Formes quadratiques
(version chantier)

Marc SAGE

6 février 2018

Table des matières

b. o. : base orthogonale

1 Un peu de dualité

Soit E un ev de dimension finie[1] *et F un sev de E.*
On se donne un sev V de $E^* \times F$ qui annule le chevron de dualité.
Montrer que $\dim V \leq \dim F$ *et donner des exemples pour le cas d'égalité.*

Solution proposée.
Le chevron de dualité s'annulant sur $F^* \times F$, on peut supposer $F = E$.

L'idée est d'introduire une forme bilinéaire sur $E^* \times E$ pour laquelle V va devenir totalement isotrope, ce qui permettra de majorer sa dimension. Pour obtenir l'isotropie souhaitée, on pense naturellement à la forme quadratique $\begin{pmatrix}\varphi\\a\end{pmatrix} \mapsto \varphi(a)$ dont la forme bilinéaire associée est[2] $B : \left(\begin{pmatrix}\varphi\\a\end{pmatrix}, \begin{pmatrix}\psi\\b\end{pmatrix}\right) \mapsto \varphi(b) + \psi(a)$. Il s'agit de calculer le rang de B, autrement dit son noyau.

Soit $\begin{pmatrix}\varphi_0\\a_0\end{pmatrix} \in \operatorname{Ker} B$. Cela signifie $\varphi_0(a) + \varphi(a_0) = 0$ pour tout $(\varphi, a) \in E^* \times E$. En prenant $\varphi = \varphi_0$, on obtient $\varphi_0(a + a_0) = 0$, d'où $\varphi_0 = 0$. Il reste donc $\varphi(a_0) = 0$ pour tout $\varphi \in E^*$, donc $a_0 \in E^{*\circ} = \{0\}$. Finalement le noyau est nul, donc B est non dégénérée. Cela permet de majorer la dimension du SETI V par $\frac{1}{2}\dim(E^* \times E) = \dim E$, *CQFD.*

D'après la toute première remarque, on aura égalité pour $V = F^* \times F$ où F est un sev de E.

2 Classifications des formes quadratiques sur un corps fini

Soit K un corps fini à q éléments. On rappelle que q est une puissance de la caractéristique de K. On pourra montrer que K contient $\frac{q+1}{2}$ carrés pour q impair.

Montrer que toute matrice symétrique S à coefficients dans K est congrue à $\begin{pmatrix} I_{n-1} & \\ & \lambda \end{pmatrix}$ *où λ est soit* 1 *(forme quadratique standard), soit n'est pas un carré dans K.*

Solution proposée.
Quitte à se placer dans une b. o., on peut toujours supposer S sous forme diagonale $S = \operatorname{Diag}(\lambda_1, ..., \lambda_n)$. Un bête calcul matriciel permet, combiné avec une récurrence, de se ramener au cas $n = 2$:

$$\begin{aligned}
S &= \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix} = \begin{pmatrix} P\begin{pmatrix} I_{n-2} & \\ & \lambda \end{pmatrix}{}^tP & \\ & \lambda_n \end{pmatrix} \text{ où } \lambda \in K \\
&= P'\begin{pmatrix} I_{n-2} & & \\ & \lambda & \\ & & \lambda_n \end{pmatrix}{}^tP' \text{ avec } P' = \begin{pmatrix} P & \\ & 1 \end{pmatrix} \\
&= P'\begin{pmatrix} I_{n-2} & & \\ & Q\begin{pmatrix} 1 & \\ & \mu \end{pmatrix}{}^tQ & \end{pmatrix}{}^tP' \text{ où } \mu = 1 \text{ ou } \mu \text{ non carré} \\
&= P''\begin{pmatrix} I_{n-1} & \\ & \mu \end{pmatrix}{}^tP'' \text{ avec } P'' = P'\begin{pmatrix} I_{n-2} & \\ & Q \end{pmatrix}.
\end{aligned}$$

Il suffit donc de traiter les cas $n = 1$ et 2.

Pour $n = 1$, la matrice S est un scalaire λ, qui est soit un carré c^2, auquel cas $S = (c)(1)\ {}^t(c)$ est la forme quadratique standard, soit un non carré, *CQFD.*

[1] Le corps de base peut être de caractéristique 2. On peut en effet faire une théorie des orthogonaux uniquement avec des formes bilinéaires sans passer par les formes quadratiques. On renvoit au *Cours d'algèbre* de D. Perrin pour plus de détails.

[2] quitte à rajouter rétrospectivement un 2 devant la forme quadratique afin d'éviter les problèmes en caractéristique 2

Pour $n=2$, soit $S=\begin{pmatrix}\lambda & \\ & \mu\end{pmatrix}$. On veut mettre un 1 en haut à gauche de la matrice, ce qui correspond à trouver un vecteur $u=(x,y)$ de K^2 tel que ${}^tuSu=1$, *i. e.* à résoudre l'équation

$$\lambda x^2+\mu y^2=1.$$

Distinguons deux cas selon que la caractéristique de K soit 2 ou non.

Si q est pair, tout élément x de K est un carré puisque $x^q=x$: en effet, l'ordre d'un $x\in K^*$ divise le cardinal de K^*, ce qui s'écrit $x^{q-1}=1$, *i. e.* $x^q=x$, ce qui reste valable pour $x=0$. S est donc congrue à l'identité, et le problème est résolu.

Pour q impair, montrons qu'il y a $\frac{q+1}{2}$ carrés dans K. Il suffit d'introduire le morphisme de groupes "élévation au carré" :

$$c:\left\{\begin{array}{ccc}K^* & \longrightarrow & K^* \\ x & \longmapsto & x^2\end{array}\right. .$$

Son noyau est $\{1,-1\}$ qui est de cardinal 2 puisqu'on est en caractéristique impaire. Le théorème de factorisation des morphismes permet d'écrire

$$\operatorname{Im} c\simeq {}^{K^*}\!\diagup_{\operatorname{Ker} c},$$

d'où le résultat en prenant les cardinaux et en rajoutant le carré manquant 0.

3 Théorème de Springer

Soit $q(x)=\sum a_{i,j}x_ix_j$ une forme quadratique anisotrope sur k^n. Soit $k\hookrightarrow K$ une extension de k. Montrer que q considérée comme polynôme homogène de degré 2 à n variables dans K reste anisotrope dans les cas suivants :

- *$K=k\left((X_i)_{i\in I}\right)$ est un corps des fractions rationnelles en des indéterminées X_i ;*
- *$k\hookrightarrow K$ est de dimension finie impaire en tant que k-ev.*

Solution proposée.

Quitte à se placer dans une b. o., on peut supposer $q(x)=\sum\lambda_ix_i^2$ où $\lambda_i\in k$. Considérons par l'absurde un vecteur $x\in K^n$ isotrope non nul.

• On peut supposer I fini en ne considérant que les indéterminées qui apparaissent dans les coordonnéées de x. Puis on peut toujours faire une récurrence sur le nombre d'indéterminées et suppposer $K=k(X)$. En éliminant les dénominateurs, on obtient une expression

$$\sum\lambda_iP_i^2=0$$

où les P_i peuvent être pris premiers entre eux quitte à diviser par leur pgcd ; en particulier, X ne peut pas tous les diviser. En évaluant en 0, on trouve un vecteur isotrope non nul dans k^n, c'est une contradiction.

• q est isotrope sur le corps $k(x_1,...,x_n)$ engendré par les x_i, et quitte à faire une récurrence sur le nombre de générateurs, on peut supposer $K=k(\alpha)$ monogène. On précède alors par récurrence sur le degré $d:=\deg\alpha=[K:k]$ de l'extension.

Les composantes de x étant des polynômes P_i en α non tous nul de degré $<d$, on peut écrire $\sum\lambda_iP_i(\alpha)^2=0$, ce qui signifie $\sum\lambda_iP_i^2$ multiple du polynôme minimal de α, mettons

$$\sum\lambda_iP_i^2=A\mu_\alpha.$$

Quitte à diviser par le pgcd des P_i dans $k[X]$ (qui doit diviser A car μ_α est irréductible), on peut supposer les P_i premiers entre eux. En notant $m=\max\deg P_i<d$, on voit par anisotropie de q que le terme en X^m du terme de gauche n'est pas nul : on en déduit

$$\deg A=2m-d\leq 2(d-1)-d=d-2$$

qui est impair. A admet donc un facteur irréductible B de degré impair, et en appelant β une racine de ce facteur dans un bon corps de décomposition (B est donc le polynôme minimal de β dans l'extension $k\hookrightarrow k(\beta)$), on voit que $\sum\lambda_iP_i(\beta)^2=0$, d'où un vecteur isotrope dans l'extension $k(\beta)$ qui est de degré $\deg B$ impair $<d$, d'où par récurrence $P_i(\beta)=0$ pour tout i, ce qui contredit la primalité relative des P_i dans $k(\beta)$ (le pgcd est inchangé par extension de corps...).

Remarque. On vient de montre la conservation de l'anisotropie par extension impaire ou transcendante pure des scalaires. Le résultat tombe complètement en défaut pour les extension de degré pair. En effet, si le nombre de variables est au moins 2, on peut contruire une extension de k de degré pair où apparait un vecteur isotrope. Soit $q(x_1, ..., x_n) = \lambda x_1^2 + \mu x_2^2 + ...$ dans une base de diagonalisation, avec $\lambda \neq 0$ (sinon $q = 0$ est isotrope). Le polynôme $\lambda X^2 + \mu$ est irréductible sur k car sans racine par anisotropie de q, donc admet une racine α dans l'extension quadratique $k \hookrightarrow {}^{k[X]}\!/_{\lambda X^2+\mu}$. Le vecteur $(\alpha, 1, 0, ..., 0)$ est alors isotrope dans l'extension.

4 Sur les sommes de carrés

TD 6 alg 1 07/08
On appelle *niveau* d'un corps K le plus petit entier n tel que -1 est somme de n carrés. On le note $\nu(K)$.

1. *Montrer que deux corps isomorphe ont même niveau. Réciproque ?*
2. *Calculer les niveaux de* $\mathbf{F}_{p^n}$, $\mathbf{Q}\left(i\sqrt{2}\right)$, $\mathbf{Q}(j)$, $\mathbf{Q}\left(j\sqrt[3]{2}\right)$
3. *Montrer que* $\nu(K(X)) = \nu(K)$.
   On suppose $\operatorname{car} K \neq 2$. *Pour* $n \geq 1$, *on regarde* $Q(\overrightarrow{a}) = \sum a_i^2$ *pour* $\overrightarrow{a} \in K^n$. *Notons* $G = \operatorname{Im} Q \setminus \{0\}$ *l'ensemble des sommes de* n *carrés.*
4. *Si* Q *est isotrope, montrer que* Q *est surjective.*
5. *On suppose* $n = 2^k$ *et* Q *anisotrope. Soit* $\overrightarrow{a} \neq 0$. *Mq* $\exists A \in M_n(K)$, ${}^tAA = Q(a)\,\mathrm{Id}$ *dont première ligne* $= a$. *En déduire que* G *est un groupe.*
6. *Montrer que si* $v(K)$ *est fini, c'est une puissance de* 2.

SOL

1. $\mathbb{Q}(i)$ et $\mathbb{C}$ ont niveau 1
2.
3. $\leq$ clair ; si $-1 = \sum_1^n F_i^2$, on réduit au même dénom, d'où $\sum_0^n P_i^2 = 0$. On prend les coef dom, on divise par celui de $P_0 \neq 0$, d'où -1 somme de n carrés et $n \leq \nu(k)$.
4. $\det_{b.c.} Q = 1$, donc Q non dégénéré. Si a isotrope, on a un plan hyperobloique Hcontenant a, dans lequel $Q \sim \begin{pmatrix} & 1 \\ 1 & \end{pmatrix}$ et $\operatorname{Im} Q_H = K$. (ainsi $G = K^*$ est un groupe)
5. Par réc sur k. Si $n = 1$, prendre $A = a$. Ensuite, $a \in K^{2n}$ est la concat de x et y. ALors $A := \begin{pmatrix} X & Y \\ -Y & {}^tY^{-1}{}^tXY \end{pmatrix}$ convient. Ainsi, $Q(a)Q(b) = {}^tb(Q(a)\,\mathrm{Id})\,b = {}^tb{}^tAAb = Q(Ab)$, et $Q(a)Q(b)^{-1} = Q\left(AbQ(b)^{-1}\right)$
6. Ecrvons $-1 = \sum_1^{2^k-1} a_i^2 + \sum_{2^k}^{\nu} a_i^2$ où k maximal. Alors $\lambda := 1 + \sum_1^{2^k-1} a_i^2$ est non nul sinon $\nu < 2^k$. Alors λ et $\mu := \sum_{2^k}^{\nu} a_i^2$ sont deux sommes de 2^k carrés, donc $-1 = \frac{\mu}{\lambda}$ aussi, d'où $\nu = 2^k$.

5 Deux formes quadratiqus de même cône sont colinéaires

Soit q *et* q' *deux formes quadratiques sur un* K-ev *où* K *est quadratiquement clos. Montrer l'équivalence*

$$C(q) = C(q') \iff \exists \lambda \in K^*,\ q' = \lambda q.$$

On pourra perturber un vecteur anisotrope selon une direction donné.
Que se passe-t-il si l'on retire l'hypothèse "K *quadratiquement clos" ?*

On suppose à présent que q et q' sont deux formes quadratiques non dégénérées mais isotropes sur un K-ev de dimension n. Montrer l'implication

$$C(q) = C(q') \iff \exists \lambda \in K^*,\ q' = \lambda q.$$

soit $c \in C(q)$ non nul : regarder le vecteurs $tc + x$ (où$x \in E$) dans $C(q)$ et en déuire que $H := x^{\perp}$ est le même pour q et q'

mq $\exists \lambda \neq 0$ tq $q' = \lambda q$ en dehors de H

mq $\widehat{q'} = \lambda \widehat{q}$ sur $(E \setminus H)^2$, conclure

Solution proposée.

Si les cônes valent tout l'espace, nos deux formes quadratiques sont nulles et c'est terminé.

Sinon, notre scalaire λ doit s'écrire $\frac{q'(a)}{q(a)}$ où a est un vecteur anisotrope ; posons donc $\lambda := \frac{q'(a)}{q(a)}$ pour un tel a et montrons $q' = \lambda q$ en suivant l'indication. Il s'agit, un vecteur v étant donné, de comparer

$$\begin{cases} q'(a+tv) = q'(a) + 2t\widehat{q'}(a,v) + t^2 q'(v) \\ \lambda q(a+tv) = \lambda q'(a) + 2\lambda t\widehat{q}(a,v) + \lambda t^2 q(v) \end{cases} \quad \text{où } t \in K.$$

On dispose de deux polynômes en t ayant même coefficient constant non nul et s'annulant aux mêmes points par hypothèse : ce sont les mêmes (les scinder sur K). Prendre $t = 1$ et $v = w - a$ où w vecteur quelconque donne $q'(w) = \lambda q(w)$, *CQFD.*

Pour $K = \mathbb{R}$, les deux formes $\begin{cases} (a,b) \mapsto a^2 + b^2 \\ (a,b) \mapsto a^2 + 2b^2 \end{cases}$ ont même cône $\left\{\overrightarrow{0}\right\}$ mais ne sont pas colinéaires.

Soit $c \in C(q)$ non nul. On regarde $q(x + tc) = q(x) + 2t\widehat{q}(x,c)$.

6 La fibre au-dessus d'un point engendre toutou rien

Soit q une forme quadratique sur un K-ev E (toujours avec $\operatorname{car} K \neq 2$).

On prend un scalaire $\lambda \neq 0$ dont note $A := q^{-1}(\{\lambda\})$ la préimage par q. Nous allons montrer que, si K a strictement plus de trois éléments, cette préimage engendre tout E (lorsqu'elle est non vide).

Par l'absurde, montrer qu'il y a une forme linéaire $\varphi \neq 0$ nulle sur A.
Fixons $a \in A$. On note $l := \widehat{q}(a, \cdot)$. Montrer que $q \times \varphi \times l = 0$.
Conclure en perturbant a.

Si $\operatorname{Vect} A \subsetneq E$, on complète $\operatorname{Vect} A$ en un hyperplan, noyau d'une forme linéiare non nulle qui convient. L'idée est alors, à partir d'un $a \in A$, d'en créer d'autre pour dire qu'ils sont annulés par φ et en tirer de l'info. On sait faire : $a - 2\frac{l(x)}{q(x)}x$!

Il revient à montrer que, si x est anisotrope, alors $\varphi(x)\, l(x) = 0$. Soit donc un tel x. Le vecteur $a - 2\frac{l(x)}{q(x)}x$ est dans A, donc est annulé par φ, d'où $\underbrace{\varphi(a)}_{=0} = \varphi\left(2\frac{l(x)}{q(x)}x\right) = 2\frac{l(x)}{q(x)}\varphi(x)$ comme voulu ($\operatorname{car} K \neq 2$).

Appliquons l'égalité $q\varphi l = 0$ en le perturbé $a + tx$ où t et x sont à choisir. On obtient

$$\begin{aligned} 0 &= q(a+tx)\,\varphi(a+tx)\,l(a+tx) \\ &= (\lambda + 2tl(x))\, t\varphi(x)\,(\lambda + tl(x)). \end{aligned}$$

Pour obtenir une contradiction, on s'arrange pour que le produit ci-dessus soit non nul. Ce sera le cas si $\varphi(x) \neq 0$ (possible car $\varphi \neq 0$) et si t évite les valeurs $\frac{-\lambda}{2l(x)}$, 0 et $\frac{-\lambda}{l(x)}$ (possible car K a au moins quatre éléments).

7 Les automorphismes fixant une sphère non vide sont les similitudes

Soit q nd, $S_\alpha = q^{-1}(\{\alpha\})$ pour $\alpha \neq 0$ supposée non vide. Alors $g \in O(q)$ ssi $g(S_\alpha) = S_\alpha$, sauf pour $q = x^2 - y^2$ sur F_3^2.

(perrin)

8 Sur les fq de discr n'anulant pas 0 dans $k[X]$

david harari 25 fev 1992, 00h44, 3 mars 1992 18h

Soit Q une forme quadratique sur l'anneau de polynomes k[X] (sous-entendu : sur une $\bigoplus$ finie de $k[X]$) Supposons que son discriminant ne s'annule pas en 0 (condition bien definie). Q est-elle isomorphe sur le corps k(X) à une forme diagonale <a_1,a_2,...a_n> avec tous les a_i elements de k(X) de valuation nulle ?

On fixe une base de notre module de rg n, on regarde la matrice M de notre fq. Elle définit un fq sur le localisé en X (ie les fractions rationnelles où 0 n'est pas un pole), et son det devient inversible, donc la fq induit est n.d., donc ? ? ? ? elle représente un inversible du localisé, puis on conclut par récurrence ? ? ? ? ?