Split octonion algebra and its zero divisors

Serpil Halici and Adnan Karataş*

Pamukkale University, Faculty of Arts and Sciences, Department of Mathematics, Denizli/TURKEY
*Corresponding Author

E-mail: shalici@pau.edu.tr, adnank@pau.edu.tr*

Abstract

Motivated by Miguel and Serodio's work [13] on the structure of quaternion rings over finite field, we studied some special elements of split octonion algebra over finite field, more precisely nilpotent and idempotent elements of split octonion algebra. For these special elements we gave some theorems and conditions which they should satisfy. Moreover, in this algebra we investigated the involutory elements and their properties.

2010 Mathematics Subject Classification. **17A20** 16N40
Keywords. octonions, idempotent elements, nilpotent elements.

1 Introduction

In this study, we examine idempotent and nilpotent elements in split octonion algebra. It is well-known that the idempotent and nilpotent elements are zero divisors. They are studied to find and give conditions for idempotent and nilpotent elements in degenerate quaternion algebras. In [15], the authors studied zero divisors especially idempotent and nilpotent elements of biquaternions. For the idempotent and nilpotent elements in split quaternion algebras over finite fields see [2,3,10]. In addition, the authors gave a survey about these special elements and they calculated the numbers of the elements in [13].

The pursue of characteristic features of idempotent and nilpotent elements can help coding theory, video processing, digital design, etc. (See [7, 12, 14, 17, 17]). In addition to idempotent and nilpotent elements, we introduce involutory elements which we have been inspired by involutory matrix [11]. Cryptography is one of the application areas of the involutory matrices [1].

The octonion algebra which is generalization of the quaternion algebra was defined by J. T. Graves in 1843 [4]. It is known that there are different constructions for octonion algebra. One of them is by using Cayley-Dickson process [9]. Cayley-Dickson process can be also used to obtain different algebras with isotropic or anisotropic norms which cause algebras to be split or real, respectively. Norm is isotropic if there exists a nonzero x with $\mathrm{N}(x) = 0$ else it is named as anisotropic norm [4, 16].

Any element k of the octonion algebra is

$$k = a_0e_0 + a_1e_1 + \cdots + a_7e_7; \;\; a_0, a_1, \ldots, a_7 \in \mathbb{R}.$$

Conjugate and norm of the element k are

$$\overline{k} = a_0e_0 - a_1e_1 - \cdots - a_7e_7$$

and

$$\mathrm{N}(k) = \overline{k}k = k\overline{k} = a_0^2 + a_1^2 + \cdots + a_7^2$$

Tbilisi Mathematical Journal Special Issue (IECMSA-2019), pp. 79–86.
Tbilisi Centre for Mathematical Sciences.
Received by the editors: 06 October 2019.
Accepted for publication: 24 December 2019 .

respectively.
After a brief summary of the octonion algebra, let us give some properties of split octonion algebras. In 1845, J. Cockle defined of the split quaternion algebra [6]. Then, his definition is used for different dimensional algebras. There are some important theorems in [16] about split algebras, one of them state *In each of the dimensions 2, 4 and 8 there is, up to isomorphism, exactly one split composition algebra.* Another important remark states that if the mentioned algebras defined over finite fields, then those algebras are split. Which means these algebras have non-trivial idempotent and nilpotent elements. In order to have better understanding of split octonion algebra and their subalgebras see [5]. In the first paper, the authors mentions null space which contains multiples of idempotent and nilpotent elements. The second paper is also mentions idempotent and nilpotent elements but on finite field $\mathbb{F}_{p^n}$ where p is a prime.
In the next section, we investigate split octonion algebra over finite fields which generalizes split quaternion algebra $\mathbb{H}/\mathbb{Z}_p$ and established conditions for idempotent and nilpotent elements. Also, we define involutory elements and give some properties of them.

2 Split octonion algebra and its zero divisors

As it is well-known, in any ring H, when $x^2 = x$ with $x \in H$ the element x is called as idempotent element. We know that the rings can be also characterized by idempotent element, for example a ring whose elements are all idempotent is called as Boolean ring which is also known as the idempotent ring.

Now, let us give the definition of split octonion algebra $\mathbb{O}/\mathbb{Z}_p$

$$\mathbb{O}/\mathbb{Z}_p = \{x | x = \sum_{i=0}^{7} a_i e_i; a_i \in \mathbb{Z}_p, \ \ p \ \text{ is a prime, } \ p \neq 2\}$$

where e_i's are basis elements of the octonion algebra $\mathbb{O}$.

Note that, due to the properties of octonions, split algebra $\mathbb{O}/\mathbb{Z}_p$ is neither commutative nor associative eight-dimensional algebra over $\mathbb{Z}_p$. Moreover, this algebra has zero divisors, nontrivial idempotent and nilpotent elements [16].

In the following theorem, we give some conditions for idempotent elements in $\mathbb{O}/\mathbb{Z}_p$.

Theorem 2.1. For the split algebra $\mathbb{O}/\mathbb{Z}_p$, following statements are true.

i) When the elements of $\mathbb{O}/\mathbb{Z}_p$ consist of only scalar part $x = a_0 e_0$ then the idempotent elements of $\mathbb{O}/\mathbb{Z}_p$ are only 0 and 1.

ii) When the elements of $\mathbb{O}/\mathbb{Z}_p$ consist of scalar part and one imaginary unit such as $x = a_0 e_0 + a_j e_j$ with $j = 1, 2, \ldots, 7$ then the idempotent elements of $\mathbb{O}/\mathbb{Z}_p$ satisfy following equation

$$x = \frac{p+1}{2} + \sqrt{\frac{p^2-1}{4}} e_j.$$

iii) When the elements of $\mathbb{O}/\mathbb{Z}_p$ consist of scalar part and a set of imaginary units such as $x = a_0e_0 + V,\ V = \{a_ie_i \mid 1 \leq i \leq 3\}$ then the idempotent elements of $\mathbb{O}/\mathbb{Z}_p$ satisfy following equation

$$a_0 = \frac{p+1}{2} \text{ and } \mathrm{N}(V) = \frac{p^2-1}{4}.$$

iv) When the elements of $\mathbb{O}/\mathbb{Z}_p$ contain all of the basis units such as $x = a_0e_0 + a_1e_1 + \cdots + a_7e_7$ then the idempotent elements of $\mathbb{O}/\mathbb{Z}_p$ satisfy following equations

$$a_0 = \frac{p+1}{2} \text{ and } \mathrm{N}(a_1e_1 + a_2e_2 + \cdots + a_7e_7) = \frac{p^2-1}{4}.$$

Proof. i) Since $x = a_0e_0$ and $(x, p) = 1$ the claim is true.

ii) From the definition of idempotent element we can write

$$(a_0 + a_je_j)(a_0 + a_je_j) = a_0^2 - a_j^2 + 2a_0a_je_j \tag{2.1}$$

$$a_0 = a_0^2 - a_j^2, \tag{2.2}$$

$$a_j = 2a_0a_j. \tag{2.3}$$

By using equation (2.3), one can obtain $a_j = 0$ or $a_0 = \frac{p+1}{2}$. When $a_j = 0$, the idempotent element x is equal to 1 or 0. If $a_j \neq 0$, then a_j is calculated as follows.

$$a_0 = \frac{p+1}{2} \text{ and } \frac{p+1}{2} = \left(\frac{p+1}{2}\right)^2 - a_j^2$$

$$a_j = \sqrt{\frac{p^2-1}{4}}.$$

Hence, we showed the idempotent elements must satisfy $a_j = \sqrt{\frac{p^2-1}{4}}$. Now, in order to determine when $\frac{p^2-1}{4}$ is quadratic, we employ the Legendre Symbol

$$\left(\frac{\frac{p^2-1}{4}}{p}\right) = \left(\frac{p^2-1}{p}\right) = (p^2-1)^{\frac{p-1}{2}} = (-1)^{\frac{p-1}{2}} = \begin{cases} 1, & \text{if } p \equiv 1 \ (mod\ 4) \\ -1, & \text{if } p \equiv 3 \ (mod\ 4) \end{cases}. \tag{2.4}$$

So, if $p \equiv 1 \ (mod\ 4)$, then there are idempotent elements having the form $a_0e_0 + a_je_j$.

iii) The basis elements $\{e_1, e_2, e_3\}$ of V can be replaced with the triples $\{e_1, e_4, e_5\}$, $\{e_1, e_7, e_6\}$, $\{e_2, e_4, e_6\}$, $\{e_2, e_5, e_7\}$, $\{e_3, e_4, e_7\}$ and $\{e_3, e_6, e_5\}$. All these triples form subalgebras of the octonion algebra with $\{e_0\}$. These triples are isomorphic to each other and can be obtained by multiplication table or Fano plane (see [4, 8]). Similar to the prior part of the prove we can write following equations

$$(a_0 + V)(a_0 + V) = a_0^2 - Nr(V) + 2a_0V, \tag{2.5}$$

$$a_0 = a_0^2 - Nr(V) \tag{2.6}$$

and

$$a_i = 2a_0a_i, \;\; 1 \leq i \leq 3. \tag{2.7}$$

In the equation (2.7), if we take $a_i = 0$, then $x = a_0$, else $a_0 = \frac{p+1}{2}$. Next, substituting $a_0 = \frac{p+1}{2}$ in the equation (2.6), we obtain following equation.

$$\mathrm{N}(V) = \frac{p^2-1}{4}.$$

Thus, the scalar and vectorial parts of idempotent elements are

$$a_0 = \frac{p+1}{2}$$

and

$$a_1^2 + a_2^2 + a_3^2 = \frac{p^2-1}{4},$$

respectively.

iv) If we consider W as $\{a_1e_1 + a_2e_2 + ... + a_7e_7\}$ and use the definition of idempotent element, then we obtain

$$a_0 = a_0^2 - \mathrm{N}(W), \tag{2.8}$$

$$a_i = 2a_0a_i, \;\; 1 \leq i \leq 7. \tag{2.9}$$

For $1 \leq i \leq 7$, $a_i \neq 0$, the equation (2.9) means $a_0 = \frac{p+1}{2}$. Thus, $\mathrm{N}(W)$ is calculated as follows.

$$\mathrm{N}(W) = \frac{p^2-1}{4}.$$

Q.E.D.

Corollary 2.2. If x has no scalar part, then x is not an idempotent element of the $\mathbb{O}/\mathbb{Z}_p$.

Proof. Let x has at least one imaginary part and no scalar part. Then we calculate x^2. Because of the property of multiplication in $\mathbb{O}/\mathbb{Z}_p$ the result has to have a scalar part. From the hypothesis, x has no scalar part, any element without scalar part can not be idempotent element of $\mathbb{O}/\mathbb{Z}_p$. Q.E.D.

In the forthcoming theorems, we focus on the nilpotent elements of $\mathbb{O}/\mathbb{Z}_p$. First, let us recall the definition of the nilpotent element. For $y \in H$, if $y^k = 0, \;\; k \in \mathbb{N}$, then the element y is called as a nilpotent element of H.

Now, we give a lemma to investigate property of the nilpotent elements in $\mathbb{O}/\mathbb{Z}_p$.

Lemma 2.3. Let y be a nilpotent element of $\mathbb{O}/\mathbb{Z}_p$. The norm of y equals to zero.

Proof. Let y be any nilpotent element of the $\mathbb{O}/\mathbb{Z}_p$ with $y^k = 0$. From the properties of the octonion algebra $\mathbb{O}/\mathbb{Z}_p$ we have

$$y^2 + \mathrm{N}(y) - 2b_0 y = 0,$$
$$y^k(y - 2b_0)^k = (-\mathrm{N}(y))^k,$$
$$0 = (-\mathrm{N}(y))^k,$$

Thus, the norm of y is equal to zero as desired.

Q.E.D.

In the theorem 2, we introduce an additional attribute for the nilpotent elements.

Theorem 2.4. Let y be a nilpotent element of $\mathbb{O}/\mathbb{Z}_p$. Then y has no scalar part.

Proof. From Lemma 1, we conclude that $\mathrm{N}(y) = 0$, using the definition of nilpotent element and for least positive integer k which satisfies $y^k = 0$ we calculate the following equations.

$$y^2 - 2b_0 y = 0,$$
$$(y^2)^{(k+1)/2} = (2b_0)^{(k+1)/2} y^{(k+1)/2},$$

and

$$2{b_0}^{(k+1)/2} y^{(k+1)/2} = 0,$$

where k is odd. Analogously, for all even positive integers k, we get

$$y^2 - 2b_0 y = 0,$$
$$y^k = 2{b_0}^{(k/2)} y^{(k/2)};\ \ y^k = 0,$$

and

$$2{b_0}^{(k/2)} y^{(k/2)} = 0,\ \ b_0 = 0.$$

Q.E.D.

Also, we can investigate general structure of the split octonion algebra $\mathbb{O}/\mathbb{Z}_p$ by introducing a new element and its properties. In order to accomplish this goal, we define the involutory element using the definition of involutory matrix [11].

In any ring H when $z^2 = 1_H$, the element z is called as an involutory element of H, where 1_H is identity element.

In the following theorem, we investigate the involutory elements of $\mathbb{O}/\mathbb{Z}_p$.

Theorem 2.5. For $z \in \mathbb{O}/\mathbb{Z}_p$, $z = c_0e_0 + \sum_{i=1}^{7} c_ie_i$, the following statements are satisfied.

i) The involutory elements which contain only scalar part such as $z = c_0e_0$ are only 1 and $p-1$.

ii) The involutory elements having the form $z = c_je_j$ where $j = 1, 2, \ldots, 7$, satisfy the following equality.

$$c_j = \sqrt{p-1}.$$

iii) The involutory elements having the form $z = \{c_1e_1 + c_2e_2 + c_3e_3\}$, have a norm which equals to $p-1$.

iv) For the involutory elements such as $z = \{c_1e_1 + c_2e_2 + ... + c_7e_7\}$, the norm must satisfy following equation

$$\mathrm{N}(z) = p-1.$$

Proof. i) Since $\mathbb{Z}_p$ is a field, the involutory elements are only 1 and $p-1$.

ii) Using the definition of involutory element, we get

$$-c_j^2 = 1 \tag{2.10}$$

From the equation (2.10), one can conclude that $c_j^2 = p-1$. Note that, if c_j not to be a square, then by using the equation (2.4) one can see that there are no involutory elements in the $\mathbb{O}/\mathbb{Z}_p$ having the form c_je_j, if $p \equiv 3 \ (mod\ 4)$.

iii) We take z as $z = \{c_1e_1 + c_2e_2 + c_3e_3\}$ and from the definition of involutory element we obtain that $\mathrm{N}(z) = -1$. Thus, the involutory elements which have the form $z = \{c_1e_1 + c_2e_2 + c_3e_3\}$ satisfy following equation;

$$c_1^2 + c_2^2 + c_3^2 = p-1.$$

iv) Analogously to the former proof, if we choose z as $z = \{c_1e_1 + c_2e_2 + ... + c_7e_7\}$, then we find that $\mathrm{N}(z) = -1$. Hence, components of the involutory elements satisfy following equation

$${c_1}^2 + {c_2}^2 + ... + {c_7}^2 = p-1.$$

Q.E.D.

Next corollaries are given without proofs.

Corollary 2.6. The involutory elements in $\mathbb{O}/\mathbb{Z}_p$ contain only one part, scalar or vectorial.

Corollary 2.7. An element is its own inverse if and only if it is involutory element in the $\mathbb{O}/\mathbb{Z}_p$.

Corollary 2.8. z is an involutory element in the $\mathbb{O}/\mathbb{Z}_p$ if and only if z satisfies the equation $(1+z)(1-z) = 0$.

3 Conclusion

In this study, we focus on the special elements of split octonion algebra over finite fields. We especially pay attention to some zero divisors of the algebra which are idempotent and nilpotent elements. Also, we define the involutory elements taking inspiration from involutory matrices. In a further study, one can calculate numbers of these elements in the $\mathbb{O}/\mathbb{Z}_p$.

References

[1] B. Acharya, G. S. Rath, S. K. Patra, and S. K. Panigrahy, *Novel methods of generating self-invertible matrix for hill cipher algorithm* (2007).

[2] M. Aristidou and A. Demetre, *Idempotent elements in quaternion rings over zp* International journal of Algebra, **6(27)** (2012) 249–254.

[3] M. Aristidou and A. Demetre, *A note on nilpotent elements in quaternion rings over zp*, International Journal of Algebra, **6(14)** (2012) 663–666.

[4] J. Baez, *The octonions*, Bulletin of the American Mathematical Society, **39(2)** (2002) 145–205.

[5] L. Bentz, *Subalgebras of the split octonions*, (2017).

[6] J. Cockle and T. S. Davies, *Lxiv. on certain functions resembling quaternions, and on a new imaginary in algebra*, Philosophical Magazine Series 3, **33(224)** (1848) 435–439.

[7] P. Di Giamberardino, S. Monaco, and D. Normand-Cyrot *Digital control through finite feedback discretizability*, Robotics and Automation, 1996. Proceedings., 1996 IEEE International Conference on, **4** (1996) 3141–3146.

[8] L. E. Dickson, *On quaternions and their generalization and the history of the eight square theorem*, Annals of Mathematics (1919) 155–171.

[9] C. Flaut, *Some equations in algebras obtained by the cayley-dickson process*, An. St. Univ. Ovidius Constanta **9(2)** (2001) 45–68.

[10] S. M. Kang, M. Munir, A. R. Nizami, M. Ali, and W. Nazeer, *On elements of split quaternions over zp*, Global Journal of Pure and Applied Mathematics **12(5)** (2016) 4253–4271.

[11] P. Lancaster and M. Tismenetsky, *The theory of matrices: with applications*, Elsevier (1985).

[12] T. Lin, *Achieving re-loss-free video coding*, IEEE Signal Processing Letters **16(4)** (2009) 323–326.

[13] C. Miguel and R. Serodio, *On the structure of quaternion rings over zp*, International Journal of Algebra **5(27)** (2011) 1313–1325.

[14] R. M. Murray, *Nilpotent bases for a class of nonintegrable distributions with applications to trajectory generation for nonholonomic systems*, Mathematics of Control, Signals and Systems **7(1)** (1994) 58–75.

[15] S. J. Sangwine and D. Alfsmann, *Determination of the biquaternion divisors of zero, including the idempotents and nilpotents*, Advances in applied Clifford algebras **20(2)** (2010) 401–410.

[16] T. A. Springer and F. D. Veldkamp, *Octonions, Jordan algebras and exceptional groups*, Springer (2013).

[17] Z. Zhu and T. Lin, *Idempotent h. 264 intraframe multi-generation coding*, Acoustics, Speech and Signal Processing, 2009. ICASSP 2009. IEEE International Conference on (2009) 1033–1036.