon e_1 \otimes f_2 + \overline{\varepsilon} f_1 \otimes e_2) \in V'$$

car $\varepsilon\lambda + \overline{\varepsilon}\overline{\lambda} \in \mathbb{F}_q$.

Donc $V' \subset V$ est stable par $\mathrm{SL}_2(\mathbb{F}_{q^2})$. On a donc un morphisme de groupes naturel $\mathrm{SL}_2(\mathbb{F}_{q^2}) \to \mathrm{GL}(V')$.

Soit alors $g = \begin{pmatrix} 1 & 0 \\ \lambda & 1 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{F}_{q^2})$. Si on note q la forme quadratique associée à b, on a

$$q(g \cdot (e_1 \otimes e_2)) = q(e_1 \otimes e_2 + (\lambda f_1 \otimes e_2 + \overline{\lambda} e_1 \otimes f_2) + \lambda\overline{\lambda} f_1 \otimes f_2) = -2\lambda\overline{\lambda} + 2\lambda\overline{\lambda} = 0 = q(e_1 \otimes e_2)$$

et

$$q(g \cdot (f_1 \otimes f_2)) = q(f_1 \otimes f_2)$$

et

$$q(g \cdot (\varepsilon e_1 \otimes f_2 + \overline{\varepsilon} f_1 \otimes e_2)) = q((\varepsilon\lambda + \overline{\varepsilon}\overline{\lambda}) f_1 \otimes f_2 + (\varepsilon e_1 \otimes f_2 + \overline{\varepsilon} f_1 \otimes e_2)) = -2\varepsilon\overline{\varepsilon} = q(\varepsilon e_1 \otimes f_2 + \overline{\varepsilon} f_1 \otimes e_2) \,.$$

Cela assure que les éléments de $\mathrm{SL}_2(\mathbb{F}_{q^2})$ agissant sur V' préservent la forme b, donc le morphisme précédent est en fait un morphisme $\rho : \mathrm{SL}_2(\mathbb{F}_{q^2}) \to \mathrm{O}(V', b)$, comme souhaité.

iii) Un calcul simple assure que le noyau du morphisme ρ construit à la question précédente est $\{\pm I_2\}$. Le calcul du groupe dérivé de $\mathrm{SL}_2(\mathbb{F}_{q^2})$ assure que le morphisme ρ est à valeurs dans $\Omega(V', b)$. Donc ce morphisme induit un morphisme injectif $\overline{\rho} : \mathrm{PSL}_2(\mathbb{F}_{q^2}) \to \Omega(V', b)$. Un calcul de cardinaux assure alors que ce morphisme induit un isomorphisme $\mathrm{PSL}_2(\mathbb{F}_{q^2}) \xrightarrow{\sim} \mathrm{P}\Omega(V', b)$. Enfin, on vérifie facilement que la forme bilinéaire symétrique b est de type $-$, et par conséquent le groupe $\mathrm{P}\Omega(V', b)$ s'identifie au groupe $\mathrm{P}\Omega_4^+(\mathbb{F}_q)$, ce qui conclut la preuve.

b) i) On sait que W est de dimension $\binom{4}{2} = 6$ sur $\mathbb{F}_p$.

ii) On définit la forme f sur la base $(e_i \wedge e_j)_{i<j}$ de W, de la façon suivante : on pose $f(e_i \wedge e_j, e_k \wedge e_k) := 1$ si la permutation $(i\,j\,k\,l)$ est paire, $f(e_i \wedge e_j, e_k \wedge e_k) := -1$ si cette permutation est impaire, et $f(e_i \wedge e_j, e_k \wedge e_k) := 0$ sinon. Il est clair que cela définit une forme bilinéaire symétrique non dégénérée vérifiant la propriété souhaitée.

iii) Il suffit de considérer l'action diagonale de $\mathrm{GL}_4(\mathbb{F}_q)$ sur W donnée par $g \cdot (x \wedge y) := g(x) \wedge g(y)$.

iv) On a construit à la question précédente un morphisme de groupes $\mathrm{SL}_4(\mathbb{F}_q) \to \mathrm{GL}(W)$. Montrons que les éléments de $\mathrm{SL}_4(\mathbb{F}_q)$ agissant sur W préservent la forme bilinéaire f. Pour cela, on considère la transvection $g = \begin{pmatrix} 1 & 0 & 0 & 0 \\ \lambda & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \in \mathrm{SL}_4(\mathbb{F}_q)$. On a alors $g \cdot (e_1 \wedge e_3) =$

$e_1 \wedge e_3 + \lambda e_2 \wedge e_3$ et $g \cdot (e_1 \wedge e_4) = e_1 \wedge e_4 + \lambda e_2 \wedge e_4$, et $g \cdot (e_i \wedge e_j) = e_i \wedge e_j$ sinon. Par conséquent, un calcul simple assure que l'on a $f(g \cdot (e_1 \wedge e_3), g \cdot (e_1 \wedge e_4)) = f(e_1 \wedge e_3 + \lambda e_2 \wedge e_3, e_1 \wedge e_4 + \lambda e_2 \wedge e_4) = \lambda - \lambda = 0 = f(e_1 \wedge e_3, e_1 \wedge e_4)$, et de même, pour tout i, j, k, l, on a $f(g \cdot (e_i \wedge e_j), g \cdot (e_k \wedge e_l)) = f(e_i \wedge e_j, e_k \wedge e_l)$. Comme les transvections engendrent $\mathrm{SL}_4(\mathbb{F}_q)$, on en déduit que l'action de $\mathrm{SL}_4(\mathbb{F}_q)$ sur W préserve la forme bilinéaire f. Par conséquent, l'action de la question précédente induit un morphisme naturel

$$\rho : \mathrm{SL}_4(\mathbb{F}_q) \to \mathrm{O}(W, f)\,.$$

v) On vérifie que $\mathrm{Ker}(\rho) = \{\pm I_4\}$, que la forme quadratique associée à f est de type $+$, et alors le calcul du groupe dérivé de $\mathrm{SL}_4(\mathbb{F}_q)$ assure que le morphisme ρ induit un morphisme de groupes injectif

$$\overline{\rho} : \mathrm{PSL}_4(\mathbb{F}_q) \to \mathrm{P}\Omega(W, f) \cong \mathrm{P}\Omega_6^+(\mathbb{F}_q)\,.$$

Un argument de cardinalité assure alors que ce morphisme est un isomorphisme.

c) i) On note ε un élément fixé de $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$. On vérifie qu'une base de X' est donnée les vecteurs

$$e_1 \wedge e_2 + e_3 \wedge e_4\,,\ e_1 \wedge e_3 + e_4 \wedge e_2\,,\ e_1 \wedge e_4 + e_2 \wedge e_3\,,\ \varepsilon e_1 \wedge e_2 + \overline{\varepsilon} e_3 \wedge e_4\,,\ \varepsilon e_1 \wedge e_2 + \overline{\varepsilon} e_3 \wedge e_4\,,\ \varepsilon e_1 \wedge e_2 + \overline{\varepsilon} e_3 \wedge e_4\,.$$

Par conséquent, $\dim_{\mathbb{F}_q} X' = 6$.

ii) On introduit la forme f comme la somme orthogonale des trois formes naturelles suivantes définies sur les trois $\mathbb{F}_q$-plans en somme directe $\{\lambda e_i \wedge e_j + \overline{\lambda} e_k \wedge e_l : \lambda \in \mathbb{F}_{q^2}\}$ (pour $(i, j, k, l) = (1, 2, 3, 4)$, $(1, 3, 4, 2)$ et $(1, 4, 2, 3)$), par les formules suivantes

$$f(\lambda e_i \wedge e_j + \overline{\lambda} e_k \wedge e_l, \mu e_i \wedge e_j + \overline{\mu} e_k \wedge e_l) := \lambda\overline{\mu} + \overline{\lambda}\mu\,.$$

Remarquons que la restriction de f à chacun de ces trois plans (deux-à-eux orthogonaux) est une forme quadratique non dégénérée de type $-$, donc f est une forme quadratique non dégénérée de type $-$ sur X'.

iii) On dispose de l'action naturelle de $\mathrm{SU}_4(\mathbb{F}_{q^2})$ sur $\bigwedge^2 X$ définie par $g \cdot (x \wedge y) := g(x) \wedge g(y)$. Or on vérifie que $\mathrm{SU}_4(\mathbb{F}_{q^2})$ est engendré par les matrices de permutation des vecteurs e_i, ainsi que par les matrices correspondant aux applications définies par $e_1 \mapsto \alpha e_1 + \beta e_2$, $e_2 \mapsto -\overline{\beta} e_1 + \overline{\alpha} e_2$, avec $\alpha, \beta \in \mathbb{F}_{q^2}$ tels que $\alpha\overline{\alpha} + \beta\overline{\beta} = 1$. Or un calcul élémentaire assure que ces éléments de $\mathrm{SU}_4(\mathbb{F}_{q^2})$ préservent tous le sous-espace X' de $\bigwedge^2 X$, et qu'ils laissent également la forme quadratique f invariante. Par conséquent, l'action susmentionnée de $\mathrm{SU}_4(\mathbb{F}_{q^2})$ sur $\bigwedge^2 X$ induit un morphisme de groupes

$$\rho : \mathrm{SU}_4(\mathbb{F}_{q^2}) \to \mathrm{O}(X', f)\,.$$

iv) On voit que $\mathrm{Ker}(\rho) = \{\pm I_4\}$, et le calcul du sous-groupe dérivé de $\mathrm{SU}_4(\mathbb{F}_{q^2})$ assure que le morphisme ρ induit un morphisme de groupes injectif

$$\overline{\rho} : \mathrm{PSU}_4(\mathbb{F}_{q^2}) \to \mathrm{P}\Omega(X', f) \cong \mathrm{P}\Omega_6^-(\mathbb{F}_q)\,.$$

Un calcul de cardinaux assure alors que le morphisme $\overline{\rho}$ est un isomorphisme.