Bulletin of the *Transilvania* University of Braşov • Vol 7(56), No. 2 - 2014
Series III: Mathematics, Informatics, Physics, 59-64

ABOUT QUATERNION ALGEBRAS AND SYMBOL ALGEBRAS

Cristina FLAUT [1] **and Diana SAVIN** [2]

Communicated to:
International Conference on Mathematics and Computer Science ,
June 26-28, 2014, Braşov, Romania

Abstract

Symbol algebras have many applications in various domains of mathematics, as for example number theory (class field theory).
Since these algebras are a natural generalization of the quaternion algebras, in this short survey we present some properties of the quaternion algebras and of the symbol algebras of prime degree.

2010 *Mathematics Subject Classification:* 11A41, 11R04, 11R18, 11R37, 11R52, 11S15, 11F85.
Key words: quaternion algebras, symbol algebras, cyclotomic fields, Kummer fields

1 Preliminaries

Let K be a field whose $char(K)$ does not divide n, where n is an arbitrary positive integer, $n \geq 3$, Let ξ be a primitive n-th root of unity such that $\xi \in K$. 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 [13], calls it *symbol algebra*. For $n = 2$, we obtain the quaternion algebra.
Let L be a field such that all vector spaces over L are finite dimensional. Let B

[1]Faculty of Mathematics and Informatics, *Ovidius* University of Constanta, Romania, e-mail: cflaut@univ-ovidius.ro
[2]Faculty of Mathematics and Informatics, *Ovidius* University of Constanta, Romania, e-mail: savin.diana@univ-ovidius.ro, corresponding author

be a simple L-algebra and $Z(B)$ be the centre of B. We recall that the L- algebra B is called central simple if $Z(B) = L$.
Quaternion algebras and symbol algebras are central simple algebras. We recall some definitions and properties used in the theory of associative algebras.

Proposition 1.1. ([12]) *If K is an algebraic number field and A is a central simple $K-$algebra, then the dimension of A over K is a square.*

Definition 1.1. *Let A be a central simple algebra of finite dimension n over K. The positive integer $d = \sqrt{n}$ is called* ***the degree*** *of algebra A.*

Definition 1.2. *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 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 ($x \neq 0, y \neq 0 \Rightarrow xy \neq 0$)* (See [17]).

Definition 1.3. *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 K be a field with $charK \neq 2$. The generalized quaternion algebras is a division algebra if and only if for $x \in \mathbb{H}_K(\alpha, \beta)$ we have that the norm $n(x) = 0$ if and only if $x = 0$. Otherwise, the algebra $\mathbb{H}_K(\alpha, \beta)$ is called *a split* algebra.
In [7] the following criteria appear for deciding if a quaternion algebra or a symbol algebra is split.

Proposition 1.2. ([7]) *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 1.1. ([7]) *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 1.2 (**Weddeburn**) ([14]) *Let A be a central simple algebra over the field K. 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.*

Definition 1.4. *With the above notations, the degree of the algebra D over K (as an algebra) is called* ***the index*** *of the algebra A.*

For some $h \in N^*$, the tensor product $A \otimes ... \otimes A$ ($h-$ times), over the field K, is isomorphic to a full matrix algebra over K.

Definition 1.5.([1]) The smallest h with the above property is called ***the exponent*** *of the algebra A.*

Theorem 1.3.([1]) *The algebra A is a division algebra if and only if its index and its degree are the same.*

Theorem 1.4. (Brauer-Hasse-Noether).([14]) *Every central simple algebra over an algebraic number field is cyclic and its index is equal to its exponent.*

2 Generalized quaternion algebras $\mathbb{H}_{\mathbb{Q}}(n,p)$, $p,n \in \mathbb{Z}^*$, p is an odd prime

It is known that a quaternion algebra is either division algebra or a split algebra. In the following, we present some conditions for the quaternion algebras $\mathbb{H}_{\mathbb{Q}}(n,p)$, $p \in \mathbb{N}^*$, p is an odd prime, $n \in \mathbb{Z}^*$ be split or with division. For $n \in \{-1,-2\}$, we have the answer in the following propositions.

Proposition 2.1 ([9]) *Let p be a prime positive integer. Therefore:*
i) *The algebra* $\mathbb{H}_{\mathbb{Q}}(-1,p)$ *is a split algebra if and only if* $p \equiv 1$ *(mod* 4*).*
ii) *The algebra* $\mathbb{H}_{\mathbb{Q}}(-2,p)$ *is a split algebra if and only if* $p \equiv 1$ *or* 3 *(mod* 8*).*

In paper [16], we obtained a necessary and sufficient condition such that the algebras $\mathbb{H}_{\mathbb{Q}}(n,p)$, be split algebras, where $n \in \{-13,-7,-5,-3\}$, $p \in \mathbb{N}^*$, p is an odd prime.

Using the Minkovski-Hasse theorem ([2]), Proposition 1.2 and some results about quaternion algebras and about primes of the form $p = x^2 + ny^2$, with $x,y \in \mathbb{Z}$ (see [3], [9], [16], [18]), we obtained the following result:

Proposition 2.2 ([16]) Let p be an odd positive prime integer and let K be an algebraic number field such that $[K:\mathbb{Q}]$ is odd. The following statements hold true:
i) the algebra $\mathbb{H}_K(-3,p)$ splits if and only if the algebra $\mathbb{H}_{\mathbb{Q}}(-3,p)$ splits if and only if $p = x^2 + 3y^2$ for some $x,y \in \mathbb{Z}$;
ii) the algebra $\mathbb{H}_K(-5,p)$ splits if and only if the algebra $\mathbb{H}_{\mathbb{Q}}(-5,p)$ splits if and only if $p = x^2 + 5y^2$ for some $x,y \in \mathbb{Z}$;
iii) the algebra $\mathbb{H}_K(-7,p)$ splits if and only if the algebra $\mathbb{H}_{\mathbb{Q}}(-7,p)$ splits if and only if $p = x^2 + 7y^2$ for some $x,y \in \mathbb{Z}$;
iv) the algebra $\mathbb{H}_K(-13,p)$ splits if and only if the algebra $\mathbb{H}_{\mathbb{Q}}(-13,p)$ splits if and only if $p = x^2 + 13y^2$ for some $x,y \in \mathbb{Z}$.

3 Some examples of split quaternion and split symbol algebras over a quadratic field or over a cyclotomic field

In our previous works, we tried to find examples of split quaternion and split symbol algebras over an extension of the field of the rational numbers.

We obtained the following results:

Proposition 3.1 ([15]) *Let p be a prime positive integer, $p \equiv 1 (\ mod\ 3)$ and let $K = \mathbb{Q}\left(\sqrt{3}\right)$. Then the quaternion algebra $\mathbb{H}_K(-1,p)$ is a split algebra.*

Proof. According to Proposition 1.2, $\mathbb{H}_{\mathbb{Q}\left(\sqrt{3}\right)}(-1,p)$ is a split algebra if and only if the associated conic $-x^2 + py^2 = z^2$ has $\mathbb{Q}\left(\sqrt{3}\right) -$ rational points. Using the Gauss's theorem, there are $a, b \in \mathbb{Z}$ such that $4p = a^2 + 27b^2$. Then, the point $(x_0, y_0, z_0) = \left(\frac{3\sqrt{3}b}{2}, 1, \frac{a}{2}\right)$ is a $\mathbb{Q}\left(\sqrt{3}\right) -$ rational point for the associated conic.$\square$

Proposition 3.2. ([15]) *Let ϵ be a primitive root of order 3 of the unity. Then, the symbol algebras $A = \left(\frac{\alpha,\beta}{\mathbb{Q}(\varepsilon),\varepsilon}\right)$, for $\alpha, \beta \in \{-1, 1\}$ are not division algebras.*

It is known that a symbol algebra of degree p is either split or a division algebra (see [10]), so the symbol algebra from the Proposition 3.2. is a split algebra.

Example. (See [15], [4]) For $\alpha = -1$ and $\beta = 1$ the algebra $A = \left(\frac{\alpha,\beta}{\mathbb{Q}(\varepsilon),\varepsilon}\right)$ is generated, for example, by the elements $X = \begin{pmatrix} -1 & 0 & 0 \\ 0 & -\varepsilon & 0 \\ 0 & 0 & -\varepsilon^2 \end{pmatrix}, Y = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$, where $X^3 = -I_3$, $Y^3 = I_3$, $YX = \varepsilon XY$.We get that $A \simeq \mathcal{M}_3(\mathbb{Q}(\varepsilon))$, therefore the index of A is $d = 1$ and the algebra A is a split algebra.

Let ϵ be a primitive root of order 3 of the unity. Using the computer algebra system MAGMA, we obtained that the class number of the Kummer field $\mathbb{Q}\left(\epsilon, \sqrt[3]{7}\right)$ is 3 and 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. Using this idea, in paper [6] we found a class of split symbol algebras, over a cyclotomic field.

Proposition 3.3. ([6]) *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 $L = K\left(\sqrt[3]{\alpha}\right)$ 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 $A = \left(\frac{\alpha,p^{h_L}}{K,\epsilon}\right)$ are split.*

A generalization of the above last proposition for symbol algebras of prime degree q ($q > 3$) is given in the following Corollary.

Corollary 3.1. ([6]) *Let q be an odd prime positive integer and ξ be a primitive root of unity of order q. Let $K = \mathbb{Q}(\xi)$ be the cyclotomic field. Let $\alpha \in K^*$, p a prime rational integers, $p \neq q$ and let $L = K\left(\sqrt[q]{\alpha}\right)$ 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.*

References

[1] Acciaro, V., *Solvability of Norm Equations over Cyclic Number Fields of Prime Degree*, Mathematics of Computation, **65**(216) (1996), 1663-1674.

[2] Borevich, Z. I. and Shafarevich, I. R., *Number Theory*, Academic Press Inc, New York, 1966.

[3] Cox, D., *Primes of the Form* $x^2 + ny^2$*: Fermat, Class Field Theory, and Complex Multiplication*, A Wiley - Interscience Publication, New York, 1989.

[4] Elduque, E., *Okubo algebras and twisted polynomials*, Contemp. Math. **224** (1999), 101-109.

[5] Flaut, C. and Savin, D., *Some properties of the symbol algebras of degree* 3, will appear in Math. Reports, **3**(2014).

[6] Flaut, C. and Savin, D., *Some examples of division symbol algebras of degree* 3 *and* 5, accepted in Carpathian J Math.

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

[8] Janusz, G. J., *Algebraic number fields*, Academic Press, London, 1973.

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

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

[11] Lemmermeyer, F., *Reciprocity laws, from Euler to Eisenstein* , Springer-Verlag, Heidelberg, 2000.

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

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

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

[15] Savin, D., Flaut, C. and Ciobanu, C., *Some properties of the symbol algebras*, Carpathian Journal of Mathematics , **25** (2009), no. 2, 239-245.

[16] Savin, D., *About some split central simple algebras*, Analele Stiintifice ale Universitatii "Ovidius" Constanta, Ser. Matematica, **22** (2014), no. 1, 263-272.

[17] Schafer, R. D., *An introduction to nonassociative algebras*, Academic Press, New-York, 1966.

[18] Stevenhagen, P., *Primes represented by quadratic forms*, websites.math.leidenuniv.nl/algebra/Stevenhagen-Primes.pdf