ÉNS de Lyon
M2 FEADéP

Cours d'algèbre
2019–2020

Feuille d'exercices n°19 : Classification des formes quadratiques

Dans toute cette feuille K est un corps de caractéristique $\mathrm{car}(K) \neq 2$. On désignera par V un K-espace vectoriel de dimension finie $n \in \mathbb{N}^*$ et par q une forme quadratique sur V.

À faire

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

Exercice 2. ***(Calcul explicite)***
Donner les signatures et rangs des formes quadratiques suivantes sur un $\mathbb{R}$-espace vectoriel :

$$M \mapsto \mathrm{Tr}(M^2) \text{ sur } \mathcal{M}_n(\mathbb{R}) \qquad \text{et} \qquad (x_1, \dots, x_n) \mapsto \sum_{1 \leq i < j \leq n} x_i x_j \text{ sur } \mathbb{R}^n.$$

Exercice 3. ***(Classification des formes quadratiques sur un corps algébriquement clos)***
On suppose que K est algébriquement clos.

1. Montrer que deux formes quadratiques sont équivalentes si, et seulement si, elles ont même rang.
2. Montrer que l'indice (voir Exercice 8) d'une forme quadratique non dégénérée est $\nu(q) = \lfloor \frac{n}{2} \rfloor$.

Exercice 4. ***(Classification des formes quadratiques réelles)***
Soit q une forme quadratique réelle de rang r et s la dimension maximale d'un sous-espace sur lequel q est définie positive. Montrer que q est équivalente à $(x_1, \dots, x_n) \mapsto x_1^2 + \cdots + x_s^2 - x_{s+1}^2 - \cdots - x_r^2$ et que $\nu(q) \geq \min(s, r - s)$ (voir Exercice 8).

Exercice 5. ***(Signature et mineurs principaux)***
Soit V un $\mathbb{R}$-espace vectoriel de dimension n et $\mathbf{e} = (e_1, \dots, e_n)$ une base de $\mathbb{R}^n$. Soit q une forme quadratique sur V, de matrice M dans la base $\mathbf{e}$. On note $\Delta_k := \det((m_{i,j})_{i,j \leq k})$ les mineurs principaux de M.

1. On suppose que $\Delta_{n-1} \neq 0$. Montrer qu'il existe $\alpha_1, \dots, \alpha_{n-1}$ dans $\mathbb{R}$ tels que $u_n = e_n - \sum_{i<n} \alpha_i e_i$ est q-orthogonal à $e_1, \dots, e_{n-1}$.
2. On suppose que $\Delta_{n-1} \neq 0$ et on note (r, s) la signature de la restriction de q à $\mathrm{Vect}(e_1, \dots, e_{n-1})$. Montrer que :
   (a) si $\Delta_n = 0$, alors q est de signature (r, s) ;
   (b) si Δ_n est de même signe que Δ_{n-1}, alors q est de signature $(r + 1, s)$;
   (c) si Δ_n est de signe opposé à Δ_{n-1}, alors q est de signature $(r, s + 1)$.
3. On suppose que $\Delta_i \neq 0$ pour tout $1 \leqslant i \leqslant n$. Montrer que q est de signature $(n - s, s)$ où s est le nombre de changements de signe dans la suite $(1, \Delta_1, \Delta_2, \dots, \Delta_n)$.

Exercice 6. ***(Classification des formes quadratiques sur un corps fini)***
On suppose que $K = \mathbb{F}_\ell$ est un corps fini de caractéristique différente de 2.

1. Montrer que $K^{\times 2}$ est un sous-groupe d'indice 2 de $K^\times$.
2. Montrer que pour $a, b \in \mathbb{F}_\ell^\times$, l'équation $ax^2 = 1 - by^2$ admet des solutions dans $\mathbb{F}_\ell$.
   Indication : on pourra estimer le cardinal de l'intersection des images de deux applications $\mathbb{F}_\ell \to \mathbb{F}_\ell$.
3. On suppose que q est non dégénérée sur K.
   (a) Si $n = 2$, montrer que q est équivalente à $(x, y) \mapsto x^2 + \alpha y^2$ avec $\alpha \in \mathrm{disc}(q)$.
   (b) En déduire, en général, que q est équivalente à $x_1^2 + \cdots + x_{n-1}^2 + \alpha x_n^2$ avec $\alpha \in \mathrm{disc}(q)$.
4. Montrer que les formes quadratiques sur un corps fini sont classifiées par le rang et le discriminant et qu'il y a exactement $2n + 1$ classes d'équivalence sur $V = \mathbb{F}_\ell^n$.

Exercice 7. Montrer qu'il y a une infinité de classes d'équivalences sur $V = \mathbb{Q}^n$.

Problèmes

Exercice 8. ***(Indice d'une forme quadratique)***
Un sous-espace vectoriel W de V est dit *totalement isotrope* (ou SETI) si chacun de ses vecteurs est isotrope. On appelle *SETIM* un tel espace maximal pour l'inclusion. On note $\nu(q)$ la dimension maximale d'un SETI, on l'appelle *indice* de q.

1. Montrer que W est un SETI si, et seulement si, $W \subset W^\perp$.
2. Montrer que si W est un SETI, alors
$$\dim W + \dim W^\perp = \dim V + \dim(W \cap \ker q).$$
3. En déduire que $\nu(q) \leq \dim V - \frac{\operatorname{rg} q}{2}$.
4. Soient W_1 et W_2 deux SETIM et $W = W_1 \cap W_2$. Soient des espaces vectoriels S_1 et S_2 tels que $W \oplus S_1 = W_1$ et $W \oplus S_2 = W_2$. Montrer que $S_1 \cap S_2^\perp = S_2 \cap S_1^\perp = 0$.
5. En déduire que les SETIM ont tous même dimension $\nu(q)$.
6. Donner cette dimension $\nu(q)$ dans le cas $K = \mathbb{R}$ et q de signature (r, s).

Exercice 9. ***(Formes de Hankel)***
Le but de cet exercice est de construire, pour $P \in \mathbb{R}[X]$ non nul, une forme quadratique réelle q_P dont la signature donne le nombres de racines réelles distinctes de P.

Supposons que P est de degré $n \geq 1$ de racines (complexes, pouvant être égales) $\alpha_1, \ldots, \alpha_n$, et posons pour tout $k \in [\![0, n]\!]$, la k-ième somme de Newton $s_k = \displaystyle\sum_{i=1}^{n} \alpha_i^k$.

1. Rappeler comment exprimer s_k en fonction des coefficients de P et justifier que c'est bien un nombre réel.

On définit alors la forme quadratique réelle $q_P(x) = \displaystyle\sum_{1 \leq k,l \leq n} s_{k+l} x_k x_l$ sur $\mathbb{R}^n$ et on note (r, s) sa signature. Pour tout $i \in [\![1, n]\!]$, on définit la forme linéaire $\varphi_i(x) = \displaystyle\sum_{k=1}^{n} \alpha_i^k x_k$ sur $\mathbb{C}^n$.

2. Soit $J \subset [\![1, n]\!]$ tel que $\{\alpha_j,\ j \in J\}$ est l'ensemble des racines de P et les α_j sont deux à deux distincts. Montrer que les φ_j sont linéairement indépendantes.
3. En déduire une décomposition de Gauss de q_P en tant que forme quadratique sur $\mathbb{C}$.
4. Montrer que le nombre de racines complexes distinctes $\operatorname{Card} J$ de P est exactement $r + s$.
5. Pour tout $i \in [\![1, n]\!]$, montrer que la forme quadratique $\varphi_i^2 + \overline{\varphi_i}^2$ est réelle, et que sa signature est $(1, 0)$ si α_i est réelle et $(1, 1)$ sinon.
6. En déduire que le nombre de racines réelles distinctes de P est $r - s$.
7. Que peut-on en dire sur la continuité du nombre de racines réelles en fonction des coefficients ?

Exercice 10. Le but de cet exercice [*] est de montrer que pour p premier, on a :

— $\exists x, y \in \mathbb{Z},\ p = x^2 + y^2 \iff p = 2$ ou $p \equiv 1 \mod 4$;
— $\exists x, y \in \mathbb{Z},\ p = x^2 + 2y^2 \iff p = 2$ ou $p \equiv 1 \mod 8$ ou $p \equiv 3 \mod 8$;
— $\exists x, y \in \mathbb{Z},\ p = x^2 + 3y^2 \iff p = 3$ ou $p \equiv 1 \mod 3$.

Une forme quadratique q sur $\mathbb{Q}^2$ est dite *primitive* s'il existe un polynôme homogène de degré 2 primitif $Q \in \mathbb{Z}[X, Y]$ tel que $q(x, y) = Q(x, y)$. On dit que q *représente proprement* un entier $m \in \mathbb{Z}$ si m est dans l'image de la fonction polynomiale $f_Q : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ associée à Q.

1. Pour $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, on considère le morphisme $\varphi_g : \mathbb{Z}[X, Y] \to \mathbb{Z}[X, Y]$ vérifiant $\varphi_g(X) = aX + bY$ et $\varphi_g(Y) = cX + dY$. Montrer que ceci définit une action de $\mathrm{SL}_2(\mathbb{Z})$ sur $\mathbb{Z}[X, Y]$ et que l'ensemble des polynômes homogènes de degré 2 primitifs est stable sous l'action de $\mathrm{SL}_2(\mathbb{Z})$.

[*]. La méthode proposée est due à Lagrange, raffinée par Gauss, appliquée aux formes quadratiques définies positives de la forme $q_n(x, y) = x^2 + ny^2$.

Deux formes quadratiques primitives sur $\mathbb{Q}^2$ sont dites *proprement équivalentes* si elles proviennent de deux polynômes homogènes de degré 2 primitifs dans une même orbite de l'action de $\mathrm{SL}_2(\mathbb{Z})$.

2. Montrer que q primitive représente proprement m si, et seulement si, q est proprement équivalente à $q' : (x, y) \mapsto mx^2 + bxy + cy^2$ primitive avec $b, c \in \mathbb{Z}$.
3. Montrer que deux formes quadratiques primitives qui sont proprement équivalentes ont le même discriminant.
4. Soit $\delta \in \mathbb{Z}$ tel que $\delta \equiv 0 \mod 4$ ou $\delta \equiv 1 \mod 4$. Soit $m \in \mathbb{Z}$ impair tel que $\mathrm{pgcd}(m, \delta) = 1$. Montrer que m est représenté par une forme quadratique primitive de discriminant δ si, et seulement si, δ est un carré de $\mathbb{Z}/m\mathbb{Z}$.

Une forme quadratique primitive est dite *réduite* si elle provient d'un polynôme $P = aX^2 + bXY + cY^2 \in \mathbb{Z}[X, Y]$ tel que $\mathrm{pgcd}(a, b, c) = 1$ et $|b| \leq a \leq c$.

5. Montrer que toute forme quadratique primitive sur $\mathbb{Q}^2$ est proprement équivalente à une forme quadratique primitive réduite.

Pour $n \in \mathbb{N}^*$, on pose $Q_n = X^2 + nY^2 \in \mathbb{Z}[X, Y]$ et q_n la forme quadratique associée dans $\mathbb{Q}^2$.

6. Vérifier que q_n est primitive et définie positive et déterminer son discriminant δ_n.
7. Montrer pour $n \in \{1, 2, 3\}$ que q_n est l'unique forme quadratique primitive de $\mathbb{Q}^2$ réduite de discriminant δ_n.
8. Soit $p > 3$ un nombre premier et $n \in \{1, 2, 3\}$.
   (a) Montrer que p est proprement représenté par q_n si, et seulement si, δ_n est un carré modulo p.
   (b) Montrer que x est un carré de $\mathbb{F}_p$ si, et seulement si, $x^{\frac{p-1}{2}} = 1$.
   (c) En déduire que :
   - $-4 \in \mathbb{F}_p^{\times 2} \iff p \equiv 1 \mod 4$;
   - $-8 \in \mathbb{F}_p^{\times 2} \iff p \equiv 1 \mod 8$ ou $p \equiv 3 \mod 8$;
   - $-12 \in \mathbb{F}_p^{\times 2} \iff p \equiv 1 \mod 3$.
9. Conclure †.

Pour aller plus loin

Exercice 11. Soit V un K-espace vectoriel de dimension 3 et q une forme quadratique non-dégénérée d'indice 1 sur V. Montrer que q est équivalente à $x^2 + y^2 - z^2$.

Exercice 12. On suppose que q est non-dégénérée sur V. Soient W, W' deux sous-espaces de V et $\sigma : W \to W'$ une isométrie. Soit $K = \ker q|_W$.

1. Montrer que $\dim K + \dim(W) \leqslant \dim(V)$ et qu'il y a égalité si, et seulement si, $W^\perp$ est totalement isotrope.
2. On suppose que $W^\perp$ n'est pas totalement isotrope. Montrer qu'il existe $u \in \mathcal{SO}(q)$ et $v \in \mathcal{O}(q) \setminus \mathcal{SO}(q)$ tels que $u|_W = v|_W = \sigma$.
3. On suppose que V est hyperbolique et que W est un SETIM de V. Soit $u \in \mathcal{O}(q)$ tel que $u(W) = W$. Montrer que $u \in \mathcal{SO}(q)$.
4. On suppose que $\dim K + \dim W = \dim(V)$. Soit $u \in \mathcal{O}(q)$ tel que $u|_W = \mathrm{id}_W$. Montrer que $u \in \mathcal{SO}(q)$. Que remarque-t-on ?
5. Soit $u \in \mathcal{O}(q)$ tel que $u(W) = W'$. Montrer qu'il existe $v \in \mathcal{SO}(q)$ tel que $v(W) = W'$ sauf si V est hyperbolique et W en est un SETIM.
6. On suppose que V est hyperbolique. Soit $\mathcal{L}$ l'ensemble des SETIM de V. Montrer que $\mathcal{L}$ est une orbite sous $\mathcal{O}(q)$ et que $\mathcal{L}$ se décompose en deux orbites sous $\mathcal{SO}(q)$.

†. Laudau a montré en 1903 que cette stratégie ne s'applique qu'aux cas où $n \in \{1, 2, 3, 4, 7\}$. En effet, ce sont les seuls entiers pour lesquels il existe une unique forme réduite de discriminant $-4n$.

Exercice 13. On suppose que $\dim(V) = 4$ et que q est une forme quadratique non-dégénérée sur V d'indice $\nu(q) \neq 0$.

1. Montrer que s'équivalent :
   (i) (V, q) est hyperbolique ;
   (ii) $\nu(q) = 2$;
   (iii) $\mathrm{disc}(q) \equiv 1 \mod K^{\times 2}$.
2. Montrer que $\nu(q) = 1$ si, et seulement si, $\mathrm{disc}(q) \notin K^{\times 2}$.
3. Soit q' une autre forme quadratique non-dégénérée sur V. Montrer que q et q' ont même discriminant (modulo $K^{\times 2}$) si, et seulement si, il existe $\lambda \in K^{\times}$ tel que q' est équivalent à λq.