École normale supérieure Année 2014-2015

Algèbre 1

Feuille d'exercices 8

Exercice 1 Soit $\mathbf{F}_q$ un corps fini à q éléments, de caractéristique différente de 2. Soient $n \geq 1$, $b \in \mathbf{F}_q$ et $d \in \mathbf{F}_q^\times / \mathbf{F}_q^{\times 2}$. Notons $S(2n, b)$, $S(2n+1, b)$ et $S_d(2n, b)$ le nombre respectif de solutions des équations

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

Montrer

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

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

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

En déduire

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

Exercice 2 Soit V un $\mathbf{R}$-espace vectoriel de dimension finie n et soit f une forme quadratique sur V. Soient $\mathscr{B}_1$ et $\mathscr{B}_2$ des bases de V telles que la matrice de f dans ces bases soit respectivement

$$\operatorname{diag}(b_1, \ldots, b_p, -b_{p+1}, \ldots, -b_r, 0, \ldots 0),$$
$$\operatorname{diag}(d_1, \ldots, d_s, -d_{s+1}, \ldots, -d_r, 0, \ldots 0),$$

avec $d_i, b_i > 0$ pour tout $1 \leq i \leq r$. Montrer que $p = s$.

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

1. Montrer que, si N contient un renversement, $N = \mathrm{SO}(V, f)$.
2. Soit N_0 la composante connexe de l'identité de N. Montrer que N_0 est un sous-groupe distingué de $\mathrm{SO}(V, f)$.
3. Montrer que $N = \{\mathrm{Id}\}$ si et seulement si $N_0 = \{\mathrm{Id}\}$.
4. 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.
5. Montrer qu'il existe $g \in N_0$ tel que $\phi(g) \leq 0$.
6. Montrer qu'il existe $g \in N_0$ tel que $\phi(g) = 0$.
7. Conclure.

Exercice 4 Soit V un $\mathbf{R}$-espace vectoriel de dimension $n \geq 5$ muni de la forme quadratique définie positive $f : (x_1, \ldots, x_n) \mapsto x_1^2 + \cdots + x_n^2$. Let 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.

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

Exercice 5 Soit $\mathbf{K}$ un corps de caractéristique différente de 2 et soit $m \geq 3$. On pose $V = \mathbf{K}^{2m}$, muni de la forme bilinéaire alternée usuelle B ; on note $\mathrm{Sp}_{2m}(\mathbf{K})$ le groupe correspondant. Soient $s, t \in \mathrm{Sp}_{2m}(\mathbf{K})$ des involutions.

1. Montrer que l'on peut écrire 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.
2. En déduire une bijection entre l'ensemble des involutions de $\mathrm{Sp}_{2m}(\mathbf{K})$ 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.

3. En considérant les familles commutatives maximales d'involutions conjuguées dans $\mathrm{Sp}_{2m}(\mathbf{K})$, montrer que tout automorphisme de $\mathrm{Sp}_{2m}(\mathbf{K})$ 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 $\mathscr{S} \subseteq \mathrm{Sp}_{2m}(\mathbf{K})$ est un ensemble d'involutions extrémales, on note $C(\mathscr{S})$ l'ensemble des involutions extrémales qui commutent à tout élément de $\mathscr{S}$.

4. 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 $C(C(\{s,t\})) = C(C(\{s',t'\}))$).
5. 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 $\phi : \mathbf{K}^n \to \mathbf{K}^n$ est dite semi-linéaire s'il existe un automorphisme de corps $\theta : \mathbf{K} \to \mathbf{K}$ tel que ϕ soit θ-linéaire, c'est-à-dire :

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

L'ensemble des applications semi-linéraires inversibles forment un groupe, noté $\Gamma\mathrm{L}_n(\mathbf{K})$ et appelé le groupe des transformations semi-linéaires de $\mathbf{K}^n$.
On admet le théorème fondamental de la géométrie projective, qui est l'énoncé suivant : *soit $\phi : \mathbf{P}^n(\mathbf{K}) \to \mathbf{P}^n(\mathbf{K})$ une bijection telle que trois points A_1, A_2, A_3 de $\mathbf{P}^n(\mathbf{K})$ sont alignés si et seulement si $\phi(A_1), \phi(A_2), \phi(A_3)$ le sont. Alors il existe un automorphisme de corps $\sigma : \mathbf{K} \to \mathbf{K}$ et une transformation σ-linéaire $\gamma \in \Gamma\mathrm{L}_{n+1}(\mathbf{K})$ telle que ϕ soit induite par γ.*
On définit enfin $\Gamma\mathrm{Sp}_{2m}(\mathbf{K})$ comme le sous-groupe de $\Gamma\mathrm{L}_{2m}(\mathbf{K})$ des éléments préservant la forme B.

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