Formes quadratiques et groupe de Brauer

Jeffrey Kranhold
Exposé de maîtrise encadré par P.Gille

1er août 2007

Résumé

Dans cet exposé je vais présenter, après une brève introduction à la théorie des espaces quadratiques, quelques résultats sur les formes quadratiques multiplicatives. Seront étudiées principalement les formes multiplicatives au sens de Pfister et de Hurwitz, incluant les théorèmes d'existence et de non-existence respectivement. Ainsi on verra comment le problème de décomposition d'une somme de carrés mène à des calculs de groupes de Brauer.

Table des matières

1 Introduction

Le point de départ de cette petite enquête est le problème de la décomposition d'une somme de carrés : dans quelles conditions peut-on, pour un entier naturel n, écrire

$$(x_1^2 + .. + x_n^2)(y_1^2 + .. + y_n^2) = z_1^2 + .. + z_n^2$$

où tous les x_i, y_i, z_i sont des éléments d'un corps de caractéristique différente de 2 ? Dans le cas des réels on pourrait définir de tels z_i à l'aide de la racine carrée, ce qui motive à poser des conditions supplémentaires.

La théorie de Pfister montre qu'on peut obtenir des z_i dépendant de manière polynômiale des x_i et des y_i (et mieux : linéairement - dans un certain sens - du vecteur $(y_1, .., y_n)$) si n est une puissance de 2.

D'autre part, par le théorème de Hurwitz, des z_i étant des fontions bilinéaires en les deux vecteurs $(x_1, .., x_n)$ et $(y_1, .., y_n)$ ne peuvent exister que si n est égal à $1, 2, 4$ ou 8, ce qui fait penser à un théorème de la topologie algébrique.

2 Préliminaires

On se donne un corps commutatif k de caractéristique différente de 2.

Définition. *Un* espace quadratique *de* dimension n *sur* k *est un couple* (V, q) *où* V *est un* k*-espace vectoriel de dimension finie* n *et* q *une* application quadratique *sur* V*, i.e. une application* $V \to k$*, vérifiant les deux conditions suivantes :*

1. *Pour tous* $v \in V$ *et* $a \in k$*, on a* $q(a \cdot v) = a^2 \cdot q(v)$ *et*
2. *l'application* $B_q : V \times V \to K$ *définie par* $(x, y) \mapsto \frac{1}{2}(q(x + y) - q(x) - q(y))$ *est* k*-bilinéaire.*

Deux espaces quadratiques (V, q) *et* (V', q') *sont* isométriques *s'il existe un* k*-isomorphisme* $T : V \to V'$ *tel que* $q' \circ T = q$*. On écrit* $(V, q) \cong (V', q')$*.*

Définition. *Une* forme quadratique *sur* k *est un polynôme homogène*

$$f(X_1, .., X_n) = \sum_{i,j}^{n} a_{ij} X_i X_j$$

de degré 2 *dans* $k[X_1, .., X_n]$*. Cette forme est dite* diagonale *si la matrice* $A_f = (a_{ij})$ *l'est, i.e.* $a_{ij} = 0$ *pour* $i \neq j$*. Deux formes* f *et* g *quadratiques sont dites* équivalentes *s'il existe une matrice* $G \in GL_n(k)$ *telle que* $M_f = G^t M_g G$*, c'est-à-dire* $f(X) = X^t M_f X = g(G \cdot X)$ *pour tous* $X \in k^n$*.*

Étant donné un espace quadratique (V, q) on y associe comme ci-dessus la forme bilinéaire symétrique B_q. En choississant une base et en écrivant $B_q(x, y) = x^t A y = \sum_{i,j}^n a_{ij} x^i y^j$ on obtient une matrice symétrique et on voit qu'il y a une correspondance bijective entre classes d'isométrie d'espaces quadratiques et classes de congruence de matrices symétriques.

D'autre part étant donné une forme quadratique f on peut supposer la matrice associée M_f symétrique (quitte à remplacer a_{ij} par $a'_{ij} = \frac{1}{2}(a_{ij} + a_{ji})$) et on obtient une correspondance entre classes d'équivalence de matrices symétriques et classes d'équivalence de formes quadratiques.

Ces correspondances permettent de confondre les notions de formes quadratiques et espaces quadratiques et des constructions portant sur les unes se transportent de façon canonique aux autres et réciproquement.

Définition. *Un espace quadratique* (V, q) *est* régulier *(ou* non dégénéré*) si l'application* B_q *l'est, i.e. si pour tout* $v \in V$ *il existe un* $w \in v$ *tel que* $B_q(v, w) \neq 0$*.*

On dit qu'un élément $a \in k$ *est* représenté *par* q *s'il existe un vecteur non nul* $v \in V$ *tel que* $q(v) = a$*. On note* $D_K(q)$ *l'ensemble des éléments représentés par* q *et on pose* $D_K^*(q) = D_K(q) \backslash \{0\}$*.*

L'espace est isotrope *si on a* $0 \in D_K(q)$ *et* anisotrope *sinon. Il est* universel *si* q *représente tout élément non nul de* k*, i.e.* $D_k^*(q) = k^\times$.

Un sous-espace $S \subset V$ *est régulier (isotrope, anisotrope) s'il l'est vu comme espace quadratique (muni de l'application* $q|_S$*).*

Lemme. *Soit* f *une forme quadratique sur* k*. Alors* f *est équivalente à une forme diagonale* f' *de matrice diagonale* (a'_{ij})*. Dans ce cas, tout élément représenté par* f *peut paraître comme* a'_{11}*.*

Démonstration. Voir [Pfi95] ou [Lan84].

Ainsi tout espace quadratique possède une représentation diagonale qui est unique à isométrie près. Pour la suite, on va donc supposer $V = k^n$ et q diagonale. On note $\langle x_1, .., x_n\rangle$ la forme diagonale de matrice $A = (a_{ij})$, $a_{ii} = x_i$.

Définition. *Soient* $f = \langle a_1, ..a_n\rangle$ *et* $f' = \langle b_1, .., b_m\rangle$ *deux formes quadratiques.*

1. *Leur* somme directe *est la forme* $f \oplus f' = \langle a_1, .., a_n, b_1, .., b_m\rangle$.
2. *Leur* produit tensoriel *est la forme* $f \otimes f' = \langle .., a_i b_j, ..\rangle$.
3. *Pour un entier* $r \in \mathbb{N}$*, on note* $r \times f$ *la forme* $f \oplus .. \oplus f$ *(*r *termes) et on pose* $0 \times f$ *la forme nulle.*

Remarque. *Donc si* (V, q) *et* (V', q') *sont deux espaces quadratiques quelconques, la définition précédente doit être interprétée comme suit. On a des* k*-isomorphismes* $T : V \to k^n$ *et* $T' : V' \to k^m$ *avec* $q \circ T^{-1}$ *et* $q' \circ (T')^{-1}$ *des formes diagonales. Le produit tensoriel des deux espaces est le* k*-espace vectoriel* $V \otimes V'$ *muni de la forme* $((q \circ T^{-1}) \otimes (q' \circ (T')^{-1})) \circ (T \otimes T')$*. Pour leur somme directe, la construction ci-dessus est une version très pompeuse de munir le* k*-espace vecoriel* $V \oplus V'$ *de l'application quadratique qui envoit* $v + v'$ *sur* $q(v) + q'(v')$.

Un calcul direct montre qu'à isométrie près, l'addition est commutative et assiciative et que la multiplication est associative, commutative et distributive par rapport à l'addition.

On note $G(k)$ le groupe abélien $k^\times/(k^\times)^2$.

Définition. *Soit* f *une forme quadratique sur* k^n *comme dans la définition précédente. On appelle* determinant *de* f *l'élément* $det(f) = \prod_{i=1}^n a_i \cdot (k^\times)^2$ *dans* $G(k)$ *et* discriminant *de* f *l'élément* $d(f) = (-1)^{\frac{(n-1)n}{2}} \cdot det(f)$*. Notons que ces deux applications sont des morphismes de groupes abéliens :*

Si (V, q) est un espace quadratique quelconque, on définit son discriminant et son déterminant comme dans le cas des sommes et des produits. On se convainc que ceci ne dépend pas du choix d'isomorphisme de diagonalisation et de plus que det et d sont invariants par des isométries d'espaces quadratiques. Pour voir ceci il suffit de montrer que si les formes $\langle a_1, .., a_n\rangle$ et $\langle a'_1, .., a'_n\rangle$ sont équivalentes, alors elles ont même déterminant (et, par conséquent, même discriminant). Soit $T \in GL_n(k)$ une matrice inversible telle que $T^t A T = A'$ ou A

et A' sont les matrices diagonales avec les entrées $a_1, ..a_n$ et $a'_1, .., a'_n$ respectivement. Soit Det l'application déterminant des matrices. Alors $Det(A) \cdot (k^\times)^2 = det(\langle a_1, .., a_n \rangle)$ et $Det(A') \cdot (k^\times)^2 = det(\langle a'_1, .., a'_n \rangle)$. Donc, par multiplication des determinants de matrices, $Det(A') = Det(T)^2 Det(A)$ et $det(\langle a_1, .., a_n \rangle) = det(\langle a'_1, .., a'_n \rangle)$.

Lemme. *Si (V, q) est un espace quadratique régulier un sous-espace $S \subset V$ est régulier si et seulement s'il existe $(T \subset V)$ tel que $(V, q) = (S, q|_S) \oplus (T, q|_T)$.*

L'anneau de Witt

Tous les résultats dans ce paragraphe sont démontrés dans [Lam80] ou dans [Lan84].

Lemme. *Pour un espace quadratique de dimension 2 (V, q), il y a équivalence entre*

1. *L'espace (V, q) est régulier et isotrope et*
2. *Il est isométrique à $(k^2, \langle 1, -1 \rangle)$.*

Un tel espace est dit *plan hyperbolique* et sa classe d'isométrie est notée $\mathcal{H}$. Un espace est *hyperbolique* s'il est isométrique à une somme directe de plans hyperboliques.

Lemme. *Soit (V, q) un espace quadratique régulier.*

1. *Si (V, q) est isotrope, alors il est universel.*
2. *Un sous-espace $U \subset V$ de dimension r est totalement isotrope (i.e. $q|_U = 0$) si et seulement s'il existe un sous-espace hyperbolique $T \subset V$ de dimension $2r$ contenant U.*
3. *L'espace (V, q) est isotrope si et seulement s'il contient un plan hyperbolique.*
4. *Un élément $a \in F^*$ est représenté par (V, q) si et seulement si $(V \oplus k, q \oplus \langle -a \rangle)$ est régulier.*

Théorème 1 (Théorème d'annulation de Witt). *Soient (V, q), (V', q') et (V'', q'') trois espaces quadratiques. Si $V \oplus V'$ et $V \oplus V''$ sont isométriques, alors V' et V'' le sont aussi.*

Théorème 2 (Décomposition de Witt). *Soit (V, q) un espace quadratique. Alors il se décompose en une somme directe $(V, q) = (V_t, q_t) \oplus (V_h, q_h) \oplus (V_a, q_a)$, où (V_t, q_t) est totalement isotrope, (V_h, q_h) est hyperbolique et (V_a, q_a) est anisotrope. Les trois termes sont uniques à isométrie près.*

Définition. *Deux espaces quadratiques (V, q) et (V', q') sont* Witt-équivalentes *si les espaces (V_a, q_a) et (V', q') sont isométriques. On écrit $(V, q) \sim (V', q')$. Le nombre $\frac{1}{2} dim V_a$ est* l'indice de Witt *de (V, q).*

Soit (V, q) un espace quadratique régulier de dimension n. On note $-(V, q)$ l'espace V muni de l'application quadratique $v \mapsto -q(v)$. La somme $(V \oplus V, q \oplus (-q))$ contient le sous-espace $(W = \{(v, v) : v \in V\}, (q \oplus (-q))|_W)$ qui est totalement isotrope et de dimension n, donc contenu dans un espace hyperbolique de dimension $2n = dim(V \oplus V)$, ce qui montre que $(V, q) \oplus (V, -q)$ est hyperbolique.

Notons $W(k)$ l'ensemble des classes d'équivalence de Witt de tous les espaces quadratiques réguliers sur k. Il est appellé le *groupe de Witt* de k. La remarque précédente montre qu'il devient un groupe abélien par rapport à la somme directe (un calcul simple montre que $q \mapsto q_a$ est, à isométrie près, stable sous $\oplus$). De plus, on observe que grâce à la distributivité du produit tensoriel des espaces quadratiques par rapport à leur somme directe et comme, pout tout $a \in k$ non nul, on a $\langle a \rangle \otimes \langle 1, -1 \rangle = \langle a, -a \rangle \cong \langle 1, -1 \rangle$ (la dernière équivalence découlant du fait que l'espace $(k^2, \langle a, -a \rangle)$ est régulier et isotrope), le produit tensoriel d'espaces quadratiques fait de $W(k)$ un anneau commutatif, appellé *anneau de Witt* de k. Les propriétés d'associativité, commutativité et distributivité découlent des calculs directs.

D'autre part, on peut considérer le semi-groupe des classes d'isométrie de tous les espaces quadratiques réguliers sur k muni de la loi de la somme directe, noté $M(k)$. Son groupe de Grothendieck est appellé *groupe de Witt-Grothendieck* de k, $WG(k)$. On a un morphisme de groupes abéliens $\mathbb{Z} \to WG(k)$, donné par $z \mapsto (z \times \mathcal{H}, 0)$. Le quotient de $WG(k)$ par son image est isomorphe comme groupe abélien à $W(K)$.

On voit facilement que, si on pose $dim_0(V, q) := dimV mod 2$, ceci induit un morphisme de groupes abéliens $dim_0 : W(k) \to Z_2$. Son noyau est noté Ik et appellé *idéal fondamental* de k. Ceci est en fait un idéal, car un élément $[(V, q)]$ de $W(k)$ est envoyé sur $0 \in \mathbb{Z}_2$ si et seulement si la dimension de V est paire. Or la dimension du produit tensoriel d'un espace vectoriel de dimension paire avec un espace vectoriel quelconque est paire. Clairement $I(k)$ est engendré comme idéal par les classes d'équivalence de Witt des espaces quadratiques $(k^2, \langle a, b \rangle)$. Notons $I^n k$ le produit n-ième de Ik avec lui-même. Par conséquence, cet idéal est engendré par les produits $\langle a_1, b_1 \rangle \otimes .. \otimes \langle a_n, b_n \rangle$.

Définissons le groupe abélien $Q(k)$ comme l'ensemble $\mathbb{Z}_2 \times G(k)$, muni de la multiplication $(e, a) \cdot (e', a') := (e + e', (-1)^{ee'} aa')$. Alors l'application $f := (dim_0, d) : W(k) \to Q(k)$ est un morphisme de groupes abéliens.

Lemme. *Le noyau de f est égal à $I^2 k$.*

Démonstration. Considérons la forme quadratique $\langle a, b \rangle \otimes \langle c, d \rangle = \langle ac, ad, bc, bd \rangle$. Clairement l'image de sa classe dans $W(k)$ sous f est $0 \in Q(k)$ (car elle est de dimension paire et son discriminant est 1). Or les classes des formes de ce type engendrent l'idéal $I^2 k$.

D'autre part, supposons que (V, q) dont la classe dans $W(k)$ est dans le noyau de f. En particulier, il est de dimension paire et de forme diagonale $\langle a_1, .., a_{2n} \rangle$. Si $n = 1$, la forme diagonale est $\langle a_1, a_2 \rangle$ et son discriminant est $-a_1 a_2 \in G(k)$. Or ce discriminant est 1, donc on doit avoir $a_1 = -x^2 a_2$ pour un $x \in k^\times$ (rappellons que la forme est régulière). Mais maintenant $\langle a_1, -x^2 a_2\rangle = \langle a_1\rangle \otimes \langle 1, -1\rangle$ et $\langle 1, -1\rangle$ est l'élément zéro dans $W(k)$, donc la classe de (V, q) est $0 \in W(k)$ qui est contenu dans $I^2 k$.

Si $n > 1$, écrivons $\langle a_1, .., a_{2_n}\rangle$ comme somme directe $\langle a_1, .., a_3\rangle \oplus \langle a_4, .., a_{2n}\rangle$ et en ajoutant un $0 \in W(k)$, on voit que ceci est équivalent au sens de Witt à $\langle a_1, a_2, a_3, a_1 a_2 a_3\rangle \oplus \langle -a_1 a_2 a_3, a_4, .., a_{2n}\rangle$. Le terme gauche dans cette somme est le produit tensoriel $\langle a_1, a_2\rangle \otimes \langle 1, a_1 a_3\rangle$ et donc bien contenu dans $I^2 k$. Le terme droit a même discriminant que q et est de dimension $2n - 2$. Par l'hypothèse de recurrence, il est donc contenu dans $I^2 k$. $\square$

Exemple. *Comme toutes les formes réelles* $\langle a_1, .., a_n\rangle$ *avec des* a_i *de signes différents représentent* 0 *et que tous les formes* $\langle a\rangle$ *avec a positif (ou négatifs, respectivement) sont équivalentes (tout réel positif est un carré), les seules espaces réels anisotropes sont l'espace nul, muni de la forme nulle ainsi que tous les* $r \times \langle 1\rangle$ *et les* $r \times \langle -1\rangle, r \in \mathbb{N}$. *Donc le groupe de Witt de* $\mathbb{R}$ *est isomorphe à* $\mathbb{Z}$ *et pour* $n \in \mathbb{N}$*, l'image de l'idéal* $I^n\mathbb{R}$ *sous cet isomorphe est* $2^n\mathbb{Z}$.

3 Les formes de Pfister

Définition. *Soient* $a_1, .., a_n$ *des éléments non nuls dans* k*. La forme quadratique*

$$\langle\langle a_a, .., a_k\rangle\rangle := \langle 1, a_1\rangle \otimes .. \otimes \langle 1, a_n\rangle$$

est appellée n-forme de Pfister *(associée aux éléments* $a_1, .., a_n$*) sur* k.

Notons que si a et b sont deux éléments de k, la somme $\langle 1, a\rangle \oplus \langle 1, -b\rangle$ est équivalente à $\langle a, b, 1, -1\rangle$. Par conséquent, dans $W(k)$ on a $(k^2, \langle a, b\rangle) \sim (k^2, \rangle 1, a\rangle) \oplus (-(k, \langle 1\rangle)) \otimes (k^2, \langle 1, -b\rangle)$. Ceci montre que l'idéal fondamental de k est engendré par les classes des formes de Pfister $\langle\langle a\rangle\rangle$ et son produit n-ième par les formes de Pfister n-ièmes.

Définition. *Une forme quadratique* $f : k^n \to k$ *est dite* multiplicative *s'il existe une fonction rationelle* $z \in k(X_1, ..X_n, Y_1, .., Y_n)$ *telle que* $f(x)f(y) = f(z(x, y))$ *pour tous* $x, y \in k^n$*. Elle est* strictement multiplicative *si l'on peut choisir* z $k(x)$*-linéaire en* y*, i.e.* $z(X, Y) = T(X) \cdot Y$ *avec* $T(X) \in M_n(K(X_1, .., X_n))$.

Remarque. *Pour la démonstration du théorème suivant, notons que si la forme* $\langle a, b\rangle$ *représente l'élément non nul* c *sur* k*, alors elle est équivalente à* $\langle c, abc\rangle$*. En effet, comme tout élément réprésenté par* $\langle a, b\rangle$ *peut paraître en première position de sa représentation diagonale et comme tout ces représentations diagonales sont équivalentes, on doit avoir* $\langle a, b\rangle \cong \langle c, e\rangle$ *pour un* $e \in k^\times$*. Or le déterminant est invariant par des isométries, donc* $ab^{\cdot} {k^\times}^2 = ce \cdot {k^\times}^2$*, en d'autres termes,* $e = abc$ *dans* $k^\times / {k^\times}^2$*. Mais par conséquent,* $\langle e\rangle \cong \langle abc\rangle$.

Théorème 3. *Pour tout* $n \in \mathbb{N}$ *et des éléments* $a_1, .., a_n \in k^\times$ *non nuls, le* n*-forme de Pfister* $\langle\langle a_1, .., a_n\rangle\rangle$ *est strictement multiplicative.*

Démonstration. Notons $\phi = \langle\langle a_1, .., a_n \rangle\rangle$ On va montrer plus : sur $k(x)$, $\phi(x)\phi$ est équivalente à ϕ, en tant que forme quadratique sur $k(x)$. Ceci entraine que cette forme est strictement multiplicative et sa matrice (qui est dans $M_n(k(x))$) est régulière.

Récurrence sur n. Si $n = 0$, on note que la forme $\langle 1 \rangle$ vérifie cette propriété trivialement sur n'importe quel corps. Soit maintenant $n > 1$. écrivons $\phi = \psi \otimes \langle 1, a \rangle$, avec ψ une $(n-1)$-forme de Pfister. Ainsi on a $\phi = \psi \oplus a\psi$. Par l'hypothèse de récurrence, ceci est équivalent, en tant que forme quadratique sur $k(x) = k(x_I)(x_{II})$ ($x = (x_I, x_{II})$) à $\psi(x_I)\psi \oplus a\psi(x_{II})\psi \cong \langle \psi(x_I), a\psi(x_{II}) \rangle \otimes \psi$. Évidemment, la forme $\langle \psi(x_I), a\psi(x_{II}) \rangle$ représente $\phi(x)$ sur $k(x)$. Cette forme est équivalente, en tant que forme quadratique sur $k(x)$, à $\langle \phi(x), \phi(x)\psi(x_I)a\psi(x_{II}) \rangle$. Donc

$$\phi \cong \langle \psi(x_I), a\psi(x_{II}) \rangle \otimes \psi \cong \phi(x)\langle 1, \psi(x_I), a\psi(x_{II}) \rangle \otimes \psi.$$

Mais ceci est égal à $\phi(x)(\psi \otimes \psi(x_I)a\psi(x_{II})\psi)$ et par l'hypothèse de récurrence, ceci est équivalent sur $k(x)$ à $\phi(x)(\psi \oplus a\psi) \cong \psi(x)\psi$. $\square$

Théorème 4. *Si f est une forme quadratique anisotrope et strictement multiplicative, alors elle est équivalente à une forme de Pfister.*

Théorème 5. *Si f est une forme quadratique isotrope et strictement multiplicative, alors elle est équivalente à un produit $r \times \langle 1, -1 \rangle$, $r \in \mathbb{N}$.*

4 Le groupe de Brauer et l'algèbre de Clifford

Quaternions

Exemple. *Soient a, b deux éléments non nuls dans k. On note $\left(\frac{a,b}{k}\right)$ la k-algèbre engendrée par les éléments i et j avec $i^2 = a$, $j^2 = b$ et $ij = -ji =: l$. On l'appelle* algèbre des quaternions *de a et b sur k. Écrivons $\mathbb{H}$ au lieu de $\left(\frac{-1,-1}{k}\right)$.*

Lemme. *Soient a, b, x, y del éléments non nuls dans k. Alors on a un isomorphisme de k-algèbres*

$$\left(\frac{ax^2, by^2}{k}\right) \cong \left(\frac{a, b}{k}\right).$$

Algèbres de division et algèbres semi-simples

Définition. *Une* **algèbre de divison** *sur k (ou plus généralement sur un anneau commutatif) est une k-algèbre dans laquelle chaque élément non nul est inversible par rapport à la multiplication.*

Exemple. *Les quaternions $\mathbb{H}$ sont une algèbre de division.*

Définition. *Une k-algèbre de dimension finie sur k est dite* simple *si elle ne possède pas d'idéaux bilatères.*

De même, si A est un anneau et M un A-module, on dit que M est *simple* s'il ne contient pas de sous-module propre.

Théorème 6 (Wedderburn). *Soit A une k-algèbre simple. Alors il existe une algèbre de dision D sur k et un entier n tels que $A \cong M_n(D)$, en tant que k-algèbres. De plus, l'entier n est uniquement déterminé et l'algèbre D est unique à isomorphisme près.*

Démonstration. Voit [Ker90]

Théorème 7. *Soit A une k-algèbre simple. Alors tous les A-modules simples sont isomorphes.*

Démonstration. Voir [Bou58a]. □

Remarque. *Donc si A est une algèbre simple, et $A \cong M_n(D)$ avec n, D comme dans le théorème ci-dessus, tous les A-modules simples sont isomorphes à D^n.*

Le groupe de Brauer

La présentation suivante du groupe de Brauer suit principalement [Ker90].

Définition. *Soient A une k algèbre et $S \subset A$ une partie. On note $C_S(A)$ l'ensemble $\{a \in A : s \cdot a = a \cdot s \forall s \in S\}$ et on appelle $Z(A) := C_A(A)$ le* centre *de A. L'algèbre A est dite* centrée *si son centre est reduit à $k \cdot 1_A$.*

Définition. *Une* algèbre d'Azumaya *sur k est une algèbre simple centrée de dimension finie.*

Deux algèbres d'Azumaya A et B sont équivalentes *s'il existe des entiers naturels r et s tels que les algèbres $A \otimes M_r(k)$ et $B \otimes M_s(k)$ sont isomorphes. Dans ce cas on écrit $A \sim B$.*

Remarque. *Le fait que $M_r(k) \otimes M_s(k)$ et $M_{rs}(k)$ sont isomorphes montre que la relation definie ci-dessus est transitive. Comme la symétrie et la reflexivité sont évidentes, elle est en fait une relation d'équivalence. On note $[A]$ la classe d'équivalence de A.*

Si A et B sont deux algèbres d'Azumaya, alors leur produit tensoriel en est aussi une.

On note $B(k)$ l'ensemble des classes d'equivalence d'algèbres d'Azumaya sur k. Muni du produit tensoriel, il devient un semi-groupe (on se convainc facilement que le produit $[A] \cdot [B] := [A \otimes B]$ ne dépend pas du choix des représentants).

En posant $A^{op} = A$, munie de la multiplication $a \cdot^{op} b := b \cdot a$, et en observant que le morphisme de k-algèbres $\rho : A \otimes A^{op} \to End_k(A), a \otimes b \mapsto [x \mapsto axb]$ est injectif (donc bijectif par des raisons de dimension), on voit

$$[A] \cdot [A^{op}] = [A^{op}] \cdot [A] = [k] = 1.$$

L'ensemble $B(k)$ devient donc un groupe abélien, appellé *groupe de Brauer* de k.

Théorème 8 (Frobenius). *Si $k = \mathbb{R}$, le groupe de Brauer $B(\mathbb{R})$ est isomorphe à $\mathbb{Z}_2$, et l'unique élément non trivial est représénté par l'algèbre des quaternions $\mathbb{H}$.*

Démonstration. Voir [Ker90]

Remarque. *Grâce à l'isomorphisme de k-algèbres $M_n(D) \cong D \otimes M_n(k)$, les éléments de $B(k)$ sont donc en correspondance $1-1$ avec les algèbres de division centrales sur k.*

Remarque. *Si $L \supset k$ est une extension de corps, on a un morphisme de groupes $r_{L/k} : B(k) \to B(L), [A] \mapsto [A \otimes_k L]$. On appelle* groupe de Brauer relatif *et en note $B(L/k)$ son noyau.*

*D'autre part, si G est un groupe quelconque, on appelle un grooupe abélien U un G-*module *s'il existe une action de groupe de G sur U qui est compatible avec la multiplication dans U, i.e. on a, pour tous σ dans G et x, y dans U, $\sigma(x \cdot y) = \sigma(x) \cdot \sigma(y)$.*

Soit U un G-module. On pose $\mathcal{C}^0(G,U) := U$ et, pour tout $n \in \mathbb{N}$, $\mathcal{C}^n(G,U)$ l'ensemble des applications $G^n = G \times .. \times G \to U$. Évidemment le $\mathcal{C}^n$ devient un groupe abélien par la multiplication $(f \cdot g)(x) := f(x) \cdot g(x)$. De plus, on définit une suite d'opérateurs $\partial_n : \mathcal{C}^n(G,U) \to \mathcal{C}^{n+1}(G,U)$ par $\partial_0(u)(\sigma) := \sigma(x)x^{-1}$ et $\partial_n(f)(\sigma_1, .., \sigma_{n+1}) := \sigma_1(f(\sigma_2, .., \sigma_{n+1})) \cdot \prod_{i=1}^n (f(\sigma_1, .., \sigma_i \cdot \sigma_{i+1}, .., \sigma_{n+1}))^{(-1)^i} \cdot f(\sigma_1, .., \sigma_n)^{(-1)^{n+1}}$. On note $H^n(G,U)$ le n-ième groupe de cohomologie de du complexe $(\mathcal{C}^*, \partial_*)$.

Dans le cas particulier où L/k est une extension galoisienne de groupe de Galois G et $U = L\backslash\{0\} = L^*$, $H^n(G, L^*)$ est le n-ième groupe de cohomologie de Galois *de cet extension. On peut démontrer*

$$H^2(G, L^*) \cong B(L/k).$$

Le groupe de Brauer-Wall

Dans cette section, je suis le chapitre IV de [Lam80].

Soit A une k-algèbre $\mathbb{Z}_2$-graduée. Un sous-espace $S \subset A$ est dit *homogène* si $S = S_0 \oplus S_1, S_i = S \cap A_i$. Pour un tel espace on définit le *centralisateur gradué* par $\hat{C}_S(A) = C_0 \oplus C_1$, où

$$C_i := \{c \in A_i . \forall a \in A_j : ca = (-1)^{ij} ac\}.$$

On note $\hat{Z}(A)$ et on appelle *centre gradué* de A la sous-algèbre $\hat{C}_A(A)$. L'algèbre A est dite *centrale* si $\hat{Z}(A) = k \cdot 1_A$.

On dit que A est simple si elle ne possède pas d'idéal bilatère **gradué**. Notons qu'une algèbre graduée simple n'a aucune raison d'être simple en tant qu'algèbre non-graduée.

Remarque. *Comme $\mathbb{R}$-algèbre non-graduée, $\mathbb{C}$ n'est pas centrale sur $\mathbb{R}$, car c'est un corps commutatif. Muni de la graduation évidente $\mathbb{C}_0 = \mathbb{R}$ et $\mathbb{C}_1 = \mathbb{R}i$,* *on a* $C_0 = \{x \in R : xz = zx \forall z \in \mathbb{C}\} = \mathbb{R}$ *et* $C_1 = \{iy \in i\mathbb{R} : \forall iy' \in i\mathbb{R} \forall x \in \mathbb{R} : x(iy) = (iy)x, (iy)(iy') = -(iy')(iy)\} = \{0\}$. *Donc* $\mathbb{C}$ *est centrale en tant qu'algèbre graduée sur* $\mathbb{R}$.

Lemme. *Si* A *et* B *sont deux algèbres graduées centrales simples, leur produit tensoriel gradué* $A \hat{\otimes} B$ *en est une.*

Démonstration. Voir [Lam80]

Exemple.

1. *Une algèbre d'Azumaya* B *devient une algèbre graduée centrale simple* (B) *en posant* $(B) := B \oplus 0$.
2. *Soit* $a \in k$. *L'extension* $k(\sqrt{a})$ *peut être graduée par* $k(\sqrt{a}) = k \oplus k\sqrt{a}$. *Comme dans la remarque ci-dessus, on voit de plus qu'elle est centrale comme algèbre* $\mathbb{Z}_2$*-graduée. Or elle est simple, car elle est un corps donc c'est une algèbre graduée centrale simple, notée* $k\langle\sqrt{a}\rangle$.
3. *Une algèbre des quaternoins* $A = \left(\frac{a,b}{k}\right)$ *devient une algèbre graduée centrale simple en posant* $A_0 = k \oplus k \cdot l$ *et* $A_1 = k \cdot i \oplus k \cdot j$. *On la note* $\langle\frac{a,b}{k}\rangle$. *Comme les algèbres* $C_1 = k\langle\sqrt{a}\rangle$ *et* $C_2 = k\langle\sqrt{b}\rangle$ *sont deux algèbre graduée centrale simple, leur produit tensoriel gradué en est une. Or c'est* A.
4. *On munit* $M_n(k)$ *de la* $\mathbb{Z}_2$*-graduation*

$$(M_n)_i = \{A = (a_{rs}) \in M_n : (r+s) \neq i \Rightarrow a_{rs} = 0\}.$$

On voit facilement que l'algèbre graduée obtenue ansi est une algèbre graduée centrale simple et on la note $\hat{M}_n(k)$.
Observation importante. On a un isomorphisme de algèbre graduée centrale simple $\langle\frac{-1,1}{k}\rangle \cong \hat{M}_2(k)$. *Ceci est évident en identifiant* i *à* $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, j *à* $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, l *à* $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ *et* 1 *à* $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.
Plus généralement, si A *est une algèbre* $\mathbb{Z}_2$ *graduée, on notera* $(M_n(A))_i = \{B = (b_{rs}) \in M_n(A) : b_{rs} \in A_{r+s}\}$. *Ainsi on obtient une algèbre* $\mathbb{Z}_2$*-graduée, notée* $\hat{M}_n(A)$. *C'est une algèbre graduée centrale simple si* A *en est une. De plus, on a* $\hat{M}_n(k) \hat{\otimes} \hat{M}_m(A) \cong \hat{M}_{mn}(A)$, *donc en particulier* $\hat{M}_n(k) \hat{\otimes} A \cong \hat{M}_n(A)$.
5. *D'autre part, étant donné une algèbre* $\mathbb{Z}_2$*-graduée* A, *on a une graduation évidente de* $M_n(A)$ *par* $(M_n(A))_i = M_n(A_i)$. *On note l'algèbre graduée obtenue* $\tilde{M}_n(A)$.

Remarque. *Si* A *et* B *sont deux algèbres* $\mathbb{Z}_2$*-graduées, leur produit tensoriel* $A \otimes B$ *peut être muni de la même graduiation que leur produit tensoriel gradué* $A \hat{\otimes} B$. *Ceci fait de* $A \otimes B$ *une algèbre graduée. Seules les lois de multiplication de ces deux algèbres diffèrent, et en général, on n'a pas* $A \otimes B \cong A \hat{\otimes} B$.

De plus, si A *et* B *sont isomorphes comme algèbres non graduées, ceci en général n'entraîne pas l'existence d'un isomorphisme d'algèbres graduées. Néanmoins on a le résultat suivant.*

Lemme. *Soient A une k-algèbre $\mathbb{Z}_2$-graduée et $n, m \geq 1$ deux entiers. On a des isomorphismes d'algèbres graduées*

$$\hat{M}_n(A) \cong A \hat{\otimes} \hat{M}_n(k) \cong A \otimes \hat{M}_n(k)$$

et

$$\hat{M}_m(k) \hat{\otimes} \hat{M}_n(A) \cong \hat{M}_m(k) \otimes \hat{M}_n(A) \cong \hat{M}_{mn}(A).$$

Soient maintenant A et A' deux algèbres graduées centrales simples sur k. On dit qu'elles sont *équvalentes* et on note $A \sim A'$ s'il existe deux k-espaces vectoriels $\mathbb{Z}_2$-gradués V et V' et un isomorphisme d'algèbres graduées

$$A \hat{\otimes} End_k(V) \cong A' \hat{\otimes} End_k(V'),$$

où l'algèbre des endomorphismes d'un k-espace vecotriel $\mathbb{Z}_2$-gradué V est elle-même $\mathbb{Z}_2$-graduée par $End_k(V) = E_0 \oplus E_1$, $E_i = \{f \in End_k(V) : f(V_j) \subset V_{i+j}\}$. Notons qu'on a un isomorphisme

$$End_k(k \times 0 \times k \times, .. \oplus 0 \times k \times 0 \times, ..) \cong \hat{M}_n(k).$$

On note $\langle A \rangle$ la classe d'équivalence d'une algèbre graduée centrale simple A et $BW(k)$ l'ensemble de toutes les classes d'équivalence. De plus, on pose $\langle A \rangle \cdot \langle B \rangle := \langle A \hat{\otimes} B \rangle$, ce qui fait de $BW(k)$ un semi-groupe avec élément neutre $(k) = k \oplus 0$. Pour obtenir une inverse de A, on note A^x l'ensemble $\{a^x, a \in A\}$, muni de la $\mathbb{Z}_2$-graduation $A_i^x := \{a^x, a \in A_i\}$ et de la multiplication induit par $a^x \cdot b^x := (-1)^{ij}(ba)^x$, pour a^x dans A_i^x et b^x dans A_j^x. Finalement, on peut montrer ([Lam80]) $\langle A \rangle \cdot \langle A^x \rangle = \langle A^x \rangle \cdot \langle A \rangle = \langle k \rangle$. Donc $BW(k)$ devient un groupe abélien, appellé *groupe de Brauer-Wall* de k.

Sur la structure des algèbres graduées simples centrales

Soit A est une algèbre graduée centrale simple, $A = A_0 \oplus A_1$, écrivons le centre non-gradué de A comm $Z(A) = k \oplus Z_1$, où $Z_1 \subset A_1$. Les démonstrations des théorèmes suivants se trouvent dans [Lam80].

Théorème 9. *Si $A_1 \neq 0$, alors :*

1. *on a $Z_1 = 0$ si et seulement si A est une algèbre d'Azumaya dur k.*
2. *D'autre part, $Z_1 \neq 0$ si et seulement si A_o est une algèbre d'Azumaya sur k.*

Grâce au théorème précédent, on peut dire que A est *de type pair* si $Z_1 = 0$ et *de type impair* sinon.

Théorème 10. *Soit A de type impair. Alors*

1. *le centre non gradué $Z(A)$ est égal à $C_A(A_0)$ et s'écrit $k \oplus kz$ pour un $z \in Z_1$ tel que $z^2 = a$, $a \in k^\times$ (en identifiant k à $k \cdot 1_A$) et la classe de a dans $G(k)$ ne dépend pas du choix de z. De plus, on a $Z(A) \cong k\langle\sqrt{a}\rangle$ comme algèbre graduées ($Z(A)$ étant munie de la graduation obtenue de son écriture comme somme directe).*

2. *On a un isomorphisme de k-algèbres graduées $A \cong (A_0)\hat{\otimes}k\langle\sqrt{a}\rangle$.*
3. *Si $a \neq 1$ dans $G(k)$, alors A est une algèbre d'Azumaya sur le corps $k(\sqrt{a})$ et $Z(A)$ est isomorphe comme algèbre non-graduée à $k(\sqrt{a})$.*
4. *Si $a = 1$ dans $G(k)$, alors $Z(A)$ est isomorphe comme algèbre non graduée à $k \times k$ et A est isomorphe comme algèbre non graduée à $A_0 \times A_0$.*
5. *L'algèbre A est séparable, donc semi-simple.*

Théorème 11. *Supposons A de type pair et $A_1 \neq 0$. Par le théorème de Wedderburn, il existe un entier $n \in \mathbb{N}$, une algèbre de division centrale D sur k et un isomorphisme d'algèbres non graduées $A \cong M_n(D)$. On a*

1. *Le centre non gradué de A_0 s'écrit $Z(A_0) = C_A(A_0) = k \oplus kz$ pour un $z \in Z(A_0)$ tel que $z^2 = a \in k^\times$. La classe de a dans $G(k)$ ne dépend pas du choix de z.*
2. *Si on a $a = 1 \in G(k)$, alors $Z(A_0)$ est isomorphe comme algèbre non graduée à $k \times k$. De plus il existe un k espace vectoriel $\mathbb{Z}_2$-gradué $V = V_0 \oplus V_1$ de dimension n tel que $A \cong End(V)\hat{\otimes}(D)$. Finalement, on a un isomorphisme d'algèbres non graduées $A_0 \cong M_r(D) \times M_s(D)$, où $r = dim(V_0)$ et $s = dim(V_1)$.*
3. *Soit $a \neq 1$ dans $G(k)$ et supposons qu'il existe un morphisme injectif de corps (non commutatifs) de $Z(A_0) \cong k(\sqrt{a})$ dans D. Alors on peut munir D d'une graduation de façon à ce qu'on ait isomorphisme de k-algèbres graduées $A \cong \tilde{M}_n(D)$. De plus, $A_0 \cong M_n(C_0)$ est une algèbre d'Azumaya zur $Z(A_0)$.*
4. *Soit $a \neq 1$ dans $G(k)$ et supposons qu'il n'existe pas de morphisme injectif de corps (non commutatifs) de $Z(A_0) \cong k(\sqrt{a})$ dans D. Alors $n = 2m$ (et forcément la dimension de A) est pair et on a un isomorphisme de k-algèbres graduées $A \cong (M_m(D))\hat{\otimes}\langle\frac{-a,1}{k}\rangle$. Finalement, on a $A_0 \cong M_m(D) \times F(\sqrt{(a)})$, le produit à droit étant une algèbre d'Azumaya sur $Z(A_0)$.*
5. *L'algèbe A_0 est séparable et donc semisimple.*

Donc pour tout algèbre graduée centrale simple A avec $A_1 \neq 0$, on obtient un élément z_A qui est unique à multiplication avec un scalaire près et $\delta(A) := [a = z_A^2] \in G(k)$. Notons que l'application $A \mapsto \delta(A)$ est bien définie. Si $A_1 = 0$, posons $z_A = 1_A$ et $\delta(A) := 1 \in G(k)$. De plus, écrivons *type*$(A) = 0$, si A est de type pair et *type*$(A) = 1$ si A est impair.

Théorème 12. *Le couple $(type, \delta)$ induit un morphisme de groupes $j : BW(k) \to Q(k)$. De plus, si on pose $i : B(k) \to BF(k), A \mapsto (A)$ on a, pour toute algèbre graduée centrale simple A telle que $j(\langle A\rangle) = 1_{Q(k)}$, $\langle A\rangle = i([A])$. En particulier ceci donne une suite exacte*

$$0 \to B(k) \xrightarrow{i} BW(k) \xrightarrow{j} Q(k) \to 0.$$

En particulier on a $BW(k) \cong Z_2$ si k est algébriquement clos.

L'algèbre de Clifford

Soit (V, q) un espace quadratique. Soit $T(V)$ l'algèbre tensorielle de V et soit $I(q)$ l'idéal engendré par les $x \oplus x - q(x) \cdot 1_{T(V)}, x \in V$, où $1_{T(V)} = 1_k$. Le quotient $C(V, q) := T(V)/I(q)$ est une algèbre unitaire associative. Notons $\theta : V \to C(V, q)$ la composition des applications canoniques $T(V) \to T(V)/I(q)$ et $V \to T(V)$. C'est un morphisme de k-espaces vectoriels injectif : la linéarité est évidente ; pour l'injectivité on voit que comme les éléments de $I(q)$ sont de degré au moins 2, $\theta(v) = 0$ entraîne $v \in I(q)$ donc $v = 0$. De plus, le couple (C, θ) est *compatible* avec (V, q), au sens que $\theta(v) \cdot \theta(v) = q(v) \cdot 1_C$. Ce couple est l'*algèbre de Clifford* de (V, q).

Cette algèbre possède une propriété universelle. Soit U une autre k-algèbre unitaire associative munie d'un morphisme d'espaces vectoriels $\lambda : V \to U$ injectif satisfaisant, pour tous $v \in V$, $\lambda(v)^2 = q(v) \cdot 1_U$. Alors il existe un unique morphisme de k-algèbres $\tilde{\lambda} : C(V, q) \to U$ tel que le diagramme suivant soit commutatif :

$$\begin{tikzcd} V \arrow[r, "\theta"] \arrow[d, "\lambda"'] & C(V,q) \arrow[dl, "\tilde{\lambda}"] \\ U & \end{tikzcd}$$

Ceci se voit comme suit. Grâce à la propriété universelle de l'algèbre tensorielle, il existe un unique morphisme de k-algèbres $\bar{\lambda} : T(V) \to U$ tel que $\bar{\lambda} \circ i = \lambda$ (voir [Bou58b]). Cet morphisme est nul sur $I(q)$, donc se factorise en un morphisme de k-algèbres $C(V, q) \to U$. Par construction ce morphisme est l'unique tel morphisme rendant le diagramme ci-dessus commutatif.

En particulier une algèbre avec ces propriétés est unique à unique isomorphisme près.

Comme l'application $(-\theta) : V \to C(V, q)$ satisfait de nouveau $((-\theta)(v))^2 = q(v) \cdot 1_C$, on obtient un endomorphisme de k-algèbres $\beta \in End_k(C(V, q))$ tel que $\beta \circ -\theta = \theta$. De la propriété universelle ci-dessus, il decoule que $\beta^2 = Id$, donc β est une involution. On pose $C_0(V, q) := \{x \in C(V, q) : \beta(x) = x\}$ et $C_1(V, q) := \{x \in C(V, q) : \beta(x) = -x\}$. Ainsi $C(V, q)$ devient la somme directe $C_0 \oplus C_1$ avec les projections évidentes $p_0 : x \mapsto \frac{1}{2}(x + \beta(x))$ et $p_1 : x \mapsto \frac{1}{2}(x - \beta(x))$ et donc une algèbre $\mathbb{Z}_2$-graduée (un calcul peu intéressant montre que $C_i \cdot C_j \subset C_{i+j}$) (cf. [Hus66]).

Il découle de ces observations que si (V, q) et (V', q') sont deux espaces quadratiques isomorphes, leurs algèbres de Clifford sont isomorphes en tant que k-algèbres graduées.

Théorème 13. *Si $e_1, .., e_n$ est une base orthogonale de (V, q), alors les $e_1^{d_1} .. e_n^{d_n}, d_i = 0, 1$ forment une base de $C(V, q)$ sur k. En particulier $C(V, q)$ est de dimension 2^{dimV} sur k.*

Démonstration. Voir [Bou59].

Théorème 14. *Il existe un isomorphisme canonique de k-algèbres $\mathbb{Z}_2$-graduées*

$$C((V,q) \oplus (V',q')) \to C(V,q)\hat{\otimes}C(V',q'),$$

où $\hat{\otimes}$ signifie le produit tensoriel gradué d'algèbres. □

Exemple. 1. *Soit a un élément non nul de k. Considérons l'espace quadratique $(k, \langle a\rangle)$. On a un isomorphisme $T(k) \cong k[X]$ et ainsi $I(\langle a\rangle)$ devient l'idéal $(X^2 - a)$. Donc $C((k, \langle a\rangle))$ est isomorphe comme algèbre $\mathbb{Z}_2$-graduée à $k[X]/(X^2 - a)$ et pour a nun nul, c'est exactement $k\langle\sqrt{a}\rangle$ definie ci-dessus.*

2. *Pour deux éléments inversibles $a, b \in k^\times$, considérons l'espace quadratique $(k^2, \langle a, b\rangle)$. Son algèbre de Clifford est isomorphe, en tant qu'algèbre graduée dur k, à $\langle\frac{a,b}{k}\rangle$. Ceci est une conséquence de l'exemple précédent en observant que*

$$k\langle\sqrt{a}\rangle\hat{\otimes}k\langle\sqrt{b}\rangle \cong \langle\frac{a,b}{k}\rangle$$

en tant que k algèbres graduées.

Le premier exemple montre que, tout espace quadratique étant diagonalisable, l'algèbre de Clifford est une algèbre graduée centrale simple.

En particulier, grâce aux théorèmes de structure des telles algèbres, on sait que l'algèbre de Clifford est - en tant qu'algèbre non graduée - semisimple et en tout cas ou bien simple ou bien produit direct de deux algèbres simples.

Par le deuxième, on a $C(\mathcal{H}) \cong \hat{M}_2(k)$ et $C(m\times\mathcal{H}) \cong \hat{M}_{2^m}(k)$. En particulier, on a une application bien definie $\Gamma : W(k) \to BW(k)$ qui envoit $[(V,q)]$ sur $\langle C(V,q)\rangle$. En fait, elle est un morphisme de groupes abéliens, appellé *l'invariant de Clifford.*

Notons $\phi_{p,q}$ la forme quadratique $p\times\langle -1\rangle \oplus r\times\langle 1\rangle$. Notons $C^{p,q}$ son algèbre de Clifford et soit $C^{0,0} = k$. De la remarque ci-dessus il decoule que, pour tous $p, q, n \in \mathbb{N}$,

$$C^{p+n,q+n} \cong \hat{M}_{2^n}(C^{p,q}).$$

Pour calculer tous les algèbres $C^{p,q}$ il suffit donc de les connaître pour les cas où $p = 0$ ou $q = 0$. On reverra ces algèbres plus tard.

Théorème 15. *Soit (V,q) un espace quadratique regulier. On a*

$$(type, \delta)(\langle C(V,q)\rangle) = f([(V,q)]) \in Q(k),$$

où f est l'application induite par (dim_0, d).

Démonstration. Notons n la dimension de V sur k et soit $e_1, .., e_n$ une base orthogonale de (V,q) (i.e une base dans laquelle la matrice de B_q est diagonale). Posons $z := e_1 \cdot .. \cdot e_n \in C(V,q)$ et écrivons $Z(C(V,q)) = k \oplus Z_1, Z_1 \subset C_1$.

Premier cas. Supposons n impair. Grâce à $x^2 = q(x)\cdot 1_{C(V,q)}$, on a $q(x+y) - q(x) - q(y) = xy + yx$, donc si x et y sont orthogonaux, $xy = -yx$. Donc $e_ie_j = -e_je_i$ pour $i \neq j$. Ceci entraîne que $ze_i = e_1..e_ne_i$ soit égal à

$(-1)^{n-1} \cdot e_i e_1..e_n$, et comme n est impair, z commute avec tout les e_i, donc $z \in Z(C(V,q))$. Comme n est impair, $z \in Z_1$ et $z \neq 0$, donc $C(V,q)$ est de type impair, $Z(C(V,q)) = k \oplus kz$ et $\delta(C(V,q))$ est égal à $z^2 = e_1,..,e_n e_1..e_n = (-1)^{(n-1)n/2} e_1^2..e_n^2$. Or c'est $(-1)^{(n-1)n/2} q(e_1)..q(e_n) 1_A$, donc $\delta(C(V,q)) = d(q)$.

Deuxième cas. Supposons n pair. Comme ci-dessus, on obtient $e_i z = -z e_i$ pour tous $i = 1..n$ et ainsi z commute avec tous les termes $e_i e_j$. Donc $0 \neq z \in Z(C_0(V))$, $C_0(V,q)$ n'est pas centrale et $C(V,q)$ est de type pair. On a $Z(C_0(V,q)) = k \oplus kz$, $z^2 = (-1)^{(n-1)n/2} e_1^2..e_n^2$ et de nouveau $\delta(C(V,q)) = d(q)$. □

Remarque. *En particulier, l'algèbre de Clifford d'un espace quadratique de dimension paire sur k est une algèbre d'Azumaya sur k et peut ainsi être considerée comme élément de $B(k)$.*

Lemme. *Soit (V,q) un espace quadratique de dimension paire de discriminant $d(q) = \delta$. Alors il existe un isomorphisme de k-algèbres $\mathbb{Z}_2$-graduées $C(V,q) \cong C(V, -\delta\dot{q})$.*

Démonstration. Soit z comme dans le théorème précédent. On a un morphisme de k-espace vectoriels $\lambda : V \to C(V,q), v \mapsto z \cdot v$, vérifiant, pour tous $v \in V$, $\lambda(v)^2 = z \cdot v \cdot z \cdot v = -z^2 v^2 = -\delta q(v)$ (rappellons que $z e_i = -e_i z$ et que les e_i forment une base de V). On obtient donc un morphisme $T(V) \to C(V,q)$ de k-algèbres graduées (en munissant $T(V)$ de la $\mathbb{Z}_2$ graduation induite par sa $\mathbb{Z}$-graduation) qui est nul sur $I(-\delta \cdot q)$, donc qui se factorise en un morphisme gradué non nul de k-algèbres simples $C(V, -\delta \cdot q) \to C(V,q)$ qui est un isomorphisme. □

Le théorème ci-dessus montre que le diagramme de suites exactes de groupes abéliens commute :

$$\begin{tikzcd}
0 \arrow[r] & B(k) \arrow[r, "i"] & BW(k) \arrow[r, "j"] & Q(k) \arrow[r] & 0 \\
0 \arrow[r] & I^2k \arrow[r] & W(k) \arrow[r] \arrow[u, "\Gamma"] & W(k)/I^2k \arrow[r] \arrow[u, "f"'] & 0
\end{tikzcd}$$

Ici f est l'isomorphisme de groupe induit par (dim_0, d). Une chasse de diagramme rend un morphisme de groupes $\gamma : I^2k \to B(k)$ tel que le diagramme reste commutatif. Soit (V,q) un espace quadratique regulier tel que $[(V,q)] \in I^2k$. Alors l'exactitude de la suite au dessous et la commutativité du diagramme montrent que $j(\langle C((V,q))\rangle) = 1_{Q(k)}$, mais alors $\langle C(V,q)\rangle = i([C(V,q)])$. Or i est injectif, donc par commutativité du diagramme, on doit avoir $\gamma([(V,q)]) = [C(V,q)]$.

Considérons encore les algèbres $C^{p,q}$. Le lemme montre qu'on a bien un isomorphisme d'algèbres graduées $C^{4,0} \cong C^{0,4}$ Mais alors on a $C^{8,0} \cong C^{4,0} \hat{\otimes} C^{4,0} \cong C^{4,0} \hat{\otimes} C^{0,4} \cong \hat{M}_{16}(k) \cong C^{0,8}$. Finalement, on a le résultat de périodicité suivant :

$$C^{p+8,q} \cong C^{p,q} \hat{\otimes} C^{8,0} \cong C^{p,q} \hat{\otimes} \hat{M}_{16}(k) \cong \hat{M}_{16}(C^{p,q}) \cong C^{p,q+8}$$

Notons que à priori ceci ne dit pas trop sur le groupe $BW(k)$. En général, une forme quadratique ne doit pas être équivalente à une des $\phi_{p,q}$. De plus, Γ n'a aucune raison d'être surjectif. En tout cas, il existe des éléments non nuls de torsion (car $k\langle\sqrt{a}\rangle$ ne peut pas être dans la classe de k, par le théorème de Wedderburn).

Lemme. *Soient a, b, c trois éléments non nuls de k. Alors*

$$\gamma([(k^4, \langle a, b, c, abc\rangle)]) = [\left(\frac{-ab, -ac}{k}\right)] \in B(k).$$

Théorème 16. *La classe de l'algèbre de Clifford d'une 3-forme de Pfister dans $BW(k)$ est l'élément neutre.*

Démonstration. En utilisant le lemme ci-dessus et en écrivant un 3-Pfister $\langle 1, a\rangle \otimes \langle 1, b\rangle \otimes \langle 1, c\rangle$ comme somme directe $\langle 1, a, b, ab\rangle \oplus \langle c, bc, ac, abc\rangle$. Les formes $\langle c, bc, ac, abc\rangle$ et $\langle c, bc, ac, abc^2\rangle$ sont équivalents (on considère la matrice diagonale à entrées $1, 1, 1, c$, qui est inversible car c est non nul). Donc dans $W(k)$, la somme précédente équivaut $\langle 1, a, b, ab\rangle - \langle -c, -ac, -bc, -abc^3\rangle$. Le lemme précédent montre que ceci est envoyé par γ sur la différence des classes d'équivalence de $\left(\frac{-a,-b}{k}\right)$ et $\left(\frac{-ac^2,-bc^2}{k}\right)$. Or cette différence est nulle, donc $\gamma([\langle 1, a\rangle \otimes \langle 1, b\rangle \otimes \langle 1, c\rangle]) = 0 \in B(k)$. L'énoncé s'ensuit car $i \circ \gamma = \Gamma$. $\square$

On a donc $\Gamma(I^3k) = 1$ et par la commutativité du diagramme et l'exactitude des suites, $\gamma(I^3k) = 1$. Les morphismes Γ et γ se factorisent en morphismes $\bar{\Gamma} : W(k)/I^3k \to BW(k)$ et $\bar{\gamma} : I^2k/I^3k \to B(k)$ et on obtient un diagramme commutatif de suites exactes

$$\begin{tikzcd}
0 \arrow[r] & B(k) \arrow[r, "i"] & BW(k) \arrow[r, "j"] & Q(k) \arrow[r] & 0 \\
0 \arrow[r] & I^2k/I^3k \arrow[r] \arrow[u, "\bar{\gamma}"] & W(k)/I^3k \arrow[r] \arrow[u, "\bar{\Gamma}"] & W(k)/I^2k \arrow[r] \arrow[u, "f"] & 0
\end{tikzcd}$$

Ceci permet de calculer le groupe de Brauer-Wall du corps $\mathbb{R}$. On sait déja que $W(\mathbb{R}) \cong \mathbb{Z}$ et $I^n\mathbb{R} \cong 2^n\mathbb{Z}$, engendré par les n-formes de Pfister. De plus, $B(\mathbb{R}) \cong \mathbb{Z}_2$, où la classe des quaternions $\mathbb{H}$ est un générateur. Mais par le lemme ci-dessus, on sait que $\bar{\gamma}$ envoit la classe de $\langle 1, 1, 1, 1\rangle$, qui es non nul donc un générateur de $I^2\mathbb{R}/I^3\mathbb{R} \cong \mathbb{Z}_2$, sur $\mathbb{H}$, qui engendre $B(\mathbb{R})$, donc cette application est un isomorphisme de groupes abéliens. Dans le diagramme ci-dessus, les morphismes verticaux à gauche et à droit sont des isomorphismes, donc le morphisme au centre en est un aussi (par lemme des cinq). Mais ceci donne

$$BW(\mathbb{R}) \cong \mathbb{Z}/8\mathbb{Z}.$$

5 Le 1-2-4-8 théorème de Hurwitz

Si (V, q) est un espace quadratique sur k, on dit que q est *multiplicative au sens de Hurwitz* s'il existe une application k-bilinéaire $\phi : V \times V \to V$ telle que, pour tous x, y dans V, $q(x)q(y) = q(\phi(x, y))$.

Dans ce chapitre il s'agit principalement de démontrer le résultat suivant :

Théorème 17 (Hurwitz). *Soit (V, q) un espace quadratique régulier. Et soit q multiplicative au sens de Hurwitz. Alors la dimension de V est égale à $1, 2, 4$ ou 8.*

Remarque. *Si $k = \mathbb{R}$, on sait déja que pour n étant une puissance de 2, on peut écrire le produit d'une la somme de n carrés par une somme de n carrés comme somme de n carrés :*

$$(x_1^2 + .. + x_n^2)(y_1^2 +, , +y_n^2) = (z_1^2 + .. + z_n^2)$$

avec des $z_i \in \mathbb{R}(x, y)$ dépendant $\mathbb{R}(x)$-linéairement de $(y_1, .., y_n)$ (Pfister). De plus, la multiplication des nombres complexes, des quaternions et des octinions est une application linéaire de $\mathbb{R}$-espaces vectoriels, et la norme satisfait $|z||z'| = |zz'|$. Donc pour $n = 1, 2, 4, 8$, il existe des z_i dépendant $\mathbb{R}$-linéairement de $(x_1, .., x_n)$ et de $(y_1, .., y_n)$. Le théorème précédent montre que ceci n'est pas possible pour des dimensions différentes.

Corps et leurs niveaux

Définition. *On appelle* niveau *du corps k et on note $S(k)$ (de l'allemand 'Stufe') le plus petit entier n tels qu'il existe des éléments $x_1, .., x_n$ dans k tels que $-1 = x_1^2 + .. + x_n^2$. On écrit $S(k) = \infty$ s'il n'existe pas de décomposition de -1 en une somme de carrés. Dans ce cas le corps est dit* réel.

Si k est de niveau 1, alors $k(\sqrt{-1})$ est isomorphe, en tant que k-algèbre, à $k \times k$: si u est tel que $u^2 = a$, alors $1 \mapsto (1, 1), u \mapsto (1, -1)$ est un tel isomorphisme. Si k est de niveau au moins 2, alors $k(\sqrt{-1})$ est un corps.

Si k est de niveau au plus 2, l'algèbre $\left(\frac{-1,-1}{k}\right)$ est isomorphe à $M_2(k)$; sinon, c'est une algèbre de division sur k.

Représentation d'algèbres

Définition. *Soit A une k-algèbre de dimension finie. Une* représentation *de A sur k est un morphisme de k algèbres $\rho : A \to End_k(W)$, où W est un k-espace vectoriel de dimension finie. La* dimension *de cette représentation est celle de W. On dit aussi que ceci est une représentation de A dans W (sur k).*

Évidemment, une telle représentation permet de voir W comme A-module. On dit que la représentation est irréductible *si c'est un module simple.*

Supposons que $M_m(k)$ admet une représentation n-dimensionale. Ceci fait de k^n un $M_m(k)$-module. Comme l'algèbre $M_m(k)$ est simple, elle est en particulier semisimple, donc tous ses modules sont isomorphes à une somme directe de modules simples. Or k^m est un $M_n(k)$-module simple, donc par le lemme k^n est isomorphe, en tant que $M_m(k)$-module, à une somme directe de copies de k^m. En particulier m divise n.

D'autre part, si $s(k) > 1$, $C := k(\sqrt{-1})$ est un corps et de nouveau $M_m(C)$ est une k-algèbre simple (car c'est une C-algèbre simple) et son unique module simple est C^m. Donc une représentation de $M_m(C)$ de dimension n sur k peut exister seulement si $2m$ divise m.

Finalement, pour $s(k) > 2$, $H := \left(\frac{-1,-1}{k}\right)$ est une algèbre de division de simension 4 sur k et en particulier $M_m(H)$ est une k-algèbre simple, de l'unique module simple H^m. En particulier une représentation de $M_m(H)$ de dimension n sur k peut exister seulement si $4m$ divise n.

La fonction de Radon-Hurwitz

On notera $\rho_k(n)$ l'entier maximal m tel que $C^{m-1,0}$ admet une représentation de dimension n. La fonction $\rho_k : \mathbb{N} \to \mathbb{N}$ est appellée *fonction de Radon-Hurwitz* de k. De plus, notons $\rho'_k(n)$ l'entier maximal m tel que $C^{0,m-1}$ admet une représentation de dimension n.

Considérons maintenant de plus près les algèbres $C^{m,0}$. Oublions à partir d'ici leurs graduations. On a déjà vu $C^{m+8,0} \cong M_{16}(C^{m,0})$. En utilisant que $C^{0,1} \cong k(\sqrt{1}) \cong k \times k$ et $C^{0,2} \cong \left(\frac{1,1}{k}\right)$, on calcule les algèbres $C^{m,0}$ pour $m = 0..7$ comme suit : $C^{0,0} \cong k$, $C^{1,0} = C := k(\sqrt{-1})$, $C^{2,0} \cong \mathbb{H}$, $C^{3,0} \cong \mathbb{H} \times \mathbb{H}$, $C^{4,0} \cong M_2(\mathbb{H})$, $C^{5,0} \cong M_4(C)$, $C^{6,0} \cong M_8(k)$ et $C^{0,7} \cong M_8(k) \times M_8(k)$.

Lemme. *Supposons $s(k) = 1$. Alors $\rho_k(n) \leq 2a+2$ si $n = 2^a n_0$ avec n_0 impair.*

Démonstration. Avec les remarques dans le deux paragraphes précédents, on voit facilement que pour $m - 1 = 2s + i$ on a $C^{m-1,0} \cong M_{2^s}(k)$ pour $i = 0$ et $C^{m-1,0} \cong M_{2^s}(k) \times M_{2^s}(k)$ si $i = 1$.

Donc $C^{m-1,0}$ possède une représentation de dimension n seulement si 2^s divise n, c'est-à-dire $s \leq a$. Il s'ensuit que $m \leq 2s + 2 \leq 2a + 2$. □

En d'autres termes, comme tout module d'une telle algèbre de Clifford doit être de de dimension divisée par celle des uniques modules simples de ses souos-algèbres simples, des arguments de la théorie des nombres permettent d'établir des conditions de dimension.

Par un calcul analogue, on obtient les deux résultats suivants :

Lemme. *Supposons $s(k) = 2$. Alors $\rho_k(n) \leq 4a + 4^b$ si $n = 2^{2a+b} n_0$ avec n_0 impair et $b \in \{0, 1\}$.* □

Lemme. *Supposons $s(k) \geq 2$. Alors $\rho_k(n) \leq 8a + 2^b$ si $n = 2^{4a+b} n_0$ avec n_0 impair et $b \in \{0, 1, 2, 3\}$.* □

En tout cas, avec l'écriture $n = 2^a n_0$, n_0 impair, on a $\rho_k(n) \leq 2a + 2$.

Le théorème

Lemme. *Supposons qu'il existe un espace quadratique régulier (V, q) de dimension n sur k, muni d'une application k-bilinéaire $\phi : V \times V \to V$ telle qu'on ait, pour tous x, y dans V,*

$$q(x)q(y) = q(\phi(x, y)).$$

Alors sur V il existe une application quadratique q' qui est un multiple de q par un scalaire faisant de V un espace quadratique régulier et une application k-bilinéaire $\psi V \times V \to V$ telle qu'on ait de nouveau, pour tous x, y dans V,

$$q'(x)q'(y) = q(\psi(x, y)).$$

De plus il existe un élément $u \in V$ vérifiant $q'(u) = 1$ tel que $\psi(u, \cdot) : V \to V$ soit l'identité.

Démonstration. Soit B la forme bilinéaire associée à a. Observons que, pour tous $x, y, z \in V$,

$$B(\phi(x, y), \phi(x, z)) = \frac{1}{2}\left(q(\phi(x, y) + \phi(x, y)) - q(\phi(x, y)) - q(\phi(x, z))\right)$$

$$= \frac{1}{2}\left(q(x)q(y + z) - q(x)q(y) - q(x)q(z)\right) = q(x)B(y, z)$$

. De même, on a $B(\phi(x, y), \phi(z, y)) = q(y)B(x, z)$. Comme (V, q) est régulier, il existe un élément $u \in V$ tel que $q(u) = a \in k^\times$. Alors l'application $\phi(u, \cdot) : V \to V$ est un morphisme de k-espaces vectoriels et c'est un isomorphisme. En effet, supposons que $\phi(u, y) = 0$. Alors, pour tous $z \in V$, $q(u)B(y, z) = B(\phi(u, y), \phi(u, z)) = 0$ et comme B est non dégénérée, on doit avoir $y = 0$. Comme V est de dimension finie, on a donc un isomorphisme de k-espaces vectoriels. Notons θ son inverse. Posons maintenant $q' := a^{-1}q$ et

$$\psi : V \times V \to V, (x, y) \mapsto \theta(\phi(x, y))$$

Alors on a, pour tous x, y dans V, $\phi(u, \psi(x, y)) = \phi(x, y)$, donc $a \cdot q(\psi(x, y)) = q(x)q(y)$, d'où le fait que ψ est une décomposition pour (V, q') comme voulue. Mais évidemment, $\psi(u, \dot{}) : V \to V$ est l'identité. $\square$

Remarque. *Si la forme q représente 1, disons par un vecteur $u' \in K$, alors on voit que $q' = q$ et $u' = u$.*

Lemme. *Supposons que (V, q) est un espace quadratique de dimension finie régulier muni d'une application k-bilinéaire $\phi : V \times V \to V$ telle qu'on ait, pour tous $x, y \in V$,*

$$q(x)q(x) = q(\phi(x, y))$$

De plus, supposons qu'il existe un élément $u \in V$ avec $q(u) = 1$ tel que $\phi(u, \cdot) : V \to V$ soit l'identité. Notons U_0 le complément orthogonal de $k \cdot u$ dans V par q. Alors l'algèbre de Clifford de $(U_0, -q|_{U_0})$ admet une représentation dans V.

Démonstration. Pour tout $x \in U_0$, notons $L_x : V \to V$ l'application $y \mapsto \phi(x, y)$. Soit B la forme bilinéaire associée à q. Alors on a, pour tout $y \in V$, $B(y, L_x(y) = B(\phi(u, y), \phi(x, y)) = B(u, x) \cdot q(y)$, où la dernière égalité découle comme dans la démonstation précédente. Mais ceci équivaut 0, car x est dans le complément orthogonal de $k \cdot u$. En particulier, on a, pour tous $x, y \in V$, $B(y, L_x(z)) = -B(z, L_x(y))$. En particulier, $B(x, L_x^2(z)) = -B(L_x(z), L_x(y)) = -(q) \cdot B(z, y)$. Donc on a, pour tous $y, z \in V$,

$$B(y, (L_x^2 + q(x)\dot{I}d_V)(z)) = 0$$

et comme B est non dégénérée, ceci donne $\lambda : L_x^2 = -q(x) \cdot Id_V$ dans $End_k(V)$.

L'application $x \mapsto L_x$ définit un morphisme injectif de k-espaces vectoriels. ($L_x = 0$ entraîne $\phi(x, y) = 0$ pour tous $y \in V$. Mais maintenant $0 = B(\phi(x, y), \phi(y, u)) = q(u)\dot{B}(x, y)$ et comme B est non dégénérée, on a $x = 0$). De plus, ce morphisme vérifie $\lambda(x)^2 = -q(x) \cdot 1_{End_k(V)}$. La propriété universelle de l'algèbre de Clifford nous garantit l'existence d'un morphisme de k-algèbres

$$C(U_0, -q) \to End_k(V)$$

voilà la représentation désírée. □

En d'autres termes, la normalisation du premier lemme permet de voir V comme module sur une algèbre de Clifford.

Maintenant, considérons l'espace quadratique $(k^n, \langle 1, .., 1 \rangle)$. Les deux lemmes et la remarque montrent que si ce dernier est multiplicative au sens de Hurwitz, alors $C^{n-1,0}$ admet une représentation de dimension n. Mais alors

$$n \leq \rho_k(n)$$

par la définition de cette fonction.

Lemme. *Soit encore f une forme quadratique régulière de dimension finie sur k qui est multiplicative au send de Hurwitz. Soit $\bar{k}$ une clôture algébrique de k. Notons $f \otimes \bar{k}$ la forme quadratique f, vue comme forme quadratique sur $\bar{k}$. Alors cette nouvelle forme quadratique est (bien sûr de même dimension et) régulière et multiplicative au sens de Hurwitz.*

Comme sur $\bar{k}$, toute forme quadratique est équivalente à une forme $\langle 1, .., 1 \rangle$. On a donc montré :

Théorème 18. *Si (V, q) est un espace quadratique régulier de dimension n sur k et multiplicative au sens de Hurwitz, alors*

$$n \leq \rho_{\bar{k}}(n).$$

En tout cas, on a donc $n \leq 2a + 2$ si $n = 2^a n_0$, n_0 impair. Ceci entraîne $2a + a \geq 2^a n_0$ et donc $n_0 = 1$, $a = 0, 1, 2$ ou 3. Finalement, n doit être égal à $1, 2, 4$ ou 8 ce qui démontre le théorème de Hurwitz.

Notons qu'en général on n'a pas d'énoncé affirmatif sur l'existence d'un espace quadratique multiplicatif au sens de Hurwitz dans ces dimensions.

Remarques

Ce théorème a été démontré pour la prémière fois par Hurwitz dans [Hur98]. En cours de ce traité, on a vu que les groupes de Brauer-Wall de $\mathbb{R}$ et de $\mathbb{C}$ sont isomorphes à $\mathbb{Z}/8\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z}$ respectivement et que dans les cas de ces deux corps ils sont donnés entièrement par des classes d'algèbres de Clifford. En topologie algébrique on démontre des résultats de périodicité modulo 8 de la KO-théorie (classes d'équivalence de fibrés vectoriels réels sur un espace topologique) et de périodicité modulo 2 de la K-théorie (classes d'équivalence de fibrés vectoriels complexes sur un espace topologique). Ces théorèmes sont connus sous le nom de 'périodicité de Bott'. À leur aide, on peut démontrer

Théorème 19. *La sphère* $\mathbb{S}^{n-1}$ *est parallélisable si et seulement si* $n = 1, 2, 4$ *ou* 8*.*

Pour deviner le lien entre ces deux résultats, notons qu'on peut trouver un isomorphisme entre un anneau déterminé par les représentations irréductibles des algèbres $C^{p,q}$ et la K-théorie (ou KO-théorie) du point (Voir [ABS64, Kar68]).

Références

[ABS64] M. F. Atiyah, R. Bott, and A. Shapiro. Clifford modules. *Topology*, 3(suppl. 1) :3–38, 1964.

[Bou58a] N. Bourbaki. *Éléments de mathématique. 23. Première partie : Les structures fondamentales de l'analyse. Livre II : Algèbre. Chapitre 8 : Modules et anneaux semi-simples.* Actualités Sci. Ind. no. 1261. Hermann, Paris, 1958.

[Bou58b] N. Bourbaki. *Éléments de mathématique. I : Les structures fondamentales de l'analyse. Fascicule VII. Livre II : Algèbre. Chapitre 3 : Algèbre multilinéaire.* Nouvelle édition. Actualités Scientifiques et Industrielles, No. 1044. Hermann, Paris, 1958.

[Bou59] N. Bourbaki. *Éléments de mathématique. Première partie : Les structures fondamentales de l'analyse. Livre II : Algèbre. Chapitre 9 : Formes sesquilinéaires et formes quadratiques.* Actualités Sci. Ind. no. 1272. Hermann, Paris, 1959.

[Hur98] A. Hurwitz. Über die composition der quadratischen formen von beliebig vielen variabeln. *Nachr. Ges. Wiss. Göttingen*, pages 309–316, 1898.

[Hus66] Dale Husemoller. *Fibre bundles.* McGraw-Hill Book Co., New York, 1966.

[Kar68] Max Karoubi. Algèbres de Clifford et K-théorie. *Ann. Sci. École Norm. Sup. (4)*, 1 :161–270, 1968.

[Ker90] Ina Kersten. *Brauergruppen von Körpern.* Aspects of Mathematics, D6. Friedr. Vieweg & Sohn, Braunschweig, 1990.

[Lam80] T. Y. Lam. *The algebraic theory of quadratic forms.* Benjamin/Cummings Publishing Co. Inc. Advanced Book Program, Reading, Mass., 1980. Revised second printing, Mathematics Lecture Note Series.

[Lan84] Serge Lang. *Algebra.* Addison-Wesley Publishing Company Advanced Book Program, Reading, MA, second edition, 1984.

[Pfi95] Albrecht Pfister. *Quadratic forms with applications to algebraic geometry and topology*, volume 217 of *London Mathematical Society Lecture Note Series.* Cambridge University Press, Cambridge, 1995.