

UNIVERSITÉ JOSEPH FOURIER

FORMES QUADRATIQUES
EXPOSÉS DE MAGISTÈRE

TANCRÈDE LEPOINT

2009

Table des matières

1	Théorèmes de Witt	5
1.1	Rappels brefs	5
1.2	Le théorème de simplification de Witt	6
1.2.1	Le groupe orthogonal	6
1.2.2	Le théorème de simplification de Witt	8
1.2.3	Contre-exemple en caractéristique 2 pour les applications bilinéaires	9
1.2.4	Le théorème d'extension de Witt	10
1.3	Théorème de décomposition	11
1.3.1	Isotropie et espaces hyperboliques	11
1.3.2	Décomposition de Witt	14
1.4	Introduction aux anneaux de Witt	15
2	Formes de Pfister et niveau d'un corps	19
2.1	Formes multiplicatives	19
2.2	Application au niveau d'un corps	21
2.3	Théorème de Cassels-Pfister et conséquences	24

TABLE DES MATIÈRES

1 | Théorèmes de Witt

Bien que la théorie des formes quadratiques soit, sans doute, aussi vieille de l'algèbre linéaire, l'étude des formes quadratiques sur un corps F quelconque, plutôt que sur un corps fini ou un corps des nombres, ne date que de 1937. Dans un article fondateur, Witt a créé la *théorie algébrique des formes quadratiques* et a démontré plusieurs résultats basiques mais très importants, comme le *théorème de simplification*. Par la suite, le sujet s'est très peu développé jusqu'au milieu des années 60. A cette date, Pfister a apporté de très belles idées nouvelles à la théorie. Ses travaux ont permis par exemple de montrer que le produit de deux sommes de 2^n carrés est également une somme de 2^n carrés.

1.1 Rappels brefs

Soit F un corps.

Définition 1.1.1. Deux formes quadratiques (V, q) et (V', q') sont dites *isomorphes* s'il existe un isomorphisme $f: V \rightarrow V'$ de F -espaces vectoriels tel que $q'(f(x)) = q(x)$ pour tout $x \in V$. On le notera $(V, q) \cong (V', q')$.

Deux formes bilinéaires symétriques (V, b) et (V', b') sont dites *isomorphes* s'il existe un isomorphisme $f: V \rightarrow V'$ de F -espaces vectoriels tel que $b'(f(x), f(y)) = b(x, y)$ pour tous $x, y \in V$. On le notera $(V, b) \cong (V', b')$.

Considérons à présente un cas où F est un corps de caractéristique différente de 2. Si deux formes quadratiques (V, q) et (V', q') sont isomorphes, alors les formes bilinéaires (V, b_q) et $(V', b_{q'})$ sont également isomorphes. En effet,

$$\begin{aligned} b_{q'}(f(x), f(y)) &= \frac{1}{2} (q'(f(x) + f(y)) - q'(f(x)) - q'(f(y))) \\ &= \frac{1}{2} (q'(f(x+y)) - q'(f(x)) - q'(f(y))) \\ &= \frac{1}{2} (q(x+y) - q(x) - q(y)) \\ &= b_q(x, y) \end{aligned}$$

En fait c'est une équivalence, du fait que $q(x) = b_q(x, x)$ pour tout $x \in V$.

Définition 1.1.2. On dit que deux matrices carrées B et B' sont *congruentes* s'il existe une matrice inversible M telle que $B' = {}^tMBM$.

Proposition 1.1.3. Soient (V, q) et (V', q') deux formes quadratiques, et soient B et B' les matrices de b_q et $b_{q'}$ dans une base (e_1, \dots, e_n) de V . Alors :

$$(V, q) \cong (V', q') \iff \text{les matrices } B \text{ et } B' \text{ sont congruentes.}$$

Démonstration. Soient (e'_1, \dots, e'_n) une autre base de V et M la matrice de changement de base, autrement dit

$$e'_j = \sum_{i=1}^n m_{i,j} e_i, \quad M = (m_{i,j})_{1 \leq i, j \leq n}$$

Comme

$$b_q(e'_i, e'_j) = b_q\left(\sum_{k=1}^n m_{k,i} e_k, \sum_{\ell=1}^n m_{\ell,j} e_\ell\right) = \sum_{k,\ell} m_{k,i} b_q(e_k, e_\ell) m_{\ell,j}$$

i.e. $B' = {}^t M B M$, on a l'équivalence voulue. □

1.2 Le théorème de simplification de Witt

Nous allons montrer un résultat fondamental de la théorie algébrique des formes quadratiques initiée par Witt : le théorème de simplification de Witt. Dans toute cette section, sous réserve de mention contraire, on considèrera un corps F de caractéristique différente de 2. Avant d'énoncer le théorème, on va montrer un résultat sur le groupe orthogonal.

1.2.1 Le groupe orthogonal

Nous allons définir le groupe orthogonal et exhiber des éléments qui vont le générer¹ et qui vont nous servir pour la démonstration du théorème de simplification.

Définition 1.2.1. Le *groupe orthogonal* d'une forme quadratique (V, q) est le groupe des automorphismes de (V, q) , et on le notera $\mathbf{O}(V, q)$ ou encore $\mathbf{O}(q)$. Autrement dit, on a :

$$\mathbf{O}(q) = \{f \in \text{Aut}(V) \mid q(f(x)) = q(x), \forall x \in V\}$$

On dira que les éléments de $\mathbf{O}(q)$ sont des *isométries*.

Les isométries sont des endomorphismes de déterminant ± 1 . En effet, soient q une forme quadratique régulière, et si α une isométrie. On a donc, pour tout $v \in V$, $q(\alpha(v)) = q(v)$. Choisissons une base \mathbf{e} de V , $\alpha(\mathbf{e})$ est donc une base de V . La formule du changement de base va alors nous dire que $\text{Mat}(q, \alpha(\mathbf{e})) = {}^t A \text{Mat}(q, \mathbf{e}) A$ où A est la matrice de passage de $\alpha(\mathbf{e})$ à \mathbf{e} , c'est-à-dire la matrice représentative de α dans la base \mathbf{e} . En passant au déterminant, on obtient $\det(q) = \det(A)^2 \det(q)$. Comme q est régulière, $\det(q) \neq 0$, d'où $\det(A) \in \{\pm 1\}$. Le déterminant induit donc un morphisme

$$\det: \mathbf{O}(V, q) \rightarrow \{\pm 1\}$$

Le noyau de ce morphisme, i.e. les isométries de déterminant 1, est appelé le *groupe spécial orthogonal* et est noté $\mathbf{SO}(V, q)$.

Nous allons maintenant exhiber une isométrie de déterminant -1 .

1. Mais on ne va pas montrer que ce sont des générateurs : ceci fait l'objet du théorème de Cartan-Dieudonné.

Définition 1.2.2. Soit (V, q) une forme quadratique régulière (i.e. non dégénérée), et un vecteur $y \in V$ tel que $q(y) \neq 0$. On appelle *réflexion hyperplane* l'automorphisme de V défini par :

$$\tau_y: x \in V \mapsto x - 2 \frac{b_q(x, y)}{q(y)} y \in V$$

Cette application est clairement une application linéaire de V dans V . Si $y \in V$, alors $\tau_y(y) = y - 2 \frac{b_q(y, y)}{q(y)} y = y - 2y = -y$, c'est-à-dire que τ envoie les éléments de Fy sur leur opposés. Si maintenant $x \in (Fy)^\perp$, alors $b_q(x, y) = 0$ et $\tau_y(x) = x$, c'est-à-dire que τ_y restreinte à $(Fy)^\perp$ est l'identité : τ_y est une involution qui laisse stable l'hyperplan $(Fy)^\perp$, d'où son nom de « réflexion orthogonale ». On en déduit alors que τ_y est un automorphisme pour tout $y \in V$. De plus, τ_y est une isométrie puisque :

$$\begin{aligned} q(\tau_y(x)) &= q\left(x - \frac{2b_q(x, y)}{q(y)} y\right) \\ &= b_q\left(x - \frac{2b_q(x, y)}{q(y)} y, x - \frac{2b_q(x, y)}{q(y)} y\right) \\ &= b_q(x, x) - 2 \times \frac{2b_q(x, y)}{q(y)} b_q(x, y) + \frac{4b_q(x, y)^2}{q(y)^2} b_q(y, y) \\ &= q(x) \end{aligned}$$

On peut voir que cette isométrie est de déterminant -1 . En effet, si l'on complète $\{y\}$ en une base orthogonale (y, e_2, \dots, e_n) de V , alors $e_2, \dots, e_n \in (Fy)^\perp$ et la matrice de τ_y respectivement à cette base est

$$\begin{pmatrix} -1 & 0 & \cdots & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ 0 & \cdots & \cdots & 0 & 1 \end{pmatrix}$$

qui est de déterminant -1 .

L'ensemble des réflexions orthogonales $\{\tau_y \mid y \in V, q(y) \neq 0\}$ est stable par la conjugaison dans le groupe orthogonal $\mathbf{O}(V, q)$: si $\sigma \in \mathbf{O}(V, q)$, alors $\sigma \tau_y \sigma^{-1} = \tau_{\sigma(y)}$. En effet, pour tout $x \in V$,

$$\begin{aligned} (\sigma \tau_y \sigma^{-1}) &= \sigma(\tau_y(\sigma^{-1}(x))) \\ &= \sigma\left(\sigma^{-1}(x) - \frac{2b_q(\sigma^{-1}(x), y)}{q(y)} y\right) \\ &= x - \frac{2b_q(x, \sigma(y))}{q(\sigma(y))} \sigma(y) = \tau_{\sigma(y)} \end{aligned}$$

Ainsi, on en déduit que le sous-groupe engendré par les τ_y , $y \in V$ tel que $q(y) \neq 0$ est un sous-groupe distingué de $\mathbf{O}(V, q)$. Par le théorème de Cartan-Dieudonné, on montre qu'en fait ce groupe coïncide avec $\mathbf{O}(V, q)$.

1.2.2 Le théorème de simplification de Witt

On peut maintenant énoncer le théorème que l'on souhaite démontrer :

Théorème 1.2.3. (simplification de Witt). Soient (V, q) , (V_1, q_1) et (V_2, q_2) trois formes quadratiques quelconques. Si

$$(V, q) \perp (V_1, q_1) \cong (V, q) \perp (V_2, q_2)$$

alors $(V_1, q_1) \cong (V_2, q_2)$.

Pour démontrer ce théorème, nous allons avoir besoin de deux lemmes préliminaires.

Lemme 1.2.4. Soient deux formes quadratiques (V_1, q_1) et (V_2, q_2) isomorphes. Soient deux sous-espaces vectoriels W_1 et W_2 respectivement de V_1 et V_2 sur lesquels q_1 et q_2 sont respectivement régulières. Supposons qu'il existe un isomorphisme $f: V_1 \rightarrow V_2$ tel que, pour tout $x \in V_1$, $q_2(f(x)) = q_1(x)$ et $f(W_1) = W_2$. On peut alors en déduire que $f(W_1^\perp) = W_2^\perp$.

Démonstration. Soit $x \in W_1^\perp$. On veut montrer que $f(x) \in W_2^\perp$, c'est-à-dire que pour tout $z \in W_2$, $b_{q_2}(f(x), z) = 0$. Soit $z \in W_2 = f(W_1)$. Il existe $y \in W_1$ tel que $f(y) = z$. Ainsi,

$$b_{q_2}(f(x), z) = b_{q_2}(f(x), f(y)) = b_{q_1}(x, y) = 0$$

car $x \in W_1^\perp$ et $y \in W_1$. Finalement, on a $f(W_1^\perp) \subset W_2^\perp$ et par égalité des dimensions, on en déduit le résultat voulu. \square

Lemme 1.2.5. Soient (V, q) une forme quadratique et $x, y \in V$ tels que $q(x) = q(y) \neq 0$. Il existe un élément $\tau \in \mathbf{O}(V, q)$ tel que $\tau(x) = y$.

Démonstration. On a $q(x+y) + q(x-y) = 4q(x) \neq 0$, donc $q(x+y) \neq 0$ ou $q(x-y) \neq 0$. Supposons par exemple que $q(x-y) \neq 0$, alors

$$\tau_{x-y}(x) = x - 2 \frac{b_q(x, x-y)}{q(x-y)}(x-y) = y$$

car $q(x-y) = q(x) + q(y) - 2b_q(x, y) = 2b_q(x, x) - 2b_q(x, y) = 2b_q(x, x-y)$. Dans ce cas là, on choisit $\tau = \tau_{x-y}$. Si maintenant $q(x-y) = 0$, alors $q(x+y) \neq 0$ et par un raisonnement équivalent, on a $\tau_{x+y}(x) = -y$. On choisit alors $\tau = -\tau_{x+y}$. \square

Démonstration du théorème 1.2.3. Nous allons faire une preuve en quatre temps :

1. Si $q = 0$ et q_1 est régulière. Alors, on note M_1 et M_2 les matrices respectives de q_1 et q_2 dans des bases fixées de V_1 et V_2 . Comme $q \perp q_1 \cong q \perp q_2$, les matrices

$$\begin{pmatrix} 0 & 0 \\ 0 & M_1 \end{pmatrix} ; \begin{pmatrix} 0 & 0 \\ 0 & M_2 \end{pmatrix}$$

sont congruentes, c'est-à-dire qu'il existe une matrice $N = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ inversible telle que

$$\begin{pmatrix} 0 & 0 \\ 0 & M_1 \end{pmatrix} = {}^t N \begin{pmatrix} 0 & 0 \\ 0 & M_2 \end{pmatrix} N = \begin{pmatrix} \star & \star \\ \star & {}^t D M_2 D \end{pmatrix}$$

Comme $\det(M_1) \neq 0$, alors $\det(D) \neq 0$ et on en déduit que M_1 et M_2 sont congruentes, i.e. $q_1 \cong q_2$.

2. Si $q = 0$ et q_1 quelconque. Quitte à renuméroter q_1 et q_2 , on peut supposer qu'il existe $r \in \mathbb{N}$ tel que

$$q_1 = \underbrace{\langle 0 \rangle \oplus \dots \oplus \langle 0 \rangle}_{r \text{ fois}} \oplus q'_1 \quad ; \quad q_2 = \underbrace{\langle 0 \rangle \oplus \dots \oplus \langle 0 \rangle}_{r \text{ fois}} \oplus q'_2$$

avec q'_1 régulière. On en déduit alors par le premier point que $q'_1 \cong q'_2$, donc $q_1 \cong q_2$.

3. Si $q = \langle a \rangle$ avec $a \neq 0$. On a donc

$$(V_1, q_1) \oplus \langle a \rangle \cong (V_2, q_2) \oplus \langle a \rangle$$

Il existe donc $e_1, e_2 \in V$ tels que $q(e_1) = q(e_2) = a$. Posons alors $U_1 = V_1 \oplus F e_1$ et $U_2 = V_2 \oplus F e_2$. Posons $Q_1 = q_1 \perp q$ et $Q_2 = q_2 \perp q$. Soit f un isomorphisme tel que $Q_2(f(x)) = Q_1(x)$ pour tout $x \in U_1$. Soit $e'_1 = f(e_1)$. On a $Q_2(e'_1) = Q_2(f(e_1)) = Q_1(e_1) = Q_2(e_2) = a$. Par le lemme 1.2.5, il existe $\tau \in \mathbf{O}(U_2, Q_2)$ tel que $\tau(e'_1) = e_2$, d'où $\tau \circ f(e_1) = e_2$. Or, $(F e_1)^\perp = V_1$ et $(F e_2)^\perp = V_2$ donc par le lemme 1.2.4, on a $\tau \circ f(V_1) = V_2$, ce qui implique que $(V_1, q_1) \cong (V_2, q_2)$.

4. Si maintenant q est quelconque, q s'écrit sous la forme $q = q' \oplus q''$ avec $q' \cong \langle a_1, \dots, a_n \rangle$, $a_i \neq 0$ pour tout i et $q'' = 0$. On a donc par hypothèse que $q_1 \perp q' \perp q'' \cong q_2 \perp q' \perp q''$. Les deux premiers points nous donnent que $q_1 \perp q' \cong q_2 \perp q'$, et en itérant la troisième étape plusieurs fois, on a $q_1 \cong q_2$, ce qui démontre le théorème de simplification de Witt. \square

1.2.3 Contre-exemple en caractéristique 2 pour les applications bilinéaires

Ce résultat ne subsiste malheureusement pas en caractéristique 2 pour les applications bilinéaires... En effet, considérons le corps $F = \mathbb{F}_2$. On va considérer l'hyperplan hyperbolique, c'est-à-dire la forme bilinéaire $H: \mathbb{F}_2^2 \times \mathbb{F}_2^2 \rightarrow \mathbb{F}_2$ définie par

$$H(v, w) = {}^t v \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} w.$$

On notera également $\underbrace{\langle 1, \dots, 1 \rangle}_{n \text{ fois}}$ la forme bilinéaire :

$$\langle 1, \dots, 1 \rangle : (v, w) \in \mathbb{F}_2^n \times \mathbb{F}_2^n \mapsto {}^t v w \in \mathbb{F}_2$$

Pour tous $a_1, a_2 \in \mathbb{F}_2$, on a

$$(a_1 \ a_2) \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} = a_1 a_2 + a_2 a_1 = 0$$

Donc $H(v, v) = 0$ pour tout $v \in \mathbb{F}_2^2$. Or,

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = 1 \neq 0$$

donc $H \neq \langle 1, 1 \rangle$

Notons $b = \langle 1, 1, 1 \rangle$. Considérons la base canonique (e_1, e_2, e_3) de \mathbb{F}_2^3 , et posons $f_1 = e_1 + e_2 + e_3$, $f_2 = e_1 + e_3$ et $f_3 = e_2 + e_3$. La famille $\mathbf{f} = (f_1, f_2, f_3)$ forme une base de \mathbb{F}_2^3 , et

$$\text{Mat}(b, \mathbf{f}) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

ce qui montre que $b \cong \langle 1 \rangle \perp H$.

1.2.4 Le théorème d'extension de Witt

Sous les hypothèses du théorème de simplification de Witt, on peut poser

$$E = (V, q \perp q_1) \perp (W_1, q \perp q_1) \quad ; \quad F = (V, q \perp q_2) \perp (W_2, q \perp q_2).$$

Sous cette dénomination, on voit que $W_1 = V^\perp$ pour la forme quadratique $q \perp q_1$ et $W_2 = V^\perp$ pour la forme quadratique $q \perp q_2$. Ainsi, une reformulation du théorème de simplification est que, si

$$(V, q) = (W, q) \perp (W^\perp, q) \quad ; \quad (V', q') = (W', q') \perp (W'^\perp, q')$$

alors

$$(W, q) \cong (W', q') \Rightarrow (W^\perp, q) \cong (W'^\perp, q')$$

Du théorème de simplification de Witt, on peut démontrer un second théorème appelé le théorème d'extension de Witt :

Théorème 1.2.6. (extension de Witt). Soient (V, q) et (V', q') des formes quadratiques, W un sous-espace vectoriel de V et $\tau : W \rightarrow V'$ un morphisme tel que

$$\forall x \in W, \quad q'(\tau(x)) = q(x).$$

On peut étendre τ en un morphisme de V sur V' tel que

$$\forall x \in V, \quad q'(\tau(x)) = q(x).$$

Démonstration. On peut supposer que $(W, q|_W)$ est une forme quadratique régulière, quitte à restreindre W . On a donc $V = W \perp W^\perp$ et $V' = \tau(W) \perp \tau(W)^\perp$. Comme $(W, q) \cong (\tau(W), q')$, le théorème de simplification de Witt donne que $W^\perp \cong \tau(W)^\perp$. Il existe donc un isomorphisme $\mu : W^\perp \rightarrow \tau(W)^\perp$ tel que

$$\forall x \in W^\perp, \quad q'(\mu(x)) = q(x).$$

On pose alors $\sigma : V \rightarrow V'$ définie par

$$\sigma(x + y) = \tau(x) + \mu(y), \quad x \in W, y \in W^\perp.$$

σ ainsi définie est un isomorphisme qui étend τ et vérifie la propriété voulue. \square

1.3 Théorème de décomposition

Une des idées importantes de Witt a été de considérer les formes quadratiques ensemble plutôt qu'individuellement. Ceci l'a conduit à définir ce qu'on appelle aujourd'hui l'anneau de Witt.

1.3.1 Isotropie et espaces hyperboliques

Rappelons d'abord quelques définitions :

Définition 1.3.1. Un vecteur $x \neq 0$ d'un espace V muni d'une forme quadratique q est dit *isotrope* si $q(x) = 0$, sinon x est dit *anisotrope*. Si (V, q) contient un vecteur isotrope, alors on dit que (V, q) est *isotrope* également, et dans le cas contraire, (V, q) est dit *anisotrope*. Finalement, on dit qu'un sous-espace $W \subset V$ est *totalelement isotrope* si $q|_W = 0$.

On rappelle qu'on se restreint à l'étude des formes quadratiques régulières, i.e. non-dégénérées.

Proposition 1.3.2. Soit (V, q) une forme quadratique régulière avec $\dim(V) = 2$. Les propriétés suivantes sont équivalentes :

1. q est isotrope
2. $\det(q) = -1 \in F^\times / F^{\times 2}$
3. $q \cong \langle 1, -1 \rangle$
4. q est isomorphe à la forme quadratique

$$\left\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle$$

Démonstration. Il suffit de montrer que (1) \Rightarrow (4) et que (2) \Rightarrow (1), le reste est trivial.

(1) \Rightarrow (4) : Soit $x \in V$, $x \neq 0$ tel que $q(x) = 0$. Soit $y \in V$ tel que $b_q(x, y) = 1$ (il existe car q est régulière), et notons $a = q(y)$. (x, y) est une base de V (puisque y ne peut-être colinéaire à x). Posons $y' = y - \frac{a}{2}x$. Alors, (x, y') est une base de V et

$$q(y') = b_q(y', y') = 0$$

Et la matrice de b_q dans la base (x, y') est $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

(2) \Rightarrow (1) : On sait que $q \cong \langle a, b \rangle$ et que $\det(q) = ab = -1$, donc $b = -a \in F^\times / F^{\times 2}$. Si (e, f) est la base de V où la matrice représentative de q est la matrice diagonale $\begin{pmatrix} a & 0 \\ 0 & -a \end{pmatrix}$ (existe quitte à multiplier f par le bon facteur) alors $q(e + f) = 0$ et q est isotrope. \square

Définition 1.3.3. Un *plan hyperbolique* (V, q) est un espace vectoriel V de dimension 2, muni d'une forme quadratique q régulière, possédant un vecteur isotrope. On notera souvent $(V, q) = H$. Une base (x, y) de vecteurs isotropes telle que $b_q(x, y) = 1$ est appelée *base hyperbolique*.

Une somme orthogonale de plans hyperboliques est alors appelée un *espace hyperbolique*. On dira alors que q est une *forme quadratique hyperbolique*.

Proposition 1.3.4. Soit (V, q) une forme quadratique régulière. Si (V, q) est isotrope, alors elle admet un plan hyperbolique comme facteur orthogonal, i.e. il existe une forme quadratique (V', q') telle que

$$V(q) \cong H \perp (V', q')$$

Démonstration. Soit x un vecteur isotrope de q et $y \in V$ tel que $b_q(x, y) = 1$ et $q(y) = 0$. Posons $W = Fx \oplus Fy$. Comme $q|_W$ est non dégénérée, on a

$$(V, q) \cong (W, q|_W) \perp (W^\perp, q|_{W^\perp})$$

Et par la proposition précédente, $(W, q|_W) \cong H$, ce qui permet de conclure. □

Proposition 1.3.5. Soit (V, q) une forme quadratique régulière. Il y a équivalence entre :

1. (V, q) est une forme quadratique hyperbolique
2. il existe un sous-espace W de V tel que $\dim(W) = \frac{1}{2} \dim(V)$ et $(W, q|_W)$ est totalement isotrope.

Démonstration. 1 \Rightarrow 2 : On a

$$V \cong H \perp H \perp \dots \perp H$$

On prend (e_i, f_i) une base de chaque plan hyperbolique. En considérant la base

$$(e_1, e_2, \dots, e_m, f_1, \dots, f_m),$$

la matrice représentative de q est la matrice par blocs

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

La matrice d'une forme hyperbolique est de la forme

$$\begin{pmatrix} 0 & C \\ {}^tC & D \end{pmatrix}.$$

Cette matrice est inversible puisque q est régulière et en échangeant les colonnes, on trouve que son déterminant est égal à $\det(C)^2 = 1 \in F^\times / F^{\times 2}$. Donc, C est inversible. En posant $A = \frac{1}{2}D$, on a

$$\begin{pmatrix} C & 0 \\ {}^tA & I \end{pmatrix} \begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix} \begin{pmatrix} {}^tC & A \\ 0 & I \end{pmatrix} = \begin{pmatrix} 0 & C \\ {}^tC & D \end{pmatrix}$$

2 \Rightarrow 1 : La réciproque revient à la construction dans l'autre sens... □

Définition 1.3.6. Soit (V, q) une forme quadratique. On dit que q représente $a \in F^\times$ si il existe $x \in V$ tel que $q(x) = a$. On notera $D(q)$ l'ensemble des éléments représentés par q .

On dira qu'une forme quadratique q est *universelle* si $D(q) = F^\times$.

Une propriété immédiate est que, si a est représenté par q , alors $\langle a \rangle$ est une sous-forme de q , c'est-à-dire il existe une forme quadratique q' telle que $q = \langle a \rangle \perp q'$. En effet, si $x \in V$ est tel que $q(x) = a$, alors $\{x\}$ peut être complété en une base orthogonale de V et le résultat s'en déduit immédiatement.

Proposition 1.3.7. *Toute forme quadratique régulière et isotrope est universelle.*

Démonstration. D'après la proposition précédente, toute forme quadratique isotrope contient comme facteur orthogonal un plan hyperbolique. Il suffit donc de montrer que H est universelle. Notons (x, y) une base hyperbolique de H et $a \in F^\times$. On a $q(\frac{a}{2}x + y) = a$, d'où le résultat. \square

Proposition 1.3.8. *Soient (V, q) une forme quadratique régulière, et $a \in F^\times$. Alors*

$$a \in D(q) \iff q \perp \langle -a \rangle \text{ est isotrope.}$$

Démonstration. Le sens direct est évident. Réciproquement, si $x + \lambda e$ est un vecteur isotrope de $q' = q \perp \langle -a \rangle$ où $q'(e) = -a$, on a

$$q'(x + \lambda e) = q(x) - \lambda^2 a = 0.$$

Si $\lambda \neq 0$, alors $q(\frac{x}{\lambda}) = a$ et $a \in D(q)$. Si $\lambda = 0$, alors $q(x) = 0$ et q est isotrope, donc universelle par la proposition précédente, donc $D(q) = F^\times$. \square

Donnons une preuve immédiate du théorème de Cartan-Dieudonné dans le cas où l'espace (V, q) est anisotrope.

Théorème 1.3.9. *(Version faible du théorème de Cartan-Dieudonné). Si (V, q) est une forme quadratique régulière anisotrope avec $\dim(V) = n$. Toute isométrie $\sigma \in \mathbf{O}(q)$ est un produit d'au plus n réflexions orthogonales.*

Démonstration. On raisonne par récurrence sur la dimension de V . Si V est de dimension 1, c'est clair. Soit maintenant $n > 1$ et supposons le résultat établi jusqu'à $n - 1$. Soient $\sigma: V \rightarrow V$ une isométrie et $x \neq 0$ un vecteur. Si $\sigma(x) = x$, alors $\sigma((Fx)^\perp) = (Fx)^\perp$ et par récurrence, $\sigma|_{(Fx)^\perp}$ est produit d'au plus $n - 1$ réflexions τ_1, \dots, τ_r . Si l'on pose $\sigma_i = \tau_i \perp \text{id}_{(Fx)^\perp}$, σ_i est une réflexion de V et le résultat est immédiat. Si maintenant $y = \sigma(x) - x \neq 0$, alors y est anisotrope, et $\tau_y \circ \sigma(x) = x$, d'où le résultat. \square

Il ne resterait en fait qu'un cas à traiter si (V, q) est régulier, c'est le cas où $\sigma(x) - x$ est isotrope. On peut alors montrer que $x + \sigma(x)$ n'est pas isotrope (cf. la démonstration 1.2.5). On a $\tau_{x+\sigma(x)}(x) = -x$ donc $\tau_x \circ \tau_{x+\sigma(x)}(x) = x$. On en déduit que $\mathbf{O}(q)$ est engendré par les réflexions, mais la technique n'aboutit pas pour montrer le théorème précédent puisqu'on prouve que σ est produit de $n + 1$ réflexions.

Nous allons maintenant présenter un corollaire au théorème d'extension de Witt qui donnera la définition de l'index de Witt, i.e. la dimension des sous-espaces totalement isotropes maximaux (s.e.t.i.m) de (V, q) .

Corollaire 1.3.10. *Tous les sous-espaces de V totalement isotropes maximaux sont de même dimension.*

Démonstration. Soient U et W deux tels sous-espaces, avec $\dim(U) \leq \dim(W)$. Soit $\sigma : U \rightarrow W$ un morphisme injectif. Comme U et W sont des sous-espaces isotropes totalement maximaux, on a

$$\forall x \in U, \quad q(\sigma(x)) = 0 = q(x)$$

Par le théorème d'extension de Witt, on peut étendre σ en une isométrie de V . Ainsi, $\sigma^{-1}(W) \supset U$ est totalement isotrope et par maximalité de U , on a l'égalité des dimensions. \square

Définition 1.3.11. La dimension commune des sous-espaces totalement isotropes maximaux d'un espace V muni d'une forme quadratique q régulière est appelé *l'index de Witt de (V, q)* et sera noté $\text{ind}(V, q)$.

1.3.2 Décomposition de Witt

Théorème 1.3.12. (décomposition de Witt). *Toute forme quadratique (V, q) admet une décomposition*

$$(V, q) \cong (V_0, q_0) \perp (V_h, q_h) \perp (V_a, q_a)$$

où (V_0, q_0) est totalement isotrope, (V_h, q_h) est hyperbolique et (V_a, q_a) est anisotrope. De plus, cette décomposition est unique à isomorphisme près.

Démonstration. Soit V' un sous-espace de V tel que $V = V^\perp \perp V'$. On pose $V_0 = V^\perp$. On a donc $q|_{V_0} = 0$ et $q|_{V'}$ est régulière. Ensuite, tant que V' est isotrope, on peut factoriser un plan hyperbolique H , et on ne peut faire cela qu'un nombre fini de fois. On en déduira alors que

$$V' = (H \perp H \perp \cdots \perp H) \perp V_a$$

et V_a sera anisotrope. Ceci prouve l'existence.

Supposons à présent que V admet une seconde décomposition

$$V = V'_0 \perp V'_h \perp V'_a$$

Comme V_0 est totalement isotrope, et que $(V'_h \perp V'_a, q|_{V'_h} \perp q|_{V'_a})$ est régulière, on a

$$V_0 = V^\perp = (V'_0)^\perp \perp (V'_h \perp V'_a)^\perp = V'_0$$

Par le théorème de simplification de Witt, on en déduit alors que

$$V_h \perp V_a \cong V'_h \perp V'_a$$

Si on écrit $V'_h = m'H$ et $V_h = mH$, le théorème de simplification nous assure que $m = m'$, ce qui permet de conclure à l'unicité. \square

On déduit de la démonstration que l'indice de Witt de (V, q) est $m = \frac{1}{2} \dim(V_h)$.

1.4 Introduction aux anneaux de Witt

On aimerait construire un anneau depuis le monoïde M des classes d'isomorphisme des formes quadratiques régulières.

Proposition 1.4.1. *Soit (V, q) une forme quadratique régulière. Alors $(V, q) \perp (V, -q)$ est hyperbolique.*

Démonstration. Soit $W = \{(x, x) \mid x \in V\}$. Alors W est un sous-espace vectoriel de dimension moitié de $V \perp V$. De plus,

$$(q \perp -q)(x, x) = q(x) - q(x) = 0$$

donc W est totalement isotrope. □

Définissons la relation \sim sur $M \times M$ par

$$q \sim q' \iff \exists h, h' \text{ des formes hyperboliques telles que } q \perp h \cong q' \perp h'$$

Cette relation est une relation d'équivalence. En effet, la réflexivité et la symétrie étant claires, considérons trois formes quadratiques q, q' et q'' telles que $q \sim q'$ et $q' \sim q''$, alors il existe h, h', h'' des formes quadratiques hyperboliques telles que

$$q + h \cong q' + h' \quad ; \quad q' + h' \cong q' + h''$$

Donc,

$$q + h \cong q' + h''$$

D'où $q \sim q''$.

Posons

$$W(F) = M / \sim$$

l'ensemble des classes d'équivalence de M par rapport à la relation d'équivalence \sim .

Lemme 1.4.2. *Si q est une forme quadratique et h une forme hyperbolique, alors $q \otimes h$ est hyperbolique.*

Démonstration. Il suffit de le vérifier pour $q \otimes \ell$ où ℓ est un plan hyperbolique par distributivité de \otimes sur \perp . On a $\ell \cong \langle 1, -1 \rangle$, donc

$$q \otimes \ell \cong q \otimes \langle 1, -1 \rangle = q \perp (-q)$$

et cette forme est bien hyperbolique. □

Proposition 1.4.3. *Les opérations \perp et \otimes passent au quotient et munissent $W(F)$ d'une structure d'anneau commutatif.*

Démonstration. Si $q \sim q'$ et $r \sim r'$, alors il existe h, h', ℓ, ℓ' des formes hyperboliques telles que

$$q \perp h \cong q' \perp h' \quad ; \quad r \perp \ell \cong r' \perp \ell'$$

d'où

$$(q \perp h) \perp (r \perp \ell) \cong (q' \perp h') \perp (r' \perp \ell')$$

i.e.

$$(q \perp r) \perp (h \perp \ell) \cong (q' \perp r') \perp (h' \perp \ell')$$

ce qui donne que $q \perp r \sim q' \perp r'$. Ainsi, \perp passe au quotient.

Avec les mêmes notations, on a

$$(q \perp h) \otimes (r \perp \ell) \cong (q' \perp h') \otimes (r' \perp \ell')$$

d'où

$$(q \otimes r) \perp (q \otimes \ell \perp h \otimes r \perp h \otimes \ell) \cong (q' \otimes r') \perp (q' \otimes \ell' \perp h' \otimes r' \perp h' \otimes \ell').$$

D'après le lemme précédent, on a $q \otimes \ell, h \otimes r, h \otimes \ell$ et $q' \otimes \ell', h' \otimes r', h' \otimes \ell'$ qui sont des formes hyperboliques, donc leur somme aussi et on en déduit que

$$q \otimes r \cong q' \otimes r'.$$

Ainsi, \otimes passe au quotient.

L'élément neutre de la somme orthogonale est la classe des formes hyperboliques, l'opposé d'une forme (V, q) est $(V, -q)$ (cf. proposition précédente). L'élément neutre du produit tensoriel est la classe de la forme $\langle 1 \rangle$. Il faut maintenant vérifier que tous les axiomes d'anneau sont vérifiées.

□

On dira que $W(F)$ est *l'anneau de Witt* de F .

Proposition 1.4.4. Soient (V, q) et (V', q') deux formes quadratiques régulières. On a

1. $q \sim q' \iff q_a \cong q'_a$
2. Si $\dim(V) = \dim(V')$, alors $q \sim q' \iff q \cong q'$.

Démonstration. Comme q et q' sont régulières, elles se décomposent sous la forme $q \cong q_h \perp q_a$ et $q' \cong q'_h \perp q'_a$. On a donc par unicité de la décomposition de Witt

$$q \cong q' \iff q_h \perp q_a \cong q'_h \perp q'_a \iff q \sim q'$$

De plus, si $\dim(V) = \dim(V')$, alors le 1) permet de conclure.

□

Exemples d'anneaux de Witt

Le corps des complexes

Considérons l'application

$$(V, q) \in M \mapsto \dim(V) \pmod{2} \in \mathbb{Z}/2\mathbb{Z}$$

Cette application est un morphisme, clairement surjectif. On sait que

$$(V, q) \cong (V', q') \iff \dim(V) = \dim(V')$$

donc

$$q \sim q' \iff \dim(V) = \dim(V') \pmod{2}$$

et l'application se factorise en un isomorphisme :

$$W(\mathbb{C}) \rightarrow \mathbb{Z}/2\mathbb{Z}$$

Le corps des réels

Considérons l'application

$$(V, q) \in M \mapsto \text{sign}(V, q) \in \mathbb{Z}$$

Cette application est clairement un morphisme, surjectif. De plus, on sait que

$$(V, q) \cong (V', q') \iff \dim(V) = \dim(V') \text{ et } \text{sign}(V, q) = \text{sign}(V', q')$$

Comme une forme hyperbolique est de signature nulle, alors on a

$$q \sim q' \iff \text{sign}(V, q) = \text{sign}(V', q')$$

et l'application se factorise en un isomorphisme :

$$W(\mathbb{R}) \rightarrow \mathbb{Z}$$

Les corps finis

Soit p un nombre premier, et soit $q = p^n$. Soit \mathbb{F}_q le corps à q éléments.

- Proposition 1.4.5.**
1. Si $q \equiv 1 \pmod{4}$, alors $W(\mathbb{F}_q) \cong \mathbb{F}_4$
 2. Si $q \equiv 3 \pmod{4}$, alors $W(\mathbb{F}_q) \cong \mathbb{Z}/4\mathbb{Z}$.

Démonstration. Soit $\alpha \in \mathbb{F}_q^\times / \mathbb{F}_q^{\times 2}$ non trivial. On rappelle que

$$\alpha = -1 \in \mathbb{F}_q^\times / \mathbb{F}_q^{\times 2} \iff q \equiv -1 \pmod{4}.$$

On a vu que toute forme quadratique régulière est isomorphe à $\langle 1, \dots, 1 \rangle$ ou à $\langle 1, \dots, 1, \alpha \rangle$.

1. Supposons que $q \equiv 1 \pmod{4}$. Alors -1 est un carré dans \mathbb{F}_q , donc $\langle 1, 1 \rangle \cong \langle 1, -1 \rangle$, donc $\langle 1, 1 \rangle$ est une forme hyperbolique. Ainsi, toute forme quadratique non dégénérée est soit hyperbolique, soit dans la même classe que Witt que l'un des formes suivantes : $\langle 1 \rangle$, $\langle \alpha \rangle$, ou $\langle 1, \alpha \rangle$. Comme $\langle \alpha, \alpha \rangle \cong \langle \alpha, -\alpha \rangle$, alors tous ces éléments sont d'ordre 2 dans $W(\mathbb{F}_q)$. Il faut maintenant étudier la multiplication des éléments pour en déduire que

$$W(\mathbb{F}_q) \cong \mathbb{F}_4.$$

2. Supposons que $q \equiv -1 \pmod{4}$, alors $\alpha = -1 \in \mathbb{F}_q^\times / \mathbb{F}_q^{\times 2}$. Toute formes quadratique non dégénérée est isomorphe à $\langle 1, \dots, 1 \rangle$ ou $\langle 1, \dots, 1, -1 \rangle$. Or $\langle -1, -1 \rangle \cong \langle 1, 1 \rangle$, donc toute formes quadratique non dégénérée est soit hyperbolique, soit dans la même classe de Witt que $\langle 1 \rangle$, $\langle 1, 1 \rangle$ ou $\langle 1, 1, 1 \rangle$ les éléments sont d'ordre respectifs 4, 2 et 4 (car $\langle 1, 1 \rangle \cong \langle -1, -1 \rangle$), donc on a bien

$$W(\mathbb{F}_q) \cong \mathbb{Z}/4\mathbb{Z}. \quad \square$$

2 | Formes de Pfister et niveau d'un corps

L'objectif de cette partie est de montrer le théorème suivant à l'aide de quelques outils élémentaires de la théorie des formes quadratiques :

Théorème 2.0.6. Soit F un corps commutatif, alors le nombre minimal de carrés dont la somme est égale à -1 (dans F) est soit l'infini (si -1 n'est pas somme de carrés), soit une puissance de 2.

Pour commencer, il convient de remarquer que ce théorème est vrai en caractéristique 2 puisque $-1 = 1^2$. On ne considèrera désormais que des corps de caractéristique différente de 2.

Introduisons des formes quadratiques particulières, appelées formes de Pfister qui permettront de démontrer le théorème qui nous intéresse.

Définition 2.0.7. Une n -forme de Pfister (ou forme de Pfister) est une forme quadratique du type :

$$\langle 1, a_1 \rangle \otimes \langle 1, a_2 \rangle \otimes \cdots \otimes \langle 1, a_n \rangle$$

et on la notera $\langle\langle a_1, \dots, a_n \rangle\rangle$.

Par exemple, si $a, b \in F^\times$, alors on a

$$\langle\langle a, b \rangle\rangle = \langle 1, a, b, ab \rangle.$$

2.1 Formes multiplicatives

Définition 2.1.1. Soit q une forme quadratique. Un élément $\alpha \in F^\times$ est appelé un *facteur de similitude* de q si αq est isomorphe à q . Notons $G(q)$ l'ensemble des facteurs de similitudes de (V, q) .

En particulier, les carrés non nuls de F sont des facteurs de similitude de q . En effet, si $\alpha = a^2 \in F^\times$, comme $\forall x \in V, \alpha q(x) = q(ax)$, alors $\alpha q \cong q$. De plus, il est clair que $G(q)$ est un sous-groupe de F^\times .

On utilisera pas la suite le résultat suivant :

Lemme 2.1.2. Si q est une forme quadratique qui représente 1, alors q représente tous ses facteurs de similitude.

Démonstration. Soit $\alpha \in G(q)$, alors αq représente α et comme $\alpha q \cong q$, alors q représente α . \square

Définition 2.1.3. On dit qu'une forme quadratique anisotrope q est *multiplicative* si $G(q) = D(q)$, i.e. ses facteurs de similitude sont les éléments de F^\times représentés par q .

On dit qu'une forme quadratique isotrope est *multiplicative* si elle est hyperbolique.

Par exemple, une forme du type $\langle 1, a \rangle$ est multiplicative. En effet, si elle est isotrope, $q \cong \langle 1, -1 \rangle$ et si elle est anisotrope, $\langle 1, a \rangle$ représente 1, donc représente tous ses facteurs de similitude. Soit $b \in D(q)$, alors

$$\langle 1, a \rangle \cong \langle b, ab \rangle = b\langle 1, a \rangle.$$

et $b \in G(q)$.

Le théorème suivant permettra alors de montrer facilement qu'une forme de Pfister est hyperbolique.

Théorème 2.1.4. (Pfister). *Si q est une forme multiplicative, alors $q \otimes \langle 1, a \rangle$ est multiplicative, pour tout $a \in F^\times$.*

Ceci implique que les formes de Pfister sont multiplicatives, donc qu'elles sont hyperboliques si et seulement si elles sont isotropes.

Démonstration. Si q est isotrope, par hypothèse, q est hyperbolique. Alors,

$$q \otimes \langle 1, a \rangle = q \perp aq$$

est aussi hyperbolique (et isotrope) donc multiplicative.

Si q est anisotrope et $q \otimes \langle 1, a \rangle$ est isotrope. On a

$$q \otimes \langle 1, a \rangle = q \perp aq.$$

Comme cette forme est isotrope, il existe des vecteurs $x, y \in V$ tels que $q(x) + aq(y) = 0$ avec $q(x) \neq 0$ et $q(y) \neq 0$. Posons $\alpha = q(x)$ et $\beta = q(y)$. α et β sont représentés par q isotrope, donc facteurs de similitude de q , si bien que

$$\begin{aligned} q \otimes \langle 1, a \rangle &= q \perp aq \\ &= (\alpha q) \perp (a\beta q) \\ &= (\alpha q) \perp (-\alpha q) \\ &= q \perp (-q) \end{aligned}$$

donc $q \otimes \langle 1, a \rangle$ est hyperbolique, donc multiplicative.

Si q est anisotrope et $q \otimes \langle 1, a \rangle$ est anisotrope. Notons $\delta = \alpha + a\beta \in D(q \perp aq)$. On a trois cas :

– si $\beta = 0$, alors $\alpha \in D(q) = G(q)$. Alors,

$$\alpha(q \perp (aq)) \cong (\alpha q) \perp (a(\alpha q)) \cong q \perp aq$$

et $\delta = \alpha \in G(q \perp aq)$.

– si $\alpha = 0$, alors $\beta \in D(q)$ et de même, $\delta = \beta \in D(q \perp aq)$.

– si $\alpha, \beta \neq 0$, alors $\alpha, \beta \in D(q) = G(q)$. On a donc

$$\begin{aligned}
 \delta(q \perp aq) &\cong (\alpha + a\beta)(q \perp aq) \\
 &= (\alpha + a\beta)(q \perp a\beta\alpha^{-1}q) \\
 &\quad \text{car } \alpha \text{ et } \beta \text{ sont des facteurs de similitude de } q \\
 &= \alpha(1 + a\beta\alpha^{-1})\langle 1, a\beta\alpha^{-1} \rangle \otimes q \\
 &\cong \alpha\langle 1, a\beta\alpha^{-1} \rangle \otimes q \\
 &\quad \text{car } \langle 1, a\beta\alpha^{-1} \rangle \text{ est multiplicative et représente } 1 + a\beta\alpha^{-1} \\
 &\cong \alpha q \perp a\beta q \\
 &\cong q \perp aq.
 \end{aligned}$$

donc $\delta \in G(q \perp aq)$.

L'autre inclusion $G(q \perp aq) \subset D(q \perp aq)$ est facile. En effet, q est anisotrope et multiplicative, donc $D(q) = G(q)$. Comme $1 \in G(q)$, alors $1 \in D(q)$ et $q \perp aq$ représente 1, donc tous ses facteurs de similitudes. \square

Corollaire 2.1.5. Si $a, b \in F^\times$ sont des sommes de 2^n carrés, alors, ab est aussi une somme de 2^n carrés.

Démonstration. Soit q la n -forme de Pfister $\langle\langle 1, \dots, 1 \rangle\rangle$. Alors,

$$D(q) = \{a \in F^\times \mid a \text{ est somme de } 2^n \text{ carrés}\}.$$

Or q est une forme de Pfister, anisotrope, donc $D(q) = G(q)$ est un groupe. \square

2.2 Application au niveau d'un corps

Définition 2.2.1. On appelle *niveau* d'un corps F (commutatif) le plus petit entier $s(F)$ tel que -1 soit somme de $s(F)$ carrés dans F . Si -1 n'est pas somme de carrés dans F , on pose $s(F) = \infty$.

La notation $s(F)$, que l'on emploie usuellement, pour le niveau d'un corps provient du mot allemand « Stufe ».

Revenons au théorème que l'on souhaitait démontrer :

Théorème 2.2.2. Le niveau d'un corps est soit infini, soit une puissance de 2.

Démonstration. Supposons que F soit de niveau fini. Il existe donc un entier $n \in \mathbb{N}$ tel que $2^n \leq s(F) < 2^{n+1}$. Considérons la $(n+1)$ -forme de Pfister

$$q = \langle\langle 1, \dots, 1 \rangle\rangle.$$

Alors, $q = q' \perp q''$ avec $q' = \langle 1, \dots, 1 \rangle$ de dimension $s(F)$ et $q'' = \langle 1, \dots, 1 \rangle$ de dimension $2^{n+1} - s(F) > 0$. Par définition de $s(F)$, -1 est somme de $s(F)$ carrés donc $-1 \in D(q')$. Comme $q'' \neq 0$, alors q'' représente 1 et q est isotrope. Comme elle est multiplicative, elle est hyperbolique, donc

$$\begin{aligned}
 q &\cong 2^n \langle 1, -1 \rangle \\
 &\cong 2^n \langle 1 \rangle \perp 2^n \langle -1 \rangle.
 \end{aligned}$$

Or, par définition, $q \cong 2^n \langle 1 \rangle \perp 2^n \langle 1 \rangle$. Par le théorème de simplification de Witt, on en déduit que $2^n \langle -1 \rangle \cong 2^n \langle 1 \rangle$. Ainsi, $2^n \langle 1 \rangle$ représente -1 , autrement dit, -1 est somme de 2^n carrés. Donc $s(F) = 2^n$. \square

Exemples

1. $s(\mathbb{Q}) = \infty$ et $s(\mathbb{R}) = \infty$. En effet, une somme de carrés est toujours positive, et -1 est strictement négatif.
2. $s(\mathbb{C}) = 1 = 2^0$ car $-1 = i^2$.
3. Si F est un corps fini de cardinal q , il y a trois possibilités :
 - (a) si F est de caractéristique 2, alors $s(F) = 1$ car $-1 = 1^2$.
 - (b) si $q \equiv 1 \pmod{4}$, alors -1 est un carré dans F .
 - (c) si $q \equiv 3 \pmod{4}$, alors -1 n'est pas un carré dans F . En revanche, -1 est somme de deux carrés dans F , car si F est de caractéristique p , q est une puissance de p et $p \equiv 3 \pmod{4}$ et dans \mathbb{F}_p , -1 est somme de deux carrés. En effet, $\{-1 - x^2 \mid x \in \mathbb{F}_p\}$ contient $(p+1)/2$ éléments, donc contient un carré. Ainsi $s(F) = 2$.

Ainsi, un corps de niveau strictement plus grand que 2 est infini, de caractéristique nulle. En effet, si ce n'était pas le cas, il contiendrait un sous-corps isomorphe à \mathbb{F}_p . Il convient maintenant de se demander si l'on peut construire un corps ayant pour niveau une puissance de 2 donnée.

Théorème 2.2.3. Soit F un corps tel que $s(F) = \infty$, et soit $d \in F^\times$ tel que d soit somme de n carrés, mais pas de $n-1$ carrés dans F . Soit r tel que $2^r \leq n < 2^{r+1}$. Alors, $F(-\sqrt{d})$ est de niveau 2^r .

La première question que l'on peut (doit?) se poser suite à l'énoncé de ce théorème est de savoir si un tel corps existe. Cela sera l'objet de la section suivante (sur le théorème de Cassels-Pfister).

Avant de démontrer le théorème, il convient de démontrer quelques lemmes introductifs.

Lemme 2.2.4. Soit $n \in \mathbb{N}$. Notons $m = 2^n$. Soient a_1, \dots, a_m des éléments de F . On pose $a = a_1^2 + \dots + a_m^2$. Il existe une matrice $M \in \mathbf{M}_m(F)$, de première ligne a_1, \dots, a_m , telle que

$$M^t M = {}^t M M = a I_m.$$

Démonstration. Démonstrons ce lemme par récurrence sur n . Pour $n = 0$, le résultat est vrai. Sinon, on applique le résultat à $a_1, \dots, a_{m/2}$ et $a_{m/2+1}, \dots, a_m$, ce qui permet d'obtenir des matrices M_0 et $M_1 \in \mathbf{M}_{m/2}(F)$ telles que

$$M_0 {}^t M_0 = {}^t M_0 M_0 = b I_{m/2} \quad ; \quad M_1 {}^t M_1 = {}^t M_1 M_1 = c I_{m/2}$$

avec

$$b = a_1^2 + \dots + a_{m/2}^2 \quad ; \quad c = a_{m/2+1}^2 + \dots + a_m^2$$

et de premières lignes respectives $(a_1, \dots, a_{m/2})$ et $(a_{m/2+1}, \dots, a_m)$.

On distingue maintenant trois cas :

2.2 Application au niveau d'un corps

1. Si $b \neq 0$, on pose

$$M = \begin{pmatrix} M_0 & M_1 \\ -1/b {}^t M_0 {}^t M_1 M_0 & {}^t M_0 \end{pmatrix}$$

2. si $b = 0$ et $c \neq 0$, on pose

$$M = \begin{pmatrix} M_0 & M_1 \\ {}^t M_1 & -1/c {}^t M_1 {}^t M_0 M_1 \end{pmatrix}$$

3. si $b = c = 0$, on pose

$$M = \begin{pmatrix} M_0 & M_1 \\ -M_0 & M_1 \end{pmatrix}$$

La matrice M a alors les propriétés recherchées. □

Lemme 2.2.5. On pose $m = 2^n$ (avec $n \in \mathbb{N}$). Soient $a_1, \dots, a_m, b_1, \dots, b_m$ des éléments de F . Il existe c_2, \dots, c_m de F tels que

$$(a_1^2 + \dots + a_m^2)(b_1^2 + \dots + b_m^2) = (a_1 b_1 + \dots + a_m b_m)^2 + c_2^2 + \dots + c_m^2.$$

Démonstration. Ceci découle du lemme précédent. On note A et B les matrices de $M_m(F)$ telles que

$$A^t A = {}^t A A = a I_m \quad ; \quad a = a_1^2 + \dots + a_m^2$$

$$B^t B = {}^t B B = b I_m \quad ; \quad b = b_1^2 + \dots + b_m^2$$

et de premières lignes respectives $(a_1, \dots, a_m), (b_1, \dots, b_m)$.

On pose $C = A^t B$ et c_1, \dots, c_m la première ligne de C . On a donc $C^t C = ab I_m$, d'où $ab = c_1^2 + \dots + c_m^2$, avec $c_1 = a_1 b_1 + \dots + a_m b_m$, ce qui achève la preuve. □

On peut maintenant prouver le résultat clé du théorème :

Lemme 2.2.6. Soit F un corps de niveau infini, et $d \in F^\times \setminus F^{\times 2}$. Alors, d est somme de $2s(F(\sqrt{-d})) - 1$ carrés dans F si $s(F(\sqrt{-d})) < +\infty$.

Démonstration. Posons $s = s(F(\sqrt{-d}))$. Il existe alors des éléments $a_1, \dots, a_s, b_1, \dots, b_s$ tels que

$$\sum_{i=1}^s (a_i + b_i \sqrt{-d})^2 = -1.$$

Donc,

$$\sum_{i=1}^s (a_i^2 - db_i^2) = -1 \quad ; \quad \sum_{i=1}^s a_i b_i = 0$$

puis en réarrangeant et en multipliant le premier membre par $\sum_{i=1}^s b_i^2$.

$$d \left(\sum_{i=1}^s b_i^2 \right)^2 = \left(\sum_{i=1}^s a_i^2 \right) \left(\sum_{i=1}^s b_i^2 \right) + \sum_{i=1}^s b_i^2.$$

D'après le lemme précédent, $(\sum_{i=1}^s a_i^2) (\sum_{i=1}^s b_i^2)$ est somme de $s - 1$ carrés. En effet, $\sum_{i=1}^s a_i b_i = 0$. De plus,

$$\sum_{i=1}^s b_i^2 \neq 0$$

sinon, on aurait $\sum_{i=1}^s a_i^2 = -1$ et ceci contredit $s(F) = \infty$. Ainsi, on peut diviser par $(\sum_{i=1}^s b_i^2)^2 \neq 0$ et d est somme de $2s - 1$ carrés dans F . \square

Démonstration du théorème. Si d est somme de n carrés, mais pas de $n - 1$ carrés, il existe des éléments $a_1, \dots, a_n \in F$ tels que

$$d = a_1^2 + \dots + a_n^2.$$

Posons $a = \sqrt{-d}$. On trouve alors,

$$-a = a_1^2 + \dots + a_n^2,$$

donc -1 est somme de n carrés dans $F(a)$, donc $s(F(a)) \leq n$, mais comme c'est une puissance de 2, $s(F(a)) \leq 2^r$ où $r \in \mathbb{N}$ tel que $2^r \leq n < 2^{r+1}$. D'autre part, d'après le lemme précédent, d est somme de $2s(F(a)) - 1$ carrés dans F , donc $n \leq 2s(F(a)) - 1$. Finalement, $s(F(a)) \geq 2^{r-1} + \frac{1}{2}$ et comme c'est une puissance de 2, $s(F(a)) \geq 2^r$ et on a $s(F(a)) = 2^r$, ce qui achève la preuve du théorème. \square

2.3 Théorème de Cassels-Pfister et conséquences

Dans le théorème de la section précédente, on a fait l'hypothèse qu'il existait un corps de niveau infini (i.e. *formellement réel*) tel qu'il existe un élément d du corps somme de n carrés mais pas de $n - 1$ carrés. L'objectif de cette section est d'exhiber un tel corps.

Comme un corps de caractéristique 2 est de niveau 1, on peut supposer pour la suite que l'on travaille sur un corps F de caractéristique différente de 2.

Lemme 2.3.1. *Soit (V, q) une forme quadratique. Si q est anisotrope sur F , alors q est anisotrope sur $F(X)$.*

Démonstration. Toute forme quadratique étant diagonalisable, on peut supposer que $q = \langle a_1, \dots, a_n \rangle$. Par contraposée, si q isotrope sur $F(X)$, alors il existerait des polynômes $P_0(X), P_1(X), \dots, P_n(X)$, avec $P_0 \neq 0$ et P_1, \dots, P_n non tous nuls tels que

$$0 = \sum_{i=1}^n a_i \left(\frac{P_i(X)}{P_0(X)} \right)^2.$$

En multipliant par $P_0(X)^2$ et en comparant les termes de plus haut degré, on trouve une relation non triviale en les a_i de somme nulle, donc q est isotrope sur F . \square

Corollaire 2.3.2. **1.** $D_{F(X)}(q) \cap F^\times = D_F(q)$.
2. -1 est une somme de n carrés dans F si et seulement si -1 est une somme de n carrés dans $F(X)$.

Démonstration. **1.** Soit $d \in D_{F(X)}(q) \cap F^\times$. On applique la contraposée du lemme précédent à $q \perp \langle -d \rangle$ (anisotrope sur $F(X)$), donc il existe $x \in V, y \in F, x \neq 0$ tels que

$$q(x) - dy^2 = 0.$$

Si $y = 0$, alors $q(x) = 0$ et q est isotrope donc représente d . Sinon, $q(xy^{-1}) = d$ et $d \in D_F(q)$.

2. On applique ce qui précède à $d = -1$ et $q = n\langle 1 \rangle$, et le résultat est immédiat. \square

Théorème 2.3.3. (Cassels-Pfister). Soient (V, φ) une forme quadratique sur F , $\varphi = \langle a_1, \dots, a_n \rangle$ et $f(X) \in D_{F(X)}(\varphi) \cap F[X]$ un polynôme représenté par φ sur le corps $F(X)$. Alors, f est représenté par φ sur l'algèbre $F[X]$.

Démonstration. Si φ est isotrope, alors $\varphi \cong \langle 1, -1, *, \dots, * \rangle$, et la formule

$$f(X) = \left(\frac{f(X) + 1}{2} \right)^2 - \left(\frac{f(X) - 1}{2} \right)^2$$

montre que f est représenté par φ sur $F[X]$.

Si φ est anisotrope sur F , alors par le lemme précédent, elle est anisotrope sur $F(X)$. Il existe donc des polynômes $P_0(X) \neq 0$ et $P_1(X), \dots, P_n(X)$ non tous nuls tels que

$$f(X) = a_1 \left(\frac{P_1(X)}{P_0(X)} \right)^2 + \dots + a_n \left(\frac{P_n(X)}{P_0(X)} \right)^2.$$

Si $d \geq 1$, on va pouvoir trouver une autre représentation de f avec un polynôme au dénominateur de degré strictement inférieur à d . Finalement, on arrivera à un dénominateur de degré nul, ce qui nous permettra alors de conclure. Supposons pour le moment que $d \geq 1$. On effectue alors la division euclidienne de P_i par P_0 pour $i \in \{1, \dots, n\}$. Il existe donc des polynômes $Q_1, \dots, Q_n \in F[X]$, $R_1, \dots, R_n \in F[X]$ avec $\deg(R_i) < d = \deg(P_0)$ tels que

$$\forall i \in \{1, \dots, n\}, \quad P_i(X) = Q_i(X)P_0(X) + R_i(X).$$

Considérons alors la forme quadratique ψ sur $F(X)$ définie par

$$\psi = \langle -f \rangle \perp \varphi = \langle -f, a_1, \dots, a_n \rangle.$$

Notons $Q_0 = 1$ et $R_0 = 0$.

Si $\psi(Q_0, Q_1, \dots, Q_n) = 0$, alors

$$0 = -fQ_0^2 + \varphi(Q_1, \dots, Q_n)$$

d'où

$$f = \varphi(Q_1, \dots, Q_n)$$

donc f est représentée par φ sur $F[X]$.

Si $\psi(Q_0, \dots, Q_n) \neq 0$, notons $P = (P_0, \dots, P_n)$, $Q = (Q_0, \dots, Q_n)$. Considérons alors

$$H = \psi(Q)P - 2b_\psi(P, Q)Q.$$

Comme $\psi(P) = 0$, alors Q n'est pas un multiple de P et $H \neq 0$. Les composantes de H sont des polynômes en X et H est isotrope. En effet,

$$\psi(H) = b_\psi(H, H) = \psi(Q)^2 \underbrace{\psi(P)}_{=0} - 4\psi(Q)b_\psi(Q, P)^2 + 4b_\psi(P, Q)^2\psi(Q) = 0.$$

Notons alors $H = (H_0, \dots, H_n)$. Supposons que $H_0 = 0$, alors

$$\psi(H) = 0 = \varphi(H_1, \dots, H_n)$$

et comme $H \neq 0$ alors φ est isotrope sur $F(X)$, ce qui est absurde. Donc $H_0 \neq 0$ et $\psi(H) = 0$ équivaut donc à

$$F(X) = a_1 \left(\frac{H_1}{H_0} \right)^2 + \dots + a_n \left(\frac{H_n}{H_0} \right)^2.$$

reste à montrer que $\deg(H_0) < d = \deg(P_0)$ et on aura trouvé une autre expression de f dans $F(X)$ avec un dénominateur de degré strictement inférieure au degré du dénominateur de l'expression initiale, et c'est ce que l'on voulait faire. Or,

$$\begin{aligned} H_0 &= \left(-fQ_0^2 + \sum_{i=1}^n a_i Q_i^2 \right) P_0 - 2 \left(-fP_0Q_0 + \sum_{i=1}^n a_i P_i Q_i \right) Q_0 \\ &= \frac{1}{P_0} \left(\sum_{i=1}^n a_i (Q_i P_0)^2 \right) - fP_0 + 2fP_0 - 2 \times \frac{1}{P_0} \left(\sum_{i=1}^n a_i P_i (Q_i P_0) \right) \quad \text{car } Q_0 = 1 \\ &= \frac{1}{P_0} \left(\sum_{i=1}^n a_i (P_i - P_0 Q_i)^2 \right) - \underbrace{\left(-fP_0 + \sum_{i=1}^n a_i P_i^2 \right)}_{=\psi(P)=0} \\ &= \frac{1}{P_0} \sum_{i=1}^n a_i R_i^2 \end{aligned}$$

donc $\deg(H_0) \leq 2 \max_{i=1, \dots, n} (\deg(R_i)) - \deg(P_0) < \deg(P_0)$. □

On va déduire de ce théorème le second¹ théorème de représentation.

Théorème 2.3.4. (*Second théorème de représentation*). Soient $n \geq 2$ et $\varphi = \langle a_1, \dots, a_n \rangle$ une forme anisotrope sur F et $\delta \in F^\times$. Posons alors $\psi = \langle a_2, \dots, a_n \rangle$. Alors

$$\delta \in D_F(\psi) \iff a_1 X^2 + \delta \in D_{F(X)}(\varphi).$$

Démonstration. Supposons que $a_1 X^2 + \delta \in D_{F(X)}(\varphi)$. Par le théorème précédent, il existe une équation

$$a_1 X^2 + \delta = a_1 P_1(X)^2 + \dots + a_n P_n(X)^2$$

1. Le premier théorème de représentation indique que si d est représenté par q si et seulement si $q \perp \langle -d \rangle$ est isotrope.

avec $P_1, \dots, P_n \in F[X]$.

Supposons qu'il existe un P_i de degré au moins 2, alors en regardant les termes de plus haut degré dans l'équation précédente, on va avoir une somme de $a_i p_i^2$ nulle alors que les p_i^2 ne seront pas nuls, donc φ est isotrope. C'est absurde, donc tous les P_i sont linéaires ou constants. Soient $a, b \in F$ tels que $P_1 = aX + b$. Un des polynômes $(a - 1)X + b$ ou $(a + 1)X + b$ n'est pas constant, donc admet une racine c . Évaluons donc l'équation précédente en c :

$$a_1 c^2 + \delta = a_1 \underbrace{P_1(c)^2}_{=c^2} + \sum_{i=2}^n a_i P_i(c)^2$$

et en simplifiant par $a_1 c^2$, on observe que $\delta \in D_F(\psi)$.

Réciproquement, si $\delta \in D_F(\psi)$, comme $X \in F(X)$, alors $a_1 X^2 + \delta \in D_{F(X)}(\varphi)$. \square

Déduisons de ce théorème deux corollaires qui vont (enfin) nous permettre de répondre au problème initial.

Corollaire 2.3.5. Soient F un corps formellement réel et $\delta \in F^\times$ tel que $\delta + X^2$ est une somme de n carrés dans $F(X)$, alors δ est une somme de $n - 1$ carrés dans F .

Démonstration. On applique le théorème précédent à $\varphi = n\langle 1 \rangle$, et le résultat tombe immédiatement \square

Corollaire 2.3.6. (Théorème de Cassels). Soit F un corps formellement réel. Alors $1 + X_1^2 + X_2^2 + \dots + X_n^2$ ne peut-être somme de n carrés dans $F(X_1, \dots, X_n)$.

Démonstration. Supposons que $1 + X_1^2 + \dots + X_n^2$ soit représenté par $\varphi = n\langle 1 \rangle$. Par le théorème précédent, $\delta = 1 + X_1^2 + \dots + X_{n-1}^2$ est représenté par $\psi = (n - 1)\langle 1 \rangle$ dans $F(X_1, \dots, X_{n-1})$ et en itérant ce procédé, on trouve que $1 + X_1^2$ est un carré dans $F(X_1)$, ce qui est faux. \square

On rappelle donc qu'on cherchait un corps formellement réel tel qu'il existe un élément d du corps somme de n carrés mais pas de $n - 1$ carrés. Considérons par exemple le corps $\mathbb{R}(X_1, \dots, X_n)$, formellement réel (sinon -1 serait somme d'un nombre fini de carrés dans \mathbb{R} d'après le corollaire 2.3.2). Considérons alors $d = X_1^2 + \dots + X_n^2$. D'après le corollaire précédent, $X_1^2 + \dots + X_n^2$ est une somme de n carrés mais pas de $n - 1$ carrés. On a alors ce que l'on voulait. On en déduit que, pour tout $r \in \mathbb{N}$, on peut construire un corps de niveau 2^r .