Matrix Representation on Quaternion Algebra

GÜLAY KORU YÜCEKAYA

Abstract. The quaternions, denoted by $\mathbb{H}$, were first defined by W.R. Hamilton in 1843 as an extension of the four dimensions complex numbers. Hamilton has included a new multiplication process to vector algebra by defining quaternions for two vectors where the division process is available. In this paper, basic operations on $\mathbb{H}/\mathbb{Z}_p$ quaternion and the matrix form which belong to $\mathbb{H}/\mathbb{Z}_p$ quaternion algebra are given.

2010 AMS Classification: 15A03, 15A33, 15A30, 20H25, 11R52
Keywords: Ring, Field, Quaternions, Quaternion Algebra.

1. INTRODUCTION

In this section, basic definitions and theorems are given for our study.

Definition 1.1. Let $\mathbb{N}$ be the set of natural numbers, and $(a, b), (c, d) \in \mathbb{N} \times \mathbb{N}$. $(a, b)$ equivalence class which includes as $(a, b)$ element is called an integer according to equivalence relation in $\mathbb{N} \times \mathbb{N}$ which is defined as

$$(a, b) \sim (c, d) \iff a + d = b + c$$

and it is denoted by $\mathbb{Z}$.

Theorem 1.1. $(\mathbb{Z}, +, \cdot)$ is a ring

Theorem 1.2. To be equal relation is an equivalence relation among the elements in $\mathbb{Z}$ module $p$.

Thus, according to module $p$, if the equivalence classes set

$$\{(x, y) \mid x \in \mathbb{Z}, y \in \mathbb{Z}x \equiv y \pmod{p}\}.$$

Which is separated from equivalence relation by $\mathbb{Z}$. is denoted $\mathbb{Z}_p$, that is

$$\mathbb{Z}_p = \{0, 1, 2, \ldots, p-1\}.$$

Theorem 1.3. $(\mathbb{Z}_p, +, \cdot)$ is an unit and commutative ring [2].
Theorem 1.4. If \( p \) is a prime, then \((\mathbb{Z}_p, +, \cdot)\) is a field [2].

Definition 1.2. The set of

\[
q = a_0e_0 + a_1e_1 + a_2e_2 + a_3e_3
\]

is called real quaternions. Such that ordered \( a_0, a_1, a_2, a_3 \) four real numbers accompany to \( e_0 = 1, e_1, e_2, e_3 \) units which enable

\[
\begin{align*}
e_1^2 &= e_2^2 = e_3^2 = -1, \\
e_1 \times e_2 &= e_3, e_2 \times e_3 = e_1, e_3 \times e_1 = e_2 \\
e_2 \times e_1 &= -e_3, e_3 \times e_2 = -e_1, e_1 \times e_3 = -e_2
\end{align*}
\]

properties. Here, \( a_0, a_1, a_2, a_3 \) real numbers are components of \( q \) quaternion and it is written as \( \{\mathbb{H}, \oplus, \mathbb{R}, +, ., \odot, \times\} \) an associative algebra where quaternions set is \( \mathbb{H} \).

This algebra is called quaternion algebra and shortly denoted by \( \mathbb{H} \). One basis of this algebra is \( \{1, e_1, e_2, e_3\} \) and the dimension is four [4].

2. \( \mathbb{H}/\mathbb{Z}_p \) Quaternion Algebra

In this study, let \( p \) be a prime \( e_0 = 1, e_1^2 = p - 1 = -1 \) and \( a, b \in \mathbb{Z}_p \). The elements of the form \( ae_0 + be_1 \) will be denoted by the set \( \mathbb{Z}_p[e_1] \).

Theorem 2.1. The set

\[
\mathbb{H}/\mathbb{Z}_p = \{q = a_0e_0 + a_1e_1 + a_2e_2 + a_3e_3 \mid a_i \in \mathbb{Z}_p, 0 \leq i \leq 3, p = 4k + 3 \text{ prime,} \\
e_0 = 1, e_1^2 = e_2^2 = e_3^2 = p - 1 = -1\}
\]

is a vector space over \((\mathbb{Z}_p, +, \cdot)\) field.

Proof. Let \( \forall q_1 = a_0e_0 + a_1e_1 + a_2e_2 + a_3e_3, q_2 = b_0e_0 + b_1e_1 + b_2e_2 + b_3e_3 \in \mathbb{H}/\mathbb{Z}_p \) and \( a_i, b_i \in \mathbb{Z}_p, i = 0, 1, 2, 3. \mathbb{H}/\mathbb{Z}_p \) under the addition is defined

\[
\oplus : \mathbb{H}/\mathbb{Z}_p \times \mathbb{H}/\mathbb{Z}_p \rightarrow \mathbb{H}/\mathbb{Z}_p
\]

\[
(q_1, q_2) \rightarrow q_1 \oplus q_2
\]

That is,

\[
q_1 \oplus q_2 = (a_0 + b_0)e_0 + (a_1 + b_1)e_1 + (a_2 + b_2)e_2 + (a_3 + b_3)e_3.
\]

So, \( (\mathbb{H}/\mathbb{Z}_p, \oplus) \) is an Abelian group.Let be the set \( \mathbb{H}/\mathbb{Z}_p \) under the multiplication

\[
\odot : \mathbb{Z}_p \times \mathbb{H}/\mathbb{Z}_p \rightarrow \mathbb{H}/\mathbb{Z}_p
\]

\[
(a, q) \rightarrow a \odot q.
\]

That is defined by (1.1)

\[
a \odot q = a \odot (a_0e_0 + a_1e_1 + a_2e_2 + a_3e_3)
\]

\[
= (aa_0)e_0 + (aa_1)e_1 + (aa_2)e_2 + (aa_3)e_3
\]

which has the properties indicated below.

V1) For \( \forall a \in \mathbb{Z}_p, \forall q_1, q_2 \in \mathbb{H}/\mathbb{Z}_p, \)

\[
a \odot (q_1 \oplus q_2) = (a \odot q_1) \oplus (a \odot q_2),
\]
V2) For \( \forall a, b \in \mathbb{Z}_p, \forall q \in \mathbb{H}/\mathbb{Z}_p, \)
\[
(a + b) \odot q = (a \odot q) \oplus (b \odot q),
\]

V3) For \( \forall a, b \in \mathbb{Z}_p, \forall q \in \mathbb{H}/\mathbb{Z}_p, \)
\[
(a, b) \odot q = a \odot (b \odot q),
\]

V4) For \( \forall q \in \mathbb{H}/\mathbb{Z}_p, 1 \in \mathbb{Z}_p \)
\[
1 \odot q = q.
\]

Therefore, \( \{\mathbb{H}/\mathbb{Z}_p, +, \odot, \oplus\} \) is a vector space. This vector space will be denoted by \( \mathbb{H}/\mathbb{Z}_p \) shortly. \( \square \)

**Definition 2.1.** Let be \( \mathbb{H}/\mathbb{Z}_p \) a vector space. A multiplication on this vector space is defined
\[
\times : \mathbb{H}/\mathbb{Z}_p \times \mathbb{H}/\mathbb{Z}_p \rightarrow \mathbb{H}/\mathbb{Z}_p
\]
\[
(q_1, q_2) \rightarrow q_1 \times q_2
\]
That is
\[
q_1 \times q_2 = (a_0 e_0 + a_1 e_1 + a_2 e_2 + a_3 e_3) \times (b_0 e_0 + b_1 e_1 + b_2 e_2 + b_3 e_3) + (a_0 b_0 + (p - 1) a_1 b_1 + (p - 1) a_2 b_2 + (p - 1) a_3 b_3) e_0
\]
\[
+ (a_0 b_1 + a_1 b_0 + a_2 b_3 + (p - 1) a_3 b_2) e_1
\]
\[
+ (a_0 b_2 + (p - 1) a_1 b_3 + a_2 b_0 + a_3 b_1) e_2
\]
\[
+ (a_0 b_3 + a_1 b_2 + (p - 1) a_2 b_1 + a_3 b_0) e_3.
\]

This multiplication is called quaternion multiplication [3].

**Theorem 2.2.** The quaternion multiplication have these properties shown below.

K1) For \( \forall q_1, q_2 \in \mathbb{H}/\mathbb{Z}_p, \)
\[
q_1 \times q_2 \in \mathbb{H}/\mathbb{Z}_p,
\]

K2) For \( \forall a \in \mathbb{Z}_p, \forall q_1, q_2 \in \mathbb{H}/\mathbb{Z}_p, \)
\[
a \odot (q_1 \times q_2) = (a \odot q_1) \times q_2 = q_1 \times (a \odot q_2),
\]

K3) For \( \forall q_1, q_2, q_3 \in \mathbb{H}/\mathbb{Z}_p, \)
\[
(q_1 \oplus q_2) \times q_3 = (q_1 \times q_2) \oplus (q_2 \times q_3)
\]
\[
q_1 \times (q_2 \oplus q_3) = (q_1 \times q_2) \oplus (q_1 \times q_3),
\]

K4) For \( \forall q_1, q_2, q_3 \in \mathbb{H}/\mathbb{Z}_p, \)
\[
(q_1 \times q_2) \times q_3 = q_1 \times (q_2 \times q_3).
\]

Thus, \( \{\mathbb{H}/\mathbb{Z}_p, +, \odot, \oplus, \times\} \) is an algebra [5]. This algebra over \( \mathbb{Z}_p \) field is called quaternion algebra and it is denoted by \( \mathbb{H}/\mathbb{Z}_p \).

**Conclusion 2.1.** Quaternion multiplication has no commutative property. That is, for \( \forall q_1, q_2 \in \mathbb{H}/\mathbb{Z}_p, \)
\[
q_1 \times q_2 \neq q_2 \times q_1.
\]
Specially, for \( \forall q_1 = a_0 e_0, q_2 = b_0 e_0 \in \mathbb{H}/\mathbb{Z}_p, \) there exists commutative property.
3. Matrix Representation of $\mathbb{H}/\mathbb{Z}_p$ Quaternion Algebra

**Theorem 3.1.** For $\forall q_1 = a_0 e_0 + a_1 e_1 + a_2 e_2 + a_3 e_3$, $q_2 = b_0 e_0 + b_1 e_1 + b_2 e_2 + b_3 e_3 \in \mathbb{H}/\mathbb{Z}_p$, this multiplication can be expressed with the help of a linear operator.

**Proof.**

$$L_{q_1} : \mathbb{H}/\mathbb{Z}_p \xrightarrow{\text{linear}} \mathbb{H}/\mathbb{Z}_p$$

$$q_2 \rightarrow L_{q_1}(q_2) = q_1 \times q_2$$

so we obtain

$$L_{q_1}(e_0) = q_1 \times e_0 = a_0 e_0 + a_1 e_1 + a_2 e_2 + a_3 e_3.$$

$$L_{q_1}(e_1) = q_1 \times e_1 = (p - 1) a_1 e_0 + a_0 e_1 + a_3 e_2 + (p - 1) a_2 e_3,$$

$$L_{q_1}(e_2) = q_1 \times e_2 = (p - 1) a_2 e_0 + (p - 1) a_3 e_1 + a_0 e_2 + a_1 e_3,$$

$$L_{q_1}(e_3) = q_1 \times e_3 = (p - 1) a_3 e_0 + a_2 e_1 + (p - 1) a_1 e_2 + a_0 e_3.$$

$L_{q_1}$ corresponds to the linear operator represented by the matrix $H^+(q_1)$

$$H^+(q_1) = \begin{bmatrix}
a_0 & (p - 1) a_1 & (p - 1) a_2 & (p - 1) a_3 \\
a_1 & a_0 & a_3 & a_2 \\
a_2 & a_3 & a_0 & (p - 1) a_1 \\
a_3 & (p - 1) a_2 & a_1 & a_0
\end{bmatrix}.$$  

So that $q_1 \times q_2$ quaternion multiplication, $H^+(q_1) q_2$ can be expressed in the form of matrix multiplication. Actually

$$H^+(q_1) q_2 = \begin{bmatrix}
a_0 & (p - 1) a_1 & (p - 1) a_2 & (p - 1) a_3 \\
a_1 & a_0 & a_3 & a_2 \\
a_2 & a_3 & a_0 & (p - 1) a_1 \\
a_3 & (p - 1) a_2 & a_1 & a_0
\end{bmatrix} \begin{bmatrix}
b_0 \\
b_1 \\
b_2 \\
b_3
\end{bmatrix} = \begin{bmatrix}
a_0 b_0 + (p - 1) a_1 b_1 + (p - 1) a_1 b_2 + (p - 1) a_3 b_3 \\
a_1 b_0 + a_0 b_1 + (p - 1) a_3 b_2 + a_2 b_3 \\
a_2 b_0 + a_3 b_1 + a_0 b_2 + (p - 1) a_1 b_3 \\
a_3 b_0 + (p - 1) a_2 b_1 + a_1 b_2 + a_0 b_3
\end{bmatrix} = q_1 \times q_2.$$

4
Therefore,

\[
H^+(q_1) = a_0 \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} + a_1 \begin{bmatrix} 0 & p-1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & p-1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \\
+ a_2 \begin{bmatrix} 0 & 0 & p-1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & p-1 & 0 & 0 \end{bmatrix} + a_3 \begin{bmatrix} 0 & 0 & 0 & p-1 \\ 0 & 0 & p-1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}.
\]

Matrix can be written by

\[
E_0 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad E_1 = \begin{bmatrix} 0 & p-1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & p-1 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \\
E_2 = \begin{bmatrix} 0 & 0 & p-1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}, \quad E_3 = \begin{bmatrix} 0 & 0 & 0 & p-1 \\ 0 & 0 & p-1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & p-1 & 0 & 0 \end{bmatrix}.
\]

\[
H^+(q_1) = a_0 E_0 + a_1 E_1 + a_2 E_2 + a_3 E_3.
\]

Here, \(E_0 = I_4, E_1, E_2, E_3\) in order corresponds to \(e_0 = 1, e_1, e_2, e_3\) units. There exists the properties shown below:

\[
E_1^2 = E_2^2 = E_3^2 = (p-1) E_0 = (p-1) I_4,
\]

\[
E_1 E_2 = E_3, \quad E_2 E_3 = E_1, \quad E_3 E_1 = E_2
\]

\[
E_2 E_1 = (p-1) E_3, \quad E_3 E_2 = (p-1) E_1, \quad E_1 E_2 = (p-1) E_2.
\]

By processes similar

\[
R_{q_1} : \mathbb{H}/\mathbb{Z}_p \xrightarrow{\text{linear}} \mathbb{H}/\mathbb{Z}_p \\
q_2 \mapsto L_{q_1}(q_2) = q_2 \times q_1
\]

linear operator where

\[
q_1 = a_0 e_0 + a_1 e_1 + a_2 e_2 + a_3 e_3,
q_2 = b_0 e_0 + b_1 e_1 + b_2 e_2 + b_3 e_3.
\]

Matrix corresponds to \(R_{q_1}\) linear operation.

\[
R_{q_1}(e_0) = e_0 \times q_1 = a_0 e_0 + a_1 e_1 + a_2 e_2 + a_3 e_3.
\]

\[
R_{q_1}(e_1) = e_1 \times q_1 = (p-1) a_1 e_0 + a_0 e_1 + (p-1) a_3 e_2 + a_2 e_3.
\]

\[
R_{q_1}(e_2) = e_2 \times q_1 = (p-1) a_2 e_0 + a_3 e_1 + a_0 e_1 + (p-1) a_1 e_3.
\]
Thus we obtain

\[
H^- (q_1) = \begin{bmatrix}
    a_0 & (p-1) a_1 & (p-1) a_2 & (p-1) a_3 \\
    a_1 & a_0 & a_3 & a_2 \\
    a_2 & a_3 & a_0 & (p-1) a_1 \\
    a_3 & a_2 & (p-1) a_1 & a_0
\end{bmatrix}
\]

So that \(q_2 \times q_1\) quaternion multiplication, \(H^- (q_1) q_2\) can be expressed in the form of matrix multiplication. Actually

\[
H^- (q_1) q_2 = \begin{bmatrix}
    a_0 & (p-1) a_1 & (p-1) a_2 & (p-1) a_3 \\
    a_1 & a_0 & a_3 & a_2 \\
    a_2 & a_3 & a_0 & (p-1) a_1 \\
    a_3 & a_2 & (p-1) a_1 & a_0
\end{bmatrix}
\begin{bmatrix}
    b_0 \\
    b_1 \\
    b_2 \\
    b_3
\end{bmatrix}
\]

Therefore,

\[
H^- (q_1) = a_0 \begin{bmatrix}
    1 & 0 & 0 & 0 \\
    0 & 1 & 0 & 0 \\
    0 & 0 & 1 & 0 \\
    0 & 0 & 0 & 1
\end{bmatrix} + a_1 \begin{bmatrix}
    0 & p-1 & 0 & 0 \\
    1 & 0 & 0 & 0 \\
    0 & 0 & 0 & p-1 \\
    0 & 0 & 1 & 0
\end{bmatrix}
\]

\[
+ a_2 \begin{bmatrix}
    0 & 0 & p-1 & 0 \\
    0 & 0 & 0 & 1 \\
    0 & 1 & 0 & 0 \\
    p-1 & 0 & 0 & 0
\end{bmatrix} + a_3 \begin{bmatrix}
    0 & 0 & 0 & p-1 \\
    0 & 0 & p-1 & 0 \\
    0 & 1 & 0 & 0 \\
    1 & 0 & 0 & 0
\end{bmatrix}.
\]

Matrix can be written by

\[
E_0 = \begin{bmatrix}
    1 & 0 & 0 & 0 \\
    0 & 1 & 0 & 0 \\
    0 & 0 & 1 & 0 \\
    0 & 0 & 0 & 1
\end{bmatrix}, \quad E_1 = \begin{bmatrix}
    0 & p-1 & 0 & 0 \\
    1 & 0 & 0 & 0 \\
    0 & 0 & 0 & p-1 \\
    0 & 0 & 1 & 0
\end{bmatrix},
\]

\[
E_2 = \begin{bmatrix}
    0 & 0 & p-1 & 0 \\
    0 & 0 & 0 & 1 \\
    1 & 0 & 0 & 0 \\
    0 & 1 & 0 & 0
\end{bmatrix}, \quad E_3 = \begin{bmatrix}
    0 & 0 & 0 & p-1 \\
    0 & 0 & 0 & 1 \\
    1 & 0 & 0 & 0 \\
    0 & p-1 & 0 & 0
\end{bmatrix}.
\]

\[
H^- (q_1) = a_0 E_0 + a_1 E_1 + a_2 E_2 + a_3 E_3.
\]

Here, \(E_0 = I_4, E_1, E_2, E_3\) in order corresponds to \(e_0 = 1, e_1, e_2, e_3\) units. There exists the properties shown below:

\[
E_1^2 = E_2^2 = E_3^2 = (p-1) E_0 = (p-1) I_4,
\]
\[ E_1 E_2 = E_3, \ E_2 E_3 = E_1, \ E_3 E_1 = E_2 \]
\[ E_2 E_1 = (p - 1) E_3, \ E_3 E_2 = (p - 1) E_1, \ E_1 E_2 = (p - 1) E_2. \]

Homomorphism where \( H^+ \) was not a homomorphism \( H^- \). Thus,

i) \( H^+ (q_1 + q_2) = H^+ (q_1) + H^+ (q_2) \)

ii) \( H^+ (q_1 x q_2) = H^+ (q_1) H^+ (q_2) \)

iii) \( H^- (q_1 + q_2) = H^- (q_2) + H^- (q_1) \)

iv) \( H^- (q_1 x q_2) = H^- (q_2) H^- (q_1) \)

\( H^+ \) and \( H^- \) operators similar to Hamilton operators\[2\]. Thus \( \forall q_1, q_2, q_3, q_4 \in \mathbb{H}/\mathbb{Z}_p \) following properties are provided.

i) \( q_1 x q_2 = H^+ (q_1) q_2 = H^- (q_2) q_1 \)

ii) \( H^+ (q_1 x q_2) = H^+ (q_1) q_2 = H^+ (q_1) H^+ (q_2) \)

iii) \( H^- (q_1 x q_2) = H^- (q_2) q_1 = H^- (q_2) H^- (q_1) \)

iv) \( H^+ (q_1 x q_2 + q_3 x q_4) = H^+ (q_1) H^+ + H^+ (q_3) H^+ (q_4) \)

v) \( H^- (q_1 x q_2 + q_3 x q_4) = H^- (q_2) H^- (q_1) + H^- (q_4) H^- (q_3) \)

vi) \( H^+ (H^- (q_1) q_2) = H^+ (q_2) H^+ (q_1) \)

vii) \( H^- (H^+ (q_1) q_2) = H^- (q_2) H^- (q_1) \)

viii) \( H^+ (q_1) H^- (q_2) = H^- (q_2) H^+ (q_1) \)

References


GÜLAY KORU YÜCEKAYA (gkoru@gazi.edu.tr) – Gazi University, Gazi Education Faculty, Mathematics Education Department, Teknikokullar, 06500, Ankara, Turkey