SPLITTING FIELDS OF CENTRAL SIMPLE ALGEBRAS OF EXPONENT TWO

KARIM JOHANNES BECHER

Abstract. By Merkurjev's Theorem every central simple algebra of exponent two is Brauer equivalent to a tensor product of quaternion algebras. In particular, if every quaternion algebra over a given field is split, then there exists no central simple algebra of exponent two over this field. This note provides an independent elementary proof for the latter fact.

Classification (MSC 2010): 11E04, 11E81, 16H05, 16K20, 16K50

Keywords: Brauer group, field, central simple algebra, quaternion algebra, splitting field, index, exponent, 2-extension, involution

Central simple algebras and the Brauer group of a field are a classical topic in algebra. The aim of this note is to give an elementary proof for the existence of certain splitting fields for central simple algebras of exponent two.

Let K be a field. Let A be a central simple K-algebra. We say that A is *split* if it is a matrix algebra over K. The *index of* A is defined as the degree of the unique K-division algebra Brauer equivalent to A. The *exponent of* A is the order of the class of A in the Brauer group of A.

By [1, Theorem 4.5.13] the exponent divides the index and both numbers have the same prime factors. Examples can easily be constructed showing that any pair of natural numbers fulfilling these two constraints occur as the index and the exponent of a central simple algebra over some field.

By [1, Corollary 4.5.9] the index of A is equal to the smallest degree $[L : K]$ of a finite separable field extension L/K such that the L-algebra $A_L = A \otimes_K L$ is split. Apart from this condition on the degree, little is known about the finite extensions that split A. For example, if A has prime index p, it is an open problem (for $p > 3$) whether there exists a cyclic extension of degree p of K that splits A. The only way to obtain general statements on the existence of splitting fields of a certain type based on the index and the exponent seems to be the Merkurjev-Suslin Theorem [1, Theorem 2.5.7], a generalisation of Merkurjev's result from [3] on central simple algebras of exponent two.

Let $\mathrm{Br}_2(K)$ denote the 2-torsion part of $\mathrm{Br}(K)$. Merkurjev's Theorem [1, Theorem 1.5.8] tells us that $\mathrm{Br}_2(K)$ is generated by the classes of the K-quaternion algebras. (By [1, Theorem 9.1.4] this statement also holds in characteristic 2, where it is due to Teichmüller.) There are different proofs of Merkurjev's

Date: 18 March, 2016.

This work was supported by the Deutsche Forschungsgemeinschaft (project *The Pfister Factor Conjecture in Characteristic Two*, BE 2614/4) and the FWO Odysseus programme (project *Explicit Methods in Quadratic Form Theory*).

Theorem in the literature (see the references in the introduction of [1, Chap. 8]), but all of them are quite involved.

Merkurjev's Theorem implies that any element of $\mathrm{Br}_2(K)$ is split by a finite Galois extension with 2-elementary abelian Galois group, so in particular by a 2-extension. In some applications to the study of algebras with involution and their cohomological invariants, only the latter fact is needed. This motivates looking for a more elementary argument for this consequence. This note provides such an argument, fitting into the basic part of the theory of central simple algebras and their involutions.

A finite extension L/K is called a 2-*extension* if it is separable and if the degree of its normal closure is a power of 2. By classical Galois theory and the fact that 2-groups are solvable, this is equivalent to the existence of $r \in \mathbb{N}$ and a tower of fields $(L_i)_{i=0}^r$ with $L_0 = K$, $L_r = L$, and where L_i/L_{i-1} is a separable quadratic extension for $i = 1, \dots, r$.

Lemma 1. *Let L/K be a finite 2-extension. If every K-quaternion algebra is split, then every L-quaternion algebra is split.*

Proof: Suppose first that $[L : K] = 2$ and consider an L-quaternion algebra Q. Let B denote the corestriction (norm) of Q with respect to L/K as defined in [2, §3.B]. Then B is a central simple K-algebra of degree 4 and exponent at most 2. By a theorem due to Albert [2, §16], B is isomorphic a tensor product of two K-quaternion algebras. Assume now that every K-quaternion algebra is split. Then B is split. In view of [2, (2.22) and (3.1)] this implies that Q is extended from a K-quaternion algebra. By the assumption this K-quaternion algebra is split. Hence Q is split.

This argument shows the statement in the case of a separable quadratic extension L/K. The general case then follows by induction, since any finite 2-extension is reached by a finite tower of separable quadratic extensions. □

Let L/K be a field extension. We denote by $\mathrm{Br}(L/K)$ the kernel of the natural homomorphism $\mathrm{Br}(K) \longrightarrow \mathrm{Br}(L)$. For an element $\alpha \in \mathrm{Br}(K)$ we denote by α_L its image in $\mathrm{Br}(L)$, and we say that L/K *splits* α or that α *splits over* L if $\alpha_L = 0$. The *index of* $\alpha \in \mathrm{Br}(K)$, denoted $\mathrm{ind}(\alpha)$, is the minimal degree of a field extension L/K such that $\alpha_L = 0$.

Lemma 2. *Let L/K be a finite 2-extension. If every K-quaternion algebra is split, then* $\mathrm{Br}(L/K) = 0$.

Proof: Let $r \in \mathbb{N}$ and let $(L_i)_{i=0}^r$ be a tower of fields such that $L_0 = K$, $L_r = L$ and L_i/L_{i-1} is a separable quadratic extension for $i = 1, \dots, r$. Assume that there exists a nontrivial element $\alpha \in \mathrm{Br}(L/K)$. Then for some $s \in \{1, \dots, r\}$ we have that $\alpha_{L_{s-1}} \neq 0$ and $\alpha_{L_s} = 0$. Since $[L_s : L_{s-1}] = 2$ it follows that $\mathrm{ind}(\alpha_{L_{s-1}}) = 2$. Set $L' = L_{s-1}$. Then L'/K is a finite 2-extension and $\alpha_{L'}$ is the class of a non-split L'-quaternion algebra. By Lemma 1 it follows that there exists a non-split K-quaternion algebra. □

We denote by $\mathrm{char}(K)$ the characteristic of K. We further write $K^\times$ for the multiplicative group of K and $K^{\times 2}$ for the subgroup of non-zero squares.

Proposition. *Assume that $K^\times = K^{\times 2}$ and that K is not algebraically closed. Let L/K be a proper finite field extension of K of minimal degree. Then* $\mathrm{Br}(M/L) = 0$ *for every finite* 2*-extension* M/L.

Proof: Consider an arbitrary L-quaternion algebra Q. If $\mathrm{char}(K) = 2$, then as $K^\times = K^{\times 2}$ we have that K is perfect, hence L is perfect, and as $\mathrm{char}(L) = 2$ it follows that Q is split. Suppose now that $\mathrm{char}(K) \neq 2$.

The hypothesis that L/K has minimal degree among all proper field extensions of K implies that every polynomial $f \in K[T]$ with $\deg(f) < [L : K]$ is split. We fix an element $x \in L \setminus K$. Then $L = K[x]$, whereby $Q \simeq (f(x), g(x))_L$ for two nonzero polynomials $f, g \in K[T]$ of degree strictly smaller than $[L : K]$. Hence f and g are split. Since $K^\times = K^{\times 2}$ we may choose f and g to be monic. If one of f or g is constant then it is equal to 1, whereby Q is split. As $-1 \in K^{\times 2}$ we also have that $Q \simeq (f(x), -g(x))_L$. If f and g are linear, then $f - g$ is a square in K, and it follows that Q is split. In the general case, writing $f = \prod_{i=1}^m f_i$ and $g = \prod_{i=1}^n g_i$ with $m, n \in \mathbb{N}$ and monic linear polynomials $f_1, \dots, f_m, g_1, \dots, g_n \in K[T]$, we conclude that $(f_i(x), g_j(x))_L$ is split for any $i \in \{1, \dots, m\}$ and any $j \in \{1, \dots, n\}$. By the bilinearity of the quaternion pairing $L^\times \times L^\times \longrightarrow \mathrm{Br}(L)$, it follows that Q is split.

Hence, we have shown that every L-quaternion algebra is split. By Lemma 2 this yields the statement. $\square$

We say that K is *quadratically closed* if every quadratic polynomial in $K[T]$ is split, or equivalently, if K admits no quadratic field extension.

Lemma 3. *Assume there exists an element $\alpha \in \mathrm{Br}(K)$ satisfying the following:*

(a) *For any finite* 2*-extension L/K we have $\alpha_L \neq 0$.*
(b) *For any proper finite field extension K'/K, there exists a* 2*-extension L/K' such that $\alpha_L = 0$.*

Then K is quadratically closed.

Proof: Suppose that K is not quadratically closed. We fix a quadratic field extension K'/K. By (b) there exists a finite 2-extension L'/K' with $\alpha_{L'} = 0$. Let K'' denote the relative separable closure of K inside L'. Then K''/K is a finite 2-extension and $[L' : K''] \leq [K' : K] = 2$. Since $\alpha_{L'} = 0$ it follows that $\mathrm{ind}(\alpha_{K''}) \leq 2$. If $\mathrm{ind}(\alpha_{K''}) = 2$, then we may choose a separable quadratic extension L/K'' such that $\alpha_L = 0$. If $\mathrm{ind}(\alpha) = 1$ then we set $L = K''$. In either case L/K is a finite 2-extension such that $\alpha_L = 0$, in contradiction to (a). $\square$

Lemma 4. *Let $\alpha \in \mathrm{Br}_2(K)$ with $\alpha \neq 0$. There exists a finite field extension L/K such that $[L : K] = \frac{1}{2}\mathrm{ind}(\alpha)$ and $\mathrm{ind}(\alpha_L) = 2$.*

Proof: Let D be the central K-division algebra whose class in $\mathrm{Br}(K)$ is α. Since $\alpha + \alpha = 0 \neq \alpha$, it follows by [2, (2.8) and (3.1)] that there exists a symplectic involution σ on D. Let L/K be a separable field extension contained in D with $\sigma|_L = \mathrm{id}_L$ and maximal for these properties. Using [2, (4.12)] it follows that $[L : K] = \frac{1}{2}\mathrm{ind}(\alpha)$ and thus $\mathrm{ind}(\alpha_L) = 2$. $\square$

We are ready to prove the main statement.

Theorem. *Every element of* $\mathrm{Br}(K)$ *of order a power of* 2 *is split by a finite* 2*-extension of* K*.*

Proof: Consider an element $\alpha \in \mathrm{Br}(K)$ of order 2^r where $r \in \mathbb{N}$. If 2α is split by a 2-extension K'/K, then $\alpha_{K'} \in \mathrm{Br}_2(K')$, and if furthermore $\alpha_{K'}$ is split by a 2-extension L/K', then L/K is a 2-extension splitting α. Hence, the statement follows by induction on r from the case where $\alpha \in \mathrm{Br}_2(K)$.

Suppose now that $\alpha \in \mathrm{Br}_2(K)$ and that α is not split by any finite 2-extension of K. Using Zorn's Lemma we obtain an algebraic field extension K'/K that is maximal for the property that $\alpha_{K'}$ is not split by any finite 2-extension of K'. By Lemma 3 this maximality implies that K' is quadratically closed. On the other hand $\alpha_{K'} \neq 0$, whereby K' is not algebraically closed. Let L/K' be a proper finite field extension of minimal degree. Then $1 < [L : K'] < \mathrm{ind}(\alpha_{K'})$, by Lemma 4. Hence, $\alpha_L \neq 0$ and by the maximality of K' there exists a finite 2-extension M/L such that $\alpha_M = 0$. This contradicts the Proposition. □

Corollary. *Assume that every* K*-quaternion algebra is split. Then every element of* $\mathrm{Br}(K)$ *has odd order.*

Proof: Since $\mathrm{Br}(K)$ is a torsion group it suffices to show that $\mathrm{Br}_2(K) = 0$. Consider $\alpha \in \mathrm{Br}_2(K)$. By the Theorem we have that $\alpha \in \mathrm{Br}(L/K)$ for some finite 2-extension L/K. Since every K-quaternion algebra is split, we obtain by Lemma 2 that $\mathrm{Br}(L/K) = 0$, whereby $\alpha = 0$. □

It would be desirable to have a more explicit version of the above Theorem that provides a bound on the degree of a splitting 2-extension for $\alpha \in \mathrm{Br}_2(K)$ in terms of $\mathrm{ind}(\alpha)$. The proof presented here does not yield any such bound, as it uses Zorn's Lemma.

Question 1. *Is every element* $\alpha \in \mathrm{Br}_2(K)$ *split by a* 2*-extension* L/K *of degree* $[L : K] = \mathrm{ind}(\alpha)$*?*

Equivalently, one may ask whether any finite-dimensional division algebra of exponent two contains a separable quadratic extension of its centre.

The answer to Question 1 is known to be positive when $\mathrm{ind}(\alpha) \leq 8$; for $\mathrm{ind}(\alpha) = 8$ this follows from a theorem due to Rowen (cf. [5, p. 279, Exercise 32] and [4, Theorem 1]).

We mention another open problem related to the above Corollary.

Question 2. *If* K *is quadratically closed, does it follow that* $\mathrm{Br}_2(L) = 0$ *for every finite field extension* L/K*?*

References

[1] P. Gille and T. Szamuely. *Central simple algebras and Galois cohomology.* Cambridge University Press (2006).

[2] M.-A. Knus, A.S. Merkurjev, M. Rost, and J.-P. Tignol. *The book of involutions. American Mathematical Society Colloquium Publications* **44**. American Mathematical Society, Providence, RI, 1998.

[3] A. S. Merkurjev. On the norm residue symbol of degree 2. (Russian) *Dokl. Akad. Nauk. SSSR* **261** (1981): 542–547. English translation: *Soviet Math. Dokl.* **24** (1981): 546–551.

[4] L.H. Rowen, Division algebras of exponent 2 and characteristic 2, *J. Algebra* **90** (1984) 71–83.

[5] L. H. Rowen. *Ring Theory, Vol. II.* Pure and Applied Mathematics, **128**. Academic Press, Inc., Boston, MA, 1988.

Departement Wiskunde–Informatica, Universiteit Antwerpen, Belgium
E-mail address: becher@maths.ucd.ie