Université Sidi Mohamed Ben Abdellah
Faculté des Sciences et Techniques de Fès

Département de mathématiques

UFR-DESA-A.T.N.A.S.I

Algèbre Théorie des Nombres et Applications aux Sciences de l'Information

Mémoire de DESA

Invariants d'une algèbre centrale simple à involution

Présenté par

Jamal Nafie

Dirigé par

Pr. Lahcen Oukhtite

Soutenu le 8 novembre 2008 devant le jury constitué par :

Pr. M. Boulagouaz	FST. Univ. de Fès	Membre Rapporteur
Pr. M.E. Charkani	FS. Univ. de Fès	Président
Pr. M.A. Elomary	FST. Errachidia	Membre Rapporteur
Pr. L. Oukhtite	FST. Errachidia	Membre Rapporteur

Année universitaire : 2007-2008

Invariants d'une algèbre centrale simple à involution

Remerciements

Je tiens à exprimer ma profonde gratitude au professeur Lahcen Oukhtite, pour avoir accepter de diriger ce travail avec toute attention et pour ses orientations fructueuses.

Je remercie le professeur M'hammed Boulagouaz pour ses orientations et son soutien durant tout ce cursus de D.E.S.A.

Je tiens à remercier tous les professeurs de D.E.S.A, "Algèbre Théorie des Nombres et Applications aux Sciences de l'Information". Ainsi que tous mes collègues.

En fin je remercie tous les amis qui m'ont apporté de l'aide.

Table des matières

Introduction

Dans ce document, sauf mention du contraire, tous les corps considérés sont commutatifs et de caractéristique différente de deux.

Le présent travail a pour but de présenter quelques invariants d'une algèbre centrale simple de dimension finie à involution.

Dans le premier chapitre, on rappelle certaines définitions et propriétés concernant les algèbres centrales simples et on cite quelques résultats élémentaires indispensables pour la suite. Les livres de Draxl [3], Pierce [12], Scharlau [13] sont des références générales sur ce sujet.

Le second chapitre est consacré à une correspondance biunivoque entre les involutions de première espèce sur l'algèbre d'endomorphismes $End_F(V)$ et les formes bilinéaires non singulières sur V. Ensuite, on expose la démonstration du résultat qui montre que les involutions de première espèce sur une algèbre centrale simple quelconque sont, après extension des scalaires à un corps neutralisant K, identifiées à des involutions de première espèce sur une algèbre d'endomorphismes $End_K(V)$.

Au troisième chapitre, après avoir établi un lien entre les involutions sur une algèbre centrale simple et une certaine classe d'idéaux, on traite le critère d'existence d'involutions de première espèce, dû à A. Albert, ainsi que celui de l'existence d'involutions de deuxième espèce (Théorème d'Albert-Riehm-Scharlau).

Puis, au chapitre 4, nous donnons un analogue du théorème de Witt, pour une algèbre centrale simple à involution. Pour cela, on expose une correspondance biunivoque entre les involutions de première espèce sur $End_D(V)$ et les formes ε-hermitiennes régulières sur V relativement à une involution sur l'algèbre à division D.

Le discriminant (chapitre 5) et la signature (chapitre 7) d'une involution de première espèce sont largement utilisés comme critères de décomposabilité d'une algèbre à involution. En particulier, Knus, Parimala et Sridharan ont montré qu'avoir un discriminant trivial est une condition nécessaire et suffisante de décomposition d'une algèbre centrale simple de degré 4. Par ailleurs, David. W. Lewis et J.P. Tignol ont montré que toute involution de signature 2 sur une algèbre de degré une puissance de deux et de centre un corps formellement réel, est indécomposable. Au chapitre 6, on donne la définition rationnelle d'une algèbre de Clifford d'une involution dûe à Tits, et le lien entre la conjugaison de deux involutions et leurs algèbres de Clifford. Le dernier chapitre est consacré au cas d'une algèbre à involution sur un corps de caractéristique deux.

Chapitre 1

Rappel sur les algèbres centrales simples

Ce chapitre constitue un rappel de certaines définitions et propriétés concernant les algèbres centrales simples dont nous aurons besoin dans ce document.

1.1 Définitions et exemples

Définition 1.1.1 *Un module non nul M sur un anneau R est dit simple s'il n'a pas de sous-modules non triviaux. L'anneau R est simple s'il n'a pas d'idéaux bilatères autre que $\{0\}$ et R.*

Exemples :

1. Soit D un anneau à division (un corps non nécessairement commutatif) :
   (i) D est un D-module simple.
   (ii) Tout D-espace vectoriel de dimension un est un D-module simple.
2. $\mathbb{Z}/p\mathbb{Z}$ est un $\mathbb{Z}$-module simple.
3. Tout anneau à division est simple.

Définition 1.1.2 *Soit A une algèbre sur un corps F. A est dite simple si A est simple pour sa structure d'anneau.*

Exemples :

1. Toute algèbre à division D est simple.
2. Si K est un corps, alors $M_n(K)$ est une algèbre simple.

Remarque : Si A est une F-algèbre (F corps) alors $F \subset Z(A)$.

Définition 1.1.3 *Une F-algèbre A est dite centrale si son centre $Z(A) = \{a \in A / a.x = x.a \ \forall x \in A\}$ est réduit à $F(= F.1)$.*

A est de dimension finie si A est de dimension finie comme étant un F-espace vectoriel. Dans toute la suite, les algèbres considérées seront et de dimension finie sur leurs centres.

Exemples :

1. $M_n(F)$ est une F-algèbre centrale simple de dimension n^2.
2. Toute algèbre à division D est centrale simple sur son centre $Z(D)$.
3. Soient a et b deux éléments non nuls d'un corps F et A le F-espace vectoriel de base $\{1, i, j, k\}$ et muni de la multiplication bilinéaire définie par : $i^2 = a$; $j^2 = b$; $ij = -ji = k$. A est une F-algèbre centrale simple de dimension 4 , notée $(\frac{a,b}{F})$ ou $(a, b)_F$ et appelée algèbre de quaternions.
4. Si A et B sont des F-algèbres centrales simples, alors leur produit tensoriel $A \otimes_F B$ est une F-algèbre centrale simple. En particulier, $M_m(F) \otimes_F M_n(F) \simeq M_{mn}(F)$.
5. Si A est une F-algèbre centrale simple, alors $M_n(A)$ est une F-algèbre centrale simple et on a : $A \otimes_F M_n(F) \simeq M_n(A)$.

Définition 1.1.4 *Soit A une F-algèbre. L'algèbre opposée de A notée A^{op} (ou A°) est A en tant que F-module mais sa multiplication $*$ est définie par $a * b = ba$ pour tout $a, b \in A$.*

1.2 Théorème de Wedderburn

La structure des algèbres simples centrales est entièrement déterminée par le théorème de Wedderburn :

Théorème 1.2.1 *Soit A une F-algèbre . Les conditions suivantes sont équivalentes :*

1. *A est centrale simple.*
2. *L'application $\varphi : A \otimes_F A^{op} \longrightarrow End_F(A)$*
   définie par : $\varphi(a \otimes b^{op})(x) = axb$ est un isomorphisme.
3. *Il existe une extension K de F telle que $A \otimes_F K \simeq M_n(K)$.*
4. *Si Ω est un corps algébriquement clos contenant F alors $A \otimes_F \Omega \simeq M_n(\Omega)$ pour un entier n.*
5. *Il existe une algèbre à division D centrale de dimension finie sur F et un entier r tels que $A \simeq M_r(D)$.*

De plus, si l'une de ces conditions est satisfaite, tous les A-modules à gauche (ou à droite) simples sont isomorphes et l'algèbre à division D de l'assertion (5) est uniquement déterminée à un isomorphisme près par $D = End_A(M)$ où M désigne un A-module à gauche simple.

Preuve : Voir [6, Theorem 1.1, page 3]. ∎

Remarques :

(i) Tout corps vérifiant l'assertion (3) du théorème précédent est appelé corps déployant de A (ou neutralisant pour A). Lorsque $A \simeq M_n(F)$, on dit que l'algèbre A est déployée.

(ii) D'après Köthe , toute F-algèbre simple centrale possède un corps déployant K tel que K/F soit une extension finie galoisienne (voir[3, §9, page 64]).

(iii) Du fait que la dimension d'une algèbre ne change pas par extension des scalaires et compte tenu de l'assertion (3) du théorème précédent, on déduit que la dimension de toute algèbre simple centrale sur son centre est le carré d'un entier naturel n : cet entier est appelé degré de A et noté $degA$.

(iv) Le degré de l'algèbre à division D de l'assertion (5) est appelé indice (de Schur) de A et noté $indA$.

Théorème 1.2.2 *(Théorème du Double Centralisateur) Soient A une F-algèbre centrale simple et B une sous algèbre de A. Le centralisateur, $C_A(B) = \{b \in B / b.x = x.b \ \forall x \in A\}$,*

de B dans A est une sous algèbre simple de A et on a : $dim_F A = dim_F B.dim_F C_A(B)$ et $C_A(C_A(B)) = B$. En outre, Si $Z(B) = F$, alors A est canoniquement isomorphe à $B \otimes C_A(B)$.

Preuve : Voir ([12, Chapitre 12, §7, Theorem, page 232]). ∎

Nous utiliserons souvent le théorème suivant :

Théorème 1.2.3 *(Théorème de Skolem-Noether) Soient A une F-algèbre simple centrale de dimension finie et B une sous-algèbre simple de A. Alors, pour tout homomorphisme de F-algèbres $f : B \longrightarrow A$, il existe $u \in A$ inversible tel que $f(y) = uyu^{-1}\ \ \forall y \in B$.*
En particulier, tout automorphisme de F-algèbres de A est un automorphisme intérieur.

Preuve : Voir ([12, Chapitre 12, §6, page 230]). ∎

1.3 Groupe de Brauer

Nous rappelons la définition d'un groupe introduit par Brauer en 1929. Grâce au théorème de Wedderburn, on vient de voir que toute F-algèbre simple centrale de dimension finie est isomorphe à une algèbre de matrices sur une algèbre à division de centre F, celle ci étant uniquement déterminée à isomorphisme près. Deux F-algèbres simples centrales A et B sont dites Brauer-équivalentes ou semblables (et on écrit $A \sim B$) si elles sont F-isomorphes à des algèbres de matrices sur des algèbres à division isomorphes ou, de façon équivalente, s'il existe deux entiers n et m tels que $M_n(A) \cong M_m(B)$. Il est clair que $\sim$ définit une relation d'équivalence sur les F-algèbres simples centrales de dimension finie ; la classe d'une F-algèbre simple centrale A sera notée $[A]$. Le produit tensoriel (sur F) de deux F-algèbres simples centrales étant une F-algèbre simple centrale, l'ensemble des classes d'équivalences de F-algèbres simples centrales muni de la loi induite par le produit tensoriel de F-algèbres est un groupe abélien appelé groupe de Brauer de F et noté $Br(F)$. L'élément neutre de $Br(F)$ est $[F]$ et l'inverse de $[A]$ est $[A^{op}]$ (par l'assertion (2) du théorème de Wedderburn) (voir [13, page 290]).

Exemples :

1. Le groupe de Brauer d'un corps algébriquement clos est trivial.
2. Le groupe de Brauer d'un corps fini est trivial.
3. $Br(\mathbb{R})$ est un groupe cyclique d'ordre 2 ; son élément non trivial est donné par la classe de l'algèbre des quaternions d'Hamilton $(-1,-1)_{\mathbb{R}}$.

1.4 Algèbre conjuguée - Norme d'une algèbre

Soit F/F_0 une extension quadratique séparable avec $Gal(F/F_0) = \{1, \sigma\}$.

Définition 1.4.1 *Soit A une F-algèbre. L'algèbre conjuguée de A notée $\overline{A}$, est A en tant qu'anneau, mais l'action de F sur $\overline{A}$ est : $\beta * a = \sigma(\beta)a$.*

Proposition 1.4.2 *Si A et B sont deux F-algèbres simples centrales, alors :*

1. *$\overline{A}$ est une F-algèbre simple centrale.*
2. *$\overline{A} \otimes_F \overline{B} = \overline{A \otimes_F B}$*
3. *$M_n(\overline{A}) = \overline{M_n(A)}$*
4. *L'application $\psi : Br(F) \longrightarrow Br(F)$ est un homomorphisme de groupes.*
$$[A] \longmapsto [\overline{A}]$$

Considérons l'application $S : \overline{A} \otimes_F A \longrightarrow \overline{A} \otimes_F A$
$$a \otimes b \longmapsto b \otimes a$$
Pour tout $a, b \in A$ et pour tout $\lambda \in F$:
$S\big(\lambda.(a \otimes b)\big) = S\big(\sigma(\lambda)a \otimes b\big) = b \otimes \sigma(\lambda)a = \sigma(\lambda)(b \otimes a) = \sigma(\lambda)S(a \otimes b)$, donc S est σ- semilinéaire, en plus S est un automorphisme de F_0-algèbres.

Définition 1.4.3 *On appelle norme (transfert, ou corestriction) de la F-algèbre A, notée $N_{F/F_0}(A)$, la sous F_0-algèbre de $\overline{A} \otimes_F A$ formée des éléments invariants par S.*
Autrement dit : $N_{F/F_0}(A) = cor_{F/F_0}(A) = \{x \in \overline{A} \otimes_F A / S(x) = x\}$.

Lemme 1.4.4 $\varphi : F \otimes_{F_0} N_{F/F_0}(A) \longrightarrow \overline{A} \otimes_F A$
$\lambda \otimes x \longmapsto \lambda x$
est un isoomomorphisme canonique de F_0-algèbres.

Corollaire 1.4.5 *Si A est une F-algèbre centrale simple alors $N_{F/F_0}(A)$ est une F_0-algèbre centrale simple et $deg\big(N_{F/F_0}(A)\big) = \big(deg(A)\big)^2$.*

Proposition 1.4.6 *1. Si A et B sont des F-algèbres centrales simples alors*

$$N_{F/F_0}(A \otimes_F B) = N_{F/F_0}(A) \otimes_{F_0} N_{F/F_0}(B).$$

2. Si A est une F_0-algèbre centrale simple alors $N_{F/F_0}(A \otimes_{F_0} F) \simeq A \otimes_{F_0} A$.

3. $N_{F/F_0} : Br(F) \longrightarrow Br(F_0)$ est un homomorphisme de groupes.
$[A] \longmapsto [N_{F/F_0}(A)]$

Preuve : Voir ([14, proposition 3.8, page 23]).

Chapitre 2

Involution d'une algèbre centrale simple

2.1 Involutions et formes bilinéaires

Définition 2.1.1 *Soit A un anneau unitaire non nécessairement commutatif.*
Une involution sur A est une application $\sigma : A \longrightarrow A$ vérifiant :

1. $\sigma(x+y) = \sigma(x) + \sigma(y)$ *pour tout* $x, y \in A$.
2. $\sigma(xy) = \sigma(y)\sigma(x)$ *pour tout* $x, y \in A$.
3. $\sigma^2 = Id_A$.

En conséquence, σ est une involution sur A si et seulement si σ est un isomorphisme d'ordre deux de A dans A^{op}.
Une involution sur une F-algèbre centrale simple A, est une involution sur l'anneau A.
Le couple (A, σ) est appelé algèbre à involution.

Exemples : Soit K un corps.

1. $t : M_n(K) \longrightarrow M_n(K)$ est une involution sur $M_n(K)$ appelée transposition.
   $(a_{ij}) \longmapsto (a_{ji})$

2. Si U est un élément inversible de $M_n(K)$ tel que $U^t = \pm U$, alors
$$\begin{array}{rccc} \sigma : & M_n(K) & \longrightarrow & M_n(K) \\ & M & \longmapsto & UM^tU^{-1} \end{array}$$
est une involution sur $M_n(K)$.

3. L'application :
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \longmapsto \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$
est une involution sur $M_2(K)$.

4. Si (A, σ) est un anneau à involution, alors $(\alpha_{ij}) \longmapsto (\sigma(\alpha_{ij}))^t$ est une involution sur $M_n(A)$.

Définition 2.1.2 *Soient (A, σ) et (A', σ') deux algèbres à involutions.*
On dit que $f : (A, \sigma) \longrightarrow (A', \sigma')$ est un homomorphisme d'algèbres à involution si $f : A \longrightarrow A'$ est un homomorphisme de F-algèbres vérifiant $\sigma' \circ f = f \circ \sigma$.

Proposition 2.1.3 *Si (A, σ) est une F-algèbre centrale simple à involution, alors $\sigma(F) = F$.*

Preuve : soit $x \in F$, pour tout $y \in A$ on a
$$\sigma(x)y = \sigma(x)\sigma(z) = \sigma(zx) = \sigma(xz) = \sigma(z)\sigma(x) = y\sigma(x)$$
donc $\sigma(x) \in F$ et $\sigma(F) \subset F$. Réciproquement, $F = \sigma\big(\sigma(F)\big) \subset \sigma(F)$. Par suite $\sigma(F) = F$. ∎

Soit (A, σ) une F-algèbre centrale simple à involution. Si on pose
$F_0 = inv(\sigma) = \{x \in F / \sigma(x) = x\}$, alors F_0 est un sous corps de F appelé le corps d'invariants de σ et on dit que σ une F/F_0-involution. La restriction de σ à F est un F_0- automorphisme de F égal à l'identité ou d'ordre 2. Autrement dit, l'une des conditons suivantes est satisfaite :

(i) $F_0 = F$ (σ est F-linéaire), dans ce cas σ est dite une involution de première espèce.

(ii) F/F_0 est une extension quadratique séparable et $Gal(F/F_0) = \{1, \sigma/F\}$, dans ce cas σ est dite une involution de deuxième espèce.

Exemples :

1. L'involution transposition est de première espèce sur $A = M_n(K)$.

2. L'involution σ définie sur $A = (a, b)_F)$ par : $\sigma(w + xi + yj + zk) = w - xi - yj - zk$ est une involution de première espèce sur A, appelée conjugaison.
3. Pour $A = M_n(\mathbb{C})$, l'involution $\sigma : M \longmapsto \overline{M}^t$ est de deuxième espèce.
4. Si σ est une involution de première espèce sur A et si K est une extension de F, alors σ se prolonge en une involution de première espèce $\sigma_K = \sigma \otimes Id_K$ sur $A_K = A \otimes_F K$.

Définition 2.1.4 *Soient V et W deux espaces vectoriels sur un corps F, V^* et W^* leurs espaces duals. Pour toute application F-linéaire $f : V \longrightarrow W$, on définit la transposée de f notée f^t par :* $f^t : W^* \longrightarrow V^*$
$g \longmapsto g \circ f$

Définition 2.1.5 *Soit V un espace vectoriel de dimension finie sur un corps F. Une forme bilinéaire $b : V \times V \longrightarrow F$ est dite non singulière si l'application*

$$\begin{array}{rccc} \widehat{b}: & V & \longrightarrow & V^* \\ & x & \longmapsto & \widehat{b}(x) : y \longmapsto b(x, y) \end{array}$$

est un isomorphisme d'espaces vectoriels.

Pour chaque forme bilinéaire non singulière b sur V, désignons par σ_b l'application :

$$End_F(V) \longrightarrow End_F(V).$$
$$f \longmapsto \widehat{b}^{-1} \circ f^t \circ \widehat{b}$$

σ_b est un anti-automorphisme F-linéaire appelé anti-automorphisme adjoint de b.
Dans la suite, $Ant_F(End_F(V))$ désignera l'ensemble des anti-automorphismes F-linéaires de $End_F(V)$ et par $Bil^\circ(V)$ l'ensemble des formes bilinéaires non singulières définies sur V.

Théorème 2.1.6 *L'application qui à chaque forme bilinéaire non singulière b associe son anti-automorphisme adjoint σ_b, induit une correspondance bijective de $Bil^\circ(V)/F^*$ dans $Ant_F(End_F(V))$.*

Preuve : Soit $\varphi : Bil^\circ(V)/F^* \longrightarrow Ant_F(End_F(V))$.
$\tilde{b} \longmapsto \sigma_b$

On a pour $b, b' \in Bil^\circ(V)$, $\tilde{b} = \tilde{b'} \Longleftrightarrow \exists \alpha \in F^*$ tel que $b' = \alpha b$. Or, $\sigma_{\alpha b} = \sigma_b$ donc $\sigma_b = \sigma_{b'}$,

par suite φ est bien définie.
Soient $b, b' \in Bil^{\circ}(V)$ telles que $\sigma_b = \sigma_{b'}$, montrons que $\tilde{b} = \tilde{b'}$.
On pose $\theta = \hat{b'} \circ \hat{b}^{-1}$, alors $\theta \in Gl(V)$ et $b'(x,y) = b\big(\theta(x), y\big)\ \forall x, y \in V$. Donc
$\sigma_b(f) = \theta \circ \sigma_{b'}(f) \circ \theta^{-1}$ pour tout $f \in End_F(V)$ de sorte que $\sigma_b = int(\theta) \circ \sigma_{b'}$. Or $\sigma_b = \sigma_{b'}$, alors $\theta \in F^*$ et par suite $b' = \theta b$, d'où $\tilde{b} = \tilde{b'}$.
Pour prouver que φ est surjective, fixons $b \in Bil^{\circ}(V)$ et soit $\sigma' \in Ant_F(End_F(V))$. Du fait que $\sigma_b \circ \sigma'^{-1}$ est un F-automorphisme de $End_F(V)$, le Théorème de Skolem-Noether assure l'existence de $u \in Gl(V)$ tel que $\sigma_b \circ \sigma'^{-1} = int(u)$. Posons $b'(x,y) = b\big(u(x), y\big)$, puisque
$b'\big(\sigma'(f)(x), y\big) = b'\Big(u^{-1} \circ \sigma_b(f)\big(u(x)\big), y\Big) = b\Big(\sigma_b(f)\big(u(x)\big), y\Big) = b\big(u(x), f(y)\big) = b'\big(x, f(y)\big)$.
On en déduit alors que $\sigma' = \sigma_{b'}$. D'où φ est bijective. ∎

Corollaire 2.1.7 *Les involutions de première espèce de $End_F(V)$ sont en correspondance bijective avec les formes bilinéaires non singulières symétriques ou anti-symétriques définies sur V à un scalaire non nul près.*

Preuve : Soit b une forme bilinéaire non singulière sur V. Si b est symétrique ou anti-symétrique alors $b(x,y) = \varepsilon b(y,x)\ \forall x, y \in V$ avec $\varepsilon = \pm 1$.
Pour tout $x, y \in V$ et pour tout $f \in End_F(V)$ on a :
$b\big(\sigma_b^2(f)(x), y\big) = b\big(x, \sigma_b(f)(y)\big) = \varepsilon b\big(\sigma_b(f)(y), x\big) = \varepsilon b\big(y, f(x)\big) = \varepsilon^2 b\big(f(x), y\big) = b\big(f(x), y\big)$.
D'où $\sigma_b^2 = Id$, par suite σ_b est une involution de première espèce de $End_F(V)$.
Inversement, si σ est une involution de première espèce de $End_F(V)$, alors d'après le théorème précédent, il existe une forme bilinéaire non singulière b sur V telle que $\sigma = \sigma_b$. Posons $b'(x,y) = b(y,x)$. On a $\sigma = \sigma_b = \sigma_{b'}^{-1}$, or $\sigma = \sigma_b$ est une involution alors $\sigma_b^2 = Id$ et $\sigma_b = \sigma_{b'}$, par suite $b = \varepsilon b'$ où $\varepsilon \in F^*$ et $\varepsilon^2 = 1$. D'où b est symétrique ou anti-symétrique. ∎

2.2 Types d'involutions sur une algèbre centrale simple

Considérons une F-algèbre centrale simple A de degré n ayant une involution σ de première espèce. Pour toute extension K de F, σ se prolonge en une involution de première espèce $\sigma_K = \sigma \otimes Id_K$ sur la K-algèbre centrale simple $A_K = A \otimes_F K$. En particulier, si K neutralise

A, alors $A_K = End_K(V)$ pour un certain K-espace vectoriel de dimension $n = deg(A)$, par suite σ_K est l'anti-automorphisme adjoint d'une forme bilinéaire non singulière b sur V qui est symétrique ou anti-symétrique.

Définition 2.2.1 *L'involution σ est dite de type +1 ou orthogonale (resp de type -1 ou symplectique) si σ_K est l'anti-automorphisme adjoint d'une forme bilinéaire symétrique (resp anti-symétrique).*

Pour montrer que cette définition ne dépend pas du choix du corps neutralisant, on va donner une caractérisation des involutions orthogonales et symplectiques.

Proposition 2.2.2 *Soit A une F-algèbre centrale simple de degré n et σ une involution de A. Posons $(A,\sigma)_+ = \{a \in A/\sigma(a) = a\}$ et $(A,\sigma)_- = \{a \in A/\sigma(a) = -a\}$.*

1. *Si σ est une involution de première espèce qui est orthogonale, alors :*
$$dim_F(A,\sigma)_+ = \frac{n(n+1)}{2} \text{ et } dim_F(A,\sigma)_- = \frac{n(n-1)}{2}.$$
2. *Si σ est une involution de première espèce qui est symplectique, alors :*
$$dim_F(A,\sigma)_+ = \frac{n(n-1)}{2} \text{ et } dim_F(A,\sigma)_- = \frac{n(n+1)}{2}.$$
Dans ce cas n est nécessairement pair.
3. *Si σ est une involution de deuxième espèce du corps d'invariants F_0, alors :* $dim_{F_0}(A,\sigma)_+ = dim_{F_0}(A,\sigma)_- = n^2$.

Preuve : On suppose que σ est de première espèce, on peut prendre
$A = M_n(F) = End_F(F^n)$, donc σ est une involution adjointe d'une forme bilinéaire non singulière b sur F^n. Désignons par $u \in GL_n(F)$ la matrice de b, $b(x,y) = x^t uy, \forall x,y \in F^n$, en plus $u^t = -u$ si b est anti-symétrique (σ symplectique). Pour n impair, toute matrice anti-symétrique de $M_n(F)$ est singulière, il est donc nécessaire que n soit pair, pour l'existence d'une involution symplectique. $b\big(\sigma(f)(x),y\big) = b\big(x,f(y)\big)\ \forall x,y \in F^n, \forall f \in M_n(F)$. Donc $\sigma(f) = u^{-1}f^t u$, on en déduit alors que : $(A,\sigma)_+ = u^{-1}(M_n(F),t)_+$ si σ est orthogonale et $(A,\sigma)_+ = u^{-1}(M_n(F),t)_-$ si σ est symplectique. Compte tenu du fait que
$A = (A,\sigma)_+ \oplus (A,\sigma)_-$, $dim_F(M_n(F),t)_+ = \frac{n(n+1)}{2}$ et $dim_F(M_n(F),t)_- = \frac{n(n-1)}{2}$, on en déduit

1 et 2).

Si σ est une involution de deuxième espèce du corps d'invariants F_0, alors il existe $a \in F$ tel que $\sigma(a) - a \neq 0$, donc $z = \sigma(a) - a \in F$ et $\sigma(z) = -z$. Ainsi, $(A,\sigma)_+ = z(A,\sigma)_- \;\; et \;\; (A,\sigma)_- = z(A,\sigma)_+$. En conséquence, $dim_{F_0}(A,\sigma)_+ = dim_{F_0}(A,\sigma)_-$ et $A = (A,\sigma)_+ \oplus (A,\sigma)_-$. Par suite,
$2dim_{F_0}(A,\sigma)_+ = 2dim_{F_0}(A,\sigma)_- = dim_{F_0}A = dim_F A.dim_{F_0}F = 2n^2$. ∎

Proposition 2.2.3 *$(A_1,\sigma_1),...,(A_n,\sigma_n)$ sont des F-algèbres centrales simples à involutions. Les propriétés suivantes sont vérifiées :*

1. *Si $\forall\ 1 \leq i \leq n \quad \sigma_i$ est une F/F_0-involution, alors $\sigma_1 \otimes ..... \otimes \sigma_n$ est une F/F_0-involution de $A_1 \otimes_F ..... \otimes_F A_n$.*
2. *Si $\forall\ 1 \leq i \leq n \quad \sigma_i$ est une involution de première espèce et de type $\varepsilon_i = \pm 1$, alors $\sigma_1 \otimes ..... \otimes \sigma_n$ est une involution de première espèce et de type $\varepsilon = \prod_{i=1}^{n} \varepsilon_i$.*

Preuve : Par récurrence sur n (Voir [11, proposition 2.3, page 14]). ∎

Remarque : Soit σ une involution de première espèce d'une F-algèbre centrale simple A, posons $\sigma_a = int(a) \circ \sigma$ pour $a \in U(A)$.

1. Si $a \in (A,\sigma)_+$, alors les involutions σ et σ_a sont de même type.
2. Si $a \in (A,\sigma)_-$, alors les involutions σ et σ_a sont de types différents.

Exemples : Soit un corps F.

1. $$\begin{array}{rccc} \sigma : & A = M_2(F) & \longrightarrow & M_2(F) \\ & \begin{pmatrix} a & b \\ c & d \end{pmatrix} & \longmapsto & \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \end{array}$$
   On a $dim_F(A,\sigma)_+ = 1 = \frac{2(2-1)}{2}$ donc σ est symplectique.
2. Soient $Q = (a,b)_F$ et $\sigma(w + xi + yj + zk) = w - xi - yj - zk$.
   On sait que σ est une involution de première espèce sur Q et $degQ = 2$, d'autre part $(Q,\sigma)_+ = F$. Ainsi $dim_F(Q,\sigma)_+ = 1 = \frac{2(2-1)}{2}$, en conséquence, σ est symplectique . Si σ' désigne une autre involution de première espèce sur Q, $\exists u \in U(A)$ tel que

$\sigma' = int(u) \circ \sigma = \sigma_u$ et $\sigma(u) = \pm u$. D'après la remarque précédente Si σ' est symplectique alors $\sigma(u) = u$, donc $u \in (Q, \sigma)_+ = F$, par suite $\sigma' = \sigma$. Si σ' est orthogonale, alors $\sigma(u) = -u$, donc u est un quaternion pur. En conclusion :

(i) Toute algèbre de quaternions a une unique involution symplectique qui est l'involution standard σ.

(ii) Toute involution orthogonale sur une algèbre de quaternions est de la forme $int(u) \circ \sigma$ avec u un quaternion pur inversible.

3. L'involution transposition $t : M_n(F) \longrightarrow M_n(F)$ est orthogonale, car $dim_F(M_n(F), t)_+ = \frac{n(n+1)}{2}$.

Théorème 2.2.4 *(Albert) Soit σ une F/F_0- involution sur une algèbre de quaternions Q. Alors il existe une unique F_0-algèbre centrale simple $Q_0 \subset Q$ telle que :*

$$Q = Q_0 \otimes_{F_0} F \quad et \quad \sigma = \gamma_0 \otimes \alpha$$

avec γ_0 l'involution canonique de Q_0 et $\alpha = \sigma/F$ le F_0-automorphisme non trivial de F, de plus Q_0 est deteminée d'une façon unique.

Preuve : Voir [13, chapitre 8. §11. Théorème 11.2]. ∎

Théorème 2.2.5 *(Théorème 90 de Hilbert) Soient E/K une extension cyclique (finie, galoisienne, et de groupe de Galois cyclique) de corps et b un élément de E. Les conditions suivantes sont équivalentes :*

1. $N_{E/K}(b) = 1$
2. *il existe $a \in E^*$ tel que $b = a\psi(a)^{-1}$, où ψ désigne un générateur du groupe de Galois de E/K.*

Preuve : Voir ([13, Lemma 6.6, page 260]). ∎

Théorème 2.2.6 *Soient A une F-algèbre centrale simple et σ une F/F_0-involution de A, alors les propriétés suivantes sont vérifiées :*

1. *Si $\lambda \in F$ satisfait $\lambda\sigma(\lambda) = 1$ et si $a \in U(A)$ tel que $a = \lambda\sigma(a)$, alors $\sigma_a = int(a) \circ \sigma$ est une F/F_0-involution de A.*

2. *Inversement, si τ une F/F_0-involution arbitraire de A, alors il existe $a \in U(A)$ vérifiant $a = \varepsilon\sigma(a)$, $\varepsilon \in F$ et $\varepsilon\sigma(\varepsilon) = 1$ tel que $\tau = \sigma_a$.*

3. *Dans le cas d'une involution de première espèce, a est unique à un scalaire près $\alpha \in F^*$. Dans le cas d'une involution de deuxième espèce, $\tau = \sigma_a$ avec $a = \sigma(a)$.*

4. *Si σ_a et σ_b sont deux F/F_0-involutions de A, alors $(A, \sigma_a) \simeq (A, \sigma_b)$ si et seulement si $\exists c \in U(A)$, $\exists \alpha \in F$ tels que $b = \alpha ca\sigma(c)$.*

où $U(A)$ désigne l'ensemble des éléments inversiblrs de A.

Preuve :

1. Il est clair que σ_a est une involution de A, montrons que $inv(\sigma) = inv(\sigma_a)$.
   Soit $x \in F$, on a : $x \in inv(\sigma) \Longleftrightarrow \sigma(x) = x \Longleftrightarrow \sigma_a(x) = a\sigma(x)a^{-1} = axa^{-1} = x$, donc $inv(\sigma) = inv(\sigma_a)$, par suite σ_a est une F/F_0-involution.

2. Soit τ une F/F_0-involution quelconque de A. On a $\tau \circ \sigma$ est un F_0-automorphisme de A, donc $\exists a \in U(A)$ tel que $\tau \circ \sigma = int(a)$, d'où $\tau = int(a) \circ \sigma = \sigma_a$. Donc $\tau^2 = int(a\sigma(a)^{-1}) = Id$, ainsi $a\sigma(a)^{-1} = \varepsilon \in F$,
   d'où $a = \varepsilon\sigma(a) = \varepsilon\sigma(\varepsilon\sigma(a)) = \varepsilon\sigma(\varepsilon)a \Longrightarrow \varepsilon\sigma(\varepsilon) = 1$.

3. Si σ est de première espèce et si $\tau = \sigma_a$, $a \in U(A)$ vérifie $\sigma(a) = \pm a$, supposons qu'il existe $b \in U(A)$ tel que $\tau = \sigma_b$, il en résulte que $a = \beta b$ avec $\beta \in F$ et on a $\sigma(b) = \pm b$.
   Dans le cas où σ est de deuxième espèce, par le théorème 90 de Hilbert, on peut choisir $\alpha \in F^*$ tel que $\alpha\sigma(\alpha^{-1}) = \varepsilon$ et en remplaçant a par $a' = \alpha^{-1}a$ nous obtenons
   $\tau = \sigma_a = \sigma_{a'}$ tel que $\sigma(a') = a'$.

4. $(A, \sigma_a) \simeq (A, \sigma_b)$ si et seulement si il existe un automorphisme de A tel que
   $\sigma_b \circ f = f \circ \sigma_a$, donc $\exists c \in U(A)$ tel que $f = int(c)$.
   On en déduit que $ac^{-1}b^{-1}\sigma^{-1}(c) = \alpha \in F$. ∎

Le but des deux sections suivantes est de caractériser l'existence d'une involution sur une algèbre centrale simple.

2.3 Existence d'involutions de première espèce

Soit A une F-algèbre centrale simple. Considérons l'application F-linéaire

$$\begin{array}{rccc} Sand: & A \otimes_F A & \longrightarrow & End_F(A) \\ & a \otimes b & \longmapsto & axb \end{array}$$

Lemme 2.3.1 *Sand est un isomorphisme de F-espaces vectoriels*

Preuve :
$Sand = \psi \circ \varphi$ avec ψ et φ sont deux isomorphismes de F-espaces vectoriels définis par :

$$\begin{array}{rccc} \psi: & A \otimes_F A & \longrightarrow & A \otimes_F A^{op} \\ & a \otimes b & \longmapsto & a \otimes b^{op} \end{array}$$

$$\begin{array}{rccc} \varphi: & A \otimes_F A^{op} & \longrightarrow & End_F(A) \\ & a \otimes b^{op} & \longmapsto & \psi(a \otimes b^{op}) : x \longmapsto axb \end{array}$$

(φ est l'isomorphisme de l'assertion (2) du théorème de Wedderburn) ∎

Soient A une F-algèbre centrale simple et K un corps déployant de A. Alors il existe
$\varphi : A \otimes_F K \longrightarrow M_n(K)$ un isomorphisme de K-algèbres.
Pour tout $a \in A$, le polynôme

$$Prd_A(a) := det(XI_n - \varphi(a \otimes 1)) = X^n - s_1X^{n-1} + s_2X^{n-2} + ... + (-1)^n s_n \in F[X]$$

ne dépend pas du choix de φ, car si $\varphi' : A \otimes_F K \longrightarrow M_n(K)$ est un isomorphisme de K-algèbres, alors d'après le théorème de Skolem-Noether, $\varphi(a \otimes 1)$ et $\varphi'(a \otimes 1)$ sont des matrices semblables et ont donc même polynôme caractéristique. On montre en plus que $Prd_A(a)$ ne dépend pas du choix du corps neutralisant K.

Définition 2.3.2 *1. $Prd_A(a)$ est appelé polynôme caractéristique réduit de a.*
2. $Trd_A(a) = s_1 = tr(\varphi(a \otimes 1))$ est appelée la trace réduite de a.
3. $Nrd_A(a) = s_n = det(\varphi(a \otimes 1))$ est appelée la norme réduite de a.

Remarque : La composée de la trace réduite $Trd_A : A \longrightarrow F$ et l'inclusion $F \hookrightarrow A$ permet de voir Trd_A comme un élément de $End_F(A)$.

Définition 2.3.3 *L'unique élément $g \in A \otimes_F A$ tel que $Sand(g) = Trd_A$ est appelé élément de Goldman de $A \otimes_F A$.*

Proposition 2.3.4 *L'élément de Goldman $g \in A \otimes_F A$ vérifie les propriétés suivantes :*

1. $g^2 = 1$
2. $g.(a \otimes b) = (b \otimes a).g \ \ \forall\, a, b \in A$
3. *Si $A = End_F(V)$, alors sous l'identification canonique $A \otimes_F A = End_F(V \otimes_F V)$, g est défini par : $g(v_1 \otimes v_2) = v_2 \otimes v_1 \ \forall v_1, v_2 \in V$.*

Preuve : Montrons (3). Pour cela, on va utiliser l'isomorphisme canonique $End_F(V) = V \otimes_F V^*$. Soient $(e_i)_{1 \le i \le n}$ une base de V et $(e_i^*)_{1 \le i \le n}$ sa base duale. Soit l'élément

$$g = \sum_{i,j} (e_i \otimes e_j^*) \otimes (e_j \otimes e_i^*) \in A \otimes_F A$$

On a $\forall f \in End_F(V) : sand(g)(f) = \sum_{i,j} \big(e_i \otimes e_j^*\big) \circ f \circ \big(e_j \otimes e_i^*\big) = \sum_{i,j} e_j^*\big(f(e_j)\big)(e_i \otimes e_i^*)$. Or, $\sum_i e_i \otimes e_i^* = Id_V$ et $\sum_j e_j^*(f(e_j)) = tr(f)$, donc $sand(g)(f) = tr(f)$, par suite g est l'élément de Goldman de $A \otimes_F A$. Par ailleurs $\forall v_1, v_2 \in V$:
$g(v_1 \otimes v_2) = \sum_{i,j} (e_i \otimes e_j^*)(v_1) \otimes (e_j \otimes e_i^*)(v_2) = \Big(\sum_i e_i.e_i^*(v_2)\Big) \otimes \Big(\sum_j e_j.e_j^*(v_1)\Big) = v_2 \otimes v_1$.
Ainsi, la démonstration de (3) est complète, et toujours sous la condition $A = End_F(V)$ on a : $g\Big(g(v_1 \otimes v_2)\Big) = g(v_2 \otimes v_1) = v_1 \otimes v_2$, d'où (1). D'autre part $\forall a, b \in A, \forall v_1, v_2 \in V$: $[g \circ (a \otimes b)](v_1 \otimes v_2) = g\Big(a(v_1) \otimes b(v_2)\Big) = b(v_2) \otimes a(v_1) = (b \otimes a)(v_2 \otimes v_1) = [(b \otimes a) \circ g](v_1 \otimes v_2)$. En conséquence, on a (2). Si A est quelconque, alors pour un corps K neutralisant A, l'élément de Goldman de $A \otimes_F A$ est celui de $A_K \otimes_K A_K$. On applique ce qui précède pour conclure. ∎

Soit A une F-algèbre centrale simple. Chaque anti-automorphisme F-linéaire σ sur A iduit une structure de $A \otimes_F A$-modules à droite sur A définie par : $x.(a \otimes b) = \sigma(a)xb$.

Lemme 2.3.5 *Soit A une F-algèbre centrale simple et σ une involution de première espèce de A. L'application $\sigma' : A \otimes_F A \longrightarrow A$ est un homomorphisme de $A \otimes_F A$-modules à droite*

$$a \otimes b \longmapsto \sigma(a)b$$

et on a : $(A \otimes_F 1) \oplus I_\sigma = A \otimes_F A = I_\sigma \oplus (1 \otimes_F A)$, où $I_\sigma = Ker_{\sigma'}$.

Preuve :
Si $x \in A$ alors $\exists y \in A$ tel que $\sigma(y) = x$, ainsi $\sigma'(y \otimes 1) = x$. Par suite σ' est surjective et que $dim_F I_\sigma = dim_F(A \otimes_F A) - dim_F A$. Or, $\sigma'(a \otimes 1) = \sigma(a)$ et $\sigma'(1 \otimes a) = a$, $\forall a \in A$, alors $(A \otimes_F 1) \cap I_\sigma = I_\sigma \cap (1 \otimes_F A) = \{0\}$. D'où $(A \otimes_F 1) \oplus I_\sigma = A \otimes_F A = I_\sigma \oplus (1 \otimes_F A)$. ∎

Lemme 2.3.6 *Si $A = End_F(V)$ et σ une involution de première espèce sur A associée à $b \in Bil^\circ(V)$, alors $I_\sigma = \{f \in End_F(V \otimes_F V)/b \circ f = 0\}$. De plus, si g est l'élément de Goldman de $A \otimes_F A$ alors $1-g \in I_\sigma$ si b est symétrique et $1+g \in I_\sigma$ si b est anti-symétrique.*

Preuve : On peut Voir b comme étant l'application linéaire $b : V \otimes_F V \longrightarrow F$.
Identifions $A \otimes_F A$ à $End_F(V \otimes_F V)$.
On a : $\forall f = f_1 \otimes f_2 \in End_F(V \otimes_F V) = End_F(V) \otimes_F End_F(V)$, $\forall x, y \in V$:
$b \circ \Big(Id_V \otimes \sigma'(f)\Big)(x \otimes y) = b\Big(x, \sigma(f_1) \circ f_2(y)\Big) = b\Big(f_1(x), f_2(y)\Big) = b \circ f(x \otimes y)$. Il en résulte que $b \circ f = b \circ \Big(Id_V \otimes \sigma'(f)\Big)$. Ainsi $b \circ f = 0 \Longleftrightarrow \sigma'(f) = 0$. D'autre part, si g est l'élément de Goldman de $A \otimes_F A$ on a :

(i) $1 - g \in Ker\sigma' \Longleftrightarrow b = b \circ g \Longleftrightarrow$ b symétrique

(ii) $1 + g \in Ker\sigma' \Longleftrightarrow b = -b \circ g \Longleftrightarrow$ b anti-symétrique. ∎

Théorème 2.3.7 *Soit A une F-algèbre centrale simple, et $g \in A \otimes_F A$ l'élément de Goldman. L'application $\sigma \longmapsto I_\sigma$ définit une correspondance bijective entre les involutions de première espèce sur A et les idéaux à droite $I \subset A \otimes_F A$ vérifiant :*

1. $(A \otimes_F 1) \oplus I = A \otimes_F A = I \oplus (1 \otimes_F A)$.
2. $1 \pm g \in I$.

Par cette correspondance, une involution σ est de type orthogonale (resp symplectique) si et seulement si l'idéal correspondant I_σ contient $1 - g$ (resp $1 + g$).

Remarquons que si $I \subset A \otimes_F A$ vérifie (2), alors chacune des deux égalités de (1) implique l'autre, en effet : $\forall a \in A, (1 \pm g)(a \otimes 1)g \in I$. Or, d'après la proposition 2.3.4 on a : $g(a \otimes 1)g = 1 \otimes a$. En conséquence, $(1 \pm g)(a \otimes 1)g = (a \otimes 1)g \pm (1 \otimes a) \in I$.
Ainsi, il vient que si I contient $a \otimes 1$ alors il contient $1 \otimes a$, et réciproquement.

Preuve du théorème 2.3.7 (voir [6, Theorem 3.8, page 34]) :

D'après le lemme 2.3.5 et le lemme 2.3.6, $Ker\sigma'$ vérifie (i) et (ii), donc l'application $\sigma \longmapsto I_\sigma$ est bien définie. Pour montrer qu'elle est bijective on va définir son application inverse. Supposons I un idéal à droite de $A \otimes_F A$ vérifiant (1) et (2). Il s'ensuit de $A \otimes_F A = I \oplus (1 \otimes_F A)$ que $\forall a \in A, \exists! \sigma_I(a) \in A \ tq \ a \otimes 1 - 1 \otimes \sigma_I(a) \in I$ Montrons que σ_I est une involution de première espèce sur A. Soient $a, b \in A$:

(i) On tire de $a \otimes 1 - 1 \otimes \sigma_I(a) \in I$ et $b \otimes 1 - 1 \otimes \sigma_I(b) \in I$:

$$(a+b) \otimes 1 - 1 \otimes \big(\sigma_I(a) + \sigma_I(b)\big) \in I$$
$$(a+b) \otimes 1 - 1 \otimes \sigma_I(a+b) \in I$$

La soustraction des deux éléments donne $1 \otimes \big(\sigma_I(a+b) - \sigma_I(a) - \sigma_I(b)\big) \in I$. Or, on sait que $I \cap 1 \otimes_F A = \{0\}$, ainsi $\sigma_I(a+b) = \sigma_I(a) + \sigma_I(b)$.

(ii) On a $\big(a \otimes 1 - 1 \otimes \sigma_I(a)\big)(b \otimes 1) \in I$; $\big(b \otimes 1 - 1 \otimes \sigma_I(b)\big)\big(1 \otimes \sigma_I(a)\big) \in I$. L'addition des deux relations donne $ab \otimes 1 - 1 \otimes \big(\sigma_I(b)\sigma_I(a)\big) \in I$.
Par conséquent : $\sigma_I(ab) = \sigma_I(b)\sigma_I(a)$.

(iii) On sait que $1 \pm g \in I$, ainsi $\forall u \in I, (1 \pm g).u - u \in I$. Alors $\forall u \in I, gu \in I$. Il en résulte que $\forall a \in A, g\big(a \otimes 1 - 1 \otimes \sigma_I(a)\big)g = 1 \otimes a - \sigma_I(a) \otimes 1 \in I$. d'où $\sigma_I(a) \otimes 1 - 1 \otimes a \in I$; $\sigma_I(a) \otimes 1 - 1 \otimes \sigma_I\big(\sigma_I(a)\big) \in I$. Ce qui entraîne que $\sigma_I^2(a) = a$.

(iv) Si $\alpha \in F$, alors $\alpha \otimes 1 - 1 \otimes \sigma_I(\alpha) = 1 \otimes \alpha - 1 \otimes \sigma_I(\alpha) = 1 \otimes \big(\alpha - \sigma_I(\alpha)\big) \in I \cap (1 \otimes_F A)$. Donc $\sigma_I(\alpha) = \alpha$. Par ailleurs σ_I est bijective d'après sa construction. Finalement, σ_I est une involution de première espèce sur A.

Soit $u = \sum_i x_i \otimes y_i \in A \otimes_F A \cap Ker\sigma'_I$. Ainsi $\sum_i \sigma_I(x_i)y_i = 0$, et

$$u = \sum_i \big(x_i \otimes y_i - 1 \otimes \sigma_I(x_i)y_i\big) = \sum_i \big(x_i \otimes 1 - 1 \otimes \sigma_I(x_i)\big).(1 \otimes y_i)$$

Mais les éléments $x_i \otimes 1 - 1 \otimes \sigma_I(x_i)$ sont dans l'idéal à droite I de $A \otimes_F A$, donc $Ker\sigma'_I \subset I$. Or, il résulte de $I \oplus (1 \otimes_F A) = Ker\sigma'_I \oplus (1 \otimes_F A)$ que $Ker\sigma'_I$ et I ont même dimension. D'où : $Ker\sigma'_I = I$. Inversement, si σ est une involution de première espèce sur A, alors : $\forall a \in A \ , \ a \otimes 1 - 1 \otimes \sigma(a) \in Ker\sigma'$. Il s'ensuit : $\sigma_{Ker\sigma'} = \sigma$. Par conséquent, les deux applications $\sigma \longrightarrow Ker\sigma'$ et $I \longrightarrow \sigma_I$ sont l'inverse l'une de l'autre. ∎

Proposition 2.3.8 *Si A est une F-algèbre centrale simple munie d'une involution σ de première espèce, alors l'application :*

$$\begin{aligned} \sigma_* : \quad A \otimes_F A &\longrightarrow End_F(A) \\ a \otimes b &\longmapsto \sigma_*(a \otimes b) : x \longmapsto \sigma(a)xb \end{aligned}$$

est un isomorphisme de F-algèbres.

Preuve : Il est facile de vérifier que σ_* est un homomorphisme de F-algèbres. Comme $A \otimes_F A$ est simple il en résulte que σ_* est injective. La surjectivité est assurée par le fait que $A \otimes_F A$ et $End_F(A)$ ont même dimension. ∎

On déduit de la proposition précédente que si A admet une involution de première espèce, alors $A \otimes_F A$ est déployée.

Théorème 2.3.9 *Soit A une F-algèbre centrale simple. A admet une involution de première espèce si et seulement si $A \otimes_F A$ est déployée.*

Preuve : Voir ([6, Theorem 3.1, page 31])

2.4 Existence d'involutions de deuxième espèce

Lemme 2.4.1 *Soient A une F-algèbre centrale simple et σ une F/F_0-involution de deuxième espèce de A. Alors l'application*

$$\begin{aligned} \sigma_* : \quad N_{F/F_0}(A) &\longrightarrow End_{F_0}\big((A,\sigma)_+\big) \\ \overline{a} \otimes b &\longmapsto \sigma_*(\overline{a} \otimes b) : x \longmapsto ax\sigma(b) \end{aligned}$$

est un isomorphisme de F_0-algèbres.

Preuve : Considérons l'application

$$\begin{aligned} \varphi : \quad \overline{A} \otimes_F A &\longrightarrow End_F(A) \\ \overline{a} \otimes b &\longmapsto \sigma_*(\overline{a} \otimes b) : x \longmapsto ax\sigma(b) \end{aligned}$$

On vérifie aisément que φ est un homomorphisme de F-algèbres. Comme $\overline{A} \otimes_F A$ est une F-algèbre simple alors φ est injective, or $dim_F(\overline{A} \otimes_F A) = dim_F End_F(A)$ donc φ est un isomorphisme de F-algèbres. Si $u \in N_{F/F_0}(A)$, c'est- à-dire $u = \overline{a} \otimes b = \overline{b} \otimes a \in \overline{A} \otimes_F A$,

alors pour tout $x \in A$ on a :
$\varphi(u)(\sigma(x)) = \varphi(\overline{a} \otimes b)(\sigma(x)) = \varphi(\overline{b} \otimes a)(\sigma(x)) = b\sigma(x)\sigma(a) = \sigma(ax\sigma(a)) = \sigma(\varphi(u)(x))$.
En particulier, si $x \in (A,\sigma)_+$ alors $\varphi(u)(x) = \sigma\big(\varphi(u)(x)\big)$. C'est-à-dire,
$\varphi(u)\big((A,\sigma)_+\big) \subset (A,\sigma)_+$. En conséquence, $\sigma_* = \varphi/N_{F/F_0}(A) : N_{F/F_0}(A) \longrightarrow End_{F_0}\big((A,\sigma)_+\big)$ est un homomorphisme injectif de F_0-algèbres.
D'autre part $dim_{F_0} End_{F_0}\big((A,\sigma)_+\big) = [dim_{F_0}(A,\sigma)_+]^2 = (degA)^4 = dim_{F_0} N_{F/F_0}(A)$, ainsi σ_* est un isomorphisme de F_0-algèbres. ∎

L'application :

$$\begin{array}{rccc} \sigma' : & N_{F/F_0}(A) & \longrightarrow & (A,\sigma)_+ \\ & u & \longmapsto & \sigma_*(u)(1) \end{array}$$

est un homomorphisme surjectif de $N_{F/F_0}(A)$-modules à gauche où l'action de $N_{F/F_0}(A)$ sur $(A,\sigma)_+$ est définie par : $x.u = \sigma_*(u)(x)$. Il suit alors que $Ker\sigma'$ est un idéal à gauche de $N_{F/F_0}(A)$ tel que $dim_{F_0}(Ker\sigma') = n^4 - n^2$ où $n = deg(A)$. Par extension des scalaires à F et compte tenu du fait que $N_{F/F_0}(A)_F = \overline{A} \otimes_F A$, σ' induit une application :

$$\begin{array}{rccc} \sigma'_F : & \overline{A} \otimes_F A & \longrightarrow & A \\ & \overline{a} \otimes b & \longmapsto & a\sigma(b) \end{array}$$

en plus $(\overline{A} \otimes_F 1) \oplus Ker\sigma'_F = \overline{A} \otimes_F A = Ker\sigma'_F \oplus (1 \otimes A)$.

Théorème 2.4.2 *Soient A une F-algèbre centrale simple et F/F_0 une extension quadratique séparable. Alors l'application $\sigma \longrightarrow ker\sigma'$ définit une correspondance bijective entre les F/F_0-involutions de deuxième espèce de A et les idéaux à droite $I \subset N_{F/F_0}(A)$ tels que $(\overline{A} \otimes_F 1) \oplus I_F = \overline{A} \otimes_F A = I_F \oplus (1 \otimes_F A)$.*

Preuve : Analogue à celle du théorème 2.3.7. ∎

Théorème 2.4.3 *(Théorème d'Albert-Riehm-Scharlau) Soient F/F_0 une extension quadratique séparable et A une F-algèbre centrale simple. A admet une F/F_0-involution de deuxième espèce si et seulement si $N_{F/F_0}(A)$ est déployée.*

Preuve : Voir ([6, Theorem 3.1, page 31]) ∎

2.5 Algèbres à involution sur un corps de caractéristique deux

Dans ce chapitre, le corps F est de caractéristique deux.
Soit (A, σ) une F-algèbre centrale simple à involution de première espèce. Les définitions de $(A, \sigma)_+$ et $(A, \sigma)_-$ sont les mêmes que précédemment, mais dans ce cas, on a :
$(A, \sigma)_+ = (A, \sigma)_-$. Notons par $Alt(A, \sigma) = \{a + \sigma(a)/a \in A\}$ l'espace des éléments alternés de A. On a : $Alt(A, \sigma) \subset (A, \sigma)_+$.

Proposition 2.5.1 *Soit σ une involution sur $M_n(F)$ de première espèce. Alors on a :*

1. *$\sigma = \sigma_u = Int(u) \circ t$, avec u une matrice inversible de $M_n(F)$ vérifiant $u^t = u$.*
2. *$(M_n(F), \sigma)_+ = u.(M_n(F), t)_+$*
3. *$dim_F(M_n(F), \sigma)_+ = \frac{n(n+1)}{2}$*
4. *$Alt(M_n(F), \sigma) = u.Alt(M_n(F), t) = Alt(M_n(F), t).u^{-1}$*
5. *$u \in Alt(M_n(F), \sigma)$ si et seulement si tous les éléments diagonaux de u sont nuls.*

Preuve :

1. La proposition 2.2.6 en caractéristique deux ($u^t = \pm u \Longleftrightarrow u^t = u$).
2. facile à vérifier.
3. D'après 2)
4. Il suffit de voir que :

$$\sigma(x) + x = ux^t u^{-1} + x = ux^t u^{-1} + uu^{-1}x = u(x^t u^{-1} + u^{-1}x) = u\big(u^{-1}x + (u^{-1}x)^t\big).$$

$$\sigma(x) + x = ux^t u^{-1} + x = (ux^t + xu)u^{-1} = \big(ux + (xu)^t\big)u^{-1}.$$

5. Si $u = m + m^t$ tel que $m \in M_n(F)$, alors $u_{ii} = 2m_{ii} = 0$. Réciproquement, si $\forall 1 \leq i \leq n$, $u_{ii} = 0$, alors $u = m + m^t$ avec $m_{ij} = u_{ij}$ si $i < j$ et $m_{ij} = 0$ si non.

Lemme 2.5.2 *Soit u une matrice inversible de $M_n(F)$ telle que $u^t = u$.*

1. *Si $u \in Alt(M_n(F), t)$, alors il existe une matrice inversible c de $M_n(F)$ telle que*

$$cuc^t = \begin{pmatrix} J & & 0 \\ & \ddots & \\ 0 & & J \end{pmatrix} \quad avec \quad J = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

2. *Si $u \notin Alt(M_n(F), t)$, alors il existe une matrice inversible c de $M_n(F)$ telle que cuc^t est diagonale.*

Preuve : Voir ([4, Theorem 20]). ∎

Définition 2.5.3 *Soit $\sigma = \sigma_u$ une involution de première espèce sur $M_n(F)$.*

(i) Si $u \notin Alt(M_n(F), t)$, σ est dite orthogonale ou de type 1.

(ii) Si $u \in Alt(M_n(F), t)$, σ est dite symplectique ou de type 0.

Proposition 2.5.4 *Soit $\sigma = \sigma_u$ une involution de première espèce sur $M_n(F)$. Alors σ est symplectique si et seulement si : $tr(m) = 0 \quad \forall m \in (M_n(F), \sigma)_+$.*

Preuve : On sait que $m \in (M_n(F), \sigma)_+$ est équivalent à $m = us$ avec $s \in (M_n(F), t)_+$.
Si σ est symplectique, alors $u = x + x^t$, $x \in M_n(F)$. On a pour tout $s \in (M_n(F), t)_+$:

$$tr(xs) = tr(sx) = tr(s^t x) = tr\big((x^t s)^t\big) = tr(x^t s)$$

Il en résulte que $tr(us) = tr\big((x + x^t)s\big) = 2.tr(xs) = 0$.
Réciproquement, Soit e_{ii} la matrice dont tous les éléments sont nuls sauf l'intersection de la i-ème ligne et colonne qui vaut 1. Ainsi, pour tout i on a : $tr(u.e_{ii}) = u_{ii} = 0$ ($u.e_{ii} \in (M_n(F), \sigma)_+$ car e_{ii} est symétrique). ∎

Proposition 2.5.5 *Soient σ_u une involution de première espèce sur $M_n(F)$ et $\omega \in (M_n(F), \sigma_u)_+ \cap Gl_n(F)$.*

1. *Si $\omega \in Alt(M_n(F), \sigma_u)$, alors $int(\omega) \circ \sigma_u$ est de type 0.*

2. *Si $\omega \notin Alt(M_n(F), \sigma_u)$, alors $int(\omega) \circ \sigma_u$ est de type 1.*

Preuve :

1. Si $\omega \in Alt(M_n(F), \sigma_u) = u.Alt(M_n(F), t)$, alors $\omega = u(x+x^t) = ux+ux^t$. Ainsi, $int(\omega)\circ \sigma_u = \sigma_{\omega u}$ avec $(\omega u)^t = \omega u$ (car $\sigma_u(\omega) = \omega$) et $\omega u = uxu + (uxu)^t \in Alt(M_n(F), t)$. Donc par définition $int(\omega) \circ \sigma_u$ est de type 0.
2. Si $\omega \notin Alt(M_n(F), \sigma_u) = u.Alt(M_n(F), t) = Alt(M_n(F), t).u^{-1}$, alors $\omega u \notin Alt(M_n(F), t)$. En conséquence $\sigma_{\omega u} = int(\omega) \circ \sigma_u$ est de type 1. ∎

Soient (A, σ) une F-algèbre centrale simple à involution σ de première espèce et K un corps neutralisant pour A, ainsi il existe un isomorphisme $\varphi : A_K = A \otimes_F K \longrightarrow M_n(K)$.
On a $\sigma_\varphi = \varphi \circ \sigma_K \circ \varphi^{-1}$ est une involution de première espèce sur $M_n(K)$,
en outre $\varphi : (A_K, \sigma_K) \longrightarrow (M_n(K), \sigma_\varphi)$ est un isomorphisme d'algèbres à involution. On définit le type de σ comme étant le type de σ_φ.

Proposition 2.5.6 *1. σ est orthogonale si $\exists a \in (A, \sigma)_+$ tq $Trd_A(a) \neq 0$.*

2. σ est symplectique si $\forall a \in (A, \sigma)_+$ on a $Trd_A(a) = 0$.

Preuve : On a $\varphi\big((A, \sigma)_+ \otimes K\big) = \big(M_n(K), \sigma_\varphi\big)_+$. Si $\forall a \in (A, \sigma)_+$ on a $Trd_A(a) = 0$, alors soit $m \in \big(M_n(K), \sigma_\varphi\big)_+$, ainsi $m = \varphi(a \otimes 1)$ avec $a \in (A, \sigma)_+$. En conséquence,
$tr(m) = tr\big(\varphi(a \otimes 1)\big) = Trd_A(a) = 0$. Par suite σ_φ est symplectique (prop 8.0.7). ∎

Proposition 2.5.7 *Soit (A, σ) une F-algèbre centrale simple à involution σ de première espèce. Alors on a :*

1. $dim_F(A, \sigma)_+ = \frac{n(n+1)}{2}$
2. $dim_F Alt(A, \sigma) = \frac{n(n-1)}{2}$

Preuve : $dim_F(A, \sigma)_+ = dim_K\big(M_n(K), \sigma_\varphi\big)_+ = dim_K(M_n(K), t)_+ = \frac{n(n+1)}{2}$.
Soit l'endomorphisme F-linéaire $Id + \sigma : A \longrightarrow A$. Le deuxième résultat découle de :
$Im(Id + \sigma) = Alt(A, \sigma)$ et $Ker(Id + \sigma) = (A, \sigma)_-$. ∎

Lemme 2.5.8 *Soient A une F-algèbre centrale simple et σ une F/F_0-involution de deuxième espèce sur A. Alors :*

1. *Il existe $\delta \in F$ tq $\delta \notin F_0$ et $F = F_0(\delta)$ et $\alpha(\delta) = \delta + 1$ où $\alpha = \sigma/F$.*
2. *Posons $(A, \sigma)_\delta = \{x \in A / \sigma(x) = \frac{\delta+1}{\delta} x\}$. On a : $A = (A, \sigma)_+ \oplus_{F_0} (A, \sigma)_\delta$.*

Preuve :

1. Soit $\delta \in F$ tq $\delta \notin F_0$. F/F_0 étant quadratique, ainsi $F = F_0(\beta)$.
   Soit $Irr(\beta, F_0) = X^2 + aX + b$, son autre racine est $\sigma(\beta)$, il en résulte que $\sigma(\beta) = \beta + a$ donc $\sigma(a^{-1}\beta) = a^{-1}\beta + 1$ ($a \neq 0$ car $\beta \notin F_0$). Par conséquent, il suffit de prendre $\delta = a^{-1}\beta$.
2. On a : $\forall x \in A$, $x = (\delta+1)x + \delta\sigma(x) + \delta\big(x + \sigma(x)\big)$, avec $(\delta+1)x + \delta\sigma(x) \in (A,\sigma)_+$ et $\delta\big(x + \sigma(x)\big) \in (A,\sigma)_\delta$. On a aussi $x \in (A,\sigma)_+ \cap (A,\sigma)_\delta \Longleftrightarrow x = 0$. ∎

Proposition 2.5.9 *Si A est une F-algèbre centrale simple et σ une F/F_0-involution de deuxième espèce sur A, alors : $dim_{F_0}(A,\sigma)_+ = n^2$.*

Preuve : Conservons les notations du lemme précédent, et soit $\eta = \frac{(\delta+1)}{\delta}$. On a F/F_0 est une extension galoisienne de groupe de Galois $G = \{1, \sigma/F\}$, ainsi :
$N_{F/F_0}(\eta) = \sigma(\eta)\eta = \sigma\Big(\frac{\delta+1}{\delta}\Big)\frac{\delta+1}{\delta} = 1$. Donc d'après le théorème 90 de Hilbert, il existe $\theta \in F$ tq $\eta = \theta\sigma(\theta)^{-1}$. Si $\sigma(x) = x$ alors $\sigma(\sigma(\theta)x) = \theta x = \frac{\theta}{\sigma(\theta)}\sigma(\theta)x = \eta.\sigma(\theta)x$. Il en résulte que l'application $\phi : (A,\sigma)_+ \longrightarrow (A,\sigma)_\delta$ est bien définie et que c'est un isomorphisme de

$$x \longmapsto \sigma(\theta)x$$

F_0-espaces vectoriels, ainsi : $dim_{F_0}(A,\sigma)_+ = dim_{F_0}(A,\sigma)_\delta$ et $A = (A,\sigma)_+ \oplus (A,\sigma)_\delta$. ∎

Chapitre 3

Les invariants d'une algèbre centrale simple à involution

3.1 Indice de Witt d'une algèbre centrale simple à involution

Soient (E,b) un espace bilinéaire symétrique régulier et S un sous espace vectoriel de E. L'orthogonal de S est $S^{\perp} = \{x \in E/b(x,y) = 0 \ \forall y \in S\}$. S est dit totalement isotrope si $S \subset S^{\perp}$. Un sous espace totalement isotrope est dit maximal, s'il n'est pas sous espace propre d'un sous espace totalement isotrope. On montre que tous les sous espaces totalement isotropes d'un sous espace quadratique régulier (E,b) ont même dimension, appelée indice de Witt de b.

Dans ce chapitre, on va donner un analogue de l'indice de Witt d'un espace quadratique, pour une algèbre centrale simple à involution.

3.1.1 Involutions et formes hermitiennes

Soit A une F-algèbre simple centrale. D'après le théorème de Wedderburn, il existe une algèbre à division D centrale sur F et un D-espace vectoriel à droite V tel que $A = End_D(V)$ et $D = End_A(V)$. Soient $\sigma : D \longrightarrow D$ une involution sur D, et $\varepsilon = \pm 1$.
Une forme ε-hermitienne h sur V relativement à σ est une application biadditive

$h : V \times V \longrightarrow D$ vérifiant pour tout $x, y \in V$ et $\alpha, \beta \in D$:

1. $h(x\alpha, y\beta) = \sigma(\alpha)h(x, y)\beta$
2. $h(x, y) = \varepsilon\sigma\big(h(y, x)\big)$

Si $\varepsilon = 1$, on dit que h est hermitienne. Dans le cas contraire, elle est dite anti-hermitienne.
Une forme ε-hermitienne sur V relativement à σ est dite régulière ou non dégénérée si : $h(x, y) = h(y, x) = 0\ \forall y \in V \Longrightarrow x = 0$.
L'espace dual V^* a une structure naturelle de D-espace vectoriel à gauche. On définit aussi une structure de D-espace vectoriel à droite sur V^* avec l'opération : $\phi.\alpha = \sigma(\alpha)\phi$ tels que $\phi \in V^*$ et $\alpha \in D$. Alors la forme ε-hermitienne h induit une aplication D-linéaire : $\widehat{h} : V \longrightarrow V^*$ définie par : $\widehat{h}(x)(y) = h(x, y)$ pour tout $x, y \in V$. Si h est régulière, $\widehat{h}$ est une bijection.

Proposition 3.1.1 *Soit h une forme ε-hermitienne régulière sur V relativement à σ. La correspondance $\sigma_h : A \longrightarrow A$ vérifiant : $h\Big(f(x), y\Big) = h\Big(x, \sigma_h(f)(y)\Big)\ \ \forall x, y \in V,\ \forall f \in A$ est une involution sur A appelée involution adjointe de h.*

Preuve : La démonstration se fait de façon analogue à celle de du théorème 2.1.6. ∎

Remarque : On a $\sigma_h(\alpha) = \sigma(\alpha)$ si $\alpha \in F$, donc σ_h et σ sont de même espèce.

Théorème 3.1.2
1. *Si σ est de première espèce, alors l'application $h \longmapsto \sigma_h$ définit une correspondance bijective entre les formes ε-hermitiennes régulières sur V relativement à σ à un scalaire non nul près, et les involutions de première espèce sur $A = End_D(V)$.*
2. *Si σ est une F/F_0-involution de deuxième espèce sur D, alors $h \longmapsto \sigma_h$ définit une correspondance bijective entre les formes hermitiennes régulières sur V relativement à σ à un scalaire non nul près de F_0 et les F/F_0-involutions de deuxième espèce sur $A = End_D(V)$.*

Preuve :
D'après la proposition précédente, l'application $h \longmapsto \sigma_h$ est bien définie.
Si $\sigma_h = \sigma_{h'}$, alors $int(g) = Id$ avec $g = \widehat{h}^{-1} \circ \widehat{h'}$. Il s'ensuit que $g \in F^*$ et $h' = gh$.
Si σ est une F/F_0-involution de deuxième espèce et h, h' sont hermitiennes, alors l'égalité

$h' = gh$ entraîne que $\sigma(g) = g$, c-à-d $g \in F_0$.
D'où l'injectivité de la correspondance $h \longmapsto \sigma_h$ dans les deux cas 1) et 2).
Montrons maintenant que $h \longmapsto \sigma_h$ est surjective.

1. Supposons que σ est de première espèce, et soient γ une involution de première espèce sur A et $(e_i)_{1\leq i\leq m}$ une base de V. Désignons par h l'application définie sur $V \times V$ par :

$$h(x,y) = \sum_i \sigma(\alpha_i)\beta_i \ \ avec \ \ x = \sum_i e_i\alpha_i \ \ et \ \ y = \sum_i e_i\beta_i$$

Il est facile de vérifier que h est une forme hermitienne. Il résulte alors du fait que σ est de première espèce, que σ_h est de première espèce sur A. Ainsi, il existe $u \in U(A)$ telle que $\gamma = int(u) \circ \sigma_h$ et $\sigma_h(u) = \pm u$. Posons $h'(x,y) = h(x, u^{-1}.y)$. On vérifie aisément que h' est une forme ε-hermitienne sur V. Par ailleurs, $\forall x, y \in V \ \forall f \in A$

$$\begin{aligned} h'\Big(x, \sigma_{h'}(f).y\Big) = h'\Big(f(x), y\Big) &= h\Big(f(x), u^{-1}.y\Big) \\ &= h\Big(x, \sigma_h(f) \circ u^{-1}.y\Big) \\ &= h\Big(x, u^{-1} \circ \gamma(f).y\Big) \\ &= h'\Big(x, \gamma(f).y\Big) \end{aligned}$$

Par conséquent, $\sigma_{h'} = \gamma$.

2. Supposons que σ est une F/F_0-involution de deuxième espèce et soit γ une F/F_0-involution de deuxième espèce sur A. On fait le même raisonnement que 1), seulement on aura dans ce cas, $\sigma_h(u) = u$, ce qui entraîne que h' est hermitienne. ∎

Soient D une algèbre à division centrale sur F et θ une involution sur D. Soit V un D-espace vetoriel à droite de dimension finie. On définit un D-espace vetoriel à gauche ${}^{\theta}V$ par :

$${}^{\theta}V = \{{}^{\theta}v / v \in V\} \ ; \ {}^{\theta}v +^{\theta} w = {}^{\theta}(v+w) \ ; \ \alpha.{}^{\theta}v = {}^{\theta}\big(v.\theta(\alpha)\big)$$

pour $v, w \in V$ et $\alpha \in D$. On peut alors considérer le produit tensoriel $V \otimes_D {}^{\theta}V$ comme un F-espace vectoriel de dimension finie qui est égale à $(dim_F V)^2 dim_F D$.
Soit $h : V \times V \longrightarrow D$ une forme ε-hermitienne non singulière sur V relativement à θ. Notons par φ_h l'application F-linéaire : $\varphi_h : V \otimes_D {}^{\theta}V \longrightarrow End_D(V)$

$$v \otimes {}^{\theta}w \longmapsto \varphi_h(v \otimes {}^{\theta}w) : x \longmapsto v.h(w,x)$$

Théorème 3.1.3 *L'application φ_h est bijective. Si σ_h est l'involution adjointe à h sur $End_D(V)$, alors pour tout $v, w \in V$: $\sigma_h\big(\varphi_h(v \otimes {}^{\theta}w)\big) = \varepsilon\varphi_h(w \otimes {}^{\theta}v)$. De plus :*

1. $Trd_{End_D(V)}\big(\varphi_h(v \otimes {}^{\theta}w)\big) = Trd_D\big(h(w,v)\big)$.
2. $\forall v_1, v_2, w_1, w_2 \in V$, $\varphi_h(v_1 \otimes {}^{\theta}w_1) \circ \varphi_h(v_2 \otimes {}^{\theta}w_2) = \varphi_h\big(v_1 h(w_1, v_2) \otimes {}^{\theta}w_2\big)$.

Preuve : Voir ([6, Theorem 5.1, page 54]) ∎

Conclusion : Si on munit $V \otimes_D {}^{\theta}V$ du produit : $(v_1 \otimes {}^{\theta}w_1) \circ (v_2 \otimes {}^{\theta}w_2) = v_1 h(w_1, v_2) \otimes {}^{\theta}w_2$ et de l'involution σ définie pour tout $v, w \in V$ par : $\sigma(v \otimes {}^{\theta}w) = \varepsilon w \otimes {}^{\theta}v$, alors on a l'identification suivante dite standard :

$$\varphi_h : (V \otimes_D {}^{\theta}V, \sigma) \cong (End_D(V), \sigma_h) \tag{3.1}$$

Notamment, si $D = F$ et de plus $\theta = Id_F$, alors ${}^{\theta}V = V$. En conséquence, l'identification standard associée à une forme bilinéaire non singulière symétrique ou anti-symétrique b sur V est $\varphi_b : (V \otimes_F V, \sigma) \longrightarrow (End_F(V), \sigma_b)$, avec $\varphi_b(v \otimes w)(x) = vb(w, x)$ et $\sigma(v \otimes w) = w \otimes v$ si b est symétrique et $\sigma(v \otimes w) = -w \otimes v$ si b est anti-symétrique.

3.1.2 Idéaux d'une algèbre centrale simple

Soient A une F-algèbre simple centrale et M un A-module. La dimension réduite (ou rang) de M est par définition :

$$rang M = \frac{dim_F M}{deg A}$$

D'après le théorème de Wedderburn, il existe une algèbre à division D centrale sur F et un D-espace vectoriel à droite V tel que $A = End_D(V)$ et $D = End_A(V)$. Soit $S \subset V$ un sous espace de V. La composition d'une application linéaire $f \in \mathrm{Hom}_D(V, S)$ avec l'inclusion $S \hookrightarrow V$ nous permet d'identifier $\mathrm{Hom}_D(V, S)$ à un sous espace de $A = End_D(V)$:

$$\mathrm{Hom}_D(V, S) = \{f \in End_D(V)/\mathrm{Im} f \subset S\}.$$

Cet espace est clairement un idéal à droite de A de rang :

$$rang \mathrm{Hom}_D(V, S) = dim_D S.deg D = dim_D S.ind A.$$

Similairement, la composition d'une application linéaire $f \in \mathrm{Hom}_D(V/S, V)$ avec l'application canonique $V \longrightarrow V/S$ permet d'identifier $\mathrm{Hom}_D(V/S, V)$ à un sous espace de

$A = End_D(V)$: $\mathrm{Hom}_D(V/S, V) = \{f \in End_D(V)/\mathrm{Ker}f \supset S\}$. Cet espace est un idéal à gauche de A du rang : $rang\mathrm{Hom}_D(V/S, V) = dim_D(V/S).degD = degA - indA.dim_D S$.

Proposition 3.1.4 *L'application* $S \longmapsto \mathrm{Hom}_D(V, S)$ *définit une correspondance bijective entre les sous espaces de dimension m de V et les idéaux à droite de* $A = End_D(V)$ *de rang : m.indA. Similairement, l'application* $S \longmapsto \mathrm{Hom}_D(V/S, V)$ *définit une correspondance bijective entre les sous espaces de dimension m de V et les idéaux à gauche de* $A = End_D(V)$ *de rang : degA-m.indA.*

Preuve : Voir ([6, proposition 1.12, page 7]). ∎

3.1.3 Indice de Witt d'une algèbre centrale simple à involution

Soit $A = End_D(V)$ une F-algèbre simple centrale avec D une algèbre à division centrale sur F et V un D-espace vectoriel à droite de dimension finie. Soient $\sigma : D \longrightarrow D$ une involution sur D et h une forme hermitienne régulière sur V relativement à σ adjointe d'une involution σ_h. Soit I un idéal à droite de A. Il existe alors un sous espace S de V tel que $I = \mathrm{Hom}_D(V, S)$.

Lemme 3.1.5 *On a :* $\mathrm{Hom}_D(V, S) \oplus \mathrm{Hom}_D(V, S^\perp) = A = End_D(V)$
avec $S^\perp = \{x \in V/h(x, y) = h(y, x) = 0\ , \forall y \in S\}$.

Preuve : Voir [10]. ∎

Lemme 3.1.6 $\mathrm{Hom}_D(V, S^\perp) = \{x \in A/\sigma_h(f).x = 0\ \forall f \in I\}$

Preuve : Soit $g \in \mathrm{Hom}_D(V, S^\perp)$, donc $\forall f \in I = \mathrm{Hom}_D(V, S)\ , \forall x, y \in V$
on a : $h\big(f(x), g(y)\big) = 0 = h\big(x, \sigma_h(f).g(y)\big)$ car $g(y) \in S^\perp$ et $f(x) \in S$. Or h est hermitienne, alors $h\big(\sigma_h(f).g(y), x\big) = 0\ \forall x \in V$ et du fait que h est régulière, on conclut que :
$\sigma_h(f).g = 0\ \forall f \in I$. Réciproquement, soit $g' \in \{x \in A/\sigma_h(f).x = 0\ \ \forall f \in I\}$, et soit $f \in I$ tel que $f(V) = S$. Ainsi $\forall x, y \in V\ h\big(x, \sigma_h(f).g'(y)\big) = 0 = h\big(f(x), g'(y)\big) = h\big(g'(y), f(x)\big)$.
Or, f(V)=S, donc $\forall y \in V$, $g'(y) \in S^\perp$, c-à-d, $g' \in \mathrm{Hom}_D(V, S^\perp)$. ∎

Définition 3.1.7 *1. Le sous espace* $\mathrm{Hom}_D(V, S^\perp)$ *est appelé orthogonal de* $I = \mathrm{Hom}_D(V, S)$ *relativement à* σ_h*, et on écrit* $I^\perp = \mathrm{Hom}_D(V, S^\perp)$.

2. *I est dit totalement isotrope si* $I \subset I^{\perp}$.
3. *Supposons I totalement isotrope. I est dit maximal s'il n'est pas strictement inclu dans un idéal totalement isotrope.*

Remarque : S est totalement isotrope dans l'espace hermitien (V,h) si et seulement si I est totalement isotrope dans l'algèbre à involution (A, σ_h).
Autrement dit : $S \subset S^{\perp} \Longleftrightarrow I \subset I^{\perp} \Longleftrightarrow \sigma_h(f).g = 0 \ \forall f, g \in I$.

Lemme 3.1.8 *Soient I et J deux idéaux à droite de* (A, σ_h). *On a :*
1) $I \subset J \Longrightarrow J^{\perp} \subset I^{\perp}$ 2) $(I+J)^{\perp} = I^{\perp} \cap J^{\perp}$
3) $rangI + rangI^{\perp} = degA$ 4) $(I \cap J)^{\perp} = I^{\perp} + J^{\perp}$
5) $I \subset J \Longrightarrow rangI \leq rangJ$ 6) $rang(I+J) = rangI + rangJ - rang(I \cap J)$

Preuve : Voir [10]. ∎

Lemme 3.1.9 *Soient I et J deux idéaux à droite de* (A, σ_h) *avec J totalement isotrope et* $rangI < rangJ$, *alors* $rang(I \cap J) < rang(I^{\perp} \cap J)$.

Preuve :
J étant totalement isotrope donc $J \subset J^{\perp}$, ainsi $I^{\perp} + J \subset I^{\perp} + J^{\perp} = (I \cap J)^{\perp}$, en conséquence, $rang(I^{\perp} + J) \leq rang(I \cap J)^{\perp}$. On en déduit, en utilisant 5) que :
$0 < rangJ - rangI \leq rang(I^{\perp} \cap J) - rang(I \cap J)$. Ainsi, le lemme est prouvé. ∎

Proposition 3.1.10 *Tous les idéaux à droite de* (A, σ_h) *totalement isotropes maximaux ont le même rang.*

Preuve : Soient I et J deux idéaux à droite de (A, σ_h) totalement isotropes maximaux. Supposons que $rangI < rangJ$. On a : $I^{\perp} \cap J \nsubseteq I$, car si non on aura : $I^{\perp} \cap J \subset I \cap J \subset I^{\perp} \cap J$. En conséquence $I^{\perp} \cap J = I \cap J$, ce qui contredit le lemme précédent. Par suite, $I^{\perp} \cap J \nsubseteq I$, ainsi il existe $f_0 \in I^{\perp} \cap J$ et $f_0 \notin I$. Posons $X = I + (I^{\perp} \cap J)$. On a :
$X^{\perp} = \big(I + (I^{\perp} \cap J)\big)^{\perp} = I^{\perp} \cap (I^{\perp} \cap J)^{\perp} = I^{\perp} \cap (I^{\perp\perp} + J^{\perp}) = I^{\perp} \cap (I + J^{\perp})$ Par ailleurs, $I \subset I^{\perp}$ et $I^{\perp} \cap J \subset I^{\perp}$, ainsi $X = I + (I^{\perp} \cap J) \subset I^{\perp}$. De même on a : $I \subset I + J^{\perp}$ et $I^{\perp} \cap J \subset J \subset J^{\perp} \subset I + J^{\perp}$, donc $X = I + (I^{\perp} \cap J) \subset I + J^{\perp}$. Il s'ensuit que $X \subset X^{\perp}$.

C'est-à-dire X est totalement isotrope et $I \subsetneq X$ (car $f_0 \in X$ et $f_0 \notin I$). Ce qui contredit la maximalité de I, donc $rangI \not< rangJ$ et de la même façon on montre que $rangJ \not< rangI$, par conséquent $rangI = rangJ$. ∎

Définition 3.1.11 *La valeur commune du rang de tous les idéaux à droite de (A, σ_h) totalement isotropes maximaux, est appelé indice de Witt de l'algèbre centrale simple à involution (A, σ_h).*

3.2 Discriminant d'une involution

3.2.1 Discriminant d'une involution orthogonale

Proposition 3.2.1 *Soit A une F-algèbre centrale simple à involution σ symplectique. Le polynôme caractéristique réduit de chaque élément de $(A, \sigma)_+$ est un carré dans F[X]. En particulier, $Nrd_A(s)$ est un carré dans F quel que soit $s \in (A, \sigma)_+$.*

Preuve : Voir ([6, proposition 2.9, page 19]). ∎

Si A est une F-algèbre centrale simple de degré pair à involution σ de première espèce, alors $\exists a \in A^\times$ tel que $\sigma(a) = \pm a$ (voir [6, corollary 2.8, page 18]).

Proposition 3.2.2 *Soit A une F-algèbre centrale simple de degré pair à involution σ orthogonale. Alors $\forall a, b \in A^\times \cap (A, \sigma)_-$ on a : $Nrd_A(a) \equiv Nrd_A(b)$ mod $F^{\times 2}$.*

Preuve : Si $a, b \in A^\times \cap (A, \sigma)_-$, alors $\sigma(a) = -a$, ainsi l'involution $\sigma' = int(a) \circ \sigma$ est symplectique et $ab \in (A, \sigma')_+$. Or la proposition précédente montre que $Nrd_A(ab) \in F^{\times 2}$, d'où le résultat. ∎

Définition 3.2.3 *Soit A une F-algèbre centrale simple de degré pair à involution σ orthogonale. Le discriminant de σ est par définition : $disc\, \sigma = Nrd_A(a) \in F^\times / F^{\times 2}$ tel que $a \in A^\times \cap (A, \sigma)_-$.*

Remarque : On définit aussi le discriminant d'une involution σ symplectique comme étant la classe carrée : $disc\, \sigma = Nrd_A(a) \in F^\times / F^{\times 2}$ tel que $a \in A^\times \cap (A, \sigma)_+$ (voir [2]).

Exemple : Soit l'algèbre à involution $(M_n(F), t)$ telle que n est pair et t l'involution transposition (orthogonale). Soit la matrice :

$$M = \begin{pmatrix} m_1 & & 0 \\ & \ddots & \\ 0 & & m_{n/2} \end{pmatrix} \text{ telle que } m_1 = \cdots = m_{n/2} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

M est un élément inversible de $(M_n(F), t)_-$ (car $detM = 1$).
Ainsi, $disc\, t = Nrd_{M_n(F)}(M) = detM = 1$.

Proposition 3.2.4 *Soit A une F-algèbre centrale simple de degré pair.*

1. *Supposons que σ est une involution orthogonale sur A, et soit $u \in A^\times$.*
   Si $int(u) \circ \sigma$ est orthogonale, alors $disc(int(u) \circ \sigma) = Nrd_A(u).disc\, \sigma$.
2. *Supposons que σ est une involution symplectique sur A, et soit $u \in A^\times$.*
   Si $int(u) \circ \sigma$ est une involution orthogonale sur A alors : $disc(int(u) \circ \sigma) = Nrd_A(u)$.
3. *Si $A = End_F(V)$ et σ_b est l'involution adjointe à une forme bilinéaire non singulière symétrique b sur V, alors $disc\, \sigma_b = detb$.*
4. *Supposons que σ est une involution orthogonale sur A. Si (B, τ) est une F-algèbre centrale simple à involution orthogonale, alors*

$$disc(\sigma \otimes \tau) = \begin{cases} disc\, \sigma & si\ degB\ est\ impair \\ 1 & si\ degB\ est\ pair \end{cases}$$

5. *Supposons que σ est une involution symplectique sur A. Si (B, τ) est une F-algèbre centrale simple à involution symplectique, alors $disc(\sigma \otimes \tau) = 1$.*

Preuve :

1. Si $int(u) \circ \sigma$ est orthogonale, alors : $\sigma(u) = u$ et $\big(A, int(u) \circ \sigma\big)_- = u.(A, \sigma)_-$.
   Soit $b \in \big(A, int(u) \circ \sigma\big)_-$, c'est-à-dire $b = u.a$ tel que $a \in (A, \sigma)_-$.
   Il s'ensuit que $disc(int(u) \circ \sigma) = Nrd_A(b) = Nrd_A(ua) = Nrd_A(u).Nrd_A(a).F^{\times 2}$.
2. On a σ est symplectique et $int(u) \circ \sigma$ est orthogonale, ainsi $\sigma(u) = -u$,
   d'où $u \in \big(A, int(u) \circ \sigma\big)_-$, en conséquence $disc(int(u) \circ \sigma) = Nrd_A(u)$.

3. On peut identifier A avec $M_n(F)$ pour un choix d'une base e de V. Soit $g \in Gl_n(F)$ la matrice de la forme bilinéaire b dans la base e. On a : $\sigma_b = int(g^{-1}) \circ t$, avec t l'involution transposition. Or, t est orthogonale et $\sigma_b = int(g^{-1}) \circ t$ l'est aussi, car b est symétrique. Ainsi, en appliquant (1), on trouve : $disc\ \sigma_b = Nrd_A(g^{-1}).disc\ t = detb$.

4. Si $a \in (A, \sigma)_- \cap A^\times$, alors $a \otimes 1 \in (A \otimes B, \sigma \otimes \tau)_-$. Le résultat est déduit de l'égalité $Nrd_{A\otimes B}(a \otimes 1) = Nrd_A(a)^{degB}$.

5. τ est symplectique, donc le degré de B est pair. Soit $a \in (A, \sigma)_- \cap A^\times$ donc $a \otimes 1$ est un élément inversible de $(A \otimes B, \sigma \otimes \tau)_-$.
   Ainsi $disc(\sigma \otimes \tau) = Nrd_{A\otimes B}(a \otimes 1) = Nrd_A(a)^{degB} = 1$. ∎

Exemples :

1. $A = (M_n(F), t)$, n pair. Si $\sigma = int(u) \circ t$ est une involution orthogonale sur A, alors d'après (2), $disc\ \sigma = Nrd_A(u).disc\ t = det(u)$.

2. Si $A = A_1 \otimes A_2$ avec A_1 et A_2 sont de degré pair et $\sigma = \sigma_1 \otimes \sigma_2$ une involution orthogonale sur A, c'est-à-dire σ_1 et σ_2 sont de même type, alors d'après (4) et (5) de la proposition précédente on a $disc\ \sigma = 1$. En particulier, le résultat est vrai si A_1 et A_2 sont des algèbres de quaternions et σ_1 et σ_2 leurs conjugaisons (symplectiques).

3.2.2 Application : Algèbre à involution décomposable

D'après le théorème du double centralisateur, si une F-algèbre centrale simple A contient une sous-algèbre A_1, centrale simple sur F et non triviale (i.e. distincte de F et de A), alors elle se décompose en un produit tensoriel $A = A_1 \otimes A_2$, où A_2 est le centralisateur de A_1 dans A . On dit alors que l'algèbre A est décomposable.

Par exemple, Albert a montré que toute algèbre centrale simple sur F de degré 4 et d'exposant 2, est décomposable, c'est-à-dire isomorphe à un produit tensoriel de deux algèbres de quaternions (Voir [6, Theorem16.1, page 233]).

Définition 3.2.5 *Soit A une F-algèbre centrale simple munie d'une involution σ. On dit que l'algèbre à involution (A, σ) est décomposable si A contient une sous-algèbre centrale*

simple non triviale A_1 stable par σ. Quand c'est le cas, le centralisateur A_2 de A_1 dans A est stable par σ et on a $A = A_1 \otimes A_2$ et $\sigma = \sigma_1 \otimes \sigma_2$, où σ_i désigne la restriction de σ à A_i.

L'étude de la décomposabilité d'une algèbre à involution est une question classique (voir par exemple [1]). L'exemple (2) précédent montre qu'avoir un discriminant trivial est une condition nécessaire de décomposition stable. Le théorème suivant montre que la réciproque est également vraie en degré 4.

Théorème 3.2.6 *Soit A une F-algèbre centrale simple de degré 4 ayant une involution orthogonale σ. Alors A admet une sous algèbre de quaternions stable par σ si et seulement si le discriminant de σ est trivial.*

Preuve : Voir [7, Theorem 3.1]. ∎

Remarques :

1. Pour les algèbres de degré 8, cette condition n'est plus suffisante. En effet Amisteur, Rowen et Tignol (voir [1]) ont construit une algèbre à division D de degré 8 à involution qui ne se décompose pas en produit tensoriel d'algèbres de quaternions. Ainsi toute involution symplectique sur D est de discriminant trivial mais ne peut pas se décomposer.
2. Hélène Dherte [2] a montré que même pour les algèbres décomposables de degré 8, la condition "avoir un discriminant trivial" ne suffit pas pour qu'il existe une sous algèbre stable.

3.3 Algèbre de Clifford d'une involution

3.3.1 Algèbre de Clifford d'un espace quadratique

Soient V un espace vectoriel sur F et q une forme quadratique sur V. Posons

$$T^n(V) = \begin{cases} V \otimes_F V \otimes_F \cdots \otimes_F V \ (nfois) & \text{si } n > 0 \\ F & \text{si } n = 0 \end{cases}$$

L'algèbre tensoriel de V est l'algèbre $T(V) = \bigoplus_{n\geq 0} T^n(V)$ telle que le produit est défini par : $(v_1 \otimes v_2 \otimes \cdots \otimes v_r) \times (v_{r+1} \otimes \cdots \otimes v_s) = v_1 \otimes \cdots \otimes v_r \otimes v_{r+1} \cdots \otimes v_s$, est prolongé par linéarité à $T(V)$. Désignons par $I(q)$ l'idéal bilatère de $T(V)$ engendré par les éléments $x \otimes x - q(x).1$ avec $x \in V$ et 1 l'élément unité de $T(V)$, alors l'algèbre de Clifford de (V, q) est :

$$C(V, q) = \frac{T(V)}{I(q)}$$

L'algèbre $T(V) = T_0(V) \oplus T_1(V) = T(V \otimes V) \oplus (V \otimes T(V \otimes V))$ est graduée de type $\mathbb{Z}/2\mathbb{Z}$. Du fait que les générateurs de $I(q)$ sont dans $T_0(V)$, cette graduation induit une graduation de $C(V, q) : C(V, q) = C_0(V, q) \oplus C_1(V, q)$ tel que $C_0(V, q)$ est le sous espace de $C(V, q)$ engendré par les produits d'un nombre pair de vecteurs de V, appelé l'algèbre de Clifford paire de (V, q). De même $C_1(V, q)$ est le sous espace de $C(V, q)$ engendré par les produits d'un nombre impair de vecteurs de V, et appelé l'algèbre de Clifford impaire de (V, q). On a (voir Knus [5, chapter 4, corollary 7]) : $dim_F C(V, q) = 2^{dim_F V}$ et $dim_F C_0(V, q) = dim_F C_1(V, q) = 2^{dim_F V - 1}$.
On a aussi le résultat suivant (voir [6, lemma 8.1, page 87]) : $C_0(V, q) = \frac{T(V \otimes V)}{I_0(q)}$. Avec $I_0(q)$ l'idéal de $T(V \otimes V)$ engendré par les éléments $x \otimes x - q(x)$ et $x \otimes y \otimes y \otimes z - q(y)x \otimes z$ pour $x, y, z \in V$.

Exemples :

1. Si $V = F$ et q la forme quadratique définie par $q(x) = \alpha x^2$, avec $\alpha \in F$ et $\alpha \neq 0$, alors $C(F, \alpha x^2) = F[X]/(X^2 - \alpha) \cong F \oplus Fx$ avec $x^2 = \alpha$.
   En particulier, si $F = \mathbb{R}$ et $\alpha = -1$, alors on a : $C(\mathbb{R}, -x^2) = \mathbb{R}[X]/(X^2 + 1) \cong \mathbb{C}$.
2. Si $q = 0$ alors $C(V, 0) = \frac{T(V)}{<x \otimes x / x \in V>}$ est appelée algèbre extérieure.

Le théorème suivant montre que les structures de $C(V, q)$ et $C_0(V, q)$ sont déteminées complètement en fonction de q.

Théorème 3.3.1 *Soit (V, q) un espace quadratique régulier, on a :*

1. *Si $dim_F V = n = 2m$, alors le centre Δ de $C_0(V, q)$ est une F-algèbre quadratique étale isomorphe à $F[X]/(X^2 - \delta)$, où δ est tel que $disc(q) = (-1)^m \delta . F^{\times 2}$. De plus on a :*
   - *Si Δ est un corps (i.e $disc(q) \neq 1$), alors $C_0(V, q)$ est une Δ- algèbre centrale simple de degré 2^{m-1}.*

– *Si* $\Delta \cong F \times F$ *(i.e* $disc(q) = 1$*), alors* $C_0(V,q)$ *est un produit direct de deux* F*-algèbres centrales simples de degré* 2^{m-1}*.*

2. *Si* $n = 2m+1$*, alors* $C_0(V,q)$ *est une* F*-algèbre centrale simple de degré* 2^m*.*

Preuve : Voir ([13, Theorem 2.10, page 332]). ∎

$C(V,q)$ et $C_0(V,q)$ sont munies d'une involution "canonique" τ qui est l'involution induite par l'identité sur V : $\tau(\overline{x_1 \otimes \cdots \otimes x_k}) = \overline{x_k \otimes \cdots \otimes x_1}$.
Le type de $\tau/C_0(V,q) = \tau_0$ est determiné par la dimension de V comme suit :

Proposition 3.3.2 1. *Si* $dimV \equiv 2 \pmod 4$*, alors* τ_0 *est de deuxième espèce.*

2. *Si* $dimV \equiv 0 \pmod 4$*, alors* τ_0 *est de première espèce. En particulier,* τ_0 *est orthogonale si* $dimV \equiv 0 \pmod 8$*, et symplectique si* $dimV \equiv 4 \pmod 8$*.*

3. *Si* $dimV \equiv 1, 7 \pmod 8$*, alors* τ_0 *est orthogonale.*

4. *Si* $dimV \equiv 3, 5 \pmod 8$*, alors* τ_0 *est symplectique.*

Preuve : Voir ([6, proposition 8.4, page 89]). ∎

3.3.2 Algèbre de Clifford d'une involution orthogonale

Soit (A,σ) une F-algèbre centrale simple à involution orthogonale. Notons par $T(A)$ l'algèbre tensorielle de A (considérée comme F-espace vectoriel), et soient l'application bilinéaire :

$$\begin{aligned} Sand: \quad A \otimes A \times A &\longrightarrow A \\ (a \otimes b, c) &\longmapsto acb \end{aligned}$$

et $I(\sigma)$ l'idéal de $T(A)$ engendré par les éléments de la forme

$$s - trd(s) \; avec \; s \in A \; tq \; \sigma(s) = s.$$
$$x - Sand(x,1) \;\; tq \; x \in A \otimes A \;\; et \;\; Sand\big(x, (A,\sigma)_-\big) = 0.$$

Définition 3.3.3 *L'algèbre de Clifford de* (A,σ) *est* $C^T(A,\sigma) = \frac{T(A)}{I(\sigma)}$*. Cette définition est appelée définition rationnelle d'après Tits.*

Proposition 3.3.4 *Si $A = End_F(V)$ et σ l'involution adjointe d'une forme bilinéaire symétrique b, alors $C(A,\sigma) = C_0(V,b)$. De plus si K/F est une extension, alors $C_0^T(A,\sigma) \otimes K \cong C_0^T(A \otimes K, \sigma \otimes Id)$.*

Preuve : Voir ([2, proposition, page 35]). ∎

Théorème 3.3.5 *Soient A une F-algèbre centrale simple de degré $n = 2m$ à involution σ orthogonale et Z le centre de $C(A,\sigma)$, alors Z est une F-algèbre quadratique étale isomorphe à $F[X]/(X^2 - \delta(\sigma))$ où $disc\,\sigma = (-1)^m\delta(\sigma).F^{\times 2}$. D'où Z est un corps ou $Z \simeq F \times F$.*

1. *Si Z est un corps (i.e $disc(\sigma) \neq 1$), alors $C(A,\sigma)$ est une Z-algèbre centrale simple de degré 2^{m-1}.*
2. *Si $Z \simeq F \times F$ (i.e $disc(\sigma) \neq 1$), alors $C(A,\sigma)$ est un produit direct de deux F-algèbres centrales simples de degré 2^{m-1}.*

Preuve : Voir ([11, Théorème 1.9, page 34]). ∎

Proposition 3.3.6 *Soit (A,σ) une F-algèbre centrale simple à involution orthogonale, alors σ induit une involution $T(\sigma) : T(A) \longrightarrow T(A)$ telle que $T(\sigma)(a_1 \otimes \cdots \otimes a_k) = \sigma(a_k) \otimes \cdots \otimes \sigma(a_1)$ et laissant stable $I(\sigma)$.*

Preuve :

1. Si $s \in A/\sigma(s) = s$, On a :

$$T(\sigma)\big(s - trd(s)\big) = T(\sigma)(s) - T(\sigma)\big(trd(s)\big) = \sigma(s) - \sigma\big(trd(s)\big) = s - trd(s)$$

2. Soit $x = \sum_i a_i \otimes b_i \in A \otimes A$ tel que pour tout $c \in (A,\sigma)_-$, $Sand(x,c) = \sum_i a_i c b_i = 0$. On a pour tout $c \in (A,\sigma)_-$,

$$\begin{aligned} Sand\big(T(\sigma)(x), c\big) &= Sand\big(\sum_i \sigma(b_i) \otimes \sigma(a_i), c\big) = \sum_i Sand\big(\sigma(b_i) \otimes \sigma(a_i), c\big) \\ &= \sum_i \sigma(b_i) c \sigma(a_i) = -\sum_i \sigma(b_i)\sigma(c)\sigma(a_i) = -\sigma\big(Sand(x,c)\big) = 0 \end{aligned}$$

En conséquence, $Sand\big(T(\sigma)(x),(A,\sigma)_-\big)=0$. Par ailleurs,

$$\begin{aligned}T(\sigma)\big(x-Sand(x,1)\big)&=T(\sigma)(x)-T(\sigma)\big(Sand(x,1)\big)\\&=T(\sigma)(x)-T(\sigma)\big(\sum_i Sand(a_i\otimes b_i,1)\big)\\&=T(\sigma)(x)-T(\sigma)\big(\sum_i a_i.1.b_i\big)\\&=T(\sigma)(x)-\sum_i\sigma(b_i)\sigma(a_i)\\&=T(\sigma)(x)-Sand\big(T(\sigma)(x),1\big)\end{aligned}$$

Par suite, 1) et 2) montrent bien que $I(\sigma)$ est stable par $T(\sigma)$. ∎

Conclusion : L'involution $T(\sigma)$ induit une involution σ^* sur $C(A,\sigma)=\frac{T(A)}{I(\sigma)}$.

Proposition 3.3.7 *Soit A une F-algèbre centrale simple de degré $n=2m$ à involution σ orthogonale. Alors :*

- *Si m est pair, on a σ^* est une involution de première espèce sur $C(A,\sigma)$. σ^* est orthogonale si $m\equiv 0\ mod\ 4$ et symplectique si $m\equiv 2\ mod\ 4$.*
- *σ^* est une involution de deuxième espèce sur $C(A,\sigma)$ si m est impair.*

En particulier, si $A=End_F(V)$ et σ est l'involution adjointe d'une forme quadratique q, alors $C(A,\sigma)=C_0(V,q)$ et σ^* est l'involution canonique de $C_0(V,q)$.

Preuve : Voir ([6, proposition 8.12, page 95]). ∎

3.3.3 Application : caractérisation des involutions conjuguées

Dans ce paragraphe on utilise l'algèbre de Clifford comme un outil permettant de caractériser les involutions conjuguées.

Définition 3.3.8 *Soit A une F-algèbre. Deux involutions σ et σ' sur A sont conjuguées s'il existe $a\in A^\times$ tel que $\sigma'=Int(a)\circ\sigma\circ Int(a)^{-1}$.*

Remarque : Deux involutions σ et σ' sur A sont conjuguées si et seulement si les algèbres (A,σ) et (A,σ') sont F-isomorphes.

Théorème 3.3.9 *Soit A une F-algèbre centrale simple de degré ≤ 4. Alors deux involutions orthogonales σ et σ' sur A sont conjuguées si et seulement si leurs algèbres de Clifford sont F-isomorphes.*

Preuve : Voir ([8, page 262]). ∎

Définition 3.3.10 *On dit qu'un corps commutatif F est formellement réel (ou simplement réel) si -1 n'est pas une somme de carrés dans F.*

Remarque :

1. Un corps fini n'est pas formellement réel, donc tout corps formellement réel est necéssairement de caractéristique 0.
2. Posons $\square F = \{x \in F/$ x est une somme de carrés dans $F\}$ et $\square F^* = \square F - \{0\}$.
   Alors F est formellement réel est équivalent à $\square F \neq F$.

Soient $W(F)$ l'anneau de Witt de F et $I(F)$ l'idéal fondamental de Witt (pour les définitions, voir [13, Definition 1.9, page 33]).
Notation : $I^3F = I(F)^3$.

Théorème 3.3.11 *Soit F un corps non formelement réel et $I^3F = 0$. Alors, deux involutions orthogonales σ et σ' sur une F-algèbre centrale simple A sont conjuguées si et seulement si leurs algèbres de Clifford sont F-isomorphes.*

Preuve : Voir ([8, page 264]). ∎

3.4 Signature d'une involution

3.4.1 La forme trace d'une involution

Lemme 3.4.1 *Soit (A, σ) une F-algèbre centrale simple à involution σ de première espèce. Alors pour tout $a \in A$ on a : $Nrd_A(\sigma(a)) = Nrd_A(a)$ et $Trd_A(\sigma(a)) = Trd_A(a)$.*

Preuve : Soit K un corps neutralisant de A, ainsi il existe un isomorphisme
$\varphi : A_K = A \otimes_F K, \longrightarrow M_n(K)$. On a : $\varphi \circ \sigma_K \circ \varphi^{-1}$ est une involution de première espèce

sur $M_n(K)$, donc il existe une matrice inversible g de $M_n(K)$ telle que $g^t = \pm g$ et
$\varphi \circ \sigma_K \circ \varphi^{-1} = \sigma_g = int(g) \circ t$.

$$\begin{aligned} Prd_A\big(\sigma(a)\big) &= det\Big(XI_n - \varphi\big(\sigma(a) \otimes 1\big)\Big) = det\big(XI_n - \varphi \circ \sigma_K(a \otimes 1)\big) \\ &= det\big(XI_n - \sigma_g \circ \sigma(a \otimes 1)\big) = det\big(XI_n - g.\varphi(a \otimes 1)^t.g^{-1}\big) \\ &= det\Big(g.\big(XI_n - \varphi(a \otimes 1)^t\big).g^{-1}\Big) = det\big(XI_n - \varphi(a \otimes 1)\big) \\ &= Prd_A(a). \end{aligned}$$

∎

Définition 3.4.2 *Soit A une F-algèbre centrale simple à involution σ de première espèce. L'application $T_\sigma : A \times A \longrightarrow F$ est une forme bilinéaire non singulière sur A,*

$$(x, y) \longmapsto Trd_A\big(\sigma(x)y\big)$$

appelée forme trace de (A, σ).

D'après le lemme précédent, on a pour tout $(x, y) \in A \times A$:
$T_\sigma(x, y) = Trd_A\big(\sigma(x)y\big) = Trd_A\Big(\sigma\big(\sigma(y)x\big)\Big) = Trd_A\big(\sigma(y)x\big) = T_\sigma(y, x)$. Ainsi T_σ est une forme bilinéaire symétrique.

Proposition 3.4.3 *Sous l'isomorphisme $\sigma_* : A \otimes_F A \longrightarrow End_F(A)$*

$$a \otimes b \longmapsto \sigma_*(a \otimes b) : x \longmapsto ax\sigma(b)$$

l'involution $\sigma \otimes \sigma$ correspond à l'involution adjointe de T_σ.

Preuve : $\forall a, b, x, y \in A$, $T_\sigma\big(\sigma_*(a \otimes b)(x), y\big) = Trd_A\big(b\sigma(x)\sigma(a)y\big)$. Par ailleurs,
$T_\sigma\Big(x, \sigma_*\big(\sigma(a) \otimes \sigma(b)\big)(y)\Big) = T_\sigma\big(x, \sigma(a)yb\big) = Trd_A\big(\sigma(x)\sigma(a)yb\big)$.

∎

Lemme 3.4.4 *Si $(A, \sigma) = (End_F(V), \sigma_b)$, alors l'identification standard $\varphi_b : V \otimes_F V \longrightarrow A$ de (3.1) induit l'isométrie d'espaces bilinéaires $\varphi_b : (V \otimes_F V, b \otimes b) \longrightarrow (End_F(V), T_\sigma)$.*

Preuve : En utilisant le théorème 3.1.3 on a $\forall x_1, x_2, y_1, y_2 \in V$:

$$\begin{aligned} T_\sigma\big(\varphi_b(x_1 \otimes x_2), \varphi_b(y_1 \otimes y_2)\big) &= Trd_A\Big(\sigma\big(\varphi_b(x_1 \otimes x_2)\big)\varphi_b(y_1 \otimes y_2)\Big) \\ &= Trd_A\big(\varepsilon\varphi_b(x_2 \otimes x_1)\varphi_b(y_1 \otimes y_2)\big) \\ &= Trd_F\big(\varepsilon b(x_1, x_2)b(y_2, y_1)\big) \\ &= \varepsilon^2 b(x_1, x_2)b(y_1, y_2) \\ &= b(x_1, x_2)b(y_1, y_2) \\ &= (b \otimes b)(x_1 \otimes x_2, y_1 \otimes y_2). \end{aligned}$$

∎

3.4.2 La signature d'une involution de première espèce

Définition 3.4.5 *Soit F un corps formellement réel. Nous disons qu'une partie $P \subset F$ est un préordre de F si P vérifie : $P + P \subset P$, $P.P \subset P$, $-1 \notin P$ et $\square F \subset F$.*
Un préordre P de F sera dit un ordre de F si de plus : $P \cup -P = F$ et $P \cap -P = \{0\}$. Dans ce cas on dit que F est ordonné.

Si F est un corps formellement réel, alors F est ordonné (voir [13, Theorem 7.1, page 54]).

Remarques :

1. Si P est un ordre sur F, les éléments de P^* sont dits positifs et les éléments de $-P^*$ sont dits négatifs.
2. Si $x \in F^*$ alors $x \in P$ ou $-x \in P$, or $x^2 = (-x)^2 \in P$, donc $F^{*2} \subset P$.
3. La relation $>$ définie sur F par : $x > y$ si $x - y \in P$ est une relation d'ordre totale.

Soit A une F-algèbre centrale simple à involution σ de première espèce.
Supposons que F est ordonné par un ordre P.
Rappelons qu' à toute forme bilinéaire symétrique non singulière b est associé un entier $sgn_P b$ appelé signature de b sur P, défini par : $sgn_P b = m^+ - m^-$ avec m^+ (resp.m^-) est le nombre des entrées positives (resp.négatives) dans une diagonalisation de b.

Proposition 3.4.6 *1. Si* $(A,\sigma)=(End_F(V),\sigma_b)$*, alors*

$$sgn_P T_\sigma = \begin{cases} (sgn_P b)^2 & si\ \sigma\ est\ orthogonale \\ 0 & si\ \sigma\ est\ symplectique \end{cases}$$

2. Si A est quelconque, la signature de la forme bilinéaire T_σ *sur P est un carré dans* $\mathbb{Z}$*.*

Preuve : Voir ([6, proposition 11.7, page 136]). ∎

Définition 3.4.7 *La signature sur P d'une involution* σ *de première espèce sur A est par définition :* $sgn_P\sigma=\sqrt{sgn_P T_\sigma}$*.*

Il découle de la dernière proposition que $sgn_P\sigma$ est un entier. Par ailleurs, on sait que $sgn_P T_\sigma \leq dimA$ et $sgn_P T_\sigma \equiv dimT_\sigma\ mod 2$. Ainsi, $0\leq sgn_P\sigma\leq degA$ et
$sgn_P\sigma \equiv degA\ mod\ 2$.

Définition 3.4.8 *Un corps formellement réel F est dit réel fermé si F n'a pas d'extension algébrique propre formellement réelle. Une extension algébrique K de F est dite clôture réelle de F si K est réel fermé.*

Théorème 3.4.9 *Soit* F_P *la clôture réelle de F pour un ordre P.*

1. *Supposons que A n'est pas neutralisée par* F_P*. Donc* $sgn_P\sigma=0$ *si* σ *est orthogonale et* $sgn_P\sigma=degA\ mod\ 4$ *si* σ *est symplectique.*
2. *Supposons que A est neutralisée par* F_P*. Alors* $sgn_P\sigma=0$ *si* σ *est symplectique. Si* σ *est orthogonale et* $\sigma_b=\sigma\otimes Id_{F_P}$ *est l'involution adjointe d'une forme bilinéaire symétrique b sur* F_P^n*, alors* $sgn_P\sigma=|sgn_P b|$*.*

Preuve : Voir ([9, Theorem 1]). ∎

3.4.3 Application : Involutions indécomposables

Lemme 3.4.10 *Soit A une F-algèbre centrale simple.*
Si $A=A_1\otimes A_2$ *et* $\sigma=\sigma_1\otimes\sigma_2$*, alors* $T_\sigma=T_{\sigma_1}\otimes T_{\sigma_2}$*.*

Preuve : Pour $x_1, y_1 \in A_1$ et $x_2, y_2 \in A_2$, on a :
$T_\sigma(x_1 \otimes x_2, y_1 \otimes y_2) = Trd_A\big(\sigma_1(x_1)y_1 \otimes \sigma_2(x_2)y_2\big) = Trd_{A_1}\big(\sigma_1(x_1)y_1\big)\ Trd_{A_2}\big(\sigma_2(x_2)y_2\big)$. ∎

Proposition 3.4.11 *Soient A une algèbre centrale simple sur un corps formellemnet réel F et P un ordre sur F. Si $A = A_1 \otimes A_2$ et $\sigma = \sigma_1 \otimes \sigma_2$, alors $sgn_P(\sigma) = sgn_P(\sigma_1)\ sgn_P(\sigma_2)$.*

Preuve : Déduction simple du lemme précédent et de la définition 3.4.7. ∎

Corollaire 3.4.12 *Soit A une algèbre centrale simple de degré une puissance de deux sur un corps formellemnet réel F, et soit P un ordre sur F. Alors toute involution de première espèce sur A telle que $sgn_P(\sigma) = 2$ est indécomposable.*

Preuve : Supposons que $\sigma = \sigma_1 \otimes \sigma_2$. D'après la proposition précédente, on a
$2 = sgn_P(\sigma_1)sgn_P(\sigma_2)$. Ainsi $sgn_P(\sigma_1) = 1$ ou $sgn_P(\sigma_2) = 1$. Or, on sait que la signature d'une involution sur une algèbre centrale simple de degré pair est divisible par 2. Donc notre supposition est impossible, en conséquence σ est indécomposable. ∎

La notion de signature peut fournir plus d'informations que le discriminant. En effet, elle peut être non triviale pour des involutions symplectiques et peut être utilisée pour exclure certains types de décompositions.

Supposons pour l'instant que : $A = Q_1 \otimes_F Q_2 \otimes_F Q_3$ est un produit tensoriel d'algèbres de quaternions sur un corps formellement réel F et que σ (resp. τ) est une involution de première espèce sur Q_1 (resp. $Q_2 \otimes_F Q_3$) telles que $sgn_P(\sigma) = sgn_P(\tau) = 2$ pour un certain ordre P de F, alors τ est indécomposable par le corollaire 3.4.12.
L'involution $\rho = \sigma \otimes \tau$ vérifie $disc(\rho) = 1$ (car ρ est décomposable) et $sgn_P(\rho) = 4$, par suite il n'existe pas d'algèbres de quaternions Q'_1, Q'_2 et Q'_3 invariants par ρ telles que
$A = Q'_1 \otimes_F Q'_2 \otimes_F Q'_3$, car sinon $sgn_P(\rho) = \prod_{i=1}^{3} sgn_P(\rho/Q'_i)$ =0 ou 8, absurde.

Bibliographie

[1] S. Amitsur, L. Rowen J.-P. Tignol : Division algebras of degree 4 and 8 with involution, Israel J. Math. 33 (1979), p. 133-148.

[2] H.Dherte : Invariants d'algèbres centrales simples à involution , Dissertation doctorale (UCL),91-92.

[3] P. K. Draxl : Skew fields, London Mathematical Society Lectur e Note Series, vol. 81, Cambridge University Press, Cambridge, 1983.

[4] I.Kaplansky. Linear Algebra and Geometry. Allyn and Bacon Inc., Boston (1969).

[5] M.A. Knus, Quadratic Forms, Clifford Algebras and Spinors, Univ. Estadual de Campinas (UNICAMP), Campinas (1988).

[6] M.-A. Knus, A.S. Merkurjev, M. Rost, J.-P. Tignol : The book of involutions, Coll. Pub. 44. Providence, RI : Amer. Math. Soc. (1998).

[7] Knus, M,A., Parimala, R., Sridharan, R. : Involutions on rank 16 central simple algebras, J. Indian Math. Soc., to appear.

[8] D.W. Lewis, J.-P. Tignol, Classification theorems for central simple algebras with involution, Manuscripta Math. 100, (1999), pp. 259-276.

[9] D.W. Lewis and J.-P. Tignol, On the signature of an involution, Archiv der Mathematik 60 (1993), 128-35.

[10] Lubikulu Punama, Indice de Witt d'une algèbre simple centrale à involution. Thèse annexe dirigée par J.P.Tignol. Louvain-la-Neuve (1992).

[11] L. Oukhtite : Algèbres centrales simples à involution, Université Sidi Mohamed Ben Abdellah, FST, Fès-Saïs , Mémoire de C.E.A 1995.

[12] R.S. Pierce, Associative algebras, Graduate Texts in Mathematics 88, Springer-Verlag, New York, 1982.

[13] W. Scharlau, Quadratic and Hermitian Forms, Grundlehren der Mathematischen Wissenschaften, vol. 270, Springer-Verlag, Berlin, 1985.

[14] J.P.Tignol, Central simple algebras, involutions and quadratic forms. Lectures at the National Taiwan university, April 1993.