

TD7 : 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

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

Solution de l'exercice 1. On applique l'algorithme de Gauss pour diagonaliser la plupart de ces formes quadratiques. On obtient :

- a) $f(x, y, z) = (x + \frac{z}{2})^2 - 2(y - \frac{z}{4})^2 - \frac{z^2}{8}$. Donc $\text{sign}(f) = (1, 2)$ et $\text{rang}(f) = 3$.
- b) $f(x, y, z) = 2(x + \frac{3}{4}y - z)^2 - \frac{25}{8}(y - \frac{8}{5}z)^2$. Donc $\text{sign}(f) = (1, 1)$ et $\text{rang}(f) = 2$.
- c) $f(x, y, z) = 3(x + \frac{y}{3} - \frac{z}{3})^2 + \frac{8}{3}(y - \frac{z}{2})^2 - 2z^2$. Donc $\text{sign}(f) = (2, 1)$ et $\text{rang}(f) = 3$.
- d) $f(x, y, z) = \frac{1}{4}(x + z + y + t)^2 - \frac{1}{4}(x + z - y - t)^2$. Donc $\text{sign}(f) = (1, 1)$ et $\text{rang}(f) = 2$.
- 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 multiplicité 1 (utiliser la trace). Donc on en déduit que $\text{sign}(f) = (1, n - 1)$ et $\text{rang}(f) = n$.
- f) La forme polaire de f est la forme bilinéaire symétrique $(A, B) \mapsto \text{tr}(AB)$. 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 engendrent $M_n(\mathbb{R})$, et ils sont orthogonaux pour q . Cela assure que $\text{sign}(q) = (\dim(S_n(\mathbb{R})), \dim(A_n(\mathbb{R}))) = (\frac{n(n+1)}{2}, \frac{n(n-1)}{2})$ et $\text{rang}(f) = n^2$. 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 $(A, B) \mapsto \text{tr}({}^tAB)$, donc f est définie positive, donc $\text{sign}(f) = (n^2, 0)$ et $\text{rang}(f) = n^2$. La décomposition 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 $\text{sign}(f) = (1, 0)$ et $\text{rang}(f) = 1$.

Exercice 2 :

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 :

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

- Montrer que B est une forme bilinéaire. Est-elle symétrique ? Antisymétrique ?
- La forme f a-t-elle des vecteurs isotropes non nuls ?
- Calculer la matrice de f dans la base $(1, X, \dots, X^n)$.
- Pour $n = 2$, déterminer la signature de f . La forme f est-elle positive ? Négative ?

Solution de l'exercice 2.

- 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.
- On a $f(1) = 0$ et donc $1 \in \mathbb{R}_n[X]$ est un vecteur isotrope.
- Notons que la forme polaire de f n'est pas B mais sa symétrisée, à savoir

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

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

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

Exercice 3 : *

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 3.

- 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 $\text{rang}(f) = 1$. 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 4 : **

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 4.

- 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 5 : ★★

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 $u|_H = \text{id}_H$.

- 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 5. 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 $u = \text{id}$ 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 $y \notin H$. Écrivons $u(y) = \alpha y + h'$ 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 $u = \text{id}$.

Exercice 6 :

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

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

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 6.

- 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 $\text{sign}(f) = (1, n)$. Donc $f|_F$ est non dégénérée, ce qui assure que $\text{sign}(f) = (1, \dim F - 1)$.

- 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 7 : ★★

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 $\text{diag} \left(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \dots, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, (-1)^{\frac{p-1}{2}} \right)$.
- d) En déduire que $|S| = q^{\frac{p-1}{2}} (q^{\frac{p-1}{2}} + (-1)^{\frac{p-1}{2}} q^{\frac{q-1}{2}})$.
- 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 7.

- 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 pour 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 un 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

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

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 $|T_1| = \left(q^{\frac{p-1}{2}} - 1\right) q^{\frac{p-3}{2}} = \left(q^{\frac{p-1}{2}} - 1\right) q^{\frac{p-1}{2}}$. 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 8 : ***

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 8.

- a) Il faut et il suffit que a, b, c ne soient pas tous de même signe.
- b) — On suppose f isotrope 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, vérifiant $ax^2 + by^2 = z^2$. 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 nécessairement $a' \geq 0$. 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 $aA'm^2 \equiv -B'[r]$. 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 9 : ***

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

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

et

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

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

- Montrer que $u(K) \geq s(K)$.
- Calculer $s(K)$ et $u(K)$ si K est algébriquement clos.
- Donner un exemple de corps K avec $s(K) = \infty$ et un exemple avec $u(K) = \infty$ et $s(K) < \infty$.
- Montrer que des corps isomorphes ont même niveau et même u -invariant. Les réciproques sont-elles vraies ?
- 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.
- 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

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

- Montrer que f_n admet un vecteur isotrope si et seulement si on a $s(K) \leq n - 1$.
- Supposons $n = 2^k$ avec $k \in \mathbb{N}$. Montrer que pour tout $x = (x_1, \dots, x_n) \in K^n$ non nul, il existe une matrice T_x de première ligne (x_1, \dots, x_n) vérifiant

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

- En déduire que l'ensemble des sommes non nulles de 2^k carrés d'éléments de K est un groupe multiplicatif.
- Montrer que le niveau d'un corps est soit infini, soit une puissance de 2.

Solution de l'exercice 9.

- Soit $n < s(K)$. Alors par définition la forme quadratique $x_1^2 + \dots + x_n^2 + x_{n+1}^2$ 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 immédiatement $s(K) \geq s(K(X))$. Supposons donc $s(K(X))$ fini, et notons s cet entier. Il existe des fractions rationnelles $R_1(X), \dots, R_s(X)$ telles que l'on ait $R_1(X)^2 + \dots + R_s(X)^2 = -1$.
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 $P_1(X)^2 + \dots + P_s(X)^2 = -Q(X)^2$ 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 $(p_1^{(\alpha)})^2 + \dots + (p_s^{(\alpha)})^2 = -1$. 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 $x_1, \dots, x_{n-1} \in K$ tels que $x_1^2 + \dots + x_{n-1}^2 + 1^2 = 0$. Réciproquement, si f_n a un vecteur isotrope (x_1, \dots, 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

$${}^t T_1 T_1 = T_1 {}^t T_1 = f_n(x_1, \dots, x_n) I_n, \quad {}^t T_2 T_2 = T_2 {}^t T_2 = f_n(x_{n+1}, \dots, x_{2n}) I_n.$$

On calcule ensuite

$$\begin{pmatrix} {}^t T_1 & {}^t A \\ {}^t T_2 & {}^t B \end{pmatrix} \begin{pmatrix} T_1 & T_2 \\ A & B \end{pmatrix} = \begin{pmatrix} {}^t T_1 T_1 + {}^t A A & {}^t T_1 T_2 + {}^t A B \\ {}^t T_2 T_1 + {}^t B A & {}^t T_2 T_2 + {}^t B B \end{pmatrix},$$

et

$$\begin{pmatrix} T_1 & T_2 \\ A & B \end{pmatrix} \begin{pmatrix} {}^t T_1 & {}^t A \\ {}^t T_2 & {}^t B \end{pmatrix} = \begin{pmatrix} T_1 {}^t T_1 + T_2 {}^t T_2 & T_1 {}^t A + T_2 {}^t B \\ A {}^t T_1 + B {}^t T_2 & A {}^t A + B {}^t B \end{pmatrix}.$$

Alors :

- i) si $f_n(x_1, \dots, x_n) \neq 0$, on prend $A = T_1^{-1} {}^t T_2 T_1$ et $B = -{}^t T_1$.
- ii) sinon, si $f_n(x_{n+1}, \dots, x_{2n}) \neq 0$, on prend $A = -{}^t T_2$ et $B = T_2^{-1} {}^t T_1 T_2$.
- iii) enfin, si $f_n(x_1, \dots, x_n) = f_n(x_{n+1}, \dots, x_{2n}) = 0$, 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 $T_x T_y$ 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, \dots, x_{2n}) . On a donc $f_n(x_1, \dots, x_n) = -f_n(x_{n+1}, \dots, x_{2n}) \neq 0$. Mais alors $f_n(x_1, \dots, x_n) f_n(x_{n+1}, \dots, x_{2n})^{-1} = -1$ 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 $K = \mathbb{R}(X_1, \dots, X_{n-1})[X_n]/(\sum X_i^2 + 1)$ (voir par exemple le théorème 2.8 du chapitre 11 de Lam, *Algebraic theory of quadratic forms*).