On a canonical form of a $3 \times 3$ Hermitian matrix over the ring of integral split octonions

Sergei Krutelevich

Department of Mathematics, Yale University, New Haven, CT 06520-8283, USA
Received 15 August 2001
Communicated by Efim Zelmanov

Abstract

We show that a $3 \times 3$ Hermitian matrix over the ring of integral split octonions has a unique canonical diagonal form under the action of the group $E_{6,6}(\mathbb{Z})$. This confirms the conjecture of J. Maldacena, G. Moore, and A. Strominger [hep-th/9903163] on a standard form of a charge vector. © 2002 Elsevier Science (USA). All rights reserved.

0. Introduction

In the paper [11] Maldacena et al. considered a model where charges of particles formed the $\mathbb{Z}^{27}$ representation of the group $E_{6,6}(\mathbb{Z})$.

They conjectured that any charge vector is equivalent to a so called standard three-charge system introduced in [12], at least if the cubic invariant of the vector is non-zero. This assertion is equivalent to diagonalizability of $3 \times 3$ Hermitian matrices over integral split octonions $\mathcal{H}_3(\mathfrak{o})$ using transformations in $E_{6,6}(\mathbb{Z})$ (see [3,11]). The authors proposed an idea to tackle this problem using the Hasse–Minkowski local $\rightarrow$ global principle and the strong approximation theorem.

The solution to the diagonalizability problem in the case of octonions over a field has been known for a long time. It follows from the results of N. Jacobson
(see, e.g., [8, Section 3]) that any $3 \times 3$ Hermitian matrix over the split octonion algebra (over a field) can be brought to a diagonal form. The answer is more interesting in the case of the octonion division algebra (over $\mathbb{R}$). It was known to H. Freudenthal in 1951 [4] (see also [9]) that an arbitrary $3 \times 3$ Hermitian matrix over the octonion division algebra can be diagonalized by an element of the group $F_4$, which is a subgroup of the group of type $E_6$.

It is interesting to note that there is a so-called exceptional cone (consisting of positive semi-definite matrices) in the space of $3 \times 3$ Hermitian matrices over the octonion division algebra. This exceptional cone is preserved under the action of the group $E_{6,2}$, which the real form of $E_6$ acting in this space (see [1] and references therein).

The answer to the diagonalizability question is different if we consider octonions over $\mathbb{Z}$. In the division case one needs to consider the lattice of $3 \times 3$ Hermitian matrices over Coxeter’s ring of integral octonions with the action of the integral form of the group $E_{6,2}$ (see [1,6] for details). Again this group stabilizes the exceptional cone. But in this case not every matrix in the cone can be brought to a diagonal form. For instance, it is easy to see that the identity matrix is the only possible diagonal form for a matrix in the set $S$ consisting of matrices with determinant 1 lying in the exceptional cone. But it was noted in [1, Section 5] that the group $E_{6,2}(\mathbb{Z})$ has two distinct orbits in the set $S$, which, in particular, implies that the answer to the diagonalizability question is negative in this case.

In the present paper we give an elementary proof that an arbitrary $3 \times 3$ Hermitian matrix over integral split octonions (i.e., any charge vector, including those with zero cubic invariant) can be brought to a diagonal form as was conjectured in [11]. Moreover, we describe an algorithm which allows one to bring any matrix to a diagonal canonical form (similar to the Smith normal form) using certain elementary transformations $\tau_{st}(q)$ in $E_{6,6}(\mathbb{Z})$.

These elementary transformations are defined using Jordan structure on the set $\mathcal{H}_3(o)$. Actually $\mathcal{H}_3(o)$ is not a linear Jordan algebra, since it is not closed under the Jordan operation $x \circ y = \frac{1}{2}(xy + yx)$ (because of the coefficient $\frac{1}{2}$). But it is a quadratic Jordan algebra in the sense of McCrimmon [10]. One can define so-called Bergman transformations $B(x, y)$ in a quadratic Jordan algebra (see, e.g., [2, Chapter 5.1]). Elementary transformations $\tau_{st}(q)$ defined by

$$
\tau_{st}(q) : A \mapsto (I_3 + q E_{st}) A (I_3 + \overline{q} E_{ts})
$$

$(A \in \mathcal{H}_3(o), \ t, s \in \{1, 2, 3\}, \ t \neq s, \ q \in o)$ are a special case of Bergman transformations.

Finally, we prove that the canonical diagonal form of every element in $\mathcal{H}_3(o)$ is unique.

**Theorem.** An arbitrary $3 \times 3$ Hermitian matrix over the ring of integral split octonions $o$ can be brought to a canonical diagonal form by a transformation from the group $E_{6,6}(\mathbb{Z})$. 
This canonical form has the following properties. Any non-zero element on the diagonal divides all diagonal elements below it. If the matrix is non-degenerate then all diagonal entries are positive, except the last one, whose sign is determined by the sign of the determinant of the original matrix. And if the matrix is degenerate, then zero diagonal entries are located in the lower right corner, and all non-zero entries are positive.

The canonical form of every element in \( \mathcal{H}_3(o) \) is unique.

A few words about notation. We will usually use small letters to denote integers, small \textbf{boldfaced} letters to denote quaternions and octonions, and capital letters to denote \( 3 \times 3 \) Hermitian matrices over octonions. As usual by \( I_n \) we denote the identity matrix of order \( n \), and by \( E_{st} \) we denote a matrix, whose \( st \)-entry is 1, and all other entries are zero. In this text such a matrix may be of order 2 or 3. The order of matrices considered will be clear from the context.

1. Integral split octonions

In this section we describe the ring of integral split octonions. First we describe a more familiar ring of integral quaternions. And then we construct the ring of integral octonions from them using the Cayley–Dickson duplication process.

The algebra of split quaternions over a field \( F \) can be described in two way: in terms of the standard basis \( 1, i, j, k \) with the following multiplication table [13, p. 34] (with \( \alpha = \beta = 1 \)):

\[
\begin{align*}
i^2 &= j^2 = 1, & k^2 &= -1, \\
ij &= -ji = k, & ik &= -ki = j, & jk &= -kj = i;
\end{align*}
\]

or as the algebra of \( 2 \times 2 \) matrices over the field \( F \) with the usual multiplication.

An isomorphism between these two realizations can be established in the following way:

\[
\begin{align*}
1 &\mapsto E_{11} + E_{22}, & i &\mapsto E_{11} - E_{22}, \\
j &\mapsto E_{12} + E_{21}, & k &\mapsto E_{12} - E_{21}.
\end{align*}
\]

It is more convenient for our purpose to use the latter realization. In these terms the concepts of conjugation, trace and norm for a quaternion

\[
a = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad (a, b, c, d \in F)
\]

look as follows:

\[
\bar{a} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}, \quad \text{Tr}(a) = a + d, \quad N(a) = \det(a) = ad - bc.
\]
The trace thus defined is evidently a linear function, and the norm is multiplicative. We can identify scalar matrices with elements of $F$, and then we have $a\overline{a} = \overline{a}a = N(a)$.

We define the ring of integral split quaternions $q$ as the ring of $2 \times 2$ matrices with entries in $\mathbb{Z}$. This ring is evidently closed under the conjugation, and the trace and the norm have integral values.

Now we construct the ring of integral octonions $o = q(v)$ by doubling the ring $q$ with the aid of a formal variable $v$ (see, e.g., [13] for details). We thus get a free $\mathbb{Z}$-module of rank 8 that consists of elements of the form $a + bv$ ($a, b \in q$) with multiplication defined by the formula

$$(a + bv) \cdot (c + dv) \triangleq (ac - \overline{d}b) + (da + b\overline{c})v, \quad a, b, c, d \in q.$$  

Now we extend the action of the conjugation, norm, and trace from $q$ to $o$ in the usual way:

$$\overline{a + bv} \triangleq \overline{a} - bv, \quad \text{Tr}(a + bv) \triangleq \text{Tr}(a),$$

$$N(a + bv) \triangleq N(a) + N(b).$$

These functions are well-defined. The trace is still linear, and the direct verification shows that the new norm is multiplicative. Note that the set of elements fixed by the involution coincides with the set of integers, embedded in the octonion ring in a natural way.

**Remark.** A more general construction [13] looks as follows. We define the doubled quaternion algebra $q(v, \gamma)$ as the set of pairs $a + bv$ with multiplication:

$$(a + bv) \cdot (c + dv) = (ac + \gamma \overline{d}b) + (da + b\overline{c})v,$$

where $a, b, c, d \in q$ and $\gamma$ is a non-zero element in the ground field. Then the norm is $N(a + bv) \triangleq N(a) - \gamma N(b)$.

In our case $\gamma$ must lie in $\mathbb{Z}$, and it was chosen to be $-1$ above. We note that $q(v, 1)$ and $q(v, -1)$ are isomorphic via $v \mapsto iv$, $i$ being the unit from the classical definition of quaternions. If we choose some other integer value for $\gamma$ then the ring $q(v, \gamma)$ is not isomorphic to $o$. And it seems that the result described below does not hold in $q(v, \gamma)$ with $\gamma \neq \pm 1$.

We will use the following properties of octonions throughout the text. The commutativity and associativity “under the trace”

$$\text{Tr}(xy) = \text{Tr}(yx), \quad \text{Tr}((xy)z) = \text{Tr}(x(yz))$$

(1)

for any $x, y, z \in o$. In addition we have the following identities:

$$\text{Tr}(x) = \text{Tr}(\overline{x}) = x + \overline{x}, \quad N(x + y) = N(x) + \text{Tr}(x\overline{y}) + N(y).$$

(2)
We also recall that though the octonion algebra is not associative, the alternative law holds in it. It means that the subalgebra generated by any two elements (and 1) is associative. An equivalent definition is that the associator is the alternative function of its arguments. (We will elaborate on that in the proof of Lemma 3 when we need it.)

We now state two easy lemmas about arithmetic of integral octonions. These lemmas will be used in the calculations below.

**Lemma 1** (Division with remainder). For any non-zero $a \in \mathbb{Z}$ and $x \in o$,

$$x = \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix} + \begin{pmatrix} x_5 & x_6 \\ x_7 & x_8 \end{pmatrix} v$$

there exists $q \in o$ such that the entries of the pair of matrices $x - qa$ are $r_l$’s, where $r_l$ is the remainder of the division of $x_l$ by $a$, $l = 1, \ldots, 8$. (We assume that the remainder is a positive integer in the interval $[0, \ldots, |a| - 1]$.)

**Proof.** We just find $q_l \in \mathbb{Z}$ such that $x_l - q_l a$ is the remainder of division of $x_l$ by $a$, $l = 1, \ldots, 8$. Then

$$q = \begin{pmatrix} q_1 & q_2 \\ q_3 & q_4 \end{pmatrix} + \begin{pmatrix} q_5 & q_6 \\ q_7 & q_8 \end{pmatrix} v$$

is the desired octonion. □

**Lemma 2.** Take any $a \in \mathbb{Z}$ and any non-zero integral octonion

$$x = \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix} + \begin{pmatrix} x_5 & x_6 \\ x_7 & x_8 \end{pmatrix} v.$$

Then for any non-zero $x_l$ ($l \in \{1, \ldots, 8\}$) there exist $q \in o$ with zero norm such that $a + \text{Tr}(qx)$ is equal to the remainder of the division of $a$ by $x_l$. (And here it is more convenient for our purposes to assume that the remainder is non-zero, i.e., it is an integer in the interval $[1, \ldots, |x_l|]$.)

**Proof.** First we find $p \in \mathbb{Z}$ such that $a - px_l$ is such a remainder. If $x_l$ is an entry in the “real part” of $x$, say, at the position $E_{st}$, then we take $q = -pE_{ts}$. Then evaluating $a + \text{Tr}(qx)$ we get the desired result.

Alternatively, if $x_l$ is an entry in the “imaginary part” of $x$, say, at the position $E_{st}v$, then we choose $q$ as follows. First we find an integral quaternion $q_1$ from the relation $\overline{q}_1 = pE_{ts}$, and then set $q = q_1 v$. Then we use $\text{Tr}(u) = \text{Tr}(\overline{u})$, $u \in o$, to verify that $a + \text{Tr}(qx) = a - px_l$.

Thus chosen $q$ evidently has zero norm. □

**Remark.** Since an octonion is essentially a pair of matrices, we will often refer to the entries of these matrices as the entries of the corresponding octonion.
2. A little bit of linear algebra over octonions

We consider the set \( \mathcal{H}_3(\mathfrak{o}) \) of Hermitian 3 \( \times \) 3 matrices over the integral split octonions. An arbitrary element \( A \) of this set has the form

\[
\begin{pmatrix}
  a & z & \bar{y} \\
  \bar{z} & b & x \\
  y & x & c
\end{pmatrix}, \quad a, b, c \in \mathbb{Z}, \quad x, y, z \in \mathfrak{o}.
\] (3)

The set \( \mathcal{H}_3(\mathfrak{o}) \) evidently has a structure of a free \( \mathbb{Z} \)-module of rank \( 3 + 3 \cdot \text{rank}_\mathbb{Z}(\mathfrak{o}) = 27 \). We define the concepts of determinant and rank for elements of this \( \mathbb{Z} \)-module following [1] and [8, Section 2].

We define the \textit{determinant} \( D : \mathcal{H}_3(\mathfrak{o}) \to \mathbb{Z} \) of a matrix \( A \) in \( \mathcal{H}_3(\mathfrak{o}) \) in the following way:

\[
D(A) = abc - a \cdot N(x) - b \cdot N(y) - c \cdot N(z) + \text{Tr}(xyz).
\]

And we define the \textit{rank} of a matrix \( A \) in \( \mathcal{H}_3(\mathfrak{o}) \) \( (0 \leq \text{rank}(A) \leq 3) \) in the following way:

- \( \text{rank}(A) = 0 \) iff \( A = 0 \).
- \( \text{rank}(A) \leq 1 \) iff the following conditions hold:
  \[
  bc - N(x) = 0, \quad ac - N(y) = 0, \quad ab - N(z) = 0,
  \] (4)
  \[
  a\bar{x} - yz = 0, \quad b\bar{y} - zx = 0, \quad c\bar{z} - xy = 0.
  \] (5)
- \( \text{rank}(A) \leq 2 \) iff \( D(A) = 0 \).
- Finally, \( \text{rank}(A) = 3 \) iff \( D(A) \neq 0 \).

**Remark.** In these terms the group \( E_{6,6}(\mathbb{Z}) \) can be described as the group of all transformations of the lattice \( \mathfrak{o} \) that preserve the determinant \( D \).

Now we introduce certain linear transformations of \( \mathfrak{o} \) and show that they preserve rank and determinant of an arbitrary element in \( \mathfrak{o} \).

We will use transformations of the following two types:

**Type I:** Transformations of the form \( \tau_{st}(q) \) with \( 1 \leq s, t \leq 3, s \neq t, q \in \mathfrak{o} \), which act on an element \( A \in \mathcal{H}_3(\mathfrak{o}) \) as follows:

\[
\tau_{st}(q) : A \mapsto (I_3 + qE_{st})A(I_3 + \bar{q}E_{ts}),
\] (6)

where \( I_3 \) is the identity 3 \( \times \) 3 matrix.\(^1\)

\(^1\) According to N. Jacobson, these transformations were introduced by H. Freudenthal in the Russian translation of [5].
An example of the action of $\tau_{12}(q)$ on a generic element in $H_3(\mathfrak{o})$ is written below
\[
\begin{pmatrix}
1 & q & 0 \\
0 & 1 & 0 \\
0 & 0 & 1
\end{pmatrix}
\begin{pmatrix}
a & z & \bar{y} \\
z & b & x \\
y & \bar{r} & c
\end{pmatrix}
\begin{pmatrix}
1 & 0 & 0 \\
\bar{q} & 1 & 0 \\
0 & 0 & 1
\end{pmatrix} =
\begin{pmatrix}
a + \text{Tr}(q\bar{z}) + bN(q) & z + qb & \bar{y} + qx \\
z + b\bar{q} & b & x \\
y + \bar{r}q & \bar{r} & c
\end{pmatrix}.
\]

Remarks. We note that though the multiplication in $\mathfrak{o}$ (and therefore in $H_3(\mathfrak{o})$) is not associative, the action of $\tau_{st}(q)$ is well-defined, since the entries of the resulting Hermitian matrix do not depend on the order in which we perform multiplication in (6).

Also we note that these transformations resemble the usual elementary transformations: adding $r$th row with a coefficient $q$ to the $s$th row. But to preserve the property of being Hermitian we need to perform the “conjugate” operation with the $t$th and $s$th columns. This results in some irregularity at the position $ss$ (see the example, $s = 1$). But as in the usual case, these transformations leave intact elements that are not located at the $s$th row/column.

Finally note that these transformations are also invertible. The inverse of $\tau_{st}(q)$ is $\tau_{st}(-q)$.

Type II: These are transformations of the form $\sigma_{st}$, $1 \leq s, t \leq 3$, $s \neq t$, which act on an element $A \in H_3(\mathfrak{o})$ as follows:
\[
\sigma_{st}: A \mapsto (E_{st} + E_{ts} + E_{uu})A(E_{st} + E_{ts} + E_{uu}),
\]
where $u$ is chosen so that we have equality of sets $\{s, t, u\} = \{1, 2, 3\}$.

An example of the action of $\sigma_{12}$ is given below:
\[
\begin{pmatrix}
0 & 1 & 0 \\
1 & 0 & 0 \\
0 & 0 & 1
\end{pmatrix}
\begin{pmatrix}
a & z & \bar{y} \\
z & b & x \\
y & \bar{r} & c
\end{pmatrix}
\begin{pmatrix}
0 & 1 & 0 \\
1 & 0 & 0 \\
0 & 0 & 1
\end{pmatrix} =
\begin{pmatrix}
b & z & x \\
z & a & \bar{y} \\
\bar{r} & y & c
\end{pmatrix}.
\]

We note that transformations of the second type can be expressed in terms of the transformations of the first type (with $q = \pm 1$). So in fact all these transformations lie in the group generated by $\tau_{st}(q)$.

Lemma 3. The transformations described above preserve determinant and rank of an arbitrary element in $H_3(\mathfrak{o})$.

Proof. Since transformations of Type II can be expressed in terms of the transformations of Type I, it is sufficient to prove the statement for transformations of the first type only.
First we show that transformations $\tau_s(t(q))$ preserve the determinant (see, e.g., [8, p. 75]). We prove it using the example of the action of $\tau_{12}(q)$ on an element $A$ of the form (3) above. The calculations in other cases are the same. So we need to evaluate the determinant of the matrix

$$
\begin{pmatrix}
  a + \text{Tr}(q \bar{z}) + b N(q) & z + qb & \bar{y} + qx \\
  z + b\bar{q} & b & x \\
  y + \bar{x}q & \bar{x} & c
\end{pmatrix}.
$$

(7)

It is equal to

$$
(a + \text{Tr}(q \bar{z}) + b N(q)) bc - (a + \text{Tr}(q \bar{z}) + b N(q)) \cdot N(x) - b \cdot N(y + \bar{x}q) - c \cdot N(z + qb) + \text{Tr}(x(y + \bar{x}q)(z + qb)).
$$

We group the original part of the determinant first and then collect all other terms:

$$
abc - a \cdot N(x) - b \cdot N(y) - c \cdot N(z) + \text{Tr}(xyz)
$$

$$+ bc \text{Tr}(q \bar{z}) + b^2 c N(q) - N(x) \text{Tr}(q \bar{z})
$$

$$- bN(x)N(q) - b \text{Tr}(yq x) - bN(x)N(q)
$$

$$- c \text{Tr}(bq \bar{z}) - b^2 c N(q) + \text{Tr}(bx yq) + \text{Tr}(N(x)qz) + \text{Tr}(bN(x)N(q)).
$$

Here we used the identity $N(u + v) = N(u) + \text{Tr}(u \bar{v}) + N(v)$, the multiplicativity of the norm, and associativity and commutativity “under the trace.” Then after cancellations we get

$$
abc - a \cdot N(x) - b \cdot N(y) - c \cdot N(z) + \text{Tr}(xyz) - 2b N(x) N(q)
$$

$$+ \text{Tr}(bN(x)N(q)).
$$

Here we used the linearity of the trace and the equality $\text{Tr}(u) = \text{Tr}(\bar{u})$. Finally we recall that for an integer $d$ we have $\text{Tr}(d) = 2d$, which yields the desired result.

Now we prove the statement about the rank. We note that it can be proved using general considerations [8, Section 2]. But here we prove it in an elementary way that requires some more calculations. We will use a similar argument once more, when we discuss the uniqueness of the canonical form in Section 3 (Lemma 4).

Evidently zero matrix is fixed by these transformations. By the statement about the determinant the property of being non-degenerate is preserved too. So we have the statement for ranks 0 and 3.

Now we show that rank 1 is also preserved. Once again we will do a sample calculation for the transformation $\tau_{12}(q)$. We need to show that the analogs of relations (4), (5) hold for the matrix (7). These calculations are routine, and we consider in detail only a couple of the most difficult cases.

So we have a matrix $A$ of rank 1, i.e., relations (4), (5) hold for $A$. We need to show that analogous relations hold for the image (7) of $A$ under $\tau_{12}(q)$. First we show that the analog of $ac = N(y)$ holds. We need to prove

$$
(a + \text{Tr}(q \bar{z}) + b N(q)) c - N(y) - \text{Tr}(yq x) - N(q) N(x) = 0.
$$
Using relations (4) we can do some cancellations and get

\[ c \, \mathrm{Tr}(q \overline{z}) - \mathrm{Tr}(y q x). \]

Using the commutativity and associativity “under the trace,” we rewrite it in the form

\[ \mathrm{Tr}\left((c \overline{z} - x y) \cdot q\right), \]

which is zero by (5).

Now we show that under the same assumptions the analog of \( a \overline{x} - yz = 0 \) holds for (7). We need to prove that

\[ a \overline{x} + \mathrm{Tr}(q \overline{z})\overline{x} + b N(q)\overline{x} - yz - yq b - (\overline{x} \overline{q})z - b N(q)\overline{x} = 0. \]

We can do some cancellations using relations (5) and arrive at

\[ \overline{x} \cdot \mathrm{Tr}(q \overline{z}) - yq b - (\overline{x} \overline{q})z \]

(\( \mathrm{Tr}(q \overline{z}) \) is proportional to 1 so it commutes with any element in the algebra).

Now we use the “commutativity under the trace” to rewrite it in the form

\[ \overline{x} \cdot \mathrm{Tr}(\overline{z} q) - yq b - (\overline{x} \overline{q})z. \]

Using the identity \( \mathrm{Tr}(u) = u + \overline{u} \) and the conjugate of the second relation in (5) we can write it as

\[ \overline{x}(\overline{z} q) + \overline{x}(\overline{q} z) - (\overline{x} \overline{z})q - (\overline{x} \overline{q})z, \]

which we can rewrite as

\[ (\overline{x}, \overline{z}, q) + (\overline{x}, \overline{q}, z). \]

Here \((\cdot, \cdot, \cdot)\) denotes the associator of a triple of elements: \((u, v, w) = u(vw) - (uv)w\). In particular, the associator is identically zero in any associative algebra. The associator is a multilinear function, so using the identity \( \mathrm{Tr}(u) = u + \overline{u} \) we can rewrite the last expression as

\[ (\overline{x}, \mathrm{Tr}(z), q) - (\overline{x}, \overline{z}, q) + (\overline{x}, \mathrm{Tr}(q), z) - (\overline{x}, q, z). \]

The trace of any element is a scalar multiple of 1, and therefore it lies in the nucleus of the octonion algebra (i.e., in the set of elements, which form an associative triple with any two elements of the algebra). Hence the two terms containing \( \mathrm{Tr} \) vanish, and we are left with

\[ -(\overline{x}, \overline{z}, q) - (\overline{x}, q, z). \]

Now we recall that in an alternative algebra the associator is the alternative function of its arguments (i.e., interchanging any two arguments changes the sign of the associator). Taking this into account we prove that the last expression is equal to zero.

We need to use the property of alternativity for other entries as well, but calculations for the remaining entries are much simpler.
We thus showed that rank 1 is also preserved under the transformations $\tau_{st}(q)$. For the remaining rank 2 we can argue as follows. Suppose that for some matrix $A$ of rank 2 the rank of its image $A'$ under $\tau_{st}(q)$ is equal to $n \neq 2$. Then the rank of $A'$ must be 0, 1, or 2, and by the above argument it is preserved. We apply $\tau_{12}(-q)$ to $A'$ and get $A$. Since the rank of $A'$ is preserved, we have $\text{rank}(A) = n$. This contradiction shows that transformations $\tau_{st}(q)$ preserve the rank of an arbitrary element in $H_3(o)$. $\Box$

**Corollary.** Transformations $\tau_{st}(q)$ lie in $E_{6,6}(\mathbb{Z})$, and therefore they generate a group $G$, which is a subgroup of $E_{6,6}(\mathbb{Z})$.

A couple of remarks are in order. First we note that the definition of rank given above coincides with the usual definition in case of Hermitian matrices over a field (ring of integers).

In the case of split octonions some surprising things may occur. For instance, if $x$ is a non-zero octonion with zero norm, then the rank of the matrix

$$
\begin{pmatrix}
0 & x & 0 \\
\bar{x} & 0 & 0 \\
0 & 0 & 0
\end{pmatrix}
$$

is 1.

Finally we note that definitions and assertions stated in this section are true in case of (not necessarily split) octonions over an arbitrary field.

### 3. The canonical form

In this section we show that we can bring any matrix in $H_3(o)$ to a diagonal form similar to the Smith normal form of usual integer matrices. For this we will use determinant preserving transformations described in the previous section. We note that the procedure makes essential use of the existence of octonions with zero norm. For instance, it will not work in the case of symmetric matrices over $\mathbb{Z}$. Also it was noted in [1] that not every $3 \times 3$ Hermitian matrix over the integral octonion division algebra is diagonalizable.

The procedure consists of two stages. First we bring any matrix to some diagonal form using transformations of Type I, and then we bring the diagonal to the *canonical* diagonal form in which each non-zero diagonal entry divides all other entries, which are below it on the diagonal.

Now we show how we do the first stage of the procedure, i.e., how we bring any matrix to a diagonal form. We start with an arbitrary matrix $A$ of the form

$$
\begin{pmatrix}
a & z & \bar{y} \\
\bar{z} & b & x \\
y & \bar{x} & c
\end{pmatrix}.
$$
For convenience we will write down the result of the action of transformations $\tau_{12}(q)$ and $\tau_{21}(q)$ on the element $A$.

$$\tau_{12}(q) : \begin{pmatrix} a & z & \bar{y} \\ \bar{z} & b & x \\ y & \bar{x} & c \end{pmatrix} \mapsto \begin{pmatrix} a + \text{Tr}(q\bar{z}) + bN(q) & z + qb & \bar{y} + qx \\
\bar{z} + bq & b & x \\
y + \bar{x}q & x & c \end{pmatrix},$$

$$\tau_{21}(q) : \begin{pmatrix} a & z & \bar{y} \\ \bar{z} & b & x \\ y & \bar{x} & c \end{pmatrix} \mapsto \begin{pmatrix} a & z + qa & \bar{y} \\
\bar{z} + aq & b + \text{Tr}(qz) + aN(q) & x + q\bar{y} \\
y & \bar{x} + y\bar{q} & c \end{pmatrix}.$$  

Note in particular that the only element in the first row affected by the transformation $\tau_{21}(q)$ is $z$ at the position 12.

If the first row (and therefore column) of $A$ has only zero entries, then we proceed to the $2 \times 2$ minor in the lower right corner. Otherwise we argue as follows.

If the entry at the position 11 is not zero, we enter the first loop (below). Otherwise we make that entry non-zero as follows. The octonion either at the position 12 or 13, say $z$ (at the position 12) is non-zero, so we can choose a non-zero entry $z_l$ in one of its constituent matrices, and by Lemma 2, find an octonion $q$ with zero norm such that $\text{Tr}(q\bar{z})$ is equal to $z_l$. Now we apply $\tau_{12}(q)$ to $A$, and since $N(q) = 0$, we get $z_l$ at the position 11. (For the purpose of effectiveness we may choose $z_l$ to be minimal by absolute value among the entries of $z$ and $\bar{y}$.) Denote the obtained matrix with a non-zero 11-entry by $A$.

**LOOP**

**Part 1.** Using transformations $\tau_{21}(q)$ and $\tau_{31}(q)$ with appropriate $q$’s chosen by Lemma 1, we can reduce entries of the octonion of $z$ and $\bar{y}$ modulo $|a|$. If after the reduction all entries of $z$ and $\bar{y}$ are zero, then we got zeros off-diagonal in the first row (and column) of $A$. So we may leave this loop and proceed further, otherwise we go to part two.

**Part 2.** Denote the matrix after the reduction by $A$ again. Then all entries of the octonions $z$, $\bar{y}$ are integers in the interval $[0, \ldots, |a| - 1]$, and at least one of them is non-zero. Say, this is entry $z_l$ of the octonion $z$. Again, by Lemma 2, we find $q$ with zero norm such that $a' \overset{\text{def}}{=} a + \text{Tr}(q\bar{z})$ is in the interval $[1, \ldots, |z_l|]$. Now we apply $\tau_{12}(q)$ and get the integer $a'$ at the position 11. By construction, we have $1 \leq a' \leq |a| - 1$. Denote the obtained matrix by $A$ again.

Now we repeat the loop several times, decreasing value of $a$ after each iteration. Since $a$ is bounded by 1 from below, the loop can not continue infinitely. So we will either leave the loop after Part 1 of some iteration; or get 1 at the position 11,
after which the reduction in Part 1 will turn off-diagonal elements in the first row/column to zero.

Thus after completing the loop above we bring the matrix $A$ to the form

$$
\begin{pmatrix}
a & 0 & 0 \\
0 & b & x \\
0 & \bar{x} & c \\
\end{pmatrix}
$$

of course, with new values of $a, b, c, x$.

At this step, we work with $2 \times 2$ minor in the lower right corner. We can use transformations of the form $\tau_{23}(q), \tau_{32}(q)$ in the loop similar to the one above to bring this $2 \times 2$ minor to the diagonal form. Since we have two zeros in the first row, these transformations do not affect the first row/column. So after completing this stage we bring the matrix to a diagonal form by a chain of transformations of the form $\tau_{st}(q)$.

Now we show how we can bring any diagonal matrix to the canonical form in which any non-zero diagonal entry divides any other diagonal entry which is below it, and if the matrix is degenerate the last several entries on the diagonal are zero. We also show that any matrix in $\mathcal{H}_3(o)$ has a unique canonical form with respect to the action of the group $G$.

We note that we can use transformations of Type II to interchange any two elements on the diagonal. This way we can move all zeros to the lower right corner of the diagonal.

The calculation below shows how we can replace a pair of integers $a, b$ on the diagonal by the pair $d, d'$, where $d = \gcd(a, b)$ and $d' = ab/d$. Then it follows that $d \mid d'$. Applying this operation at most three times we can bring our matrix to the desired form.

Without loss of generality we can assume that $a$ and $b$ are the first two entries on the diagonal. We let $d$ denote $\gcd(a, b)$, and $m, n$ be integers such that $am + bn = d$. We will also need an auxiliary octonion of norm zero and trace one, e.g.,

$$
\begin{pmatrix}
1 & 0 \\
0 & 0 \\
\end{pmatrix}
$$

We apply the following chain of transformations:

$$
\begin{pmatrix}
a & 0 & 0 \\
0 & b & 0 \\
0 & 0 & c \\
\end{pmatrix}
\xrightarrow{\tau_{12}((n-1)r)}
\begin{pmatrix}
a & (n-1)b \bar{r} & 0 \\
(n-1)b \bar{r} & b & 0 \\
0 & 0 & c \\
\end{pmatrix}
\xrightarrow{\tau_{21}(m-1)\bar{r}}
\begin{pmatrix}
a & ((m-1)a + (n-1)b) \bar{r} & 0 \\
((m-1)a + (n-1)b) \bar{r} & b & 0 \\
0 & 0 & c \\
\end{pmatrix}
$$
We can rewrite the last matrix in the form
\[
\begin{pmatrix}
d & dp & 0 \\
dp & b & 0 \\
0 & 0 & c
\end{pmatrix}
\]
with an appropriate \( p \in \mathfrak{o} \) (which can be easily calculated), and finally apply \( \tau_{21}(\overline{p}) \) to get
\[
\begin{pmatrix}
d & 0 & 0 \\
0 & b - dN(p) & 0 \\
0 & 0 & c
\end{pmatrix}.
\]

Since all transformations above were determinant-preserving, we should necessarily have \( d \cdot (b - dN(p)) = ab \). And this equality can be also verified directly.

Note that we could also get \(-d\) instead of \(d\) at the position of the element \(a\), therefore we can also make all non-zero diagonal entries positive, with the exception of the last one, the sign of which is determined by sign of the determinant of the original matrix.

One remark about the sign of the entries in the degenerate case, i.e., when at least one diagonal entry is zero. We can work with the pair \(a, 0\). In that case we can choose \(m\) to be \(-1\), so \(d = -a\). Since \(b = 0\), we will have \(N(p) = 0\), so we end up with the pair \(-a, 0\). Thus in the degenerate case we can make all diagonal entries nonnegative.

Summing up all above calculations, we arrive at the following

**Proposition 1.** Let \(G\) be the group of linear transformations of \(\mathcal{H}_3(\mathfrak{o})\) generated by \(\tau_{st}(q)\), \(1 \leq s, t \leq 3\), \(s \neq t\), \(q \in \mathfrak{o}\) (see (6)). An arbitrary \(3 \times 3\) Hermitian matrix over the ring of integral split octonions \(\mathfrak{o}\) can be brought to a canonical diagonal form by a transformation from the group \(G\).

This canonical form has the following properties. Any non-zero element on the diagonal divides all diagonal elements below it. If the matrix is non-degenerate then all diagonal entries are positive, except the last one, whose sign is determined by the sign of the determinant of the original matrix. And if the matrix is degenerate, then zero diagonal entries are located in the lower right corner, and all non-zero entries are positive.

We now show that matrices in the canonical form lie in distinct orbits under the action of the group \(G\) (and by the above we know that the union of the orbits is the whole \(\mathcal{H}_3(\mathfrak{o})\)).
We need to introduce another definition. We say that a non-zero integer \( d \) divides an integral octonion \( x \in o \), if there is an \( x_1 \in o \) such that \( x = d \cdot x_1 \). It follows from the definition of octonions that it happens if and only if all entries of \( x \) are divisible by \( d \). It is not difficult to verify that the last condition is equivalent to the condition

\[
\text{for any } u \in o \text{ we have } d \mid \text{Tr}(x \cdot u). \tag{8}
\]

Now we introduce two integers that can be associated with a matrix \( A \) and show that these numbers are invariant under the action of the group \( G \). For an arbitrary matrix \( A \in H_3(o) \) we define \( d_1(A) \) to be the g.c.d. of all entries of \( A \). Essentially this is the g.c.d. of the collection of 27 integers that form entries of \( A \).

We define \( d_2(A) \) to be the g.c.d. of left-hand sides of the expressions (4) and (5), where \( A \) is a matrix of the form (3). Note that this number can be interpreted as the g.c.d. of the determinants of \( 2 \times 2 \) minors of the original matrix. (For completeness one needs to consider three more minors conjugate to (5), but the others do not influence the value of \( d_2 \).) We will give another interpretation for these minors below.

Here we assume that the g.c.d. is by definition non-negative, and the g.c.d. of a collection of zeros is defined to be zero.

**Lemma 4.** For any \( A \in H_3(o) \) and any \( g \in G \) we have

\[
\begin{align*}
    d_1(gA) &= d_1(A), \\
    d_2(gA) &= d_2(A), \\
    D(gA) &= D(A).
\end{align*}
\]

**Proof.** It is sufficient to verify the statement for generators \( \tau_{st}(q) \). Since these transformations lie in \( E_{6,6}(\mathbb{Z}) \), it follows that the statement is true for \( D \). We will do sample calculations with \( g = \tau_{12}(q) \) to verify the statement for \( d_1, d_2 \). We assume that \( A \) is of the form (3), and then its image \( gA \) has the form (7).

Let \( d_1 = d_1(A) \) be the g.c.d. of entries of \( A \). It follows from (8) that \( d_1 \) divides \( a + \text{Tr}(q\overline{z}) + bN(q) \), and for other entries of (7) it is just obvious. Hence the g.c.d. does not decrease under the action of \( \tau_{12}(q) \). To prove that it does not increase we use the following “reverse” argument. Let \( A' \) denote the image of \( A \). Then \( \tau_{12}(-q) \) maps \( A' \) to \( A \). By the above argument the g.c.d. does not decrease in the process. Therefore g.c.d.(\( A \)) = g.c.d.(\( A' \)), and the assertion for \( d_1 \) follows.

Let \( d_2 = d_2(A) \). First we show that \( d_2 \) divides the corresponding expressions for the image \( A' \) of \( A \). The argument here is the same as in the case of rank 1 of Lemma 3. One just needs to replace the condition “equal to 0” by the condition “divisible by \( d_2 \).” This argument shows that the g.c.d. can not decrease, that is \( d_2 \mid d_2(A') \). Using the “reverse” argument from the previous paragraph, we prove that the g.c.d. does not increase. Therefore it is indeed invariant, i.e., \( d_2(A) = d_2(gA) \). \( \square \)
Now let us see how the invariants of a matrix in a canonical form are related to the entries of the matrix. Consider a matrix \( C \) in a canonical diagonal form with entries \( c_1, c_2, c_3 \in \mathbb{Z} \). We have \( c_1 | c_2, c_2 \mid c_3, c_1 \geq 0, c_2 \geq 0 \). Then it follows that

\[
\begin{align*}
d_1(C) &= c_1, \\
d_2(C) &= c_1c_2, \\
D(C) &= c_1c_2c_3.
\end{align*}
\]

In particular, these invariants uniquely determine entries of \( C \) (as a matrix in a canonical form). This assertion is obvious, if all the invariants are non-zero.

The entry \( c_1 \) is always uniquely determined by \( d_1(C) \). If \( c_1 = 0 \), then \( c_2 = c_3 = 0 \) by definition, otherwise \( c_2 = d_2(C)/c_1 \). So \( c_2 \) is also uniquely determined.

Finally, if \( c_2 = 0 \) then \( c_3 = 0 \); otherwise \( c_2 \neq 0 \) and \( c_1 \neq 0 \). So in this case \( c_3 \) is uniquely determined by \( c_3 = D(C)/c_1c_2 \).

**Lemma 5.** Let \( A \) be an arbitrary matrix in \( \mathcal{H}_3(\mathfrak{o}) \), and let \( C \) be a matrix in the canonical form such that there exists \( g \in G \) such that \( C = gA \) (it exists by Proposition 1). Then \( C \) is uniquely defined by \( A \), and its diagonal entries \( c_1, c_2, c_3 \) satisfy equations:

\[
\begin{align*}
d_1(A) &= c_1, \\
d_2(A) &= c_1c_2, \\
D(A) &= c_1c_2c_3,
\end{align*}
\]

where \( d_1, d_2 \) are the invariants described above.

**Proof.** Since \( C = gA \), by Lemma 4 we have that their invariants are equal: \( D(A) = D(C), d_i(A) = d_i(C), i = 1, 2 \). And by the above remark these invariants uniquely determine entries of \( C \). \( \square \)

It follows from Lemma 5 that the \( G \)-orbit of any element in \( \mathcal{H}_3(\mathfrak{o}) \) contains a unique matrix in the canonical form. Now we want to show that numbers \( d_1, d_2 \) are invariant with respect to the action of \( E_{6,6}(\mathbb{Z}) \), which allows us to extend the uniqueness of the canonical form to \( E_{6,6}(\mathbb{Z}) \)-orbits.

First we make a few general remarks about the \( \mathbb{Z} \)-module \( \mathcal{H}_3(\mathfrak{o}) \). We recall that it is a free \( \mathbb{Z} \)-module, so we have a basis such that any element in \( \mathcal{H}_3(\mathfrak{o}) \) is a unique linear combination of basis elements with integer coefficients. For instance we can choose such a basis in the following way. We consider basis \( B_1 = \{e_{11}, e_{12}, e_{21}, e_{22}\} \) in the ring of integral quaternions \((= 2 \times 2\text{-matrices})\). Then the set of eight elements

\[
B_2 = \{b, bv | b \in B_1, v \text{ is the imaginary unit from the duplication process}\}
\]

forms a basis of \( \mathfrak{o} \). Finally we can take the set

\[
B = \{E_{11}, E_{22}, E_{33}, bE_{ij} + \bar{b}E_{ji} | b \in B_2, 1 \leq i < j \leq 3\}
\]

as a basis of \( \mathcal{H}_3(\mathfrak{o}) \).

Using such a basis we can write any element of \( \mathcal{H}_3(\mathfrak{o}) \) as a row of length 27 with integer entries.
We will also need to consider vector space $\mathcal{H}_3(o_F) \overset{\text{def}}{=} \mathcal{H}_3(o \otimes_\mathbb{Z} F)$, where $F$ is any field of characteristic zero. Then the basis of $\mathcal{H}_3(o)$ will give rise to a basis of the vector space $\mathcal{H}_3(o_F)$.

Next we note that any endomorphism of the $\mathbb{Z}$-module $\mathcal{H}_3(o)$ can be extended uniquely to an endomorphism of the vector space $\mathcal{H}_3(o_F)$. And in terms of the basis that we have, any endomorphism of $\mathcal{H}_3(o_F)$ can be written as a $27 \times 27$ matrix with entries in $F$ (acting on rows from the right by matrix multiplication).

Of course not all such matrices will define an endomorphism of the module $\mathcal{H}_3(o)$, since not all of them will preserve this lattice. Let us see which conditions we should impose on the entries of a matrix $\tau \in \text{Mat}(27 \times 27, F)$ so that it defines an endomorphism of $\mathcal{H}_3(o)$.

Evidently, if all entries of $\tau$ are integers, then it maps a row of integers into a row of integers, and therefore preserves the module $\mathcal{H}_3(o)$. Conversely, suppose that $\tau$ has a non-integer entry, say $t_{ij}$. Then acting by $\tau$ on the vector

$$b_i \overset{\text{def}}{=} (0, \ldots, 0, 1, 0, \ldots, 0)$$

we get $t_{ij}$ at the $j$th position of the resulting vector. So in this case $\tau$ is not an endomorphism of the module $\mathcal{H}_3(o)$.

It follows from the above argument that $\tau$ is an endomorphism of $\mathcal{H}_3(o)$ if and only if all entries of the corresponding $27 \times 27$ matrix are integers. Now we are ready to prove our next lemma.

**Lemma 6.** The invariant $d_1$ (the g.c.d. of all entries of a matrix in $\mathcal{H}_3(o)$) is preserved under the action of the group $E_{6,6}(\mathbb{Z})$.

**Proof.** Let $A$ denote an arbitrary element of $\mathcal{H}_3(o)$. We know that using our basis we can represent $A$ as a row of 27 integers. And the invariant $d_1$ is the g.c.d. of this collection.

Pick an arbitrary transformation $\tau$ in $E_{6,6}(\mathbb{Z})$. By the above we know that we can write it as a matrix with integer entries. The result $A_1$ of the action of $\tau$ on $A$ is a row whose entries are linear combinations of entries of $A$ with integer coefficients. Therefore $d_1$ divides all of them, and hence we have $d_1(A) \mid d_1(A_1)$.

To prove that this invariant can not increase we apply the reverse argument that we used in previous sections. Namely, we have that $\tau^{-1}$ also lies in $E_{6,6}(\mathbb{Z})$. We apply the above argument to the data $\tau^{-1} : A_1 \mapsto A$, which will give us $d_1(A_1) \mid d_1(A)$.

Therefore we indeed have $d_1(A) = d_1(\tau(A))$ for any $\tau$ in $E_{6,6}(\mathbb{Z})$. □

Note that we did not use in the proof of the lemma that $\tau$ preserves the determinant of elements. In fact this assertion holds for any endomorphism of $\mathcal{H}_3(o)$ whose inverse is also an endomorphism of $\mathcal{H}_3(o)$. 
We now proceed to proving the invariance of $d_2$. For this we need to introduce a few more concepts and definitions. One can use the work [8, Section 2] as a reference point.

We can associate an element $A \in \mathfrak{o}$ to an element denoted by $A^\sharp$ (Jacobson [8] uses notation $A \times A$ for this element), which is defined in the following way:

$$A^\sharp \overset{\text{def}}{=} A^2 - \text{Tr}(A)A + \frac{1}{2}((\text{Tr}(A))^2 - \text{Tr}(A^2))1. \tag{10}$$

(The product on the right-hand side is the Jordan multiplication, but since all elements lie in the subalgebra (with 1) generated by $A$, the Jordan multiplication coincides with the usual multiplication of $3 \times 3$ matrices. One can think of $A^\sharp$ as the adjoint matrix of $A$.)

If $A$ has form

$$A = \begin{pmatrix} a & z & \overline{y} \\ \overline{z} & b & x \\ y & \overline{x} & c \end{pmatrix}$$

then $A^\sharp$ looks as follows:

$$A^\sharp = \begin{pmatrix} bc - N(x) & \overline{yx} - cz & zx - b\overline{y} \\ xy - c\overline{z} & ac - N(y) & \overline{zx} - ax \\ \overline{yz} - b\overline{x} & yz - a\overline{x} & ab - N(z) \end{pmatrix}.$$ 

In particular we have that the operation $\sharp$ leaves $H_3(\mathfrak{o})$ invariant. Also note that entries of $A^\sharp$ are $2 \times 2$ minors of the matrix $A$, which appear in (4), (5). It follows that $\text{rank}(A) \leq 1$ if and only if $A^\sharp = 0$.

Another important consequence of definitions is that

$$d_2(A) = d_1(A^\sharp). \tag{11}$$

We will also need two facts about automorphisms of Jordan algebras due to N. Jacobson. (We state them in somewhat weaker form sufficient for our purposes.)

**Lemma 7** [7, Theorems 1, 4]. Let $J$ be a central simple Jordan algebra over a field $F$ of characteristic zero, and let $T$ and $N$ denote the generic trace and norm of elements of $J$. Let $L$ denote the group of all invertible norm preserving transformations of $J$. Then

- for any $u \in J$ and any automorphism $\tau$ of $J$ we have $T(u) = T(\tau(u))$ and $N(u) = N(\tau(u))$.
- $\tau$ is an automorphism of $J$ if and only if $\tau \in L$ and $\tau(1) = 1$.

In the case of the exceptional Jordan algebra of $3 \times 3$ Hermitian matrices over octonions the generic trace and norm coincide with the usual trace and determinant defined above.
We now state a series of a few simple lemmas, which will prove the invariance of $d_2$ under the action of the group $E_{6,6}(\mathbb{Z})$.

**Lemma 8.** Let $\tau$ be an element of $E_{6,6}(\mathbb{Z})$ and in addition assume that $\tau$ is an automorphism of the Jordan algebra $\mathcal{H}_3(o_F)$. Then $\tau$ preserves the invariant $d_2$ of any element $A$ in $\mathcal{H}_3(o)$.

**Proof.** We have the following chain of equalities:

$$d_2(\tau(A)) = d_1(\tau(A)^2) = d_1(\tau(A^2)) = d_1(A^2) = d_2(A).$$

The first and the last equalities follow from the relation (11), and the second equality follows from (10) using the definition of automorphism and the first part of Lemma 7. Finally, we have the third equality by Lemma 6, since $\tau \in E_{6,6}(\mathbb{Z})$. $\square$

**Lemma 9.** Any element $\eta$ in $E_{6,6}(\mathbb{Z})$ can be represented in the form

$$\eta = T \tau,$$

where $T$ belongs to the group $G$, and $\tau$ is an automorphism of the Jordan algebra $\mathcal{H}_3(o_F)$ preserving the lattice $\mathcal{H}_3(o)$.

**Proof.** Denote by $B$ the result of the action of $\eta$ on $1$: $B \overset{\text{def}}{=} \eta(1)$. Since $\eta \in E_{6,6}(\mathbb{Z})$ we have $B \in \mathcal{H}_3(o)$ and $N(B) = 1$. It follows from the results on $G$-orbits (Proposition 1) that the group $G$ acts transitively on the set of elements with determinant $1$ in $\mathcal{H}_3(o)$ (the only possible canonical form for such elements is the identity matrix).

Therefore there exists $T \in G$ such that $T(1) = B$. Consider element $\tau \overset{\text{def}}{=} T^{-1}\eta$. We have $\tau(1) = 1$, hence by Lemma 7, $\tau$ is an automorphism of $\mathcal{H}_3(o_F)$. Hence $\eta = T \tau$ as desired. Finally $\tau$ preserves the lattice, since $\tau = T^{-1}\eta \in E_{6,6}(\mathbb{Z})$. $\square$

**Lemma 10.** The invariant $d_2$ is preserved under the action of the group $E_{6,6}(\mathbb{Z})$.

**Proof.** The proof is just a combination of the two previous results. Let $\eta$ be an arbitrary element in $E_{6,6}(\mathbb{Z})$. By Lemma 9 write $\eta$ in the form $\eta = T \tau$, where $T \in G$ and $\tau$ is an automorphism. Then $T$ preserves $d_2$ by Lemma 4, and so does $\tau$ by Lemma 8. Hence $\eta$ also preserves $d_2$. $\square$

**Theorem.** An arbitrary $3 \times 3$ Hermitian matrix over the ring of integral split octonions $o$ can be brought to a canonical diagonal form by a transformation from the group $E_{6,6}(\mathbb{Z})$.

This canonical form has the following properties. Any non-zero element on the diagonal divides all diagonal elements below it. If the matrix is non-degenerate
then all diagonal entries are positive, except the last one, whose sign is determined by the sign of the determinant of the original matrix. And if the matrix is degenerate, then zero diagonal entries are located in the lower right corner, and all non-zero entries are positive.

The canonical form of every element in \( \mathcal{H}_3(\mathfrak{o}) \) is unique.

**Proof.** The existence of a canonical form has been proved in Proposition 1. We can actually use transformations \( \tau_{st}(q) \) to bring any matrix to a canonical form.

So it only remains to prove the uniqueness of the canonical form. The argument here is similar to the argument in Lemma 5.

Take an arbitrary element \( A \in \mathcal{H}_3(\mathfrak{o}) \), and let \( C \) be a matrix in a canonical form (with diagonal entries \( c_1, c_2, c_3 \in \mathbb{Z} \)) such that there exists \( \eta \in E_{6,6}(\mathbb{Z}) \) with \( C = \eta(A) \). We need to show that such a \( C \) is unique.

As we have seen before,

\[
c_1 = d_1(C), \quad c_1c_2 = d_2(C), \quad c_1c_2c_3 = D(C),
\]

and \( c_i \)'s are uniquely determined by the numbers on the right. It follows from Lemmas 6, 10, and the definition that

\[
d_1(A) = d_1(C), \quad d_2(A) = d_2(C), \quad D(A) = D(C).
\]

Combining these two assertions we get that the entries \( c_i \) of \( C \) are uniquely determined by \( A \), so the canonical form of \( A \) is unique. \( \square \)

Note that we can repeat all arguments above (with obvious simplifications) in the case of integral split quaternions. Therefore we get the following corollary.

**Corollary.** The above theorem also holds in the case of \( 3 \times 3 \) Hermitian matrices over the ring of integral split quaternions \( q \).

**Acknowledgments**

The author is grateful to G. Moore and E. Zelmanov for helpful discussions.

**References**


