Algèbres simples centrales à involution de première espèce

Karim Johannes Becher

Fachbereich Mathematik und Statistik, D204, Universität Konstanz, D-78457 Konstanz, Allemagne. E-mail: becher@maths.ucd.ie

Summary

This article provides new and elementary proofs for some of the crucial theorems in the theory of central simple algebras with involution of the first kind.

In the first place Albert's criterion for the existence of an involution of the first kind and Kneser's extension theorem for such involutions are presented in a unified way. These two results are retrieved as corollaries of a new theorem which gives a criterion to decide whether an antiautomorphism of a central simple algebra is an involution of the first kind. Two examples are given to indicate that the analogous approach cannot be applied to involutions of the second kind.

Quaternion algebras give the easiest nontrivial examples of central simple algebras which carry an involution of the first kind. Albert has shown that any central simple algebra of dimension 16 with involution of the first kind is a tensor product of two quaternion algebras. This theorem is presented here with a new proof essentially using basic linear algebra.

1 Introduction

Le présent travail a pour but de fournir des preuves nouvelles et élémentaires de quelques résultats clés en théorie des algèbres simples centrales à involution. Il vise à permettre au lecteur familier des notions de base sur les algèbres simples centrales et sur les involutions (rappelées en Section 2) d'aborder directement la question de la structure des algèbres admettant une involution de première espèce.

On traite en premier lieu le critère d'existence d'involutions de première espèce, dû à A. A. Albert ainsi qu'un théorème d'extension d'une involution de M. Kneser, ici pour une involution de première espèce. Ces deux résultats

sont obtenus comme corollaires du théorème 1 qui donne un critère simple pour qu'un anti-automorphisme d'une algèbre simple centrale soit une involution. Deux exemples indiquent que cette approche ne s'applique pas aux involutions de deuxième espèce.

On démontre ensuite, à partir des propriétés usuelles des algèbres de quaternions, deux résultats, dûs à Albert et à J.-P. Tignol et L. H. Rowen, sur la structure des algèbres simples centrales à involution de première espece et de degré 4.

2 Préliminaires

Dans toute la suite, F désigne un corps et A une F-algèbre simple centrale. L'algèbre opposée de A est notée A^{op}. Si B est une sous-F-algèbre de A, on note $C_A(B)$ le centralisateur de B dans A.

Si A' est une autre F-algèbre simple centrale alors on écrit $A \sim A'$ lorsque A et A' sont *(Brauer-)équivalentes.* L'ensemble des classes d'équivalence pour cette relation est muni d'une structure de groupe abélien, avec la loi induite par le produit tensoriel de F-algèbres. Ce groupe s'appelle le *groupe de Brauer de* F et on le note $\mathrm{Br}(F)$. La loi de $\mathrm{Br}(F)$ sera notée additivement. La classe de A dans $\mathrm{Br}(F)$ est notée $[A]$ et son ordre est appelé *exposant de* A. On note $\mathrm{Br}_2(F)$ la 2-torsion de $\mathrm{Br}(F)$, i.e. le sous-groupe des éléments d'ordre 1 ou 2 de $\mathrm{Br}(F)$. Par abus de notation, on écrira parfois $A \sim 0$ pour signifier que $[A] = 0$ dans $\mathrm{Br}(F)$, ce qui revient à dire que A est déployée (en une algèbre de matrices sur F).

Soit K/F une extension de corps. Par extension des scalaires on obtient à partir de A la K-algèbre simple centrale $A_K = A \otimes_F K$. Si K/F est contenue dans A alors $C_A(K)$ est une K-algèbre simple centrale, Brauer-équivalente à A_K [13, Theorem 8.5.4.].

Rappelons que pour tout $u \in A^\times$, l'application qui à $x \in A$ associe uxu^{-1} est un automorphisme de A dit *automorphisme intérieur* et noté $\mathrm{Int}(u)$. Pour que deux éléments de $A^\times$ définissent le même automorphisme intérieur de A il faut et il suffit qu'ils soient proportionnels sur F.

Soit α un anti-automorphisme d'anneau de A. Il est facile de vérifier que α stabilise le centre F de A. Soit k le sous-corps de F fixé par α. Si $k = F$ (resp. $k \neq F$), on dit aussi que α est un *F-anti-automorphisme* (resp. un *F/k-anti-automorphisme*) de l'algèbre A. Si de plus $\alpha^2 = \mathrm{id}_A$ on dit que α est une F-involution (resp. F/k-involution) ou *involution de première espèce* (resp. *de deuxième espèce*) de A. Il est clair que pour une F/k-involution, l'extension F/k est séparable de degré 2.

Dans cet article, nous utiliserons essentiellement les deux théorèmes sui-

vants que le lecteur peut trouver dans les ouvrages de référence sur la théorie des algèbres simples centrales comme [4, § 10, n^o 1, 2], [9, § 12.6-12.7], [3, Chap. III, § 1] et [13, Chap. 8, § 4] :

2.1 Théorème du double centralisateur. *Soient B une sous-F-algèbre simple de A et B' le centralisateur de B dans A. Alors :*

(1) *B' est une F-algèbre simple.*

(2) *On a $[B : F] \cdot [B' : F] = [A : F]$.*

(3) *B est le centralisateur de B' dans A.*

2.2 Théorème de Skolem–Noether. *Soit B une F-algèbre simple et soient $\sigma, \tau : B \to A$ deux homomorphismes de F-algèbres. Alors il existe $u \in A^\times$ tel que $\tau = \mathrm{Int}(u) \circ \sigma$. En particulier, tout automorphisme de A est intérieur.*

Pour les anti-automorphismes on déduit du dernier résultat :

2.3 Lemme. *Soit α un F-anti-automorphisme de A.*

(*a*) *Pour tout $u \in A^\times$ on a l'égalité $\alpha \circ \mathrm{Int}(u) \circ \alpha^{-1} = \mathrm{Int}(\alpha(u^{-1}))$.*

(*b*) *Tout anti-automorphisme d'anneau d'une sous-F-algèbre simple de A qui fixe les éléments de F s'étend en un F-anti-automorphisme de A de la forme $\mathrm{Int}(u) \circ \alpha$, avec $u \in A^\times$.*

Démonstration : (*a*) Pour $u \in A^\times$ et $x \in A$, on calcule $[\mathrm{Int}(\alpha(u^{-1}))](x) = \alpha(u^{-1})\ \alpha(\alpha^{-1}(x))\ \alpha(u) = \alpha\,(u\,\alpha^{-1}(x)\,u^{-1}) = [\alpha \circ \mathrm{Int}(u) \circ \alpha^{-1}](x)$.
(*b*) Soit B une sous-F-algèbre simple de A et β un anti-automorphisme de B qui fixe les éléments de F. Alors $\alpha \circ \beta^{-1}$ est un homomorphisme de F-algèbres de B dans A. Le théorème de Skolem-Noether appliqué à $\alpha \circ \beta^{-1}$ et à l'inclusion de B dans A, implique que β s'étend à A en $\mathrm{Int}(u) \circ \alpha$, avec $u \in A^\times$. □

De [6, §2.C], nous rappelons les conventions et faits suivants sur les algèbres de quaternions. Quelle que soit la caractéristique de F, on appelle *F-algèbre de quaternions* toute F-algèbre simple centrale de degré 2.

Soient $a, b \in F^\times$. Si F est de caractéristique différente de 2, on note $(a, b)_F$ la F-algèbre de base $(1, i, j, k)$ telle que $i^2 = a, j^2 = b$ et $k = ij = -ji$. Si la caractéristique de F est égale à 2, on note $[a, b)_F$ la F-algèbre de base $(1, i, j, k)$ telle que $i^2 + i = a, j^2 = b$ et $k = ij = ji + j$. Il s'avère que toute

F-algèbre de quaternions admet une telle base et donc est de la forme décrite ci-dessus [4, §11, Proposition 1 et Exercice 4].

Dans la preuve du Théorème 4.3, nous utiliserons les règles de calcul usuelles du symbole quaternionien. Énoncer ces règles revient à dire, en caractéristique différente de deux, que l'application $F^\times/F^{\times 2} \times F^\times/F^{\times 2} \longrightarrow \mathrm{Br}(F)$ qui au couple $(aF^{\times 2}, bF^{\times 2})$ associe la classe de Brauer de l'algèbre de quaternions $(a,b)_F$, est bilinéaire et symétrique, et en caractéristique égale à deux, que l'application $F \times F^\times/F^{\times 2} \longrightarrow \mathrm{Br}(F)$ (où la première composante est le groupe additif de F) qui au couple $(a, bF^{\times 2})$ associe la classe de $[a,b)_F$ est bilinéaire. Notons encore qu'en caractéristique différente de deux on a $(a,b)_F \cong (a+b, -ab)_F$ pour tout $a, b \in F^\times$ tels que $a+b \neq 0$, et qu'en caractéristique deux la F-algèbre de quaternions $[a,a)_F$ est déployée pour tout $a \in F^\times$.

Toute algèbre de quaternions admet une involution de première espèce. En effet, si Q est une F-algèbre de quaternions et si l'on note Trd_Q la forme trace réduite de Q sur F, alors l'application $x \longmapsto (\mathrm{Trd}_Q(x) - x)$ de Q dans elle-même est une F-involution appelée *involution canonique de Q*.

Rappelons aussi que le corps F est dit *non réel* si -1 est une somme de carrés dans F et *réel* sinon. Si F est réel alors on sait que F est de caractéristique 0 et que la F-algèbre de quaternions $(-1,-1)_F$ est à division. On dit que F est *réellement clos* si F est réel et si toute extension algébrique non triviale de F est non réelle. Dans ce cas, $(-1,-1)_F$ est la seule F-algèbre centrale à division non-commutative. Pour le cas typique du corps des nombres réels, cette observation remonte à Frobenius.

2.4 Lemme. *On suppose qu'il existe $d \in F^\times \setminus F^{\times 2}$ tel que $d \in K^{\times 2}$ pour toute extension finie non triviale K/F. Alors, ou bien F est réellement clos et $(-1,-1)_F$ est la seule F-algèbre centrale à division non triviale, ou bien F est non réel et toute F-algèbre simple centrale est déployée.*

Démonstration : Il suffit d'examiner le cas où il existe une F-algèbre à division non triviale D. Montrons alors que F est réellement clos et que D est isomorphe à $(-1,-1)_F$.

On sait que D contient une extension L de F non triviale et séparable [4, § 10, n^o 3, Lemme 1]. Par hypothèse, l'extension $F(\sqrt{d})/F$ se plonge sur une sous-extension K/F de L/F. En particulier, $F(\sqrt{d})/F$ est séparable et ainsi F est de caractéristique différente de 2. En vertu du théorème de Skolem-Noether, l'automorphisme non trivial de K/F s'étend en un automorphisme de D de la forme $\mathrm{Int}(u)$ avec $u \in D^\times$. Alors u ne commute pas avec K. Cependant, u^2 commute avec K puisque $\mathrm{Int}(u^2)|_K = \mathrm{id}_K$. De plus, K ne peut être contenu dans $F(u^2)$ (qui commute avec u). Le fait que les racines carrées de d dans le corps $K(u^2)$ appartiennent déjà à K entraîne que d

n'est pas un carré dans $F(u^2)$. L'hypothèse faite sur F et d permet alors de conclure que $u^2 \in F$.

Il s'ensuit que K et u engendrent dans D une F-algèbre de quaternions à division Q. Comme $F(\sqrt{d})$ est par hypothèse la seule extension quadratique de F, il vient $Q \cong (d,d)_F \cong (-1,d)_F$. On voit alors que l'unique extension quadratique de F est $F(\sqrt{-1})$ et que $Q \cong (-1,-1)_F$. Ainsi, les seules classes de carrés de F sont $F^{\times 2}$ et $-F^{\times 2}$ et l'algèbre de quaternions $(-1,-1)_F$ est à division. On en déduit que -1 ne peut pas s'écrire comme une somme de 2 carrés dans F, et ensuite, que toute somme de carrés est égale à un carré dans F. Ceci montre que F est un corps réel. De plus, comme l'élément -1 devient un carré dans toute extension finie non triviale de F, le corps F est réellement clos.

Soit M un sous-corps (commutatif) maximal de $C_D(Q)$. Alors $M \otimes_F K$ est un sous-corps maximal de D. Comme $\sqrt{d} \in K \setminus F$, il s'ensuit que $\sqrt{d} \notin M$. Par l'hypothèse faite sur d, on en déduit que $M = F$. Il vient $C_D(Q) = F$. Ainsi, $D = Q \cong (-1,-1)_F$. □

3 Involutions de première espèce

L'exemple le plus simple de F-involution est la transposition pour une algèbre de matrices à coefficients dans F. Toute F-algèbre simple centrale qui représente la classe triviale dans $\mathrm{Br}(F)$ admet donc une F-involution. Un autre exemple de F-involution est l'involution canonique d'une F-algèbre de quaternions.

Notre but principal est de démontrer le théorème d'Albert qui affirme que l'existence d'une involution de première espèce sur A est équivalente à ce que A soit d'exposant au plus 2 (3.4). La preuve qu'on va donner s'inspire partiellement de la démarche suivie dans [13, Chap. 8, §8] et [12]. Dans [12], la proposition suivante, attribuée à Albert, est obtenue comme conséquence du théorème d'Albert. Ici on en donne une preuve directe.

3.1 Proposition. *Soit α un F-anti-automorphisme de A. Alors il existe $a \in A^\times$, unique au signe près, tel que $\alpha^2 = \mathrm{Int}(a)$ et $\alpha(a) = a^{-1}$. Pour que α soit une F-involution il faut et il suffit que $a = \pm 1$.*

Démonstration : Nous nous restreignons à montrer l'existence de a, le reste de l'énoncé étant facile à vérifier.

Supposons d'abord que A est une algèbre de matrices sur F et notons t la transposition. La partie (b) du lemme (2.3) implique $\alpha = \mathrm{Int}(u) \circ t$

avec $u \in A^\times$. Ceci nous donne $\alpha^2 = \mathrm{Int}(u) \circ (t \circ \mathrm{Int}(u) \circ t) = \mathrm{Int}(u\,u^{-t})$. Posons $a = u\,u^{-t}$. Comme $\alpha(u^t) = u$ on a bien $a\,\alpha(a) = u\,u^{-t}\,\alpha(u^{-t})\,\alpha(u) = (u\,u^{-t}\,u^{-1})\,\alpha(u) = \alpha(u^{-1})\alpha(u) = 1$.

Dans le cas général, le théorème de Skolem-Noether permet de choisir $c \in A^\times$ tel que $\alpha^2 = \mathrm{Int}(c)$. Le calcul $\mathrm{Int}(c) = \alpha^2 = \alpha \circ \mathrm{Int}(c) \circ \alpha^{-1} = \mathrm{Int}(\alpha(c^{-1}))$ montre que $c\,\alpha(c) \in F^\times$. S'il existe $r \in F^\times$ tel que $c\,\alpha(c) = r^2$ alors l'élément $a = rc^{-1}$ vérifiera les égalités souhaitées.

Pour montrer $c\alpha(c) \in F^{\times 2}$, considérons une extension K/F telle que A_K est déployée. Notons α_K le K-anti-automorphisme de A_K obtenu par extension des scalaires à partir de α. D'après la première partie de la preuve, il existe un élément $a_K \in A_K^\times$ tel que $(\alpha_K)^2 = \mathrm{Int}(a_K)$ et $\alpha_K(a_K) = a_K^{-1}$. Comme les éléments c et a_K définissent sur A_K le même automorphisme intérieur, il vient $c \in K^\times a_K$; on en déduit que $c\alpha(c)$ est un carré dans K.

Or, pour tout élément $d \in F^\times \setminus F^{\times 2}$, on peut trouver une extension K/F qui déploie A et telle que d n'est pas un carré dans K. En effet, si l'on prend pour K le corps des fonctions de la variété de Severi-Brauer de A, alors A_K est déployée et F est algébriquement clos dans K. De façon plus élémentaire, on se place sur un corps non reel F' qui contient F et tel que d n'est pas un carré dans F' (e.g. $F' = F$ si F est non reel et $F' = F(X)(\sqrt{-1 - X^2})$ si F est réel) ; parmi les extensions algébriques de K/F' telles que d n'est pas un carré dans K, on en choisit une qui est maximale ; ainsi $\mathrm{Br}(K)$ est trivial, d'après (2.4). □

Remarque : Dans [5], à chaque F-anti-automorphisme α est associé de manière intrinsèque un élément appelé *asymétrie de* α. C'est l'un des deux éléments $\pm a$ exhibés dans la proposition. Dans le cas où α est une involution et F de caractéristique différente de 2, le signe de $a = \pm 1$ donne alors le *type* d'involution de α (*orthogonale* ou *symplectique*).

3.2 Théorème. *Soient K un sous-corps de A contenant F, B le centralisateur de K dans A et α un F-anti-automorphisme de A qui fixe les éléments de K. Pour que α soit une F-involution de A, il faut et il suffit que $\alpha|_B$ soit une K-involution de B.*

Démonstration : D'après le théorème du double-centralisateur, B est une K-algèbre simple centrale. Comme α fixe les éléments de K il stabilise B et sa restriction à B est un K-anti-automorphisme de B.

Si α est involutif alors il en est de même de $\alpha|_B$. Réciproquement, supposons que $\alpha|_B$ est une K-involution. D'après la proposition (3.1), on peut choisir $a \in A^\times$ tel que $\alpha^2 = \mathrm{Int}(a)$ et $\alpha(a) = a^{-1}$. Puisque $\alpha|_B$ est une involution, $\mathrm{Int}(a)|_B = \mathrm{id}_B$, d'où $a \in C_A(B) = K$. Il vient alors $a = \alpha(a) = a^{-1}$, puis $a = \pm 1$ car K est un corps. Ainsi α est une involution. □

Avant d'appliquer ce théorème à nos propos, convainquons-nous que l'hypothèse que α est une K-involution (et non pas seulement une involution qui stabilise K) est essentielle.

3.3 Exemple. Soient K/F une extension quadratique séparable contenue dans une F-algèbre de quaternions Q et τ l'involution canonique de Q. K est égal à son centralisateur dans Q. Choisissons $u \in K$ tel que $u^2 \notin F$ et posons $\alpha = \mathrm{Int}(u) \circ \tau$. Alors α est un F-anti-automorphisme de Q et sa restriction à K est une K/F-involution, à savoir l'automorphisme non trivial de K/F. Comme $\tau(u)u \in F^\times$, il vient $\alpha^2 = \mathrm{Int}(u\tau(u^{-1})) = \mathrm{Int}(u^2) \neq \mathrm{id}_Q$. Ainsi, α n'est pas une involution.

3.4 Corollaire (Albert). *Pour que A admette une F-involution il faut et il suffit que A soit d'exposant 1 ou 2.*

Démonstration : Une F-involution de A est en particulier un isomorphisme de F-algèbres de A sur A^{op}. La condition est donc nécessaire.

Supposons maintenant que A est d'exposant au plus 2 et montrons qu'elle admet une F-involution. A se décompose en produit tensoriel $D \otimes E$ d'une sous-F-algèbre à division D et d'une sous-F-algèbre déployée E. Soit K un sous-corps maximal de D. Ainsi K est son propre centralisateur dans D. Comme D est équivalente à A et est ainsi d'exposant 1 ou 2, il existe un isomorphisme de F-algèbres de D sur D^{op}, i.e. un F-anti-automorphisme de D. D'après le lemme (2.3), l'identité de K se prolonge en un F-anti-automorphisme α de D. Comme la restriction de α à K est la K-involution identité, le théorème (3.2) assure que α est une F-involution de D. E étant isomorphe à une algèbre de matrices sur F, elle admet une F-involution τ. Alors $\alpha \otimes \tau$ est une F-involution de A. □

3.5 Corollaire (Kneser). *On suppose que A est d'exposant 1 ou 2. Soit B une sous-F-algèbre simple de A. On note K le centre de B. Alors toute K-involution de B se prolonge en une F-involution de A.*

Démonstration : Supposons que β est une K-involution de B. En particulier, B est d'exposant au plus 2. Si l'on note C le centralisateur de B dans A, le théorème du centralisateur dit que C est simple de centre K et que $C_A(K) = B \otimes_K C$. Avec $[C_A(K)] = [A_K] \in \mathrm{Br}_2(K)$ [13, 8.5.4. Theorem] ceci implique que $[C] = [C_A(K)] - [B] = [A_K] - [B] \in \mathrm{Br}_2(K)$. Par suite, d'après (3.4), il existe une K-involution γ sur C. Alors $\beta \otimes \gamma$ est une K-involution de $C_A(K)$ et, en vertu de (2.3), s'étend en un F-anti-automorphisme α de A. Le théorème (3.2) assure alors que α est une F-involution, et elle prolonge β. □

Le corollaire (3.4) indique que l'existence d'un F-anti-automorphisme et celle d'une F-involution sur A sont des propriétés équivalentes. L'exemple suivant montre que l'énoncé analogue pour des K/F-anti-automorphismes et K/F-involutions, où K/F est une extension quadratique, n'est pas valable en général.

3.6 Exemple. On suppose que F est de caractéristique différente de 2, que le degré et l'exposant de A sont égaux à 4 et que K est une extension quadratique de F contenue dans A. Le centralisateur C de K dans A est une K-algèbre de quaternions à division. On note $\mathrm{res}_{K/F}$ (resp. $\mathrm{cor}_{K/F}$) l'homomorphisme de restriction $\mathrm{Br}(F) \to \mathrm{Br}(K)$ (resp. de corestriction $\mathrm{Br}(K) \to \mathrm{Br}(F)$) associé à l'extension K/F. Leur composition $\mathrm{cor}_{K/F} \circ \mathrm{res}_{K/F}$ est égale à la multiplication par 2 dans $\mathrm{Br}(F)$ [6, 3.13 Proposition (5)]. On calcule

$$\mathrm{cor}_{K/F}[C] = \mathrm{cor}_{K/F} \circ \mathrm{res}_{K/F}[A] = 2 \cdot [A] \neq 0$$

dans $\mathrm{Br}(F)$. Donc C n'admet aucune F-involution [13, 8.9.5 Theorem]. De l'égalité précédente on déduit $\mathrm{res}_{K/F} \circ \mathrm{cor}_{K/F}[C] = 2 \cdot [A_K] = 2 \cdot [C] = 0$ dans $\mathrm{Br}(K)$. Il s'ensuit que C admet quand même un K/F-anti-automorphisme [13, 8.9.2. Lemma].

4 Algèbres de biquaternions

[1] Une F-algèbre qui se décompose en un produit tensoriel de deux F-algèbres de quaternions est appelée une *F-algèbre de biquaternions.* En particulier, une F-algèbre de biquaternions est une F-algèbre simple centrale de degré 4 et d'exposant 1 ou 2. Albert a prouvé que la réciproque est également vraie. Il existe déjà plusieurs démonstrations de ce résultat (cf. [6, §16]). Nous en donnons une nouvelle qui, à l'instar de celle de Racine [10], utilise un argument standard de comparaison de dimensions de sous-F-espaces de A.

4.1 Théorème (Albert). *On suppose que A est de degré 4 et d'exposant 1 ou 2. Soit K une extension quadratique séparable de F contenue dans A. Alors il existe deux F-algèbres de quaternions Q_1 et Q_2 contenues dans A telles que $A = Q_1 \otimes_F Q_2$ et telles que K est un sous-corps maximal de Q_1.*

Démonstration : Si la F-algèbre A n'est pas à division alors elle est isomorphe à une algèbre de matrices $\mathcal{M}_2(B)$ sur une F-algèbre de quaternions

[1] Dans cette partie, l'adaptation des démonstrations au cas général incluant le cas de caractéristique 2 a été réalisée avec le soutien très aimable de Jean-Pierre Tignol.

B, donc aussi à $\mathcal{M}_2(F) \otimes_F B$; comme $\mathcal{M}_2(F)$, la F-algèbre de quaternions déployée, contient une image homomorphe de K, l'isomorphisme de F-algèbres $A \longrightarrow \mathcal{M}_2(F) \otimes_F B$ peut, en vertu du Théorème de Skolem–Noether, être choisi de sorte que l'image de K par cet isomorphisme soit contenue dans le facteur $\mathcal{M}_2(F)$. On prend alors pour Q_1 et Q_2 les images réciproques des deux facteurs $\mathcal{M}_2(F)$ et B par cet isomorphisme.

On suppose dorénavant que A est à division. On considère $C = C_A(K)$, le centralisateur de K dans A, qui est une K-algèbre de quaternions. D'après (3.5), l'involution canonique de C s'étend en une F-involution σ sur A. En tant que F-espace vectoriel A est de dimension 16, et l'on sait que l'un de ses deux sous-F-espaces $\mathrm{Sym}(\sigma) = \{x \in A \mid \sigma(x) = x\}$ et $\mathrm{Skew}(\sigma) = \{x \in A \mid \sigma(x) = -x\}$ est de dimension 10 [13, 8.7.5. Theorem].

Pour $v \in A^\times$, le sous-F-espace $C\,v$, isomorphe à C, est de dimension 8 et contient donc un élément non nul x tel que $\sigma(x) = \pm x$.

Le théorème de Skolem-Noether permet d'étendre l'automorphisme non trivial de K/F en un automorphisme $\mathrm{Int}(u)$ de A avec $u \in A^\times$. On peut toujours multiplier u par un facteur non nul dans $C = C_A(K)$ sans changer la restriction de $\mathrm{Int}(u)$ à K. Le sous-F-espace $C\,u$ est de dimension 8 et il a donc une intersection non nulle avec $\mathrm{Sym}(\sigma)$ ou avec $\mathrm{Skew}(\sigma)$. On peut alors choisir u de telle sorte que, en plus, on a $\sigma(u) = \pm u$. Il vient alors $\sigma(u^2) = u^2 \in C$.

On choisit un élement $c \in C^\times$ de trace réduite sur K égale à 1 (si F est de caractéristique différente de 2 on peut prendre $c = \frac{1}{2}$). Comme $\sigma|_C$ est l'involution canonique sur C, il s'ensuit que $1 = \mathrm{Trd}_C(c) = c + \sigma(c)$. comme $\mathrm{Int}(ucu)$ est l'identité sur K, on a $ucu \in C$ et ainsi $u^2 = u(c + \sigma(c))u = ucu + \sigma(ucu) = \mathrm{Trd}_C(ucu) \in K$.

Finalement, K ne peut pas être égal à $F(u^2)$, puisque $\mathrm{Int}(u)$ n'est pas l'identité sur K. Donc $u^2 \in F$ et ainsi u et K engendrent une F-algèbre de quaternions Q_1 dans A, dans laquelle K est un sous-corps maximal. On pose alors $Q_2 = C_A(Q_1)$ et on a $A = Q_1 \otimes_F Q_2$. □

4.2 Corollaire (Albert). *Toute algèbre simple centrale de degré* 4 *et d'exposant* 1 *ou* 2 *est une algèbre de biquaternions.*

Démonstration : Soit A une F-algèbre simple centrale de degré 4 et d'exposant 1 ou 2. D'après (3.4), A admet une F-involution σ. Si A n'est pas à division alors on voit comme au début de la preuve du théorème (4.1) que A se décompose en produit de deux F-algèbres de quaternions dont l'une est déployée. On peut alors supposer A à division. Tout revient alors, en vertu du théorème (4.1), à mettre en évidence l'existence d'une extension quadratique séparable K de F contenue dans A.

Considérons d'abord le cas où la caractéristique de F est différente de 2. On choisit un élément $x \in A^\times$ tel que $\sigma(x) = -x$. Les éléments de $F(x^2)$ étant fixés par σ, il vient $x \notin F(x^2)$. Comme le degré de l'extension $F(x)/F$, qui est contenue dans A, ne peut excéder 4, ou bien $F(x)$ ou bien $F(x^2)$ est une extension quadratique de F, contenue dans A. Comme F est supposé de caractéristique différente de 2, toute extension quadratique de F est séparable.

Pour le reste, on suppose que la caractéristique de F est égale à 2. On choisit un élément $u \in A$ tel que $\sigma(u) \neq u$ et on considère la F-involution $\tau = \mathrm{Int}(u + \sigma(u)) \circ \sigma$. On pose $y = u(u + \sigma(u))^{-1}$ et on calcule $1 = y + \tau(y)$. Comme τ fixe $y^2 + y$ mais pas y, le corps $F(y)$, qui est contenu dans A, est une extension stricte de $F(y^2 + y)$. En particulier, on a $y^2 \notin F$. Le degré de l'extension $F(y)$ de F divise le degré de la F-algèbre A, qui est 4. Par conséquent, ou bien y^2+y appartient à F, ou bien $F(y^2+y)$ est une extension quadratique de F. Dans le premier cas, $F(y)$ est une extension quadratique séparable de F. Dans le deuxième cas, soit l'extension quadratique $F(y^2+y)$ de F est elle-même séparable, soit elle est inséparable, d'où $y^4+y^2 = (y^2+y)^2 \in F$, et alors $F(y^2)$ est une extension quadratique séparable de F. □

Remarque : Soit A une F-algèbre centrale à division et d'exposant 2. Le degré de A est alors égal à 2^n pour un certain entier $n \geq 1$. Si $n = 1$, on sait que A est une algèbre de quaternions. Si $n = 2$, le dernier résultat assure que A se décompose en produit tensoriel sur F de deux F-algèbres de quaternions. Pour $n > 2$, Tignol a montré que A n'est pas nécessairement isomorphe à un produit tensoriel de F-algèbres de quaternions. (cf. [2]) Cependant, il a été démontré par Merkurjev, que A est toujours Brauer équivalente à un tel produit. (cf. [8]).

Le résultat suivant a d'abord été obtenu en caractéristique différente de 2 par J.-P. Tignol [14, 2.8 Corollaire] (voir aussi [7, Proposition 5.2]), puis a été établi par L. H. Rowen en caractéristique 2 [11, Corollary 5]. Nous en donnons ici une preuve nouvelle valable dans les deux cas.

4.3 Théorème (Tignol, Rowen). *On suppose que A est d'exposant 1 ou 2. Soient K_1 et K_2 deux extensions quadratiques séparables de F. Pour que A soit déployée par K_1K_2 il faut et il suffit que A soit équivalente à un produit $Q_1 \otimes_F Q_2$ où Q_i est une F-algèbre de quaternions contenant K_i $(i = 1, 2)$.*

Démonstration : Supposons que Q_1 et Q_2 sont deux F-algèbres de quaternions telles que K_i est contenu dans Q_i $(i = 1, 2)$. Alors Q_i est déployée par K_i $(i = 1, 2)$. Si A est équivalente à $Q_1 \otimes_F Q_2$, alors elle est déployée

par K_1K_2. La condition est donc suffisante. Pour voir qu'elle est nécessaire, supposons A déployée par K_1K_2. Sans perte de généralité, on peut supposer que A est une algèbre à division. Du fait que A soit déployée par le composé de deux extensions quadratiques de F, on déduit que le degré de A divise 4 [4, § 10, Corollaire 1].

Si A est de degré 1 alors l'énoncé est trivial : on peut prendre pour Q_i $(i = 1, 2)$ la F-algèbre de quaternions déployée, qui contient K_i [4, §10, Proposition 7].

Le cas où le degré de A est égal à 4 se traite à l'aide du cas où le degré de A est égal à 2. En effet, supposons que A est de degré 4. Alors on peut considérer K_1K_2 comme sous-corps maximal de A [4, § 10, Propositions 3 et 7]. Le théorème (4.1) assure que $A = Q'_1 \otimes_F Q'_2$ où Q'_1 et Q'_2 sont deux F-algèbres de quaternions contenues dans A telles que K_1 soit contenue dans Q'_1. Ainsi Q'_2 est également déployée par K_1K_2. Si l'énoncé du théorème est vrai pour toute F-algèbre A de degré 2, alors Q'_2 est équivalente à un produit de deux F-algèbres de quaternions $Q''_1 \otimes_F Q''_2$ tel que K_i est contenu dans Q''_i $(i = 1, 2)$; comme l'algèbre $Q'_1 \otimes_F Q''_1$ est déployée par K_1 elle est équivalente à une algèbre de quaternions Q_1 qui contient K_1 comme sous-corps [4, §10, Proposition 7] ; avec $Q_2 = Q''_2$, il vient

$$A \sim Q'_1 \otimes_F Q'_2 \sim Q'_1 \otimes Q''_1 \otimes_F Q''_2 \sim Q_1 \otimes Q_2.$$

Ainsi, on s'est ramené à examiner le cas où A est de degré 2, donc une F-algèbre de quaternions. Si F est de caractéristique différente de 2 (resp. égale à 2), notons $P(X)$ le polynôme X^2 (resp. X^2+X). Soit z un élément de F qui n'est pas représenté par $P(X)$ sur F. Ainsi $K = F[X]/(P(X) - z)$ est une extension quadratique séparable de F. On rappelle que K déploie A si et seulement si K est F-isomorphe à un sous-corps (nécessairement maximal) de A [4, § 10, Propositions 3 et 7] si et seulement si z est représenté par le polynôme $P(X)$ sur A. Si F est de caractéristique différente de 2 (resp. égale à 2), ces conditions sont également équivalentes à ce que A soit de la forme $(z, \cdot)_F$ (resp. $[z, \cdot)_F$).

Choisissons des éléments a, b de $F^\times$ tels que $K_1 \cong F[X]/(P(X) - a)$ et $K_2 \cong F[X]/(P(X) - b)$. On veut montrer que A est équivalente à un produit de deux F-algèbres de quaternions dont la première contient $F[X]/(P(X) - a)$ et la deuxième $F[X]/(P(X) - b)$ comme sous-corps maximal.

Posons $c = a + b$ si F est de caractéristique 2 et $c = ab$ sinon. Si l'un des éléments a, b ou c est représenté par $P(X)$ sur A, alors l'énoncé se déduit facilement de l'observation ci-dessus par les règles de calcul pour le symbole quaternionien. Supposons désormais qu'aucun des éléments a, b et c n'est représenté par $P(X)$ sur A. En particulier, la K_1-algèbre de quaternions

$A_{K_1} = A \otimes_F K_1$ est à division. Puisqu'elle est déployée par l'extension quadratique $K_1K_2 \cong K_1[X]/(P(X) - b)$ de K_1, il existe $\beta \in A_{K_1}$ tel que $P(\beta) = b \otimes 1$. Notons par α une racine du polynôme $P(X) - a$ dans K_1 et écrivons $\beta = \beta_1 \otimes 1 + \beta_2 \otimes \alpha$ avec $\beta_1, \beta_2 \in A$. Pour le reste, nous procédons à une disjonction de cas suivant la caractéristique de F.

Considérons d'abord le cas où F est de caractéristique différente de 2. Le calcul

$$b \otimes 1 = \beta^2 = (\beta_1^2 + a\beta_2^2) \otimes 1 + (\beta_1\beta_2 + \beta_2\beta_1) \otimes \alpha$$

montre alors que $\beta_1^2 + a\beta_2^2 = b$ et $\beta_1\beta_2 + \beta_2\beta_1 = 0$ dans A. Ces égalités et le fait que le polynôme $P(X) = X^2$ ne représente ni b ni ab sur A entraînent que β_1 et β_2 forment une paire d'éléments non nuls de A qui anticommutent. Ainsi $b_1 = \beta_1^2$ et $b_2 = \beta_2^2$ sont dans F et $A \cong (b_1, b_2)_F$. De l'égalité $b_1 + ab_2 = b$ on déduit $(b_1, ab_2)_F \cong (b, -ab_1b_2)_F$, puis

$$A \sim (b_1, a)_F \otimes (b_1, ab_2)_F \sim (a, b_1)_F \otimes (b, -ab_1b_2)_F.$$

Traitons enfin le cas où la caractéristique de F est égale à 2. Les identités $a = P(\alpha) = \alpha^2 + \alpha$ permettent d'effectuer le calcul

$$b \otimes 1 = P(\beta) = \beta^2 + \beta = (\beta_1^2 + a\beta_2^2 + \beta_1) \otimes 1 + (\beta_1\beta_2 + \beta_2\beta_1 + \beta_2^2 + \beta_2) \otimes \alpha$$

duquel on déduit les égalités $b = P(\beta_1) + a\beta_2^2$ et $0 = \beta_1\beta_2 + \beta_2\beta_1 + P(\beta_2)$ dans A. En caractéristique 2, la forme trace réduite de A sur F vérifie l'identité $\mathrm{Trd}_A(x^2) = \mathrm{Trd}_A(x)^2$ pour tout $x \in A$. On obtient alors les égalités $0 = P(\mathrm{Trd}_A(\beta_1)) + a\mathrm{Trd}_A(\beta_2)^2$ et $0 = P(\mathrm{Trd}_A(\beta_2))$ valables dans F. Il s'ensuit que $\mathrm{Trd}_A(\beta_2) = 0$, puisque $P(X)$ ne représente pas a sur F. Par conséquent, β_2^2 est un élément de F. On pose $d = \beta_2^2$ et on observe que $P(\beta_2)^2 = (\beta_2^2 + \beta_2)^2 = d^2 + d$ et $P(\beta_1) = ad + b$. Comme on a exclu la possibilité que $P(\beta_1)$ soit égal à l'un des éléments a et $c = a + b$, il s'ensuit que d est différent de 0 et de 1. Ainsi, $d^2 + d \neq 0$. Le calcul

$$0 = \beta_1\beta_2 + \beta_2\beta_1 + P(\beta_2) + (\beta_1\beta_2^2 + \beta_2^2\beta_1) = \beta_1 P(\beta_2) + P(\beta_2)\beta_1 + P(\beta_2)$$

montre alors que l'algèbre de quaternions A est de la forme $[ad + b, d^2 + d)_F$. À l'aide des règles de calcul pour le symbole quaternionien en caractéristique2 (cf. [11, Section 2]), on obtient

$$[ad, d^2 + d)_F \cong [ad, a(d + 1))_F \cong [ad + a(d + 1), a(d + 1))_F \cong [a, a(d + 1))_F$$

et finalement $\quad A \cong [ad + b, d^2 + d)_F \sim [a, a(d + 1))_F \otimes [b, d^2 + d)_F.$ $\square$

Toutefois, il serait illusoire de croire qu'une F-algèbre de quaternions Q qui est déployée par une extension galoisienne L/F de groupe de Galois

$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ le soit nécessairement déjà par une extension quadratique K/F contenue dans L/F. Nous allons en donner un contre-exemple ci-dessous. D'ailleurs, il avait déjà été remarqué par E. Noether qu'une F-algèbre de quaternions Q peut être déployée par une extension *cyclique* L/F de degré supérieur à un nombre donné et telle que Q_K est à division pour toute sous-extension K/F de L/F avec $K \neq L$ (voir [9, § 13.2, Exercise]).

Le contre-exemple developpé ici fait appel à des connaissances plus avancées, concernant la *forme d'Albert* d'une algèbre de biquaternions que le lecteur peut trouver dans [6, §16A]. Cette forme quadratique, définie à similitude près, donne des informations sur cette algèbre, notamment sur son *indice de Schur* [6, 16.5 Theorem].

4.4 Exemple. Soit A une algèbre de biquaternions à division sur un corps k de caractéristique différente de 2. Soit φ une forme d'Albert associée à A. Notons par F le corps des fonctions $k(\varphi)$. Alors A_F est équivalente à une F-algèbre de quaternions Q. Soit $k(\sqrt{a}, \sqrt{b})$ une extension biquadratique de k, avec $a, b \in k^\times$, qui déploie A. Alors $F(\sqrt{a}, \sqrt{b})$ déploie Q. Cependant aucune extension $F(\sqrt{c})$ avec $c \in k^\times$ ne déploie Q. En effet, dans le cas contraire, il existe $c \in k^\times$ tel que $\varphi_{k(\sqrt{c})(\varphi)}$ est hyperbolique. Il en est donc de même de $\varphi_{k(\sqrt{c})}$ puisque $\varphi_{k(\sqrt{c})}$ n'est pas une forme de Pfister [13, 4.5.4. Theorem (i)]. Ainsi, on voit que $k(\sqrt{c})$ déploie A, ce qui est impossible puisque A est à division et de degré 4.

Remerciements

Le présent travail fait partie de la thèse de doctorat de l'auteur, effectuée à l'*Université de Franche-Comté* sous la direction de Eva Bayer-Fluckiger et Detlev Hoffmann. Il a été commencé lors d'un stage pré-doctoral de l'auteur à l'invitation de David Lewis à *University College Dublin* dans le cadre du réseau *Algebraic K-Theory, Linear Algebraic Groups and Related Structures* (TMR Network ERB FMRX-CT97-0107). Il a bénéficié ensuite des commentaires judicieux de Jean-Pierre Tignol. Le travail a été achevé pendant un stage post-doctoral de l'auteur à l'*Université Catholique de Louvain* à l'invitation de Jean-Pierre Tignol dans le cadre du même réseau. Enfin, le soutien pour la rédaction de la part de Emmanuel Lequeu et Anne Cortella a été très précieux. L'auteur tient à exprimer toute sa gratitude à ces personnes et institutions.

Références

[1] A.A. Albert. *Structure of algebras.* American Mathematical Society Colloquium Publ. 24, New York, 1939.

[2] S.A. Amitsur, L.H. Rowen et J.-P. Tignol. Division algebras of degree 4 and 8 with involution, *Israel J. Math.*, 33:133–148, 1979.

[3] A. Blanchard. *Les corps non commutatifs.* Collection SUP: Le Mathématicien, No. 9. Presses Universitaires de France, Vendôme, 1972.

[4] N. Bourbaki. *Éléments de mathématique. 23. Première partie: Les structures fondamentales de l'analyse. Livre II: Algèbre. Chapitre 8: Modules et anneaux semi-simples.* Hermann, Paris, 1958.

[5] A. Cortella et J.-P. Tignol. The asymmetry of an anti-automorphism. *J. Pure Appl. Algebra*, 167:175–193, 2002.

[6] M.-A. Knus, A.S. Merkurjev, M. Rost et J.-P. Tignol. *The book of involutions.* American Mathematical Society, Providence, RI, 1998.

[7] T. Y. Lam, D. B. Leep et J.-P. Tignol. Biquaternion algebras and quartic extensions. *I.H.E.S. Publ. Math.*, No. 77, pp. 63–102, 1993.

[8] A.S. Merkurjev, On the norm residue symbol of degree 2. *Sov. Math., Dokl.*, 24:546–551, 1981.

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

[10] M. L. Racine. A simple proof of a theorem of Albert. *Proc. Amer. Math. Soc.*, 43:487–488, 1974.

[11] L.H. Rowen. Division Algebras of Exponent 2 and Characteristic 2. *J. Algebra*, 90:71–83, 1984.

[12] W. Scharlau. Zur Existenz von Involutionen auf einfachen Algebren. *Math. Z.*, 145:29–32, 1975.

[13] W. Scharlau. *Quadratic and Hermitian forms*, Grundlehren der mathematischen Wissenschaften 270, Springer-Verlag, Berlin, 1985.

[14] J.-P. Tignol. Corps à involution neutralisés par une extension abélienne élémentaire. Dans: *Groupe de Brauer (Sem., Les Plans-sur-Bex, 1980)* (M. Kervaire et M. Ojanguren, éd.), Lecture Notes in Math. 844, pp. 1–34, Springer, Berlin, 1981.