Université de Rennes 1
Préparation à l'agrégation
de mathématiques
Auteur du document :

M. Coste

Formes quadratiques, groupe orthogonal

Michel Coste

Mars 2003

Introduction

Dans la première section on passe en revue les résultats sur les formes quadratiques, notamment ceux utiles pour l'étude des quadriques projectives et affines. On parle de la classification des formes quadratiques sur $\mathbb{C}$, sur $\mathbb{R}$, sur un corps fini (de caractéristique $\neq 2$). On donne le résultat d'engendrement du groupe orthogonal par les réflexions. On pousse ensuite jusqu'au théorème de Witt, qui est sans doute le premier résultat consistant de la théorie algébrique des formes quadratiques. Il ne figure pas dans le programme de l'agrégation, mais il est traité dans bon nombre d'ouvrages classiques de la préparation à l'agrégation : [Per], [Tau], [Ber]. Dans tout ce texte, on se contente de donner les idées des démonstrations. Les détails peuvent se trouver dans l'un des ouvrages cités précédemment.

1 Notations et définitions pour les formes bilinéaires symétriques

Soit E un espace vectoriel de dimension finie sur un corps K. Une forme bilinéaire symétrique $b : E \times E \to K$ induit une application linéaire que l'on notera $\varphi_b : E \to E^*$ de E dans son dual. L'application φ_b est définie par $\varphi_b(x)(y) = b(x, y)$.

Si on a choisi une base $(e_1, \ldots, e_n)$ de E, on associe à b la matrice symétrique $B = (b(e_i, e_j))_{i,j=1,\ldots,n}$. Noter que B est la matrice de φ_b dans les bases (e_i) au départ et (e_i^*) à l'arrivée. Si on effectue un changement de base de matrice P, la matrice de b dns la nouvelle base est ${}^tPBP$.

Une *isométrie* $\sigma : (E, b) \to (E', b')$ est un isomorphisme linéaire tel que $b'(\sigma(x), \sigma(y)) = b(x, y)$.

On dit que b est *non dégénérée* si et seulement si φ_b est un isomorphisme (si et seulement si B est inversible). Le *rang* de b est le rang de φ_b (de B). Le *noyau* (ou *radical*) de (E, b) est

$$\ker \varphi_b = \{x \in E \; ; \; \forall y \in E \; b(x, y) = 0\} \; .$$

Exercice 1 *Soit E_0 est le noyau de (E, b). Vérifier que b induit sur E/E_0 une forme bilinéaire non dégénérée $\overline{b}$ par $\overline{b}(\overline{x}, \overline{y}) = b(x, y)$. Soit U est un supplémentaire quelconque de E_0. Montrer que U muni de la restriction de b est isométrique à $(E/E_0, \overline{b})$; on en déduit que deux supplémentaires quelconques du noyau sont isométriques.*

Deux vecteurs x et y de E sont dits *orthogonaux* (pour b) si et seulement si $b(x, y) = 0$. Si F est un sous-espace vectoriel de E, son *orthogonal* est

$$F^\perp = \{x \in E \; ; \; \forall y \in F \; b(x, y) = 0\}$$

(en particulier $E^\perp$ est le noyau de (E, b)). Si b est non dégénérée, $\varphi_b(F^\perp) \subset E^*$ est l'orthogonal de F pour la dualité et donc $\dim F + \dim F^\perp = \dim E$. Deux sous-espaces F et G sont dits *en somme directe orthogonale* si et seulement si $F \cap G = \{0\}$ et $\forall x \in F \; \forall y \in G \; b(x, y) = 0$. On note alors $F \perp G$ leur somme (munie de la forme bilinéaire restreinte). De manière générale, si on a (E_1, b_1) et (E_2, b_2), leur *somme orthogonale* est $E_1 \oplus E_2$ avec la forme bilinéaire symétrique $b((x_1, x_2), (y_1, y_2)) = b_1(x_1, y_1) + b_2(x_2, y_2)$; on la note $E_1 \perp E_2$. Remarquer que b est non dégénérée si et seulement si b_1 et b_2 le sont.

Tout (E, b) se décompose comme $E = E_0 \perp E_{\mathrm{nd}}$, où E_0 est le noyau et la restriction de b à E_{nd} est non dégénérée. Cette décomposition est unique à isométrie près (voir l'exercice 1). On peut donc appeler E_{nd} la partie non dégénérée de (E, b)

2 Formes quadratiques. Isotropie

A partir de maintenant, on suppose que la caractéristique de K est différente de 2.

La forme quadratique $q : E \to K$ associée à b est définie par $q(x) = b(x, x)$. On a

$$b(x, y) = \frac{1}{2}(q(x + y) - q(x) - q(y)) ,$$

donc la donnée de b équivaut à celle de q (b est la *forme polaire* de q). On dit que q est non dégénérée si et seulement si b l'est. Un *vecteur isotrope* pour b (ou pour q) est un $x \neq 0$ tel que $q(x) = 0$.

Soit $F \subset E$ un sous-espace vectoriel.

- Si $q|_F$ est non dégénérée, on dit que F est *régulier* (ou non singulier, ou non dégénéré). Ceci veut dire que $F \cap F^\perp = \{0\}$, et alors $E = F \perp F^\perp$.
- Si $q|_F$ est dégénéré, c.-à-d. si $F \cap F^\perp \neq \{0\}$, on dit que F est *isotrope* (ou singulier). Le sous-espace $F \cap F^\perp$ est le noyau de F (de $(F, q|_F)$).
- Si $q|_F$ est nulle, c.-à-d. si $F \subset F^\perp$, on dit que F est *totalement isotrope* (ou totalement singulier).

3 Décomposition en carrés. Classification sur certains corps

Theorème 1 (Décomposition en carrés) *Soit q une forme quadratique sur E. Alors E admet une base orthogonale pour q, c'est-à-dire une base formée de vecteurs deux à deux orthogonaux.*

Du point de vue matriciel, ceci veut dire qu'il existe une base de E dans laquelle la matrice de q est diagonale. La forme q est donc isométrique à une forme du genre $(x_1, \ldots, x_n) \mapsto a_1x_1^2 + \cdots + a_nx_n^2$ sur K^n. On note $\langle a_1, \ldots, a_n\rangle$ cette forme.

Il faut absolument connaître l'algorithme de Gauss pour la décomposition en carrés.

Exercice 2 *Trouver une base de $\mathbb{R}^3$ orthogonale pour la forme $x_1x_2 + x_2x_3 + x_3x_1$.*

On s'intéresse au problème de la classification (à isométrie près) des formes quadratiques. Si deux formes quadratiques (qu'on suppose bien sûr de même dimension n) sont isométriques, elle ont même rang : le rang est un invariant d'isométrie. On peut exhiber un autre invariant d'isométrie pour des formes non dégénérées. Si deux matrices inversibles B et B' représentent des formes quadratiques isométriques, il existe une matrice inversible P telle que $B' = {}^tPBP$. Soit $K^\times$ le groupe multiplicatif des éléments non nuls du corps K, $K^{\times 2}$ le sous-groupe formé des carrés non nuls. Les images de $\det(B)$ et $\det(B')$ dans le quotient $K^\times/K^{\times 2}$ sont donc égales. Le *discriminant* d'une forme quadratique non dégénérée q est l'image dans $K^\times/K^{\times 2}$ du déterminant de la matrice de q dans une base quelconque. C'est un invariant d'isométrie.

La décomposition en carrés est la clé de la classification sur certains corps, avec la remarque que $\langle a_1, \ldots, a_n\rangle$ est isométrique à $\langle \lambda_1^2 a_1, \ldots, \lambda_n^2 a_n\rangle$, quelque soient les éléments $\lambda_1, \ldots, \lambda_n$ de $K^\times$. La connaissance de $K^\times/K^{\times 2}$ est importante pour la classification.

Cas $K = \mathbb{C}$ (ou plus généralement K algébriquement clos). Toute forme de rang r est isométrique à $\langle \underbrace{1, \ldots, 1}_{r}, 0, \ldots, 0\rangle$. Le rang suffit à classifier les formes quadratiques sur $\mathbb{C}$.

Cas $K = \mathbb{R}$ Toute forme q est isométrique à une forme du genre

$$\langle \underbrace{1, \ldots, 1}_{s}, \underbrace{-1, \ldots, -1}_{t}, 0, \ldots, 0\rangle .$$

Le couple (s, t) ne dépend que de la forme q, et c'est un invariant d'isométrie sur $\mathbb{R}$ (théorème d'inertie de Sylvester) ; ce théorème se montre en vérifiant que s (resp. t) est le maximum des dimensions de sous-espaces sur lesquels q est *définie positive* (resp. définie négative). Le couple (s, t) est la *signature* de q. La signature suffit à classifier les formes quadratiques sur $\mathbb{R}$.

Exercice 3 *Soit q une forme quadratique non dégénérée de signature (s,t) sur un espace vectoriel réel E. Soit H un hyperplan vectoriel de E. Quelle peut être la signature de la forme $q|_H$ restriction de q à H ? (Indication : $(s-1,t)$, $(s,t-1)$ ou $(s-1,t-1)$)*

Cas $K = \mathbb{F}_\ell$ (un corps fini de caractéristique $\neq 2$). C'est un cas plus exotique, mais où la classification est aussi très simple (voir [Per]). On sait que $\mathbb{F}_\ell^{\times 2}$ est un sous-groupe d'indice 2 de $\mathbb{F}_\ell^\times$. Soit $\alpha \in \mathbb{F}_\ell^\times$ qui n'est pas un carré. Toute forme quadratique non dégénérée sur $\mathbb{F}_\ell$ est isométrique à une forme donnée par une matrice diagonale avec uniquement des 1 et des α sur la diagonale. La remarque clé qui vient maintenant est l'objet de l'exercice suivant :

Exercice 4 *Montrer que l'équation $\alpha x^2 + \alpha y^2 = 1$ a une solution (x,y) dans $\mathbb{F}_\ell \times \mathbb{F}_\ell$. En déduire que $\langle \alpha, \alpha \rangle$ est isométrique à $\langle 1, 1 \rangle$ sur $\mathbb{F}_\ell$*

On peut donc remplacer deux par deux dans la diagonale les α par des 1. Ainsi, toute forme quadratique non dégénée sur $\mathbb{F}_\ell$ est isométrique à l'une des deux formes $\langle 1, \dots, 1 \rangle$ ou $\langle 1, \dots, 1, \alpha \rangle$. Dans le premier cas le discriminant est la classe de 1 (la classe des carrés), dans le deuxième cas celle de α (la classe des non carrés). A dimension fixée, le discriminant suffit pour classifier les formes non dégénérées. Les formes quadratiques dégénérées ou non sont classifiées par le rang et le discriminant de la partie non dégénérée.

4 Groupe orthogonal, réflexions

Dans toute cette section, (E,q) est non dégénéré.

Le sous-groupe de $\mathrm{GL}(E)$ formé des isométries de q s'appelle le *groupe orthogonal de q* et est noté $\mathrm{O}(q)$. Si B est la matrice de q dans une base de E, le groupe ortogonal de q s'dentifie au groupe des matrices inversibles P vérifiant ${}^tPBP = B$. Le déterminant d'un élément de $\mathrm{O}(q)$ est ± 1. Les isométries de q de déterminant 1 forment le sous groupe $\mathrm{O}_+(q)$ (noté aussi $\mathrm{SO}(q)$) qui est distingué d'indice 2 dans $\mathrm{O}(q)$.

Exercice 5 *Soit q la forme quadratique de matrice $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Déterminer $\mathrm{O}(q)$, $\mathrm{O}_+(q)$.*

Parmi les isométries de q il y a celles dont le sous-espace des points fixes est un hyperplan : les *symétries hyperplanes* ou *réflexions*. Elles s'obtiennent ainsi : si y est un vecteur de E tell que $q(y) \neq 0$, alors $\tau_y : E \to E$ défini par

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

est une isométrie qui est l'identité sur $y^\perp$ et telle que $\tau_y(y) = -y$. Remarquer que la réflexion τ_y n'est définie que si y est non isotrope, c'est-à-dire si l'hyperplan $y^\perp$ est régulier.

Exercice 6 *Soit σ une involution dans $\mathrm{O}(q)$ ($\sigma^2 = \mathrm{Id}_E$). On sait que E se décompose en somme directe de E_1 et E_{-1}, les noyaux de $\sigma - \mathrm{Id}_E$ et $\sigma + \mathrm{Id}_E$. Montrer que $E_{-1} = E_1^\perp$. En déduire une bijection canonique entre involutions de $\mathrm{O}(q)$ et sous-espaces réguliers de E.*

Lemme 2 *Soit (E,q) non dégénéré, u et u' deux vecteurs de E tels que $q(u) = q(u') \neq 0$, alors il existe une isométrie $\tau : E \to E$ telle que $\tau(u) = u'$. On peut choisir τ comme produit de réflexions dans $\mathrm{O}(q)$.*

Avec u et u' comme ci-dessus, si $y = u - u'$ vérifie $q(y) \neq 0$, on prend $\tau = \tau_y$; sinon, $z = u + u'$ vérifie $q(z) = 0$ (on a l'identité du parallélogramme $q(y) + q(z) = 2(q(u) + q(u')))$ et $\tau_z(u) = -u'$; on prend alors $\tau = \tau_{u'} \circ \tau_z$.

Theorème 3 *Soit (E,q) non dégénéré. Le groupe orthogonal $\mathrm{O}(q)$ est engendré par les réflexions.*

On utilise le lemme 2 pour faire une récurrence sur la dimension, d'une manière tout à fait analogue à ce qu'on fait pour le groupe orthogonal d'un espace euclidien. Soit σ est une isométrie de q ; on choisit un vecteur u vérifiant $q(u) \neq 0$. Il y a un produit de réflexions τ tel que $\tau(\sigma(u)) = u$. Pour montrer que σ est un produit de réflexions, il suffit de le faire pour $\sigma' = \tau \circ \sigma$. Comme u est fixé par σ' il suffit de considérer la restriction de σ' à $u^\perp$.

On a aussi le fait que tout élément de $\mathrm{O}(q)$ est produit d'au plus $\dim(E)$ réflexions (théorème de Cartan-Dieudonné). Mais ici la démonstration demande plus de travail que dans le cas d'un espace euclidien : ce qui pose problème, c'est le cas $u' - u$ isotrope dans le lemme 2, où on a besoin de deux réflexions.

On trouvera dans [Per] plus de renseignements algébriques sur $\mathrm{O}(q)$. Dans le cas où q est la forme $\langle 1, \dots, 1, -1, \dots, -1\rangle$ de signature (s, t) sur $\mathbb{R}^n$, son groupe orthogonal est noté $O(s, t)$ et on trouvera des renseignements de nature topologique sur ce groupe dans [MnTe] ou [Ser].

5 Espaces hyperboliques. Complétion régulière d'un sous-espace.

Un *plan hyperbolique* est un espace vectoriel P de dimension 2, muni d'une forme bilinéaire symétrique b non dégénérée, possédant un vecteur isotrope u.

Exercice 7 . *Montrer que dans la situation ci-dessus on peut trouver $v \in P$ tel que (u, v) soit une base de P et que la matrice de b dans cette base soit $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.*

Exercice 8 *Soit P un plan vectoriel et q une forme quadratique non dégénérée sur P. Montrer que (P, q) et un plan hyperbolique si et seulement si son discriminant est la classe de -1. (Cet exercice continue dans [Tau2], p.249.)*

Un *espace hyperbolique* est une somme orthogonale de plans hyperboliques. Deux espaces hyperboliques de mme dimension sont isométriques.

Le résultat de complétion régulière d'un sous-espace va servir dans la démonstration du théorème de Witt.

Proposition 4 *Soit (E, b) non dégénéré, F un sous-espace de E, F_0 le noyau de F. Soit $(e_1, \dots, e_p)$ une base de F_0 et U un supplémentaire de F_0 dans F (de sorte que $F = F_0 \perp U$). Alors on peut trouver $f_1, \dots, f_p$ dans E tels que $Ke_i + Kf_i$ soit un plan hyperbolique P_i et que*

$$F' = P_1 \perp P_2 \perp \dots \perp P_p \perp U$$

soit une somme orthogonale dans E. Noter qu'alors F' est régulier.

La démonstration se fait par récurrence sur p. Si $F_1 = Ke_1 + \dots + Ke_{p-1} + U$, on choisit f_p dans $F_1^\perp \setminus F^\perp$ (vérifier que c'est non vide). Vérifier que $P_p = Ke_p + Kf_p$ est un plan hyperbolique, et appliquer l'hypothèse de récurrence à $F_1 \perp P_p$.

En conséquence du théorème précédent, on peut caractériser les espaces hyperboliques comme les (E, q) non dégénérés de dimension paire qui possèdent un sous-espace totalement isotrope de dimension moitié.

6 Théorème de Witt

Theorème 5 *Soit (E, b) non dégénéré. On suppose qu'il existe une isométrie $\sigma : F \to F'$ entre deux sous-espaces F et F' de E. Alors il existe une isométrie $\overline{\sigma} : E \to E$ telle que $\overline{\sigma}|_F = \sigma$.*

Les outils de la démonstration du théorème de Witt sont d'une part la complétion régulière, et d'autre part le lemme 2. On se ramène d'abord au cas où F et F' sont réguliers, en utilisant la complétion régulière (Proposition 4). Il suffit de voir que l'on peut étendre σ en une isométrie d'une complétion régulière $\overline{F}$ de F sur une complétion régulière $\overline{F}'$ de F'.

Ensuite, quand F est régulier, on procède par récurrence sur la dimension de F. Pour $\dim(F) = 0$, pas de problème. Si $\dim(F) > 0$, on choisit $u \in F$ tel que $q(u) \neq 0$, et on prend $u' = \sigma(u)$. D'après le Lemme 2, il existe une isométrie $\tau : E \to E$ telle que $\tau(u) = u'$. On remplace F' par $\tau^{-1}(F')$ et σ par $\tau^{-1} \circ \sigma$, ce qui permet de supposer $\sigma(u) = u$ (si $\rho : E \to E$ est une isométrie qui étend $\tau^{-1} \circ \sigma$, alors $\tau \circ \rho$ est une isométrie qui étend σ).

On raisonne ensuite sur $u^\perp$ et $F \cap u^\perp$ (qui est régulier). Puisque $\sigma(u) = u$ on a $\sigma(F \cap u^\perp) \subset u^\perp$. On applique l'hypothèse de récurrence pour obtenir une isométrie $\overline{\sigma}_1 : u^\perp \to u^\perp$ qui étend $\sigma|_{F\cap u^\perp}$. On étend $\overline{\sigma}_1$ à une isométrie $\overline{\sigma} : E \to E$ en posant $\overline{\sigma}(u) = u$. On a bien $\overline{\sigma}|_F = \sigma$.

Passons maintenant aux conséquences du théorème de Witt.

- On suppose (E, b) non dégénéré. Tous les *sous-espaces totalement isotropes maximaux* de E ont même dimension. Cette dimension est appelée *l'indice de Witt*. Les complétions régulières de sous-espaces totalement isotropes maximaux sont des sous-espaces hyperboliques maximaux. En particulier l'indice de Witt est inférieur ou égal à la moitié de la dimension de E.
  On trouvera une étude directe des sous-espaces totalement isotropes maximaux dans [Gou], p. 234.
- *Théorème de simplification.* Si $E \perp F_1$ est isométrique à $E \perp F_2$, alors F_1 est isométrique à F_2 (sans hypothèse de non dégénérescence). On se ramène aux cas où tous les espaces sont non dégénérés en considérant des supplémentaires des noyaux. Dans le cas non dégénéré, on applique le théorème de Witt pour trouver une isométrie $E \perp F_1 \to E \perp F_2$ qui soit l'identité sur E, et qui envoie donc F_1 sur F_2.
- *Théorème de décomposition de Witt.* Tout (E, b) se décompose comme

$$E = E_0 \perp E_{\text{hyp}} \perp E_{\text{def}} ,$$

  où E_0 est le noyau, E_{hyp} est un espace hyperbolique et E_{def} est défini (c.-à-d. sans vecteur isotrope, on dit aussi anisotrope). Cette décomposition est unique à isométrie près. La dimension de la partie hyperbolique E_{hyp} est deux fois l'indice de Witt. Cette décomposition ramène la classification à isométrie près des formes quadratiques sur un corps quelconque à celle des formes définies, mais on n'est pas beaucoup plus avancé pour celà.

Exercice 9 *Mettre en relation l'indice de Witt avec les autres invariants de formes non dégénérées : dimension pour $K = \mathbb{C}$, signature pour $K = \mathbb{R}$, dimension et discriminant pour $K = \mathbb{F}_\ell$.*

Le théorème de Witt est un outil pour l'étude de $\mathrm{O}(q)$.

Exercice 10 *Montrer que* $\mathrm{O}(q)$ *agit de façon transitive sur l'ensemble des droites vectorielles isotropes*

Références

[Ber] M. Berger. *Géométrie - volume 4 : formes quadratiques, quadriques et coniques.* Cedic - Fernand Nathan, 1979.

[Gou] X. Gourdon. *Les Maths en Tête, Algèbre.* Ellipses.

[MnTe] R. Mneimné, F. Testard. *Groupes de Lie Classiques.* Hermann.

[Per] D. Perrin. *Cours d'Algèbre.*

[Ser] D. Serre. *Les Matrices.* Dunod.

[Tau] P. Tauvel. *Mathématiques Générales pour l'Agrégation.* Masson.

[Tau2] P. Tauvel. *Exercices de Mathématiques pour l'Agrégation, Algèbre 2.* Masson.