École normale supérieure Année 2014-2015
Algèbre 1

Feuille d'exercices 8

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

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

Montrons $S(2,b)$. 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

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

Montrons enfin $S_d(2,b)$. Soit $\mathbf{K} = \mathbf{F}_q[\sqrt{d}]$. On a $\mathbf{K} \simeq \mathbf{F}_{q^2}$ et les éléments de $\mathbf{K}$ s'écrivent sous la forme $x + y\sqrt{d}$, avec $x, y \in \mathbf{F}_q$. On définit la norme $N(x + y\sqrt{d}) = x^2 - dy^2$. On déduit que $S_d(2,b)$ est le nombre d'éléments de $\mathbf{K}$ de norme b. Or $N : \mathbf{K}^{\times} \to \mathbf{F}_q^{\times}$ est un morphisme de groupes surjectif, son noyau a cardinal $q+1$. On déduit que $S_d(2,b) = q+1$. Montrons maintenant la formule (1). Les solutions à (1) sont les solutions à

$$x_1^2 - y_1^2 + \cdots + x_{n-1}^2 - y_{n-1}^2 = a, \qquad x_n^2 - y_n^2 = b - a, \qquad a \in \mathbf{F}_q. \tag{0.1}$$

Si $b = 0$, ce nombre vaut

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

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

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

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

Montrons $|\,\mathrm{O}^+_{2n}(\mathbf{F}_q)| = 2q^{n(n-1)}(q^n-1)\prod_{i=1}^{n-1}(q^{2i}-1)$ (les autres formules se prouvent de façon analogue. Le cas où $n=1$ a été fait en cours (et le cas $n=0$?). 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 $\mathrm{O}^+_{2n}(\mathbf{F}_q) = \mathrm{O}_{2n}(Q,\mathbf{F}_q)$. Soit $v \in \mathbf{F}_q^{2n}$ tel que $Q(v)=1$. Il est facile de voir que l'orbite de v sous l'action de $\mathrm{O}_{2n}(Q,\mathbf{F}_q)$ est l'ensemble des $w \in \mathbf{F}_q^{2n}$ tels que $Q(w)=1$ (pensez à vous ramener à un espace de dimension 2...)
On a donc $|\mathrm{Orb}(v)| = S(2n,1) = q^{2n-1}-q^{n-1}$. D'un autre côté, puisque $\mathbf{F}_q^{2n} = \langle v\rangle \oplus \langle v\rangle^\perp$, on a $\mathrm{Stab}(v) = \mathrm{O}(\langle v\rangle^\perp) = \mathrm{O}_{2n-1}(\mathbf{F}_q)$.
On déduit

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

Exercice 2 Notons $(v_1,\ldots,v_n)$ et $(w_1,\ldots,w_n)$ les bases $\mathscr{B}_1$ et $\mathscr{B}_2$. Soit $V_1 = \langle v_1,\ldots,v_p\rangle$ et $V_2 = \langle w_s,\ldots,v_n\rangle$. Si $v \in V_1$, on a $f(v) > 0$ et si $v \in V_2$, on a $f(v) \leq 0$. On déduit que $V_1 \cap V_2 = 0$ et donc $\dim V_1 + \dim V_2 \leq n$. On trouve donc que $p \leq s$. On prouve de façon analogue $s \leq p$.

Exercice 3

1. On a vu en cours que les renversements engendrent $\mathrm{SO}(V,f)$ et ils sont tous conjugués.
2. Par définition N_0 contient l'identité. L'application

$$\begin{aligned}
\varphi : \quad N_0 \times N_0 &\longrightarrow N \\
(x,y) &\longmapsto xy^{-1}
\end{aligned}$$

est continue, et $N_0 \times N_0$ étant connexe, on en déduit que l'image de φ est un connexe de N. De plus elle contient l'identité, donc est incluse dans N_0, ce qui montre que N_0 est un sous-groupe de N.
Si on suppose désormais que $N \lhd \mathrm{SO}(3)$ et si $h \in \mathrm{SO}(3)$, alors l'application

$$\begin{aligned}
\mathrm{Int}_h : \quad N &\longrightarrow N \\
g &\longmapsto hgh^{-1}
\end{aligned}$$

est bien définie. Le même argument que plus haut montre que Int_h envoie N_0 dans N_0, et ce pour tout $h \in \mathrm{SO}(3)$, ce qui siginifie que N_0 est un sous-groupe distigué de $\mathrm{SO}(3)$.

3. Si $N_0 = \{\mathrm{Id}\}$ alors montrons que $N = \{\mathrm{Id}\}$. Soit $g \in N$. L'application continue

$$\begin{aligned} \varphi : \mathrm{SO}(3) &\longrightarrow N \\ h &\longmapsto hgh^{-1}g^{-1} \end{aligned}$$

est bien définie car $N \lhd \mathrm{SO}(3)$ et est continue. Le groupe $\mathrm{SO}(3)$ est connexe donc l'image de φ est un connexe contenant Id, donc est égale à $\{\mathrm{Id}\}$. Cela signifie que g est dans le centre de $\mathrm{SO}(3)$, ce qui montre que $g = Id$.

4. Soit $r \in \mathrm{SO}(3)$. Il existe une base orthonormée de $\mathbf{R}^3$ telle que la matrice de l'application linéaire canoniquement associée à r dans cette base soit

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{pmatrix}.$$

On a $\mathrm{Tr}(r) = 1 + 2\cos\theta$, donc la fonction

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

est bien définie.

5. Cherchons un élément $s \in N$ tel que $\varphi(s) \leq 0$. Soit g un élément de N distinct de l'identité. On a

$$\frac{\mathrm{Tr}(g) - 1}{2} = \cos\theta$$

où θ est défini au signe près. Quitte à changer g en g^{-1} on peut supposer que $\theta \in]0, \pi]$. Si $\theta \in [\pi/2, \pi]$ alors $s = g$ convient. Sinon, soit $N = E\left(\frac{\pi}{2\theta}\right)$. On a

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

donc $s = g^{N+1}$ convient.

6. Par hypothèse N est connexe, et φ est clairement continue, donc $\varphi(N)$ est un connexe de $[-1, 1]$ contenant $\varphi(s) \leq 0$ et $\varphi(Id) = 1$. Or, les connexes de $\mathbf{R}$ sont les intervalles, donc il existe $g \in N$ tel que $\varphi(g) = 0$, c'est-à-dire N contient une rotation d'angle $\pm\frac{\pi}{2}$. L'élément $R = g^2 \in N$ est donc un retournement.

Exercice 5

1. 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

$$-b(e_+, e_-) = b(s(e_+), s(e_-)) = b(e_+, e_-) = 0.$$

2. L'application $s \mapsto E_+(s)$ est une bijection comme voulue.
3. Soit $\mathscr{F}$ une telle famille. Elle est composée d'involutions de type $(2r, 2m-2r)$ pour un r fixé (puisque les éléments de $\mathscr{F}$ sont conjugués). Comme ils commutent, tous les éléments de $\mathscr{F}$ 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 $b(e_i, e_j) = 0$ autrement, 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 $|\mathscr{F}| \leq C_m^r$.
   En particulier si s est une involution extrémale, alors elle est incluse dans une famille maximale d'involutions conjuguées commutant deux à deux à m éléments. Parce que cette dernière propriété est conservée par un automorphisme de $\mathrm{Sp}_{2m}(\mathbf{K})$ et que l'on a $C_m^r \neq m$ pour $r \notin \{1, m-1\}$, tout automorphisme de $\mathrm{Sp}_{2m}(\mathbf{K})$ envoie involutions extrémales sur involutions extrémales.
4. 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 $E_2(s) \cap E_2(t) = \varnothing$. 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 $E_2(s') + E_2(t') \subsetneq E_2(s) + E_2(t)$ et $E_{2m-2}(s') \cap E_{2m-2}(t') \supsetneq E_{2m-2}(s) \cap E_{2m-2}(t)$. On a alors $C(C(\{s', t'\})) \neq C(C(\{s,t\}))$.
5. 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.

6. 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 de $\mathrm{Sp}_{2m}(\mathbf{K})$ commutant avec tout élément de $I_1(V_1)$. On en déduit que tout automorphisme de $\mathrm{Sp}_{2m}(\mathbf{K})$ préserve $\{I_1(x) \mid x \in \mathbf{P}^{2m-1}(\mathbf{K})\}$.
Soit ϕ un automorphisme de $\mathrm{Sp}_{2m}(\mathbf{K})$. On lui associe la bijection $\theta_\phi : \mathbf{P}^{2m-1}(\mathbf{K}) \to \mathbf{P}^{2m-1}(\mathbf{K})$ via $\phi.I_1(x) = I_1(\theta_\phi x)$. Maintenant, $x, y \in \mathbf{P}^{2m-1}(\mathbf{K})$ sont deux droites orthogonales si et seulement si elles engendrent un plan anisotrope ; ceci est encore équivalent à $I(x) \cap I(y) = \varnothing$. 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 $a \in \Gamma\mathrm{L}_{2m}(\mathbf{K})$ tel que l'on ait $\theta_\phi(\mathbf{K}x) = \mathbf{K}(ax)$ pour tout $x \in \mathbf{K}^{2m} \setminus \{0\}$. Comme a préserve l'orthogonalité, on a même $a \in \Gamma\mathrm{Sp}_{2m}(\mathbf{K})$. 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 $\phi(s) = asa^{-1}$. Si g est un élément de $\mathrm{Sp}_{2m}(\mathbf{K})$, 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 $\mathrm{Sp}_{2m}(\mathbf{K}) \to \mathbf{K}^\times$. Par simplicité de $\mathrm{PSp}_{2m}(\mathbf{K})$, le noyau de ce dernier est $\{1\}$, $Z(\mathrm{Sp}_{2m}(\mathbf{K}))$ ou $\mathrm{Sp}_{2m}(\mathbf{K})$. 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.