Formes quadratiques

J. Le Borgne

Table des matières

1 Espaces quadratiques **1**
1.1 Définitions et premières propriétés 1
1.2 Orthogonalité et dualité 3

2 Classification **4**
2.1 Rang et discriminant 4
2.2 Bases orthogonales 5
2.3 Espaces quadratiques sur un corps algébriquement clos 6
2.4 Espaces quadratiques réels 7
2.5 Espaces quadratiques sur les corps finis 8

3 Groupe orthogonal d'une forme quadratique **8**
3.1 Théorème de Cartan-Dieudonné 9
3.2 Groupes orthogonaux réels 10
3.2.1 Les groupes $O(s,t)$ 10
3.2.2 Le groupe $O(3,1)$ et l'espace-temps de Minkowski (garanti sans théorème) . . . 10

4 Théorie de Witt **11**
4.1 Prolongement des isométries 11
4.2 Théorème de Witt 11

1 Espaces quadratiques

Soit K un corps de caractéristique différente de 2.

1.1 Définitions et premières propriétés

Définition 1. *Soit E un K-espace vectoriel. Une forme quadratique sur E est une application $q : E \to K$ telle que :*
- *pour tout $\lambda \in K$ et $x \in E$, $q(\lambda x) = \lambda^2 q(x)$,*
- *l'application $(x,y) \mapsto q(x+y) - q(x) - q(y)$ est une forme bilinéaire symétrique.*

Proposition 1. *Soit q une forme quadratique sur E, alors $b : (x,y) \mapsto \frac{1}{2}(q(x+y) - q(x) - q(y))$ est l'unique forme bilinéaire symétrique telle que pour tout $x \in E$, $b(x,x) = q(x)$. On l'appelle* forme polaire *de q.*

Exemple 1. *Si f, g sont des formes linéaires, fg est une forme quadratique dont la forme polaire est $(x,y) \mapsto \frac{1}{2}(f(x)g(y) + f(y)g(x))$. En particulier, le carré d'une forme linéaire est une forme quadratique, et donc une combinaison linéaire de carrés de formes linéaires est une forme quadratique.*

Définition 2. *On appelle* espace quadratique *sur K la donnée d'un couple (E,q) où E est un K-espace vectoriel et q est une forme quadratique sur E.*

Lemme 1 (Écriture en coordonnées)**.** *Soit (E,q) un espace quadratique de forme polaire b. Soit $(e_1, \ldots, e_n)$ une base de E. On note $x_i = e_i^*$ et $a_{ij} = b(e_i, e_j)$ pour $1 \leqslant i,j \leqslant n$. Alors on a $q = \sum_{1 \leqslant i,j \leqslant n} a_{ij} x_i x_j$.*

Démonstration. Soit $x \in E$, on note $\xi_i = x_i(x) = e_i^*(x)$. On a alors, par bilinéarité de b :

$$q(x) = b(x,x) = \sum_{1 \leqslant i,j \leqslant n} a_{ij}\xi_i\xi_j = \sum_{1 \leqslant i,j \leqslant n} a_{ij}x_i(x)x_j(x).$$

c.q.f.d.

Définition 3. *On dit que $x \in E$ est* isotrope *si $q(x) = 0$.*
Le cône isotrope de q, noté $I(q)$ est l'ensemble des vecteurs isotropes.
Le noyau de q, noté $N(q)$, est l'ensemble des $x \in E$ tels que pour tout $y \in E$, $b(x,y) = 0$.

Remarque 1. *On a toujours $N(q) \subset I(q)$, mais on n'a pas égalité en général. Par exemple, pour la forme quadratique $q(x) = e_1^*e_2^*$ en dimension 2, on a $I(q) = Ke_1 \cup Ke_2$ et $N(q) = \{0\}$.*

Remarque 2. *La restriction d'une forme quadratique à un sous-espace vectoriel est toujours une forme quadratique.*

Théorème 1. *Soit q une forme quadratique sur E de forme polaire b. L'application :*

$$\Phi \ : \left| \begin{array}{ccc} E & \to & E^* \\ x & \mapsto & \Phi_x \ : \left| \begin{array}{ccc} E & \to & K \\ y & \mapsto & b(x,y) \end{array} \right. \end{array} \right.$$

est bien définie et linéaire. Son noyau est $N(q)$.

Démonstration. Immédiat. *c.q.f.d.*

Corollaire 1. *Soit E un K-espace vectoriel de dimension finie. L'application Φ est un isomorphisme si et seulement si $N(q) = \{0\}$.*

Définition 4. *On dit que l'espace quadratique (E,q) est non dégénéré si $N(q) = \{0\}$. De manière équivalente, un espace quadratique est non dégénéré lorsque l'application Φ du théorème 1 est un isomorphisme.*

Lemme 2. *Soit (E,q) un espace quadratique de dimension finie, soit $\mathcal{B}$ une base de E et soit B^* sa base duale. Alors on a $Mat_{\mathcal{B},\mathcal{B}^*}(\Phi) = (b(e_i,e_j))$.*

Démonstration. Le résultat du calcul est immédiat. *c.q.f.d.*

La matrice M décrite dans le lemme 2 s'appelle la *matrice de la forme quadratique q dans la base $\mathcal{B}$*.

Définition 5. *Soient $(E,q),(E',q')$ des espaces quadratiques. Un morphisme d'espaces quadratiques est une application linéaire $u : E \to E'$ telle que $q' \circ u = q$. Un tel morphisme est un isomorphisme si c'est un isomorphisme d'espaces vectoriels.*

Remarque 3. *Cette définition présente un intérêt, car si u est linéaire et q' est une forme quadratique, alors $q' \circ u$ est une forme quadratique. Si b' est la forme polaire de q', alors la forme polaire de $q = q' \circ u$ est $b : (x,y) \mapsto b'(u(x),u(y))$.*

Exemple 2. *Soit K vu comme K-espace vectoriel de dimension 1. Les formes quadratiques sur K sont les applications de la forme $x \mapsto \lambda x^2$, avec $\lambda \in K$; on note (K,λ) l'espace quadratique associé à la forme quadratique $x \mapsto \lambda x^2$. Les applications linéaires sont les applications de la forme $x \mapsto ax$. Ainsi, un morphisme $(K,\lambda) \to (K,\mu)$ est une homothétie de rapport a, a vérifiant la relation $\mu a^2 = \lambda$. Ainsi, il existe un tel morphisme si et seulement si $\lambda = 0$ ou bien $\mu/\lambda \in (K^\times)^2$. En particulier, (K,λ) et (K,μ) sont isomorphes si et seulement si λ et μ ont la même classe dans $K/(K^\times)^2$.*

Exemple 3. *Soit $E = K^2$. On note $x_1 = e_1^*$ et $x_2 = e_2^*$, et on considère les formes quadratiques $q = x_1^2 - x_2^2$ et $q' = x_1x_2$. Alors, l'unique application linéaire u telle que $u(e_1) = e_1 + e_2$ et $u(e_2) = e_1 - e_2$ vérifie $q' \circ u = q$. Comme u est bijective, ces deux espaces quadratiques sont isomorphes.*

1.2 Orthogonalité et dualité

Définition 6. *Soit (E, q) un espace quadratique de forme polaire b. On dit que $x, y \in E$ sont orthogonaux si $b(x, y) = 0$.*
Si $A \subset E$, l'orthogonal de A est $A^\perp = \{y \in E \mid \forall x \in A, b(x, y) = 0\}$.

Exemple 4. *On a $E^\perp = N(q)$. Si F est un sous-espace vectoriel, le noyau de la restriction de q à F est $F \cap F^\perp$.*

Lemme 3. *Soit (E, q) un espace quadratique, et soit $\pi : E \to E/N(q)$ la projection canonique. La forme polaire b induit par passage au quotient une forme bilinéaire $\bar{b}$ sur $E/N(q)$ dont la forme quadratique associée $\bar{q} : E/N(q) \to K$ est un morphisme d'espaces quadratiques.*

Démonstration. L'existence de $\bar{b}$ est justifiée par deux applications successives de la propriété universelle du quotient. La forme quadratique $\bar{q}$ est alors bien définie, et vérifie bien $\bar{q} \circ \pi = q$: c'est un morphisme d'espaces quadratiques. Pour voir que $\bar{q}$ est non dégénérée, il suffit de montrer que $N(\bar{q}) = \{0\}$. Par définition, on a $\pi(x) \in N(\bar{q})$ si et seulement si pour tout $y \in E$, $b(\pi(x), \pi(y)) = 0$, c'est-à-dire si $b(x, y) = 0$. Ainsi, $\pi(x) \in N(\bar{q})$ si et seulement si $x \in N(q)$, autrement dit si $\pi(x) = 0$. Cela montre que $\bar{q}$ est non dégénérée. *c.q.f.d.*

Proposition 2. *Soit (E, q) un espace quadratique et soit $F \subset E$ un supplémentaire de $N(q)$ dans E. Alors le morphisme canonique $(E, q) \to (E/N(q), \bar{q})$ induit un isomorphisme d'espaces quadratiques $(F, q_{|F}) \to (E/N(q), \bar{q})$.*

Démonstration. Comme π est la projection canonique sur $E/N(q)$ et que F est un supplémentaire de $N(q)$, $\pi_{|F} : F \to E/N(q)$ est un isomorphisme. D'après le lemme 3, c'est aussi un morphisme d'espaces quadratiques. *c.q.f.d.*

Remarque 4. *Cette proposition montre que la classe d'isomorphisme de $(F, q_{|F})$ ne dépend pas du choix de F. La classe d'isomorphisme d'un espace quadratique est entièrement déterminée par (la dimension de) son noyau et la classe d'isomorphisme de n'importe quel supplémentaire du noyau.*

On rappelle que la notion d'orthogonalité est définie dans le cadre de la dualité : l'orthogonal A^0 (pour la dualité) d'une partie A de E est l'ensemble des formes linéaires φ qui s'annulent sur A.

Proposition 3. *Soient $A, B \subset E$, alors :*
- *A^0 est un sous-espace vectoriel de E^*,*
- *(Vect A)$^0 = A^0$,*
- *Si $A \subset B$, alors $B^0 \subset A^0$,*
- *$A^0 + B^0 \subset (A \cap B)^0$, $(A \cup B)^0 = A^0 \cap B^0$,*
- *Si E est de dimension finie, on a $\dim A^0 + \dim \mathit{Vect} A = \dim E$.*

Démonstration. Le seul point dont la vérification n'est pas immédiate est le dernier. Il suffit de le démontrer dans le cas où A est un sous-espace vectoriel (que nous noterons F). On dispose de la projection canonique $\pi : E \to E/F$. Son application transposée est ${}^t\pi : (E/F)^* \to E^*$. Par propriété universelle du quotient, ${}^t\pi$ induit une bijection $(E/F)^* \to F^0$. Le résultat en découle par la formule $\dim F + \dim E/F = \dim E$. *c.q.f.d.*

Lemme 4. *Soit (E, q) un espace quadratique et soit Φ l'application linéaire canonique $E \to E^*$. Soit $A \subset E$, alors $A^\perp = \Phi^{-1}(A^0)$.*

Démonstration. On raisonne par double inclusion. Soit $y \in A^\perp$, et soit $\varphi = \Phi(y)$. Alors, si $x \in A$, on a $\varphi(x) = b(x, y) = 0$. Ainsi, $\varphi \in A^0$ et $y \in \Phi^{-1}(A^0)$. Réciproquement, soit $\varphi \in A^0$. Supposons qu'on dispose de $y \in E$ tel que $\Phi(y) = \varphi$. Alors, pour tout $x \in A$, $\varphi(x) = 0$ et donc $b(x, y) = 0$: on a bien $y \in A^\perp$. *c.q.f.d.*

Corollaire 2. *Soit (E, q) un espace quadratique non dégénéré. Soient $A, B \subset E$, alors :*
- *$A^\perp$ est un sous-espace vectoriel de E,*

— (*Vect* $A)^\perp = A^\perp$,
— $A \subset (A^\perp)^\perp$,
— *Si* $A \subset B$, *alors* $B^\perp \subset A^\perp$,
— $(A \cup B)^\perp = A^\perp \cap B^\perp$,
— $A^\perp + B^\perp \subset (A \cap B)^\perp$,
— $\dim A^\perp + rg\ A = \dim E$.

Démonstration. L'hypothèse de non dégénérescence montre que Φ est un isomorphisme, qui induit donc une bijection entre A^0 et $A^\perp$ pour tout $A \subset E$. Le résultat découle alors de la proposition 3. *c.q.f.d.*

Corollaire 3. *Soit (E, q) un espace quadratique non dégénéré, et soit F un sous-espace vectoriel de E. Alors $(F, q_{|F})$ est non dégénéré si et seulement si $F \oplus F^\perp = E$.*

Démonstration. Le corollaire 2 montre que $\dim F + \dim F^\perp = \dim E$, donc $F \oplus F^\perp = E$ si et seulement si $F \cap F^\perp = \{0\}$. Or, on a vu que $F \cap F^\perp = N(q_{|F})$, ainsi cette intersection est réduite à $\{0\}$ si et seulement si $(F, q_{|F})$ est non dégénéré. *c.q.f.d.*

2 Classification

Le but de cette partie est de présenter la classification des formes quadratiques sur différents corps, c'est-à-dire de décrire les classes d'isomorphisme d'espaces quadratiques. Comme le laisse penser le cas de la dimension 1, cette classification dépend en effet du corps de base (notamment par l'intermédiaire du groupe $K^\times/(K^\times)^2$).

2.1 Rang et discriminant

Dans un premier temps, nous identifions deux invariants qui permettent de dégrossir la classification.

Définition 7. *Soit (E, q) un espace quadratique. On appelle* rang *de cet espace quadratique le rang de l'application linéaire Φ associée dans le théorème 1.*

Lemme 5. *Soient (E, q) et (E', q') des espaces quadratiques, et soit $u : E \to E'$ un morphisme d'espaces quadratiques. Soit Φ (resp. Φ') l'application linéaire $E \to E^*$ (resp. $E' \to (E')^*$) associée à q (resp. à q'). Alors le diagramme suivant est commutatif :*

$$\begin{array}{ccc} E & \xrightarrow{\Phi} & E^* \\ {\scriptstyle u}\downarrow & & \uparrow{\scriptstyle {}^t u} \\ E' & \xrightarrow[\Phi']{} & (E')^* \end{array} .$$

Démonstration. Si on note b, b' les formes polaires respectives de q et q', on a vu que pour tout $(x, y) \in E^2$, $b'(u(x), u(y)) = b(x, y)$. Cela signifie que $\Phi'(u(x))(u(y)) = \Phi(x, y)$, c'est-à-dire que ${}^t u \circ \Phi' \circ u = \Phi$. Cette relation traduit précisément la commutativité du diagramme de l'énoncé. *c.q.f.d.*

Proposition 4. *Le rang d'un espace quadratique est invariant par isomorphisme.*

Démonstration. Si $u : E \to E'$ est un isomorphisme, alors ${}^t u$ est aussi un isomorphisme, et la commutativité du diagramme du lemme 5 montre que rg Φ = rg Φ'. *c.q.f.d.*

Proposition 5. *Soit (E, q) un espace quadratique et soit $\mathcal{B}$ une base de E. Soit $M = Mat_{\mathcal{B}}(q) = Mat_{\mathcal{B},\mathcal{B}^*}(\Phi)$. Alors* det$M$ *ne dépend de $\mathcal{B}$ qu'à multiplication par un carré près ; la classe de* det$M$ *dans $K/(K^\times)^2$ ne dépend pas de $\mathcal{B}$.*

Démonstration. Si $\mathcal{B}'$ est une autre base de E et P est la matrice de passage de $\mathcal{B}$ à $\mathcal{B}'$, alors en notant $M' = \text{Mat}_{\mathcal{B}'}(q)$, le lemme 5 montre qu'on a ${}^t(P^{-1})M'(P^{-1}) = M$, c'est-à-dire $M' = {}^t PMP$. *c.q.f.d.*

Définition 8. *Soit (E, q) un espace quadratique et soit $\mathcal{B}$ une base de E. Alors le* discriminant *de q est la classe de* det$Mat_{\mathcal{B}}(q)$ *dans $K/(K^\times)^2$.*

Corollaire 4. *Le discriminant d'un espace quadratique est invariant par isomorphisme.*

Démonstration. La relation ${}^t u\Phi' u = \Phi$ du lemme 5 et le fait qu'une matrice et sa transposée ont le même déterminant montrent que detM' et det$M$ sont égaux à multiplication par un carré près. *c.q.f.d.*

2.2 Bases orthogonales

Soit $\mathcal{F}$ une famille de représentants dans K de $K/(K^\times)^2$.

Théorème 2 (Existence d'une base orthogonale)**.** *Soit (E, q) un espace quadratique, alors il existe une base $(e_1, \dots, e_n)$ de E constituée de vecteurs deux à deux orthogonaux et telle que pour tout $1 \leqslant i \leqslant n$, $q(e_i) \in \mathcal{F}$.*

Démonstration. Par récurrence sur $n = \dim E$. Si $n = 0$, le résultat est immédiat. Supposons-le acquis en dimension n, et supposons que $\dim E = n + 1$. Si q est dégénérée, on dispose de $x \in N(q)$ non nul. Si $F \subset E$ est un supplémentaire de x, alors par hypothèse de récurrence F admet une base orthogonale dont l'image par q est dans $\mathcal{F}$, et x complète cette base en une base orthogonale de E dont l'image par q est dans $\mathcal{F}$ (puisque $q(x) = 0 \in \mathcal{F}$.).
On est donc ramené au cas où q est non dégénérée. Dans ce cas, on dispose de $x \in E$ telle que $q(x) \neq 0$. Soit $F = \text{Vect}(x)$, alors $q_{|F}$ est non dégénérée, et donc $E = F \oplus F^\perp$. En outre, on dispose de $\lambda \in K^\times$ tel que $q(\lambda x) = \lambda^2 q(x) \in \mathcal{F}$. On conclut comme précédemment en prenant par hypothèse de récurrence une base orthogonale de $F^\perp$ que l'on complète par λx. *c.q.f.d.*

Remarque 5. *Si $e_1, \dots, e_n$ est une base orthogonale pour q, le rang de la forme quadratique q est le nombre i tels que $q(e_i) \neq 0$. En effet, dans cette base, la matrice de q est diagonale et les coefficients diagonaux sont les $q(e_i)$.*

En adoptant le point de vue des coordonnées, le théorème précédent peut se reformuler ainsi :

Corollaire 5. *Soit (E, q) un espace quadratique. Alors il existe une famille libre de formes linéaires $f_1, \dots, f_r$ et des scalaires $\lambda_1, \dots, \lambda_r$ non nuls tels que $q = \sum_{i=1}^r \lambda_i f_i^2$.*

Démonstration. Soit $e_1, \dots, e_n$ une base orthogonale pour q dont l'image est dans $\mathcal{F}$. Posons pour tout $1 \leqslant i \leqslant n$, $f_i = e_i^*$ et $q(e_i) = \lambda_i \in \mathcal{F}$. Quitte à permuter les vecteurs de base, on peut supposer que $\lambda_1, \dots, \lambda_r$ sont non nuls, et $\lambda_{r+1} = \cdots = \lambda_n = 0$.
Soit $x \in E$, on a par définition $x = \sum_{i=1}^r f_i(x) e_i$. Ainsi, $q(x) = \sum_{i=1}^n q(e_i) f_i(x)^2$, c'est-à-dire que $q = \sum_{i=1}^r \lambda_i f_i^2$. La famille $f_1, \dots, f_r$ est libre car c'est une sous-famille de la base $f_1, \dots, f_n$. *c.q.f.d.*

Remarque 6. *Réciproquement, si $f_1, \dots, f_r$ est une famille libre de formes linéaires telles que $q = \sum_{i=1}^r \lambda_i f_i^2$ avec $\lambda_i \in \mathcal{F}$, on peut compléter cette famille en une base $f_1, \dots, f_n$ de E^*, et le calcul de la preuve précédente montre que la base antéduale $e_1, \dots, e_n$ est orthogonale pour q et a son image dans $\mathcal{F}$. De plus $\lambda_i f_i = b(e_i, \cdot)$.*

Remarque 7. *La démonstration du corollaire montre aussi que l'entier r est égal au rang de q, puisque c'est le nombre de i tels que $q(e_i) \neq 0$ pour une base orthogonale e_i. En particulier, il est indépendant de l'écriture en combinaison linéaire de carrés de formes linéaires indépendantes.*

Décrivons maintenant un algorithme permettant de calculer directement une telle famille $f_1, \dots, f_r$.

Proposition 6. *L'algorithme de Gauss termine et renvoie le résultat attendu.*

Démonstration. Pour $S = [(f_i, \lambda_i), 1 \leqslant i \leqslant r]$, on note $Q(S) = \sum_{i=1}^r \lambda_i f_i^2$. On montre que :
— à chaque passage dans l'une des boucles "Tant que" internes, le nombre de variables de q diminue strictement ;

Entrées : Une forme quadratique q écrite en coordonnées : $q = \sum_{1 \leqslant i \leqslant j \leqslant n} a_{ij} x i x_j$.
Output : Une famille de formes linéaires indépendantes $f_1, \ldots, f_r$ et des scalaires $\lambda_1, \ldots, \lambda_r$ non nuls tels que $q = \sum_{i=1}^{r} \lambda_i f_i^2$.

$S := \emptyset$;
tant que $q \neq 0$ **faire**
  tant que *il existe* $1 \leqslant i \leqslant n$ *tel que* $a_{ii} \neq 0$ **faire**
    trouver i minimal tel que $a_{ii} \neq 0$;
    $f \leftarrow x_i + \sum_{j=i+1}^{n} \frac{a_{ij}}{a_{ii}} x_j$;
    $q \leftarrow q - a_{ii} f^2$;
    $S \leftarrow S + [(f, a_{ii})]$;
  fin
  tant que *pour tout* $1 \leqslant i \leqslant n$, $a_{ii} = 0$ **faire**
    trouver (i, j) minimal tel que $a_{ij} \neq 0$;
    $g_1 \leftarrow x_i + \sum_{k=j+1}^{n} \frac{a_{jk}}{a_{ij}} x_k$;
    $g_2 \leftarrow x_j + \sum_{k=j+1}^{n} \frac{a_{ik}}{a_{ij}} x_k$;
    $q \leftarrow q - a_{ij} g_1 g_2$;
    $S \leftarrow S + [\left(\frac{g_1+g_2}{4}, a_{ij}\right), \left(\frac{g_1-g_2}{4}, -a_{ij}\right)]$
  fin
fin
retourner S

Algorithme 1 : Algorithme de réduction de Gauss

— $q + Q(S)$ est un invariant de boucle ;
— à chaque étape, la famille de formes linéaires données dans S est libre.

Pour le premier point, il suffit de remarquer que $q - a_{ii} f^2$ ne dépend plus de x_i (c'est-à-dire que c'est une combinaison linéaire des $x_j x_k$ avec $j, k > i$) ; de même, $q - a_{ij} g_1 g_2$ ne dépend plus de x_i et x_j.
Pour le deuxième point, c'est immédiat si on note que $g_1 g_2 = \frac{1}{4}\left((g_1 + g_2)^2 - (g_1 - g_2)^2\right)$.
Pour le dernier point, on voit que par construction, dans la base $(x_1, \ldots, x_n)$ de E^*, la famille f_i s'écrit à l'aide d'une matrice triangulaire inférieure par blocs dont les blocs diagonaux sont de taille 1 avec le coefficient 1, ou de taille 2 et de la forme $\begin{pmatrix} 1/4 & 1/4 \\ 1/4 & -1/4 \end{pmatrix}$. *c.q.f.d.*

Exemple 5. *Soit $q(x, y, z, t) = xy + yz + zt$. Les étapes de l'algorithme donnent les écritures suivantes :*

$$\begin{aligned} q &= (x+z)y + zt \\ &= \tfrac{1}{4}(x+y+z)^2 - \tfrac{1}{4}(x-y+z)^2 + zt \\ &= \tfrac{1}{4}(x+y+z)^2 - \tfrac{1}{4}(x-y+z)^2 + \tfrac{1}{4}(z+t)^2 - \tfrac{1}{4}(z-t)^2. \end{aligned}$$

On verra dans la partie suivante que cet algorithme est surtout utile pour calculer la signature d'une forme quadratique réelle.

2.3 Espaces quadratiques sur un corps algébriquement clos

Théorème 3. *Deux espaces quadratiques sur un corps algébriquement clos sont isomorphes si et seulement si ils ont même dimension et même rang.*

Démonstration. Comme K est algébriquement clos, $K/(K^\times)^2 = \{\bar{0}, \bar{1}\}$. Le théorème d'existence de bases orthogonales montre qu'un espace quadratique de dimension n et de rang r est isomorphe à (K^n, q_r) où $q_r(x_1, \ldots, x_n) = x_1^2 + \cdots + x_r^2$. Il y a donc une seule classe d'isomorphisme de tels espaces. *c.q.f.d.*

Remarque 8. *L'argument précédent reste valable dès que $K^\times/(K^\times)^2 = \{\bar{1}\}$, c'est-à-dire dès que K est* quadratiquement clos *(tout élément de K admet une racine carrée). C'est par exemple le cas pour le corps des nombres constructibles.*

2.4 Espaces quadratiques réels

Théorème 4 (Théorème d'inertie de Sylvester)**.** *Soit (E, q) un espace quadratique sur $\mathbf{R}$. Alors il existe une base orthogonale de E, $(e_1, \dots, e_n)$, et des entiers (s, t) tels que :*

— $q(e_1) = \cdots = q(e_s) = 1$,
— $q(e_{s+1} = \cdots = q(e_{s+t}) = -1$,
— $\forall i > s + t, q(e_i) = 0$.

Les entiers s et t ne dépendent pas de la base choisie.

Démonstration. L'existence est une application directe du théorème 2. Pour l'unicité, supposons qu'on dispose d'une autre telle base $(e'_1, \dots, e'_n)$ associée aux entiers (s', t'). Montrons que la famille $(e_1, \dots, e_s, e'_{s'+1}, \dots, e$ est libre dans $E/N(q)$.
On suppose qu'on a une relation de la forme : $\sum_{i=1}^{r} \lambda_i e_i = z + \sum_{j=1}^{t'} \mu_j e'_{j+s'}$, avec $z \in N(q)$. En appliquant q, on obtient $\sum_{i=1}^{r} \lambda_i^2 = -\sum_{j=1}^{t'} \mu_j^2$. Il en résulte que tous les coefficients sont nuls, donc la famille considérée est libre dans $E/N(q)$.
Maintenant, on a $s + t' \leqslant \dim E/N(q) = \operatorname{rg} q = s + t = s' + t'$, d'où $t' \leqslant t$ et $s \leqslant s'$. Par symétrie, on a les inégalités contraires, donc $s = s'$ et $t = t'$. *c.q.f.d.*

Définition 9. *Pour (E, q) un espace quadratique sur $\mathbf{R}$, le couple (s, t) obtenu dans le théorème de Sylvester s'appelle la* signature *de q.*

Corollaire 6. *Deux espaces quadratiques réels sont isomorphes si et seulement s'ils ont la même dimension et la même signature.*

Remarque 9.
— *On peut généraliser la notion de signature aux formes quadratiques sur un corps K ordonné ; le même argument que ci-dessus montre que le nombre de i tels que $q(e_i) > 0$ et le nombre de i tels que $q(e_i) < 0$ sont indépendants du choix d'une base orthogonale.*
— *Si K est un corps* réels clos *(c'est-à-dire ordonné tel que tout élément positif soit un carré et tel que tout polynôme de degré impair admette une racine) alors le résultat de classification sur $\mathbf{R}$ est aussi vrai sur K. C'est par exemple le cas pour $\overline{\mathbf{Q}} \cap \mathbf{R}$.*

Exemple 6. *Soit $P \in \mathbf{R}[X]$. Soient $\lambda_1, \dots, \lambda_n$ les racines complexes de P. Pour $k \geqslant 0$, la k-ème somme de Newton est le nombre $s_k = \sum_{i=1}^{n} \lambda_i^k$. Comme c'est un polynôme symétrique en les λ_i, c'est en fait un nombre réel qui peut s'exprimer comme un polynôme en les coefficients de P. La forme quadratique $q(x_0, \dots, x_{n-1}) = \sum_{k,\ell} s_{k+\ell} x_k x_\ell$ peut se réécrire $q = \sum_{i=1}^{n} \sum_{k,\ell} \lambda_i^{k+\ell} x_k x_\ell = \sum_{i=1}^{n} (\sum_k \lambda_i^k x_k)^2$. En séparant les racines réelles et les racines complexes non réelles, que l'on peut rassembler par paires conjuguées, on voit grâce à cette écriture que la signature de cette forme quadratique est $(r + s, s)$ où r est le nombre de racines réelles distinctes et s est le nombre de racines complexes non réelles distinctes ; en particulier, on peut déterminer le nombre de racines réelles et le nombre de racines complexes en calculant cette signature, ce qui est possible car les s_k peuvent être calculés à partir des coefficients de P sans le factoriser.*

Corps réels clos.

Un corps réel clos est un corps K ordonné, c'est-à-dire muni d'un ordre total $\leqslant$ compatible avec les opérations (*i.e.*, si $a \leqslant a'$ et $b \leqslant b'$ alors $a + b \leqslant a' + b'$, et si $0 \leqslant a$ et $0 \leqslant b$, alors $0 \leqslant ab$), et tel que :
— tout nombre positif est un carré ;
— tout polynôme de degré impair admet une racine.

Les propriétés suivantes sont équivalentes :
— K est un corps réel clos ;
— K n'est pas algébriquement clos, mais $K(\sqrt{-1})$ est algébriquement clos ;
— K n'est pas algébriquement clos et sa clôture algébrique est une extension finie de K ;
— K est un corps ordonné et le théorème des valeurs intermédiaires est vrai pour cet ordre.

2.5 Espaces quadratiques sur les corps finis

Dans cette sous-partie, K désigne un corps fini de caractéristique différente de 2. On notera q le cardinal de K.

Lemme 6. *Le groupe $(K^\times)^2$ est d'indice 2 dans $K^\times$. En particulier, il y a $\frac{q-1}{2}$ carrés non nuls dans K.*

Démonstration. Le morphisme $x \mapsto x^2$ a pour image $(K^\times)^2$ et pour noyau $\{\pm 1\}$ qui est d'ordre 2. *c.q.f.d.*

Remarque 10. *Un élément $a \in K^\times$ est un carré si et seulement si $a^{\frac{q-1}{2}} = 1$. En effet, il est clair qu'un carré doit vérifier cette relation, et la réciproque découle du fait que le polynôme $X^{\frac{q-1}{2}} - 1$ possède au plus $\frac{q-1}{2}$ racines, donc les carrés sont précisément ces racines.*

Lemme 7. *Soient $a, b \in K$ non nuls, et soit $c \in K$. Alors l'équation $ax^2 + by^2 = c$ admet une solution dans K^2.*

Démonstration. Les ensembles $\{ax^2, x \in K\}$ et $\{c - by^2, y \in K\}$ sont tous deux en bijection avec les carrés de K, donc de cardinal $\frac{q+1}{2}$. Leur intersection est donc non vide. *c.q.f.d.*

Proposition 7. *Soit (E, q) un espace quadratique sur K de dimension n et de rang r. Soit $d \in K^\times$ un représentant du discriminant de $(E/N(q), \bar{q})$. Alors (E, q) est isomorphe à $(K^n, q_{r,d})$ où $q_r = x_1^2 + \cdots + x_{r-1}^2 + dx_r^2$.*

Démonstration. Il suffit de démontrer le résultat pour $E/N(q)$, on peut donc supposer $r = n$. On procède alors par récurrence sur n. En fixant une base orthogonale, on se ramène au cas où $q = \sum_{i=1}^n \lambda_i x_i^2$, avec les λ_i dans $\mathcal{F}$.
En dimension 1, le résultat est connu.
Supposons $n \geqslant 2$. D'après le lemme 7, on dispose de $z \in E$ tel que $q(z) = 1$. Soit alors $F = \text{Vect}(z)^\perp$, par hypothèse de récurrence le résultat vaut pour F. Par ailleurs, $d = 1 \times \text{disc}(F)$. Cela montre le résultat pour E. *c.q.f.d.*

Corollaire 7. *Deux espaces quadratiques sur K sont isomorphes si et seulement s'ils ont même dimension, même rang et si les espaces quadratiques non dégénérés canoniquement associés (par quotient par le noyau) ont le même discriminant.*

Démonstration. Immédiat. *c.q.f.d.*

Remarque 11. *En particulier, la classe d'isomorphisme d'un espace quadratique non dégénéré sur un corps fini est déterminée par son discriminant (ce qui se résume à savoir si le déterminant de la matrice correspondante est un carré ou non).*

Exemple 7. *Le dénombrement de l'ensemble des p-uplets $(x_1, \ldots, x_p) \in \mathbf{F}_q^p$ tels que $\sum_{i=1}^p x_i^2 = 1$, fait de deux façons différentes en utilisant ce théorème, conduit à une démonstration de la loi de réciprocité quadratique : c'est un développement classique.*

Remarque 12. *Ici, l'argument clé est que toute forme quadratique de rang au moins 2 prend la valeur 1 ; ceci est bien sûr faux dans le cas réel puisqu'il existe des formes quadratiques négatives.*

3 Groupe orthogonal d'une forme quadratique

Dans cette section, on étudie le groupe des isométries d'un espace quadratique, c'est-à-dire le sous-groupe de $GL(E)$ défini par :

$$O(q) = \{u \in GL(E) \mid u \circ q = u\}.$$

3.1 Théorème de Cartan-Dieudonné

Définition 10. *Soit (E, q) un espace quadratique de forme polaire b, et soit $z \in E$ non isotrope (c'est-à-dire tel que $q(z) \neq 0$. La* réflexion d'axe z *est l'application linéaire σ_z définie par la formule :*

$$\sigma_z(x) = x - 2\frac{b(x,z)}{q(z)}z.$$

Lemme 8. *Les réflexions sont des isométries involutives.*

Démonstration. Soit $x \in E$, et soit u la réflexion d'axe z. Alors :

$$q(u(x)) = b(x,x) - 4\frac{b(x,z)^2}{q(z)} + 4\frac{b(x,z)^2}{q(z)^2}q(z) = b(x,x) = q(x).$$

Enfin, $\sigma_z^2(x) = \sigma_z(x) + 2\frac{b(x,z)}{q(z)}z = x$, ce qui montre l'involutivité. *c.q.f.d.*

Remarque 13. *Soit u la réflexion d'axe z. Alors la restriction de u à $\{z\}^\perp$ est l'identité, et $u(z) = -z$.*

On rappelle qu'un sous-espace est dit totalement istrope s'il est contenu dans $I(q)$.

Lemme 9. *Si (E, q) est non dégénéré et $F \subset E$ est totalement isotrope, alors $2\dim F \leqslant \dim E$*

Démonstration. Si F est totalement isotrope alors $F \subset F^\perp$, donc $\dim F \leqslant \dim F^\perp$. Ainsi, $2\dim F \leqslant \dim F + \dim F^\perp = \dim E$. *c.q.f.d.*

Théorème 5 (Cartan-Dieudonné)**.** *Soit (E, q) un espace quadratique non dégénéré de dimension n. Alors tout élément de $O(q)$ est produit d'au plus n réflexions.*

Démonstration. Soit $u \in O(q)$, on procède par récurrence sur n.
Si $n = 0$, alors $u = id_E$ et donc u est produit de 0 réflexions.
Supposons le résultat acquis en dimension $n-1$ et démontrons-le en dimension n. Pour cela, on considère trois cas :
Cas 1. Il existe $x \in E$ tel que $u(x) = x$ et $q(x) \neq 0$.
Alors $D = \text{Vect}(x)$ et $F = D^\perp$ sont stables par u, l'espace quadratique F est non dégénéré, et $E = D \oplus F$. Par hypothèse de récurrence, il existe $x_1, \ldots, x_k \in F$ tel que $u_{|F} = \sigma_{x_1} \cdots \sigma_{x_k}$ (avec $k \leqslant n-1$). Les applications u et $\sigma_{x_1} \cdots \sigma_{x_k}$ coïncident aussi sur D, elles sont donc égales.
Cas 2. Il existe $x \in E$ tel que et $q(x) \neq 0$ et $q(u(x) - x) \neq 0$.
Alors $D = \text{Vect}(x)$ et $F = D^\perp$ sont stables par u. De plus, un calcul immédiat montre que $u(x) + x \in D^\perp$. Posons alors $z = u(x) - x$, on a $\sigma_z(u(x) - x) = -u(x) + x$ et $\sigma_z(u(x) + x) = u(x) + x$. Ainsi, $\sigma_z(u(x)) = x$, de sorte que $\sigma_z \circ u$ admet x comme point fixe. Comme $q(x) \neq 0$, on est ramené au cas 1 : $\sigma_z \circ u$ est produit d'au plus $n-1$ réflexions, donc u est produit d'au plus n réflexions.
Cas 3. Pour tout $x \in E$ tel que $q(x) \neq 0$, on a $q(u(x) - x) = 0$.
Soit $x \in E$ tel que $q(x) \neq 0$. Supposons $\dim E = 2$, et soit $D = \text{Vect}(x)$. On a alors $E = D \oplus D^\perp$, et $D^\perp$ est une droite non isotrope. Or $x - u(x) \in D^\perp$ et est isotrope, c'est donc que $x = u(x)$, et on est encore ramené au cas 1.
On suppose maintenant que $\dim E \geqslant 3$ et que l'on ne se trouve pas dans l'un des deux premiers cas. Alors $\ker(u - id) \subset I(q)$. Montrons que $\text{Im}(u - id) \subset I(q)$. Soit $x \in E$, si $q(x) \neq 0$ alors comme on n'est pas dans le cas 2, $q(u(x) - x) = 0$. Soit alors $x \in E$ tel que $q(x) = 0$. On a $\dim \text{Vect}(x)^\perp = \dim E - \dim \text{Vect}(x) > (\dim E)/2$, donc $\text{Vect}(x)^\perp \not\subset I(q)$: on dispose de $z \in \text{Vect}(x)^\perp$ tel que $q(z) \neq 0$. On a alors $q(x+z) = q(x-z) = q(z) \neq 0$, et comme on n'est pas dans le cas 2, $q(u(x+z)-(x+z)) = 0$, $q(u(x-z)-(x-z)) = 0$, et $q(u(z)-z) = 0$. La combinaison de ces trois relations montre que $q(u(x) - x) = 0$. Pour conclure, remarquons que le théorème du rang montre que $\dim \ker(u - id) = \text{rg}(u-id) = (\dim E)/2$; en particulier, $\dim E$. Enfin, remarquons que $\text{Im}(u-id) = \ker(u-id)$: en effet, ces deux sous-espaces sont orthogonaux (si $u(x) = x$, alors $b(u(y)-y, x) = b(u(y), u(x)) - b(y, x) = 0$) et donc leur somme est totalement isotrope. Ainsi, la matrice de $u - id_E$ dans une base adaptée est triangulaire supérieure par blocs, avec 2 blocs diagonaux de taille $(\dim E)/2$ et nuls. On a $\det(u) = 1$; en particulier, si $q(x) \neq 0$, $u \circ \sigma_x$ est de déterminant -1 et donc nécessairement dans le cas 1 ou 2. C'est un produit d'un nombre impair de réflexions, qui est donc $< \dim E$, et on obtient le résultat en composant par σ_x. *c.q.f.d.*

Ce théorème est en particulier vrai pour les groupes $O(n)$, $n \in \mathbf{N}$ qui sont les groupes orthogonaux « classiques » des espaces euclidiens $\mathbf{R}^n$. Notons par exemple que tout élément de $O(2)$ est produit d'au plus 2 réflexions (plus précisément, toute rotation non triviale est produit de deux réflexions dont les axes forment un angle moitié de l'angle de la rotation).

3.2 Groupes orthogonaux réels

3.2.1 Les groupes $O(s,t)$

On note $O(s,t)$ le groupe orthogonal de la forme quadratique de signature (s,t) sur $\mathbf{R}^{s+t}$. Remarquons tout d'abord que si q est de signature (s,t), alors le lieu d'équation $\{q = \alpha\}$ est homéomorphe à $\mathbf{S}^p \times \mathbf{R}^q$ si $\alpha > 0$, et le lieu d'équation $\{q > 0\}$ est homéomorphe à $\mathbf{S}^p \times \mathbf{R}^q \times \mathbf{R}_+^*$.
On a $O(s) \times O(t)$ comme sous-groupe compact de $O(s,t)$. Le sous-groupe $SO^+(s,t)$ est constitué des matrices dont les 2 blocs diagonaux sont de déterminant positif.
Voir Perrin pour d'autres propriétés....

3.2.2 Le groupe $O(3,1)$ et l'espace-temps de Minkowski (garanti sans théorème)

Dans la théorie de la relativité restreinte, on identifie l'espace-temps ambiant à l'espace $\mathbf{R}^4$, que l'on munit de la forme $q : (x,y,z,t) \mapsto c^2t^2 - x^2 - y^2 - z^2$. La variable t représente le temps, et les variables (x,y,z) représentent l'espace usuel, et c est la vitesse de la lumière dans le vide.

Les transformations de l'espace-temps qui préservent q s'appellent les *transformations de Lorentz* : ce n'est rien d'autre que le groupe $O(3,1)$. Le fait que la lumière se déplace à la même vitesse dans tous les référentiels se traduit précisément par le fait que les transformations de Lorentz sont les changements de référentiels admissibles. Le cône isotrope est l'ensemble des points de l'espace-temps vérifiant $d = c|t|$, où d est la distance à l'origine : c'est l'ensemble des points que l'on peut atteindre à partir de l'origine en se déplaçant constamment à la vitesse de la lumière. Pour cette raison, on l'appelle *cône de lumière* : son invariance par transformation de Lorentz reflète l'invariance de la vitesse de la lumière par changement de référentiel. Le cône de lumière, de même que les points dont l'image par q est > 0 (resp. < 0) est stable par transformations de Lorentz. Un événement se produisant en (x,y,z,t) ne peut être causé par un événement se produisant en l'origine que si $q(x,y,z,t) < 0$.

Si D est une droite passant par l'origine et contenue dans $\{q < 0\}$, on dit que D est un observateur galiléen : D est la trajectoire suivie par un observateur se déplaçant à vitesse constante (et $< c$) depuis l'origine. Le groupe G agit transitivement sur l'ensemble des opérateurs galiléens ; en effet, si $p_0 = (t_0, x_0, y_0, z_0)$ est le vecteur directeur d'une telle droite, avec $q(p_0) = q(p_1) = -1$, alors il suffit de montrer que p_0 peut être envoyé par transformation de Lorentz sur la droite $x = y = z = 0$ de vecteur directeur $e = (1,0,0,0)$. Pour cela, remarquons d'abord que $\{p_0\}$ se complète en une base orthogonale de $\mathbf{R}^4$ dont les autres vecteurs vérifient $q(p_1) = q(p_2) = q(p_3) = 1$. Le même argument montre le même résultat pour e, et ainsi, l'unique application linéaire envoyant la première base sur la deuxième est une transformation de Lorentz. Notons au passage que les vecteurs (p_1, p_2, p_3) engendrent $\mathrm{Vect}(p_0)^\perp$ et donc ce sous-espace est contenu dans $\{q > 0\}$. Ce résultat de transitivité traduit le fait que l'on peut toujours changer de référentiel pour se placer du point de vue d'un autre observateur galiléen. Quitte à composer par (un conjugué de) la réflexion d'axe $(1,0,0,0)$ et par (un conjugué de) la réflexion d'axe $(0,0,0,1)$, on peut supposer que la transformation préserve le sens du temps (c'est-à-dire stabilise le demi-cône $\{q < 0\} \cap \{t > 0\}$) et l'orientation de l'espace. Ainsi, le sous-groupe qui préserve le sens du temps et l'orientation de l'espace, qui n'est autre que $SO^+(1,3)$ agit aussi transitivement sur les observateurs galiléens.

Notons enfin que le groupe $SL_2(\mathbf{C})$ agit sur l'espace-temps de Minkowski : on peut associer à un point (t,x,y,z) une matrice de Pauli : $X = \begin{pmatrix} ct+z & x-iy \\ x+iy & ct-z \end{pmatrix}$, et l'action de $S \in SL_2(\mathbf{C})$ est donnée par $X \mapsto SXS^*$. Cela donne un morphisme $SL_2(\mathbf{C}) \to SO^+(3,1)$ dont on montre que le noyau est $\{\pm 1\}$: $SO^+(1,3) \simeq PSL_2(\mathbf{C})$.

4 Théorie de Witt

4.1 Prolongement des isométries

Proposition 8. *Soient $(E,q),(E',q')$ des espaces quadratiques non dégénérés. On suppose E et E' isométriques. Soient F,F' des sous-espaces respectifs de E et E', et $u : F \to F'$ une isométrie, alors il existe une isométrie $\hat{u} : E \to E'$ qui prolonge u.*

Démonstration. Quitte à composer par une isométrie $E \to E'$, on peut supposer que $E = E'$. On démontre le résultat par récurrence sur $\dim E/F$, le cas $n = 0$ étant évident. On notera b, b' les formes polaires respectives de q, q'.
Traitons d'abord le cas où $q_{|F}$ est dégénéré : on dispose de $x \in F$ non nul tel que $b(x,y) = 0$ pour tout $y \in F$. Soit $z \in E$ tel que $b(x,z) = 1$ (cela existe car q est non dégénéré). Quitte à remplacer z par $z + \lambda x$ pour un λ convenable, on peut supposer que $q(z) = 0$. Maintenant, par le même argument, on dispose d'un $z' \in F'$ tel que $b'(u(x),z') = 1$ et $q'(z) = 0$. On prolonge alors u par $z \mapsto z'$, ce qui donne bien une isométrie de $F \oplus Kz \to F' \oplus Kz'$ et conclut par récurrence.
On suppose maintenant $q_{|F}$ non dégénéré, et on procède par récurrence sur $d = \dim F$. Supposons $d = 1$, soit $x \in F$ non isotrope, alors $u(x) - x$ ou $u(x) + x$ est non isotrope. La symétrie d'axe $u(x) - x$ envoie x sur $u(x)$ donc c'est une isométrie qui coïncide avec u sur F ; dans le cas où $u(x) - x$ est isotrope, on peut prolonger u par $-\sigma$ où σ est la réflexion d'axe $u(x) + x$. Il reste à justifier l'hérédité. Supposons F de dimension d, fixons $x \in F$ tel que $q(x) \neq 0$. Alors $G = x^\perp \cap F$ est un sous-espace de dimension $d-1$, et par le cas $d = 1$ on dispose de $s \in O(E)$ tel que su stabilise Vect(x) et G. Par hypothèse de récurrence, su se prolonge en une isométrie de $G \oplus F^\perp$. En composant par s^{-1}, on obtient un prolongement de u. *c.q.f.d.*

Corollaire 8. *Soient (E,q) et (E',q') deux espaces quadratiques isométriques. Soient F,F' des sous-espaces respectifs de E,E' que l'on suppose isométriques. Alors les espaces quadratiques $F^\perp$ et $(F')^\perp$ sont isométriques.*

Démonstration. On dispose d'une isométrie $u : F \to F'$. Cette isométrie se prolonge en une isométrie $\hat{u} : E \to E'$ qui induit une isométrie $F^\perp \to (F')^\perp$. *c.q.f.d.*

4.2 Théorème de Witt

Lemme 10. *Soit (E,q) non dégénéré. Les sous-espaces totalement isotropes maximaux de (E,q) sont tous de même dimension.*

Démonstration. Si $F, F' \subset E$ sont totalement isotropes, avec $\dim F \leqslant \dim F'$, toute injection $u : F \to F'$ est une isométrie. D'après le théorème de prolongement, une telle isométrie se prolonge à E. Si F est maximal, alors l'image de F par une telle isométrie est maximale, donc $F' = \text{Im}(F)$ et $\dim F = \dim F'$. *c.q.f.d.*

Remarque 14. *L'argument précédent montre plus généralement que l'action de $O(q)$ sur l'ensemble des sous-espaces totalement isotropes de dimension k est transitive.*

Définition 11. *On appelle* plan hyperbolique *tout espace quadratique de dimension 2 et isométrique à $(K^2, e_1^* e_2^*)$.*

Dans la suite, H désigne un plan hyperbolique sur K.

Corollaire 9. *Soit (E,q) un espace quadratique non dégénéré. Alors il existe un unique entier k et un espace quadratique F anisotrope et unique à isométrie près tels que $E \simeq H^k \oplus F$ (les sommes sont orthogonales).*

Démonstration. Raisonnons par récurrence sur $\dim E$. Si E n'a pas de vecteur isotrope alors il ne contient pas de plan hyperbolique, donc la seule décomposition de E sous la forme voulue est $k = 0$, $F = E$.
Supposons que E ait un vecteur isotrope x, alors on dispose de $y \in E$ tel que $b(x,y) = 1$ et $q(y) = 0$.

Ainsi $H = \text{Vect}(x, y)$ est un plan hyperbolique. On peut alors poser $F = H^\perp$ et conclure par récurrence pour l'existence. L'unicité découle alors du théorème d'annulation de Witt. *c.q.f.d.*

Remarque 15. *L'entier k comptant le nombre de plans hyperboliques dans une décomposition de Witt est un invariant, appelé* indice d'isotropie *de q. Il est en fait égal à la dimension (commune) des sous-espaces totalement isotropes maximaux. En effet, une somme orthogonale de k plans hyperboliques a clairement un sous-espace F isotrope de dimension k, qui est donc maximal (prendre le premier vecteur de base de chaque plan hyperbolique). Si $E = H \oplus G$ avec H sous-espace hyperbolique et G anisotrope, alors $I(q) \subset H$ (en effet, si $x = h + g \in E$ est isotrope alors $0 = q(x) = q(g)$ donc $g = 0$) et F est maximal dans H donc dans E. Ainsi $k = (\dim H)/2$ est bien la dimension des sous-espaces totalement isotropes maximaux.*

Remarque 16. *Dans le cas des formes quadratiques réelles non dégénérées, si q est de signature (s, t) alors en regroupant, l'indice d'isotropie est $|s - t|$ (on le voit en regroupant deux à deux les éléments d'une base orthogonale convenable). La partie anisotrope est munie d'une forme définie positive (si $s \geqslant t$ ou définie négative (si $s \leqslant t$).*

Ainsi l'ensemble des espaces quadratiques non dégénérés peut être muni de la relation d'équivalence suivante : $E \sim E'$ si les parties anisotropes de E et E' sont isométriques. Cet ensemble est naturellement muni d'une structure de groupe : $q \oplus (-q) = 0$. Le groupe appelé groupe de Witt ne dépend que du corps de base, il est toujours engendré par $K^\times/(K^\times)^2$. Par exemple :

- $W(\mathbf{C}) = \mathbf{Z}/2\mathbf{Z}$
- $W(\mathbf{R}) = \mathbf{Z}$
- $W(\mathbf{F}_q) = \mathbf{Z}/4\mathbf{Z}$ si $q = 3 \pmod 4$ (c'est-à-dire -1 non carré, groupe engendré par $< 1 >$), et $W(\mathbf{F}_q) = \mathbf{Z}/2\mathbf{Z}[\alpha]$ sinon (c'est-à-dire -1 est carré, générateurs $< 1 >$ et $< \alpha >$ avec α non carré).

Remarque 17. *Le groupe de Witt peut même être muni d'une structure d'anneau, la multiplication étant donnée par le produit tensoriel d'espaces quadratiques.*

On peut montrer que les éléments d'ordre fini du groupe de Witt sont d'ordre une puissance de 2. Si L est la clôture pythagoricienne de K (la plus petite extension de K dans laquelle tout élément de la forme $a^2 + b^2$ a une racine carrée) alors L alors $W(K) \subset W(L)$ et le noyau de cette inclusion est précisément l'ensemble des éléments d'ordre fini de $W(K)$.