TD10 : Formes sesquilinéaires, formes hermitiennes, formes quadratiques.

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

Exercice 1 : $\star$
Montrer que toute forme sesquilinéaire réelle est bilinéaire.

Exercice 2 : $\star$
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 ?

Exercice 3 : $\star\star$
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.

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

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 $d_\phi(E)$.

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 $x, y \in E_1$.

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 $\mathrm{PSU}_n(\mathbb{F}_{q^2})$.

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

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

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 ?

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.

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 $E = \mathbb{R}^2$.

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.

Exercice 12 :

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

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

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 $\dim F - 1$.

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 $S := \{(x_1, \ldots, x_p) \in \mathbb{F}_q^p : \sum_i x_i^2 = 1\}$.

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 $\mathrm{diag}\left(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \ldots, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, (-1)^{\frac{p-1}{2}}\right)$.

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).

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.

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

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

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.