Formes quadratiques

Dans tout ce qui suit, les corps considérés seront toujours de caractéristique différente de 2.

Exercice 1. Les formes quadratiques $q(x,y) = x^2 + y^2$ et $q'(x,y) = x^2 + 2y^2$ sont-elles isométriques sur $\mathbf{Q}$? Sur $\mathbf{R}$? Sur $\mathbf{C}$?

Exercice 2.

1. Déterminer le rang, le noyau, la signature et une base d'orthogonalisation de la forme quadratique $(x,y,z) \mapsto xy + yz$ définie sur $\mathbf{R}^3$.
2. Déterminer la signature de la forme $(x_1,\dots,x_n) \mapsto \sum_{\substack{1\leq i,j\leq n \\ i\neq j}} x_i x_j$ définie sur $\mathbf{R}^n$.

Exercice 3. (Théorie de Witt)
Soit k un corps. On appelle *espace quadratique* la donnée d'un k-espace vectoriel de dimension finie V et d'une forme quadratique q sur V. Un tel espace est dit *isotrope* s'il admet un vecteur non nul isotrope pour q et *totalement isotrope* si tous les vecteurs sont isotropes pour q.

1. Montrer qu'un sous-espace $\mathrm{U} \subset \mathrm{V}$ d'un espace quadratique non dégénéré vérifie l'égalité $\dim \mathrm{U} + \dim \mathrm{U}^\perp = \dim \mathrm{V}$ et qu'il est lui-même non dégénéré si et seulement si $\mathrm{V} = \mathrm{U} \oplus \mathrm{U}^\perp$.
2. On appelle *plan hyperbolique* tout espace quadratique isométrique au plan quadratique $(k^2, (x,y) \mapsto x^2 - y^2)$. Montrer que l'espace quadratique $(k^2, (x,y) \mapsto xy)$, tout plan quadratique non dégénéré et de discriminant -1 ainsi que tout plan quadratique non dégénéré et isotrope sont des plans hyperboliques.
3. On appelle *espace hyperbolique* tout espace quadratique isomorphe à la somme directe d'un certain nombre de plans hyperboliques (c'est-à-dire tout espace quadratique isomorphe à $(k^{2n}, (x_1,y_1,\dots,x_n,y_n) \mapsto x_1y_1 + \cdots + x_ny_n)$. Montrer le *théorème de gonflement de Witt* : tout sous-espace totalement isotrope $\mathrm{U} \subset \mathrm{V}$ d'un espace quadratique non dégénéré (V, q) est contenu dans un sous-espace hyperbolique $\mathrm{H} \subset \mathrm{V}$ de dimension $2 \dim \mathrm{U}$.
4. On dit qu'un espace quadratique (V, q) *représente* $\lambda \in k^\times$ s'il existe $x \in \mathrm{V}$ tel que $q(x) = \lambda$. Montrer qu'une forme isotrope représente tous les éléments de $k^\times$ (on dit qu'elle est *universelle*).
5. Si $\lambda \in k$, on note $\langle\lambda\rangle$ la droite quadratique $(k, x \mapsto \lambda x^2)$. Montrer qu'une forme quadratique non dégénérée (V, q) représente λ si et seulement si la somme directe $\mathrm{V} \oplus \langle -\lambda \rangle$ est isotrope.
6. Démontrer le *théorème de décomposition de Witt* : tout espace quadratique (V, q) est isomorphe à la somme directe $(\mathrm{V}_{\mathrm{ti}}, q_{\mathrm{ti}}) \oplus (\mathrm{V}_{\mathrm{hyp}}, q_{\mathrm{hyp}}) \oplus (\mathrm{V}_{\mathrm{an}}, q_{\mathrm{an}})$, où les espaces quadratiques intervenant dans la somme sont totalement isotrope, hyperbolique et anisotrope, respectivement.
7. Soit (V, q) un espace quadratique et b la forme bilinéaire associée. Pour tout vecteur non isotrope $y \in \mathrm{V}$, on définit l'endomorphisme $\tau_y : \mathrm{V} \to \mathrm{V}$ par la formule

$$\tau_y(x) = x - \frac{2b(x,y)}{q(y)} y.$$

Montrer que τ_y est un élément du groupe orthogonal de (V, q) fixant $\mathrm{Vect}(y)^\perp$ et calculer son déterminant.

8. Soit (V, q) un espace quadratique et x, y deux vecteurs tels que $q(x) = q(y) \neq 0$. Montrer qu'il existe $\tau \in \mathrm{O}(\mathrm{V}, q)$ tel que $\tau(x) = y$.
9. Démontrer le *théorème de simplification de Witt* : si (V, q), (V_1, q_1) et (V_2, q_2) sont des espaces quadratiques tels que $(\mathrm{V}, q) \oplus (\mathrm{V}_1, q_1)$ et $(\mathrm{V}, q) \oplus (\mathrm{V}_2, q_2)$ soient isométriques, alors (V_1, q_1) et (V_2, q_2) sont isométriques.
10. En déduire que dans la décomposition de Witt, les trois facteurs sont bien définis, à isométrie près.

Exercice 4. (Formes quadratiques sur un corps fini)
Soit q la puissance d'un nombre premier impair et $\alpha \in \mathbf{F}_q^\times$ qui ne soit pas un carré.

1. Montrer que quels que soient a et b dans $\mathbf{F}_q^\times$, l'équation $ax^2 + by^2 = 1$ possède des solutions dans $\mathbf{F}_q$.
2. Montrer que toute forme quadratique régulière sur un $\mathbf{F}_q$-espace vectoriel de dimension 2 est isométrique à une forme quadratique de matrice I_2 ou $\mathrm{diag}(1, \alpha)$.
3. Montrer qu'en général, toute forme quadratique régulière sur un $\mathbf{F}_q$-espace vectoriel est isométrique à une forme quadratique de matrice $\mathrm{diag}(1, \ldots, 1, 1)$ ou $\mathrm{diag}(1, \ldots, 1, \alpha)$. En déduire qu'il y a deux classes d'équivalence de formes quadratiques non dégénérées sur un $\mathbf{F}_q$-espace vectoriel de dimension > 0.

Exercice 5. (Nombres premiers de la forme $x^2 + ny^2$)
Soit $a, b, c \in \mathbf{Z}$ avec $\mathrm{pgcd}(a, b, c) = 1$. L'application $\mathrm{Q}(x, y) = ax^2 + bxy + cy^2$ est une forme quadratique $\mathrm{Q} = \mathrm{Q}_{a,b,c} : \mathbf{Z}^2 \to \mathbf{Z}$ et on pose $\mathrm{D}(\mathrm{Q}) = b^2 - 4ac$. Dans la suite, on dit qu'un entier $m \in \mathbf{Z}$ est *representé* par Q s'il existe $x, y \in \mathbf{Z}$ tels que $m = \mathrm{Q}(x, y)$ et on dit que cette représentation est *propre* si l'on peut choisir x et y premiers entre eux.
On dit que deux formes quadratiques Q et $\mathrm{Q}' : \mathbf{Z}^2 \to \mathbf{Z}$ sont *équivalentes* (resp. *proprement équivalentes*) s'il existe $u \in \mathrm{GL}_2(\mathbf{Z})$ (resp. $u \in \mathrm{SL}_2(\mathbf{Z})$) tel que $\mathrm{Q}' = \mathrm{Q} \circ u$. On note ces relations d'équivalence $\sim$ et $\overset{+}{\sim}$.

1. Soit $m \in \mathbf{Z}$. Montrer que si $\mathrm{Q} \sim \mathrm{Q}'$, alors m est representé (resp. proprement representé) par Q si et seulement s'il l'est par Q'. Montrer que si $\mathrm{Q} \sim \mathrm{Q}'$, alors $\mathrm{D}(\mathrm{Q}) = \mathrm{D}(\mathrm{Q}')$.
2. Montrer que si $\mathrm{D}(\mathrm{Q}) < 0$, alors Q est définie positive ou définie négative.
3. Soit $m \in \mathbf{Z}$. Montrer que m est proprement representé par Q si et seulement s'il existe $b', c' \in \mathbf{Z}$ tels que $\mathrm{Q} \overset{+}{\sim} \mathrm{Q}_{m,b',c'}$.
4. Si $\mathrm{Q}_{a,b,c}$ est définie positive, on dit qu'elle est *réduite* si $|b| \leq a \leq c$ et qu'en outre, quand l'une de ces inégalités est une égalité, on a $b \geq 0$. On admet le fait suivant, dû à Legendre : si Q est une forme définie positive, il existe une unique forme réduite Q' telle que $\mathrm{Q} \overset{+}{\sim} \mathrm{Q}'$.
   Soit $n \in \{2, 3\}$. Montrer que $\mathrm{Q}_{1,0,n}$ est l'unique forme réduite définie positive telle que $\mathrm{D}(\mathrm{Q}) = -4n$.
5. Soit $\mathrm{D} \in \mathbf{Z}$ un entier tel que $\mathrm{D} \equiv 0, 1 \pmod 4$ et $m \in \mathbf{Z}$ impair. Montrer que m est proprement representé par Q si et seulement si $\mathrm{D} = \mathrm{D}(\mathrm{Q})$ est un carré modulo m.
6. Soit $p > 0$ un nombre premier. En déduire que :
   - $p = x^2 + 2y^2$ avec $x, y \in \mathbf{Z}$ si et seulement si $p = 2$ ou $p \equiv 1, 3 \pmod 8$. (*Indication :* il suffit de montrer que -2 est un carré modulo p si et seulement si $8 | p^2 - 1$).
   - $p = x^2 + 3y^2$ avec $x, y \in \mathbf{Z}$ si et seulement si $p = 3$ ou $p \equiv 1 \pmod 3$ (*Indication :* il suffit de montrer que -3 est un carré modulo p si et seulement si p est un carré modulo 3).