Bull. Math. Soc. Sci. Math. Roumanie
Tome 60 (108) No. 3, 2017, 307–312

About split quaternion algebras over quadratic fields and symbol algebras of degree n

by

Diana Savin

Abstract

In this paper we determine sufficient conditions for a quaternion algebra to split over a quadratic field. In the last section of the paper, we find a class of non-split symbol algebras of degree n (where n is a positive integer, $n \geq 3$) over a $p-$ adic field or over a cyclotomic field.

Key Words: quaternion and symbol algebras; quadratic fields, cyclotomic fields; Kummer fields; $p-$ adic fields
2010 Mathematics Subject Classification: Primary 11R52, 11R18, 11S15, 11R37, Secondary 11R04, 11A41, 11F85.

1 Introduction

Let K be a field with char$K \neq 2$. Let $K^* = K \backslash \{0\}$, $a, b \in K^*$. The quaternion algebra $H_K(a, b)$ is the K-algebra with K-basis $\{1; e_1; e_2; e_3\}$ satisfying the relations: $e_1^2 = a$, $e_2^2 = b$, $e_3 = e_1 \cdot e_2 = -e_2 \cdot e_1.$
Let n be an arbitrary positive integer, $n \geq 3$ and let ξ be a primitive n-th root of unity. Let K be a field with char$K \neq 2$, char$K$ does not divide n and $\xi \in K$. Let $a, b \in K^*$ and let A be the algebra over K generated by elements x and y where

$$x^n = a, y^n = b, yx = \xi xy.$$

This algebra is called a *symbol algebra* and it is denoted by $\left(\frac{a,\ b}{K, \xi}\right)$. For $n = 2$, we obtain the quaternion algebra. Quaternion algebras and symbol algebras are central simple algebras of dimension n^2 over K, non-commutative, but associative algebras (see [11]).

In this article we find sufficient conditions for a quaternion algebra to split over a quadratic field. In the paper [12] we found a class of division quaternion algebra over the quadratic field $\mathbb{Q}(i)$ ($i^2 = -1$), respectively a class of division symbol algebra over the cyclotomic field $\mathbb{Q}(\xi)$, where ξ is a primitive root of order q (prime) of unity. In the last section of this article we generalize these results for symbol algebras of degree $n \geq 3$, not necessarily prime.

2 Preliminaries

We recall some results of the theory of cyclotomic fields, Kummer fields and $p-$ adic fields, associative algebras, which will be used in our paper. Let n be an integer, $n \geq 3$ and let

K be a field of characteristic prime to n in which $x^n - 1$ splits; and let ξ be a primitive n th root of unity. The following lemma (which can be found in [2]) gives information about certain extension of K.

Lemma 1. *If a is a non-zero element of K, there is a well-defined normal extension $K\left(\sqrt[n]{a}\right)$, the splitting field of $x^n - a$. If α is a root of $x^n = a$, there is a map of the Galois group $G\left(K\left(\sqrt[n]{a}\right)/K\right)$ into K^* given by $\sigma \longmapsto \sigma(\alpha)/\alpha$; in particular, if a is of order n in $K^*/\left(K^*\right)^n$, the Galois group is cyclic and can be generated by σ with $\sigma(\alpha) = \xi\alpha$. Moreover, the discriminant of $K\left(\sqrt[n]{a}\right)$ over K divides $n^n \cdot a^{n-1}$; p is unramified if $p \nmid na$.*

Let $A \neq 0$ be a central simple algebra over a field K. We recall that if A is a finite-dimensional algebra, then A is a division algebra if and only if A is without zero divisors $(x \neq 0, y \neq 0 \Rightarrow xy \neq 0)$. A is called *split* by K if A is isomorphic with a matrix algebra over K. If $K \subset L$ is a fields extension, we recall that A is called *split* by L if $A \otimes_K L$ is a matrix algebra over L. The Brauer group $(\mathrm{Br}(K), \cdot)$ of K is $\mathrm{Br}(K) = \left\{[A] \,|\, A \textit{ is a central simple } K - \textit{algebra}\right\}$, where, two classes of central simple algebras are equals $[A] = [B]$ if and only if there are two positive integers r and s such that $A \otimes_K M_r(K) \cong B \otimes_K M_s(K)$.
The group operation in $\mathrm{Br}(K)$ is : "$\cdot$": $\mathrm{Br}(K) \times \mathrm{Br}(K) \longrightarrow \mathrm{Br}(K)$, $[A] \cdot [B] = [A \otimes_K B]$, for $(\forall)$ $[A], [B] \in \mathrm{Br}(K)$ (see [11], [7]). A result due Albert-Brauer-Hasse-Noether says that for any number field K, the following sequence is exact:

$$0 \longrightarrow Br(K) \longrightarrow \oplus_v Br(K_v) \longrightarrow \mathbb{Q}/\mathbb{Z} \longrightarrow 0$$

Remark 1. *([9]). Let n be a positive integer, $n \geq 3$ and let ξ be a primitive n-th root of unity. Let K be a field such that $\xi \in K$, $a, b \in K^*$. If n is prime, then the symbol algebra $\left(\frac{a,\ b}{K, \xi}\right)$ is either split or a division algebra.*

Theorem 1. *([10]) (Albert-Brauer-Hasse-Noether). Let H_F be a quaternion algebra over a number field F and let K be a quadratic field extension of F. Then there is an embedding of K into H_F if and only if no prime of F which ramifies in H_F splits in K.*

Proposition 1. *([5]). Let F be a number field and let K be a field containing F. Let H_F be a quaternion algebra over F. Let $H_K = H_F \otimes_F K$ be a quaternion algebra over K. If $[K : F] = 2$, then K splits H_F if and only if there exists an F-embedding $K \hookrightarrow H_F$.*

3 Quaternion algebras which split over quadratic fields

Let p, q be two odd prime integers, $p \neq q$. If a quaternion algebra $H(p, q)$ splits over $\mathbb{Q}$, of course it splits over each algebraic number fields. It is known that if K is an algebraic number field such that $[K : \mathbb{Q}]$ is odd and $\alpha, \beta \in \mathbb{Q}^*$, then the quaternion algebra $H_K(\alpha, \beta)$ splits if and only if the quaternion algebra $H_{\mathbb{Q}}(\alpha, \beta)$ splits (see [8]). But, when $[K : \mathbb{Q}]$ is even there are quaternion algebras $H(\alpha, \beta)$ which does not split over $\mathbb{Q}$, but its split over K. For example, the quaternion algebra $H(11, 47)$ does not split over $\mathbb{Q}$, but it splits over the quadratic field $\mathbb{Q}(i)$ (where $i^2 = -1$).
We want to determine sufficient conditions for a quaternion algebra $H(p, q)$ to split over a

quadratic field $K=\mathbb{Q}\left(\sqrt{d}\right)$. Let $\mathcal{O}_K$ be the ring of integers of K. Since p and q lie in $\mathbb{Q}$, the problem whether $H_{\mathbb{Q}(\sqrt{d})}(p,q)$ splits reduces to whether $H_{\mathbb{Q}}(p,q)$ splits under scalar extension to $\mathbb{Q}\left(\sqrt{d}\right)$.

It is known that, for each prime positive integer p, $Br\left(\mathbb{Q}_p\right)\cong\mathbb{Q}/\mathbb{Z}$ (the isomorphism is $inv_p: Br\left(\mathbb{Q}_p\right)\to\mathbb{Q}/\mathbb{Z}$) and for $p=\infty$, $Br\left(R\right)\cong\mathbb{Z}/2\mathbb{Z}$.

We obtain sufficient conditions for a quaternion algebra $H\left(p,q\right)$ to split over a quadratic field.

Theorem 2. *Let $d\neq 0,1$ be a free squares integer, $d\not\equiv 1$ (mod 8) and let p,q be two prime integers, $q\geq 3$, $p\neq q$. Let $\mathcal{O}_K$ be the ring of integers of the quadratic field $K=\mathbb{Q}\left(\sqrt{d}\right)$ and Δ_K be the discriminant of K. Then, we have:*

i) if $p\geq 3$ and the Legendre symbols $\left(\frac{\Delta_K}{p}\right)\neq 1$, $\left(\frac{\Delta_K}{q}\right)\neq 1$, then, the quaternion algebra $H_{\mathbb{Q}(\sqrt{d})}(p,q)$ splits;

ii) if $p=2$ and the Legendre symbol $\left(\frac{\Delta_K}{q}\right)\neq 1$, then, the quaternion algebra $H_{\mathbb{Q}(\sqrt{d})}(2,q)$ splits.

Proof: i) Applying Albert-Brauer-Hasse-Noether theorem, we obtain the following description of the Brauer group of $\mathbb{Q}$ and of the Brauer group of the quadratic field $\mathbb{Q}\left(\sqrt{d}\right)$.

$$\begin{tikzcd}
0 \arrow[r] & Br\left(\mathbb{Q}\right) \arrow[r] \arrow[d] & \oplus_p Br\left(\mathbb{Q}_p\right)\cong\left(\oplus_p\mathbb{Q}/\mathbb{Z}\right)\oplus\mathbb{Z}/2\mathbb{Z} \arrow[r] \arrow[d, "\oplus_p\varphi_p\oplus 0"] & \mathbb{Q}/\mathbb{Z} \arrow[r] & 0 \\
0 \arrow[r] & Br\left(\mathbb{Q}\left(\sqrt{d}\right)\right) \arrow[r] & \oplus_P Br\left(\mathbb{Q}\left(\sqrt{d}\right)_P\right)\cong\left(\oplus_P\mathbb{Q}/\mathbb{Z}\right) \arrow[r] & \mathbb{Q}/\mathbb{Z} \arrow[r] & 0
\end{tikzcd}$$

where φ_p is the multiplication by 2 when there is single $P\in\mathrm{Spec}(\mathcal{O}_K)$ above the ideal $p\mathbb{Z}$ i.e. $p\mathbb{Z}$ is inert in $\mathcal{O}_K$ or $p\mathbb{Z}$ is ramified in $\mathcal{O}_K$, respectively φ_p is the diagonal map $\mathbb{Q}/\mathbb{Z}\to\mathbb{Q}/\mathbb{Z}\oplus\mathbb{Q}/\mathbb{Z}$ if there are two primes P, P' of $\mathcal{O}_K$ above $p\mathbb{Z}$ i.e. $p\mathbb{Z}$ is totally split in $\mathcal{O}_K$. Using this description we determine sufficient conditions for a quaternion algebra $H\left(p,q\right)$ to split over a quadratic field $K=\mathbb{Q}\left(\sqrt{d}\right)$.

It is known that $\Delta_K=d$ (if $d\equiv 1$ (mod 4)) or $\Delta_K=4d$ (if $d\equiv 2,3$ (mod 4)). Since $\left(\frac{\Delta_K}{p}\right)\neq 1$, $\left(\frac{\Delta_K}{q}\right)\neq 1$ it results $\left(\frac{d}{p}\right)=-1$ or $\left(\frac{d}{p}\right)=0$, respectively $\left(\frac{d}{q}\right)=-1$ or $\left(\frac{d}{q}\right)=0$. Applying the theorem of decomposition of a prime integer p in the ring of integers of a quadratic field (see for example [4], p. 190), it results that p is ramified in $\mathcal{O}_K$ or p is inert in $\mathcal{O}_K$, respectively q is ramified in $\mathcal{O}_K$ or q is inert in $\mathcal{O}_K$. So, p and q do not split in K. Let Δ denote the discriminant of the quaternion algebra $H_{\mathbb{Q}(\sqrt{d})}(p,q)$.

It is known that a prime positive integer p' ramifies in $H_{\mathbb{Q}(\sqrt{d})}(p,q)$ if $p'|2\Delta$ ([6], [7], [13]). This implies $p'|2pq$.

Since $d\not\equiv 1$ (mod 8) and the decomposition of 2 in $\mathcal{O}_K$ (see [4], p. 190), it results that 2 does not split in K.

From the previously proved and applying Theorem 1 and Proposition 1, it results that the quaternion algebra $H_{\mathbb{Q}\left(\sqrt{d}\right)}\left(p,q\right)$ splits.
ii) Let $p^{'}$ be a prime positive integer which ramifies in $H_{\mathbb{Q}\left(\sqrt{d}\right)}\left(2,q\right)$. In this case the condition $p^{'}|2\Delta$ implies $p^{'}|2q$. With similar reasoning as i) we get that the quaternion algebra $H_{\mathbb{Q}\left(\sqrt{d}\right)}\left(2,q\right)$ splits. □

Remark 2. *The conditions* $\left(\frac{\Delta_K}{p}\right)\neq 1$, $\left(\frac{\Delta_K}{q}\right)\neq 1$ *from Theorem 2 are not necessary for the quaternion algebra* $H_{\mathbb{Q}\left(\sqrt{d}\right)}\left(q,p\right)$ *splits. For example, if* $d=-1$, *the conditions* $\left(\frac{\Delta_K}{p}\right)\neq 1$, $\left(\frac{\Delta_K}{q}\right)\neq 1$ *are equivalent to* $p\equiv q\equiv 3(mod\ 4)$. *We consider the quaternion algebra* $H_{\mathbb{Q}(i)}\left(5,29\right)$, *so* $p=5\equiv 1(mod\ 4)$ *and* $q=29\equiv 1(mod\ 4)$. *Doing some calculations in software MAGMA, we obtain that the algebra* $H_{\mathbb{Q}(i)}\left(5,29\right)$ *splits. Analogous, for* $p=5\equiv 1(mod\ 4)$ *and* $q=19\equiv 3(mod\ 4)$, *we obtain that the algebra* $H_{\mathbb{Q}(i)}\left(5,19\right)$ *splits. Another example: if* $d=3$, $p=7, q=47$, *we have* $\left(\frac{\Delta_K}{p}\right)\neq 1$, *but* $\left(\frac{\Delta_K}{q}\right)=1$. *However the quaternion algebra* $H_{\mathbb{Q}\left(\sqrt{3}\right)}\left(7,47\right)$ *splits. Another remark is that the quaternion algebra* $H_{\mathbb{Q}}\left(7,47\right)$ *does not split.*

We wonder what happens with a quaternion algebra $H_{\mathbb{Q}\left(\sqrt{d}\right)}\left(p,q\right)$ from Theorem 2 when instead of p or q we consider an arbitrary integer α. Immediately we obtain the following result:

Corollary 1. *Let* $d\neq 0,1$ *be a free squares integer,* $d\not\equiv 1\ (mod\ 8)$ *and let* α *be an integer and* p *be an odd prime integer. Let* $\mathcal{O}_K$ *be the ring of integers of the quadratic field* $K=\mathbb{Q}\left(\sqrt{d}\right)$ *and* Δ_K *be the discriminant of* K. *If the Legendre symbols* $\left(\frac{\Delta_K}{p}\right)\neq 1$, $\left(\frac{\Delta_K}{q}\right)\neq 1$, *for each odd prime divisor* q *of* α *then, the quaternion algebra* $H_{\mathbb{Q}\left(\sqrt{d}\right)}\left(\alpha,p\right)$ *splits.*

Proof: We want to determine the primes $p^{'}$ which ramifies in $H_{\mathbb{Q}\left(\sqrt{d}\right)}\left(\alpha,p\right)$, i.e the primes $p^{'}$ with the property $p^{'}|2\Delta$. This implies $p^{'}|2\alpha\cdot p$. Since $\left(\frac{\Delta_K}{p}\right)\neq 1$, $\left(\frac{\Delta_K}{q}\right)\neq 1$, for each odd prime divisor q *of* α, using a reasoning similar with that of Theorem 2, we get that such primes do not exist, so the quaternion algebra $H_{\mathbb{Q}\left(\sqrt{d}\right)}\left(\alpha,p\right)$ splits.
□

4 Symbol algebras of degree n

In the paper [12] we found a class of division quaternion algebras over the quadratic field $\mathbb{Q}\left(i\right)$ ([12], Th. 3.6) and a class of division symbol algebras of degree q (where q is an odd prime positive integer) over a p- adic field or over a cyclotomic field ([12], Th. 3.7). Here we generalize theorem 3.7 from [12], when A is a symbol algebra over the n-th cyclotomic field, where n is a positive integer, $n\geq 3$.

Theorem 3. *Let n be a positive integer, $n \geq 3$, p be a prime positive integer such that $p \equiv 1$ (mod n), ξ be a primitive root of order n of unity and let $K = \mathbb{Q}(\xi)$ be the n th cyclotomic field. Then there is an integer α not divisible by p, α is not a l power residue modulo p, for $(\forall)$ $l \in \mathbb{N}$, $l|n$ and for every such an α, we have:*
i) if A is the symbol algebra $A = \left(\frac{\alpha,p}{K,\xi}\right)$, then $A \otimes_K \mathbb{Q}_p$ is a non-split algebra over $\mathbb{Q}_p$;
ii) the symbol algebra A is a non-split algebra over K.

Proof: i) Let be the homomorphism $f : \mathbb{F}_p^* \to \mathbb{F}_p^*$, $f(x) = x^n$. Since $p \equiv 1$ $(mod\ n)$, it results $Ker(f) = \left\{x \in F_p^* | x^n \equiv 1\ (mod\ p)\right\}$ is non -trivial, so f is not injective. So, f is not surjective. It results that there exists $\overline{\alpha}$ (in $\mathbb{F}_p^*$,) which does not belong to $\left(\mathbb{F}_p^*\right)^n$. Let β be an n th root of α (modulo p). Since α is not a l power residue modulo p, for $(\forall)$ $l \in \mathbb{N}$, $l|n$, it results that the extension of fields $\mathbb{F}_p\left(\overline{\beta}\right)/\mathbb{F}_p$ is a cyclic extension of degree n. Applying a consequence of Hensel's lemma (see for example [1]) and the fact that $p \equiv 1$ (mod n), it results that $\mathbb{Q}_p$ contains the n-th roots of the unity, therefore $\mathbb{Q}(\xi) \subset \mathbb{Q}_p$. Let the symbol algebra $A \otimes_K \mathbb{Q}_p = \left(\frac{\alpha,p}{\mathbb{Q}_p,\xi}\right)$. Applying Lemma 1, it results that the extension $\mathbb{Q}_p\left(\sqrt[n]{\alpha}\right)/\mathbb{Q}_p$ is a cyclic unramified extension of degree n, therefore a norm of an element from this extension can be a positive power of p, but cannot be p. According to a criterion for splitting of the symbol algebras (see Corollary 4.7.7, p. 112 from [3]), it results that $\left(\frac{\alpha,p}{\mathbb{Q}_p,\xi}\right)$ is a non-split algebra.
ii) Applying i) and the fact that $K \subset \mathbb{Q}_p$, it results that A is a non-split algebra. □

Remark 3. *Although Theorem 3 is the generalization of Theorem 3.7 from [12] for symbol algebras of degree n, there are some differences between these two theorems, namely:*
- One of the conditions of the hypothesis of Theorem 3.7 from [12] is: α is not a q power residue modulo p. With a similar condition in the hypothesis of Theorem 3, namely: α is not a n power residue modulo p, Theorem 3 does not work. We give an example in this regard: let $p = 7$, $n = 6$, $\alpha = 2$. 2 is not a 6 power residue modulo 7, but 2 is a quadratic residue modulo 7. Let β be an 6 th root of α (modulo 7). We obtain that the polynomial $Y^6 - \overline{2}$ is not irreducible in $\mathbb{F}_7[Y]$. We have $Y^6 - \overline{2} = \left(Y^3 - \overline{3}\right) \cdot \left(Y^3 + \overline{3}\right)$ (in $\mathbb{F}_7[Y]$). So, the extension of fields $\mathbb{F}_7 \subset \mathbb{F}_7\left(\overline{\beta}\right)$ has not the degree $n = 6$. For this reason, in the hypothesis of Theorem 3 we put the condition: α is not a l power residue modulo p, for $(\forall)$ $l \in \mathbb{N}$, $l|n$;
- In Theorem 3.7 from [12] we proved that $A \otimes_K \mathbb{Q}_p$ is a non-split symbol algebra over $\mathbb{Q}_p$ (respectively A is a non-split symbol algebra over K) and applying Remark 1 this is equivalent to A is a division symbol algebra over $\mathbb{Q}_p$ (respectively A is a division symbol algebra over K). But, Remark 1 holds if and only if n is prime. For this reason, the conclusion of Theorem 3 is: A is a non-split symbol algebra over $\mathbb{Q}_p$ (respectively A is a non-split symbol algebra over K).

Conclusions. In the last section of the paper, we found a class of non-split symbol algebras of degree n (where n is a positive integer, $n \geq 3$) over a $p-$ adic field, respectively over a cyclotomic field. In a further research we intend to improve Theorem 3 from this paper, in order to find a class of division symbol algebras of degree n (where $n \in \mathbb{N}^*$, $n \geq 3$) over a cyclotomic field.

Ackowledgement. The author dedicates the article to her late father, hydrologist Constantin Savin.

References

[1] V. Alexandru, N.M. Gosoniu, *Elements of Number Theory* (in Romanian), Ed. Bucharest University (1999).

[2] J. W. S. Cassels, A. Fröhlich (editors), *Algebraic Number Theory (Proceedings of an instructional conference organized by the London Mathematical Society),* Academic Press (1967).

[3] P. Gille, T. Szamuely, *Central Simple Algebras and Galois Cohomology*, Cambridge University Press (2006).

[4] K. Ireland, M. Rosen, *A classical introduction to modern number theory*, Springer-Verlag (1990).

[5] M. Kirschmer, J. Voight, *Algorithmic enumeration of ideal classes for quaternion orders,* SIAM J. Comput. (SICOMP) **39**, no. 5, 1714-1747 (2010) .

[6] D. Kohel, *Quaternion algebras,* echidna.maths.usyd.edu.au/kohel/alg/doc/AlgQuat.pdf

[7] D. Kohel, *Hecke module structure of quaternions,* Proceedings of Class Field Theory - Centenary and Prospect (Tokyo, 1998), K. Miyake, ed., Advanced Studies in Pure Mathematics, **30**, 177-196, (2000).

[8] T. Y. Lam, *Introduction to Quadratic Forms over Fields,* American Mathematical Society (2004).

[9] A. Ledet, *Brauer Type Embedding Problems* , American Mathematical Society (2005).

[10] B. Linowitz, *Selectivity in quaternion algebras*, Journal of Number Theory **132**, pp. 1425-1437 (2012).

[11] J.S. Milne, *Class Field Theory*, http://www.math.lsa.umich.edu/ jmilne.

[12] D. Savin, *About division quaternion algebras and division symbol algebras*, Carpathian Journal of Mathematics, **32(2)**, p. 233-240 (2016).

[13] J. Voight, The Arithmetic of Quaternion Algebras. Available on the author's website: http://www.math.dartmouth.edu/ jvoight/ crmquat/book/quat-modforms-041310.pdf, 2010.

Received: 14.04.2016
Revised: 30.09.2016
Accepted: 22.10.2016

Faculty of Mathematics and Computer Science
Ovidius University,
Bd. Mamaia no.124, Constanta 900527, România
E-mail: `savin.diana@univ-ovidius.ro`