ÉNS de Lyon — Cours d'algèbre
M2 FEADEP — 2018-2019

Feuille d'exercices n°12 : 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 d'une forme quadratique non dégénérée est $\nu(q) = \left\lfloor \frac{n}{2} \right\rfloor$.

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.

1. Montrer que q est équivalente à $(x_1, \dots, x_n) \mapsto x_1^2 + \cdots + x_s^2 - x_{s+1}^2 - \cdots - x_r^2$.
2. Montrer que $\nu(q) \geq \min(s, r - s)$ *.

Exercice 5. ***(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 6. Montrer qu'il y a une infinité de classes d'équivalences sur $V = \mathbb{Q}^n$.

Problèmes

Exercice 7. ***(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) $\alpha_1, \dots, \alpha_n$, 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.

*. En fait, on pourrait montrer l'égalité en utilisant le théorème de Witt. Voir par exemple le *Cours d'algèbre* de D. Perrin, chap. VIII.4.

On définit alors la forme quadratique réelle $q_P(x) = \sum_{1\leq k,l\leq n} s_{k+l}x_kx_l$ sur $\mathbb{R}^n$ et on note (r,s) sa signature. Pour tout $i \in [\![1,n]\!]$, on définit la forme linéaire $\varphi_i(x) = \sum_{k=1}^{n} \alpha_i^k x_k$ 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 8. 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 $\mathrm{SL}_2(\mathbb{Z})$.

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 $\operatorname{pgcd}(m,\delta) = 1$. 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 $\operatorname{pgcd}(a,b,c) = 1$ 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 [‡].

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

‡. 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 $-4n$.