About some properties of algebras obtained by the Cayley-Dickson process

Cristina FLAUT

Abstract. This paper is a short survey about some properties of algebras obtained by the Cayley-Dickson process and some of their applications.

Keywords. Cayley-Dickson process, Fibonacci Quaternions, Multiplication table for algebras obtained by the Cayley-Dickson process.

AMS Classifications. 17A35.

1. Introduction

It is well known that in October 1843, William Rowan Hamilton made a great discovery finding quaternion algebra, a 4-dimensional algebra over \( \mathbb{R} \) which is an associative and a noncommutative algebra. In December 1843, John Graves discovered the octonions, an 8-dimensional algebra over \( \mathbb{R} \) which is nonassociative and noncommutative algebra. These algebras were later rediscovered by Arthur Cayley in 1845 and are also known sometimes as the Cayley numbers. This process, of passing from \( \mathbb{R} \) to \( \mathbb{C} \), from \( \mathbb{C} \) to \( \mathbb{H} \) and from \( \mathbb{H} \) to \( \mathbb{O} \) has been generalized to algebras over fields and over rings. It is called the Cayley-Dickson doubling process or the Cayley-Dickson process.

Even if are old, Quaternion and Octonion algebras have at present many applications, especially in physics, coding theory, computer science, etc. For example, reliable high rate of transmission can be obtained using Space-Time coding. For constructing Space-Time codes, Quaternion division algebras were chosen as a new tool, as for example the Alamouti code, which can be built from a quaternion division algebra (see [Al; 98]).

The classical Cayley-Dickson process is briefly presented in the following. For details about this, the reader is referred to [Sc; 66] and [Sc; 54]. From now on, in the whole paper, we will consider \( K \) a field with \( \text{char} K \neq 2 \).
Let $A$ be an algebra over the field $K$. A unitary algebra $A \neq K$ such that we have $x^2 + \alpha(x)x + \beta(x) = 0$, for each $x \in A$, with $\alpha(x), \beta(x) \in K$, is called a quadratic algebra.

Let $A$ be a finite dimensional unitary algebra over a field $K$ with a scalar involution

$$\overline{\cdot} : A \to A, a \to \overline{a},$$

i.e. a linear map satisfying the following relations:

$$\overline{ab} = \overline{b}\overline{a}, \overline{a} = a,$$

and

$$a + \overline{a}, a\overline{a} \in K \cdot 1 \text{ for all } a, b \in A.$$

An element $\overline{a}$ is called the conjugate of the element $a$, the linear form

$$t : A \to K, t(a) = a + \overline{a}$$

and the quadratic form

$$n : A \to K, n(a) = a\overline{a}$$

are called the trace and the norm of the element $a$, respectively. Therefore, such an algebra $A$ with a scalar involution is quadratic.

Let $\gamma \in K$ be a fixed non-zero element. On the vector space $A \oplus A$, we define the following algebra multiplication:

$$A \oplus A : (a_1, a_2)(b_1, b_2) = (a_1b_1 + \gamma b_2a_2, a_2b_1 + b_2a_1).$$

We obtain an algebra structure over $A \oplus A$, denoted by $(A, \gamma)$ and called the algebra obtained from $A$ by the Cayley-Dickson process. It results that $\dim (A, \gamma) = 2 \dim A$.

For $x \in (A, \gamma)$, $x = (a_1, a_2)$, the map

$$\overline{\cdot} : (A, \gamma) \to (A, \gamma), x \to \overline{x} = (\overline{a_1}, -a_2),$$

is a scalar involution of the algebra $(A, \gamma)$, extending the involution $\overline{\cdot}$ of the algebra $A$. Let

$$t(x) = t(a_1)$$

and

$$n(x) = n(a_1) - \gamma n(a_2)$$

be the trace and the norm of the element $x \in (A, \gamma)$, respectively.

If we take $A = K$ and apply this process $t$ times, $t \geq 1$, we obtain an algebra over $K$,

$$A_t = \left( \frac{\alpha_1, \ldots, \alpha_t}{K} \right).$$

(1.3)
By induction in this algebra, the set \( \{1, e_2, \ldots, e_n\} \), \( n = 2^t \), generates a basis with the properties:
\[
e_i^2 = \alpha_i 1, \; \alpha_i \in K, \alpha_i \neq 0, \; i = 2, \ldots, n \tag{1.4}
\]
and
\[
e_i e_j = -e_j e_i = \beta_{ij} e_k, \; \beta_{ij} \in K, \; \beta_{ij} \neq 0, i \neq j, i, j = 2, \ldots, n, \tag{1.5}
\]
\( \beta_{ij} \) and \( e_k \) being uniquely determined by \( e_i \) and \( e_j \).

From [Sc; 54], Lemma 4, it results that in any algebra \( A_t \) with the basis \( \{1, e_2, \ldots, e_n\} \) satisfying the above relations we have:
\[
e_i (e_i x) = \alpha_i^2 = (xe_i)e_i, \tag{1.6}
\]
for every \( x \in A \) and for all \( i \in \{1, 2, \ldots, n\} \).

A finite-dimensional algebra \( A \) is a division algebra if and only if \( A \) does not contain zero divisors (see [Sc; 66]).

An algebra \( A \) is called central simple if the algebra \( A_F = F \otimes_K A \) is simple for every extension \( F \) of \( K \). An algebra \( A \) is called alternative if \( x^2 y = x (xy) \) and \( xy^2 = (xy) y \), for all \( x, y \in A \). An algebra \( A \) is called flexible if \( x(yx) = (xy)x = xyx \), for all \( x, y \in A \) and power associative if the subalgebra \( \langle x \rangle \) of \( A \) generated by any element \( x \in A \) is associative. Each alternative algebra is a flexible algebra and a power associative algebra.

Algebras \( A_t \) of dimension \( 2^t \) obtained by the Cayley-Dickson process, described above, are central-simple, flexible and power associative for all \( t \geq 1 \) and, in general, are not division algebras for all \( t \geq 1 \). But there are fields (for example, the rational function field) on which, if we apply the Cayley-Dickson process, the resulting algebras \( A_t \) are division algebras for all \( t \geq 1 \). (See [Br; 67] and [Fl; 13]).

2. About Fibonacci Quaternions

Since the above described algebras are usually without division, finding quickly examples of invertible elements in an arbitrary algebra obtained by the Cayley-Dickson process appear to be a not easy problem. A partial solution for generalized real Quaternion algebras can be found using Fibonacci quaternions.

Let \( \mathbb{H}(\alpha_1, \alpha_2) \) be the generalized real quaternion algebra. In this algebra, every element has the form \( a = a_1 \cdot 1 + a_2 e_2 + a_3 e_3 + a_4 e_4 \), where \( a_i \in \mathbb{R}, i \in \{1, 2, 3, 4\} \).

In [Ho; 61], the Fibonacci quaternions were defined to be the quaternions on the form
\[
F_n = f_n \cdot 1 + f_{n+1} e_2 + f_{n+2} e_3 + f_{n+3} e_4, \tag{2.1}
\]
called the $n$th Fibonacci quaternions, where

$$f_n = f_{n-1} + f_{n-2}, \quad n \geq 2,$$  \hspace{1cm} (2.2)

with $f_0 = 0, f_1 = 1$, are Fibonacci numbers.

The norm formula for the $n$th Fibonacci quaternions is:

$$n (F_n) = F_n F_n^* = 3f_{2n+3},$$  \hspace{1cm} (2.3)

where $F_n = f_n \cdot 1 - f_{n+1}c_2 - f_{n+2}c_3 - f_{n+3}c_4$ is the conjugate of the $F_n$ in the algebra $\mathbb{H}(\alpha_1, \alpha_2)$ (see [Ho; 61]). There are many authors which studied Fibonacci quaternions in the real division quaternion algebra giving more and surprising new properties (see [Sw; 73], [Sa-Mu; 82] and [Ha; 12], [Fl, Sh; 13], [Fl, Sh; 13(1)]).

**Theorem 2.1.** ([Fl, Sh; 13] Theorem 2.4.) The norm of the $n$th Fibonacci quaternion $F_n$ in a generalized quaternion algebra is

$$n (F_n) = h_{2n+2}^{1+2\alpha_2, 3\alpha_2} + (\alpha_1-1)h_{2n+3}^{1+2\alpha_2, \alpha_2} - 2(\alpha_1-1)(1+\alpha_2)f_nf_{n+1}. \hspace{1cm} (2.4)$$

We know that the expression for the $n$th term of a Fibonacci element is

$$f_n = \frac{1}{\sqrt{5}}[a^n - b^n] = \frac{a^n}{\sqrt{5}}[1 - b^n], \hspace{1cm} (2.5)$$

where $a = \frac{1+\sqrt{5}}{2}$ and $b = \frac{1-\sqrt{5}}{2}$.

Using the above notations, we can compute the following limit

$$\lim_{n \to \infty} n (F_n) = \lim_{n \to \infty} (f_n^2 + \alpha_1f_{n+1}^2 + \alpha_2f_{n+2}^2 + \alpha_1\alpha_2f_{n+3}^2) =$$

$$= \lim_{n \to \infty} \left( \frac{a^{2n}}{5} + \alpha_1 \frac{a^{2n+2}}{5} + \alpha_2 \frac{a^{2n+4}}{5} + \alpha_1\alpha_2 \frac{a^{2n+6}}{5} \right) =$$

$$= sgnE(\alpha_1, \alpha_2) \cdot \infty.$$ 

Since $a^2 = a + 1$, we have $E(\alpha_1, \alpha_2) = \left( \frac{1}{5} + \frac{\alpha_1}{5}a^2 + \frac{\alpha_2}{5}a^4 + \frac{\alpha_1\alpha_2}{5}a^6 \right) = \frac{1}{5}(1 + \alpha_1 (a + 1) + \alpha_2 (3a + 2) + \alpha_1\alpha_2 (8a + 5)) = \frac{1}{5}[1 + \alpha_1 + 2\alpha_2 + 5\alpha_1\alpha_2 + a (\alpha_1 + 3\alpha_2 + 8\alpha_1\alpha_2)].$

If $E(\alpha_1, \alpha_2) > 0$, there exist a number $n_1 \in \mathbb{N}$ such that for all $n \geq n_1$ we have

$$h_{2n+2}^{1+2\alpha_2, 3\alpha_2} + (\alpha_1-1)h_{2n+3}^{1+2\alpha_2, \alpha_2} - 2(\alpha_1-1)(1+\alpha_2)f_nf_{n+1} > 0.$$ 

If $E(\alpha_1, \alpha_2) < 0$, there exist a number $n_2 \in \mathbb{N}$ such that for all $n \geq n_2$ we have

$$h_{2n+2}^{1+2\alpha_2, 3\alpha_2} + (\alpha_1-1)h_{2n+3}^{1+2\alpha_2, \alpha_2} - 2(\alpha_1-1)(1+\alpha_2)f_nf_{n+1} < 0.$$
It results that for all $\alpha_1, \alpha_2 \in \mathbb{R}$ with $E(\alpha_1, \alpha_2) \neq 0$, in the algebra $\mathbb{H}(\alpha_1, \alpha_2)$ there is a natural number $n_0 = \max\{n_1, n_2\}$ such that $n(F_n) \neq 0$, hence $F_n$ is an invertible element, for all $n \geq n_0$.

In this way, Fibonacci Quaternion elements can provide us many important information in the algebra $\mathbb{H}(\alpha_1, \alpha_2)$ providing sets of invertible elements in algebraic structures without division. For other details, see [Fl, Sh; 13].

3. Multiplication table in Cayley-Dickson algebras

Multiplication table for algebras obtained by the Cayley-Dickson process over the real field was studied in [Ba; 09]. In this paper, the author gave an algorithm to find quickly product of two elements in these algebras. In the following, we shortly present this algorithm. In [Ba; 13], the author gave all 32 possibilities to define a "Cayley-Dickson product" used in the Cayley-Dickson doubling process, such that the obtained algebras are isomorphic.

If we consider multiplication (1.1) under the form

$$A \oplus A : (a_1, a_2)(b_1, b_2) := (a_1b_1 + \gamma_n b_2\overline{a_2}, a_1b_2 + b_1a_2),$$

the obtained algebras are isomorphic with those obtained with multiplication (1.1).

For $\alpha_1 = \ldots = \alpha_t = -1$ and $K = \mathbb{R}$, in [Ba; 09] the author described how we can multiply the basis vectors in the algebra $A_t$, $\dim A_t = 2^t = n$. He used the binary decomposition for the subscript indices.

Let $e_p, e_q$ be two vectors in the basis $B$ with $p, q$ representing the binary decomposition for the indices of the vectors, that means $p, q$ are in $\mathbb{Z}_2^n$. We have that $e_p e_q = \gamma_n (p, q) e_{p \oplus q}$, where:

i) $p \otimes q$ are the "exclusive or" for the binary numbers $p$ and $q$ (the sum of $p$ and $q$ in the group $\mathbb{Z}_2^n$);

ii) $\gamma_n : \mathbb{Z}_2^n \times \mathbb{Z}_2^n \rightarrow \{-1, 1\}$ is a map, called the twist map.

In this section, we will consider $K = \mathbb{R}$. Using the same notations as in the Bales's paper, we consider the following matrices:

$$A_0 = A = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}, \quad C = \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix}.$$ (3.2)

In the same paper [Ba; 09], the author find the properties of the twist map $\gamma_n$ and put the signs of this map in a table. He partitioned the twist table for $\mathbb{Z}_2^n$ into $2 \times 2$ matrices and obtained the following result:
Theorem 3.1. ([Ba; 09], Theorem 2.2., p. 88-91) For \( n > 0 \), the Cayley-Dickson twist table \( \gamma_n \) can be partitioned in quadratic matrices of dimension 2 of the form \( A, B, C, -B, -C \), defined in the relation (3.2).

![Twist trees](Fig. 1: Twist trees([Ba; 09], Table 9)]

Definition 3.2. Let \( x = x_0, x_1, x_2, \ldots \) and \( y = y_0, y_1, y_2, \ldots \) be two sequences of real numbers. The ordered pair

\[
(x, y) = x_0, y_0, x_1, y_1, x_2, y_2, \ldots
\]

is a sequence obtained by \textit{shuffling} the sequences \( x \) and \( y \).

Proposition 3.3. Let \( A_2 = \left( \frac{1}{2} \ldots \frac{1}{2} \right) \) be an algebra obtained by the Cayley-Dickson process with multiplication given by relation (3.1) and \( \{ e_0 = 1, e_1, \ldots, e_{n-1} \} \), \( n = 2^t \) a basis in \( A_2 \). Let \( r \geq 1 \), \( r < k \leq i < t \). We have

\[
\begin{array}{c|cc}
& e_T & e_{T+1} \\
e_{2^k-r+1} & (1)^{r+2} e_M & (1)^{r+2} e_{M+1} \\
e_{2^k-r+1+1} & (1)^{r+2} e_M & (1)^{r+2} e_M \\
\end{array}
\]

(3.3)

where the binary decomposition of \( M \) is \( M_2 = 2^k \otimes T \).

Proof. We compute \( e_{2^k-r+1} e_T \). We have \( e_{2^k-r+1} e_T = \gamma(s, q) e_M \), where the binary decomposition of \( M \) is \( M_2 = 2^{k-r+1} \otimes T \) and \( s \) is the binary decomposition for \( 2^{k-r+1} \) and \( q \) is the binary decomposition for \( T \),

\[
s = \begin{array}{cccccccc}
0 & 0 & \ldots & 0 & 1 & 0 & \ldots & 0 \\
i-k+r-1 & k-r+2 & & & i-k-1 & k-r+1 & r
\end{array}
\]

\[
q = \begin{array}{cccccccc}
1 & 0 & \ldots & 1 & 1 & 0 & \ldots & 0 \\
i-k & k-2r-1 & k-r+2 & r+2 & & & &
\end{array}
\]

By "shuffling" \( s \otimes q \), it results

\[
\begin{array}{ccc}
01 & 00 & 00 \ldots 00 \\
i-k & k-2r-1 & k-r+2
\end{array}
\]

\[
11 & 01 & 01 \ldots 01 \\
r+2 & r
\]

\[
00 & 00 \ldots 00 \\
k-1 &
\]

Starting with \( A_0 \), we get:

6
\(A_0 \overset{01}{\rightarrow} A \overset{00}{\rightarrow} \cdots \overset{00}{\rightarrow} A \overset{01}{\rightarrow} A \overset{01}{\rightarrow} \cdots \overset{01}{\rightarrow} A \overset{11}{\rightarrow} -C \overset{01}{\rightarrow} C \overset{01}{\rightarrow} -C \overset{01}{\rightarrow} C \cdots \overset{01}{\rightarrow} (-1)^{r+2} C \overset{00}{\rightarrow} \cdots \overset{00}{\rightarrow} (-1)^{r+2} C.

\)

Therefore \(\gamma(s, q) = (-1)^{k-r+1}\).

Now, we compute \(e_{2^{k-r+1}e_{T+1}}\). For this, we will "shuffling" \(\begin{array}{c}
00\ldots 0 \\
i-k+r-1 k-r+2
\end{array}\)

with \(100\ldots 0111\ldots 10\ldots 1\). It results

\(\begin{array}{c}
01 00 00\ldots 00 01 01 01 \ldots 01 11 01 01 \ldots 01 00 00 \ldots 00 01.
\end{array}\)

Starting with \(A_0\), we get:

\(\begin{array}{c}
A_0 \overset{01}{\rightarrow} A \overset{00}{\rightarrow} \cdots \overset{00}{\rightarrow} A \overset{01}{\rightarrow} A \overset{01}{\rightarrow} \cdots \overset{01}{\rightarrow} A \overset{11}{\rightarrow} -C \overset{01}{\rightarrow} C \overset{01}{\rightarrow} -C \overset{01}{\rightarrow} C \cdots \overset{01}{\rightarrow} (-1)^{r+2} C \overset{00}{\rightarrow} \cdots \overset{00}{\rightarrow} (-1)^{r+3} C.
\end{array}\)

For \(e_{2^{k-r+1}e_{T+1}}\), "shuffling" \(\begin{array}{c}
00\ldots 0 \\
i-k+r-1 k-r+2
\end{array}\) with \(100\ldots 0111\ldots 10\ldots 0\) it results

\(\begin{array}{c}
01 00 00\ldots 00 01 01 01 \ldots 01 11 01 01 \ldots 01 00 00 \ldots 00 10.
\end{array}\)

Starting with \(A_0\), we get:

\(\begin{array}{c}
A_0 \overset{01}{\rightarrow} A \overset{00}{\rightarrow} \cdots \overset{00}{\rightarrow} A \overset{01}{\rightarrow} A \overset{01}{\rightarrow} \cdots \overset{01}{\rightarrow} A \overset{11}{\rightarrow} -C \overset{01}{\rightarrow} C \overset{01}{\rightarrow} -C \overset{01}{\rightarrow} C \cdots \overset{01}{\rightarrow} (-1)^{r+2} C \overset{00}{\rightarrow} \cdots \overset{00}{\rightarrow} (-1)^{r+3} C.
\end{array}\)

For \(e_{2^{k-r+1}e_{T+1}}\), we compute first \((2^{k-r+1} + 1) \otimes (T + 1)\). We obtain:

\[(2^{k-r+1} + 1) \otimes (T + 1) =
\]

\[= \left( \begin{array}{c}
00\ldots 0 \\
i-k+r-1 k-r+2
\end{array}\right) \otimes \left( \begin{array}{c}
100\ldots 1 \\
i-k-1k-r+1 r
\end{array}\right) =
\]

\[= \begin{array}{c}
10\ldots 0111\ldots 10 & 1\ldots 1 & 0\ldots 0
\end{array} = 2^{k-r+1} \otimes T = M.
\]

Now, "shuffling" \(\begin{array}{c}
00\ldots 0 \\
i-k+r-1 k-r+2
\end{array}\) with \(100\ldots 0111\ldots 10\ldots 1\) it results

\(\begin{array}{c}
01 00 00\ldots 00 01 01 01 \ldots 01 11 01 01 \ldots 01 00 00 \ldots 00 11.
\end{array}\)
Starting with $A_0$, we get:

\begin{align*}
A_0 & \overset{01}{\rightarrow} A \overset{00}{\rightarrow} \ldots \overset{00}{\rightarrow} A \overset{01}{\rightarrow} A \overset{01}{\rightarrow} \ldots \overset{01}{\rightarrow} A \\
& \overset{i-k}{\rightarrow} \overset{k-2r-1}{\rightarrow} \overset{11}{\rightarrow} \overset{-C}{\rightarrow} \overset{01}{\rightarrow} C \overset{01}{\rightarrow} \ldots \overset{01}{\rightarrow} (-1)^{r+2} C \overset{00}{\rightarrow} \ldots \overset{11}{\rightarrow} (-1)^{r+3} C.
\end{align*}

□

4. Some applications in Algebra and Coding Theory

Let $A_t$ be an algebra obtained by the Cayley-Dickso process over the field $\mathbb{R}$, with the basis $\{1, e_2, \ldots, e_n\}$, $n = 2^t$. The unit elements in $A_t$ are $\{\pm 1, \pm e_2, \ldots, \pm e_n\}$.

In [Ma, Be, Ga; 09], the authors defined the integers of the $A_t$ to be the set

$$A_t[\mathbb{Z}] = \{x_1 \cdot 1 + \sum_{i=2}^{2^n} x_i \cdot e_i, \ x_1, x_i \in \mathbb{Z}, i \in \{2, \ldots, n\}\}.$$ 

$A_t[\mathbb{Z}]$ is a non-associative and non-commutative ring on which the following equivalence relation can be defined.

**Definition 4.1.** Let $a, x, y \in A_t[\mathbb{Z}]$. We say that $x, y$ are right(left) congruent modulo $a$ if and only if there is the element $b \in A_t[\mathbb{Z}]$ such that

$$x - y = ba \ (or \ x - y = ab). \quad (4.1)$$

We denote this relation with $x \equiv_r y \mod a \ (or \ x \equiv_s y \mod a)$ and this relation is well defined. We will consider the quotient ring

$$A_t[\mathbb{Z}]_a = \{x \mod a / x \in A_t[\mathbb{Z}]\}.$$ 

If $a \neq 0$ is not a zero divisor, then $A_t[\mathbb{Z}]_a$ has $N(a)^{2^n-1}$ elements (see [Ma, Be, Ga; 09] for other details).

Since algebras $A_t$ are poor in properties, due to the power-associativity, if we take $w \in A_t[\mathbb{Z}]$, then the set $\mathbb{U} = \{a + bw / a, b \in \mathbb{Z}\}$ become an associative and a commutative ring with $\mathbb{U} \subset A_t[\mathbb{Z}]$.

Let $\mathbb{U}$ be the ring defined above, included in $A_t[\mathbb{Z}]$, with $t \in \{2, 3\}$.

**Definition 4.2.** An element $x \in \mathbb{U}$ is prime in $\mathbb{U}$ if $x$ is not an invertible element in $\mathbb{U}$ and if $x = ab$, then $a$ or $b$ is an invertible element in $\mathbb{U}$.

It is obvious that if $\pi \in \mathbb{U}$ is a prime element, then $n(\pi)$ is a prime element in $\mathbb{Z}$. 

8
If we consider relation (4.1) on $\mathbb{U}$, due to commutativity, "the right" is the same with "the left" and if $\pi$ is a prime element in $\mathbb{U}$, therefore $\mathbb{U}_\pi$ is a field isomorphic with $\mathbb{Z}_p$, where $n(\pi) = p$, $p$ a prime element in $\mathbb{Z}$, as we can see from the above statements.

Proposition 4.3. ([Fl; 14], [Gu; 13], [Hu; 94])

i) If $x, y \in \mathbb{V}$, then there are $z, v \in \mathbb{V}$ such that $x = zy + v$, with $N(v) < N(y)$.

ii) With the above notation, we have that the remainder $v$ has the formula

$$v = x - \left\lfloor \frac{x\pi}{y\pi} \right\rfloor y,$$

(4.2)

where the symbol $\lfloor \cdot \rfloor$ is the rounding to the closest integer. For the octonions, the rounding of an octonion integer can be found by rounding the coefficients of the basis, separately, to the closest integer.

Proposition 4.4. ([Fl; 14], [Gu; 13], [Hu; 94])

i) The above relation is an equivalence relation on $\mathbb{U}$. The set of equivalence class is denoted by $\mathbb{U}_\pi$ and is called the residue class of $\mathbb{U}$ modulo $\pi$.

ii) The modulo function $\mu : \mathbb{U} \to \mathbb{U}_\pi$ is $\mu(x) = x \mod \pi = x - \left\lfloor \frac{x\pi}{\pi} \right\rfloor y$, where $x = z\pi + v$, with $N(\pi) < N(y)$.

iii) $\mathbb{U}_\pi$ is a field isomorphic with $\mathbb{Z}_p$, $p = N(\pi)$, $p$ a prime number.

Remark 4.6. ([Ne, In,Fa, El, Pa; 01]) From the above, we have that for $v_i, v_j \in \mathbb{U}_\pi, i, j \in \{1, 2, ..., p - 1\}$, $u_i + u_j = u_k$ if and only if $k = i + j \mod p$ and $u_i \cdot u_j = u_k$ if and only if $k = i \cdot j \mod p$. From here, we have the following labelling procedure:

1) Let $\pi \in \mathbb{U}$ be a prime, with $n(\pi) = p$, $p$ a prime number, $\pi = a + bw, a, b \in \mathbb{Z}$.

2) Let $s \in \mathbb{Z}$ be the only solution of the equation $a + bx \mod p, x \in \{0, 1, 2, ..., p - 1\}$.

3) The element $k \in \mathbb{Z}_p$ is the label of the element $u = m + nw \in \mathbb{U}$ if $m + ns = k \mod p$ and $n(u)$ is minimum.

In this way, we obtain the map

$$\alpha : \mathbb{Z}_p \to \mathbb{U}_\pi, \alpha(m) = \mu(m + \pi) = (m + \pi) \mod \pi.$$

Example 4.5.

Let $t = 2, w = 1 + e_2 + e_3 + e_4, p = 13, \pi = -1 + 2w$. We remark that $n(\pi) = 13$ and $w^2 - 2w + 4 = 0$. The field $\mathbb{U}_\pi$ isomorphic with $\mathbb{Z}_{13}$ is

$$\mathbb{U}_\pi = \{0, 1, 2, 3, -3 + w, -2 + w, -1 + w, 1 - w, 2 - w, 3 - w, -3, -2, -1\}$$

Indeed, using relations $w^2 = 2w - 4$ and $\overline{w} = 2 - w$, we have:

- $4 = 4 + \pi = 3 + 2w = -3 + w$, since $3 + 2w = (-1 + 2w)\overline{w} + w - 3$, with $n(w - 3) = 7 < 13 = n(\pi)$;
- $5 = 5 + \pi = 4 + 2w = -2 + w;$
Using the above labelling procedure, we have
\[ \alpha : \mathbb{Z}_p \to \mathbb{U}_\pi, \alpha (0) = 0, \alpha (1) = 1, \alpha (2) = 2, \alpha (3) = 3, \]
\[ \alpha (4) = -3 + w, \alpha (5) = -2 + w, \alpha (6) = -1 + w, \alpha (7) = 1 - w, \]
\[ \alpha (8) = 2 - w, \alpha (9) = 3 - w, \alpha (10) = -3, \alpha (11) = -2, \alpha (12) = -1. \]

Remark 4.6. Since each natural number can be written as a sum of four squares, if \( m \in \mathbb{N} \), such that \( m = a_1^2 + a_2^2 + a_3^2 + a_4^2, a_i \in \mathbb{N}, i \in \{1, 2, 3\} \) and if \( q = 2a_1 \), therefore the equation
\[ x^2 - qx + m = 0, \] (4.3)
has always solutions in \( A_t \), for all \( t \). Indeed, let \( z = a_1 \cdot 1 + a_2 \cdot e_i + a_3 \cdot e_j + a_4 \cdot e_k \), where \( i \neq j \neq k \) and \( e_i, e_j, e_k \in \{ e_2, ..., e_n \}, n = 2^t \). The element \( z \) is always a solution of the equation (4.3), since \( t(z) = 2a_1 = q \) and \( n(x) = a_2^2 + a_3^2 + a_4^2 = m \).

Remark 4.7. Such a field obtained above have many applications in Coding Theory, since on these fields can be constructed good codes which can detected and corrected some error patterns which occur most frequently (see [Fl; 14], [Gu; 13], [Hu; 94], [Ma, Be, Ga; 09], [Ne, In, Fa, El, Pa; 01]).

References

[Al; 98] S.M. Alamouti, A simple transmit diversity technique for wireless communications, IEEE J. Selected Areas Communications, 16(1998), 1451-1458.
[Ba; 13] J.W. Bales, A Catalog of Cayley-Dickson-like Products, http://arxiv.org/pdf/1107.1301v4.pdf.
[Ba; 09] J. W. Bales, A Tree for Computing the Cayley-Dickson Twist, Missouri J. Math. Sci., 21(2)(2009), 83–93.
[Br; 67] R. B. Brown, On generalized Cayley-Dickson algebras, Pacific J. of Math., 20(3)(1967), 415-422.
[Fl; 14] C. Flaut, Codes over a subset of Octonion Integers, http://arxiv.org/pdf/1401.7828.pdf.
[Fl; 13] C. Flaut, Levels and sublevels of algebras obtained by the Cayley-Dickson process, Ann Mat Pur Appl 192(2013), 1099-1114.
[Fl, Sh; 13] C. Flaut, V. Shpakivskyi, On Generalized Fibonacci Quaternions and Fibonacci-Narayana Quaternions, Adv. Appl. Clifford Algebras 23(2013), 673–688.
[Fl, Sh; 13(1)] C. Flaut, V. Shpakivskyi. Real Matrix Representations for the Complex Quaternions, Adv. Appl. Clifford Algebras 23(2013), 657–671.
[Gu; 13] M. Güzeltepe, Codes over Hurwitz integers, DiscreteMath, 313(5)(2013), 704-714.

[Ha; 12] S. Halici, On Fibonacci Quaternions, Adv. in Appl. Clifford Algebras, 22(2)(2012), 321-327.

[Ho; 61] A. F. Horadam, A Generalized Fibonacci Sequence, Amer. Math. Monthly, 68(1961), 455-459.

[Hu; 94] K. Huber, Codes over Gaussian integers, IEEE Trans. Inform. Theory, 40(1994), 207–216.

[Ma, Be, Ga; 09] C. Martinez, R. Beivide, E. Gabidulin, Perfect codes from Cayley graphs over Lipschitz integers, IEEE Trans. Inform. Theory 55(8)(2009), 3552–3562.

[Ne, In,Fa, El, Pa; 01] T.P. da N. Neto, J.C. Interlando, M.O. Favareto, M. Elia, R. Palazzo Jr., Lattice constellation and codes from quadratic number fields, IEEE Trans. Inform. Theory 47(4)(2001) 1514–1527.

[Sa-Mu; 82] P. V. Satyanarayana Murthy, Fibonacci-Cayley Numbers, The Fibonacci Quarterly, 20(1)(1982), 59-64.

[Sc; 66] R. D. Schafer, An Introduction to Nonassociative Algebras, Academic Press, New-York, 1966.

[Sc; 54] R. D. Schafer, On the algebras formed by the Cayley-Dickson process, Amer. J. Math., 76(1954), 435-446.

[Sw; 73] M. N. S. Swamy, On generalized Fibonacci Quaternions, The Fibonacci Quaterly, 11(5)(1973), 547-549.

Cristina FLAUT
Faculty of Mathematics and Computer Science,
Ovidius University,
Bd. Mamaia 124, 900527, CONSTANTA,
ROMANIA

http://cristinaflaut.wikispaces.com/
http://www.univ-ovidius.ro/math/
e-mail:
cflaut@univ-ovidius.ro
cristina_flaut@yahoo.com