Gulf Journal of Mathematics
Vol 4, Issue 4 (2016) 16-21

QUATERNION ALGEBRAS AND SYMBOL ALGEBRAS OVER ALGEBRAIC NUMBERS FIELD K, WITH THE DEGREE $[K:\mathbb{Q}]$ EVEN

DIANA SAVIN[1]

ABSTRACT. Let F be a quadratic field $\left(F=\mathbb{Q}\left(\sqrt{d}\right)\right.$, where $d\neq 0,1$ is a square-free integer). Let K be the pure algebraic quartic field $K=\mathbb{Q}\left(\sqrt[4]{d}\right)$. In this paper we determine connections between split quaternion algebras over F and split quaternion algebras over K.

1. INTRODUCTION

Let F be an algebraic number field with char$F\neq 2$ and let $H_F(a,b)$ (where $a,b\in F\backslash\{0\}$) be the generalized quaternion algebra over the field F. The quaternion algebra $H_F(a,b)$ is a central simple algebra of dimension 4 over F. If $\{1;i;j;k\}$ is a F-basis for $H_F(a,b)$, the elements of the basis satisfy the relations: $i^2=a$, $j^2=b$, $k=i\cdot j=-j\cdot i$.

Let n be a positive integer, $n\geq 3$, let ξ be a primitive n-th root of unity and let F be a field with char$F$ does not divide n, char$F\neq 2$, and $\xi\in F$. If $a,b\in F\backslash\{0\}$, the algebra A over F generated by elements x and y which satisfy the relations

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

is called a *symbol algebra* (also known as a *power norm residue algebra*) and A is denoted by $\left(\frac{a,\ b}{F,\xi}\right)$ (see [15]). J. Milnor, in [16], calls a such algebra a symbol algebra. For $n=2$, we obtain the quaternion algebra. Symbol algebras are also central simple algebras of dimension n^2 over F.

Many properties of the quaternion algebras and symbol algebras were obtained using the theory of ramification numbers fields and class field theory.

Quaternion algebras or symbol algebras which split over $\mathbb{Q}$ were very much studied in recent years (see Lam's book [11], Pierce's book [17], Szamuely's book [6], Ledet's book [12], [3], [18], [4], [5]).

In the paper [19] 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 $\mathbb{Q}(\xi)$. In the paper [20] we studied quaternion algebras

Date: Accepted: Oct 24, 2016.
* Corresponding author.
2010 *Mathematics Subject Classification.* 15A24; 15A06; 16G30; 11R52; 11R37.
Key words and phrases. Quaternion algebras,Quadratic fields, Quartic fields.

which split over a quadratic field. Using these results, in this paper we study quaternion algebras which split over a pure quartic field.

2. Preliminaries

We recall some definitions and properties of central simple algebras, which will be used in our paper.

Definition 2.1. ([15]). Let $A \neq 0$ be an algebra over the field F. If the equations $ax = b$, $ya = b, \forall a, b \in A, a \neq 0$, have unique solutions, then the algebra A is called *a division algebra.* If A is a finite-dimensional algebra, then A is a division algebra if and only if A is without zero divisors ($x \neq 0, y \neq 0 \Rightarrow xy \neq 0$).

Definition 2.2. ([15]). Let $F \subset K$ be a fields extension and let A be a central simple algebra over the field F. We recall that:
i) A is called *split* by F if A is isomorphic with a matrix algebra over F.
ii) A is called *split* by K and K is called a *splitting field* for A if $A \otimes_F K$ is a matrix algebra over K.

Proposition 2.3. *([6]). Let F be an algebraic numbers field, $a, b \in F\setminus\{0\}$. Then, the quaternion algebra $\mathbb{H}_F(a, b)$ is split if and only if the conic $C(a, b) : ax^2 + by^2 = z^2$ has a rational point over F (i.e. if there are $x_0, y_0, z_0 \in F$ such that $ax_0^2 + by_0^2 = z_0^2$).*

Remark 2.4. ([11], [6]). *Let F be an algebraic numbers field, $a, b \in F\setminus\{0\}$ and let $H_F(a, b)$ be a quaternion algebra over F. Then $H_F(a, b)$ is either split either a division algebra.*

Remark 2.5. ([12]). *Let p be an odd prime positive integer and let ξ be a primitive p-th root of unity. Let F be an algebraic numbers field such that $\xi \in F$. Let $a, b \in F\setminus\{0\}$ and the symbol algebra $\left(\frac{a,\ b}{F,\xi}\right)$. Then, the symbol algebra $\left(\frac{a,\ b}{F,\xi}\right)$ is either split either a division algebra.*

Now, we recall some definitions and results in quaternion algebras.

Definition 2.6. ([10]). Let a, b be two nonzero rational numbers. Let $H_{\mathbb{Q}}(a, b)$ be a quaternion algebra over the rational numbers field $\mathbb{Q}$. R is an *order* in $H_{\mathbb{Q}}(a, b)$ if R is a subring which is a $\mathbb{Z}$ -module of of rank 4.

Definition 2.7. ([10]). Let $\{\alpha_1; \alpha_2; \alpha_3; \alpha_4\}$ be a basis of R and

$$< \alpha, \beta >= Nr(\alpha + \beta) - Nr(\alpha) - Nr(\beta).$$

Then the determinant of the matrix $(< \alpha_i, \alpha_j >)_{i,j=\overline{1,4}}$ is the square of an integer. The *discriminant* of R is the positive integer disc(R) such that

$$det(< \alpha_i, \alpha_j >)_{i,j=\overline{1,4}} = disc(R)^2.$$

The discriminant of the quaternion algebra $H_{\mathbb{Q}}(a, b)$ is defined as the discriminant of a maximal order in $H_{\mathbb{Q}}(a, b)$.

Theorem 2.8. *([13]) (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 2.9. *([8]). 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 $K \hookrightarrow H_F$.*

The next theorem gives us the decomposition of a prime integer p in the ring of integers of a quadratic field.

Theorem 2.10. *([1]). Let $d \neq 0, 1$ be a square-free integer. Let $\mathcal{O}_F$ be the ring of integers of the quadratic field $F = \mathbb{Q}\left(\sqrt{d}\right)$. Let p be a prime integer. Then, we have:*
i) if $p \geq 3$, the Legendre symbol $\left(\frac{d}{p}\right) = 1$ or $p = 2$, $d \equiv 1$ (mod 8), then $p\mathcal{O}_F = P_1 \cdot P_2$, where $P_1, P_2 \in Spec(\mathcal{O}_F)$, $P_1 \neq P_2$, $N(P_1) = N(P_2) = p$;
ii) if $p \geq 3$, $p|d$ or $p = 2$, $d \equiv 2$ or 3 (mod 4), then $p\mathcal{O}_F = P^2$, where $P \in Spec(\mathcal{O}_F)$, $N(P) = p$;
iii) if $p \geq 3$, the Legendre symbol $\left(\frac{d}{p}\right) = -1$ or $p = 2$, $d \equiv 5$ (mod 8), then $p\mathcal{O}_F$ is a prime ideal of $\mathcal{O}_F$.

3. Quaternion algebras over pure quartic fields

In the paper [20] we determined sufficient conditions for a quaternion algebra $H(p, q)$ to split over a quadratic field $K = \mathbb{Q}\left(\sqrt{d}\right)$. We obtained the following results:

Theorem 3.1. *([20], Th. 3.1) Let $d \neq 0, 1$ be a square-free 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.

Corollary 3.2. *([20], Cor. 3.1)Let $d \neq 0, 1$ be a square-free 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 $H_{\mathbb{Q}(\sqrt{d})}(\alpha, p)$ splits.*

In the paper [4] we found a class of symbol algebras which split over a cyclotomic field. We obtained the following results:

Proposition 3.3. *([4], Proposition 4.1) Let ϵ be a primitive root of order 3 of unity and let $K=\mathbb{Q}(\epsilon)$ be the cyclotomic field. Let $\alpha\in K^*$, p be a prime rational integer, $p\neq 3$ and let $L=K(\sqrt[3]{\alpha})$ be the Kummer field such that α is a cubic residue modulo p. Let h_L be the class number of L. Then, the symbol algebras $A=\left(\frac{\alpha,p^{h_L}}{K,\epsilon}\right)$ split.*

Corollary 3.4. *([4], Cor. 4.2) Let q be an odd prime positive integer and ξ be a primitive root of order q of unity and let $K=\mathbb{Q}(\xi)$ be the cyclotomic field. Let $\alpha\in K^*$, p a prime rational integers, $p\neq 3$ and let $L=K(\sqrt[q]{\alpha})$ be the Kummer field such that α is a q power residue modulo p. Let h_L be the class number of L. Then, the symbol algebras $A=\left(\frac{\alpha,p^{h_L}}{K,\xi}\right)$ are split.*

It is known ([11]) that if F is an algebraic number field such that $[F:\mathbb{Q}]$ is odd and $a,b\in\mathbb{Q}\backslash\{0\}$, then the quaternion algebra $H_F(a,b)$ splits if and only if the quaternion algebra $H_{\mathbb{Q}}(a,b)$ splits. This property is not true when $[F:\mathbb{Q}]$ is an even number. For example, with some simple computations using the computer algebra system MAGMA we find that the quaternion algebra $H(2,3)$ does not split over $\mathbb{Q}$ (its discriminant is 6) but it splits over the quadratic field $\mathbb{Q}(\sqrt{45})$. Let p,q be two odd prime integers, $p\neq q$ and $d\neq 0,1$ be a square-free integer. In the following theorem we obtain a connection between: when the quaternion algebra $H(p,q)$ splits over the quadratic field $\mathbb{Q}\left(\sqrt{d}\right)$ and when the same algebra splits over the the pure quartic field $\mathbb{Q}\left(\sqrt[4]{d}\right)$.

Theorem 3.5. *Let $d\neq 0,1$ be a square free integer, $d\not\equiv 1$ (mod 8) and let p,q be two odd prime integers, $p\neq q$. Let F and K be the quadratic field $F=\mathbb{Q}\left(\sqrt{d}\right)$ respectively the pure quartic field $K=\mathbb{Q}\left(\sqrt[4]{d}\right)$. Then, the quaternion algebra $H_F(p,q)$ splits if and only if the quaternion algebra $H_K(p,q)$ splits.*

Proof. " $\Rightarrow$ " It is immediate, according to Proposition 2.3.
" $\Longleftarrow$ " Let $\mathcal{O}_F$ be the ring of integers of the quadratic field $F=\mathbb{Q}\left(\sqrt{d}\right)$ and let $\mathcal{O}_K$ be the ring of integers of the quartic field $K=\mathbb{Q}\left(\sqrt[4]{d}\right)$.
If $H_K(p,q)$ splits, according to Theorem 2.8 and Proposition 2.9 we know that no prime of F which ramifies in $H_F(p,q)$ splits in K. We will prove that no prime of $\mathbb{Z}$ which ramifies in $H_{\mathbb{Q}}(p,q)$ splits in F.
We know that a prime positive integer p' can be ramified in $H_{\mathbb{Q}}(p,q)$ if $p'|2pq$ (see [9], [10], [22]). We know that $\mathcal{O}_F$ and $\mathcal{O}_K$ are Dedekind rings, so, each prime ideal of $\mathbb{Z}$ has a unique decomposition in a product of primes ideals of $\mathcal{O}_F$ (respectively a unique decomposition in a product of primes ideals of $\mathcal{O}_K$). We have the following cases of decomposition of the ideal $p\mathcal{O}_K$, respectively the same cases of decomposition of the ideal $q\mathcal{O}_K$ (see [21]):
Case 1: $p\mathcal{O}_K=P$ where $P\in\mathrm{Spec}(\mathcal{O}_K)$;

Case 2: $p\mathcal{O}_K = P_1^{e_1} \cdot P_2^{e_1} P_3^{e_3}$, where $P_1,\ P_2,\ P_3 \in \text{Spec}(\mathcal{O}_K)$ and $e_1 + e_2 + e_3 = 4$;
Case 3: $p\mathcal{O}_K = P_1 \cdot P_2 \cdot P_3$, where $P_1,\ P_2,\ P_3 \in \text{Spec}(\mathcal{O}_K)$;
Case 4: $p\mathcal{O}_K = P_1 \cdot P_2 \cdot P_3 \cdot P_4$, where $P_1,\ P_2,\ P_3,\ P_4 \in \text{Spec}(\mathcal{O}_K)$;
Case 5: $p\mathcal{O}_K = P^4$ where $P \in \text{Spec}(\mathcal{O}_K)$.
Using the computer algebra system MAGMA we can find immediately some examples of ideals $p\mathcal{O}_K$ in each from these five cases.
Now, we study each of these cases.
Case 1: If $p\mathcal{O}_K = P$, $P \in \text{Spec}(\mathcal{O}_K)$ it results that p is inert in $\mathcal{O}_K$. But, we have the extensions of fields $\mathbb{Q} \subset F \subset K$. This implies that p is inert in $\mathcal{O}_F$. (3.1).
Case 2: If $p\mathcal{O}_K = P_1^{e_1} \cdot P_2^{e_1} \cdot P_3^{e_3}$, where $P_1,\ P_2,\ P_3 \in \text{Spec}(\mathcal{O}_K)$ and $e_1+e_2+e_3 = 4$, we consider for example $p\mathcal{O}_K = P_1^2 \cdot P_2 \cdot P_3$, where $P_1,\ P_2,\ P_3 \in \text{Spec}(\mathcal{O}_K)$. In this case, applying Theorem 2.10, it results that, the decomposition of p in F is the following: $p\mathcal{O}_F = P_1^{'} \cdot P_2^{'}$, where $P_1^{'}, P_2^{'} \in \text{Spec}(\mathcal{O}_F)$ and the decompositions of $P_1^{'}$ and $P_2^{'}$ in $\mathcal{O}_K$ are: $P_1^{'}\mathcal{O}_K = P_1^2$ and $P_2^{'}\mathcal{O}_K = P_2 \cdot P_3$ (or vice versa). In this situation $P_2^{'}$ is ramified in $H_F(p, q)$, but $P_2^{'}\mathcal{O}_K$ splits in $\mathcal{O}_K$. Applying Theorem 2.8 and Proposition 2.9 is results that the quaternion algebra $H_K(p, q)$ does not split, so we cannot have this case. (3.2).
Case 3: If $p\mathcal{O}_K = P_1 \cdot P_2 \cdot P_3$, where $P_1,\ P_2,\ P_3 \in \text{Spec}(\mathcal{O}_K)$, applying Theorem 2.10, it results that $p\mathcal{O}_F = P_1^{'} \cdot P_2^{'}$, where $P_1^{'}, P_2^{'} \in \text{Spec}(\mathcal{O}_F)$ and the decompositions of $P_1^{'}$ and $P_2^{'}$ in $\mathcal{O}_K$ are: $P_1^{'}\mathcal{O}_K = P_1 \cdot P_2$ and $P_2^{'}\mathcal{O}_K = P_3$ (or vice versa). It results $P_1^{'}$ is ramified in $H_F(p, q)$, but $P_1^{'}\mathcal{O}_K$ splits in $\mathcal{O}_K$. According to Theorem 2.8 and Proposition 2.9 it results that the quaternion algebra $H_K(p, q)$ does not split, so we cannot have this case. (3.3).
Case 4: If $p\mathcal{O}_K = P_1 \cdot P_2 \cdot P_3 \cdot P_4$, with $P_1,\ P_2,\ P_3,\ P_4 \in \text{Spec}(\mathcal{O}_K)$, applying Theorem 2.10, it results that $p\mathcal{O}_F = P_1^{'} \cdot P_2^{'}$, where $P_1^{'}, P_2^{'} \in \text{Spec}(\mathcal{O}_F)$ and the decompositions of $P_1^{'}$ and $P_2^{'}$ in $\mathcal{O}_K$ are: $P_1^{'}\mathcal{O}_K = P_1 \cdot P_2$ and $P_2^{'}\mathcal{O}_K = P_3 \cdot P_4$ (or vice versa). So, $P_1^{'}$, $P_2^{'}$ are ramified in $H_F(p, q)$, but $P_1^{'}\mathcal{O}_K$, $P_2^{'}\mathcal{O}_K$ split in $\mathcal{O}_K$. According to Theorem 2.8 and Proposition 2.9 is results that the quaternion algebra $H_K(p, q)$ does not split, so we cannot have this case. (3.4).
Case 5: If $p\mathcal{O}_K = P^4$, with $P \in \text{Spec}(\mathcal{O}_K)$, applying Theorem 2.10, it results that $p\mathcal{O}_F = P_{11}^2$, with $P_{11} \in \text{Spec}(\mathcal{O}_F)$ and $P_{11}\mathcal{O}_K = P^2$. According to Theorem 2.8 and Proposition 2.9, it results the quaternion $H_K(p, q)$ splits and also the quaternion $H_F(p, q)$ splits. (3.5).
From the relations (3.1), (3.2), (3.3), (3.4), (3.5) we obtain that if the quaternion $H_K(p, q)$ splits, then the quaternion $H_F(p, q)$ splits.

□

References

1. S. Alaca, K. Williams, *Introductory algebraic number theory*, Cambridge University Press, 2004.
2. L. El Fadil, *Explicit Factorization of Prime Integers in Quartic Number Fields defined by* $X^4 + aX + b$, http://arxiv.org/pdf/1008.3674.pdf
3. R. Flatley, *Trace forms of Symbol Algebras, Algebra Colloquium*, **19** (2012), 1117-1124.
4. C. Flaut, D. Savin, *Some examples of division symbol algebras of degree 3 and* 5, Carpathian Journal of Mathematics , vol. 31, No. 2 (2015), p. 197-204.

5. C. Flaut, D. Savin, *Quaternion algebras and generalized Fibonacci- Lucas quaternions*, Adv. Appl. Clifford Algebras, vol. **25** issue 4 (2015), p. 853-862.
6. P. Gille, T. Szamuely, *Central Simple Algebras and Galois Cohomology*, Cambridge University Press, 2006.
7. J. Guardia, J. Montes and E. Nart, *Higher Newton polygons in the computation of discriminant and prime ideal decomposition in number fields*, Journal de Theorie des nombres de Bordeaux, vol. **23** issue: 3 (2011), p. 667-696.
8. M. Kirschmer, J. Voight, *Algorithmic enumeration of ideal classes for quaternion orders,* SIAM J. Comput. (SICOMP) **39** (2010), no. 5, 1714-1747.
9. D. Kohel, *Quaternion algebras,* echidna.maths.usyd.edu.au/kohel/alg/doc/ AlgQuat.pdf
10. 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.
11. T. Y. Lam, *Introduction to Quadratic Forms over Fields,* American Mathematical Society, 2004.
12. A. Ledet, *Brauer Type Embedding Problems* , American Mathematical Society, 2005.
13. B. Linowitz, *Selectivity in quaternion algebras*, Journal of Number Theory **132** (2012), pp. 1425-1437.
14. http://magma.maths.usyd.edu.au/magma/handbook/
15. J.S. Milne, *Class Field Theory*, http://www.math.lsa.umich.edu/ jmilne.
16. J. Milnor, *Introduction to Algebraic K-Theory,* Annals of Mathematics Studies, Princeton Univ. Press, 1971.
17. R.S. Pierce, *Associative Algebras*, Springer Verlag, 1982.
18. D. Savin, *About some split central simple algebras*, An. Stiin. Univ. "'Ovidius" Constanta, Ser. Mat, **22** (1) (2014), p. 263-272.
19. D. Savin, *About division quaternion algebras and division symbol algebras*, Carpathian Journal of Mathematics, **32(2)(2016)**, p. 233-240.
20. D. Savin, *About split quaternion algebras over quadratic fields and symbol algebras of degree n*, accepted for publication in Bull. Math. Soc. Sci. Math. Roumanie, (https://arxiv.org/abs/1511.07509).
21. H. Sullivan,*A survey of pure algebraic quartic fields*, master thesis, University of Northern British Columbia, 2012, http://arcabc.ca/islandora/object/unbc
22. 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.

[1] Faculty of Mathematics and Computer Science, Ovidius University of Constanta, Constanta 900527, Bd. Mamaia no.124, România.

E-mail address: savin.diana@univ-ovidius.ro; dianet72@yahoo.com