École normale supérieure Année 2014-2015
Algèbre 1

Corrigé de la Feuille d'exercices 9

Exercice 1 En considérant les équations $X^2 - a^2$ pour $a \in \mathbf{R}$, on voit qu'un automorphisme de $\mathbf{R}$ préserve $\mathbf{R}^+$ et donc la relation $\leq$. Aussi, il induit l'identité sur le sous-corps $\mathbf{Q}$ des nombres rationnels. En écrivant tout élément de $x \in \mathbf{R}$ comme

$$\sup\{y \in \mathbf{Q} \mid y \leq x\} = x = \inf\{y \in \mathbf{Q} \mid x \leq y\},$$

on obtient le résultat voulu.

Exercice 2

1. Notons ψ_ϕ l'image de ϕ. Pour tous $x, y \in E$ et $\lambda, \mu \in \mathbf{K}$, on vérifie :
   $\psi_\phi((\lambda + i\mu)x, y) = (\lambda - i\mu)\psi_\phi(x, y)$;
   $\psi_\phi(x, (\lambda + i\mu)y) = (\lambda + i\mu)\psi_\phi(x, y)$.
   Réciproquement, toute forme sesquilinéaire ψ sur $E' \times E'$ s'écrit $\psi = \phi_1 + i\phi_2$ où ϕ_1 et ϕ_2 sont des formes $\mathbf{K}$-bilinéaires sur $E \times E$. On a, pour tous $x, y \in E \times E$, les égalités $\phi_1(ix, iy) + i\phi_2(ix, iy) = \psi(ix, iy) = \psi(x, y) = \phi_1(x, y) + i\phi_2(x, y)$. Autrement dit, ϕ_1 et ϕ_2 sont invariantes par i. Aussi, on a $\phi_1(ix, y) + i\phi_2(ix, y) = \psi(ix, y) = -i\psi(x, y) = \phi_2(x, y) - i\phi_1(x, y)$, de sorte que l'on a $\phi_2(x, y) = \phi_1(ix, y)$.
2. On a $\psi_\phi(y, x) = \phi(y, x) - i\phi(y, ix)$.
3. Si ϕ est symétrique invariante par i, on a $\phi(ix, y) + \phi(iy, x) = \phi(ix, y) + \phi(-y, ix) = 0$.

Exercice 3

1. Supposons (i). Alors u^* stabilise $\ker d_\phi$. Soit S un supplémentaire de $\ker d_\phi$ dans E ; si $u_0^* : E \to E$ désigne l'identité de $\ker d_\phi$ prolongée par 0 sur S, $u^* + u_0^*$ est un endomorphisme satisfaisant aussi l'égalité voulue. De ce fait, on a $u_0^* = 0$ et $\ker d_\phi = 0$. Aussi, on a $d_\phi(x) \circ u = d_\phi(u^*(x))$ pour tout $x \in E$.
   Réciproquement, supposons (ii). L'inclusion ${}^t u(d_\phi(E)) \subseteq d_\phi(E)$ nous permet de définir une application ensembliste $u^* : E \to E$ vérifiant $\phi(u^*(x), y) = \phi(x, u(y))$ pour tous $x, y \in E$. L'injectivité de d_ϕ nous assure l'unicité d'un tel u^*, et sa linéarité en découle.
2. Soient $\mathbf{K}$ un corps et E un espace vectoriel sur $\mathbf{K}$ possédant une base dénombrable $(e_n)_{n \geq 1}$. On définit une forme bilinéaire ϕ sur $E \times E$ en posant $\phi(e_i, e_j) = \delta_{i,j+1}$ pour tous $i, j \geq 1$. Soit u l'application linéaire définie par $e_i \mapsto \delta_{1i} e_2$. Alors on a ${}^t u(e_2^*) = e_1^* \notin d_\phi(E)$ et $e_2^* \in d_\phi(E)$.

Exercice 4

1. Soit b un élément du noyau de u. La condition implique alors $\phi_1(.,b) = 0$, et comme ϕ_1 est non dégénérée, on a $b = 0$.
2. D'après (a) et les hypothèses de non dégénérescence, pour tout $y \in E_1$, $d_{\phi_1}(y)$ et $d_{\phi_2}(u(y))$ sont deux éléments non nuls de E_1^* possédant le même hyperplan. Alors, il existe $m(y) \in \mathbf{K}^\times$ vérifiant $\phi_2(u(x), u(y)) = \phi_1(x, y)m(y)$ pour tout $x \in E_1$.
3. On voit tout d'abord que $m : E_1 \to \mathbf{K}^\times$ est constante sur les droites. Maintenant, si y et y' sont deux éléments non colinéaires de E_1 (qui est alors de dimension supérieure à 2), on a $\phi_1(x, y + y')m(y + y') = \phi_1(x, y)m(y) + \phi_1(x, y')m(y')$. En prenant successivement x dans $\ker d_{\phi_1}(y) \smallsetminus \ker d_{\phi_1}(y')$ et $\ker d_{\phi_1}(y) \smallsetminus \ker d_{\phi_1}(y')$ (c'est possible parce que ϕ_1 est non dégénérée !), on obtient $m(y) = m(y')$ et le résultat voulu.

Exercice 6

2) Le nombre de vecteurs de $\mathbf{F}_{q^2}^n$ est $q^{2n} = 1 + z_n + (q-1)y_n$. Aussi, en séparant le cas où la dernière coordonnée est nulle ou non, on obtient $z_{n+1} = z_n + (q-1)(q+1)y_n$. On en déduit $z_{n+1} = (q^{2n} - 1)(q + 1) - qz_n$; comme z_1 vaut 0, on prouve la formule voulue par récurrence.

3) Les éléments de $\mathrm{U}_n(\mathbf{F}_{q^2}/\mathbf{F}_q)$ sont en bijection avec les bases orthonormales de $\mathbf{F}_{q^2}^n$. On en déduit

$$|\,\mathrm{U}_n(\mathbf{F}_{q^2}/\mathbf{F}_q)| = \prod_{i=1}^{n} q^{i-1}(q^i - (-1)^i) = q^{\frac{n(n-1)}{2}} \prod_{i=1}^{n}(q^i - (-1)^i).$$

4) La condition ${}^t u^{(q)} u = 1$, où $u^{(q)}$ désigne la matrice de coefficients les puissances q-ème des coefficients de la matrice $u \in \mathrm{U}_n(\mathbf{F}_{q^2}/\mathbf{F}_q)$, donne $\det \mathrm{U}_n(\mathbf{F}_{q^2}/\mathbf{F}_q) = \{x^{q+1} \mid x \in \mathbf{F}_{q^2}^\times\}$. On a alors

$$|\,\mathrm{SU}_n(\mathbf{F}_{q^2}/\mathbf{F}_q)| = q^{\frac{n(n-1)}{2}} \prod_{i=2}^{n}(q^i - (-1)^i), \quad |\,\mathrm{PSU}_n(\mathbf{F}_{q^2}/\mathbf{F}_q)| = \frac{q^{\frac{n(n-1)}{2}}}{n \wedge (q+1)} \prod_{i=2}^{n}(q^i - (-1)^i).$$

Exercice 7

1. On fait agir $\mathfrak{S}_6$ sur $\mathbf{F}_2^6$ par permutation des coordonnées. Le sous-espace $E = \{(x_i)_i \in \mathbf{F}_2^6 \mid \sum_i x_i = 0\}$ est stable par cette action. Cet espace est muni de la forme bilinéaire alternée $b : (x, y) \mapsto \sum_i x_i y_i$. Le sous-espace $E^\perp = \mathbf{F}_2(1, 1, 1, 1, 1, 1)$ est encore stable par $\mathfrak{S}_6$ et on a donc une action de $\mathfrak{S}_6$ sur $E/E^\perp$ qui est de dimension 4 comme voulu. De plus, la forme b se factorise $E \times E \to E/E^\perp \times E/E^\perp \to \mathbf{F}_2$.
2. On a donc un morphisme $\mathfrak{S}_6 \to \mathrm{Sp}_4(\mathbf{F}_2)$. Comme $\mathfrak{A}_6$ est simple et que l'image a plus de 2 éléments, ce dernier est injectif. La cardinalité permet de conclure.

Exercice 8

1. Un petit calcul donne que ce sont $\mathbf{K}(1,0,0)$ et les $\mathbf{K}(\alpha,\beta,1)$ avec $\alpha+\alpha^q+\beta^{1+q}=0$. Le nombre de solutions de cette équation est $q^2\cdot q$ (car $\begin{array}{ccc}\mathbf{F}_{q^2} & \to & \mathbf{F}_q \\ x & \mapsto & x^{1+q}\end{array}$ est surjective et $\begin{array}{ccc}\mathbf{F}_{q^2} & \to & \mathbf{F}_q \\ x & \mapsto & x+x^q\end{array}$ est $\mathbf{F}_q$-linéaire). Le cardinal de Δ est donc q^3+1.
2. On vérifie que les $t_{\alpha,\beta}$ et $h_{\gamma,\delta}$ stabilisent bien $\mathbf{K}e_1$. Notons respectivement T et H les sous-groupes de $\mathrm{PU}_3(\mathbf{F}_{q^2}/\mathbf{F}_q)$ engendrés par les $t_{\alpha,\beta}$ et les $h_{\gamma,\delta}$; ils forment un produit semi-direct (le vérifier !). L'image réciproque de $T\rtimes H$ dans $\mathrm{U}_3(\mathbf{F}_{q^2}/\mathbf{F}_q)$ est de cardinal $q^3\cdot(q^2-1)(q+1)$. De plus, l'action de $\mathrm{U}_3(\mathbf{F}_{q^2}/\mathbf{F}_q)$ sur Δ étant transitive, on a
$$|\operatorname{Stab}_{\mathrm{U}_3}\mathbf{K}e_1| = |\,\mathrm{U}_3(\mathbf{F}_{q^2}/\mathbf{F}_q)|\cdot|\Delta|^{-1} = q^3(q^2-1)(q+1).$$
Ceci montre que le stabilisateur de $\mathbf{K}e_1$ dans $\mathrm{PU}_3(\mathbf{F}_{q^2}/\mathbf{F}_q)$ est exactement $T\rtimes H$.
3. Un petit calcul donne que l'action de T est transitive sur $\Delta\smallsetminus\{\mathbf{K}e_1\}$.

Exercice 9

3. Rappelons que, d'après le cours, les automorphismes de $\mathbf{H}$ de la forme $x\mapsto qxq^{-1}$ pour un certain $q\in\mathbf{H}$ de norme 1 préservent $\mathbf{R}$ et $\Im(\mathbf{R})$, leur restriction à $\mathbf{R}$ est l'identitité et leur restriction à $\Im(\mathbf{H})$ appartient à $\mathrm{SO}(3,\mathrm{N})$, où N est la norme. De plus tout élément de $\mathrm{SO}(3,\mathrm{N})$ provient d'un tel morphisme intérieur.

   Soit ϕ un automorphisme d'anneaux de $\mathbf{H}$. Il préserve le centre donc il induit un automorphisme de $\mathbf{R}$, qui est donc l'identité (exercice 1). Du coup, c'est un automorphisme $\mathbf{R}$-linéaire. Par 1, les quaternions purs sont conservés. Ensuite un tel automorphisme préserve la norme donc appartient à $\mathrm{O}_3(\mathbf{R})$. Il est facile de voir que, en fait, il appartient à $\mathrm{SO}_3(\mathbf{R})$: en effet, i,j,k et $\phi(i),\phi(j),\phi(k)$ sont des bases orthonormés ; on a $\phi(i)\phi(j)=\epsilon\phi(k)$ pour un certain $\epsilon\in\{\pm1\}$. Or $\phi(i)\phi(j)=\phi(ij)=\phi(k)$. Donc $\epsilon=1$ et ϕ préserve l'orientation.

Exercice 10

1. Soient $a,b\in F^\times$ des racines carrées respectives de α et β. Le morphisme d'algèbres défini par $i\mapsto\begin{pmatrix} a & \\ & -a\end{pmatrix}$ et $j\mapsto\begin{pmatrix} & b\\ b & \end{pmatrix}$ est l'isomorphisme voulu.
2. Supposons que $\mathbf{H}_{\alpha,\beta}$ soit une algèbre à division. Soient $z\in\mathbf{H}_{\alpha,\beta}$ et z' un inverse. On a alors $\mathrm{N}(z)\,\mathrm{N}(z')=1$ et par ce fait $\mathrm{N}(z)\neq 0$. Réciproquement, si N est anisotrope, pour tout élément z, $\mathrm{N}(z)^{-1}\overline{z}$ fournit un inverse.

Exercice 11 (Théorème de Lagrange)

1. On a $\mathrm{N}(a+bi+cj+dk) = a^2+b^2+c^2+d^2$, qui est bien un élément de A. Aussi, on a $\mathrm{N}(z_1z_2) = z_1z_2\overline{z}_2\overline{z}_1 = \mathrm{N}(z_1)\,\mathrm{N}(z_2)$.
2. Que $(H,+)$ forme un sous-groupe de $(\mathbf{H}(\mathbf{Q}),+)$ est clair. Il contient 1, vérifions qu'il est stable par multiplication. Pour cela, posons, $u = \dfrac{1}{2}(1+i+j+k) \in H$. Il suffit de vérifier que $u.1$, $u.i$, $u.j$, $u.k$ et u^2 sont encore des éléments de H.
   Lorsque z est un élément de $\mathbf{H}(\mathbf{Z})$, $\mathrm{N}(z)$ est entier par la question 1. Considérons donc un $z \in H$ qui s'écrit $u+a+bi+cj+dk$, avec $a,b,c,d \in \mathbf{Z}$. On a alors $\mathrm{N}(z) = a^2+a+b^2+b+c^2+c+d^2+d+1 \in \mathbf{Z}$.
   Maintenant, si z est de norme 1, son inverse est $\overline{z}$. Réciproquement, si z est inversible, alors il existe $z' \in H$ vérifiant $zz' = 1$. Il en résulte $\mathrm{N}(z)\,\mathrm{N}(z') = 1$, et donc $\mathrm{N}(z) = 1$ puisque la norme est à valeurs entières positives.
3. Commençons par une remarque. Si $x = a+bi+cj+dk$ est un élément de $\mathbf{H}(\mathbf{Q})$, il existe $a',b',c',d' \in \mathbf{Z}$ tels que $|a-a'| \leq 2^{-1}$, $|b-b'| \leq 2^{-1}$, $|c-c'| \leq 2^{-1}$ et $|d-d'| \leq 2^{-1}$. Pour $x' = a'+b'i+c'j+d'k$, on a alors $\mathrm{N}(x-x') \leq 1$, avec égalité si et seulement si $x \in H \smallsetminus \mathbf{H}(\mathbf{Z})$. Prouvons l'assertion voulue pour les idéaux à droite. Soient $\mathfrak{a}$ un idéal à droite propre de H et $z \in \mathfrak{a}$ un élément de norme minimale non nulle. Soit $y \in \mathfrak{a}$; par la remarque précédente, il existe $t \in H$ avec $\mathrm{N}(z^{-1}y-t) < 1$. On a alors $\mathrm{N}(y-zt) < \mathrm{N}(z)$; par minimalité, on obtient $\mathrm{N}(y-zt) = 0$ et donc $y = zt$.
4. Comme on a $2 = 1^2+1^2+0^2+0^2$, on peut supposer p impair. L'idéal pH est bilatère et on peut former l'anneau quotient H/pH. Parce que p est impair, H/pH est isomorphe à $\mathbf{H}(\mathbf{Z})/p\mathbf{H}(\mathbf{Z}) \simeq \mathbf{H}(\mathbf{F}_p)$. Aussi, $a^2+b^2+c^2+d^2 = 0$ a une solution non triviale dans $\mathbf{F}_p$, qui engendre alors un idéal à droite propre de $\mathbf{H}(\mathbf{F}_p)$. L'antécédent dans H de cet idéal est un idéal z_0H par la question (d), et il vérifie $pH \subsetneq z_0H \subsetneq H$. En particulier, il existe un élément $z' \in H$ vérifiant $z_0z' = p$. On obtient $\mathrm{N}(p) = p^2 = \mathrm{N}(z_0)\,\mathrm{N}(z')$; et parce que l'on a $\mathrm{N}(z_0) > 1$ et $\mathrm{N}(z') > 1$, on a finalement $\mathrm{N}(z_0) = p$.
5. On veut montrer que z_0 peut être pris dans $\mathbf{H}(\mathbf{Z})$. Supposons que ce ne soit pas le cas et regardons l'image de $\xi = 2z_0$ dans $\mathbf{H}(\mathbf{Z})/4\mathbf{H}(\mathbf{Z}) \simeq \mathbf{H}(\mathbf{Z}/4\mathbf{Z})$. Là-dedans, la norme de ξ est nulle, c'est-à-dire $\xi\overline{\xi} = 0$. Il suffit alors de relever $\overline{\xi}$ en un élément de $\{\pm 1 \pm i \pm j \pm k\} \subseteq \mathbf{H}(\mathbf{Z})$, et de poser $z_1 = 2^{-1}\overline{\xi}$ dans H. Il en résulte $\mathrm{N}(z_0z_1) = p$ avec $z_0z_1 \in \mathbf{H}(\mathbf{Z})$.
   Le résultat pour tout entier naturel suit de (a) et de la décomposition en facteurs premiers dans $\mathbf{Z}$.