Université de Bretagne Occidentale

Faculté des Sciences et Techniques

Département de Mathématiques

Projet TER

THÉORIE DE WITT

Réalisé par :
Mohamed EL BAHA

Encadré par :
Pr. Thierry LEVASSEUR

2020

Je tiens à remercier tout particulièrement mon encadrant, M. Thierry Levasseur, pour son implication personnelle afin que le projet se déroule dans des bonnes conditions. La disponibilité et l'aide qu'il m'a apportées tout au long de cette période ont été précieuses et très appréciables.

Table des matières

1 Introduction

La théorie de Witt, ainsi nommée d'après les travaux du mathématicien allemand Ernst WITT (1911-1991), est un outil fondamental de la théorie algébrique des formes quadratiques. E. Witt est considéré comme le premier mathématicien à avoir étudié les formes quadratiques sur un corps quelconque ; avant lui les formes quadratiques avaient été considérées sur $\mathbb{R}$ (Sylvester) et sur $\mathbb{Q}$ (Minkowski & Hasse). Cette théorie s'applique à la classification des formes quadratiques sur un corps $\mathbb{K}$ arbitraire grâce à l'anneau et au groupe de Witt $W(\mathbb{K})$.

Les formes quadratiques apparaissent dans plusieurs domaines et l'on peut réduire la classification de certains objets mathématiques à celle des formes quadratiques ; on peut par exemple utiliser cette classification pour étudier les coniques. Lorsque l'on considère le problème de la classification des formes quadratiques, on pose les questions : étant données deux formes quadratiques sur un corps $\mathbb{K}$ quand sont-elles équivalentes ? peut-on obtenir l'une à partir de l'autre ? Ces questions sont faciles lorsque le corps est $\mathbb{R}$ ou $\mathbb{C}$, mais elles deviennent plus difficiles sur un corps quelconque ; on introduit ici des invariants qui aident à y répondre. Dans ce contexte, un invariant est un objet mathématique associé à une forme quadratique qui ne change pas quand on remplace cette forme par une forme équivalente. Ces invariants sont donc utilisés pour distinguer deux formes quadratiques qui ne sont pas équivalentes.

Nous nous appuyons principalement dans ce mémoire sur l'excellent ouvrage de Clément de Seguins Pazzis « Invitation aux formes quadratiques ».

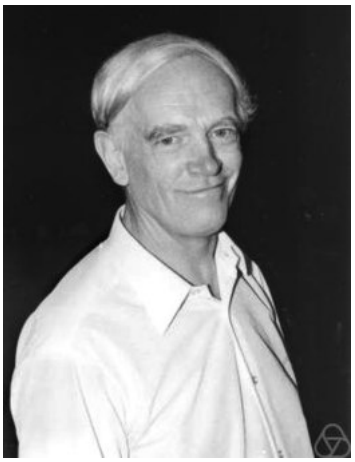

Figure 1 – Ernst WITT

2 Chapitre I : Pré-requis

Dans tout le chapitre, $\mathbb{K}$ est un corps de caractéristique différente de 2. Tous les espaces vectoriels considérés sont (sauf mention contraire) dimension finie.

2.1 Généralités sur les formes quadratiques

Définition 2.1. *Soit E un $\mathbb{K}$-espace vectoriel. On dit qu'une application $q : E \to \mathbb{K}$ est une **forme quadratique** sur E, s'il existe une forme bilinéaire f sur E, telle que :*

$$\forall x \in E, \quad q(x) = f(x, x)$$

Remarque 2.1. *Si f est une forme bilinéaire symétrique sur E, alors l'application $q : E \to \mathbb{K}$ définie par :*

$$\forall x \in E, \quad q(x) = f(x, x)$$

est une forme quadratique sur E, appelée forme quadratique associée à la forme bilinéaire symétrique f. Réciproquement, à toute forme quadratique, on peut associer une forme bilinéaire symétrique unique, que l'on appelle la forme polaire associée à q.

Exemple 2.1. *Un exemple de forme bilinéaire est le produit scalaire dans un espace euclidien. Soit $x = (x_1, x_2, x_3), y = (y_1, y_2, y_3)$*

$$\langle x, y \rangle = x_1y_1 + x_2y_2 + x_3y_3.$$

La norme élevée au carré est une forme quadratique :

$$||x||^2 = \langle x, x \rangle = x_1^2 + x_2^2 + x_3^2.$$

Définition 2.2. *Soit E un $\mathbb{K}$-espace vectoriel, un **espace bilinéaire** (symétrique) (E, f) est un espace vectoriel E muni d'une forme bilinéaire symétrique f. On appelle **espace quadratique** tout couple (E, q) où q est une forme quadratique sur E.*

*Soient (E, f) et (E, f') deux espaces bilinéaires et $u : E \to E'$ une application linéaire. On dit que u est une **isométrie** si u est injective et $f'(u(x), u(y)) = f(x, y)$ pour tous $x, y \in E$.*

Définition 2.3. *Soit (E, q) un espace quadratique, notons f la forme polaire associée à q. On appelle **noyau** de la forme quadratique q l'ensemble :*

$$\mathrm{Ker}(q) = \{x \in E : \forall y \in E, f(x, y) = 0\}.$$

*On appelle **rang** de q et on note $\mathrm{rg}(q)$ l'entier :*

$$\mathrm{rg}(q) = \dim E - \dim \mathrm{Ker}(q).$$

Remarque 2.2. *Si $\dim E = n$ et $\beta = (e_1, e_2, \ldots, e_n)$ est une base de E on définit la matrice de f dans β par $\mathrm{mat}_\beta(f) = [f(e_i, e_j)]_{i,j}$, alors on a :*

$$\mathrm{rg}(q) = \mathrm{rg}(f) = \mathrm{rg}\,\mathrm{mat}_\beta(f).$$

Avec les notations de la remarque précédente, rappelons que $\mathrm{mat}_\beta(f)$ est symétrique et que si β, β' sont deux bases de E alors $\mathrm{mat}_{\beta'}(f) = {}^tP\,\mathrm{mat}_\beta(f)P$ où $P \in \mathrm{GL}_n(\mathbb{K})$ est la matrice de passage de β à β', i.e. les matrices $\mathrm{mat}_\beta(f)$ et $\mathrm{mat}_{\beta'}(f)$ sont congruentes. Ceci implique que $\det \mathrm{mat}_{\beta'}(f) = (\det \mathrm{mat}_\beta(f))(\det P)^2$ avec $(\det P)^2$ appartenant au sous-groupe $(\mathbb{K}^*)^2$ des carrés de $\mathbb{K}^*$.

2.2 Diagonalisation des formes quadratiques

Définition 2.4. *Soit $(e_1, \ldots, e_n)$ une base de E, On dit que la base $(e_1, \ldots, e_n)$ est q-orthogonale si la matrice représentant q dans cette base est diagonale.*

Notation 2.1. *On note $\langle a_1, \ldots, a_n \rangle$ la forme quadratique diagonale définie sur l'espace $\mathbb{K}^n$ par :*

$$(x_1, \ldots, x_n) \to a_1 x_1^2 + \cdots + a_n x_n^2.$$

Définition 2.5. *Soient (E, q) et (E', q') deux espaces quadratiques, on dit que q et q' sont équivalentes et on écrit $q \simeq q'$ lorsqu'il existe un isomorphisme $\phi : E \to E'$ tel que :*

$$\forall x \in E, \quad q'(\phi(x)) = q(x).$$

De manière équivalente : si f, f' sont les formes polaires associées à q, q', il existe une isométrie bijective de (E, f) sur (E, f').

Exemple 2.2. *Considérons les deux formes quadratiques de dimension 2 :*

$$q = X_1 X_2 \quad \textit{et} \quad q' = Y_1^2 - Y_2^2$$

Considérons la forme bilinéaire $f : (X_1, X_2) \to (Y_1 + Y_2, Y_1 - Y_2)$ Ainsi :

$$q(f(X_1, X_2)) = q(Y_1 + Y_2, Y_1 - Y_2) = (Y_1 + Y_2) \times (Y_1 - Y_2) = Y_1^2 - Y_2^2 = q'.$$

On a donc $q \simeq q'$.

Remarque 2.3. *La définition de l'équivalence signifie simplement que l'expression de q' dans une base $(e_i)_{1<i<n}$ est identique à l'expression de q dans la base $(\phi(e_i))_{(1<i<n)}$.*

Corollaire 2.1. *Soit q une forme quadratique sur un espace E de dimension n, il existe un n-uplet $(a_i)_{1 \leq i \leq n} \in \mathbb{K}^n$ tel que :*

$$q \simeq \langle a_1, \ldots, a_n \rangle.$$

De manière équivalente, tout espace quadratique (de dimension finie) admet une base orthogonale.

Démonstration. Par ([4] Th L, p.118) il existe une base orthogonale de E pour q. À la forme quadratique q est associée une unique classe de congruence de matrices symétriques (celle des $\mathrm{mat}_\beta(f)$ où β base de E), il existe donc une matrice diagonale $D(a_1, \ldots, a_n)$ dans cette classe. Par conséquent $q \simeq \langle a_1, \ldots, a_n \rangle$. □

2.3 Classification des formes quadratiques

On notera par la suite f la forme polaire associée à la forme quadratique q.

Définition 2.6. *Soit E un K-espace vectoriel et f une forme bilinéaire symétrique sur E. On considère l'application $\Phi : E \to E^*$ définie par :*

$$\forall y \in E, \ \Phi(y) = \phi_y \ \textit{où} \ \forall x \in E \ \phi_y(x) = f(x, y).$$

*Si Φ est injective, on dit que f est **non dégénérée**.*

Remarque 2.4. *D'après la définition précédente, f est non dégénérée si et seulement si :*

$$\forall x \in E, \quad f(x, y) = 0 \Longrightarrow y = 0.$$

Cela signifie que si pour un certain $y \in E$, on a $f(x, y) = 0$ pour tout $x \in E$ alors $y = 0$.

Définition 2.7. *Soient E un $\mathbb{K}$-espace vectoriel et f une forme bilinéaire symétrique sur E. Soit A une partie non vide de E, on définit l'orthogonal de A, par rapport à la forme bilinéaire f, noté $A^\perp$ par :*

$$\forall y \in E, \quad y \in A^\perp \text{ si } f(x,y) = 0 \text{ pour tout } x \in A.$$

Remarque 2.5. *Soit (E,q) un espace quadratique, on dit qu'une forme quadratique est non dégénérée lorsque sa forme polaire est non dégénérée, ce qui est équivaut à dire que $\mathrm{Ker}(q) = (0)$. On dit que q est **régulière**, ou que (E,q) est **régulier**, lorsque q est non dégénérée. Par ce qui précède, q régulière équivaut à $\mathrm{rg}(q) = \dim E$.*

Proposition 2.1. *Soient E un $\mathbb{K}$-espace vectoriel et f une forme bilinéaire symétrique sur E, alors pour tout sous-espace vectoriel F de E on a :*
- $\dim(F) + \dim(F^\perp) \geq \dim(E)$;
- *si de plus f est non dégénérée alors on a l'égalité.*

Démonstration. Les assertions sont démontrées dans ([4], Th I, page 117). □

Exemple 2.3. *Même si f est non dégénérée, on n'a pas toujours $E = F \bigoplus F^\perp$. Prenons par exemple $E = \mathbb{R}^2$, muni de la forme bilinéaire f définie par :*

$$\forall (x,y) \in E^2, \quad f(x,y) = x_1y_1 - x_2y_2.$$

Soient (e_1, e_2) la base canonique de E et $A = \mathrm{mat}_{(e_1,e_2)}(f)$, alors on a :

$$A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Donc $\det(A) = -1 \neq 0$, par suite f est non dégénérée.
Soit $F = \mathrm{vec}(e_1 + e_2)$ et soit $y \in E$, avec $y = (y_1, y_2)$; alors on a :

$$y \in F^\perp \iff f(e_1 + e_2, y) = 0 \iff y_1 - y_2 = 0 \iff y \in F.$$

Donc $F = F^\perp$.

Définition 2.8. *Soient E un $\mathbb{K}$-espace vectoriel et f une forme bilinéaire symétrique sur E.*
- *On dit que deux vecteurs x et y dans E sont **orthogonaux**, si $f(x,y) = 0$.*
- *On dit qu'un vecteur $x \in E$ est **isotrope**, si $f(x,x) = 0$.*
- *On dit qu'un sous espace vectoriel F de E est **isotrope** si $F \cap F^\perp \neq 0$*
- *On dit que F est **totalement isotrope** si $F \subseteq F^\perp$*

Partie Régulière L'étude des formes bilinéaires symétriques se ramène à l'étude des formes non dégénérées en quotientant E par le noyau des formes concernées. Ceci se fait via la construction de la partie régulière d'une forme quadratique que nous rappelons ci-dessous.
Soit f une forme bilinéaire symétrique ; pour tout $(x,y) \in E^2$ et pour tout $(x_0, y_0) \in \mathrm{Ker}(f)^2$, on a :

$$f(x + x_0, y + y_0) = f(x,y) + f(x,y_0) + f(x_0, y + y_0) = f(x,y).$$

Ainsi $f(x,y)$ ne dépend pas du choix du représentant des classes de x et y dans l'espace quotient $E/\mathrm{Ker}(f)$. On peut donc définir l'application

$$\bar{b} : E/\mathrm{Ker}(b) \times E/\mathrm{Ker}(b) \to \mathbb{K}$$

telle que :

$$\forall (x,y) \in E^2, \quad \bar{b}(\bar{x}, \bar{y}) = b(x,y).$$

Il s'agit bien d'une forme bilinéaire symétrique sur $E/\mathrm{Ker}(b)$, elle est de plus non dégénérée par construction. Comme $E/\mathrm{Ker}(b)$ est de dimension finie, la forme $\bar{b}$ est régulière.

L'application $\bar{b}$ est appelé la **partie régulière** de b.

Définition 2.9. *On appelle* ***partie régulière*** *de q notée $\bar{q}$, la forme quadratique associée à $\bar{b}$:*

$$\forall x \in E, \;\; \bar{q}(\bar{x}, \bar{y}) = q(x, y).$$

Définition 2.10. *Soient b et b' deux formes bilinéaires symétriques sur les espaces vectoriels E et F. On appelle somme orthogonale extérieure de b et b', notée $b \perp b'$, la forme bilinéaire symétrique définie par :*

$$b \perp b' \; : \; \begin{cases} (E \times F) \times (E \times F) \to \mathbb{K} \\ ((x, x'), (y, y')) \to b(x, y) + b'(x', y'). \end{cases}$$

Proposition 2.2. *Soit (E, b) un espace bilinéaire tel que $E = A \overset{\perp}{\oplus} B$, alors :*

$$b \simeq b_A \perp b_B.$$

Démonstration. Considérons l'application $\phi : A \times B \to E$ définie telle que $\phi(x, y) = x + y$ Cette application est un isomorphisme d'espaces vectoriels. Pour tout couple $(x, x') \in A \times B$ et $(y, y') \in A \times B$ on a :

$$\begin{aligned} b_A \perp b_B((x, x'), (y, y')) &= b_A(x, y) + b_B(x', y'). \\ &= b(x, y) + b(x', y'). \\ &= b(x + y, x' + y') \\ &= b(\phi(x, y), \phi(x', y')), \end{aligned}$$

ce qui prouve $b \simeq b_A \perp b_B$. □

Définition 2.11. *Soient (E, b) et (F, b') deux espaces bilinéaires symétriques et q, q' les formes quadratiques associées. La forme quadratique associée à $b \perp b'$, notée $q \perp q'$, est appelée la somme directe orthogonale des formes quadratiques q et q' et vérifie pour tout $(x, y) \in E \times F$:*

$$(q \perp q')(x, y) = (b \perp b')((x, y), (x, y)) = b(x, x) + b'(y, y) = q(x) + q'(y).$$

Définition 2.12. *Soit (E, q) un espace quadratique régulier. Si β est une base de E on a $\det(\mathrm{mat}_\beta(f)) \in \mathbb{K}^*$ et on peut définir (voir après la Remarque 2.2) le* ***déterminant de*** *q en posant*

$$\det(q) = \textit{classe de } \det(\mathrm{mat}_\beta(f)) \textit{ dans } \mathbb{K}^*/(\mathbb{K}^*)^2.$$

Le lemme qui suit est évident par définition de la congruence des matrices.

Lemme 2.1. *Soient q, q' deux formes quadratiques régulières équivalentes, alors $\det(q) = \det(q')$.*

3 Chapitre III : Théorème de Witt

3.1 Isotropie et plan quadratique

On étudie ici la notion d'isotropie.

Proposition 3.1. *Soit (E, q) un espace quadratique de dimension finie. Si q est anisotrope, alors q est régulière.*

Démonstration. Démontrons le résultat par l'absurde. Notons f la forme polaire associée à q et supposons que q est dégénérée. Il existe alors $x \in E$ non nul tel que $f(x, y) = 0$ pour tout y dans E, donc en particulier pour $y = x$ on a $q(x) = f(x, x) = 0$. Comme q est anisotrope ceci est absurde. □

Définition 3.1. *On appelle* ***cône isotrope*** *de q l'ensemble :*

$$Co(q) = \{x \in E : q(x) = 0\}.$$

Définition 3.2. *Un plan quadratique est dit* ***hyperbolique*** *lorsqu'il est isomorphe au plan quadratique $(\mathbb{K}^2, q : (X, Y) \mapsto XY)$.*

Théorème 3.1. *Les plans hyperboliques sont les plans quadratiques réguliers isotropes.*

Démonstration. ($\Longrightarrow$) Il est clair qu'un plan hyperbolique est un espace quadratique régulier isotrope.
($\Longleftarrow$) Soit (P, q) un plan quadratique régulier isotrope. Fixons un vecteur isotrope $x_0 \neq 0$ de ce plan. Soit b la forme polaire de q ; puisque b est non dégénérée, il existe $x \in E$ tel que $b(x_0, x) = 1/2$. Si $\lambda \in \mathbb{K}$ il vient $q(\lambda x_0 + x) = \lambda + q(x)$. Donc pour $\lambda_0 = -q(x)$ le vecteur $x_1 = \lambda_0 x_0 + x$ est isotrope tel que $b(x_0, x_1) = b(x_0, x) = 1/2$. Dans la base (x_0, x_1) de E la forme q s'écrit $(X, Y) \mapsto XY$ comme voulu □

Pour démontrer un théorème caractérisant les plans hyperboliques nous utiliserons le principe, dit « de complétion », suivant.

Proposition 3.2 (Principe de complétion)**.** *Soient (E, q) un espace quadratique et $(a_1, \cdots, a_p) \in (\mathbb{K}^*)^p$. On suppose qu'il existe un sous espace $F \subset E$ de dimension p tel que $q_F \simeq \langle a_1, \cdots, a_p \rangle$. Alors il existe $(b_{p+1}, \ldots, b_n) \in \mathbb{K}^{n-p}$ tel que :*

$$q \simeq q_F \perp \langle b_{p+1}, \cdots, b_n \rangle \simeq \langle a_1, \cdots, a_p, b_{p+1}, \cdots, b_n \rangle.$$

Démonstration. L'hypothèse implique que le sous-espace quadratique (F, q_F) est régulier ; on a donc $E = F \bigoplus F^\perp$. Si $\mathcal{F}$ est une base de F dans laquelle la matrice de q_F est $\mathrm{diag}(a_1, \cdots, a_p)$ on obtient le résultat en complétant $\mathcal{F}$ par une base $\mathcal{F}'$ de $F^\perp$ telle que la matrice de $q_{F'}$ est $\mathrm{diag}(b_{p+1}, \cdots, b_n)$. □

Théorème 3.2 (caractérisation des plans hyperboliques)**.** *Soit (P, q) un plan quadratique régulier, les conditions suivantes sont équivalentes.*

(1) *La forme quadratique q est hyperbolique ;*

(2) *la forme quadratique q est isotrope ;*

(3) $q \simeq \langle 1, -1 \rangle$ *;*

(4) $q \simeq \langle a, -a \rangle$ *pour* $a \in \mathbb{K}^*$ *;*

(5) *q est équivalente à $(x, y) \mapsto xy$;*

(6) *q est représentée par la matrice* $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ *;*

(7) $\det(q) = -1$ *dans* $(\mathbb{K}^*/\mathbb{K}^{*2})$.

Démonstration. (1) $\Longleftrightarrow$ (2). Cf. Théorème 3.1.

(1) $\Longleftrightarrow$ (3) et (4). Le vecteur $(1, 1)$ est un vecteur isotrope pour les deux formes régulières $\langle 1, -1 \rangle$ et $\langle a, -a \rangle$ qui sont isotropes.

(1) $\Longleftrightarrow$ (6). C'est immédiat, car la matrice $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ représente la forme $(x, y) \mapsto 2xy$ qui est régulière et isotrope dans la base canonique de $\mathbb{K}^2$.

(1) $\Longrightarrow$ (7). Supposons que q est hyperbolique. Elle est donc équivalente à la forme $\langle 1, -1 \rangle$, d'où $\det(q) = -1$ dans $\mathbb{K}^*/(\mathbb{K}^*)^2$.

(7) $\Longrightarrow$ (1). Comme q est régulière elle est non nulle. Soient $a \in \mathbb{K}^*$ et $x \neq 0$ tels que $q(x) = a$. Alors $q_{|vect(x)} \simeq \langle a \rangle$ où $vect(x)$ est une droite de E. En utilisant le principe de complétion et l'hypothèse sur le déterminant on a :

$$q \simeq q_{|vect(x)} \perp \langle -a \rangle \simeq \langle a \rangle . \langle -a \rangle \simeq \langle a, -a \rangle.$$

Donc q est hyperbolique. □

3.2 Espaces quadratiques hyperboliques

Définition 3.3. *On appelle* ***espace quadratique hyperbolique*** *tout espace quadratique isomorphe à une somme orthogonale (finie) de plans hyperboliques.*

Définition 3.4. *Soit V un $\mathbb{K}$-espace vectoriel de dimension finie n et V^* son dual. On définit l'application $\mathbb{H}(V)$ par :*

$$\mathbb{H}(V) \ : \ \begin{cases} V \times V^* \to \mathbb{K} \\ (x, f) \mapsto 2f(x). \end{cases}$$

Alors, $\mathbb{H}(\mathbb{V})$ est une forme quadratique de forme polaire associée

$$b \ : \ \begin{cases} (V \times V^*) \times (V \times V^*) \to \mathbb{K} \\ ((x, f), (x', f')) \mapsto f(x') + f'(x). \end{cases}$$

On dit que $\mathbb{H}(V)$ est la forme hyperbolique associée à V.

En identifiant V avec $V \times \{0\}$ et V^* avec $\{0\} \times V^*$, on peut voir V et V^* comme deux espaces supplémentaires dans $V \times V^*$. On a donc $V \times V^* = V \bigoplus V^*$ avec $q_V = q_{V^*} = 0$.

Par concaténation d'une base $(e_1, \ldots, e_n)$ de V avec la base duale $(e_1^*, \ldots, e_n^*)$ de V^* on obtient une base $(e_1, \ldots, e_n, e_1^*, \ldots, e_n^*)$ de $V \times V^*$ dans laquelle la matrice de la forme quadratique $\mathbb{H}(V)$ s'écrit :

$$\begin{pmatrix} 0 & I_n \\ I_n & 0 \end{pmatrix}.$$

Remarquons que si l'on pose $P_j = \mathrm{vec}\{e_j, e_j^*\}$, on obtient :

$$V \times V^* = P_1 \perp \cdots \perp P_n \ \text{ avec } q_{P_j} \simeq \langle 1, -1 \rangle.$$

Théorème 3.3. *Soit (E, q) un espace quadratique de dimension $2n$. Les conditions suivantes sont équivalentes :*

(1) *la forme quadratique q est hyperbolique ;*

(2) $q \simeq n.\langle 1, -1 \rangle$ *;*

(3) $q \simeq \phi \perp (-\phi)$ *pour une forme régulière ϕ ;*

(4) *la matrice* $\begin{pmatrix} 0 & I_n \\ I_n & 0 \end{pmatrix}$ *représente q ;*

(5) $q \simeq \mathbb{H}(V)$ *où V est un $\mathbb{K}$-espace vectoriel de dimension n.*

Démonstration. (1) $\Longrightarrow$ (2). Comme q est hyperbolique, elle s'écrit comme une somme orthogonale n plans quadratiques et chacun de ces plans est isomorphe à $(\mathbb{K}^2, \langle 1, -1 \rangle)$ d'où l'assertion.

(2) $\Longrightarrow$ (1). Par définition d'une forme hyperbolique.

(2) $\Longrightarrow$ (3). On a $q \simeq n.\langle 1,-1\rangle \simeq n.\langle 1\rangle \perp n\langle -1\rangle$. Si $\phi = n.\langle 1\rangle$, on a donc $q \simeq \phi\perp(-\phi)$ avec q régulière.

(2) $\Longleftarrow$ (3). Soit ϕ une forme quadratique régulière telle que $q \simeq \phi\perp(-\phi)$. Comme ϕ est régulière on sait que $\phi \simeq \langle a_1,\dots,a_n\rangle$ avec $a_i \neq 0$ pour tout i. D'où :

$$\begin{aligned}\phi\perp(-\phi) &\simeq \langle a_1,\dots,a_n\rangle\perp\langle -a_1,\dots,-a_n\rangle.\\ &\simeq \langle a_1,\dots,a_n,-a_1,\dots,-a_n\rangle.\\ &\simeq \langle a_1,-a_1\rangle\perp\dots\perp\langle a_n,-a_n\rangle.\\ &\simeq \langle 1,-1\rangle\perp\dots\perp\langle 1,-1\rangle.\\ &\simeq n.\langle 1,-1\rangle.\end{aligned}$$

(4) $\Longrightarrow$ (5). Supposons q représentée par la matrice $\begin{pmatrix}0 & I_n\\ I_n & 0\end{pmatrix}$ dans une base. Si V est un espace vectoriel de dimension n, on a vu ci-dessus que $\mathbb{H}(V)$ est aussi représentée par la même matrice, d'où $q \simeq \mathbb{H}(V)$.

(5) $\Longleftrightarrow$ (4). Si pour un V de dimension n on a $q \simeq \mathbb{H}(V)$, alors comme $\mathbb{H}(V)$ est représentée par $\begin{pmatrix}0 & I_n\\ I_n & 0\end{pmatrix}$, la forme q l'est également par congruence.

(5) $\Longrightarrow$ (1). Comme (5) $\Leftrightarrow$ (4), q est représentée par la matrice $\begin{pmatrix}0 & I_n\\ I_n & 0\end{pmatrix}$ qui est congruente à la matrice diagonale par blocs $D(K,\dots,K)$ avec K=$\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$. Or, on sait que cette matrice représente la forme quadratique $q' = \underbrace{q_1\perp\dots\perp q_1}_{n fois}$ où $q_1(x,y) = 2xy$ pour tous $x, y \in \mathbb{K}$. On a donc $q \simeq q'$ avec q' hyperbolique.

(1) $\Longrightarrow$ (5). Supposons q hyperbolique. Par définition, q est (isomorphe à une) somme orthogonale de n formes hyperboliques de dimension 2. Ainsi :

$$q \simeq q_1\perp\dots\perp q_1 \quad \text{où} \quad (x,y) \in \mathbb{K}^2 \mapsto 2xy.$$

Par conséquent q est représentée par la matrice $D(K,\dots,K)$, qui est congruente à $\begin{pmatrix}0 & I_n\\ I_n & 0\end{pmatrix}$. Le résultat voulu en découle. □

Exemple 3.1. *Le déterminant pfaffien intervient dans l'étude des matrices antisymétriques. On note* Alt_4 *le sous-espace de* $M_4(\mathbb{K})$ *formé des matrices antisymétriques; c'est un espace vectoriel de dimension* 6 *sur* $\mathbb{K}$*. On introduit le Pfaffien d'une matrice antisymétrique; il s'agit de l'application :*

$$\mathrm{Pf} : \mathrm{Alt}_4 \to \mathbb{K}, \quad \mathrm{Pf}(A) = af + cd - be$$

où

$$A = \begin{pmatrix}0 & a & b & c\\ -a & 0 & d & e\\ -b & -d & 0 & f\\ -c & -e & -f & 0\end{pmatrix} \in \mathrm{Alt}_4.$$

On a $\det(A) = \mathrm{Pf}(A)^2$ *et l'espace quadratique* $(\mathrm{Alt}_4, \mathrm{Pf})$ *est hyperbolique.*

Définition 3.5. *Soit* (E,q) *un espace quadratique de dimension paire*[1]*. On appelle* ***lagrangien*** *de* (E,q) *tout sous-espace vectoriel totalement isotrope de* E *de dimension* $\frac{\dim(E)}{2}$*.*
Deux lagrangiens F *et* G *de* E *sont dits* ***transverses*** *lorsque* $F \cap G = \{0\}$*, ce qui équivaut à dire* $E = F \bigoplus G$*.*

1. Insistons sur le fait que l'on ne parle de lagrangien que pour des espaces de dimension paire.

Définition 3.6. *Un sous-espace totalement isotrope de (E, q) est dit **maximal** lorsqu'il n'est pas strictement inclus dans un autre sous-espace totalement isotrope.*

Notation 3.1. *Dans toute la suite :*
- *un SETI désigne un sous-espace totalement isotrope.*
- *un SETIM désigne un sous-espace totalement isotrope maximal.*

Remarque 3.1. *Si un espace quadratique régulier contient un SETI non nul, alors il contient un plan hyperbolique.*

Théorème 3.4 (principe de gonflement hyperbolique)**.** *Soit F un lagrangien d'un espace quadratique régulier (E, q) alors :*

(i) *la forme q est hyperbolique ;*

(ii) *il existe un lagrangien de E transverse à F ;*

(iii) *toute base de F peut être complétée en une base hyperbolique.*

Démonstration. (i) Décomposons E en somme directe de deux sous-espaces $E = F \oplus G$ tels que $\dim F = \dim G = n$. Soit $\beta = (g_1, \ldots, g_n)$ une base orthogonale de G, cf. Corollaire 2.1, et posons $D(a_1, \ldots, a_n) = Mat_\beta(q_G)$. Considérons l'application linéaire

$$\phi \; : \; \begin{cases} F \to G^* \\ x \mapsto b_q(x, -)_{|G}. \end{cases}$$

où b_q est la forme polaire associée à q_G. Montrons que ϕ est injective. Soit $x \in \mathrm{Ker}(\phi)$; alors, $x \in G^\perp$ par définition et $x \in F^\perp$ car F est un SETI. Il vient donc $x \in F^\perp \cap G^\perp = (F+G)^\perp = E^\perp = 0$, d'où $\mathrm{Ker}(\phi) = \{0\}$. Comme $\dim F = \dim G$, l'application ϕ est un isomorphisme. Définissons la base $(f_1, \ldots, f_n)$ de F par $\phi(f_i) = g_i^*$ pour tout i, j ; on a donc $b_q(f_i, g_j) = \delta_{i,j}$ pour $1 \leq i, j \leq n$. On a ainsi construit une base $(f_1, \ldots, f_n, g_1, \ldots, g_n)$ de E telle que q est représentée dans cette base par :

$$\begin{pmatrix} 0 & I_n \\ I_n & D(a_1, \ldots, a_n). \end{pmatrix}$$

Soit $P_k = \mathrm{vec}(f_k, g_k)$ pour $k \in [1, n]$; alors la matrice de q_{p_k} est représentée par $\begin{pmatrix} 0 & 1 \\ 1 & a_k \end{pmatrix}$. On reconnaît ici une matrice qui représente une forme hyperbolique et puisque $E = \overset{\perp}{\bigoplus} P_k$, la forme q est hyperbolique.

ii) Montrons qu'il existe un lagrangien G de E qui est transverse à F, *i.e.* $F \cap G = 0$. Prenons dans chacun des plans hyperboliques P_k précédents un vecteur y_k isotrope et non colinéaire à f_k. La famille $(y_1, \cdots, y_n)$ est libre et les vecteurs y_k sont isotropes deux à deux orthogonaux. Cette famille engendre un sous-espace vectoriel G de E tel que : G est un SETI, $\dim G = \frac{\dim E}{2} = n$ et $F \cap G = 0$. D'où le résultat.

iii) D'après ii) il existe un lagrangien de E transverse à F que l'on note G. Soit $B = (e_1, \cdots, e_n)$ une base quelconque de F. Comme en i) on voit que l'application

$$\phi \; : \; \begin{cases} G \to F^* \\ x \mapsto f_q(x, -)_{|F}. \end{cases}$$

est un isomorphisme. Notons $(g_1, \cdots, g_n)$ les antécédents de $B^* = (e_1^*, \cdots, e_n^*)$ par ϕ ; c'est une base de G et l'on a $f_q(g_i, e_j) = \delta_{i,j}$, pour tous i, j. En complétant B par $(g_1, \cdots, g_n)$ on obtient ainsi une base hyperbolique $(e_1, \cdots, e_n, g_1, \cdots, g_n)$ de E. □

Nous utiliserons à plusieurs reprises le principe de gonflement généralisé qui suit.

Théorème 3.5 (principe de gonflement hyperbolique, cas général)**.** *Soient (E, q) un espace quadratique régulier et F un SETI de E. Il existe un sous-espace hyperbolique H de (E, q) tel que F est un lagrangien de H.*

Démonstration. Soit G un supplémentaire quelconque de F dans $F^\perp$, i.e. $F^\perp = F \bigoplus G$, et posons $H = G^\perp$. De $G \subset F^\perp$ il découle que $F = F^{\perp\perp} \subset H = G^\perp$. En outre, de $\dim H = \dim E - \dim G$ on tire facilement que $\dim H = 2 \dim F$.

Compte tenu du théorème précédent, il reste à montrer que H est régulier, c'est-à-dire que $G \cap G^\perp = \{0\}$. On observe que $G \cap G^\perp \subset F^\perp \cap G^\perp = (F + G)^\perp = F^{\perp\perp} = F$. On obtient ainsi $G \cap G^\perp \subset F \cap G = \{0\}$, comme voulu. □

Définition 3.7. *Un scalaire $a \in \mathbb{K}^*$ est représenté par q lorsqu'il existe $x \in E$ tel que $a = q(x)$. On appelle domaine de la forme quadratique, noté $D(q)$, l'ensemble des valeurs non nulles prises par q. La forme q est dite universelle lorsque $D(q) = \mathbb{K}^*$.*

Proposition 3.3. *Soit (E, q) un espace quadratique régulier isotrope. Alors, q est universelle.*

Démonstration. Supposons que $\dim(E) = 2$. Alors q est une forme régulière hyperbolique ; elle est équivalente à la forme quadratique $q' : (x, y) \to xy$ qui est universelle car tout élément non nul de E est représentable en prenant par exemple $y = 1$. Donc q est universelle. Supposons maintenant que $\dim(E) > q$ alors comme q est isotrope il existe $x \neq 0$ tel que $q(x) = 0$, donc $vect(x)$ est un espace totalement isotrope, par le principe de gonflement hyperbolique généralisé, on peut trouver un plan hyperbolique P tel que la restriction de q dans P soit hyperbolique et donc d'après le premier cas où la dimension est égale à 2 elle serai donc universelle. Ainsi $q_{|P}$ est universelle alors q universelle. □

Théorème 3.6 (principe de représentation)**.** *Soit (E, q) un espace quadratique régulier et $a \in \mathbb{K}^*$. Alors a est représenté par q si et seulement si la forme $\phi = q \perp \langle -a \rangle$ est isotrope*[2]*.*

Démonstration. Soit ϕ la forme quadratique régulière sur $E \times \mathbb{K}$ définie par $\phi = q \perp \langle -a \rangle$, i.e. $\phi : E \times \mathbb{K} \to \mathbb{K}$ est définie par $\phi(x, \lambda) = q(x) + \langle -a \rangle \lambda = q(x) - a\lambda^2$. Si a est représenté par q, il existe $x \neq 0$ tel que $q(x) = a$, donc $\phi(x, 1) = q(x) - a = 0$ et ϕ est isotrope.

Réciproquement, supposons que ϕ est isotrope ; il existe donc $(x, \lambda) \neq (0, 0)$ tel que $\phi(x, \lambda) = 0$.

Si $\lambda \neq 0$, de $q(x) - a\lambda^2 = 0$ on tire $q(\frac{x}{\lambda}) = a$, ce qui montre que a est représenté par q.

Si $\lambda = 0$ on a nécessairement $x \neq 0$ et $\phi(x, \lambda) = \phi(x, 0) = q(x) = 0$, donc q est isotrope. Comme (E, q) est régulier et isotrope, q est universelle par la proposition précédente. □

Exemple 3.2. *Considérons par exemple la forme quadratique diagonale q définie sur $\mathbb{Q}^2$ par $q(x, y) = x^2 + 5y^2$. Si l'entier 39 est représenté par q, il existe $(x_0, y_0) \in (Q^2)$ tel que :*

$$q(x_0, y_0) = x_0^2 + 5y_0^2 = 39, \quad \textit{soit } x_0^2 + 5y_0^2 - 39 = 0.$$

La forme diagonale $\langle 1, 5, -39 \rangle \simeq q \perp \langle -39 \rangle$ est alors isotrope.

Remarque 3.2. *Il faut souligner que deux formes quadratiques régulières équivalentes représentent les mêmes éléments.*

On peut supposer que q_1 et q_2 sont deux formes quadratiques régulières équivalentes sur $E = \mathbb{K}^n$. Soient $a \in \mathbb{K}$ tel que q_1 représente a et $X \in \mathbb{K}^n$ tel que $q_1(X) = a$. Soit β une base de E. Comme $q_1 \simeq$

2. Ainsi, le fait qu'un scalaire a est représenté par q implique l'isotropie de la forme q $\perp \langle -a \rangle$ et non pas de q

q_2 il existe une matrice inversible P telle que $\mathrm{mat}_\beta(q_1) = {}^tP\,\mathrm{mat}_\beta(q_2)P$. Puisque ${}^tX\,\mathrm{mat}_\beta(q_1)X = a$ on obtient :

$$ {}^tX\,{}^tP\,\mathrm{mat}_\beta(q_2)PX = {}^t\big(PX\big)\,\mathrm{mat}_\beta(q_2)\big(PX\big) = a.$$

Donc $q_2(PX) = a$, q_2 représente aussi a.

Nous allons terminer cette section par quelques propriétés des formes quadratiques lorsque $\mathbb{K} = \mathbb{F}_q$ est un corps fini [3] de cardinal q. Rappelons que $(\mathbb{K}^*)^2$ est le groupe multiplicatif des carrés de $\mathbb{K}^*$. Le lemme suivant est classique.

Lemme 3.1. *Le groupe $\mathbb{F}_q/(\mathbb{F}_q^*)^2$ est d'ordre 2 et on a :*

$$-1 \in (\mathbb{F}_q^*)^2 \iff (-1)^{\frac{q-1}{2}} = 1 \ \textit{i.e.}\ \ q \equiv 1 \pmod 4.$$

Démonstration. L'application $x \mapsto x^2$ est un morphisme de $\mathbb{F}_q^*$ dans $\mathbb{F}_q^*$ d'image $(\mathbb{F}_q^*)^2$ et de noyau $\{\pm 1\}$. Il en découle que $\mathbb{F}_q^*/\{\pm 1\} \cong (\mathbb{F}_q^*)^2$ puis $\big|\mathbb{F}_q/(\mathbb{F}_q^*)^2\big| = 2$.

Considérons le morphisme $\phi : x \mapsto x^{\frac{q-1}{2}}$ de $\mathbb{F}_q^*$ dans $\mathbb{F}_q^*$. On a clairement $\phi(x) = 1$ pour tout $x \in (\mathbb{F}_q^*)^2$, donc $(\mathbb{F}_q^*)^2 \subset \mathrm{Ker}(\phi)$. Puisque $\big|\mathbb{F}_q/(\mathbb{F}_q^*)^2\big| = 2$ il s'ensuit que $\mathrm{Ker}(\phi) = (\mathbb{F}_q^*)^2$ ou $\mathbb{F}_q^*$. Si $\mathrm{Ker}(\phi) = \mathbb{F}_q^*$ il vient $x^{\frac{q-1}{2}} = 1$ pour tout $x \in \mathbb{F}_q^*$, ce qui entraîne $|\mathbb{F}_q^*| \leq \frac{q-1}{2}$ et une contradiction. Par conséquent $-1 \in (\mathbb{F}_q^*)^2$ si et seulement si $\phi(-1) = (-1)^{\frac{q-1}{2}} = 1$. □

Théorème 3.7. *Soit (E, q) un espace quadratique sur $\mathbb{F}_q$.*

(1) *Si $\mathrm{rg}(q) \geq 2$, alors q est universelle.*

(2) *Si q est régulière et $n = \dim E \geq 3$, alors q est isotrope.*

(3) *Si q est régulière et $\dim E = 4$, alors q est hyperbolique.*

Démonstration. Rappelons que $|(\mathbb{F}_q^*)^2| = (q-1)/2$, cf. lemme ci-dessus, donc le cardinal de l'ensemble $(\mathbb{F}_q)^2$ des carrés de $\mathbb{F}_q$ est $(q+1)/2$.

(1) Quitte à diagonaliser la forme quadratique et multiplier par un scalaire il suffit de prouver l'universalité de la forme $\langle 1, \alpha\rangle$ avec $\alpha \in \mathbb{F}_q^*$. Soit $a \in \mathbb{F}_q^*$. Les ensembles $(\mathbb{F}_q)^2$ et $a - \alpha(\mathbb{F}_q)^2$ sont de cardinal $(q+1)/2$; s'il étaient disjoints le corps $\mathbb{F}_q$ contiendrait $2 \times (q+1)/2 = q+1$ éléments, ce qui est absurde. On en déduit qu'il existe $x, y \in \mathbb{F}_q$ tels que $x^2 + \alpha y^2 = a$.

(2) Diagonalisons la forme q et supposons $q = \langle a_1, a_2, \ldots, a_n\rangle$ avec $a_j \in \mathbb{F}_q^*$ pour tout j. Par (1) on sait que la forme $\langle a_1, a_2\rangle$ est universelle, il en est donc de même pour $q_1 = \langle a_1, a_2, \ldots, a_{n-1}\rangle$ (car $n \geq 3$). Par le principe de représentation du Théorème 3.6, on obtient que $q \simeq q_1 \perp \langle a_n\rangle$ est universelle.

(3) Puisque q est isotrope, par gonflement hyperbolique on a $q \simeq \langle 1, -1\rangle \perp q_1$ avec q_1 régulière de dimension 2. Mais $\det(q_1) = -\det(q) = -1$, donc par la caractérisation des plans hyperboliques la forme q_1 est hyperbolique. D'où le résultat cherché. □

3.3 Théorème de Witt

Dans cette section nous exposons le résultat fondamental de Witt sur lequel est basé l'ensemble de la théorie algébrique des formes quadratiques. Il s'avère qu'il y a équivalence entre deux résultats : le théorème de simplification et celui de prolongement.

3. On espère qu'il n'y aura pas de confusion entre le q du cardinal de $\mathbb{K}$ et les formes quadratiques notées q.

Théorème 3.8 (Simplification de Witt). *Soit q, ϕ et ψ trois formes quadratiques régulières, alors :*

$$q \perp \phi \simeq q \perp \psi \Longrightarrow \phi \simeq \psi.$$

Version matricielle de de ce résultat. *Soient A, B_1 et B_2 trois matrices symétriques inversibles, respectivement dans $M_p(\mathbb{K})$, $M_n(\mathbb{K})$ et $M_n(\mathbb{K})$. Alors :*

$$\begin{pmatrix} A & 0 \\ 0 & B_1 \end{pmatrix} \simeq \begin{pmatrix} A & 0 \\ 0 & B_2 \end{pmatrix} \Longrightarrow B_1 \simeq B_2.$$

Théorème 3.9 (Prolongement de Witt). – Version interne. *Soient (E, q) un espace quadratique régulier, F un sous-espace vectoriel régulier de E et $u : F \to E$ une isométrie. On peut alors prolonger u en un automorphisme orthogonal de E.*

– Version externe. *Soient (E_1, q_1) et (E_2, q_2) deux espaces quadratiques réguliers isomorphes, F un sous-espace vectoriel régulier de E_1 et $u : F \to E_2$ une isométrie. On peut prolonger u en une isométrie (bijective) de E_1 sur E_2.*

Lemme 3.2. *La version interne et la version externe du théorème de prolongement sont équivalentes.*

Démonstration. Avec les notations du Théorème 3.9, choisissons une isométrie $v : E_1 \xrightarrow{\simeq} E_2$. Par composition on obtient une isométrie $v^{-1} \circ u : F \hookrightarrow E_1$. Par la version interne du théorème on peut prolonger v en un automorphisme orthogonal $w : E_1 \xrightarrow{\simeq} E_2$. Alors, $v \circ w$ est une isométrie (composition de deux isométries) de E_1 sur E_2 qui prolonge u d'oú la version externe du théorème. □

Démontrons l'équivalence entre le théorème de prolongement, Théorème 3.9, et le théorème de simplification, Théorème 3.8.

Démonstration. Supposons vrai le théorème de prolongement. Soient trois espaces quadratiques réguliers (E, q), (F, ϕ) et (G, ψ) tels que $q \perp \phi \simeq q \perp \psi$. Considérons $E = E \oplus \{0\}$ comme un sous-espace de $(E \oplus F, q \perp \phi)$. Alors l'injection naturelle, $x \mapsto x + 0 \in E \oplus G$, est une isométrie de (E, q) dans $(E \oplus G, q \perp \psi)$. Par le théorème de prolongement il existe une isométrie $f : E \overset{\perp}{\oplus} F \xrightarrow{\simeq} E \overset{\perp}{\oplus} G$ telle que $f(x) = x$ pour tout $x \in E$. Si $x \in F$, le vecteur $f(x)$ appartient à l'orthogonal de E dans $(E \oplus G, q \perp \psi)$, c'est-à-dire à G. On en déduit que f est une isométrie de (F, ϕ) sur (G, ψ).

Réciproquement, supposons prouvé le théorème de simplification et adoptons les notations du théorème de prolongement (version interne). Puisque F est régulier c'est aussi le cas pour $u(F)$ (qui est isomorphe à F), $F^\perp$ et $u(F)^\perp$. On a donc :

$$E = F \overset{\perp}{\oplus} F^\perp = u(F) \overset{\perp}{\oplus} u(F)^\perp.$$

Considérons maintenant les deux formes quadratiques $\phi = q_{F^\perp}$ et $\psi = q_{u(F)^\perp}$. Comme u est une isométrie on a $q_F \simeq q_{u(F)}$ et donc $q_F \perp \phi \simeq q_F \perp \psi$. Par le théorème de simplification on obtient $\phi \simeq \psi$, donc $(F^\perp, \phi) \simeq (u(F)^\perp, \psi)$. Soit $v : F^\perp \xrightarrow{\simeq} u(F)^\perp$ une isométrie. Le prolongement de u est est obtenu en recollant $u : F \xrightarrow{\simeq} F^\perp$ et $v : F^\perp \xrightarrow{\simeq} u(F)^\perp$: on obtient $\widetilde{u} : x + y \mapsto u(x) + v(y)$ pour $x \in F, y \in F^\perp$, tel que :

$$\widetilde{u} : \underbrace{F \overset{\perp}{\oplus} F^\perp}_{=E} \xrightarrow{\simeq} \underbrace{u(F) \overset{\perp}{\oplus} u(F)^\perp}_{=E}$$

Alors, $\widetilde{u} : E \xrightarrow{\simeq} E$ une isométrie bijective (i.e. un automorphisme orthogonal) qui prolonge u. Ainsi on a montré l'équivalence entre les deux théorèmes. □

La preuve du théorème de prolongement peut se réduire au cas où F est de dimension 1 en raisonnant comme suit.

– Dans ce cas le théorème de simplification est vrai lorsque $\dim E = 1$ et on en tire le théorème de simplification en toute généralité. En effet, si $q \simeq \langle a_1\rangle \perp \cdots \perp \langle a_n\rangle$ et $q \perp \varphi \simeq q \perp \psi$ comme dans le Théorème 3.8, on peut simplifier successivement par $\langle a_1\rangle, \ldots, \langle a_n\rangle$ (grâce au cas de la dimension 1) jusqu'à obtenir $\varphi \simeq \psi$.

– Comme le théorème de simplification est équivalent au théorème de prolongement, on aura le résultat cherché.

Montrons maintenant le théorème de prolongement lorsque F est de dimension 1. Pour ce faire nous aurons besoin du lemme suivant.

Lemme 3.3. *Soient x, y deux vecteurs anisotropes dans (E, q), tels que $q(x) = q(y)$ et $q(x-y) \neq 0$. Alors la réflexion de vecteur $x - y$ échange x et y.*

Démonstration. Soit f la forme bilinéaire symétrique associée à q, Il vient :

$$\begin{aligned} q(x-y) &= f(x-y, x-y). \\ &= f(x,x) - 2f(x,y) + f(y,y). \\ &= 2(f(x,x) - f(x,y)). \\ &= 2f(x, x-y). \end{aligned}$$

Puisque

$$s_x(y) = y - 2\frac{f(x,y)}{f(x,x)}x$$

on obtient :

$$\begin{aligned} s_{x-y}(x) &= x - 2\frac{f(x-y,x)}{q(x-y)}.(x-y) \\ &= x - (x-y) = y \end{aligned}$$

Ainsi la réflexion de vecteur $x - y$ permute x et y. □

Continuons la démonstration du prolongement en dimension 1.

Choisissons un vecteur non nul $x \in F$ (on a $q(x) \neq 0$ car $F = \mathbb{K}x$ est régulier). Si $u : F \to E$ est comme dans le Théorème 3.9, posons $y = u(x)$. Le but est de trouver un automorphisme orthogonal $f : E \to E$ tel que $f(x) = y$. Remarquons que $q(y) = q(u(x)) = f(u(x), u(x)) = f(x,x) = q(x)$. Donc d'après le lemme précédent, si $q(x-y) \neq 0$ alors s_{x-y} envoie x sur y. Si $q(x+y) \neq 0$ on a :

$$y \xrightarrow{s_{x+y}} -y \xrightarrow{s_y} y \ .$$

Or, on est toujours dans l'un de ces deux cas, car $q(x+y) + q(x-y) = 2q(x) + 2q(y) = 4q(x) \neq 0$. On peut donc prendre :

$$\begin{cases} f := s_{x-y} & \textit{si} \quad q(x-y) \neq 0. \\ f := s_{x+y} \circ s_y & \textit{si} \quad q(x+y) \neq 0. \end{cases}$$

Ceci termine la démonstration des différentes formes du théorème de Witt. □

Corollaire 3.1. *Soient $(a_1, \ldots, a_n) \in \mathbb{K}^n$ et deux p-uplets $(b_1, \ldots, b_p) \in \mathbb{K}^p$, $(c_1, \ldots, c_p) \in \mathbb{K}^p$. Alors :*

$$\langle a_1, \ldots, a_n, b_1, \ldots, b_p\rangle \simeq \langle a_1, \ldots, a_n, c_1, \ldots, c_p\rangle \implies \langle b_1, \ldots, b_p\rangle \simeq \langle c_1, \ldots, c_p\rangle. \qquad (1)$$

Démonstration. Pour $(a_1, \ldots, a_n) \in \mathbb{K}^n$ et $(b_1, \ldots, b_p) \in \mathbb{K}^p$, les formes quadratiques diagonales $\langle a_1, \ldots, a_n\rangle$ et $\langle b_1, \ldots, b_n\rangle$ sont représentées, respectivement, dans les bases canoniques de $\mathbb{K}^n$ et $\mathbb{K}^p$ par $D(a_1, \ldots, a_n)$ et $D(b_1, \ldots, b_n)$. La matrice $D(a_1, \ldots, a_n, b_1, \ldots, b_n)$ représente la forme $\langle a_1, \ldots, a_n\rangle \perp \langle b_1, \ldots, b_p\rangle$ et cette matrice est dans la classe de congruence de la matrice associée à la forme quadratique $\langle a_1, \ldots, a_n, b_1, \ldots, b_n\rangle$. On a donc :

$$\langle a_1, \ldots, a_n\rangle \perp \langle b_1, \ldots, b_p\rangle \simeq \langle a_1, \ldots, a_n, b_1, \ldots, b_p\rangle.$$

Soit maintenant $(c_1, \ldots, c_n) \in \mathbb{K}^p$, alors on a

$$\langle a_1, \ldots, a_n, b_1, \ldots, b_p\rangle \simeq \langle a_1, \ldots, a_n\rangle \perp \langle b_1, \ldots, b_p\rangle.$$

et de même

$$\langle a_1, \ldots, a_n, c_1, \ldots, c_p\rangle \simeq \langle a_1, \ldots, a_n\rangle \perp \langle c_1, \ldots, c_p\rangle.$$

De (1) on tire :

$$\langle a_1, \ldots, a_n\rangle \perp \langle b_1, \ldots, b_p\rangle \simeq \langle a_1, \ldots, a_n\rangle \perp \langle c_1, \ldots, c_p\rangle.$$

Par simplification de Witt cf. Théorème 3.8 il vient $\langle b_1, \ldots, b_p\rangle \simeq \langle c_1, \ldots, c_p\rangle$. □

La généralisation du théorème du prolongement consiste à s'affranchir de la règularité de F. Dans le cas général on considère un sous-espace vectoriel F quelconque de l'espace quadratique régulier (E, q).

Théorème 3.10 (Prolongement de Witt généralisé)**.** *Soit F un sous-espace vectoriel d'un espace quadratique règulier (E, q), et $u : F \mapsto E$ une isométrie. Alors u se prolonge en un automorphisme orthogonal de (E, q).*

Démonstration. Cas 1. On suppose F totalement isotrope. Alors $u(F)$ est aussi totalement isotrope car u est une isométrie. Par gonflement hyperbolique (généralisé) on peut trouver deux sous-espaces hyperboliques H_1 et H_2 de E tels que $F \subset H_1$ et $u(F) \subset H_2$ avec $\dim H_1 = \dim H_2 = 2 \dim F$. Choisissons des bases $B = (e_1, \cdots, e_p)$ de F et $B_u = (u(e)_1, \cdots, u(e_p))$ de $u(F)$. Par le troisième point du Théorèrme 3.4 on complète B en une base hyperbolique B_1 de H_1 et B_u en une base hyperbolique B_2 de H_2. L'unique injection linéraire $v : H_1 \hookrightarrow E$ envoyant B_1 sur B_2 prolonge u et est une isométrie. Ainsi par le Théorème 3.9, on peut prolonger v en un automorphisme orthogonal de (E, q).

Cas 2. Soit F quelconque. On choisit un supplémentaire G de $F \cap F^\perp$ dans F. Comme $F \cap F^\perp \subset F^\perp \subset G^\perp$ on a une somme directe orthogonale $F = G \perp (F \cap F^\perp)$. Montrons que G (et donc $G^\perp$) est régulier, c'est-à-dire que $G \cap G^\perp = \{0\}$. On remarque que

$$G \cap G^\perp \subset G^\perp \cap F = G^\perp \cap F^{\perp\perp} = (G + F^\perp)^\perp$$

et

$$F = G \oplus (F \cap F^\perp) \subset G + F^\perp \text{ implique } (G + F^\perp)^\perp \subset F^\perp.$$

Il s'ensuit $G \cap G^\perp \subset F^\perp \cap G \subset G \cap F \cap F^\perp = \{0\}$.

La restriction $u_{|G} : G \to E$ se prolonge donc (par le cas régulier) en $u_1 \in \mathrm{O}(q)$. Soit $v = u_1^{-1} \circ u : F \to E$. On a $v(x) = x$ pour tout $x \in G$ puisque u_1 prolonge $u_{|G}$. Donc, si $y \in F \cap F^\perp$ et $x \in G$ on obtient (en notant ϕ la forme polaire de q) :

$$\phi(v(y), x) = \phi(v(y), v(x)) = \phi(y, x) = 0.$$

Par conséquent $F \cap F^\perp$ est un SETI contenu dans $G^\perp$, qui est régulier, et l'on a $v(F \cap F^\perp) \subset G^\perp$; la restriction $v_{|F\cap F^\perp}$ se prolonge donc en $w \in \mathrm{O}(G^\perp, q)$ par le cas 1. Il s'ensuit que $\tilde{v} = \mathrm{id}_G \perp w$ est un automorphisme orthogonal de $E = G \perp G^\perp$ qui prolonge v puisque $v_{|F\cap F^\perp} = w_{|F\cap F^\perp}$ et $\tilde{v}_{|G} = \mathrm{id}_G = v_{|G}$. Alors, $u_1 \circ \tilde{v}$ fournit le prolongement cherché de u. □

3.4 Indice et partie anisotrope

Lemme 3.4. *Soit (E, q) un espace quadratique régulier contenant un sous espace totalement isotrope maximal de dimension p. Alors il existe une forme quadratique anisotrope q_1 telle que :*

$$q \simeq p.\langle 1, -1\rangle \perp q_1.$$

Démonstration. Soit F un sous espace totalement isotrope maximal de dimension p. Par le principe de gonflement hyperbolique (généralisé), il existe un sous-espace H de dimension $2p$ tel que $F \subset H$ avec q_H hyperbolique ; donc q_H est équivalente à la forme $p.\langle 1, -1\rangle$. Comme (H, q) est un sous-espace régulier on sait que $H \overset{\perp}{\bigoplus} H^\perp = E$ et on obtient :

$$q \simeq q_H \perp q_{H^\perp} \simeq p.\langle 1, -1\rangle \perp q_{H^\perp}.$$

On a donc prouvé l'existence de la forme quadratique $q_1 = q_{H^\perp}$ de l'énoncé ; il reste à montrer que cette forme est anisotrope. Supposons, par l'absurde, que $q_{H^\perp}$ est isotrope. Alors $H^\perp$ contient un vecteur isotrope non nul x tel que $x \notin H$ et par conséquent $x \notin F$. Ainsi l'espace $\mathrm{vec}(x) \oplus F$ est totalement isotrope, ce qui contredit le fait que F est isotrope maximal. Donc $q_{H^\perp}$ est anisotrope. □

Le théorème qui suit montre que toute forme quadratique sur un corps se dècompose de façon unique, á une isométrie près, en une somme de formes isotropes de type $\langle 1, -1\rangle$ et une forme anisotrope.

Théorème 3.11 (Décomposition de Witt)**.** *Soit (E, q) un espace quadratique régulier. Il existe alors un entier naturel p et une forme quadratique anisotrope q_a tels que :*

$$q \simeq p.\langle 1, -1\rangle \perp q_a.$$

1. *Dans cette écriture, l'entier p est déterminé de manière unique et q_a de manière unique à équivalence près.*

2. *Tout SETIM de E est de dimension p.*

Démonstration. La décomposition de q a été établie au lemme précédent.

1. Montrons que p et q_a sont uniques. Pour cela, supposons qu'il existe p_1 et p_2 entiers naturels tels que $p_1 \neq p_2$ et qu'il existe deux formes anisotropes q_{a_1} et q_{a_2} tels que :

$$q \simeq p_1.\langle 1, -1\rangle \perp q_{a_1} \quad \text{et} \quad q \simeq p_2.\langle 1, -1\rangle \perp q_{a_2}.$$

On peut supposer (sans perte de généralité) que $p_1 \leq p_2$. Alors on a :

$$p_2.\langle 1, -1\rangle \perp q_{a_2} \simeq p_1.\langle 1, -1\rangle \perp (p_2 - p_1).\langle 1, -1\rangle \perp q_{a_2}.$$

Or, par simplification de Witt

$$\underbrace{(p_2 - p_1).\langle 1, -1\rangle \perp q_{a_2}} \perp \overbrace{p_1.\langle 1, -1\rangle} \simeq \overbrace{p_1.\langle 1, -1\rangle} \perp \underbrace{q_{a_1}} \Longrightarrow (p_2 - p_1).\langle 1, -1\rangle \perp q_{a_2} \perp \simeq q_{a_1}.$$

Si $p_2 - p_1 \geq 0$, la forme quadratique $(p_2 - p_1).\langle 1, -1\rangle \perp q_2$ contient une partie hyperbolique non nulle qui est isotrope, ce qui contredit le fait qu'elle est équivalente à q_{a_1} qui est elle anisotrope par hypothèse. On a donc $p_1 = p_2$; posons $p = p_1 = p_2$.

On est dans la situation :

$$q \simeq p.\langle 1, -1\rangle \perp q_{a_1} \simeq p.\langle 1, -1\rangle \perp q_{a_2}.$$

Par simplification de Witt on obtient $q_{a_1} \simeq q_{a_2}$, d'où l'unicité de la partie anisotrope à équivalence près.

2. Ce point découle immédiatement de ce qui précède et du Lemme 3.1.

□

Définition 3.8. *Avec les notations du théorème précèdent, l'entier p est appelé l'**indice** (de Witt) de q et est noté $\nu(q)$. On appelle **partie anisotrope** de q toute forme quadratique équivalente à q_a.*

Proposition 3.4. *On a :*

1. $\nu(q) = \dim F$ *pour tout SETIM F de E ;*
2. $\nu(q) \leq \frac{\dim E}{2}$ *avec égalité si et seulement si q est hyperbolique ;*
3. $\nu(q) = 0$ *si et seulement si q est anisotrope ;*
4. $\nu(q)$ *est la dimension maximale d'un sous-espace vectoriel inclus dans le cône isotrope $Co(q)$.*

Démonstration. 1. C'est l'assertion 2 du théorème précédent.

2. Soit $W \subset E$ un SETI, i.e. $W \subset W^\perp$. On a $\dim W \leq \dim W^\perp$, donc :

$$\dim E = \dim W + \dim W^\perp \geq 2 \dim W$$

et

$$\dim W \leq \frac{\dim E}{2}.$$

D'où le résultat $\nu(q) \leq \frac{\dim E}{2}$. Si E contient un SETIM de dimension $p = \frac{\dim E}{2}$, le Lemme 3.1 implique que (E, q) est hyperbolique de dimension $2p$.

3. Si $\nu(q) = 0$, alors avec les mêmes notations $q \simeq 0.\langle 1, -1\rangle \perp q_a \simeq q_a$, donc q est anisotrope.

4. Il est clair que tout sous-espace vectoriel F contenu dans $Co(q)$ est un SETI car $q_F = 0$. Donc un sous-espace de E contenu dans $Co(q)$ et de dimension maximale est un SETIM. □

Exemples. Il est facile de déterminer l'indice d'une forme lorsque $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.

– Soit ϕ une forme quadratique régulière complexe de dimension n, alors ϕ est de rang n et par diagonalisation il existe $(a_1, \cdots, a_n) \in (\mathbb{C}^*)^n$ tel que $\phi \simeq \langle a_1, \cdots, a_n\rangle$. Or comme tout élément dans $\mathbb{C}$ possède une racine carrée, on a $\phi \simeq \langle 1, \cdots, \rangle \simeq n.\langle 1\rangle$.

1. Si $n = 2p$ on a donc $\phi \simeq 2p.\langle 1\rangle \simeq p\langle 1\rangle \perp p\langle 1\rangle$ et puisque $\mathbb{C}^*/(\mathbb{C}^*)^2 = \{1\}$ on peut écrire $\phi \simeq p.\langle 1\rangle \perp p.\langle -1\rangle \simeq p.\langle 1, -1\rangle$. Ainsi, l'indice $\nu(\phi)$ est égal à p et la partie anisotrope de ϕ est $0.\langle 1\rangle$.
2. Si $n = 2p + 1$ on voit de même que $\phi \simeq (2p + 1)\langle 1\rangle \simeq 2p.\langle 1\rangle \perp \langle 1\rangle \simeq p.\langle 1, -1\rangle \perp \langle 1\rangle$. On en déduit que $\nu(\phi) = p$ et que la partie anisotrope de ϕ est $\langle 1\rangle$.

– Soit q une forme quadratique régulière réelle de signature (r, s) ; on a donc $q \simeq r.\langle 1\rangle \perp s.\langle -1\rangle$.

1. Si $r \geq s$, il vient $q \simeq s.\langle 1, -1\rangle \perp (r - s).\langle 1\rangle$. La forme $(r - s).\langle 1\rangle$ est anisotrope et par la décomposition de Witt c'est la partie anisotrope de q. L'indice est $\nu(q) = s$.

2. Si $r \leq s$ on trouve de même manière, ou en considérant $-q$, que $\nu(q) = r$ et que la partie anisotrope de q est $(s-r).\langle -1\rangle$.

On donc $\nu(q) = \min(r, s)$ dans les deux cas.

Définition 3.9. *On appelle **indice** d'une forme quadratique q - régulière ou non - l'indice de sa partie régulière . $\bar{q}$.*

Ainsi, dans un premier temps on a ramené le problème de la classification des formes quadratiques à celui de la classification des formes quadratiques régulières, puis dans un deuxième temps à celui de la classification des formes quadratiques anisotropes via le théorème de décomposition de Witt. C'est le principe de **classification de Witt**.

3.5 Witt-équivalence

Définition 3.10. *Soient q et q' deux formes quadratiques régulières sur $\mathbb{K}$. On note q_a la partie anisotrope de q et q'_a celle de q'. On dit que q est q' sont **Witt-équivalentes**, ce que l'on note $q \overset{W}{\sim} q'$, si q_a et q'_a sont équivalentes.*

Proposition 3.5. *Soient q et q' deux formes quadratiques régulières. Alors q et q' sont Witt-équivalentes si et seulement si, il existe deux entiers naturels m et n tels que :*

$$q \perp m.\langle 1, -1\rangle \simeq q' \perp n.\langle 1, -1\rangle.$$

Démonstration. Soit q et q' deux formes quadratiques régulières Witt-équivalentes ; par définition, leurs parties anisotropes q_a et q'_a sont donc équivalentes. Par le Théorème 3.8 on peut décomposer q et q' de sorte que :

$$q \simeq p_1.\langle 1, -1\rangle \perp q_a, \quad q' \simeq p_2.\langle 1, -1\rangle \perp q'_a.$$

Supposons $p_1 \geq p_2$; il vient :

$$q \simeq (p_1 - p_2).\langle 1, -1\rangle \perp p_2.\langle 1, -1\rangle \perp q_a.$$

Puisque $q_a \simeq q'_a$ on a aussi :

$$q \simeq (p_1 - p_2).\langle 1, -1\rangle \perp p_2.\langle 1, -1\rangle \perp q'_a.$$

Grâce la décomposition de q' on trouve

$$q \simeq (p_1 - p_2).\langle 1, -1\rangle \perp \underbrace{p_2.\langle 1, -1\rangle \perp q'_a}_{\simeq q'}$$

puis $q \simeq (p_1 - p_2).\langle 1, -1\rangle \perp q'$. On a ainsi obtenu deux entiers n et $m = 0$ et $n = p_1 - p_2$ comme voulu.

Inversement, supposons qu'il existe $(m, n) \in \mathbb{N}^2$ tel que :

$$q \perp m.\langle 1, -1\rangle \simeq q' \perp n.\langle 1, -1\rangle. \qquad (1).$$

Par le Théorème 3.8 appliqué à q et q' on a :

$$q \simeq p_1.\langle 1, -1\rangle \perp q_a \qquad \text{et} \qquad q' \simeq p_2.\langle 1, -1\rangle \perp q'_a.$$

En remplaçant q et q' par des formes équivalentes dans (1) on obtient :

$$(p_1 + m).\langle 1, -1\rangle \perp q_a \simeq (p_2 + n).\langle 1, -1\rangle \perp q'_a.$$

L'unicité de l'indice de Witt implique alors $p_1 + m = p_2 + n$ et par le théorème de simplification il vient $q_a \simeq q'_a$, i.e. $q_a \overset{W}{\sim} q'_a$. □

Proposition 3.6. *Soient q_1, q_2, q_1' et q_2' des formes quadratiques régulières. Alors :*

$$q_1 \overset{W}{\sim} q_1' \text{ et } q_2 \overset{W}{\sim} q_2' \Longrightarrow q_1 \perp q_2 \overset{W}{\sim} q_1' \perp q_2'.$$

Démonstration. Comme $q_1 \overset{W}{\sim} q_1'$ il existe $(m_1, n_1) \in \mathbb{N}^2$ tel que :

$$q_1 \perp m_1.\langle 1, -1\rangle \simeq q_1' \perp n_1.\langle 1, -1\rangle.$$

De même, comme $q_2 \overset{W}{\sim} q_2'$, il existe $(m_2, n_2) \in \mathbb{N}^2$ tel que :

$$q_2 \perp m_2.\langle 1, -1\rangle \simeq q_2' \perp n_2.\langle 1, -1\rangle.$$

Il vient donc :

$$(q_1 \perp q_2) \perp (m_1 + m_2).\langle 1, -1\rangle \simeq (q_1' \perp q_2') \perp (n_1 + n_2).\langle 1, -1\rangle.$$

Posons $m = m_1 + m_2$ et $n = n_1 + n_2$; on a obtenu l'existence de deux entiers tels que :

$$(q_1 \perp q_2) \perp m.\langle 1, -1\rangle \simeq (q_1' \perp q_2') \perp n.\langle 1, -1\rangle.$$

Par Proposition 3.2 les deux formes quadratiques $(q_1 \perp q_2)$ et $(q_1' \perp q_2')$ sont Witt-équivalentes. □

Remarque 3.3. *La relation de Witt-équivalence entre les formes quadratiques régulières est une relation d'équivalence sur la collection des formes quadratiques régulières.*

1. *Réflexivité* : pour tout forme quadratique régulière q il est clair que $q \overset{W}{\sim} q$.
2. *Symétrie :* est immédiate car la relation $\simeq$ est symétrique.
3. *Transitivité* : soient q_1, q_2 et q_3 des formes quadratiques régulières telles que $q_1 \overset{W}{\sim} q_2$ et $q_2 \overset{W}{\sim} q_3$. Par définition de la Witt-équivalence cf. Définition 3.10, leurs formes anisotropes associées sont équivalentes, i.e. $q_{1,a} \simeq q_{2,a}$, et $q_{2,a} \simeq q_{3,a}$. Comme $\simeq$ est transitive on a $q_{1,a} \simeq q_{3,a}$,d'où $q_1 \overset{W}{\sim} q_3$.

3.6 Discriminant d'une forme quadratique

Pour faire la classification des formes quadratiques on se pose naturellement la question de l'existence d'invariants, c'est-à-dire de quantités inchangées par équivalence. Le *rang* en est un exemple. Le deuxième invariant est le *déterminant* $\det(q) \in K^*/(K^*)^2$ d'une forme régulière, comme défini dans la section 2.3. Pour des raisons techniques, il est nécessaire de modifier par un signe le déterminant.

Définition 3.11. *Soit q une forme quadratique régulière sur un espace vectoriel de dimension n. La classe*

$$\Delta := (-1)^{\frac{n(n-1)}{2}} \det(q) \in \mathbb{K}^*/(\mathbb{K}^*)^2.$$

est appelée ***le discriminant*** *de q.*

Proposition 3.7. *Soit ϕ et ψ deux formes quadratiques régulières. On suppose que ψ est de dimension 2, alors on a $\Delta(\phi \perp \psi) = \Delta(\phi)\Delta(\psi)$.*

Démonstration. Notons n dimension de ϕ, alors $\dim(\phi\perp\psi) = n+2$ et on a :

$$\begin{aligned}
\Delta(\phi\perp\psi) &= (-1)^{\frac{(n+2)(n+1)}{2}} \det(\phi\perp\psi) \\
&= (-1)^{\frac{(n+2)(n+1)}{2}} \det(\phi)\det(\psi) \\
&= (-1)^{\frac{(n^2+n+2n+1)}{2}} \det(\phi)\det(\psi) \\
&= (-1)^{\frac{n(n+1)}{2}}(-1)^{2n+1}\det(\phi)\det(\psi) \\
&= \underbrace{(-1)^{\frac{n(n+1)}{2}}\det(\phi)}_{\Delta(\phi)}\underbrace{(-\det(\psi))}_{\Delta(\psi)} \\
&= \Delta(\phi)\Delta(\psi).
\end{aligned}$$

□

Le discriminant est donc multiplicatif sur la somme orthogonale avec des espaces de dimension paire. On en déduit :

Proposition 3.8. *Deux formes quadratiques régulières Witt-équivalentes ont le même discriminant.*

Démonstration. Soient q et q' deux formes régulières qui sont Witt équivalentes. Il existe alors $m, n \in \mathbb{N}$ tels que :

$$q\perp m.\langle 1,-1\rangle \simeq q'\perp n.\langle 1,-1\rangle.$$

D'autre part on a :

$$\Delta(n.\langle 1,-1\rangle) = \Pi_{i=1}^{n}\Delta(\langle 1,-1\rangle) = (-1\times -1)^n = 1$$

Comme un plan hyperbolique est de discriminant 1, cf. Théorème 3.2, il vient :

$$\Delta(q) = \Delta(q\perp m.\langle 1,-1\rangle) = \Delta(q'\perp n.\langle 1,-1\rangle) = \Delta(q').$$

D'où le résultat. □

4 Groupe de Witt

4.1 Défintion et construction du groupe de Witt

Nous allons vérifier que la somme directe orthogonale, introduite précédemment, induit une structure de groupe abélien sur l'ensemble $W(\mathbb{K})$ des classes de Witt-équivalence de formes quadratiques régulières sur $\mathbb{K}$.

Notation 4.1. *Soit q une forme quadratique régulière sur $\mathbb{K}$. On note*

$$[q]_W = \{q' \,:\, q' \overset{W}{\sim} q\}$$

la classe de Witt-équivalence de q. L'ensemble des classes de Witt-équivalence de formes quadratiques régulières est désigné par $W(\mathbb{K})$.

La proposition qui suit assure que la loi d'addition orthogonale des formes quadratiques permet de munir $W(\mathbb{K})$ d'une structure de groupe abélien.

On notera dans toute la suite par $+$ l'application :

$$\begin{aligned}
W(\mathbb{K})\times W(\mathbb{K}) &\to W(\mathbb{K}) \\
([q]_W, [q']_W) &\mapsto [q\perp q']_W
\end{aligned}$$

Proposition 4.1. *$(W(\mathbb{K}), +)$ est un groupe abélien.*

Démonstration. Montrons d'abord que $+$ définit une loi de composition interne sur $W(\mathbb{K})$. Soient q_1, q_2, q_1' et q_2' des formes quadratiques régulières telles que $q_1 \overset{W}{\sim} q_1'$ et $q_2 \overset{W}{\sim} q_2'$. On a montré à la Proposition 3.6 que $(q_1 \perp q_2) \overset{W}{\sim} (q_1' \perp q_2')$. Ceci prouve que si $[q]_W, [q']_W \in W(\mathbb{K})$, l'addition $[q]_W + [q']_W \in W(\mathbb{K})$ est bien définie. La loi $+$ est donc une loi de composition interne sur $W(\mathbb{K})$. D'autre part, la somme directe orthogonale $\perp$ étant associative et commutative à isomorphisme près, il en est de même à Witt-équivalence près. Ceci donne à $(W(\mathbb{K}), +)$ une structure de monoïde ayant comme élement neutre la classe $[0]_W$ des formes hyperboliques. Pour toute forme quadratique régulière q, la forme $q \perp (-q)$ est hyperbolique ; par conséquent $[q \perp (-q)]_W = [q]_W + [-q]_W = [0]_W$ et $[-q]_W$ est l'opposé de $[q]_W$ pour la loi $+$. On a ainsi établi que $(W\mathbb{K}), +)$ est une groupe abélien. □

Définition 4.1. *Le **groupe de Witt** de $\mathbb{K}$ est l'ensemble $W(\mathbb{K})$ muni de la loi $+$.*

Comme nous l'avons vu dans la démonstration précédente, l'élement nul de $W(\mathbb{K})$ est $[0]_W$ et pour toute forme quadratique régulière q, on a $-[q]_W = [-q]_W$.

Notation 4.2. *Soient $a_1, a_2, \cdots, a_n$ des scalaires non nuls, la classe de Witt-équivalence de $\langle a_1, a_2, \cdots, a_n\rangle$ est notée $\langle\langle a_1, a_2, \cdots, a_n\rangle\rangle$, i.e. :*

$$[\langle a_1, a_2, \cdots, a_n\rangle]_W = \langle\langle a_1, a_2, \cdots, a_n\rangle\rangle.$$

Par définition de la loi $+$ on a donc :

$$[\langle a_1, a_2, \cdots, a_n\rangle]_W = [\langle a_1\rangle \perp \langle a_2\rangle \perp \cdots \perp \langle a_n\rangle]_W = \langle\langle a_1\rangle\rangle + \langle\langle a_2\rangle\rangle + \cdots + \langle\langle a_n\rangle\rangle.$$

Lemme 4.1. *L'ensemble des classes de Witt-équivalence $\langle\langle a\rangle\rangle$ formé en prenant dans chaque classe de $\mathbb{K}^*/(\mathbb{K}^*)^2$ un représentant a est une partie génératrice de $W(\mathbb{K})$.*

Démonstration. Soit q une forme quadratique régulière de dimension n. Par le Corollaire 2.1 on sait que :

$$\exists\, (a_1, a_2, \cdots, a_n) \in (\mathbb{K}^*)^n \text{ tel que } q \simeq \langle a_1, a_2, \cdots, a_n\rangle.$$

On a donc $q \overset{W}{\sim} \langle a_1, a_2, \cdots, a_n\rangle$ et on obtient :

$$[q]_W = \langle\langle a_1\rangle\rangle + \langle\langle a_1\rangle\rangle + \cdots + \langle\langle a_n\rangle\rangle,$$

ce qui prouve le lemme. □

4.2 Exemples de groupes de Witt

Commençons par décrire les groupes de Witt $W(\mathbb{C})$ et $W(\mathbb{R})$. Rappelons que l'on a

$$\mathbb{C}^*/(\mathbb{C}^*)^2 = \{\bar{1}\}, \qquad \mathbb{R}^*/(\mathbb{R}^*)^2 = \{\pm\bar{1}\},$$

où $\bar{x}$ est la classe de $x \in \mathbb{K}^*$ modulo les carrés.

Proposition 4.2. 1. *Le groupe $W(\mathbb{C})$ est engendré par $\langle\langle 1\rangle\rangle$ et isomorphe à $\mathbb{Z}/2$.*

2. *Le groupe $W(\mathbb{R})$ est engendré par $\langle\langle 1\rangle\rangle$ et isomorphe à $\mathbb{Z}$.*

Démonstration. 1. Par le Lemme 4.1 on sait que $\langle\langle 1\rangle\rangle$ engendre $W(\mathbb{C})$. Comme la seule forme anisotrope à équivalence près sur $\mathbb{C}$ est la forme $\langle 1\rangle$, on a $2.\langle\langle 1\rangle\rangle = 0$. On en déduit $W(\mathbb{C}) \cong \mathbb{Z}/2$.

Puisque $\mathbb{R}^*/(\mathbb{R}^*)^2 = \{\overline{1}, -\overline{1}\}$, le groupe de Witt de $\mathbb{R}$ est monogène engendré par $\langle\langle 1\rangle\rangle$, cf. Lemme 4.1. Montrons qu'il n'est pas cyclique d'ordre $n \in \mathbb{N}^*$. Si c'est le cas il vient $n.\langle\langle 1\rangle\rangle = \langle\langle 0\rangle\rangle$ et donc $n.\langle 1\rangle \overset{W}{\sim} 0$, c'est-à-dire que $n.\langle 1\rangle$ est hyperbolique. Mais la forme $n.\langle 1\rangle$ est anisotrope, d'où une contradiction. On a donc $W(\mathbb{R}) \cong \mathbb{Z}$. □

Étudions maintenant le groupe de Witt d'un corps fini $\mathbb{K} = \mathbb{F}_q$ de cardinal q. Rappelons, voir le Lemme 4.1, que $\mathbb{K}^*/(\mathbb{K}^*)^2 = \{\bar{1}, \bar{\epsilon}\}$ où ϵ un représentant de la classe des non carrés de $\mathbb{K}^*$.

Proposition 4.3. *Avec les notations précédentes on a :*
- *si* $q \equiv 1\,[4]$, *alors* $W(\mathbb{K}) \cong \mathbb{Z}/2 \times \mathbb{Z}/2$;
- *si* $q \equiv 3\,[4]$, *alors* $W(\mathbb{K}) \cong \mathbb{Z}/4$.

Démonstration. Du Lemme 4.1 on tire que $W(\mathbb{K}) = \langle\langle 1, \epsilon\rangle\rangle$.

– Si $q \equiv 1[4]$, -1 est un carré dans $\mathbb{K}$, cf. Lemme 3.1, donc les formes diagonales, $\langle 1, 1\rangle \simeq \langle 1, -1\rangle$ et $\langle \epsilon, \epsilon\rangle \simeq \langle \epsilon, -\epsilon\rangle$ sont hyperboliques. Il en découle $2.\langle\langle 1\rangle\rangle = 2.\langle\langle \epsilon\rangle\rangle = 0_{W(K)}$. En outre, les formes $\langle 1\rangle, \langle \epsilon\rangle$ étant anisotropes on obtient la description suivante du groupe de Witt :

$$W(\mathbb{K}) = \{0_{W(K)}, \langle\langle 1\rangle\rangle, \langle\langle \epsilon\rangle\rangle, \langle\langle 1; \epsilon\rangle\rangle\} \cong \{\langle\langle 0\rangle\rangle, \langle\langle 1\rangle\rangle\} \times \{\langle\langle 0\rangle\rangle, \langle\langle \epsilon\rangle\rangle\} \cong \mathbb{Z}/2 \times \mathbb{Z}/2.$$

– Si $q \equiv 3[4]$, -1 n'est pas un carré dans $\mathbb{K}$ et l'on a $\langle\langle 1, \epsilon\rangle\rangle = \langle\langle 1, -1\rangle\rangle$. La forme $\langle 1, -1\rangle$ étant hyperbolique on obtient $\langle\langle 1, \epsilon\rangle\rangle = 0_{W(\mathbb{K})}$, ou encore $\langle\langle 1\rangle\rangle = -\langle\langle \epsilon\rangle\rangle$. On en déduit que le groupe $W(\mathbb{K})$ est cyclique engendré par $\langle\langle 1\rangle\rangle$. Observons que $\langle 1, 1\rangle$ n'est pas hyperbolique car son déterminant est 1, qui est différent de -1. On a donc $2.\langle\langle 1\rangle\rangle \neq \langle\langle 0\rangle\rangle$. Pour obtenir $W(\mathbb{K}) \cong \mathbb{Z}/4$, on peut :

– soit utiliser $2.\langle\langle 1\rangle\rangle \neq \langle\langle 0\rangle\rangle$ et rappeler que les groupes d'ordre 4 sont (à isomorphisme près) $\mathbb{Z}/2 \times \mathbb{Z}/2$ et $\mathbb{Z}/4$;

– soit rappeler que $\langle 1, 1, 1, 1\rangle$ est hyperbolique, voir Théorème 3.7, ce qui prouve $4.\langle\langle 1\rangle\rangle = \langle\langle 0\rangle\rangle$. □

Références

[1] Clément de Seguins Pazzis, Invitations aux formes quadratiques, Calvage et Monet

[2] Algebraic Theory of Quadratic Forms, T-Y.Lam, 1973

[3] Théorie de Witt et Algèbres de Clifford Application à l'étude des formes quadratiques rationnelles, Mémoire de Doyen Nicolas, 2012

[4] Cours d'algèbre M1, Thierry LEVASSEUR 2019-2020. https ://levasseur.perso.math.cnrs.fr/pub/M1-groupes.html

[5] Introduction To Quadratic Forms Over Fields by T. Y. Lam, Graduate studies in mathematics, Volume 67.