TD9 : Formes sesquilinéaires, groupe unitaire, quaternions

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

Exercice 1 : ⋆
Montrer que toute forme sesquilinéaire réelle est bilinéaire.

Solution de l'exercice 1. Il est classique que l'identité est l'unique automorphisme de corps de $\mathbb{R}$. Par conséquent, l'identité est la seule involution de corps de $\mathbb{R}$, ce qui assure le résultat.

Exercice 2 : ⋆
Soient K un corps de caractéristique différente de 2 et $\sigma \in \mathrm{Aut}(K)$ une involution distincte de id_K. Montrer que $k = K^\sigma := \{x \in K : \sigma(x) = x\}$ est un sous-corps de K, qu'il existe $a \in K \setminus k$ tel que $a^2 \in k$, $\sigma(a) = -a$ et $K = k(a) := \{\lambda a + \mu : (\lambda, \mu) \in k^2\}$.
Que dire si K est de caractéristique 2 ?

Solution de l'exercice 2.
- On vérifie facilement que $k := K^\sigma$ contient 0 et 1, qu'il est stable par somme et produit, ainsi que par opposé et par inverse. Cela assure que k est un sous-corps de K.
- On suppose que la caractéristique de K n'est pas 2. Par hypothèse, il existe $b \in K \setminus k$. Posons $a := b - \sigma(b)$. On voit que a vérifie que $\sigma(a) = -a$ et donc $a \notin k$ (puisque $a \neq 0$ et K n'est pas de caractéristique 2). On a donc $a^2 = -a\sigma(a) \in K$. En outre, il est clair que $k(a) \subset K$. Réciproquement, soit $x \in K$. Posons $\lambda := \frac{x+\sigma(x)}{2}$ et $y := \frac{x-\sigma(x)}{2}$. Alors $x = \lambda + y$ et en outre, $\lambda \in k$ et $\sigma(y) = -y$. Donc $\frac{y}{a}$ est fixe par σ, donc $\frac{y}{a} \in k$, i.e. il existe $\mu \in k$ tel que $y = \mu a$. Finalement, on a $x = \lambda + \mu a$, avec $\lambda, \mu \in k$. Cela assure que $K = k(a)$.
- On suppose maintenant que K est de caractéristique 2. On sait qu'il existe $b \in K \setminus k$. Posons $a := \frac{b}{b+\sigma(b)}$. On voit que $\sigma(a) = a + 1$, donc $a \notin k$. En outre, $\alpha := a\sigma(a)$ est un élément de k, et on a la relation suivante : $a^2 + a + \alpha = 0$ (on note en revanche que $a^2 \notin k$). On a bien $k(a) \subset K$. Réciproquement, soit $x \in K \setminus k$. Posons $y := \frac{x}{x+\sigma(x)}$. Alors $\sigma(y) = y + 1$, donc $\sigma(a + y) = a + y$, donc $a + y \in k$. Donc $y \in k(a)$, donc $x = (x + \sigma(x))y \in k(a)$ car $x + \sigma(x) \in k$. Donc $K = k(a)$.

Exercice 3 : ⋆⋆
Soient K un sous-corps de $\mathbb{R}$ et $K' = K(i) := \{x + iy : (x, y) \in K^2\}$. On munit K' de l'involution induite par la conjugaison complexe. Soient E' un K'-espace vectoriel et E le K-espace vectoriel sous-jacent. Une forme K-bilinéaire f sur $E \times E$ est dite *invariante par* i si l'on a $f(ix, iy) = f(x, y)$ pour tous $x, y \in E$.

a) Montrer que l'application $\phi \mapsto \big((x, y) \mapsto \phi(x, y) + i\phi(x, iy)\big)$ est un isomorphisme de l'espace des formes bilinéaires sur $E \times E$ invariantes par i vers celui des formes sesquilinéaires sur $E' \times E'$.

b) Montrer qu'elle induit un isomorphisme de l'espace des formes symétriques sur $E \times E$ invariantes par i vers l'espace des formes hermitiennes sur $E' \times E'$.

c) Montrer que si ϕ est symétrique invariante par i, alors $(x, y) \mapsto \phi(x, iy)$ est antisymétrique.

Solution de l'exercice 3.

a) Notons ψ_ϕ l'image de ϕ. Pour tous $x, y \in E$ et $\lambda, \mu \in k$, on vérifie que

$$\psi_\phi((\lambda + i\mu)x, y) = \lambda\phi(x, y) + i\lambda\phi(x, iy) - \mu\phi(x, iy) + i\mu\phi(x, y) = (\lambda + i\mu)\psi_\phi(x, y)$$

et

$$\psi_\phi(x,(\lambda+i\mu)y) = \lambda\phi(x,y) + i\lambda\phi(x,iy) + \mu\phi(x,iy) - i\mu\phi(x,y) = (\lambda - i\mu)\psi_\phi(x,y)\,.$$

Donc ψ_ϕ est bien une forme sesquilinéaire sur $E' \times E'$.
Et il est clair que l'application $\phi \mapsto \psi_\phi$ est k-linéaire.
Réciproquement, tout forme sesquilinéaire ψ sur $E' \times E'$ s'écrit $\psi = \phi_1 + i\phi_2$ où ϕ_1 et ϕ_2 sont des formes 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 l'égalité

$$\phi_1(x,iy) + i\phi_2(x,iy) = \psi(x,iy) = -i\psi(x,y) = \phi_2(x,y) - i\phi_1(x,y)\,,$$

de sorte que l'on a $\phi_2(x,y) = \phi_1(x,iy)$.
Cela assure que l'application $\psi \mapsto \phi_\psi := \phi_1$ est la réciproque de l'application précédente, i.e. que pour toute forme sesquilinéaire ψ, on a $\psi_{\phi_\psi} = \psi$, et pour toute forme bilinéaire ϕ, on a $\phi_{\psi_\phi} = \phi$.
D'où l'isomorphisme souhaité.

b) On a $\psi_\phi(y,x) = \phi(y,x) - i\phi(iy,x)$, ce qui assure le résultat souhaité.

c) Si ϕ est symétrique invariante par i, on a $\phi(x,iy) + \phi(y,ix) = \phi(x,iy) + \phi(iy,-x) = 0$.

Exercice 4 :
Soient K un corps, E un espace vectoriel sur K, ϕ une forme sesquilinéaire sur $E \times E$ et u un endomorphisme de E.
Si $v : E \to F$ est une application linéaire entre deux espaces vectoriels, on définit sa *transposée* comme étant l'application $\begin{array}{rccc} {}^tv : & F^* & \to & E^* \\ & f & \mapsto & f \circ v \end{array}$.

a) Montrer que les deux conditions suivantes sont équivalentes :
   i) il existe un unique endomorphisme u^* de E vérifiant $\phi(u(x),y) = \phi(x,u^*(y))$ pour tous $x, y \in E$;
   ii) l'application $d_\phi : E \to E^*$ induite par ϕ est injective et ${}^tu(d_\phi(E)) \subseteq d_\phi(E)$.

b) Donner un exemple où E est de dimension infinie, d_ϕ est injective, mais où ${}^tu(d_\phi(E))$ n'est pas contenu dans $d_\phi(E)$.

Solution de l'exercice 4.

a) 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. Par unicité, on a donc $u_0^* = 0$ et $\ker d_\phi = 0$. Aussi, on a ${}^tu(d_\phi(y)) = d_\phi(y) \circ u = d_\phi(u^*(y))$ pour tout $y \in E$.
   Réciproquement, supposons (ii). L'inclusion ${}^tu(d_\phi(E)) \subseteq d_\phi(E)$ 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.

b) Soient k un corps et E un espace vectoriel sur k possédant une base dénombrable $(e_n)_{n\geq 1}$ (par exemple $E = k[X] = k^{(\mathbb{N})}$). 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 $e_i \mapsto \delta_{1,i}e_2$. Alors d_ϕ est injective et on a ${}^tu(e_2^*) = e_1^* \notin d_\phi(E)$ alors que $e_2^* = d_\phi(e_1) \in d_\phi(E)$.

Exercice 5 :
Soient K un corps, E_0 et E_1 deux espaces vectoriels sur K et ϕ_0, ϕ_1 des formes sesquilinéaires respectivement sur $E_0 \times E_0$ et $E_1 \times E_1$. On suppose que ϕ_1 est non dégénérée et qu'il existe un élément $\alpha \in K$ et une bijection $v : E_0 \to E_1$ tels que l'on ait $\phi_1(v(x),v(y)) = \phi_0(x,y)\alpha$ pour tous $x, y \in E_0$.

a) Montrer que ϕ_0 est non dégénérée et que v est linéaire.

Soient E_2 un espace vectoriel sur K et ϕ_2 une forme sesquilinéaire non dégénérée sur $E_2 \times E_2$. On suppose l'existence d'une application linéaire surjective $u : E_1 \to E_2$ qui vérifie

$$\phi_2(u(x), u(y)) = 0 \Rightarrow \phi_1(x, y) = 0 \quad \text{pour tous } x, y \in E_1.$$

b) Montrer que u est un isomorphisme de E_1 sur E_2.

c) Montrer que pour tout $y \in E_1$, il existe un élément $m(y) \in K$ tel que l'on ait $\phi_2(u(x), u(y)) = \phi_1(x, y)m(y)$ pour tout $x \in E_1$.

d) En déduire qu'il existe $\beta \in K^*$ tel que l'on ait $\phi_2(u(x), u(y)) = \phi_1(x, y)\beta$ pour tous $x, y \in E_1$.

Solution de l'exercice 5.

a) Comme ϕ_1 est non dégénérée, on voit que $v(0) = 0$. Soit $x \in E_0$ tel que $\phi_0(., x) = 0$. Alors $\phi_1(., v(x)) = 0$, donc $v(x) = 0 = v(0)$. Or v est injective, donc $x = 0$, donc ϕ_0 est non dégénérée. Un raisonnement analogue utilisant la non-dégénérescence de ϕ_1 assure la linéarité de v.

b) 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 $b = 0$. Donc u est injective, donc un isomorphisme.

c) 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 $m(y) \in k^*$ vérifiant $\phi_2(u(x), u(y)) = \phi_1(x, y)m(y)$ pour tout $x \in E_1$.

d) On voit tout d'abord que $m : E_1 \to k^*$ 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 $\ker d_{\phi_1}(y) \setminus \ker d_{\phi_1}(y')$ et $\ker d_{\phi_1}(y) \setminus \ker d_{\phi_1}(y')$ (c'est possible parce que ϕ_1 est non dégénérée), on obtient $m(y) = m(y')$ et le résultat voulu.

Exercice 6 :
Déterminer les groupes unitaires, orthogonaux et symplectiques en dimension 1 et 2.

Solution de l'exercice 6. Voir cours.

Exercice 7 : $\star\star$
Soient p un nombre premier impair et $q = p^r$ une puissance d'un tel nombre premier, avec $r \geq 1$.

a) Montrer qu'il existe une involution non triviale sur $\mathbb{F}_q$ si et seulement si r est pair.

b) Vérifier que $\sigma : x \mapsto x^q$ est l'unique involution non triviale de $\mathbb{F}_{q^2}$ et que son corps des invariants est $\mathbb{F}_q$.

c) On note $E_n := \mathbb{F}_{q^2}^n$. Montrer qu'il y a sur (E_n, σ) une unique classe d'équivalence de formes hermitiennes non dégénérées. Montrer qu'une telle forme admet dans une base convenable la matrice identité.

d) Soit z_n (resp. y_n) le nombre de vecteurs non triviaux de E_n de norme 0 (resp. 1). Par récurrence, montrer que l'on a pour tout entier $n \geq 1$,

$$z_n = (q^n - (-1)^n)(q^{n-1} + (-1)^n) \quad \text{et} \quad y_n = q^{n-1}(q^n - (-1)^n).$$

e) Calculer l'ordre de $\mathrm{U}_n(\mathbb{F}_{q^2})$.

f) En déduire l'ordre de $\mathrm{SU}_n(\mathbb{F}_{q^2})$ et de $\mathrm{PSU}_n(\mathbb{F}_{q^2})$.

Solution de l'exercice 7.

a) L'exercice 2 assure que si $\mathbb{F}_q$ admet une involution non triviale σ, alors $\mathbb{F}_q$ est un $\mathbb{F}_q^\sigma$-espace vectoriel de dimension 2, ce qui assure que $|\mathbb{F}_q|$ est un carré, donc $q = p^r$ est un carré, donc r est pair.

Réciproquement, si $r = 2s$ est pair, alors l'application $\sigma : \mathbb{F}_q \to \mathbb{F}_q$ définie par $x \mapsto x^{p^s}$ est une involution non triviale de $\mathbb{F}_q$ (c'est un morphisme de corps car c'est une puissance de l'automorphisme de Frobenius, c'est une involution par le théorème de Lagrange, et ce n'est pas l'identité car les points fixes de σ sont les racines de $X^{p^s} - X$ dans $\mathbb{F}_q$, qui sont au plus $p^s < q = |\mathbb{F}_q|$).

b) On a vu à la question a) que σ était une involution non triviale, et que son corps des invariants était un corps de cardinal q. Il reste à montrer l'unicité de σ. Soit τ une involution non triviale de $\mathbb{F}_{q^2}$. Alors $\mathbb{F}_{q^2}^\sigma$ et $\mathbb{F}_{q^2}^\tau$ sont deux sous-corps de $\mathbb{F}_{q^2}$ de cardinal q. Donc $\left(\mathbb{F}_{q^2}^\sigma\right)^*$ et $\left(\mathbb{F}_{q^2}^\tau\right)^*$ sont deux sous-groupes de même cardinal du groupe cyclique $\mathbb{F}_{q^2}^*$, donc ils sont égaux, donc $\mathbb{F}_{q^2}^\sigma = \mathbb{F}_{q^2}^\tau \subset \mathbb{F}_{q^2}$. On notera $k := \mathbb{F}_{q^2}^\sigma$. L'exercice 2 assure qu'il existe $a \in \mathbb{F}_{q^2}^*$ tel que $\sigma(a) = -a$, $\mathbb{F}_{q^2} = k(a)$ et $a^2 \in k$. Alors $\tau(a)^2 = \tau(a^2) = a^2$, donc $\tau(a) = \pm a$. Si $\tau(a) = a$, alors $\tau = \mathrm{id}$, ce qui est exclu. Donc $\tau(a) = -a = \sigma(a)$. Cela suffit pour conclure que $\tau = \sigma$. D'où l'unicité recherchée.

c) L'application $N : \mathbb{F}_{q^2}^* \to \mathbb{F}_q^*$ définie par $x \mapsto x\sigma(x) = x^{q+1}$ est un morphisme de groupes surjectif, dont le noyau est de cardinal $q+1$. Soit f une forme hermitienne non dégénérée sur (E_n, σ). Alors il existe une base orthogonale $(e_1, \dots, e_n)$ de E_n pour f. Puisque f est non dégénérée, pour tout i, $f(e_i) \in \mathbb{F}_q^*$. Donc pour tout i, il existe $\lambda_i \in \mathbb{F}_{q^2}^*$ tel que $f(e_i) = N(\lambda_i)$. Alors $f\left(\frac{e_i}{\lambda_i}\right) = 1$ pour tout i, ce qui assure que la matrice de f dans la base $\left(\frac{e_i}{\lambda_i}\right)$ est bien l'identité.

d) La surjectivité du morphisme $N : \mathbb{F}_{q^2}^* \to \mathbb{F}_q^*$ défini plus haut assure que pour tout $\alpha \in \mathbb{F}_q^*$, l'ensemble des vecteurs $x \in E_n$ de norme α est de cardinal exactement y_n. Or E_n est la réunion disjointe des sous-ensembles formés des vecteurs de norme α, pour α décrivant $\mathbb{F}_q$, donc $|E_n| = 1 + z_n + (q-1)y_n$. On a donc $q^{2n} = 1 + z_n + (q-1)y_n$.

En écrivant l'ensemble des vecteurs $\neq 0$ de E_{n+1} de norme nulle comme réunion disjointe de l'ensemble des vecteurs $\neq 0$ dont la dernière coordonée est nulle et de celui des vecteurs de norme nulle dont la dernière coordonnée n'est pas nulle, on obtient que $z_{n+1} = z_n + (q^2-1)y_n$. On en déduit grâce à la relation précédente que $z_{n+1} = (q^{2n}-1)(q+1) - qz_n$. Comme z_1 vaut 0, on prouve la formule voulue par récurrence sur n.

e) La question c) assure que les éléments de $\mathrm{U}_n(\mathbb{F}_{q^2})$ sont en bijection avec les bases orthonormales de $\mathbb{F}_{q^2}^n$. On en déduit donc que

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

f) La condition ${}^t u^{(q)} u = 1$, où $u^{(q)}$ désigne la matrice de coefficients les puissances q-ième des coefficients de la matrice $u \in \mathrm{U}_n(\mathbb{F}_{q^2})$, assure que $\det\left(\mathrm{U}_n(\mathbb{F}_{q^2})\right) = \{x^{q+1} \mid x \in \mathbb{F}_{q^2}^*\}$. Comme ce dernier ensemble est de cardinal $q-1$, on a

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

et comme le centre de $\mathrm{SU}_n(\mathbb{F}_{q^2})$ est réduit aux homothéties unitaires, on a $Z(\mathrm{SU}_n(\mathbb{F}_{q^2})) = \{\lambda I_n : \lambda^{q+1} = 1 \text{ et } \lambda^n = 1\}$, donc

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

Exercice 8 : ⋆⋆⋆

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 $b(u, v) = u_1 v_3^q + u_2 v_2^q + u_3 v_1^q$

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 8.

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 9 : $\star\star$

Soit $\mathbf{H}$ la $\mathbb{R}$-algèbre des quaternions. Un élément $z \in \mathbf{H}$ est dit *pur* s'il s'écrit sous la forme $z = bi + cj + dk$ avec $a, b, c \in \mathbb{R}$.

a) Montrer que $z \in \mathbf{H}$ est pur si et seulement si $z^2 \in \mathbb{R}^-$.

b) Montrer que tout élément de $\mathbf{H}$ est produit de deux quaternions purs.

c) Montrer que tout automorphisme d'anneaux de $\mathbf{H}$ est de la forme $x \mapsto qxq^{-1}$ pour un certain $q \in \mathbf{H}$ de norme 1.

d) Vérifier que la transposée sur $\mathrm{Mat}_2(\mathbf{H})$ ne conserve pas le groupe $\mathrm{GL}_2(\mathbf{H})$.

Solution de l'exercice 9.

a) C'est un calcul immédiat.

b) Soient $z, z' \in \mathbf{H}$ deux quaternions purs, identifiés à deux vecteurs $Z, Z' \in \mathbb{R}^3$. Un calcul direct assure que $zz' \in \mathbf{H}$ est le quaternion dont la coordonnée réelle est l'opposé du produit scalaire $-Z \cdot Z'$ et les trois autres coordonnées sont les coordonnées du produit vectoriel $Z \wedge Z'$ dans $\mathbb{R}^3$. Soit alors $z_0 = \alpha + Y \in \mathbf{H}$, avec $\alpha \in \mathbb{R}$ et Y pur. L'équation vectorielle dans $\mathbb{R}^3$ donnée par $Z \wedge Z' = Y$ admet clairement une solution $Z, Z' \in \mathbb{R}^3$, avec $Z \neq 0$. Alors pour tout $\lambda \in \mathbb{R}$, $Y = Z \wedge (Z' + \lambda Z)$, et $Z \cdot (Z' + \lambda Z) = Z \cdot Z' + \lambda \|X\|^2$. Il est alors clair qu'il existe $\lambda \in \mathbb{R}$ tel que $Z \wedge (Z' + \lambda Z) = Y$ et $Z \cdot (Z' + \lambda Z) = -\alpha$, donc $z_0 = zz'$, avec $z, z' \in \mathbf{H}$ purs.

c) Soit $\varphi : \mathbf{H} \to \mathbf{H}$ un morphisme d'anneaux. Alors $\varphi(Z(\mathbf{H})) = Z(\mathbf{H})$, où $Z(\mathbf{H}) = \{x \in \mathbf{H} : \forall y \in \mathbf{H},\ xy = yx\}$. Donc $\varphi(\mathbb{R}) = \mathbb{R}$. Donc la restriction de φ à $\mathbb{R}$ est un automorphisme d'anneau de $\mathbb{R}$, donc $\varphi_{|\mathbb{R}} = \mathrm{id}_{\mathbb{R}}$.
La question a) assure qu'un quaternion z est pur si et seulement si $z^2 \in \mathbb{R}^-$, donc pour tout $z \in \mathbf{H}$, z est pur si et seulement si $z^2 \in \mathbb{R}^-$ si et seulement si $\varphi(z^2) = \varphi(z)^2 \in \mathbb{R}^-$ si et seulement si $\varphi(z)$ est pur. Donc si on note $\mathbf{P} \subset \mathbf{H}$ le sous-espace vectoriel des quaternions purs, la restriction de φ à $\mathbf{P}$ induit un isomorphisme de groupes $\varphi_{|\mathbf{P}} : \mathbf{P} \to \mathbf{P}$. Or pour tout $z \in \mathbf{P}$, on a $N(z) = -z^2$ et $N(\varphi(z)) = -z^2$, donc $\varphi_{|\mathbf{P}} \in \mathrm{O}(\mathbf{P}, N) \cong \mathrm{O}_3(\mathbb{R})$. Or (i, j, k) est une base orthonormée de $(\mathbf{P}, N)$, donc $(\varphi(i), \varphi(j), \varphi(k))$ également, donc il existe une rotation $r \in \mathrm{SO}_3(\mathbb{R})$ telle que $r(i) = \varphi(i)$, $r(j) = \varphi(j)$ et $r(k) = \pm\varphi(k)$. Or on dispose de l'isomorphisme $\psi : \{x \in \mathbf{H} : N(x) = 1\}/\{\pm 1\} \xrightarrow{\sim} \mathrm{SO}(\mathbb{P}, N) \cong \mathrm{SO}_3(\mathbb{R})$ défini par $\psi(x) : z \mapsto xzx^{-1}$, ce qui assure que la rotation r est de la forme $\psi(x)$ pour un certain $x \in \mathbf{H}$ de norme 1. Alors on a $xix^{-1} = \varphi(i)$ et $xjx^{-1} = \varphi(j)$, donc $xkx^{-1} = \varphi(i)\varphi(j) = \varphi(k)$. Cela assure que φ est la conjugaison par x sur $\mathbf{H}$.

d) On peut considérer par exemple la matrice $\begin{pmatrix} 1 & j \\ i & k \end{pmatrix}$.

Exercice 10 : $\star\star$
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 10.

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 11 : $\star\star\star$

Soient A un anneau commutatif unitaire et $\mathbf{H}(A)$ la A-algèbre des éléments $a + bi + cj + dk$ avec $a, b, c, d \in A$ telle que 1 est neutre pour la multiplication et avec les relations :

$$i^2 = j^2 = k^2 = -1,\ ij = -ji = k,\ jk = -kj = i,\ ki = -ik = j.$$

a) Définir la norme réduite $N : \mathbf{H}(A) \to A$ et la conjugaison $\mathbf{H}(A) \to \mathbf{H}(A)$.

b) Montrer que pour tout $x, y \in \mathbf{H}(A)$, $N(xy) = N(x)N(y)$.

c) On définit les *quaternions d'Hurwitz* par

$$\mathrm{H} := \left\{ a + bi + ck + dk \in \mathbf{H}(\mathbb{Q}) \mid (a, b, c, d) \in \mathbb{Z}^4 \cup \left(\frac{1}{2} + \mathbb{Z}^4\right) \right\}.$$

Montrer que H est un sous-anneau de $\mathbf{H}(\mathbb{Q})$ contenant $\mathbf{H}(\mathbb{Z})$ et vérifiant $N(z) = 1$ si et seulement si z est inversible dans H.

d) Montrer que tout idéal à droite (respectivement à gauche) de H est principal.

e) Montrer que, pour tout nombre premier p, il existe $z \in \mathrm{H}$ tel que $N(z) = p$.

f) Montrer que tout entier naturel est somme de quatre carrés.

Solution de l'exercice 11.

a) On pose $N(a + bi + cj + dk) = a^2 + b^2 + c^2 + d^2$, qui est bien un élément de A. De même, on définit le conjugué par $\overline{a + bi + cj + dk} = a - bi - cj - dk$.

b) On a $N(z_1 z_2) = z_1 z_2 \overline{z}_2 \overline{z}_1 = N(z_1)N(z_2)$.

c) Il est clair que $(H, +)$ forme un sous-groupe de $(\mathbf{H}(\mathbb{Q}), +)$. 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, ce qui est immédiat.

Lorsque z est un élément de $\mathbf{H}(\mathbb{Z})$, $N(z)$ est entier. Soit alors $z \in H \setminus \mathbf{H}(\mathbb{Z})$: un tel z s'écrit $u + a + bi + cj + dk$, avec $a, b, c, d \in \mathbb{Z}$. On a alors $N(z) = a^2 + a + b^2 + b + c^2 + c + d^2 + d + 1 \in \mathbb{Z}$. Donc pour tout $z \in H$, $N(z) \in \mathbb{Z}$.

Soit $z \in H$ de norme 1 : son inverse dans $\mathbf{H}(\mathbb{Q})$ est $\overline{z}$, qui est bien dans H. Réciproquement, si z est inversible dans H, alors il existe $z' \in H$ vérifiant $zz' = 1$. Il en résulte $N(z)N(z') = 1$, et donc $N(z) = 1$ puisque la norme sur H est à valeurs entières positives.

d) Commençons par une remarque. Si $x = a + bi + cj + dk$ est un élément de $\mathbf{H}(\mathbb{Q})$, il existe $a', b', c', d' \in \mathbb{Z}$ tels que $|a - a'| \leq \frac{1}{2}$, $|b - b'| \leq \frac{1}{2}$, $|c - c'| \leq \frac{1}{2}$ et $|d - d'| \leq \frac{1}{2}$. Pour $x' = a' + b'i + c'j + d'k$, on a alors $N(x - x') \leq 1$, avec égalité si et seulement si $x \in H \smallsetminus \mathbf{H}(\mathbb{Z})$.

Prouvons maintenant l'assertion voulue pour les idéaux à droite (le cas des idéaux à gauche est symétrique). 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 $N(z^{-1}y - t) < 1$. On a alors $N(y - zt) < N(z)$; par minimalité, on obtient que $N(y - zt) = 0$ et donc $y = zt$. Donc $\mathfrak{a}$ est principal, engendré par z.

e) 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. Comme p est impair, H/pH est isomorphe à $\mathbf{H}(\mathbb{Z})/p\mathbf{H}(\mathbb{Z}) \simeq \mathbf{H}(\mathbb{F}_p)$. Or l'équation $a^2 + b^2 + c^2 + d^2 = 0$ a une solution non triviale dans $\mathbb{F}_p$, et l'élément de $\mathbf{H}(\mathbb{F}_p)$ correspondant à une telle solution engendre un idéal à droite propre de $\mathbf{H}(\mathbb{F}_p)$. L'image réciproque dans H de cet idéal est un idéal principal de la forme 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 que $p^2 = N(p) = N(z_0)N(z')$. Or $N(z_0) > 1$ et $N(z') > 1$ (sinon z_0 ou z_1 est inversible dans H), donc on a finalement $N(z_0) = p$ par primalité.

f) Il suffit de montrer que dans la question précédente, on peut trouver $z \in \mathbf{H}(\mathbb{Z})$ tel que $N(z) = p$. Supposons que ce ne soit pas le cas et regardons l'image de $\xi = 2z_0$ dans $\mathbf{H}(\mathbb{Z})/4\mathbf{H}(\mathbb{Z}) \simeq \mathbf{H}(\mathbb{Z}/4\mathbb{Z})$ (où $z_0 \in H \setminus \mathbf{H}(\mathbb{Z})$ vérifie $N(z_0) = p$). Dans $\mathbf{H}(\mathbb{Z}/4\mathbb{Z})$, la norme de ξ est nulle, c'est-à-dire que $\xi\overline{\xi} = 0$. Il suffit alors de relever $\overline{\xi}$ en un élément de $\{\varepsilon_1 1 + \varepsilon_2 i + \varepsilon_3 j + \varepsilon_4 k : \varepsilon_1, \ldots, \varepsilon_4 \in \{\pm 1\}\} \subseteq \mathbf{H}(\mathbb{Z})$, et de poser $z_1 := \frac{1}{2}\overline{\xi}$ dans H. Il en résulte que $N(z_0z_1) = p$ (puisque $N(z_1) = 1$) avec $z_0z_1 \in \mathbf{H}(\mathbb{Z})$. On peut donc supposer dans la question e) que $z \in \mathbf{H}(\mathbb{Z})$.

Le résultat pour tout entier naturel se déduit alors de la question b) et de la décomposition en facteurs premiers dans $\mathbb{Z}$.

Exercice 12 : $\star\star\star$

Soient K un corps de caractéristique $\neq 2$, $\alpha, \beta \in K^*$. On note $\mathbf{H} := \mathbf{H}_{\alpha,\beta}$ (voir l'exercice 10 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 $\mathbf{P} \subset \mathbf{H}$ 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 12.

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 10, 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 :

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

(noter que ce résultat généralise l'isomorphisme obtenu à l'exercice 7, question d), de la feuille de TD7, dans le cas où K était un corps fini).

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

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

isomorphisme qui généralise le cas des corps finis traité à la question e) de l'exercice 7 de la feuille de TD7.