About division quaternion algebras and division symbol algebras

DIANA SAVIN

ABSTRACT. In this paper, we find a class of division quaternion algebras over the field $\mathbb{Q}(i)$ and a class of division symbol algebras over a cyclotomic field.

1. INTRODUCTION

Let K be a field with *char* $K \neq 2$. Let A be a simple K-algebra and $Z(A)$ be the center of A. We recall that the K- algebra A is called central simple if $Z(A) = K$.
Let n be an arbitrary positive integer, $n \geq 3$ and let ξ be a primitive n-th root of unity. If $char(K)$ does not divide n and $\xi \in K$, let $K^* = K \backslash \{0\}$, $a, b \in K^*$ 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* (also known as a *power norm residue algebra*) and it is denoted by $\left(\frac{a, b}{K, \xi} \right)$. J. Milnor, in [20], calls it the symbol algebra. For $n = 2$, we obtain the quaternion algebra. Quaternion algebras and symbol algebras are central simple algebras. Quaternion algebras and symbol algebras have many applications in number theory (see [8], [10], [13], [14], [21], [23], [24], [25], [26]). Conditions of some algebras to be split or with division were intensively studied in various papers, as for example in the papers [6], [7], [8], [10], [24], [25], in which the authors found some interesting examples of quaternion division algebras and quaternion algebras, respectively symbol algebras which split. In this paper, using some of these results and some properties of quadratic fields, cyclotomic fields and $p-$ adic fields, we find a class of division quaternion algebras over the field $\mathbb{Q}(i)$ (Theorem 3.6) as well as a class of division symbol algebras over a cyclotomic field (Theorem 3.7).

2. PRELIMINARIES

In the following, we assume that K is a commutative field and A is a finite dimensional algebra over K. If A is a central simple $K-$ algebra, then the dimension n of A over K is a square. The positive integer $d = \sqrt{n}$ is called *the degree* of the algebra.
We recall some definitions and properties of the theory of associative algebras, cyclotomic fields and $p-$ adic fields, which will be used in our paper.

Definition 2.1. Let $A \neq 0$ be an algebra over the field K. 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. Let $K \subset L$ be a fields extension and let A be a central simple algebra over the field K. We recall that:
i) A is called *split by* K if A is isomorphic with a matrix algebra over K.
ii) A is called *split by* L and L is called *a splitting field for* A if $A \otimes_K L$ is a matrix algebra over L.

Let $\alpha, \beta \in K^*$. We will denote by $\mathbb{H}_K (\alpha, \beta)$ *the generalized quaternion algebra* over the field K, the algebra of the elements of the form $a = a_1 \cdot 1 + a_2 \cdot e_2 + a_3 \cdot e_3 + a_4 \cdot e_4$, where $a_i \in K, i \in \{1, 2, 3, 4\}$, and the elements of the basis $\{1, e_2, e_3, e_4\}$ satisfy the following multiplication table:

$\cdot$	1	e_2	e_3	e_4
1	1	e_2	e_3	e_4
e_2	e_2	α	e_4	αe_3
e_3	e_3	$-e_4$	β	$-\beta e_2$
e_4	e_4	$-\alpha e_3$	βe_2	$-\alpha\beta$

We denote by $\boldsymbol{n}(a)$ the norm of a generalized quaternion a. This norm has the following expression $\boldsymbol{n}(a) = a_1^2 - \alpha a_2^2 - \beta a_3^2 + \alpha\beta a_4^2$. This algebra is a division algebra if and only if for $x \in \mathbb{H}_K (\alpha, \beta)$ we have $\boldsymbol{n}(x) = 0$ if and only if $x = 0$. Otherwise, the algebra $\mathbb{H}_K (\alpha, \beta)$ is called *a split* algebra. In the books [9], [14], [19], [22], [27] appear the following criterions to decide if a quaternion algebra or a symbol algebra is split.

Proposition 2.1. ([19]) *The quaternion algebra* $\mathbb{H}_K (\alpha, \beta)$ *is a split algebra if and only* β *is a norm from the extension* $K \subseteq K(\sqrt{\alpha})$.

Proposition 2.2. ([9]) *The quaternion algebra* $\mathbb{H}_K (\alpha, \beta)$ *is split if and only if the conic* $C(\alpha, \beta)$: $\alpha x^2 + \beta y^2 = z^2$ *has a rational point over* K(*i.e. if there are* $x_0, y_0, z_0 \in K$ *such that* $\alpha x_0^2 + \beta y_0^2 = z_0^2$).

Theorem 2.1. ([9]) *Let* K *be a field such that* $\zeta \in K$, $\zeta^n = 1, \zeta$ *is a primitive root, and let* $\alpha, \beta \in K^*$. *Then the following statements are equivalent:*
i) *The cyclic algebra* $A = \left(\frac{\alpha, \beta}{K, \zeta} \right)$ *is split.*
ii) *The element* β *is a norm from the extension* $K \subseteq K(\sqrt[n]{\alpha})$.

Theorem 2.2. (**The Wedderburn norm criterion**) ([16]) *Let* n *be a positive integer,* $n \geq 3$ *and let* L/K *be a cyclic fields extension of order* n. *Let* σ *be a generator of the Galois group* $\mathrm{Gal}(L/K)$. *Then* (M, σ, a) *is a division algebra if* a^d *is not a norm in* L/K *for* $d|n, d < n$.

Theorem 2.3. (**Wedderburn**) ([19]) *Let* A *be a central simple algebra over the field* K. *Therefore there are* $n \in \mathbb{N}^*$ *and a division algebra* D, $K \subseteq D$, *such that* $A \simeq \mathcal{M}_n(D)$. *The division algebra* D *is unique up to an isomorphism.*

Theorem 2.4. ([15]) *Let* K *be a field,* n *be an arbitrary positive integer such that* $g.c.d.(n, char K)$ $= 1$ *and* K *contains a primitive root of order* n *of unity.*
i) *Let* L *be a cyclic extension of degree* n. *Then, there is* $\alpha \in K$ *such that* $L = K(\alpha)$ *and* α *satisfies the equation* $x^n - a = 0$ *for some* $a \in K$.
ii) *Conversely, let* $a \in K$ *and* α *be a root of the equation* $x^n - a$. *Then* $K(\alpha)$ *is cyclic over* K, *of degree* d, $d|n$ *and* $\alpha^d \in K$.

In [4] E. Brown and J. Parry determined all imaginary bicyclic biquadratic fields $K = \mathbb{Q}\left(\sqrt{l}, \sqrt{d}\right)$ with class number 1. From these fields, we use in section 3 the imaginary biquadratic number fields $K = \mathbb{Q}\left(\sqrt{l}, \sqrt{d}\right)$ with $l = -1$.

Theorem 2.5. ([4]) *Let $d < -1$ be a square free integer and the biquadratic field $K = \mathbb{Q}\left(i, \sqrt{d}\right)$. Then, the only values of d for which K has class number 1 are:*

$$d \in \{-163, -67, -43, -37, -19, -13, -11, -7, -5, -3, -2\}.$$

3. DIVISION QUATERNION ALGEBRAS AND SYMBOL ALGEBRAS, OVER A QUADRATIC FIELD OR OVER A CYCLOTOMIC FIELD

It is known that a quaternion algebra or a symbol algebra of degree p (with p a prime number) is either split or a division algebra (see [14], [16]).

In the papers [8], [24], we found some examples of split quaternion and symbol algebras over a quadratic field or over a cyclotomic field. We obtained the following results:

Proposition 3.3. ([24]) *Let p be a prime positive integer, $p \equiv 1(\bmod\ 3)$ and let $K = \mathbb{Q}\left(\sqrt{3}\right)$. Then the quaternion algebra $\mathbb{H}_K(-1, p)$ is a split algebra.*

Proposition 3.4. ([24]) *Let ϵ be a primitive root of order 3 of the unity. Then the algebras $A = \left(\frac{\alpha, \beta}{\mathbb{Q}(\epsilon), \epsilon}\right)$, for $\alpha, \beta \in \{-1, 1\}$ are split algebras.*

Let ϵ be a primitive root of order 3 of the unity and $\mathbb{Q}(\epsilon)$ be the cyclotomic field. In the paper [8] using the computer algebra system MAGMA, we obtained that the symbol algebras $\left(\frac{7, 11^3}{\mathbb{Q}(\epsilon), \epsilon}\right)$, $\left(\frac{7, (11+\epsilon)^3}{\mathbb{Q}(\epsilon), \epsilon}\right)$, $\left(\frac{7, 5^3}{\mathbb{Q}(\epsilon), \epsilon}\right)$ are split algebras and the class number of the Kummer field $\mathbb{Q}\left(\epsilon, \sqrt[3]{7}\right)$ is 3. Moreover, in the paper [8], we found a class of split symbol algebras, over a cyclotomic field.

Proposition 3.5. ([8]) *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 be a prime rational integer, $p \neq 3$ 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.*

In this paper we find a class of quaternion division algebras or division symbol algebras over a p-adic field, over a quadratic field or over a cyclotomic field.

We consider the quadratic field $\mathbb{Q}(i)$ $(i^2 = -1)$ and the cyclotomic field $\mathbb{Q}(\epsilon)$, where ϵ is a primitive root of order 3 of the unity. Using the computer algebra system MAGMA, we found some examples of division quaternion algebras over the quadratic field $\mathbb{Q}(i)$ and some examples of division symbol algebras over the cyclotomic field field $\mathbb{Q}(\epsilon)$.

For example, we declare (in input) the quadratic field $E := \mathbb{Q}(i)$, the biquadratic field $K := \mathbb{Q}\left(i, \sqrt{10}\right)$ and the quaternion algebra $A := \mathbb{H}_{\mathbb{Q}(i)}(10, 29)$. In output, with the procedure *NormEquation*(K, 29) we test if 29 is or not a norm of an element from the biquadratic field K. We obtain that 10 is not a quadratic residue modulo 29, $29 \equiv 1\ (\bmod\ 4)$ and 29 is not a norm from the extension $\mathbb{Q}(i) \subseteq \mathbb{Q}\left(i, \sqrt{10}\right)$. Using similar calculations in Magma we obtain that 15 is not a quadratic residue modulo 29, 29 is not a norm from the extension $\mathbb{Q}(i) \subseteq \mathbb{Q}\left(i, \sqrt{15}\right)$ and 5 is a quadratic residue modulo 29, 29 is a norm from the extension $\mathbb{Q}(i) \subseteq \mathbb{Q}\left(i, \sqrt{5}\right)$. So, applying Proposition 2.1 it results that the quaternion algebras $\mathbb{H}_{\mathbb{Q}(i)}(10, 29)$, $\mathbb{H}_{\mathbb{Q}(i)}(15, 29)$ are division algebras and the quaternion algebra $\mathbb{H}_{\mathbb{Q}(i)}(5, 29)$ is a split algebra.

Using similar calculations in Magma (for symbol algebras), it results that 29 is a norm

from the extension $\mathbb{Q}\left(\epsilon\right) \subseteq \mathbb{Q}\left(\epsilon, \sqrt[3]{7}\right)$, but $43; 13; 19$ are not norms from the extension $\mathbb{Q}\left(\epsilon\right) \subseteq \mathbb{Q}\left(\epsilon, \sqrt[3]{7}\right)$. So, applying Theorem 2.1 or Theorem 2.2, it results that the symbol algebra $\left(\frac{7,29}{\mathbb{Q}(\epsilon),\epsilon}\right)$ is a split algebra, but $\left(\frac{7,43}{\mathbb{Q}(\epsilon),\epsilon}\right)$, $\left(\frac{7,13}{\mathbb{Q}(\epsilon),\epsilon}\right)$, $\left(\frac{7,19}{\mathbb{Q}(\epsilon),\epsilon}\right)$ are division algebras. We remark that $29 \equiv 2 \pmod{3}$, but $43; 13; 19 \equiv 1 \pmod 3$.

Let ω be a primitive root of order 5 of the unity and let the cyclotomic field $\mathbb{Q}\left(\omega\right)$. Similarly with previous examples, using the computer algebra system MAGMA, we obtain that the symbol algebra $\left(\frac{19,37}{\mathbb{Q}(\omega),\omega}\right)$ is a split symbol algebra, but $\left(\frac{19,11}{\mathbb{Q}(\omega),\omega}\right)$, $\left(\frac{19,31}{\mathbb{Q}(\omega),\omega}\right)$ are division symbol algebras. We remark that $37 \equiv 2 \pmod 5$, but $11; 31 \equiv 1 \pmod 5$.

Considering these things, we obtain the following results. In these results we use the notations: $(\cdot,\cdot)_p$ for the Hilbert symbol in the $p-$ adic field $\mathbb{Q}_p$, $\epsilon\left(\frac{\cdot,\cdot}{K}\right)_v$ for the Hasse invariant at a place v of a field K, $\left(\frac{\cdot}{p}\right)$ for the Legendre symbol in $\mathbb{Z}$, respectively $\left[\frac{\cdot}{p}\right]$ for the Legendre symbol in $\mathbb{Z}\left[i\right]$.

Theorem 3.6. *Let p be a prime positive integer such that $p \equiv 1$ (mod 4) and let the quadratic field $\mathbb{Q}\left(i\right)$ ($i^2 = -1$). Let α be an integer which is not a quadratic residue modulo p. Then the quaternion algebra $\mathbb{H}_{\mathbb{Q}(i)}\left(\alpha, p\right)$ is a division algebra.*

Proof. Since α is not a quadratic residue modulo p, it results that $\overline{\alpha}\notin\left(\mathbb{F}_p^*\right)^2$. Therefore, $\mathbb{F}_p\left(\sqrt{\alpha}\right)/\mathbb{F}_p$ is a cyclic extension of degree 2. From Hensel 's lemma ([1], [3]), we know that the $p-$ adic field $\mathbb{Q}_p$ contains the roots of order $p - 1$ of the unity. Since $p \equiv 1$ (mod 4), we have that $i\in\mathbb{Q}_p$, therefore $\mathbb{Q}\left(i\right) \subset \mathbb{Q}_p$. We consider the quaternion algebra $\mathbb{H}_{\mathbb{Q}(i)}\left(\alpha, p\right) \otimes_{\mathbb{Q}(i)} \mathbb{Q}_p = \mathbb{H}_{\mathbb{Q}_p}\left(\alpha, p\right)$.

We consider the equation $\alpha x^2 + py^2 = z^2$. We calculate the Hilbert symbol in $\mathbb{Q}_p : (\alpha, p)_p$. Since α is not a quadratic residue modulo p, it results that p does not divide α. Therefore $(\alpha, p)_p = \left(\frac{\alpha}{p}\right) = -1$. This implies that the equation $\alpha x^2 + py^2 = z^2$ does not have solutions in the p-adic field $\mathbb{Q}_p$. Applying Proposition 2.2, it results that $\mathbb{H}_{\mathbb{Q}_p}\left(\alpha, p\right)$ is not split, therefore $\mathbb{H}_{\mathbb{Q}_p}\left(\alpha, p\right)$ is a division algebra. This implies that $\mathbb{H}_{\mathbb{Q}(i)}\left(\alpha, p\right)$ is a division algebra. $\qquad\square$

A question which appears in the following is: what happens with the quaternion algebra $\mathbb{H}_{\mathbb{Q}(i)}\left(\alpha, p\right)$ when α is a quadratic residue modulo p. Using Theorem 2.5, the decomposition of a prime integer in the ring of integers of a biquadratic field (see [18], [17]) and a reasoning similar to that which we used in the proof of Proposition 3.5 (see [8]) we obtain:

Proposition 3.6. *Let $\alpha\in \{\pm2, \pm3, \pm5, \pm7, \pm11, \pm13, \pm19, \pm37, \pm43, \pm67, \pm163\}$ and let p be an odd prime positive integer such that $|\alpha|$ is a quadratic residue modulo p and let the quadratic field $\mathbb{Q}\left(i\right)$ ($i^2 = -1$). Then the quaternion algebra $\mathbb{H}_{\mathbb{Q}(i)}\left(\alpha, p\right)$ is a split algebra.*

Proof. Our first remark is the fact that for every α from the set $\{\pm2, \pm3, \pm5, \pm7, \pm11, \pm13, \pm19, \pm37, \pm43, \pm67, \pm163\}$ there exists an odd prime positive integer p such that $|\alpha|$ is quadratic residue modulo p.

Let $\mathcal{O}_K$ be the ring of integers of the biquadratic field $K = \mathbb{Q}\left(i, \sqrt{\alpha}\right) = \mathbb{Q}\left(i, \sqrt{-\alpha}\right)$. From Theorem 2.5 follows immediately that $\mathcal{O}_K$ is a principal ring. We know that, if $p \equiv 1$ (mod 4), then p splits in the ring $\mathbb{Z}\left[i\right]$ in a product of two primes from $\mathbb{Z}\left[i\right]$, respectively, if $p \equiv 3$ (mod 4), then p is inert in the ring $\mathbb{Z}\left[i\right]$.

Case 1: if $p \equiv 1$ (mod 4). We know that $\mathbb{Z}\left[i\right]$ is a principal ring. So, we have:

$$p\mathbb{Z}\left[i\right] = p_1\mathbb{Z}\left[i\right] p_2\mathbb{Z}\left[i\right],$$

where p_1, p_2 are prime elements from $\mathbb{Z}[i]$. Since $|\alpha|$ is a quadratic residue modulo p, it results that $|\alpha|$ is a quadratic residue modulo p_1, p_2. So, we obtain the following decomposition of the ideal $p\mathcal{O}_K$:

$$p\mathcal{O}_K = P_{11}P_{12}P_{21}P_{22},$$

where P_{i1} and P_{i2}, $i = \overline{1,2}$ are prime, principal conjugate ideals from the ring $\mathcal{O}_K$. It results that $p = N_{K/\mathbb{Q}(i)}(P_{11})$. But P_{11} is a principal ideal, therefore, there exists $a \in K$ such that $p = N_{K/\mathbb{Q}(i)}(a)$. Applying Proposition 2.1 it results that the quaternion algebra $\mathbb{H}_{\mathbb{Q}(i)}(\alpha, p)$ is a split algebra.

Case 2: if $p \equiv 3$ (mod 4), we know that p is inert in the ring $\mathbb{Z}[i]$ and having in view that $|\alpha|$ is quadratic residue modulo p, we obtain that $p\mathcal{O}_K = P_1 P_2$, where P_i, $i = \overline{1,2}$ are prime, principal conjugate ideals from the ring $\mathcal{O}_K$. Similarly with the case 1, we obtain that the quaternion algebra $\mathbb{H}_{\mathbb{Q}(i)}(\alpha, p)$ is a split algebra. $\qquad\square$

In the case when p' is a prime positive integer, $p' \equiv 1$ (mod 4), we obtain the result:

Proposition 3.7. *Let p' be a prime positive integer such that $p' \equiv 1$ (mod 4) and let the quadratic field $\mathbb{Q}(i)$ ($i^2 = -1$). Let α be an integer such that each divisor of α is a quadratic residue modulo p'. Then the quaternion algebra $\mathbb{H}_{\mathbb{Q}(i)}\left(\alpha, p'\right)$ is a split algebra.*

Proof. We prove that the equation $\alpha x^2 + p' y^2 = z^2$ has solutions over $\mathbb{Q}(i)$. For this we determine the ramified primes in the quaternion algebra $\mathbb{H}_{\mathbb{Q}(i)}\left(\alpha, p'\right)$. It is known that a such prime p divides $2\alpha p'$ ([11], [12], [26]). Since $p' \equiv 1$ (mod 4) it results that $p'\mathbb{Z}[i] = p'_1\mathbb{Z}[i] \cdot p'_2\mathbb{Z}[i]$, where $p'_1\mathbb{Z}[i], p'_2\mathbb{Z}[i] \in \mathrm{Spec}(\mathbb{Z}[i])$.

We calculate the Hasse invariant: $\epsilon\left(\frac{\alpha, p'}{\mathbb{Q}(i)}\right)_{p'_j} = \left[\frac{\alpha}{p'_j}\right] = 1$, $j = \overline{1,2}$. It results that p'_1, p'_2 are not ramified in $\mathbb{H}_{\mathbb{Q}(i)}\left(\alpha, p'\right)$.

Case 1: if $2 \nmid \alpha$.

Let $\alpha = q_1^{\beta_1} \cdot q_2^{\beta_2} \cdot \ldots \cdot q_r^{\beta_r}$, where r is a natural number, q_j, $j = \overline{1,r}$ are odd prime integers and $\beta_j \in \mathbb{N}^*$, for $j = \overline{1,r}$.

Let $p \in \{q_1, q_2, ..., q_r\}$. From hypothesis, it results that $p \equiv 3$ (mod 4) or $p \equiv 1$ (mod 4).

If $p \equiv 3$ (mod 4), it results that p remains prime in the ring $\mathbb{Z}[i]$. Using the properties of the Hasse invariant we obtain:

(3.1)
$$\epsilon\left(\frac{\alpha, p'}{\mathbb{Q}(i)}\right)_p = \prod_{k=1, k \neq j}^{r} \epsilon\left(\frac{q_k^{\beta_k}, p'}{\mathbb{Q}(i)}\right)_p \cdot \epsilon\left(\frac{p^{\beta_j}, p'}{\mathbb{Q}(i)}\right)_p =$$

$$= \left(\epsilon\left(\frac{p, p'}{\mathbb{Q}(i)}\right)_p\right)^{\beta_j} = \left[\frac{p'}{p}\right]^{\beta_j}.$$

Since $p' \equiv 1$ (mod 4), it results that $p'\mathbb{Z}[i] = p'_1\mathbb{Z}[i] \cdot p'_2\mathbb{Z}[i]$, where $p'_1\mathbb{Z}[i], p'_2\mathbb{Z}[i]$ are prime ideals in $\mathbb{Z}[i]$ and $p'_2 = \overline{p'_1}$.

Taking into account (3.1) we obtain:

$$\epsilon\left(\frac{\alpha, p'}{\mathbb{Q}(i)}\right)_p = \left[\frac{p'_1}{p}\right]^{\beta_j} \cdot \left[\frac{p'_2}{p}\right]^{\beta_j} = 1.$$

So, each divisor $p \equiv 3$ (mod 4) of α does not ramify in $\mathbb{H}_{\mathbb{Q}(i)}\left(\alpha, p'\right)$.

If $p \equiv 1$ (mod 4), it results that $p\mathbb{Z}[i] = p_1\mathbb{Z}[i] \cdot p_2\mathbb{Z}[i]$, where $p_1\mathbb{Z}[i], p_2\mathbb{Z}[i] \in \mathrm{Spec}(\mathbb{Z}[i])$.

Analogously to the previous considerations, we obtain the Hasse invariant $\epsilon \left(\frac{\alpha, p'}{\mathbb{Q}(i)} \right)_{p_1} =$ $\epsilon \left(\frac{\alpha, p'}{\mathbb{Q}(i)} \right)_{p_2} = 1$. So, p_1, p_2 do not ramify in $\mathbb{H}_{\mathbb{Q}(i)} \left(\alpha, p' \right)$.

Case 2: if $2 | \alpha$.

We know that $2 = -i \left(1 + i \right)^2$, $1 + i$ is a prime element in $\mathbb{Z}[i]$, $i \in U(\mathbb{Z}[i])$. Considering the results obtained in case 1 and that $\prod_{p} \epsilon \left(\frac{\alpha, p'}{\mathbb{Q}(i)} \right)_p = 1$, it results that $\epsilon \left(\frac{\alpha, p'}{\mathbb{Q}(i)} \right)_{1+i} = 1$. So, $1 + i$ does not ramify in $\mathbb{H}_{\mathbb{Q}(i)} \left(\alpha, p' \right)$.

From the previously proved, applying Minkovski-Hasse theorem we get that the equation $\alpha x^2 + p' y^2 = z^2$ has solutions over $\mathbb{Q}(i)$, so applying Proposition 2.2 it results that $\mathbb{H}_{\mathbb{Q}(i)} \left(\alpha, p' \right)$ is a split algebra.

We wonder if the quaternion algebra $\mathbb{H}_{\mathbb{Q}} \left(\alpha, p \right)$ is a split algebra when p is a prime positive integer, $p \equiv 1 \pmod 4$ and α is an integer such that α is a quadratic residue modulo p. When a F- quaternion algebra splits over a quadratic field $F \left(\sqrt{w} \right)$, in paper [5] are given sufficient conditions for the F- quaternion algebra splits over F. But these conditions are given only when w is totally positive; this is not our situation (when $F \left(\sqrt{w} \right) = \mathbb{Q}(i)$). When α is also prime, in [2] is realized a classification of quaternion algebras $\mathbb{H}_{\mathbb{Q}} \left(\alpha, p' \right)$ (in split algebras, respectively division algebras) after congruences satisfied by into α and p'.

Making some computations in Magma we obtain that the answer at our question is negative. For example, if $\alpha = 33 \, p = 29$, we have that $29 \equiv 1 \pmod 4$ and 33 is a quadratic residue modulo 29. Using Magma we obtain that the discriminant (in fact the generator of this discriminant) of the quaternion algebra $\mathbb{H}_{\mathbb{Q}(i)} \left(33, 29 \right)$ is 1, so the algebra $\mathbb{H}_{\mathbb{Q}(i)} \left(33, 29 \right)$ splits, but the discriminant of the quaternion algebra $\mathbb{H}_{\mathbb{Q}} \left(33, 29 \right)$ is 33, so the $\mathbb{H}_{\mathbb{Q}} \left(33, 29 \right)$ is a division algebra. All ramified primes in the algebra $\mathbb{H}_{\mathbb{Q}} \left(33, 29 \right)$ are 3 and 11 and we remark that 3 and 11 are not quadratic residues modulo 29. In another example: if $\alpha = 35$, $p = 29$ we obtain that the quaternion algebra $\mathbb{H}_{\mathbb{Q}(i)} \left(35, 29 \right)$ splits, also the quaternion algebra $\mathbb{H}_{\mathbb{Q}} \left(35, 29 \right)$ splits; 35 is a quadratic residue modulo 29 and 5; 7 are also quadratic residues modulo 29. Considering these things, we get the following result. $\square$

Proposition 3.8. *Let p' be a prime positive integer such that $p' \equiv 1$ (mod 4). Let α be an integer such that each divisor of α is a quadratic residue modulo p'. Then the quaternion algebra $\mathbb{H}_{\mathbb{Q}} \left(\alpha, p' \right)$ is a split algebra.*

Proof. The proof is similar to the proof of Proposition 3.7. The only difference is when instead of the relation (3.1) from the proof of Proposition 3.7 appears the following situation (using the properties of the Hilbert symbol):

$$\left(\alpha, p' \right)_p = \prod_{k=1, k \neq j}^{r} \left(q_k^{\beta_k}, p' \right)_p \cdot \left(p^{\beta_j}, p' \right)_p = \left(\left(p, p' \right)_p \right)^{\beta_j} = \left(\frac{p'}{p} \right)^{\beta_j}.$$

Since $p' \equiv 1 \pmod 4$, applying quadratic reciprocity law, it results $\left(\frac{p'}{p} \right) = \left(\frac{p}{p'} \right)$. Since each divisor of α is a quadratic residue modulo p', it results that $\left(\frac{p}{p'} \right) = 1$. We obtain that $\left(\alpha, p' \right)_p = 1$ so, each divisor $p \equiv 3 \pmod 4$ of α does not ramify in $\mathbb{H}_{\mathbb{Q}} \left(\alpha, p' \right)$. $\square$

Now, we generalize Theorem 3.6 for symbol algebras.

Theorem 3.7. *Let p and q be prime positive integers such that $p \equiv 1 \pmod{q}$, ξ be a primitive root of order q of unity and let $K = \mathbb{Q}(\xi)$ be the cyclotomic field. Then there is an integer α not divisible by p whose residue class mod p does not belongs to $\left(\mathbb{F}_p^*\right)^q$ and for every such an α, we have:*
i) the algebra $A \otimes_K \mathbb{Q}_p$ is a division algebra over $\mathbb{Q}_p$, where A is the symbol algebra $A = \left(\frac{\alpha, p}{K, \xi}\right)$;
ii) the symbol algebra A is a division algebra over K.

Proof. Let be the homomorphism $f : \mathbb{F}_p^* \to \mathbb{F}_p^*$, $f(x) = x^q$. Since q divides $p - 1$, it results $Ker(f) = \left\{x \in F_p^* | x^q \equiv 1 \pmod{p}\right\}$ 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 belongs to $\left(\mathbb{F}_p^*\right)^q$. So, $\mathbb{F}_p \subset \mathbb{F}_p\left(\sqrt[q]{\alpha}\right)$.

The extension of fields $\mathbb{F}_p\left(\sqrt[q]{\alpha}\right)/\mathbb{F}_p$ is a cyclic extension of degree q. Applying Hensel 's lemma and the fact that $p \equiv 1 \pmod{q}$, it results that $\mathbb{Q}_p$ contains the q-th roots of the unity, therefore $\mathbb{Q}(\xi) \subset \mathbb{Q}_p$. We consider the symbol algebra $A \otimes_K \mathbb{Q}_p = \left(\frac{\alpha, p}{\mathbb{Q}_p, \xi}\right)$. Applying Theorem 2.4, it results that the extension $\mathbb{Q}_p\left(\sqrt[q]{\alpha}\right)/\mathbb{Q}_p$ is a cyclic unramified extension of degree q, therefore a norm of an element from this extension can be a positive power of p, but can not be p. Applying Theorem 2.1, we get that $\left(\frac{\alpha, p}{\mathbb{Q}_p, \xi}\right)$ is not a split algebra, therefore it is a division algebra. This implies that A is a symbol division algebra. $\qquad\square$

Conclusions. In this paper we found a class of quaternion division algebras or division symbol algebras over a p-adic field, over a quadratic field or over a cyclotomic field.

Using the computer algebra system MAGMA over the quadratic field $\mathbb{Q}(i)$ $(i^2 = -1)$ and the cyclotomic field $\mathbb{Q}(\epsilon)$, where ϵ is a primitive root of order 3 of the unity, we obtain very good examples which allowed us to find conditions in Theorem 3.6, Proposition 3.6, Proposition 3.7, Proposition 3.8 and Theorem 3.7.

REFERENCES

[1] Alexandru, V. and Gosoniu, N. M., *Elements of Number Theory* (in Romanian), Ed. Bucharest University, 1999
[2] Alsina, M. and Bayer, P., *Quaternion Orders, Quadratic Forms and Shimura Curves*, CRM Monograph Series, **22**, American Mathematical Society, 2004
[3] Borevich, Z. I. and Shafarevich, I. R., *Number Theory*, Academic Press Inc, New York, 1966
[4] Brown, E. and Parry, C. J., *The imaginary bicyclic biquadratic fields with class - number* 1, J. Reine Angew Math., **226** (1974), 118–120
[5] Elman, R. and Lam, T. Y., *Classification theorems for quadratic forms over fields*, Comment. Math. Helv., **49** (1974), 373–381
[6] Flaut, C., *Division algebras with dimension* 2^t, $t \in \mathbb{N}$, An. Sti. U. Ovid. Co-Mat., **13** (2005), No. 2, 31–38
[7] Flaut, C. and Savin, D., *Some properties of symbol algebras of degree three*, Math. Rep. (Bucur.), **16(66)** (2014), No. 3, 443–463

[8] Flaut, C., Savin, D., *Some examples of division symbol algebras of degree* 3 *and* 5, Carpathian J. Math., **31** (2015), No. 2, 197–204

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

[10] Kyrchei, I., *The column and row immanants over a split quaternion algebra*, Adv. Appl. Clifford Algebr, **25** (2015), No. 3, 611–619

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

[12] Kohel, D., *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

[13] Kohel, D., Lauter, K., Petit, C. and Tignol, J.-P., *On the quaternion ℓ-isogeny path problem*, LMS J. Comput. Math., **17** (2014), 418–432

[14] Lam, T. Y., *Introduction to Quadratic Forms over Fields*, AMS, 2004

[15] Lang, S., *Algebra*, Springer-Verlag, 2002

[16] Ledet, A., *Brauer Type Embedding Problems*, American Mathematical Society, 2005

[17] Lemmermeyer, F., *Reciprocity laws, from Euler to Eisenstein*, Springer, 2000

[18] Marcus, D., *Number fields*, Universitext, 1995

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

[20] Milnor, J., *Introduction to Algebraic K-Theory,* , Annals of Mathematics Studies, Princeton Univ. Press, 1971

[21] Olteanu, G., *Baer-Galois connections and applications*, Carpathian J. Math., **30** (2014), No. 2, 225–229

[22] Pierce, R. S., *Associative Algebras*, Springer Verlag, 1982

[23] Ramirez, J. L., *Some combinatorial properties of the k-Fibonacci and the k-Lucas quaternions*, An. tiin. Univ. "Ovidius" Constana Ser. Mat., **23** (2015), No. 2, 201–212

[24] Savin, D., Flaut, C. and Ciobanu, C., *Some properties of the symbol algebras*, Carpathian J. Math. , **25** (2009), No. 2, 239–245 (arXiv:0906.2715)

[25] Savin, D., *About some split central simple algebras*, An. Stiin. Univ. "'Ovidius" Constanta, Ser. Mat, **22** (2014), No. 1, 263–272

[26] Vigneras, M. F., *Arithmetique des alg'ebres de quaternions*, Lecture Notes in Math., No. 800, Springer, 1980

[27] Voight, J., *The Arithmetic of Quaternion Algebras*, available on the website: http://www.math. dartmouth.edu/ jvoight/crmquat/book/quat-modforms-041310.pdf, 2010

DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE
OVIDIUS UNIVERSITY
BD. MAMAIA 124, 900527 CONSTANTA, ROMANIA
E-mail address: savin.diana@univ-ovidius.ro, http://www.univ-ovidius.ro/math/