ANNALES SCIENTIFIQUES
DE L'UNIVERSITÉ DE CLERMONT-FERRAND 2
Série Mathématiques

BERTIN DIARRA

Remarques sur les matrices orthogonales (resp. symétriques) à coefficients p-adiques

Annales scientifiques de l'Université de Clermont-Ferrand 2, tome 95, série *Mathématiques*, n° 26 (1990), p. 31-50
<http://www.numdam.org/item?id=ASCFM_1990__95_26_31_0>

Ann. Sci. Univ. "Blaise Pascal", Clermont II, Sér. Math., Fasc. 26ème, pp. 31-50

Remarques sur les matrices orthogonales (resp. symétriques) à coefficients p-adiques

par

Bertin DIARRA

Université Blaise Pascal - Clermont II - 63177 Aubière Cédex

I - La forme quadratique standard

I-1. *Formes quadratiques*

Soient K un corps de caractéristique $\neq 2$, E un K-espace vectoriel de dimension n. Une application $q : E \to K$ est appelée forme quadratique s'il existe une forme bilinéaire symétrique $f : E \times E \to K$ telle que $q(x) = f(x,x)$. On a

$$f(x,y) = \tfrac{1}{2}(q(x+y) - (q(x) - q(y))).$$

On dit que q est *régulière* si f est non dégénérée.

Un élément x de E tel que $q(x) = 0$ est dit *isotrope.*

Soit V un sous-espace vectoriel de E ; on note $V^{\perp}$ l'ensemble des $y \in E$ tels que $f(x,y) = 0$ pour tout $x \in V$ et on dit que V est *totalement isotrope* si $V \subset V^{\perp}$. On démontre (c.f. par exemple [1] ou [2]) que tout sous-espace totalement isotrope est contenu dans un espace totalement isotrope maximal. Tous les sous-espaces totalement isotropes maximaux ont la même dimension υ, appelée *indice* de q ; de plus $2\upsilon \leq n$.

Supposons q régulière. Soit $u \in \mathrm{End}_K(E)$. Il existe un unique opérateur $u^* \in \mathrm{End}_K(E)$, appelé *adjoint de* u *par rapport à* f, tel que $f(u(x), y) = f(x, u^*(y))$ pour $x,y \in E$; on a $u^{**} = u$. On dit que u est *symétrique* si $u = u^*$ et que u est *un opérateur orthogonal* si u est inversible tel que $u^{-1} = u^*$, ce qui équivaut à $f(u(x), u(y)) = f(x,y))$ pour $x,y \in E$.

I-2. *La forme quadratique standard*

Considérons $E = K^n$ et soit $B = (e_1, \dots, e_n)$ la base canonique de E. La forme bilinéaire standard est définie par le produit scalaire $< x,y > = \sum_{j=1}^{n} x_j y_j$ où $x = \sum_{i=1}^{n} x_j e_j$,

$y = \sum_{j=1}^{n} y_j e_j$; c'est une forme bilinéaire symétrique non dégénérée ; la forme quadratique associée est donnée par $q(x) = \sum_{j=1}^{n} x_j^2$. Si K est un corps ordonné, la forme quadratique standard est d'indice 0.

Identifiant $End_K(K^n)$ à l'anneau de matrice carrée $Mat_n(K)$; l'adjoint de $u \in End_K(K^n)$ par rapport à $<\,,\,>$ est la matrice transposée ${}^t u$ de u. La matrice u est un opérateur orthogonal (resp. symétrique) si et seulement si ${}^t u = u^{-1}$ (resp. ${}^t u = u$).

Remarque 1 :

(i) *Soit* $u = (a_{ij})_{1 \le i,j \le n} \in Mat_n(K)$; u *est orthogonale si et seulement si tout vecteur colonne* C *(resp. tout vecteur ligne* L*) est non isotrope tel que* $q(C) = 1$ (resp. $q(L) = 1$) *et les vecteurs colonnes (resp. les vecteurs lignes) sont deux à deux orthogonaux.*

(ii) *Si* u *est orthogonale*, alors $(\det u)^2 = 1$.

Lemme 1 :

Soit $u \in Mat_n(K)$ *une matrice orthogonale.*

(i) *Si* $x \in K^n$ *est un vecteur propre non isotrope de* u, *la valeur propre correspondant à* x *est* ± 1.

(ii) *Si* λ *est une valeur propre de* u, *on a* $\lambda \neq 0$ *et* λ^{-1} *est une valeur propre de* u.

(i) En effet si $u(x) = \lambda x$ et $< x,x > \neq 0$, on a
$< u(x), u(x) > = < \lambda x, \lambda x > = \lambda^2 < x,x > = < x, x >$; donc $\lambda^2 = 1$ et $\lambda = \pm 1$.

(ii) Soit $P_u(X) = \det(u - X I_n)$ le polynôme caractéristique de u ; on a
$P_{u^{-1}}(X) = \det(u^{-1} - X I_n) = \det u^{-1} \det(I_n - X u) = \det u^{-1} (-1)^n X^n \det(u - X^{-1} I_n)$
$= \det u^{-1} (-1)^n X^n P_u(X^{-1})$. Donc si ${}^t u = u^{-1}$, alors on voit que
$P_u(X) = P_{{}^t u}(X) = P_{u^{-1}}(X) = \det u^{-1} (-1)^n X^n P_u(X^{-1}) = \pm (-1)^n X^n P_u(X^{-1})$.
Ainsi $P_u(\lambda) = 0 \Leftrightarrow \pm (-1)^n \lambda^n P_u(\lambda^{-1}) = 0 \Leftrightarrow P_u(\lambda^{-1}) = 0$.

Remarque 2 :

Soit $u \in Mat_n(K)$ *une matrice orthogonale ayant toutes ses valeurs propres dans* K. *Si* $\lambda \neq \pm 1$ *est une valeur propre de* u, *tout vecteur propre associé à* λ *est un vecteur isotrope.*

Exemple : $n = 2$.

Soit $u = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in Mat_2(K)$ orthogonale. On a dét $u = ad - bc = \pm 1$; de plus $a = \dfrac{d}{ad - bc}$ et $b = -\dfrac{c}{ad - bc}$.

(i) Supposons $b = 0$ $(\Leftrightarrow c = 0)$

alors $u = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$ avec $ad = \pm 1$. On voit donc que u est égale à l'une des quatres

matrices suivantes $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$.

(ii) Supposons $b \neq 0$ $(\Leftrightarrow c \neq 0)$

1er cas : dét $u = 1$, alors $u = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ et $P_u(\lambda) = (a - \lambda)^2 + b^2$; les valeurs propres de u sont donc $\lambda_1 = a + i\,b$ et $\lambda_2 = a - i\,b$ dans $L = K[i]$ où $i = \sqrt{-1}$; de plus $\lambda_1 \lambda_2 = a^2 + b^2 = 1$. Ainsi u est diagonalisable sur $L = K[i]$. Le vecteur $\varepsilon_1 = i\,e_1 - e_2 \in L^2$ (resp. $\varepsilon_2 = e_1 - i\,e_2$) est un vecteur propre associé à λ_1 (resp. λ_2) ; ε_1 et ε_2 sont deux vecteurs isotropes tels que $< \varepsilon_1 , \varepsilon_2 > = 2\,i$.

2ème cas : dét $u = -1$, alors $u = \begin{pmatrix} a & b \\ b & -a \end{pmatrix}$, on a dét $u = -a^2 - b^2 = -1$ et $u^2 = I_2$; les valeurs propres de u sont donc $\lambda_1 = 1$ et $\lambda_2 = -1$. Ainsi u est diagonalisable sur K avec $\varepsilon_1 = (1+a)\,e_1 + b\,e_2$ (resp. $\varepsilon_2 = b\,e_1 - (1 + a)\,e_2$) vecteur propre associé à 1 (resp. -1) .

I−3. La forme quadratique standard sur Q_p^n

Soit p un nombre premier et soit Q_p le corps des nombres p-adiques. On munit le Q_p-espace vectoriel Q_p^n du produit scalaire standard. Soit [ ] la fonction partie entière des nombres réels. On a :

Proposition 1 :

La forme quadratique standard $q(x) = \sum_{j=1}^{n} x_j^2$ *sur* Q_p^n *a pour indice*

(i) $\quad v = \left[\frac{n}{2}\right]$ *si* $p \equiv 1$ *(mod. 4)*

(ii) $\quad v = \left[\frac{n}{2}\right]$ *si* $p \equiv 3$ *(mod. 4) et* $n \not\equiv 2$ *(mod. 4)*

(iii) $\quad v = \left[\frac{n}{2}\right] - 1$ *si* $p \equiv 3$ *(mod. 4) et* $n \equiv 2$ *(mod. 4)*

Démonstration :

Rappelons que -1 est un carré dans Q_p si et seulement si $p \neq 2$ et le symbole de Legendre $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ est égal à 1, c'est-à-dire si et seulement si p est de la forme $4m+1$. Alors
$i = \sqrt{-1} \in Q_p$ si et seulement si $p \equiv 1$ (mod. 4).

1° Supposons donc $p \equiv 1$ (mod. 4) soit $(e_j)_{1 \leq j \leq n}$ la base canonique de $E = Q_p^n$. Posons $v_0 = \left[\frac{n}{2}\right]$ et considérons les vecteurs

$$\varepsilon_1 = ie_1 + e_2 \ ; \ \varepsilon_2 = ie_3 + e_4, \dots, \varepsilon_j = ie_{2j-1} + e_{2j}, \dots, \varepsilon_{v_0} = ie_{2v_0-1} + e_{2v_0}$$

Pour $1 \leq \ell \neq j \leq v_0$, on a $< \varepsilon_\ell, \varepsilon_j > = < ie_{2\ell-1} + e_{2\ell}, ie_{2j-1} + e_{2j} > =$ $i^2 < e_{2\ell-1}, e_{2j-1} > + i < e_{2\ell-1}, e_{2j} > + i < e_{2\ell}, e_{2j-1} > + < e_{2\ell}, e_{2j} > = 0$ et pour $1 \leq j \leq v_0$, $< \varepsilon_j, \varepsilon_j > = i^2 < e_{2j-1}, e_{2j-1} > + 2i < e_{2j-1}, e_{2j} > + < e_{2j}, e_{2j} > = 0.$

Il est clair que $(\varepsilon_j)_{1 \leq j \leq v_0}$ est libre dans E . Le sous-espace vectoriel $V = \bigoplus_{j=1}^{v_0} Q_p \varepsilon_j$ de E, de dimension v_0, est totalement isotrope car si $x = \sum_{j=i}^{v_0} \lambda_j \varepsilon_j$, $y = \sum_{j=i}^{v_0} \mu_j \varepsilon_j$, on a $< x,y > = \sum_{\ell,j} \lambda_\ell \mu_j < \varepsilon_\ell, \varepsilon_j > = 0.$

Si υ est l'indice de q , on a $\upsilon \leq \left[\frac{n}{2}\right] = \upsilon_0$, donc $\upsilon_0 = \upsilon = \left[\frac{n}{2}\right]$.

Ce qui achève la démonstration de (i) .

2°) Supposons que $p \not\equiv 1 \pmod{4}$; c'est-à-dire $p = 2$ ou $p \equiv 3 \pmod{4}$ alors $i = \sqrt{-1} \notin \mathbf{Q}_p$.

a) $n = 2$; si $q(x) = x_1^2 + x_2^2 = 0$ avec $x_2 \neq 0$, on aurait $\left(\frac{x_1}{x_2}\right)^2 = -1$ et

$i = \frac{x_1}{x_2} \in Q_p$, ce qui est absurde. Ainsi pour tout $x = x_1 e_1 + x_2 e_2 \in Q_p^2$, $x \neq 0$

on a $q(x) \neq 0$; d'où $\upsilon = 0$.

b) $n = 3$; on a $q(x) = x_1^2 + x_2^2 + x_3^2$. Considérons la forme quadratique $\bar{q}(x) = \bar{x}_1^2 + \bar{x}_2^2 + \bar{x}_3^2$ sur $\mathbf{F}_p^3$. On a $d^\circ \bar{q} = 2 < 3$; on déduit du théorème de Chevalley, qu'il existe $\bar{x} = (\bar{x}_1, \bar{x}_2, \bar{x}_3) \neq 0$ dans $\mathbf{F}_p^3$ tel que $\bar{q}(\bar{x}) = 0$. On a $\frac{\partial \bar{q}}{\partial x_j} = 2\bar{x}_j$. *Supposons* $p \equiv 3 \pmod{4}$ alors il existe $x \in \mathbf{Z}_p^3$ et $x \neq 0$, $1 \leq j \leq 3$

tels que $q(x) \equiv 0 \pmod{p}$ et $v\left(\frac{\partial q}{\partial x_j}(x)\right) = 0$. On déduit de la méthode de Newton

(c.f. par exemple [3]) qu'il existe $x = \sum_{j=1}^{3} x_j e_j \in Z_p^3$, $x \neq 0$ tel que

$q(x) = x_1^2 + x_1^2 + x_3^2 = 0$. Supposons $x_3 \neq 0$ et posons $a = \frac{x_1}{x_3}$, $b = \frac{x_2}{x_3}$, on a alors

$a^2 + b^2 + 1 = 0$.

De plus $a \neq 0$ et $b \neq 0$ car si on avait $b = 0$ on aurait $a^2 + 1 = 0$ et $a = \pm i \in \mathbf{Q}_p$, absurde.

Posons $\varepsilon_1 = a e_1 + b e_2 + e_3$; alors le sous-espace $V = \mathbf{Q}_p \varepsilon_1$ de $\mathbf{Q}^3_p$ est totalement isotrope ; comme $2\upsilon \leq 3$, on a $\upsilon = 1 = \left[\frac{3}{2}\right]$.

c) Supposons $\underline{n \equiv 0\ (\mathrm{mod.}4)}$ c'est-à-dire $n = 4m$.

Considérons $\varepsilon_1 = ae_1 + be_2 + e_3$; $\varepsilon_2 = -be_1 + ae_2 + e_4 ; \dots ;$

$\varepsilon_{2j-1} = ae_{4j-3} + be_{4j-2} + e_{4j-1}$; $\varepsilon_{2j} = -be_{4j-3} + ae_{4j-2} + e_{4j} ; \dots ;$

$\varepsilon_{2m-1} = ae_{4m-3} + be_{4m-2} + e_{4m-1}$; $\varepsilon_{2m} = -be_{4m-3} + ae_{4m-2} + e_{4m}$.

On vérifie aussitôt que $(\varepsilon_1, \varepsilon_2, \dots, \varepsilon_{2m-1}, \varepsilon_{2m})$ est libre. De plus $< \varepsilon_{2j-1}, \varepsilon_{2j-1} > = a^2 + b^2 + 1 = 0$; $< \varepsilon_{2j}, \varepsilon_{2j} > = b^2 + a^2 + 1 = 0$; $< \varepsilon_{2j-1}, \varepsilon_{2j} > = -ab + ba = 0$ et $< \varepsilon_{2j-1}, \varepsilon_{2\ell} > = 0$ si $1 \leq \ell \neq j \leq m$.

On voit que le sous-espace $V = \bigoplus_{j=1}^{m} (Q_p \varepsilon_{2j-1} \oplus Q_p \varepsilon_{2j})$ de $E = Q_p^n$ de dimension $2m = \frac{n}{2}$ est totalement isotrope, donc $\upsilon = 2m = [\frac{n}{2}]$.

d) Supposons $\underline{n \equiv 1\ (\mathrm{mod.}4)}$ c'est-à-dire $n = 4m + 1$. Posant pour $1 \leq j \leq m$, $\varepsilon_{2j-1} = ae_{4j-3} + be_{4j-2} + e_{4j-1}$ et $\varepsilon_{2j} = -be_{4j-3} + ae_{4j-2} + e_{4j}$, on voit comme en c) que

$$V = \bigoplus_{j=1}^{m} (Q_p \varepsilon_{2j-1} \oplus Q_p \varepsilon_{2j}) \text{ est totalement isotrope de dimension}$$

$2m = [2m + \frac{1}{2}] = [\frac{n}{2}]$; donc $\upsilon = [\frac{n}{2}]$.

e) Supposons $\underline{n \equiv 3\ (\mathrm{mod.}4)}$ et posons $n = 4m + 3$. Posant pour $1 \leq j \leq m$, $\varepsilon_{2j-1} = ae_{4j-3} + be_{4j-2} + ce_{4j-1}$; $\varepsilon_{2j} = -be_{4j-3} + ae_{4j-2} + e_{4j}$ et $\varepsilon_{2m+1} = ae_{4m+1} + be_{4m+2} + e_{4m+3}$, on voit comme ci-dessus que

$$V_o = \bigoplus_{j=1}^{m} (Q_p \varepsilon_{2j-1} \oplus Q_p \varepsilon_{2j}) \text{ est totalement isotrope.}$$

Mais $< \varepsilon_{2j-1}, \varepsilon_{2m+1} > = 0 = < \varepsilon_{2j}, \varepsilon_{2m+1} >$ et $< \varepsilon_{2m+1}, \varepsilon_{2m+1} > = a^2 + b^2 + 1 = 0$; il vient que $V = V_0 \oplus Q_p \varepsilon_{2m+1}$ est totalement isotrope de dimension

$$2m + 1 = [\frac{4m+3}{2}] = [\frac{n}{2}] ; \text{ainsi } \upsilon = [\frac{m}{2}] = 2m + 1 .$$

Avec b), c), d), e) on a donc démontré (ii).

f) Supposons <u>$n \equiv 2 \pmod{4}$</u> et posons $n = 4m + 2$. Soient comme ci-dessus $\varepsilon_{2j-1} = a e_{4j-3} + b e_{4j-2} + e_{4j-1}$ et $\varepsilon_{2j} = -b e_{4j-3} + a e_{4j-2} + e_{4j}$, $1 \le j \le m$.

Le sous-espace $V = \bigoplus_{j=1}^{m} (\mathbf{Q}_p \varepsilon_{2j-1} \oplus \mathbf{Q}_p \varepsilon_{2j})$ de $E = \mathbf{Q}_p^n$ est totalement isotrope.

Soit $x = \sum_{\ell=1}^{n} x_\ell e_\ell \in E$ un vecteur isotrope, orthogonal à V;

on a $\sum_{\ell=1}^{n} x_\ell^2 = 0$ et $<x, V_j> = 0$ où $V_j = \mathbf{Q}_p \varepsilon_{2j-1} \oplus \mathbf{Q}_p \varepsilon_{2j}$, $1 \le j \le m$.

Mais si $<x, \varepsilon_{2j-1}> = a x_{4j-3} + b x_{4j-2} + x_{4j-1} = 0$ et $<x, \varepsilon_{2j}> = -b x_{4j-3} + a x_{4j-2} + x_{4j} = 0$, on a $x_{4j-1} = -a x_{4j-3} - b x_{4j-2}$ et $x_{4j} = b x_{4j-3} - a x_{4j-2}$.

$$\text{Alors } \sum_{\ell=1}^{n} x_\ell^2 = \sum_{\ell=1}^{m} (x_{4j-3}^2 + x_{4j-2}^2 + x_{4j-1}^2 + x_{4j}^2) + x_{4m+1}^2 + x_{4m+2}^2 = 0$$

avec pour $1 \le j \le m$, $x_{4j-3}^2 + x_{4j-3}^2 + x_{4j-2}^2 + x_{4j-2}^2 + x_{4j}^2 =$

$$= x_{4j-3}^2 + x_{4j-2}^2 + a^2 x_{4j-3}^2 + 2ab\ x_{4j-3} + b^2\ x_{4j-2}^2 +$$

$$+ b^2 x_{4j-3}^2 - 2ab\ x_{4j-3}\ x_{4j-2} + a^2\ x_{4j-2}^2 = (a^2 + b^2 + 1)(x_{4j-3}^2 + x_{4j-2}^4) = 0.$$

Ainsi $\sum_{\ell=1}^{n} x_\ell^2 = 0 + x_{4m+1}^2 + x_{4m+2}^2 = 0$ et comme $i \notin \mathbf{Q}_p$, on a $x_{4m+1} = x_{4m+2} = 0$.

Puisque $x_{4j-1} = -a x_{4j-3} - b x_{4j-2}$ et $x_{4j} = b x_{4j-3} - a x_{4j-2}$, on a $x_{4j-3} = a x_{4j-1} - b x_{4j}$ et $x_{4j-2} = b x_{4j-1} + a x_{4j}$. D'où $x_{4j-3} e_{4j-3} + x_{4j-2} e_{4j-2} + x_{4j-1} e_{4j-1} + x_{4j} e_{4j} = (a x_{4j-1} - b x_{4j}) e_{4j-3} + (b x_{4j-1} + a x_{4j}) e_{4j-2} + x_{4j-1} e_{4j-1} + x_{4j} e_{4j} = x_{4j-1} (a e_{4j-3} + b e_{4j-2} + e_{4j-1}) + x_{4j}(-b e_{4j-3} + a e_{4j-2} + e_{4j}) = x_{4j-1}\ \varepsilon_{2j-1} + x_{4j}\ \varepsilon_{2j}$. Ainsi

$$x = \sum_{j=1}^{m} (x_{4j-3} e_{4j-3} + x_{4j-2} e_{4j-2} + x_{4j-1} e_{4j-1} + x_{4j} e_{4j}) =$$

$= \sum_{j=1}^{m} x_{4j-1} \varepsilon_{2j-1} + x_{4j}\ \varepsilon e_j \in V$. Par suite $V = \bigoplus_{j=1}^{m} (\mathbf{Q}_p\ \varepsilon_{2j-1} \oplus \mathbf{Q}_p \varepsilon_{2j})$ est un

sous–espace isotrope maximal de E et $\upsilon = 2m = 2m+1-1 = \left[\frac{n}{2}\right] - 1$.
Ce qui démontre (iii) .

Remarque 3 : $i \notin \mathbf{Q}_2$.
La forme quadratique standard sur $\mathbf{Q}_2^n$ *a pour indice* $\upsilon = 0$ *lorsque* $1 \leq n \leq 4$.

Si $n \geq 5$ *on sait que toute forme quadratique sur* $\mathbf{Q}_2^n$ *est d'indice* $\upsilon \geq 1$. [Ceci est vrai pour tout p – c.f. [5]] .

En fait posant $n = 8m+s$, $0 \leq s \leq 7$, *on a*
$\upsilon = 4m$ *lorsque* $0 \leq s \leq 4$.
$\upsilon = 4m+t$ *lorsque* $s = 4+t$ $(1 \leq t \leq 3)$.

N.B.
i) Soit K un corps de niveau 1 ou 2 (resp.4) (c.f. III-2. b)) alors l'indice de forme quadratique standard sur K^n est donné par la Proposition 1(i) ou (ii) et (iii) (resp. la Remarque 3).On peut de la même manière calculer l'indice de la forme quadratique standard pour tout corps de niveau 2^r, $r \geq 0$.
ii) Appliquant la Proposition 1 et la Remarque 3 , on obtient une description de la structure de l'algèbre de Clifford de l'espace quadratique standard $(\mathbf{Q}_p^n, q)$.

II - Matrices orthogonales pour la forme quadratique standard

Dans la suite K est toujours un corps de caractéristique $\neq 2$; $E = K^n$ est muni du produit scalaire $<x,y> = \sum_{j=1}^{n} x_j y_j$ et $q(x) = \sum_{j=1}^{n} x_j^2$; $u \in \mathrm{Mat}_n(K)$ est orthogonale c'est-à-dire $<u(x), u(y)> = <x,y>$, $(x,y \in E)$ ou encore $q(u(x)) = q(x)$, $x \in E$.

II-1. *Le polynôme caractéristique d'une matrice orthogonale*

On a vu que si $u \in \mathrm{Mat}_n(K)$ est une matrice orthogonale, le polynôme caractéristique P_u de u est tel que $P_u(X) = \text{dét}\, u^{-1} (-1)^n X^n P_u(X^{-1})$. Donc si λ est une racine de P_u, alors λ^{-1} est une racine de P_u . Soit $(\lambda_j)_{j \in J}$ l'ensemble des racines de P_u

distinctes de ± 1 ; on a card $J = 2m \leq n$ et $(\lambda_j)_{j \in J} = \{\lambda_i , 1 \leq j \leq m\} \cup \{\lambda_j^{-1} , 1 \leq j \leq m\}$;

alors $P_u(X) = (-1)^n (X-1)^r (X+1)^s \prod_{j=1}^{m} (X-\lambda_j)^{t_j} (X-\lambda_j^{-1})^{t_j}$;

dét $u = P_u(0) = (-1)^{n+r}$. De plus si $P_u(X) = \sum_{\ell=0}^{n} a_\ell X^\ell$; on a $a_\ell = (-1)^n a_{n-\ell}$ dét u,

$1 \leq \ell \leq n-1$. En particulier si $n = 2n'$, $P_u(X) = X^{2n'} + \sum_{\ell=1}^{n'-1} a_\ell (X^\ell + \text{dét}\, u\, X^{2n'-\ell}) + \text{dét}\, u$

et si $n = 2n'+1$, $P_u(X) = -X^{2n'+1} + \sum_{\ell=1}^{n'} a_\ell (X^\ell - \text{dét}\, u\, X^{2n'+1-\ell}) + \text{dét}\, u$.

Remarque 4 :

Si K *est un corps ordonné , la forme quadratique standard sur* K^n *est d'indice* $\upsilon = 0$. *Plongeant* K *dans un corps ordonné maximal* K_0 *l'extension* $L = K_0[i]$ *est algébriquement close. On montre comme pour* $\mathbb{R}$ *et* $\mathbb{C}$ *que toute matrice orthogonale* $u \in Mat_n(K)$ *pour la forme quadratique standard est diagonalisable sur* L.

Si $\lambda \in K$ est une valeur propre de $u \in Mat_n(K)$, on note $E(\lambda)$ l'espace des vecteurs propres dans $E = K^n$ associés à λ.

Lemme 2 :

Soit $u \in Mat_n(K)$ *une matrice orthogonale pour la forme quadratique standard* q *sur* $E = K^n$ *et ayant toutes ses valeurs propres dans* K.

Si $\left(\lambda_j , \lambda_j^{-1}\right) 1 \leq j \leq m$ *est l'ensemble des valeurs propres de* u *distinctes de* ± 1 *alors le sous-espace* $E^+(m) = \bigoplus_{j=1}^{m} E(\lambda_j)$ *de* E *est totalement isotrope.*

Soit λ une valeur propre de u distincte de ± 1 ; si $x \in E(\lambda)$, on a $u(x) = \lambda x$ et $q(u(x)) = \lambda^2 q(x) = q(x)$; comme $\lambda^2 \neq 1$, on a $q(x) = 0$. Ainsi pour $x,y \in E(\lambda)$, on a $< x,y > = \frac{1}{2}(q(x+y) - q(x) - q(y)) = 0$ c'est-à-dire $E(\lambda) \subset E(\lambda)^{\perp}$. D'autre part si μ est une autre valeur propre de u distincte de ± 1 et de λ^{-1}, on a pour $x \in E(\lambda)$ et $y \in E(\mu)$, $< u(x), u(y) > = \lambda\mu < x,y > = < x,y >$, d'où $< x,y > = 0$ car $\lambda\mu \neq 1$, c'est-à-dire $E(\mu) \perp E(\lambda)$.

En conclusion $E^+(m) = \bigoplus_{j=1}^{m} E(\lambda_j)$ somme directe orthogonale de sous-espaces totalement isotropes est isotrope $\square$.

<u>Remarque 5</u> :

(i) *De la même manière* $E^-(m) = \bigoplus_{j=1}^{m} E(\lambda_j^{-1})$ *est un sous-espace totalement isotrope de* E.

(ii) $E^+(m) \oplus E^-(m)$ *est un sous-espace de* E *stable par* u.

(iii) *Soient* $1 \leq \ell \neq j \leq m$; *on a* $E(\lambda_j) \subset E(\lambda_\ell^{-1})^{\perp}$ *et* $E(\lambda_\ell^{-1}) \subset E(\lambda_j)^{\perp}$.

(iv) $u(E(\lambda_j)) = E(\lambda_j)$ *et* $u(E(\lambda_j)^{\perp}) = E(\lambda_j)^{\perp}$.

<u>N.B.</u>

Puisque $P_u(X) = (X-1)^r (X+1)^s \prod_{j=1}^{m} (X - \lambda_j)^{t_j} (X - \lambda_j^{-1})^{t_j}$, de façon classique u est diagonalisable si et seulement si $n = r + s + 2 \sum_{j=1}^{m} t_j$; alors $E = E(-1) \oplus E(1) \oplus E^+(m) \oplus E^-(m)$.

II - 2- *Exemples de matrices orthogonales non diagonalisables*

Rappelons (c.f. [2]) que si E est un K-espace vectoriel de dimension finie n muni d'une forme bilinéaire symétrique non dégénérée f (K de caractéristique $\neq 2$) et si v est

l'indice de f, considérant V et W deux sous-espaces isotropes maximaux distincts et posant $U = (V \oplus W)^{\perp}$, on dit qu'une transformation orthogonale de la forme $u(x) = x + v(x)$ est *singulière* si l'on a $u(x) = x$ pour $x \in U + V$. Alors puisque $f(u(x), u(y)) = f(x,y)$, on a ① $f(x, v(y)) + f(v(x), y) + f(v(x), v(y)) = 0$ pour $x,y \in E$.
Mais $U \oplus V \subset \ker v$; ainsi avec ① on obtient $v(E) \subset V$; car $(U \oplus V)^{\perp} = V$. On a alors $f(v(x), v(y)) = 0$ pour $x,y \in E$ et ① devient $f(x, v(y)) + f(x, v^*(y)) + f(v(x), v(y)) = f(x, (v + v^*)(y)) = 0$ pour tous $x,y \in E$, c'est-à-dire $v + v^* = 0$ ou encore $v^* = -v$.

Comme $u^{-1} = u^*$, on a pour $x \in U \oplus V$, $u^*(x) = u^{-1}(x) = x = x + v^*(x)$; donc $U \oplus V \subset \ker v^*$ et u^* est un opérateur orthogonal singulier tel que $u^*(x) = x$ pour $x \in U \oplus V$; on a $v^*(E) \subset V$.

Puisque $E = V \oplus W \oplus U$ avec $V \perp U$, il existe une base $(\varepsilon_j)_{1 \le j \le n}$ de E telle que $(\varepsilon_j)_{1 \le j \le \upsilon} \subset V$; $(\varepsilon_j)_{\upsilon+1 \le j \le 2\upsilon} \subset W$; $(\varepsilon_j)_{2\upsilon+1 \le j \le n} \subset U$ et $f(\varepsilon_\ell, \varepsilon_{j+\upsilon}) = \delta_{\ell,j}$ pour $1 \le \ell, j \le \upsilon$. Il vient que $u(\varepsilon_j) = \varepsilon_j$ pour

$j \in [1,\upsilon] \cup [2\upsilon+1, n]$ et $u(\varepsilon_{j+\upsilon}) = \varepsilon_{j+\upsilon} + v(\varepsilon_{j+\upsilon}) = \varepsilon_{j+\upsilon} + \sum_{\ell=1}^{\upsilon} \alpha_{\ell, j+\upsilon}\, \varepsilon_\ell$, $1 \le j \le \upsilon$

c'est-à-dire $v(\varepsilon_{j+\upsilon}) = \sum_{\ell=1}^{\upsilon} \alpha_{\ell,j+\upsilon}\, \varepsilon_\ell$, $1 \le j \le \upsilon$. De la même manière

$$v^*(\varepsilon_{j+\upsilon}) = \sum_{\ell=1}^{\upsilon} \beta_{\ell,j+\upsilon}\, \varepsilon_\ell \quad , \ 1 \le j \le \upsilon .$$

On obtient $f(v(\varepsilon_{j+\upsilon}), \varepsilon_{\ell+\upsilon}) = \sum_{k=1}^{\upsilon} \alpha_{k,j+\upsilon} f(\varepsilon_k, \varepsilon_{\ell+\upsilon}) = \sum_{k=1}^{\upsilon} \alpha_{k,j+\upsilon}\delta_{k,\ell} =$

$$= \alpha_{\ell,j+\upsilon} = f(\varepsilon_{j+\upsilon}, v^*(\varepsilon_{\ell+\upsilon})) = \sum_{k=1}^{\upsilon} \beta_{k,j+\upsilon}\delta_{j,k} = \beta_{j,\ell+\upsilon} \text{ d'où } \beta_{j,\ell+\upsilon} = \alpha_{\ell,j+\upsilon}.$$

Comme $v = -v^*$ on a $\beta_{j,\ell+\upsilon} = -\alpha_{\ell,j+\upsilon}$, $1 \le \ell, j \le \upsilon$.
Posons $\gamma_{\ell,j} = \alpha_{\ell,j+\upsilon}$, $1 \le \ell, j \le \upsilon$, on a $\gamma_{\ell,j} = -\gamma_{j,\ell}$ et la matrice $S = (\gamma_{\ell,j})_{1 \le \ell,j \le \upsilon}$ est antisymétrique : ${}^tS = -S$. <u>En conclusion</u>, la matrice de u dans la base $(\varepsilon_j)_{1 \le j \le n}$ est de la forme

$$T = \begin{pmatrix} I_\upsilon & S & 0 \\ 0 & I_\upsilon & 0 \\ 0 & 0 & I_{n-2\upsilon} \end{pmatrix}$$ avec $S = -{}^tS$. Il devient clair que l'ensemble des transformations orthogonales singulières laissant invariants les éléments de $U \oplus V$ est un groupe abélien isomorphe à $K^{\frac{\upsilon(\upsilon-1)}{2}}$.

Exemples :

a) $n = 2$ ou $n = 3$; on a $\upsilon \leq \left[\frac{n}{2}\right] = 1$. L'application identique est la seule transformation orthogonale singulière. C'est clair si $\upsilon = 0$ et si $\upsilon = 1$, on a $S = (\gamma)$ avec ${}^tS = \gamma = -S = -\gamma$, donc $\gamma = 0$.

b) $n = 4$; on a $\upsilon \leq 2$.
Si $\upsilon = 0$ ou 1, toute transformation orthogonale singulière est l'identité.
Si $\upsilon = 2$, les transformations orthogonales singulières sont de la forme

$$T = \begin{pmatrix} I_2 & S \\ 0 & I_2 \end{pmatrix} \text{ où } S = \begin{pmatrix} 0 & -\gamma \\ \gamma & 0 \end{pmatrix}, \ \gamma \in K.$$

Lemme 3 :

Soit $u = id_E + v$ *une transformation orthogonale singulière laissant invariants les éléments de* $U \oplus V$. *Alors* 1 *est l'unique valeur propre de* u ; *on a* $U \oplus V \subset E(1)$ *et si* $u \neq id_E$, u *n'est pas diagonalisable.*

Supposons $\lambda \neq 1$ valeur propre de u ; il existe $x \in E$, $x \neq 0$ tel que $u(x) = \lambda x = x + v(x)$; d'où $(\lambda - 1)x = v(x) \in V$ et $x \in V$; on obtient alors $u(x) = x = \lambda x$, ce qui absurde. Le seul sous-espace propre de u étant $E(1) = \ker(u - id_E) = \ker v$; si $u \neq id_E$, on $v \neq 0$ avec $U \oplus V \subset \ker v = E(1) \neq E$ et u n'est pas diagonalisable ; de plus $n - \upsilon \leq \dim E(1) < n$.

Application $K = \mathbf{Q}_p$

On a vu – Proposition 1 – que la forme quadratique standard sur $E = Q_p^n$ a pour indice $\upsilon = \left[\frac{n}{2}\right]$ si $p \equiv 1 \pmod 4$ ou si $p \equiv 3 \pmod 4$ avec $n \not\equiv 2 \pmod 4$ et $\upsilon = \left[\frac{n}{2}\right] - 1$ si $p \equiv 3 \pmod 4$ avec $n \equiv 2 \pmod 4$.

a) Supposons $\mathbf{p \equiv 1 \pmod 4}$

(i) Si **n est pair**, on a $n = 2\upsilon$. Soit $V = \bigoplus_{j=1}^{\upsilon} Q_p \varepsilon_j$ un sous–espace totalement isotrope maximal ; $W = \bigoplus_{j=1}^{\upsilon} Q_p \varepsilon_{j+\upsilon}$ un autre sous–espace totalement isotrope où $(\varepsilon_{j+\upsilon})_{1 \le j \le \upsilon}$ est une base de W conjuguée à $(\varepsilon_j)_{1 \le j \le n}$; c'est-à-dire $< \varepsilon_\ell , \varepsilon_{j+\upsilon} > = \delta_{\ell,j}$. On a $E = V \oplus W$. Considérons $S = (\gamma_{\ell,j})_{1 \le \ell,j \le \upsilon} \subset \mathbf{Q}_p$ telle que $\gamma_{\ell,j} = -\gamma_{j,\ell}$; $1 \le j, \ell \le \upsilon$. L'opérateur u défini par $u(\varepsilon_j) = \varepsilon_j$, $1 \le j \le \upsilon$ et $u(\varepsilon_{j+\upsilon}) = \varepsilon_{j+\upsilon} + \sum_{\ell=1}^{\upsilon} \gamma_{\ell,j}\, \varepsilon_\ell$, $1 \le j \le \upsilon$, est une transformation orthogonale singulière de E. La matrice correspondante $u \in \mathrm{Mat}_n(\mathbf{Q}_p)$, dans la base canonique de E, est une matrice **orthogonale non diagonalisable** dès que $S \neq 0$.

<u>N.B.</u> (1) On a $u = P^{-1} T P$ où P est la matrice de passage de la base $(\varepsilon_j)_{1 \le 1 \le n}$ à la base canonique $(e_j)_{1 \le j \le n}$ et $T = \begin{pmatrix} I_\upsilon & S \\ 0 & I_\upsilon \end{pmatrix}$.

(2) La matrice T de u dans la base $(\varepsilon_j)_{1 \le j \le n}$ n'est pas une matrice orthogonale pour $S \neq 0$. □

(ii) Si **n est impair**, on a $n = 2\upsilon + 1$. Considérons, avec les notations de a) (i), $\varepsilon_n \in E$, $\varepsilon_n \perp V \oplus W$; on a $E = V \oplus W \oplus \mathbf{Q}_p\, \varepsilon_n$; on définit alors une transformation orthogonale singulière u en posant $u(\varepsilon_j) = \varepsilon_j$, $1 \le j \le \upsilon$ ou $2\upsilon+1 \le j \le n$;

$$u(\varepsilon_{j+\upsilon}) = \varepsilon_{j+\upsilon} + \sum_{\ell=1}^{\upsilon} \gamma_{\ell,j}\, \varepsilon_\ell \, , \; 1 \le j \le \upsilon$$

et $u(\varepsilon_n) = \varepsilon_n$. La matrice correspondante $u \in \mathrm{Mat}_n(\mathbf{Q}_p)$ dans la base canonique de E est une **matrice orthogonale non diagonalisable** dès que $S \neq 0$.

$$\text{On a} \quad u = P^{-1} \begin{pmatrix} I_\upsilon & S & 0 \\ 0 & I_\upsilon & 0 \\ 0 & 0 & 1 \end{pmatrix} P \, .$$

b) Supposons **$p \equiv 3$ (mod. 4) et $n \not\equiv 2$ (mod. 4)** .

Si n est pair, on a $n = 2\upsilon$; on se trouve dans le cas a) - (i) . Si n est impair, on a $n = 2\upsilon + 1$ et on se trouve dans un cas analogue à a) - (ii) .

c) Supposons **$p \equiv 3$ (mod. 4) et $n \equiv 2$ (mod. 4).**

On a $n = 2\upsilon + 2$. Considérons , comme en a) deux sous-espaces totalement isotropes maximaux V et W ; Soit $(\varepsilon_{n-1}, \varepsilon_n) \subset E$, libre telle que $\varepsilon_{n-1} \perp V \oplus W$ et $\varepsilon_n \perp V \oplus W$. L'opérateur u défini par $u(\varepsilon_j) = \varepsilon_j$, $1 \le j \le \upsilon$ ou $2\upsilon + 1 \le j \le n$;

$u(\varepsilon_{j+\upsilon}) = \varepsilon_{j+\upsilon} + \sum_{\ell=1}^{\upsilon} \gamma_{\ell,j}\varepsilon_\ell$, $1 \le j \le \upsilon$ (notations de a)) ; $u(\varepsilon_{n-1}) = \varepsilon_{n-1}$ et $u(\varepsilon_n) = \varepsilon_n$, est une transformation orthogonale singulière. La matrice correspondante $u \in \mathrm{Mat}_n(\mathbf{Q}_p)$ est une **matrice orthogonale non diagonalisable** dès que $S \neq 0$.

$$\text{On a} \quad u = P^{-1} \begin{pmatrix} I_\upsilon & S & 0 & 0 \\ 0 & I_\upsilon & 0 & 0 \\ 0 & 0 & 1 & 0 \\ & & 0 & 1 \end{pmatrix} P \, .$$

On a donc démontré :

<u>Proposition 2</u> :

Considérons le corps p-adique $\mathbf{Q}_p$, $p \neq 2$.

Pour tout entier $n \ge 4$, *il existe des matrices orthogonales d'ordre* n *à coefficients dans* $\mathbf{Q}_p$ *qui ne sont pas diagonalisables. On peut prendre les matrices dans la base canonique de* $\mathbf{Q}_p^n$ *de transformations orthogonales singulières.*

<u>N.B.</u> Les matrices orthogonales ci-dessus ne sont orthogonalisables sur aucune extension finie de $\mathbf{Q}_p$.

<u>Remarque 6</u> :

(i) *Si* $p = 2$, *il existe pour tout entier* $n \geq 5$ *des matrices orthogonales à coefficients dans* $\mathbb{Q}_2$ *d'ordre* n *non diagonalisables.*

(ii) *Soit* K *un corps de niveau* 2^r, $r \geq 0$, *et de caractéristique* $\neq 2$ *pour tout entier* $n \geq 1 + 2^r$, *il existe des matrices orthogonales d'ordre* n *non diagonabilisables.*

<u>N.B.</u>

Les coefficients des matrices orthogonales de la Proposition 2 ne peuvent être tous rationnels. En effet, soit $u \in \mathrm{Mat}_n(\mathbb{Q})$ une matrice orthogonale pour la forme quadratique standard ; alors u est diagonalisable sur $\mathbb{C}$. Les racines du polynôme caractéristique de u sont des nombres algébriques et les coordonnées de ses vecteurs propres sont donc des nombres algébriques. Plongeant la clôture algébrique de $\mathbb{Q}$ dans celle de $\mathbb{Q}_p$, on voit que toute matrice orthogonale $u \in \mathrm{Mat}_n(\mathbb{Q}_p)$ à coefficients **rationnels** est diagonalisable sur une extension finie de $\mathbb{Q}_p$.

III - Exemples de matrices symétrique p-adiques non diagonalisables

III-1. $n = 2$.

Soit $u = \begin{pmatrix} a & b \\ b & d \end{pmatrix} \in \mathrm{Mat}_2(\mathbb{Q}_p)$ symétrique. On a

$$P_u(X) = \text{dét}(u - X\, I_2) = (a-X)(d-X) - b^2 = X^2 - (a+d)X + ad - b^2 = \left(X - \frac{a+d}{2}\right)^2 - \frac{\Delta}{4}$$

où $\Delta = (a-d)^2 + 4b^2$.

a) Supposons $\mathbf{p \equiv 3 \ (mod.\, 4)}$ ou $\mathbf{p = 2}$; alors $i \notin \mathbb{Q}_p$.

(i) Ou bien $\Delta = (a-d)^2 + 4b^2 = 0$ et comme $i \notin \mathbb{Q}_p$ ceci équivaut à $a = d$ et $b = 0$; on a $u = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ matrice diagonale.

(ii) ou bien $\Delta = (a-d)^2 + 4\,b^2 \neq 0$ ce qui équivaut à $b \neq 0$ ou $a \neq d$. Le polynôme caractéristique P_u de u a deux racines distinctes dans $\mathbf{Q}_p(\sqrt{\Delta}) = K_p$ et u est diagonalisable sur K_p .

b) Supposons **$p \equiv 1$ (mod. 4)** ; alors $i = \sqrt{-1} \in \mathbf{Q}_p$.

(i) Ou bien $\boldsymbol{\Delta = (a-d)^2 + 4\,b^2 \neq 0}$; alors u est diaganalisable sur $K_p = \mathbf{Q}_p(\sqrt{\Delta})$.

(ii) Ou bien $\Delta = (a-d)^2 + 4\,b^2 = 0$ ce qui équivaut à $b = \pm \frac{i}{2}(a-d)$; alors si $a = d$ on a $b = 0$ et $u = a\,I_2$;

sinon $a-d \neq 0$ et $u = \begin{pmatrix} a & i\frac{(a-d)}{2} \\ i\frac{(a-d)}{2} & d \end{pmatrix}$ $\left(\text{resp. } u = \begin{pmatrix} a & -i\frac{(a-d)}{2} \\ -i\frac{(a-d)}{2} & d \end{pmatrix}\right)$

a pour unique valeur propre $\lambda = \dfrac{a+d}{2}$.

Ainsi, on a $u - \lambda I_2 = \dfrac{a-d}{2}\begin{pmatrix} 1 & i \\ i & -1 \end{pmatrix}\left(\text{resp. } u = \dfrac{a-d}{2}\begin{pmatrix} 1 & -i \\ -i & -1 \end{pmatrix}\right)$ avec $u - \lambda I_2$ de rang 1. Le sous-espace propre associé à λ est donc de dimension 1 et la matrice symétrique u n'est pas diagonalisable. En fait u est semblable à $\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$ où $\lambda = \dfrac{a+d}{2}$.

<u>En résumé</u> :

Si **$p \not\equiv 1$ (mod.4)** , toute matrice symétrique d'ordre 2 à coefficients dans $\mathbf{Q}_p$ est diagonalisable sur une extension de $\mathbf{Q}_p$.

Si **$p \equiv 1$ (mod.4)** , toute matrice symétrique $u = \begin{pmatrix} a & b \\ b & d \end{pmatrix}$ à coefficients dans $\mathbf{Q}_p$ est diagonalisable sur une extension de $\mathbf{Q}_p$ **sauf** lorsque $b = \pm i\,\dfrac{(a-d)}{2}$.

III-2. *Un exercice classique*.

Soit K un corps.

Considérons $a_1, \dots, a_n \in K$ et posons $u = (a_\ell a_j)_{1 \leq \ell, j \leq n} \in Mat_n(K)$.

Il est clair que u est une matrice carrée symétrique de trace $tr\, u = \sum_{j=1}^{n} a_j^2$. Tout vecteur ligne de u est proportionnel au vecteur $(a_1, a_2, \dots, a_n)$. Il vient que u est de rang 1. Ainsi le sous-espace propre de u associé à la valeur propre $\lambda = 0$ à savoir $E(0) = \ker u$ est de dimension n–1. Mais le polynôme caractéristique P_u de u est donné par
$P_u(X) = (-1)^n X^n + (-1)^{n-1} tr\, u X^{n-1} + \dots + \det u.$
Puisque $\lambda = 0$ est un zéro d'ordre $\geq n-1$ de P_u, on a $P_u(X) = (-1)^n X^{n-1}(\alpha X + \beta)$; ainsi $\alpha = 1$, $\beta = -tr\, u$ et

$$P_u(X) = (-1)^n X^{n-1}(X - tr\, u) = (-1)^n X^{n-1}\left(X - \sum_{j=1}^{n} a_j^2\right).$$

a) Si K est un **corps ordonné** et si l'un des a_j est non nul, $\lambda = \sum_{j=1}^{n} a_j^2 \neq 0$ est un zéro simple de P_u. Alors $K^n = E(0) \oplus E(\lambda)$ et u est diagonalisable. Ceci est un cas particulier du fait que toute matrice symétrique à coefficients dans un corps ordonné est diagonalisable sur une extension ordonnée de K (plonger K dans un corps ordonné maximal et raisonner comme pour **R**.)

b) Si K est un corps **non ordonné** ; rappelons que l'on appelle *niveau de* K, le plus petit entier s tel que $-1 = \sum_{j=1}^{s} a_j^2$ où $a_j \in K$, $a_j \neq 0$. On sait (c.f. 4]) que $s = 2^r$, $r \geq 0$. Alors pour tout entier $n \geq 1 + 2^r$, il existe $a_1, \dots, a_n \in K$ non tous nuls tels que $\sum_{j=1}^{n} a_j^2 = 0$. Dans ces conditions, on a $P_u(X) = (-1)^n X^n$; comme $E(0) = \ker u$ est de dimension n–1, u n'est pas diagonalisable.

c) Les corps $\mathbf{Q}_p$ sont de **niveau** 1 si $p \equiv 1 \pmod{4}$ et de **niveau** 2, si $p \equiv 3 \pmod{4}$ (c.f. démonstration Proposition 1). Le corps $\mathbf{Q}_2$ est de **niveau** 4. Ainsi la forme quadratique standard sur $\mathbf{Q}_p^n$ admet des vecteurs isotropes non nuls pour $n \geq 2$ lorsque $p \equiv 1 \pmod{4}$; pour $n \geq 3$ lorsque $p \equiv 3 \pmod{4}$ et pour $n \geq 5$ lorsque $p = 2$.

Soit donc $a = \sum_{j=1}^{n} a_j e_j \in \mathbf{Q}_p^n$ un vecteur isotrope non nul ; on a $\sum_{j=1}^{n} a_j^2 = 0$ et la matrice symétrique non nulle $u = (a_\ell a_j)_{1 \leq \ell, j \leq n}$ n'est pas diagonalisable d'après b).

On a donc démontré :

Proposition 3.

Il existe des matrices carrées symétriques d'ordre n *à coefficients dans* $\mathbf{Q}_p$ *non diagonalisables pour* $n \geq 2$ *lorsque* $p \equiv 1 \pmod{4}$; *pour* $n \geq 3$ *lorsque* $p \equiv 3 \pmod{4}$ *et pour* $n \geq 5$ *lorsque* $p = 2$.

N.B Les matrices symétriques ci-dessus ne sont diagonalisables sur aucune extension de $\mathbf{Q}_p$.

III-3. *Scholie*

Soit K un corps ordonné maximal ; tout comme sur $\mathbb{R}$; toute matrice carrée symétrique u d'ordre n à coefficients dans K est diagonalisable et l'espace vectoriel K^n contient une base de vecteurs propres de u deux à deux orthogonaux.

Si K est un corps non ordonné et si $u \in \mathrm{Mat}_n(K)$ symétrique est diagonalisable dans une extension finie L de K, l'espace L^n muni du produit scalaire standard contient-il une base de vecteurs propres de u deux à deux orthogonaux ? On a bien sûr une réponse affirmative quand les valeurs propres sont simples :

Remarque 7

Soit K *un corps,* $u \in \mathrm{Mat}_n(K)$ *une matrice symétrique ayant toutes ses valeurs propres distinctes dans une extension (finie)* L *de* K. *Alors il existe dans* L^n *muni du produit scalaire standard une base orthogonale formée de vecteurs propres de* u ; *de plus tout vecteur propre de* u *est non isotrope*.

En effet si $\lambda \neq \mu$ sont deux valeurs propres de u, on a $E(\lambda) \perp E(\mu)$. Les valeurs propres λ_j, $1 \leq j \leq n$ étant distinctes, on a $\dim E(\lambda_j) = 1$; si $\{\varepsilon_j\}$

est une base de $E(\lambda_j)$, on a $L^n = \bigoplus_{j=1}^{n} L\,\varepsilon_j$ avec $<\varepsilon_\ell, \varepsilon_j> = 0$ si $\ell \neq j$. La matrice $B = (b_{\ell,j})_{1 \leq \ell, j \leq n}$ du produit scalaire de L^n dans la base orthogonale $(\varepsilon_j)_{1 \leq j \leq n}$ est telle que $b_{\ell,j} = 0$ si $\ell \neq j$ et $b_{jj} = <\varepsilon_j, \varepsilon_j>$. Comme B est inversible, on a
$<\varepsilon_j, \varepsilon_j> \neq 0$.

<u>Remarque 8</u>

Soit K *un corps non ordonné de niveau* 2^r, $r \geq 0$. *Pour tout entier* $n \geq 1+2^r$ *la forme quadratique standard sur* K^n *est d'indice* ≥ 1. *Ainsi, on a des énoncés semblables aux* Propositions 2 *et* 3.

Il vient que si pour tout entier $n \geq 1$, *toute matrice symétrique d'ordre* n *est diagonalisable sur un sur-corps de* K, *alors* K *est ordonné* ; *la réciproque est vraie (plonger* K *dans un corps ordonné maximal et raisonner comme pour* $\mathbb{R}$).

Ceci est une réponse à la question posée dans [3].

<u>Question</u>

Soit K un corps non ordonné de niveau 2^r. Soit $n \leq 2^r$; toute matrice symétyrique d'ordre n est-elle diagonalisable sur K ou sur une extension finie de K ?

Je remercie Alain Escassut d'avoir soulevé le problème traité dans cet article.

BIBLIOGRAPHIE

[1] R. DEHEUVELS : *Formes quadratiques et groupes classiques,* P.U.F. - Paris - 1981.

[2] J. DIEUDONNE : *Sur les groupes classiques* Hermann - Paris - 1973.

[3] S.H.FRIEDBERG : *Extending the principal axis theorem to fields other than* $\mathbb{R}$, Ann. Math. Monthly - vol 97, n°2 - 1990 - p. 147-149.

[4] P. RIBENBOIM : *L'arithmétique des corps,* Hermann - collection Méthodes - Paris - 1972.

[5] J.P. SERRE : *Cours d'arithmétique,* P.U.F. - Le Mathématicien - 1970.

BERTIN DIARRA

Département de Mathématiques Pures, U.F.R. Sciences Exactes et Naturelles, Complexe Scientifique des Cézeaux - 63177 AUBIERE CEDEX

Manuscrit reçu le 30 Octobre 1990.