TD10 : Formes sesquilinéaires, formes hermitiennes, formes quadratiques.

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 $\begin{array}{rccc} {}^t v : & F^* & \to & E^* \\ & f & \mapsto & f \circ v \end{array}$.

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 ${}^t u(d_\phi(E)) \subseteq d_\phi(E)$.

b) Donner un exemple où E est de dimension infinie, d_ϕ est injective, mais où ${}^t u(d_\phi(E))$ 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 ${}^t u(d_\phi(y)) = d_\phi(y) \circ u = d_\phi(u^*(y))$ pour tout $y \in E$.
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.

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 ${}^t u(e_2^*) = e_1^* \notin d_\phi(E)$ 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 : $\star\star$
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 6.

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 7 : $\star$

Décomposer sous forme de combinaison linéaire de carrés les formes quadratiques réelles suivantes ; en déduire leur signature et leur rang.

a) $f(x,y,z) = x^2 - 2y^2 + xz + yz$.

b) $f(x,y,z) = 2x^2 - 2y^2 - 6z^2 + 3xy - 4xz + 7yz$.

c) $f(x,y,z) = 3x^2 + 3y^2 + 3z^2 - 2xy - 2xz - 2yz$.

d) $f(x,y,z,t) = xy + yz + zt + tx$.

e) $f(x_1,\dots,x_n) = \sum_{1\leq i<j\leq n} x_i x_j$.

f) $f(A) = \mathrm{tr}(A^2)$, pour $A \in M_n(\mathbb{R})$.

g) $f(A) = \mathrm{tr}({}^tAA)$, pour $A \in M_n(\mathbb{R})$.

h) $f(A) = \mathrm{tr}(A)^2$, pour $A \in M_n(\mathbb{R})$.

Solution de l'exercice 7. On applique l'algorithme de Gauss pour diagonaliser la plupart de ces formes quadratiques. On obtient :

a) $f(x,y,z) = \left(x + \frac{z}{2}\right)^2 - 2\left(y - \frac{z}{4}\right)^2 - \frac{z^2}{8}$. Donc $\mathrm{sign}(f) = (1,2)$ et $\mathrm{rang}(f) = 3$.

b) $f(x,y,z) = 2\left(x + \frac{3}{4}y - z\right)^2 - \frac{25}{8}\left(y - \frac{8}{5}z\right)^2$. Donc $\mathrm{sign}(f) = (1,1)$ et $\mathrm{rang}(f) = 2$.

c) $f(x,y,z) = 3\left(x + \frac{y}{3} - \frac{z}{3}\right)^2 + \frac{8}{3}\left(y - \frac{z}{2}\right)^2 - 2z^2$. Donc $\mathrm{sign}(f) = (2,1)$ et $\mathrm{rang}(f) = 3$.

d) $f(x,y,z) = \frac{1}{4}(x + z + y + t)^2 - \frac{1}{4}(x + z - y - t)^2$. Donc $\mathrm{sign}(f) = (1,1)$ et $\mathrm{rang}(f) = 2$.

e) On peut par exemple remarquer que la matrice associée à f dans la base canonique admet pour valeurs propres $-\frac{1}{2}$ avec multiplicité $n-1$ (avec des vecteurs propres de la forme $e_i - e_1$, $2 \leq i \leq n$, où (e_i) est la base canonique) et $\frac{n-1}{2}$ avec mutiplicité 1 (utiliser la trace). Donc on en déduit que $\mathrm{sign}(f) = (1, n-1)$ et $\mathrm{rang}(f) = n$.

f) La forme polaire de f est la forme bilinéaire symétrique $(A,B) \mapsto \mathrm{tr}(AB)$. On remarque que la restriction de f au sous-espace $S_n(\mathbb{R})$ des matrices symétriques est définie positive, alors que la restriction de f au sous-espace $A_n(\mathbb{R})$ des matrices antisymétriques est définie négative. En outre, ces deux sous-espaces sont en somme directe et engendre $M_n(\mathbb{R})$, et ils sont orthogonaux pour q. Cela assure que $\mathrm{sign}(q) = (\dim(S_n(\mathbb{R})), \dim(A_n(\mathbb{R}))) = \left(\frac{n(n+1)}{2}, \frac{n(n-1)}{2}\right)$ et $\mathrm{rang}(f) = n^2$. On peut aussi trouver directement la décomposition en carrés en remarquant que si $A = (a_{i,j})$, on a

$$f(A) = \sum_{i,j} a_{i,j}a_{j,i} = \sum_i a_{i,i}^2 + 2\sum_{i<j} a_{i,j}a_{j,i} = \sum_i a_{i,i}^2 + \frac{1}{2}\sum_{i<j}(a_{i,j} + a_{j,i})^2 - \frac{1}{2}\sum_{i<j}(a_{i,j} - a_{j,i})^2.$$

g) Il est classique que f est la forme quadratique associée au produit scalaire canonique $(A,B) \mapsto \mathrm{tr}({}^tAB)$, donc f est définie positive, donc $\mathrm{sign}(f) = (n^2, 0)$ et $\mathrm{rang}(f) = n^2$. La décoposition en carrés est donnée par $f(A) = \sum_{i,j} a_{i,j}^2$.

h) Par définition, f est le carré d'une forme linéaire non nulle (la trace), donc $\mathrm{sign}(f) = (1,0)$ et $\mathrm{rang}(f) = 1$.

Exercice 8 :
Soit $n \geq 1$ et soit $\mathbb{R}_n[X]$ l'espace vectoriel des polynômes réels de degré inférieur ou égal à n. Pour tous $P, Q \in \mathbb{R}_n[X]$, on pose :

$$B(P,Q) = \int_0^1 tP(t)Q'(t)dt \qquad \text{et} \qquad f(P) = B(P,P).$$

a) Montrer que B est une forme bilinéaire. Est-elle symétrique ? Antisymétrique ?

b) La forme f a-t-elle des vecteurs isotropes non nuls ?

c) Calculer la matrice de f dans la base $(1, X, \dots, X^n)$.

d) Pour $n = 2$, déterminer la signature de f. La forme f est-elle positive ? Négative ?

Solution de l'exercice 8.

a) La linéarité de l'intégrale assure que B est bilinéaire. On a $B(1,X) = 1/2$ et $B(X,1) = 0$ et donc B n'est ni symétrique ni antisymétrique.

b) On a $f(1) = 0$ et donc $1 \in \mathbb{R}_n[X]$ est un vecteur isotrope.

c) Notons que la forme polaire de f n'est pas B mais sa symétrisée, à savoir

$$B_s(P,Q) := \frac{1}{2}\left(B(P,Q) + B(Q,P)\right).$$

Un petit calcul assure que la matrice de f (i.e. de B_s) dans la base indiquée est $M_n = \left(\frac{i+j-2}{2(i+j-1)}\right)_{1\leq i,j\leq n}$.

d) La signature est $(1,2)$.

Exercice 9 : $\star$

Soit K un corps de caractéristique différente de 2. Soit P un K-espace vectoriel de dimension 2, muni d'une forme quadratique f. Quelles sont valeurs possibles pour le nombre de droites isotropes de f ? Donner un exemple dans chaque cas.

Solution de l'exercice 9.

— La forme f n'a aucune droite isotrope si et seulement si elle est anisotrope (par définition). Or il existe une forme quadratique anisotrope sur P si et seulement si le corps K n'est pas quadratiquement clos : il suffit de considérer la forme $f(x,y) = x^2 - \alpha y^2$ sur K^2, où $\alpha \in K^* \setminus (K^*)^2$. En particulier, ce cas n'arrive pas sur un corps algébriquement clos.

— La forme f a une unique droite isotrope si et seulement si $\mathrm{rang}(f) = 1$. Ceci arrive sur tout corps K, il suffit de considérer par exemple la forme quadratique $f(x,y) = x^2$ sur K^2 (la seule droite isotrope est la droite d'équation $x = 0$).

— La forme f a exactement deux droites isotropes si et seulement si elle est hyperbolique, i.e. non dégénérée et admettant un vecteur isotrope. Une telle forme existe sur tout corps K, comme le montre l'exemple $f(x,y) = x^2 - y^2$ sur K^2 (droites isotropes d'équations $x+y=0$ et $x-y=0$).

— Supposons que la forme f ait au moins 3 droites isotropes. Notons alors v_1, v_2, v_3 trois vecteurs isotropes deux-à-deux non proportionnels. Puisque (v_1, v_2) est une base de P, il existe $\lambda, \mu \in K^*$ tels que $v_3 = \lambda v_1 + \mu v_2$. On applique la forme f, et si on note b la forme polaire de f, on obtient

$$0 = f(v_3) = f(\lambda v_1 + \mu v_2) = \lambda^2 f(v_1) + \mu^2 f(v_2) + 2\lambda\mu b(v_1, v_2) = 2\lambda\mu b(v_1, v_2).$$

Donc $b(v_1, v_2) \neq 0$, donc la matrice de f dans la base (v_1, v_2) est la matrice nulle (c'est une base orthogonale formée de vecteurs isotropes), donc $f = 0$.

Finalement, une forme quadratique sur un plan vectoriel admet soit aucune droite isotrope, soit une droite isotrope, soit deux droites isotropes, soit toutes les droites de P sont isotropes. Tous ces cas arrivent sur tout corps K, sauf le premier (aucune droite isotrope) qui existe si et seulement si K n'est pas quadratiquement clos.

Exercice 10 : $\star\star$

Soit K un corps de caractéristique différente de 2 et soit E un K-espace vectoriel de dimension finie. Soient f et f' des formes quadratiques sur E vérifiant $f^{-1}(0) = (f')^{-1}(0)$.

a) Supposons K algébriquement clos. Montrer qu'il existe $a \in K^\times$ tel que l'on ait $f' = af$.

b) Donner un contre-exemple pour $K = \mathbb{R}$ et $E = \mathbb{R}^2$.

Solution de l'exercice 10.

a) Soient b et b' les formes bilinéaires respectives de f et f'. Si f est totalement isotrope, le résultat est clair. Supposons que ce ne soit pas le cas : il existe $x \in E$ avec $f(x) \neq 0$. Posons $a = f'(x)f(x)^{-1} \in K^\times$. Soit $y \in E$. Les polynômes $af(y + \lambda x)$ et $f'(y + \lambda x)$ de $K[\lambda]$ sont de degré 2, ont mêmes racines par hypothèse, et ils ont même coefficient dominant $f'(x)$: ils sont donc égaux puisque K est algébriquement clos. En particulier, on a $f'(y) = af(y)$. Donc $f' = af$.

b) Il suffit de considérer les formes quadratiques x^2+y^2 et x^2+2y^2.

Cet exercice est un cas très particulier du théorème des zéros de Hilbert (le Nullstellensatz de Hilbert) : soit K un corps algébriquement clos, $I \subset K[X_1,\dots,X_n]$ un idéal et notons $Z(I)$ l'ensemble des zéros communs à tous les polynômes de I. Si f est un polynôme qui s'annule sur $Z(I)$, alors il existe $n \in \mathbb{N}$ tel que $f^n \in I$.

Exercice 11 : $\star\star$
Soit K un corps de caractéristique différente de 2, soit E un K-espace vectoriel de dimension finie non nulle et soit H un hyperplan de E. Soient de plus f une forme quadratique non dégénérée sur E et u un élément de $\mathcal{O}(E,f)$ vérifiant $u_{|H} = \mathrm{id}_H$.

a) Si $f_{|H}$ est non dégénérée, montrer que u est soit l'identité, soit la réflexion orthogonale d'hyperplan H.

b) Si $f_{|H}$ est dégénérée, montrer que u est l'identité.

Solution de l'exercice 11. Notons b la forme bilinéaire associée à f.

a) Si $f_{|_H}$ est non dégénérée, l'orthogonal de H pour b est un supplémentaire de H, de dimension 1, disons égal à Kx. Alors $b(u(x),u(h)) = b(x,h) = 0$ pour tout $h \in H$, ce qui assure que $u(x) \in Kx$ et $f(u(x)) = f(x)$ donne $u(x) = \pm x$ (car $f(x) \neq 0$ puisque $x \notin H\ \perp$). Donc $u = \mathrm{id}$ ou u est la réflexion orthogonale (i.e. parallèlement à $H^\perp$) d'hyperplan H.

b) Si $f_{|_H}$ est dégénérée, il existe $h \in H^\perp \cap H$ non nul. On peut le compléter en un plan hyperbolique (au passage, comme $H^\perp$ est de dimension 1, cela force $H^\perp \cap H$ à être égal à $H^\perp$) grâce à un $y \notin H$. Ecrivons $u(y) = \alpha y + h'$ avec $\alpha \in K$ et $h' \in H$. On a $1 = b(y,h) = b(u(y),u(h)) = \alpha$ et $b(u(y)-y,n) = 0$ pour tout $n \in H$. On peut donc écrire $u(y) = y + \beta h$. Mais alors on a $f(y) + 2\beta = f(u(y)) = f(y)$, d'où $\beta = 0$. Donc $u = \mathrm{id}$.

Exercice 12 :
Soit $n \geq 1$ et soit $E = \mathbb{R}^{n+1}$ muni de la forme quadratique

$$f(x_0,\dots,x_n) = x_0^2 - (x_1^2 + \cdots + x_n^2),$$

de forme bilinéaire b. Un sous-espace F de E est dit *elliptique* si $f_{|F}$ est définie négative, *hyperbolique* si $f_{|F}$ est de signature $(1,m)$ avec $m \geq 1$ et *parabolique* si F est isotrope.

a) Soit F un sous-espace de dimension au moins 2 tel qu'il existe $x \in F$ avec $f(x) > 0$. Montrer que F est hyperbolique.

b) Soit F un sous-espace elliptique de dimension au plus $n-1$. Montrer que $F^\perp$ est hyperbolique.

c) Soit F un sous-espace parabolique. Montrer que $f|_F$ est de rang $\dim F - 1$.

Solution de l'exercice 12.

a) C'est évident. Montrons même que $f_{|_F}$ est non dégénérée. Supposons le contraire : il existe $t \in F \cap F^\perp$ non nul. On a alors $f(x+t) = f(x) > 0$ et la restriction de f au plan engendré par x et t est définie positive, ce qui contredit le fait que $\mathrm{sign}(f) = (1,n)$. Donc $f_{|F}$ est non dégénérée, ce qui assure que $\mathrm{sign}(f) = (1, \dim F - 1)$.

b) Supposons $f(t') \leq 0$ pour tout $t' \in F^\perp$. Comme on a $E = F \oplus F^\perp$ (pas de vecteur isotrope dans F), écrivons tout élément $e = t(e) + t'(e)$ suivant cette décomposition. On aurait alors $f(e) = f(t(e)) + f(t'(e)) \leq 0$, ce qui n'est pas vrai pour $(1,0,\dots,0)$. De ce fait, il existe $x \in F^\perp$ avec $f(x) > 0$ et on applique la question a).

c) Supposons $f_{|_F}$ de rang $\leq \dim F - 2$. Alors $f_{|_F}$ possède deux vecteurs isotropes qui se complètent en deux plans hyperboliques distincts dans E. Or E ne contient pas de somme directe de deux plans hyperboliques (sinon sa signature serait (p,q) avec $p \geq 2$). L'hypothèse initiale est donc erronée.

Exercice 13 : $\star\star$

Soient $p \neq q$ deux nombres premiers impairs. On note $\left(\frac{p}{q}\right)$ l'entier qui vaut 1 si p est un carré modulo q et -1 sinon. On note $S := \{(x_1, \dots, x_p) \in \mathbb{F}_q^p : \sum_i x_i^2 = 1\}$.

a) Montrer que $\left(\frac{q}{p}\right) \equiv q^{\frac{p-1}{2}}\ [p]$.

b) En considérant une action de groupe, montrer que $|S| \equiv 1 + \left(\frac{p}{q}\right)\ [p]$.

c) Montrer qu'il existe une base de $\mathbb{F}_q^p$ dans laquelle la forme quadratique $\sum_i X_i^2$ admet pour matrice $\operatorname{diag}\left(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \dots, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, (-1)^{\frac{p-1}{2}}\right)$.

d) En déduire que $|S| = q^{\frac{p-1}{2}}(q^{\frac{p-1}{2}} + (-1)^{\frac{p-1}{2}\frac{q-1}{2}})$.

e) Conclure que $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$ (c'est la loi de réciprocité quadratique).

Solution de l'exercice 13.

a) Soit $a \in \mathbb{F}_p^*$. S'il existe $b \in \mathbb{F}_p^*$ tel que $a = b^2$, alors $a^{\frac{p-1}{2}} = b^{p-1} = 1$. Donc les $\frac{p-1}{2}$ carrés non nuls dans $\mathbb{F}_p$ sont racines du polynôme $X^{\frac{p-1}{2}} - 1 \in \mathbb{F}_p[X]$. Or ce polynôme admet au plus $\frac{p-1}{2}$ racines, donc ses racines sont exactement les carrés non nuls. Or pout tout $a \in \mathbb{F}_p^*$, $\left(a^{\frac{p-1}{2}}\right)^2 = 1$, donc $a^{\frac{p-1}{2}} = \pm 1$. Cela assure que pour tout $a \in \mathbb{Z}$ non divisible par p, $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}}\ [p]$ (le symbole $\left(\frac{a}{p}\right)$ est défini de façon évidente). D'où le résultat.

b) Le groupe $G = \mathbb{Z}/p\mathbb{Z}$ agit sur S par permutation circulaire. L'équation aux classes assure que $|S^G| \equiv |S|\ [p]$. Or $S^G \cong \{x \in \mathbb{F}_q : (x, \dots, x) \in S\} = \{x \in \mathbb{F}_q : px^2 = 1\}$. Donc $S^G = \emptyset$ si p n'est pas un carré modulo q, et $|S^G| = 2$ si p est u carré modulo q. D'où le résultat.

c) Les deux formes quadratiques mentionnées sont de rang p et de discriminant 1, donc elles sont équivalentes sur $\mathbb{F}_q$ (voir le théorème de classification des formes quadratiques sur un corps fini). D'où le résultat.

d) La question c) assure que

$$|S| = \left|\{(x_1, \dots, x_p) \in \mathbb{F}_q^p : x_1x_2 + \dots + x_{p-2}x_{p-1} + (-1)^{\frac{p-1}{2}}x_p^2 = 1\}\right|.$$

Notons $T := \{(x_1, \dots, x_p) \in \mathbb{F}_q^p : x_1x_2 + \dots + x_{p-2}x_{p-1} + (-1)^{\frac{p-1}{2}}x_p^2 = 1\}$, $T_0 := \{(x_1, \dots, x_p) \in T : x_1 = \dots = x_{p-2} = 0\}$ et $T_1 := T \setminus T_0$. Il est clair que $|T_0| = \left(1 + \left(\frac{(-1)^{\frac{p-1}{2}}}{q}\right)\right) q^{\frac{p-1}{2}} = \left(1 + (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\right) q^{\frac{p-1}{2}}$. Ensuite, pour tout $(x_1, \dots, x_{p-2}) \in \mathbb{F}_q^{\frac{p-1}{2}} \setminus \{0\}$, et tout $x_p \in \mathbb{F}_q$, l'équation

$$x_1x_2 + \dots + x_{p-2}x_{p-1} + (-1)^{\frac{p-1}{2}}x_p^2 = 1$$

définit un hyperplan affine de $\mathbb{F}_q^{\frac{p-1}{2}}$, donc l'ensemble des solutions de cette équation est de cardinal $q^{\frac{p-3}{2}}$. Cela assure que $|T_1| = \left(q^{\frac{p-1}{2}} - 1\right) q q^{\frac{p-3}{2}} = \left(q^{\frac{p-1}{2}} - 1\right) q^{\frac{p-1}{2}}$. Donc finalement

$$|S| = |T| = |T_0| + |T_1| = q^{\frac{p-1}{2}}\left(q^{\frac{p-1}{2}} + (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\right).$$

e) Les questions a), b) et d) assurent que

$$1 + \left(\frac{p}{q}\right) \equiv q^{\frac{p-1}{2}}\left(q^{\frac{p-1}{2}} + (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\right)\ [p],$$

donc en utilisant la question a),

$$\left(\frac{p}{q}\right) \equiv (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{q}{p}\right)\ [p].$$

Puisque ces nombres valent ± 1, on en déduit que

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{q}{p}\right).$$

Exercice 14 : $\star\star\star$

Soient $a, b, c \in \mathbb{Z}$ sans facteurs carrés. On considère la forme quadratique $f(x, y, z) := ax^2 + by^2 + cz^2$ sur $\mathbb{Q}^3$.

a) À quelle condition sur a, b, c la forme f est-elle isotrope sur $\mathbb{R}$?

b) On suppose $a, b > 0$ et $c = -1$ et on note d le pgcd de a et b. Montrer que la forme quadratique f est isotrope sur $\mathbb{Q}$ si et seulement si les trois conditions suivantes sont satisfaites

   i) a est un carré modulo b.

   ii) b est un carré modulo a.

   iii) $-\frac{ab}{d^2}$ est un carré modulo d.

c) On suppose désormais a, b, c deux-à-deux premiers entre eux. Montrer que f est isotrope sur $\mathbb{Q}$ si et seulement si f est isotrope sur $\mathbb{R}$ et les trois conditions suivantes sont satisfaites

   i) $-ab$ est un carré modulo c.

   ii) $-ac$ est un carré modulo b.

   iii) $-bc$ est un carré modulo a.

d) Sous les hypothèses de la question c), montrer que f est isotrope sur $\mathbb{Q}$ si et seulement si f est isotrope sur $\mathbb{R}$ et pour tout nombre premier p, pour tout entier $m \geq 1$, il existe $(x, y, z) \in \mathbb{Z}^3$ non tous divisibles par p tels que $f(x, y, z) \equiv 0\ [p^m]$.

e) Vérifier que dans l'équivalence précédente, il suffit de prendre $p|abc$ et $m = 2$.

f) Soit q une forme quadratique non dégénérée sur $\mathbb{Q}^3$. Donner un algorithme permettant de décider si q est isotrope.

Solution de l'exercice 14.

a) Il faut et il suffit que a, b, c ne soient pas tous de même signe.

b) — On suppose f isortrope sur $\mathbb{Q}$: il existe $(x, y, z) \in \mathbb{Q}^3 \setminus \{(0, 0, 0)\}$ tel que $f(x, y, z) = 0$. Quitte à multiplier x, y, z par le ppcm des dénominateurs de x, y, z, et à diviser par le pgcd des numérateurs, on peut supposer que $x, y, z \in \mathbb{N}$ sont des entiers premiers entre eux dans leur ensemble, vérfiant $ax^2 + by^2 = z^2$. Soit p un nombre premier divisant b et x. Alors $p|z$, donc $p^2|by^2$. Comme b est sans facteur carré, $p|y$, donc p divise x, y et z. Or x, y, z sont premiers entre eux, donc $\text{pgcd}(b, x) = 1$. Donc en réduisant l'égalité modulo b, on obtient que $ax^2 \equiv z^2\ [b]$. Comme x et b sont premiers entre eux, x est inversible modulo b, donc a est un carré modulo b. Par symétrie, on a également que b est un carré modulo a.
Comme d divise a et b, on sait que $d|z^2$. Comme a et b sont sans facteur carré, d est sans facteur carré, ce qui assure que $d|z$, i.e. $z = dz'$ avec $z' \in \mathbb{Z}$. Écrivons de même $a = da'$ et $b = db'$. On peut donc diviser l'égalité $ax^2 + by^2 = z^2$ par d pour obtenir $a'x^2 + b'y^2 = dz'^2$. On réduit modulo d cette égalité et on obtient $a'x^2 + b'y^2 \equiv 0\ [d]$, ce qui assure, puisque x et y sont premiers à d, que $a'b'$ est un carré modulo d. Donc $\frac{ab}{d^2}$ est un carré modulo d.
— Réciproquement, supposons les conditions i), ii) et iii) satisfaites. On raisonne par récurrence sur a. Si $a = 1$, le résultat est évident, car $(x, y, z) = (1, 0, 1)$ est un vecteur isotrope de f. Soit alors $a > 1$. Quitte à échanger a et b, alors on peut supposer que $a \geq b$. Dans le cas où $a = b$, la condition iii) assure que -1 est un carré modulo b, donc b est somme de deux carrés dans $\mathbb{Z}$, i.e. $a = b = s^2 + t^2$, et on vérifie que $(s, t, s^2 + t^2)$ est un vecteur isotrope de f. Donc on peut supposer $a > b$.
On construit maintenant $0 < a' < a$ tel que f est isotrope si $a'x^2 + by^2 - z^2$ l'est. Pour ce faire, on sait que la propriété ii) implique l'existence de $c, k \in \mathbb{Z}$ tels que $b = c^2 - ka$. Il existe $a', m \in \mathbb{Z}$ tels que $k = a'm^2$, avec a' sans facteur carré. On peut en outre supposer

que $|c| \leq \frac{a}{2}$. Montrons que $0 < a' < a$. On a $c^2 = b + aa'm^2$. Comme $c^2 > 0$ et $a > b$, on a néssairement $a' \geq 0$. Or b est sans facteur carré, donc $a \neq 0$, donc $a > 0$. La condition $|c| \leq \frac{a}{2}$ implique que $b + aa'm^2 \leq \frac{a^2}{4}$, donc $aa' < \frac{a^2}{4}$, donc $a < \frac{a}{4} < a$.

Vérifions maintenant que les propriétés i), ii) et iii) sont satisfaites pour la forme quadratique $a'x^2 + by^2 - z^2$. On écrit toujours $a = dA$ et $b = dB$, avec $d = \text{pgcd}(a, b)$. Alors $c^2 = dB + dAa'm^2$, ce qui implique, comme d est sans facteur carré, que $d|c$, i.e. $c = dC$ avec $C \in \mathbb{Z}$. On a donc $dC^2 = B + Aa'm^2$. Donc $Aa'm^2 \equiv -B\,[d]$, donc $a'A^2m^2 \equiv -AB\,[d]$. Or $\text{pgcd}(d, m) = 1$, et par iii), $-AB$ est un carré modulo d, donc a' est un carré modulo d. De même, la relation $c^2 \equiv a'am^2\,[B]$ et l'hypothèse i) assurent que a' est un carré modulo B. Donc a' est un carré modulo $Bd = b$.

Notons maintenant $r := \text{pgcd}(a', b)$, $a' = rA'$, $b = rB'$. Montrons que $-A'B'$ est un carré modulo r. Par définition, on a $c^2 = rB' + raA'm^2$, donc $r|c$ (car r est sans facteur carré), donc en notant $c = rC$, on a $rC^2 = B' + aA'm^2$. On réduit modulo r et on obtient $aA'm^2 = -B'\,[r]$. Or par i), a est un carré modulo b, donc modulo r, donc $-A'B'$ est bien un carré modulo r.

Supposons maintenant que la forme quadratique $f'(x, y, z) = a'x^2 + +by^2 - z^2$ soit isotrope sur $\mathbb{Q}^3$, et notons (x_0, y_0, z_0) un vecteur isotrope dans $\mathbb{Q}^3$. Alors $a'x_0^2 = z_0^2 - by_0^2$, et en multipliant cette égalité avec $aa'm^2 = c^2 - b$, on obtient $a(a'mx_0)^2 = (z_0^2 - by_0^2)(c^2 - b)$, i.e. $a(a'mx_0)^2 + b(cy_0 + z_0)^2 - (cz_0 + by_0)^2 = 0$, donc $f(a'mx_0, cy_0 + z_0, cz_0 + by_0) = 0$, donc f est isotrope sur $\mathbb{Q}^3$.

Cela conclut la preuve par récurrence sur a.

c) On suppose que a et b sont de même signe et c de signe opposé. On pose $a' := -ac$, $b' := -bc$. En multipliant f par $-c$, on obtient que la forme quadratique f est $\mathbb{Q}$-isométrique à la forme quadratique $f'(x, y, z) = a'x^2 + b'y^2 - z^2 = 0$.

Alors la question b) assure que f est isotrope sur $\mathbb{Q}^3$ si et seulement si f' l'est si et seulement si $-ac$ est un carré modulo $-bc$, $-bc$ est un carré modulo $-ac$ et $-ab$ est un carré modulo c. On voit facilement que cela équivaut aux conditions i), ii) et iii) de l'énoncé.

Enfin, les conditions i),ii),iii) sont symétriques en a, b, c, ce qui assure que l'équivalence souhaitée : en effet, si f est isotrope sur $\mathbb{R}$, deux des coefficients de f sont de même signe et l'autre est de signe opposé, donc quitte à permuter a, b, c (ce qui n'affecte pas les conditions i),ii),iii)), on peut bien supposer a et b de même signe et c de signe opposé. D'où le résultat.

d) Le sens direct est clair. Montrons la réciproque. On suppose donc les conditions de l'énoncé vérifiées. Prenons $m = 2$ et p un facteur premier de a. Par hypothèse, il existe $x, y, z \in \mathbb{Z}^3$ non tous divisibles par p, tels que $f(x, y, z) \equiv 0\,[p^2]$. Il est clair que p ne divise pas yz (sinon $p^2|a$), donc $by^2 + cz^2 \equiv 0\,[p]$ implique que $-bc$ est un carré modulo p. Ceci étant valable pour tout $p|a$, on en déduit que $-bc$ est un carré modulo a. Par symétrie, on a également que $-ac$ est un carré modulo b et $-ab$ est un carré modulo c. La question c) assure alors que f est isotrope sur $\mathbb{Q}$.

e) C'est une conséquence immédiate de la solution à question d).

f) Montrons d'abord que q est isométrique sur $\mathbb{Q}$ à une forme quadratique $f(x, y, z) = ax^2 + by^2 + cz^2$ avec $a, b, c \in \mathbb{Z}$ deux-à-deux premiers entre eux. Pour cela, on commence d'abord par diagonaliser q, chasser les dénominateurs et diviser par le pgcd des coefficients apparaissant pour écrire q sous la forme $q(x, y, z) = a'x^2 + b'y^2 + c'z^2$, avec $a', b', c' \in \mathbb{Z}$ premiers entre eux dans leur ensemble et sans facteur carré. Notons $d := \text{pgcd}(a', b')$, avec $a' = da''$ et $b' = db''$. En multipliant q par d, on voit que q est équivalente à la forme quadratique $(x, y, z) \mapsto a''x^2 + b''y^2 + c''z^2$, avec $c'' := dc'$. Alors a'' et b'' sont premiers entre eux et a'', b'', c'' sont sans facteur carré, et $\text{pgcd}(a'', c'') = \text{pgcd}(a'', c')|\text{pgcd}(a', c')$ et $\text{pgcd}(b'', c'') = \text{pgcd}(b'', c')|\text{pgcd}(b', c')$. On répète successivement cette opération avec le couple de coefficients (a'', c''), ce qui donne des nouveaux coefficients $(a^{(3)}, b^{(3)}, c^{(3)})$, puis avec $(b^{(3)}, c^{(3)})$, ce qui fournit les coefficients (a, b, c) recherchés (tels que a, b, c soient sans facteur carré et deux-à-deux premiers entre eux. On applique alors la question e) pour décider algorithmiquement si la forme quadratique q est isotrope : on décompose a, b et c en facteurs premiers, et pour chaque p premier divisant a, b ou c, on teste si l'équation $ax^2 + by^2 + cz^2 = 0$ a une solution modulo p^2 non divisible par p. Enfin, on teste

si les trois entiers a, b, c sont de même signe ou non.

Remarque : cet exercice est un cas particulier du théorème de Hasse-Minkowski, qui affirme que pour toute forme quadratique non dégénérée q sur $\mathbb{Q}^n$ (que l'on peut supposer diagonale à coefficients premiers premiers entre eux dans leur ensemble), la forme q est isotrope si et seulement si elle est isotrope sur $\mathbb{R}$ et pour tout premier p et tout entier $n \geq 1$, l'équation $q = 0$ admet une solution modulo p^n formée d'entiers non tous divisibles par p (cela signifie que q est isotrope sur tous les corps p-adiques $\mathbb{Q}_p$).

Exercice 15 : $\star\star\star$

Soit K un corps. On définit son niveau $s(K) \in \mathbb{N} \cup \{\infty\}$ et, si la caractéristique de K n'est pas 2, son u-invariant $u(K) \in \mathbb{N} \cup \{\infty\}$ par

$$s(K) := \inf\{n \geq 1 \mid \exists (x_1, \ldots, x_n) \in K^n \quad x_1^2 + \cdots + x_n^2 = -1\}$$

et

$$u(K) := \sup\{\dim(q) : q \text{ forme quadratique anisotrope sur } K\},$$

avec la convention que l'infimum de l'ensemble vide est ∞.

a) Montrer que $u(K) \geq s(K)$.

b) Calculer $s(K)$ et $u(K)$ si K est algébriquement clos.

c) Donner un exemple de corps K avec $s(K) = \infty$ et un exemple avec $u(K) = \infty$ et $s(K) < \infty$.

d) Montrer que des corps isomorphes ont même niveau et même u-invariant. Les réciproques sont-elles vraies ?

e) Montrer que le niveau d'un corps fini est égal à 1 ou 2. Montrer que le u-invariant d'un corps fini vaut 2.

f) Montrer l'égalité $s(K) = s(K(X))$.

On suppose désormais que K de caractéristique différente de 2. Pour $n \geq 1$, on considère la forme quadratique

$$f_n(x_1, \ldots, x_n) = \sum_{i=1}^{n} x_i^2.$$

g) Montrer que f_n admet un vecteur isotrope si et seulement si on a $s(K) \leq n - 1$.

h) Supposons $n = 2^k$ avec $k \in \mathbb{N}$. Montrer que pour tout $x = (x_1, \ldots, x_n) \in K^n$ non nul, il existe une matrice T_x de première ligne $(x_1, \ldots, x_n)$ vérifiant

$${}^tT_xT_x = T_x{}^tT_x = f_n(x_1, \ldots, x_n)I_n.$$

i) En déduire que l'ensemble des sommes non nulles de 2^k carrés d'éléments de K est un groupe multiplicatif.

j) Montrer que le niveau d'un corps est soit infini, soit une puissance de 2.

Solution de l'exercice 15.

a) Soit $n < s(K)$. Alors par définition la forme quadratique $x_1^2 + \cdots + x_n^2 + x_{n+1}^2$ est anisotrope sur K^{n+1} (sinon, un vecteur isotrope contredit le fait que $n < s(K)$). Donc $u(K) \geq n + 1$. En appliquant ceci à $n = s(K) - 1$, on trouve $u(K) \geq s(K)$.

b) Si K est algébriquement clos, on a clairement $s(K) = 1$, et comme toute forme quadratique de rang 2 est isotrope, on a $u(K) = 1$.

c) Si $K = \mathbb{R}$, on a $s(K) = \infty$ (et donc $u(K) = \infty$). Si $K = \mathbb{C}(T_i; i \in \mathbb{N})$, alors $s(K) = 1$ et $u(K) = \infty$; en effet, pour tout $n \geq 0$, la forme quadratique $\sum_{i=0}^{n} T_i x_i^2$ est anisotrope sur K^{n+1}.

d) Le sens direct est évident. Les réciproques sont fausses, puisqu'on voit que $s(\mathbb{F}_5) = s(\mathbb{F}_{13}) = 1$ et $u(\mathbb{F}_5) = u(\mathbb{F}_{13}) = 2$. De même, pour tout corps algébriquement clos, $s(K) = s(\mathbb{C}) = u(K) = u(\mathbb{C}) = 1$.

e) L'élément -1 est un carré dans $\mathbb{F}_q$ si et seulement si $q = 2^r$ ou $q \equiv 1\,[4]$. Dans ce cas, on a $s(\mathbb{F}_q) = 1$, et sinon $s(\mathbb{F}_q) = 2$. Et pour tout q impair, on sait que $u(\mathbb{F}_q) = 2$.

f) On a immédiatemment $s(K) \geq s(K(X))$. Supposons donc $s(K(X))$ fini, et notons s cet entier. Il existe des fractions rationnelles $R_1(X), \ldots, R_s(X)$ telles que l'on ait $R_1(X)^2 + \cdots + R_s(X)^2 = -1$.
Supposons dans un premier temps K infini. En notant $Q(X)$ un dénominateur commun des $R_i(X)$, on obtient une identité de la forme $P_1(X)^2 + \cdots + P_s(X)^2 = -Q(X)^2$ dans $K[X]$. Comme K est infini, il existe $\alpha \in K$ tel que $Q(\alpha) \neq 0$. Pour tout i, notons $p_i^{(\alpha)} = P_i(\alpha)Q(\alpha)^{-1} \in K$. On a alors $(p_1^{(\alpha)})^2 + \cdots + (p_s^{(\alpha)})^2 = -1$. Ceci donne $s(K) \leq s(K(X))$.
Dans le cas où K est fini, par la question e), on peut supposer $s(K(X)) = 1$. Alors $R_1(X)$ s'écrit $\frac{P_1(X)}{Q(X)}$ avec $P_1(X), Q(X) \in K[X]$. En choisissant $P_1(X)$ et $Q(X)$ premiers entre eux, on voit que $R_1(X)$ est un élément de K^*. Cela donne $s(K) = 1$ aussi. Ce qui conclut la preuve.

g) Si on a $s(K) \leq n-1$, alors il existe $x_1, \ldots, x_{n-1} \in K$ tels que $x_1^2 + \cdots + x_{n-1}^2 + 1^2 = 0$. Réciproquement, si f_n a un vecteur isotrope $(x_1, \ldots, x_n)$ avec $x_i \neq 0$, alors $\sum_{j \neq i} \left(\frac{x_j}{x_i}\right)^2 = -1$.

h) Montrons le par récurrence sur $k \geq 0$. Le cas $k = 0$ est trivial. Supposons la propriété vraie au rang k et prouvons le rang $k+1$. Par hypothèse de récurrence, on a T_1 et T_2 vérifiant

$$ {}^tT_1T_1 = T_1{}^tT_1 = f_n(x_1, \ldots, x_n)I_n, \quad {}^tT_2T_2 = T_2{}^tT_2 = f_n(x_{n+1}, \ldots, x_{2n})I_n. $$

On calcule ensuite

$$ \begin{pmatrix} {}^tT_1 & {}^tA \\ {}^tT_2 & {}^tB \end{pmatrix} \begin{pmatrix} T_1 & T_2 \\ A & B \end{pmatrix} = \begin{pmatrix} {}^tT_1T_1 + {}^tAA & {}^tT_1T_2 + {}^tAB \\ {}^tT_2T_1 + {}^tBA & {}^tT_2T_2 + {}^tBB \end{pmatrix}, $$

et

$$ \begin{pmatrix} T_1 & T_2 \\ A & B \end{pmatrix} \begin{pmatrix} {}^tT_1 & {}^tA \\ {}^tT_2 & {}^tB \end{pmatrix} = \begin{pmatrix} T_1{}^tT_1 + T_2{}^tT_2 & T_1{}^tA + T_2{}^tB \\ A{}^tT_1 + B{}^tT_2 & A{}^tA + B{}^tB \end{pmatrix}. $$

Alors :

i) si $f_n(x_1, \ldots, x_n) \neq 0$, on prend $A = T_1^{-1}{}^tT_2T_1$ et $B = -{}^tT_1$.

ii) sinon, si $f_n(x_{n+1}, \ldots, x_{2n}) \neq 0$, on prend $A = -{}^tT_2$ et $B = T_2^{-1}{}^tT_1T_2$.

iii) enfin, si $f_n(x_1, \ldots, x_n) = f_n(x_{n+1}, \ldots, x_{2n}) = 0$, on prend $A = -T_1$ et $B = T_2$.

Les calculs précédents assurent alors que la matrice $T_x := \begin{pmatrix} T_1 & T_2 \\ A & B \end{pmatrix}$ convient.

i) Si $f_n(x)$ et $f_n(y)$ sont deux sommes non nulles de 2^k carrés d'éléments, il suffit de définir $x \cdot y$ comme étant la première ligne de T_xT_y et on a $f_n(x \cdot y) = f_n(x)f_n(y)$. De même, si $[-1].x$ désigne la première ligne de T_x^{-1}, on obtient $f_n([-1].x) = f_n(x)^{-1}$.

j) Supposons $s(K)$ fini, vérifiant $n := 2^k \leq s(K) < 2n = 2^{k+1}$ pour un certain $k \geq 0$. Alors f_{2n} possède un vecteur isotrope par la question g), disons $(x_1, \ldots, x_{2n})$. On a donc $f_n(x_1, \ldots, x_n) = -f_n(x_{n+1}, \ldots, x_{2n}) \neq 0$. Mais alors $f_n(x_1, \ldots, x_n)f_n(x_{n+1}, \ldots, x_{2n})^{-1} = -1$ est une somme de 2^k carrés par la question i).
Remarque : réciproquement, pour tout $n = 2^k$, il existe un corps K de niveau n. On peut par exemple considérer le corps $K = \mathbb{R}(X_1, \ldots, X_{n-1})[X_n]/(\sum X_i^2 + 1)$ (voir par exemple le théorème 2.8 du chapitre 11 de Lam, *Algebraic theory of quadratic forms*).