Algebra & Number Theory

Volume 18

2024

No. 12

Separating G_2-invariants of several octonions

Artem Lopatin and Alexandr N. Zubkov

msp

ALGEBRA AND NUMBER THEORY 18:12 (2024)
https://doi.org/10.2140/ant.2024.18.2157

Separating G_2-invariants of several octonions

Artem Lopatin and Alexandr N. Zubkov

We describe separating G_2-invariants of several copies of the algebra of octonions over an algebraically closed field of characteristic two. We also obtain a minimal separating and a minimal generating set for G_2-invariants of several copies of the algebra of octonions in case of a field of odd characteristic.

1. Introduction

All vector spaces and algebras are considered over an algebraically closed field $\mathbb{F}$ of arbitrary characteristic $p = \operatorname{char} \mathbb{F} \geq 0$.

We continue the study of the invariants of the diagonal action of the exceptional simple group G_2 on the space of several octonions, over a field of positive characteristic. Over the field of complex numbers, this was done in [20]. This result has been generalized to an arbitrary infinite field of odd characteristic in [23], using a much finer technique of modules with good filtration, together with some results from the theory of groups with triality.

Unfortunately, the technique of modules with good filtration no longer works over a field of characteristic two and the complete description of the generating invariants in this case seems to be an extremely difficult problem. Thus, it makes sense to describe separating invariants, since they satisfy the most important property of ordinary invariants to separate closed orbits in the Zariski topology. The latter problem is usually more accessible and it does not require extremely technical methods. We describe the separating invariants over an algebraically closed field of characteristic two, using a detailed description of the subalgebras of the octonion algebra (up to the action of G_2) and the Hilbert–Mumford criterion (the "if" part; see Section 3B).

The article is organized as follows. In Sections 2A and 2B we define the octonion algebra $\boldsymbol{O}$, the group G_2 and the algebra of G_2-invariants $\mathbb{F}[\boldsymbol{O}^n]^{G_2}$ of n copies of the algebra of octonions $\boldsymbol{O}$. We use notation from [23]. Generators and relations between generators for $\mathbb{F}[\boldsymbol{O}^n]^{G_2}$ were described by Schwarz [20] over $\mathbb{F} = \mathbb{C}$. Zubkov and Shestakov described generators for $\mathbb{F}[\boldsymbol{O}^n]^{G_2}$ over an arbitrary field with $\operatorname{char} \mathbb{F} \neq 2$ (see Section 2D), but generators for the algebra $\mathbb{F}[\boldsymbol{O}^n]^{G_2}$ are still not known in case $p = 2$. The invariants for the action of F_4 on several copies of the split Albert algebra were studied in [10]. Our results are formulated in Section 2E. In Section 3 some definitions and notation are given. In Section 4

The work was supported by UAEU grant G00003324 and partially supported in accordance with the state task of the IM SB RAS, project FWNF-2022-0003.
MSC2020: 14L30, 17A75, 17D05, 20F29, 20G05.
Keywords: polynomial invariants, exceptional groups, separating set, generating set, matrix invariants, positive characteristic.

we describe a minimal generating and a minimal separating set for $\mathbb{F}[\boldsymbol{O}^n]^{G_2}$ in case $p \neq 2$. In Section 5 a minimal generating set is constructed for the subalgebra $T_n \subset \mathbb{F}[\boldsymbol{O}^n]^{G_2}$ of trace invariants in case $p = 2$. In Section 6 subalgebras of $\boldsymbol{O}$ of dimension ≤ 3 are described modulo G_2-action in case $p = 2$. This result is applied in Section 7 to obtain our main result which is the description of a separating set for $\mathbb{F}[\boldsymbol{O}^n]^{G_2}$ in case $p = 2$.

2. Invariants of octonions

2A. ***Octonions.*** The *octonion algebra* $\boldsymbol{O} = \boldsymbol{O}(\mathbb{F})$, also known as the *split Cayley algebra*, is the vector space of all matrices

$$a = \begin{pmatrix} \alpha & \boldsymbol{u} \\ \boldsymbol{v} & \beta \end{pmatrix} \quad \text{with } \alpha, \beta \in \mathbb{F} \text{ and } \boldsymbol{u}, \boldsymbol{v} \in \mathbb{F}^3,$$

endowed with the multiplication

$$aa' = \begin{pmatrix} \alpha\alpha' + \boldsymbol{u} \cdot \boldsymbol{v}' & \alpha\boldsymbol{u}' + \beta'\boldsymbol{u} - \boldsymbol{v} \times \boldsymbol{v}' \\ \alpha'\boldsymbol{v} + \beta\boldsymbol{v}' + \boldsymbol{u} \times \boldsymbol{u}' & \beta\beta' + \boldsymbol{v} \cdot \boldsymbol{u}' \end{pmatrix}, \quad \text{where } a' = \begin{pmatrix} \alpha' & \boldsymbol{u}' \\ \boldsymbol{v}' & \beta' \end{pmatrix},$$

$\boldsymbol{u} \cdot \boldsymbol{v} = u_1v_1 + u_2v_2 + u_3v_3$ and $\boldsymbol{u} \times \boldsymbol{v} = (u_2v_3 - u_3v_2, u_3v_1 - u_1v_3, u_1v_2 - u_2v_1)$. For short, define $\boldsymbol{c}_1 = (1, 0, 0)$, $\boldsymbol{c}_2 = (0, 1, 0)$, $\boldsymbol{c}_3 = (0, 0, 1)$, $\boldsymbol{0} = (0, 0, 0)$ from $\mathbb{F}^3$. Consider the following basis of $\boldsymbol{O}$:

$$e_1 = \begin{pmatrix} 1 & \boldsymbol{0} \\ \boldsymbol{0} & 0 \end{pmatrix}, \quad e_2 = \begin{pmatrix} 0 & \boldsymbol{0} \\ \boldsymbol{0} & 1 \end{pmatrix}, \quad \boldsymbol{u}_i = \begin{pmatrix} 0 & \boldsymbol{c}_i \\ \boldsymbol{0} & 0 \end{pmatrix}, \quad \boldsymbol{v}_i = \begin{pmatrix} 0 & \boldsymbol{0} \\ \boldsymbol{c}_i & 0 \end{pmatrix}$$

for $i = 1, 2, 3$. The unity of $\boldsymbol{O}$ is denoted by $1_{\boldsymbol{O}} = e_1 + e_2$. We identify octonions

$$\alpha 1_{\boldsymbol{O}}, \quad \begin{pmatrix} 0 & \boldsymbol{u} \\ \boldsymbol{0} & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & \boldsymbol{0} \\ \boldsymbol{v} & 0 \end{pmatrix}$$

with $\alpha \in \mathbb{F}$, $\boldsymbol{u}, \boldsymbol{v} \in \mathbb{F}^3$, respectively. Similarly to $\boldsymbol{O}(\mathbb{F})$ we define the algebra of octonions $\boldsymbol{O}(\mathcal{A})$ over any commutative associative $\mathbb{F}$-algebra $\mathcal{A}$.

The algebra $\boldsymbol{O}$ has a linear involution

$$\bar{a} = \begin{pmatrix} \beta & -\boldsymbol{u} \\ -\boldsymbol{v} & \alpha \end{pmatrix}, \quad \text{satisfying } \overline{aa'} = \bar{a}'\bar{a},$$

a *norm* $n(a) = a\bar{a} = \alpha\beta - \boldsymbol{u} \cdot \boldsymbol{v}$, and a nondegenerate symmetric bilinear *form*

$$q(a, a') = n(a + a') - n(a) - n(a') = \alpha\beta' + \alpha'\beta - \boldsymbol{u} \cdot \boldsymbol{v}' - \boldsymbol{u}' \cdot \boldsymbol{v}.$$

Define the linear function *trace* by $\mathrm{tr}(a) = a + \bar{a} = \alpha + \beta$. The subspace $\{a \in \boldsymbol{O} \mid \mathrm{tr}(a) = 0\}$ of traceless octonions is denoted by $\boldsymbol{O}_0$. Notice that

$$\mathrm{tr}(aa') = \mathrm{tr}(a'a) \quad \text{and} \quad n(aa') = n(a)n(a'). \tag{2-1}$$

The following quadratic equation holds:

$$a^2 - \mathrm{tr}(a)a + n(a) = 0. \tag{2-2}$$

Since

$$n(a+a') = n(a) + n(a') - \mathrm{tr}(aa') + \mathrm{tr}(a)\,\mathrm{tr}(a'), \tag{2-3}$$

the linearization of (2-2) implies

$$aa' + a'a - \mathrm{tr}(a)a' - \mathrm{tr}(a')a - \mathrm{tr}(aa') + \mathrm{tr}(a)\,\mathrm{tr}(a') = 0. \tag{2-4}$$

The algebra $\boldsymbol{O}$ is a simple *alternative* algebra, i.e., the following identities hold for $a, b \in \boldsymbol{O}$:

$$a(ab) = (aa)b, \quad (ba)a = b(aa). \tag{2-5}$$

The linearization implies that

$$a(a'b) + a'(ab) = (aa' + a'a)b, \quad (ba)a' + (ba')a = b(aa' + a'a). \tag{2-6}$$

The trace is associative, i.e., for all $a, b, c \in \boldsymbol{O}$ we have

$$\mathrm{tr}((ab)c) = \mathrm{tr}(a(bc)). \tag{2-7}$$

Note that

$$2n(a) = -\mathrm{tr}(a^2) + \mathrm{tr}^2(a) \quad \text{for each } a \in \boldsymbol{O}. \tag{2-8}$$

More details on $\boldsymbol{O}$ can be found in Sections 1 and 3 of [23].

2B. ***The group G_2.*** The group $G_2 = G_2(\mathbb{F})$ is known to be the group $\mathrm{Aut}(\boldsymbol{O})$ of all automorphisms of the algebra $\boldsymbol{O}$. The group G_2 contains a Zariski closed subgroup $\mathrm{SL}_3 = \mathrm{SL}_3(\mathbb{F})$. Namely, every $g \in \mathrm{SL}_3$ defines the following automorphism of $\boldsymbol{O}$:

$$a \to \begin{pmatrix} \alpha & \boldsymbol{u}g \\ \boldsymbol{v}g^{-T} & \beta \end{pmatrix},$$

where g^{-T} stands for $(g^{-1})^T$ and $\boldsymbol{u}, \boldsymbol{v} \in \mathbb{F}^3$ are considered as row vectors. In what follows SL_3 is regarded as this subgroup of G_2. For every $\boldsymbol{u}, \boldsymbol{v} \in \boldsymbol{O}$ define $\delta_1(\boldsymbol{u}), \delta_2(\boldsymbol{v})$ from $\mathrm{Aut}(\boldsymbol{O})$ as

$$\delta_1(\boldsymbol{u})(a') = \begin{pmatrix} \alpha' - \boldsymbol{u}\cdot\boldsymbol{v}' & (\alpha' - \beta' - \boldsymbol{u}\cdot\boldsymbol{v}')\boldsymbol{u} + \boldsymbol{u}' \\ \boldsymbol{v}' - \boldsymbol{u}' \times \boldsymbol{u} & \beta' + \boldsymbol{u}\cdot\boldsymbol{v}' \end{pmatrix}, \quad \delta_2(\boldsymbol{v})(a') = \begin{pmatrix} \alpha' + \boldsymbol{u}'\cdot\boldsymbol{v} & \boldsymbol{u}' + \boldsymbol{v}' \times \boldsymbol{v} \\ (-\alpha' + \beta' - \boldsymbol{u}'\cdot\boldsymbol{v})\boldsymbol{v} + \boldsymbol{v}' & \beta' - \boldsymbol{u}'\cdot\boldsymbol{v} \end{pmatrix}.$$

The group G_2 is generated by SL_3 and $\delta_1(t\boldsymbol{u}_i), \delta_2(t\boldsymbol{v}_i)$ for all $t \in \mathbb{F}$ and $i = 1, 2, 3$ (for example, see Section 3 of [23]). By straightforward calculations we can see that

$$\hbar : \boldsymbol{O} \to \boldsymbol{O}, \quad \text{defined by } a \to \begin{pmatrix} \beta & -\boldsymbol{v} \\ -\boldsymbol{u} & \alpha \end{pmatrix}, \tag{2-9}$$

belongs to G_2 (see also the proof of Lemma 1 of [23]).

The action of G_2 on $\boldsymbol{O}$ satisfies the properties

$$\overline{ga} = g\bar{a}, \quad \mathrm{tr}(ga) = \mathrm{tr}(a), \quad n(ga) = n(a), \quad q(ga, ga') = q(a, a').$$

Thus, $\boldsymbol{O}_0$ is a G_2-submodule of $\boldsymbol{O}$.

Consider the diagonal action of G_2 on the vector space $\boldsymbol{O}^n = \boldsymbol{O} \oplus \cdots \oplus \boldsymbol{O}$ (n copies), that is, $g(a_1, \dots, a_n) = (ga_1, \dots, ga_n)$ for all $g \in G_2$ and $a_1, \dots, a_n \in \boldsymbol{O}$. The coordinate ring of the affine variety $\boldsymbol{O}^n$ is the polynomial $\mathbb{F}$-algebra $K_n = \mathbb{F}[\boldsymbol{O}^n] = \mathbb{F}[z_{ij} \mid 1 \le i \le n,\ 1 \le j \le 8]$, where $z_{ij} : \boldsymbol{O}^n \to \mathbb{F}$ is defined by $(a_1, \dots, a_n) \to \alpha_{ij}$ for

$$a_i = \begin{pmatrix} \alpha_{i1} & (\alpha_{i2}, \alpha_{i3}, \alpha_{i4}) \\ (\alpha_{i5}, \alpha_{i6}, \alpha_{i7}) & \alpha_{i8} \end{pmatrix} \in \boldsymbol{O}. \tag{2-10}$$

The action of $\mathrm{GL}(\boldsymbol{O})$ on $\boldsymbol{O}$ induces the action on K_n by $(gf)(\underline{a}) = f(g^{-1}\underline{a})$ for all $g \in \mathrm{GL}(\boldsymbol{O})$, $f \in K_n$, $\underline{a} \in \boldsymbol{O}^n$.

To explicitly describe the action of G_2 on K_n consider the *generic octonions*

$$Z_i = \begin{pmatrix} z_{i1} & (z_{i2}, z_{i3}, z_{i4}) \\ (z_{i5}, z_{i6}, z_{i7}) & z_{i8} \end{pmatrix} \in \boldsymbol{O}(K_n)$$

for $1 \le i \le n$. Given $g \in G_2$, denote by $g \bullet Z_i$ the octonion

$$\begin{pmatrix} gz_{i1} & (gz_{i2}, gz_{i3}, gz_{i4}) \\ (gz_{i5}, gz_{i6}, gz_{i7}) & gz_{i8} \end{pmatrix} \in \boldsymbol{O}(K_n).$$

For any commutative algebra $\mathcal{A}$, the action of G_2 on $\boldsymbol{O}$ extends for $\boldsymbol{O}(\mathcal{A})$ by $\mathcal{A}$-linearity. In particular, G_2 acts on $\boldsymbol{O}(K_n)$. It is easy to see that

$$g \bullet Z_i = g^{-1} Z_i, \tag{2-11}$$

where $g^{-1}Z_i$ stands for the action of g^{-1} on the octonion $Z_i \in \boldsymbol{O}(K_n)$.

The algebra of *G_2-invariants of several octonions* (*octonion G_2-invariants*, for short) is

$$K_n^{G_2} = \mathbb{F}[\boldsymbol{O}^n]^{G_2} = \{f \in \mathbb{F}[\boldsymbol{O}^n] \mid gf = f \text{ for all } g \in G_2\}.$$

In other words,

$$K_n^{G_2} = \{f \in \mathbb{F}[\boldsymbol{O}^n] \mid f(g\underline{a}) = f(\underline{a}) \text{ for all } g \in G_2,\ \underline{a} \in \boldsymbol{O}^n\}.$$

Similarly we can define $\mathbb{F}[\boldsymbol{O}_0^n]^{G_2}$, since $\boldsymbol{O}_0 \subset \boldsymbol{O}$ is invariant with respect to G_2-action. Namely, the coordinate ring of the affine variety $\boldsymbol{O}_0^n$ is $K_{0,n} = \mathbb{F}[\boldsymbol{O}_0^n] = \mathbb{F}[z_{ij} \mid 1 \le i \le n,\ 1 \le j \le 7]$. The *generic traceless octonions* are

$$X_i = \begin{pmatrix} z_{i1} & (z_{i2}, z_{i3}, z_{i4}) \\ (z_{i5}, z_{i6}, z_{i7}) & -z_{i1} \end{pmatrix}.$$

The analogue of formula (2-11) also holds for the generic traceless octonions, namely, $g \bullet X_i = g^{-1}X_i$ for all $g \in G_2$ and $1 \le i \le n$. The algebra of *G_2-invariants of several traceless octonions* is $K_{0,n}^{G_2}$.

2C. *Separating sets.* Consider a finite-dimensional vector space $\mathcal{V}$ and a linear group $G < \mathrm{GL}(\mathcal{V})$. In 2002, Derksen and Kemper [2] introduced the notion of separating invariants as a weaker concept than generating invariants. Given a subset S of $\mathbb{F}[\mathcal{V}]^G$ and u, v of $\mathcal{V}$, we write $S(u) \neq S(v)$ if there exists an invariant $f \in S$ with $f(u) \neq f(v)$. In this case we say that *u, v are separated by S*. If $u, v \in \mathcal{V}$

are separated by $\mathbb{F}[\mathcal{V}]^G$, then we say that they *are separated.* A subset $S \subset \mathbb{F}[\mathcal{V}]^G$ of the invariant ring is called *separating* if for any u, v from $\mathcal{V}$ that are separated we have that they are separated by S. It is well-known that there always exists a finite separating set (see [2, Theorem 2.3.15]). We say that a separating set is minimal if it is minimal w.r.t. inclusion. Obviously, any generating set is also separating. Minimal separating sets and upper bounds on degrees of elements of a separating set for different actions were constructed in [1; 3; 4; 5; 7; 11; 12; 14; 16; 21].

2D. ***Known results.*** Denote by $\mathrm{alg}_{\mathbb{F}}\{Z\}_n$ the nonassociative $\mathbb{F}$-algebra generated by the generic octonions $Z_1, \dots, Z_n$ and $1_{\boldsymbol{O}}$. Any product of the generic octonions is called a word of $\mathrm{alg}_{\mathbb{F}}\{Z\}_n$. The unit $1_{\boldsymbol{O}} \in \mathrm{alg}_{\mathbb{F}}\{Z\}_n$ is called the empty word. For every $A, B \in \mathrm{alg}_{\mathbb{F}}\{Z\}_n$ we have

$$\mathrm{tr}(gA) = \mathrm{tr}(A), \quad n(gA) = n(A), \quad g(AB) = (gA)(gB). \tag{2-12}$$

Lemma 2.1. (a) *The trace of any* (*nonassociative*) *product of* $X_1, \dots, X_n$ *and* $n(X_i)$ *belongs to* $K_{0,n}^{G_2}$.

(b) *The trace of any* (*nonassociative*) *product of* $Z_1, \dots, Z_n$ *and* $n(Z_i)$ *belongs to* $K_n^{G_2}$.

(c) *The trace of any* (*nonassociative*) *product of* $Z_1, \dots, Z_n, \overline{Z_1}, \dots, \overline{Z_n}$ *belongs to* $K_n^{G_2}$.

Proof. Let $w = w(Z_1, \dots, Z_n)$ be some (nonassociative) product of $Z_1, \dots, Z_n$. Given $g \in G_2$, equalities (2-11), (2-12) imply that

$$g\,\mathrm{tr}(w) = \mathrm{tr}(w(g \bullet Z_1, \dots, g \bullet Z_n)) = \mathrm{tr}(w(g^{-1}Z_1, \dots, g^{-1}Z_n)) = \mathrm{tr}(g^{-1}w) = \mathrm{tr}(w).$$

The case of $n(Z_i)$ is considered similarly. Part (b) is proven. The proof of part (a) is the same. Part (c) follows from part (b) and formulas

$$\mathrm{tr}(\bar{a}) = \mathrm{tr}(a), \quad n(\bar{a}) = n(a), \quad \mathrm{tr}(\bar{a}b) = \mathrm{tr}(a)\,\mathrm{tr}(b) - \mathrm{tr}(ab)$$

for all $a, b \in \boldsymbol{O}$. □

In case $\mathbb{F} = \mathbb{Q}$ for every $A_1, \dots, A_4 \in \mathrm{alg}_{\mathbb{F}}\{Z\}_n$ denote by $Q'(A_1, A_2, A_3, A_4)$ the complete skew symmetrization of $\mathrm{tr}\big(((A_1A_2)A_3)A_4\big)$ with respect to its arguments, i.e.,

$$Q'(A_1, A_2, A_3, A_4) = \frac{1}{24} \sum_{\sigma \in \mathcal{S}_4} (-1)^{\sigma}\, \mathrm{tr}\big(((A_{\sigma(1)}A_{\sigma(2)})A_{\sigma(3)})A_{\sigma(4)}\big).$$

In [23] it was shown that all coefficients of $Q'(X_1, X_2, X_3, X_4)$ belong to $\mathbb{Z}\big[\frac{1}{2}\big]$. Lemma 4.1 (see below) implies that all coefficients of $Q'(Z_1, Z_2, Z_3, Z_4)$ also belong to $\mathbb{Z}\big[\frac{1}{2}\big]$. Thus $Q'(A_1, A_2, A_3, A_4)$ is well-defined over an arbitrary field of odd characteristic.

In case $\mathrm{char}\,\mathbb{F} \neq 2$,

- the algebra of invariants $K_{0,n}^{G_2}$ is generated by $\mathrm{tr}(X_iX_j)$, $\mathrm{tr}((X_iX_j)X_k)$, $Q'(X_i, X_j, X_k, X_l)$;
- the algebra of invariants $K_n^{G_2}$ is generated by $\mathrm{tr}(Z_i)$, $\mathrm{tr}(Z_iZ_j)$, $\mathrm{tr}((Z_iZ_j)Z_k)$, $Q'(Z_i, Z_j, Z_k, Z_l)$

for all $1 \le i, j, k, l \le n$ (see [23, Corollary 9 and Section 1]).

2E. ***New results.*** Denote by $S_{0,n}$ the set

$$\{n(X_i) \mid 1 \le i \le n\} \cup \bigl\{\mathrm{tr}\bigl(\bigl(\cdots((X_{i_1}X_{i_2})X_{i_3})\cdots\bigr)X_{i_k}\bigr) \mid 1 \le i_1 < \cdots < i_k \le n,\ k > 1\bigr\}$$

and by S_n the set

$$\{n(Z_i) \mid 1 \le i \le n\} \cup \bigl\{\mathrm{tr}\bigl(\bigl(\cdots((Z_{i_1}Z_{i_2})Z_{i_3})\cdots\bigr)Z_{i_k}\bigr) \mid 1 \le i_1 < \cdots < i_k \le n,\ k > 0\bigr\}.$$

Given $1 \le k \le n$, denote by $S_{0,n}^{(k)}$ and $S_n^{(k)}$ the subset of $S_{0,n}$ and S_n (respectively) of elements of degree less or equal to k.

In case $\mathrm{char}\,\mathbb{F} = 2$ generators for the algebras $K_{0,n}^{G_2}$ and $K_n^{G_2}$ are not known. We introduce the algebra of *trace G_2-invariants of octonions $T_n \subset K_n^{G_2}$*, i.e., the algebra T_n is generated by $n(Z_1), \dots, n(Z_n)$ and the traces of all (nonassociative) products of $Z_1, \dots, Z_n$ (see Lemma 2.1). In case $\mathrm{char}\,\mathbb{F} \neq 2$ we obviously have that $T_n = K_n^{G_2}$. We obtain the following results:

- $S_n^{(4)}$ is a minimal (w.r.t. inclusion) generating set for $K_n^{G_2}$ in case $\mathrm{char}\,\mathbb{F} \neq 2$ (see Proposition 4.3).
- $S_n^{(4)}$ is a minimal (w.r.t. inclusion) separating set for $K_n^{G_2}$ in case $\mathrm{char}\,\mathbb{F} \neq 2$ (see Proposition 4.5).
- T_n is minimally generated by S_n in case $\mathrm{char}\,\mathbb{F} = 2$ (see Theorem 5.2).
- $S_n^{(8)}$ is a separating set for $K_n^{G_2}$ in case $\mathrm{char}\,\mathbb{F} = 2$ (see Theorem 7.11).

3. Auxiliaries

3A. ***Indecomposable invariants.*** Denote by $\mathbb{F}\{\mathbb{X}\}_n$ the free nonassociative and noncommutative unital $\mathbb{F}$-algebra with free generators $x_1, \dots, x_n$, which are called letters. A word w is a nonempty product of letters. The number of letters in w is the degree $\deg(w)$ of w. The degree of w in x_i is denoted by $\deg_{x_i}(w)$ and the total degree of w is denoted by $\deg(w)$. The multidegree of a word w is $\mathrm{mdeg}(w) = (\deg_{x_1}(w), \dots, \deg_{x_n}(w))$. A word w with $\deg_{x_i}(w) \le 1$ for all i is called multilinear. An element $f = \sum_i \alpha_i w_i$ of $\mathbb{F}\{\mathbb{X}\}_n$, where $\alpha_i \in \mathbb{F}$ and w_i is a word, is $\mathbb{N}$-homogeneous ($\mathbb{N}^n$-homogeneous, respectively) if there exists d ($\Delta \in \mathbb{N}^n$, respectively) such that $\deg(w_i) = d$ ($\mathrm{mdeg}(w_i) = \Delta$, respectively) for all i, where $\mathbb{N}$ stands for nonnegative integers. Define homomorphisms of $\mathbb{F}$-algebras $\phi_0 : \mathbb{F}\{\mathbb{X}\}_n \to \mathrm{alg}_{\mathbb{F}}\{X\}_n$ and $\phi : \mathbb{F}\{\mathbb{X}\}_n \to \mathrm{alg}_{\mathbb{F}}\{Z\}_n$ by $x_i \to X_i$ and $x_i \to Z_i$ (respectively) for all i. In other words, for $f = f(x_1, \dots, x_n) \in \mathbb{F}\{\mathbb{X}\}_n$ we have $\phi(f) = f(Z_1, \dots, Z_n) \in \mathrm{alg}_{\mathbb{F}}\{Z\}_n$. We write $x_{i_1} \circ \cdots \circ x_{i_k}$ for some nonassociative product of $x_{i_1}, \dots, x_{i_k}$. Similar notation we use for nonassociative products in $\mathrm{alg}_{\mathbb{F}}\{Z\}_n$.

For $f \in K_n$ denote by $\deg(f)$ its degree and by $\mathrm{mdeg}(f)$ its multidegree, i.e., $\mathrm{mdeg}(f) = (t_1, \dots, t_n)$, where t_i is the total degree of the polynomial f in z_{ij}, $1 \le j \le 8$, and $\deg(f) = t_1 + \cdots + t_n$. For $f \in K_{0,n}$ the degree and multidegree are defined as above. It is well-known that the algebras $K_{0,n}^{G_2}$ and $K_n^{G_2}$ have $\mathbb{N}$-gradings by degrees and $\mathbb{N}^n$-gradings by multidegrees.

Consider an $\mathbb{N}^n$-graded unital (possibly, nonassociative) algebra $\mathcal{A}$ with the component of degree zero equal to $\mathbb{F}$. Denote by $\mathcal{A}^+$ the subalgebra generated by homogeneous elements of positive degree. A set $\{a_i\} \subseteq \mathcal{A}$ is a minimal (by inclusion) $\mathbb{N}^n$-homogeneous generating set (m.h.g.s.) of $\mathcal{A}$ as a unital algebra if and only if the a_i's are $\mathbb{N}^n$-homogeneous and $\{\overline{a_i}\} \cup \{1\}$ is a basis of the vector space $\overline{\mathcal{A}} = \mathcal{A}/(\mathcal{A}^+)^2$.

We say that an element $a \in \mathcal{A}$ is *decomposable* and we write $a \equiv 0$ if $a \in (\mathcal{A}^+)^2$. In other words, a decomposable element is equal to a polynomial in elements of strictly less degree. Therefore, the largest degree of indecomposable elements of $\mathcal{A}$ is equal to the least upper bound for the degrees of elements of a m.h.g.s. for $\mathcal{A}$.

3B. ***One-parameter subgroups of G_2.*** Consider a finite-dimensional vector space $\mathcal{V}$ and a linear (closed) group $G < \mathrm{GL}(\mathcal{V})$. For a point $v \in \mathcal{V}$ and for a one-parameter subgroup $\theta : \mathbb{F}^\times \to G$ we have $\theta(t)v = \sum_{i \in I(v)} t^i v^{(i)}$ for all $t \in \mathbb{F}^\times$, where $I(v) = \{i \in \mathbb{Z} \mid v^{(i)} \neq 0\}$. Following [13] we say that $\lim_{t\to 0}\theta(t)v$ exists if and only if $I(v)$ consists of nonnegative integers. Then $\lim_{t\to 0}\theta(t)v = 0$ if and only if $I(v)$ consists of positive integers only, otherwise $\lim_{t\to 0}\theta(t)v = v^{(0)}$. It is clear that if $\lim_{t\to 0}\theta(t)v$ exists, then it is contained in $\overline{Gv}$. Indeed, if f is a polynomial function on $\mathcal{V}$, that vanishes on the G-orbit of v, then $h(t) = f(\theta(t)v)$ is a polynomial in t, such that $h(t) = 0$ for any $t \neq 0$. Since $\mathbb{F}$ is infinite, $h(t)$ is identically zero, that is, $h(0) = f(v^{(0)}) = 0$.

Given $\underline{\lambda} \in \mathbb{Z}^3$ with $\lambda_1 + \lambda_2 + \lambda_3 = 0$, the *standard* one-parameter subgroup $\theta_{\underline{\lambda}}$ of G_2 is defined by

$$\theta_{\underline{\lambda}}(t)e_i = e_i, \quad \theta_{\underline{\lambda}}(t)\boldsymbol{u}_j = t^{\lambda_j}\boldsymbol{u}_j, \quad \theta_{\underline{\lambda}}(t)\boldsymbol{v}_j = t^{-\lambda_j}\boldsymbol{v}_j,$$

for all $i = 1, 2$ and $1 \leq j \leq 3$.

4. Minimal generating and separating sets

In this section we write $\mathrm{tr}(i_1, \ldots, i_k)$ for $\mathrm{tr}((\cdots((Z_{i_1}Z_{i_2})Z_{i_3})\cdots)Z_{i_k})$, where $1 \leq i_1, \ldots, i_k \leq n$. The following lemma can be proven by straightforward calculations.

Lemma 4.1. *Assume that* $\mathrm{char}\,\mathbb{F} \neq 2$. *Then*

$$\begin{aligned} Q'(Z_1, Z_2, Z_3, Z_4) &\\ = \mathrm{tr}(1234) + \tfrac{1}{2}\big(&-\mathrm{tr}(1)\,\mathrm{tr}(2)\,\mathrm{tr}(3)\,\mathrm{tr}(4) - \mathrm{tr}(1)\,\mathrm{tr}(234) - \mathrm{tr}(2)\,\mathrm{tr}(134) - \mathrm{tr}(3)\,\mathrm{tr}(124) \\ &- \mathrm{tr}(4)\,\mathrm{tr}(123) - \mathrm{tr}(12)\,\mathrm{tr}(34) + \mathrm{tr}(13)\,\mathrm{tr}(24) - \mathrm{tr}(14)\,\mathrm{tr}(23)\,\mathrm{tr}(1)\,\mathrm{tr}(2)\,\mathrm{tr}(34) \\ &+ \mathrm{tr}(1)\,\mathrm{tr}(4)\,\mathrm{tr}(23) + \mathrm{tr}(2)\,\mathrm{tr}(3)\,\mathrm{tr}(14) + \mathrm{tr}(3)\,\mathrm{tr}(4)\,\mathrm{tr}(12)\big). \end{aligned}$$

Recall that the definition of T_n was given in Section 2E.

Lemma 4.2. *Let* $w \in \mathbb{F}\{\mathbb{X}\}_n$ *be a word.*

1. *If w is not multilinear and* $\deg(w) > 2$, *then* $\mathrm{tr}(w(Z_1, \ldots, Z_n)) \equiv 0$ *in* T_n.
2. *If w is multilinear and w is a product of letters $x_{i_1}, \ldots, x_{i_k}$ for* $1 \leq i_1 < \cdots < i_k \leq n$, *then*
$$\mathrm{tr}(w(Z_1, \ldots, Z_n)) \equiv \pm\mathrm{tr}(i_1, \ldots, i_k) \quad \textit{in } T_n.$$
3. *For all* $1 \leq i_1 < \cdots < i_k \leq n$ *with* $k \geq 3$ *and every permutation* $\sigma \in \mathcal{S}_k$ *we have*
$$\mathrm{tr}(i_{\sigma(1)}, \ldots, i_{\sigma(k)}) \equiv (-1)^\sigma\,\mathrm{tr}(i_1, \ldots, i_k) \quad \textit{in } T_n.$$

Proof. Combining (2-4) and (2-6) we obtain that

$$a(a'b)+a'(ab)=(\operatorname{tr}(a)a'+\operatorname{tr}(a')a+\operatorname{tr}(aa')-\operatorname{tr}(a)\operatorname{tr}(a'))b$$

for all $a, a', b \in \boldsymbol{O}$. Since $\mathbb{F}$ is infinite, the same equality holds for the generic octonions. We multiply it from the left and from the right by the generic octonions and then apply the trace. Since the trace is a linear function, we obtain that

$$\operatorname{tr}\big(C_1\circ\cdots\circ C_r\circ(A(A'B))\circ C_{r+1}\circ\cdots\circ C_s\big)\equiv-\operatorname{tr}\big(C_1\circ\cdots\circ C_r\circ(A'(AB))\circ C_{r+1}\circ\cdots\circ C_s\big) \quad (4\text{-}1)$$

for all products of the generic octonions A, A', B, $C_1, \dots, C_s$ with $0 \le r \le s$ and $s \ge 0$. Similarly, we obtain that

$$\operatorname{tr}\big(C_1\circ\cdots\circ C_r\circ((BA)A')\circ C_{r+1}\circ\cdots\circ C_s\big)\equiv-\operatorname{tr}\big(C_1\circ\cdots\circ C_r\circ((BA')A)\circ C_{r+1}\circ\cdots\circ C_s\big). \quad (4\text{-}2)$$

In the same manner as above, (2-2) and (2-4) imply that

$$\operatorname{tr}(C_1\circ\cdots\circ C_r\circ(A^2)\circ C_{r+1}\circ\cdots\circ C_s)\equiv 0, \quad (4\text{-}3)$$

$$\operatorname{tr}(C_1\circ\cdots\circ C_r\circ(AA')\circ C_{r+1}\circ\cdots\circ C_s)\equiv-\operatorname{tr}(C_1\circ\cdots\circ C_r\circ(A'A)\circ C_{r+1}\circ\cdots\circ C_s), \quad (4\text{-}4)$$

where in both cases $0 \le r \le s$ and $s > 0$. We claim that

If $W = Z_{i_1}\circ\cdots\circ Z_{i_k}$ is a product of generic octonions where $1 \le i_1, \dots, i_k \le n$,
then $\operatorname{tr}(W) \equiv \pm\operatorname{tr}(i_{\sigma(1)}, \dots, i_{\sigma(k)})$ for some $\sigma \in \mathcal{S}_k$. (4-5)

Assume that claim (4-5) does not hold. Then there exists $\tau \in \mathcal{S}_k$ and the maximal $2 \le r < k$ such that some product $W' = Z_{i_{\tau(1)}}\circ\cdots\circ Z_{i_{\tau(k)}}$ satisfies $\operatorname{tr}(W) \equiv \pm\operatorname{tr}(W')$ and

$$W' = C_1\circ\cdots\circ(U(V_1V_2))\circ\cdots\circ C_s \quad \text{or} \quad W' = C_1\circ\cdots\circ(VU)\circ\cdots\circ C_s,$$

where

- $U = \big(\cdots((Z_{j_1}Z_{j_2})Z_{j_3})\cdots\big)Z_{j_r}$ for some $1 \le j_1, \dots, j_r \le n$,
- V, V_1, V_2 are some products of generic octonions,
- $C_1, \dots, C_s$ are generic octonions with $s \ge 0$.

By (2-1) and (4-4), we can assume that $W' = C_1\circ\cdots\circ(U(V_1V_2))\circ\cdots\circ C_s$. Consequently, applying equivalence (4-1) and equivalence (2-1) or (4-4), we obtain that

$$\operatorname{tr}\big(C_1\circ\cdots\circ(U(V_1V_2))\circ\cdots\circ C_s\big)\equiv-\operatorname{tr}\big(C_1\circ\cdots\circ(V_1(UV_2))\circ\cdots\circ C_s\big)\equiv\pm\operatorname{tr}\big(C_1\circ\cdots\circ((UV_2)V_1)\circ\cdots\circ C_s\big).$$

If V_2 is a product of more than one generic octonions, then $V_2 = V_2'V_2''$ for some products V_2', V_2'' of generic octonions and we repeat the reasoning for $C_1\circ\cdots\circ(U(V_2'V_2''))\circ\cdots\circ C_s$, and so on. Finally, we can assume that $V_2 = Z_j$ for some j; a contradiction to the maximality of r.

Equivalences (4-2) and (4-4) imply that part 3 is valid for $1 \le i_1, \dots, i_k \le n$, where $k \ge 3$. This fact together with claim (4-5) imply part 2. Similarly, this fact together with claim (4-5) and formula (4-3) imply part 1. □

Proposition 4.3. *In case* char $\mathbb{F} \neq 2$ *the algebra of invariants* $K_n^{G_2}$ *is minimally generated by* $S_n^{(4)}$.

Proof. The description of generators for $K_n^{G_2}$ from [23] (see Section 2D for the details) together with Lemmas 4.1, 4.2 and formula (2-8) imply that the set $S_n^{(4)}$ generates the algebra $K_n^{G_2}$. By Corollary 1 of [23] and formula (2-8), the invariants

$$\mathrm{tr}(i), \quad n(Z_i), \quad \mathrm{tr}(12), \quad \mathrm{tr}(13), \quad \mathrm{tr}(23), \quad \mathrm{tr}(123),$$

where $1 \le i \le 3$, are algebraically independent over $\mathbb{F}$. Thus the required statement is proven for $n \le 3$.

Assume $n \ge 4$. Thus $S_n^{(4)} \backslash \{f\}$ is not a generating set for any $f \in S_n^{(4)}$ with $\deg(f) \neq 4$.

Assume that $S_n^{(4)} \backslash \{\mathrm{tr}(1234)\}$ is a generating set. Then tr(1234) is a linear combination of tr(12) tr(34), tr(13) tr(24), tr(14) tr(23) and products containing $\mathrm{tr}(i)$ for some $1 \le i \le 4$. Considering substitutions

$$Z_1 \to \boldsymbol{v}_1, \quad Z_2 \to \boldsymbol{v}_2, \quad Z_3 \to \boldsymbol{v}_3, \quad Z_4 \to e_1 - e_2$$

and using equalities $\mathrm{tr}(((\boldsymbol{v}_1\boldsymbol{v}_2)\boldsymbol{v}_3)(e_1 - e_2)) = -1$ and $\mathrm{tr}(\boldsymbol{v}_i(e_1 - e_2)) = 0$ for $1 \le i \le 3$, we obtain a contradiction. The proposition is proven. □

Remark 4.4. 1. By (2-8), in the formulation of Proposition 4.3 we can replace $n(Z_i)$ by $\mathrm{tr}(Z_i^2)$ for all $1 \le i \le n$.

2. It easily follows from the proof of Proposition 4.3 (see also Section 1 of [23]) that $K_{0,n}^{G_2}$ is minimally generated by $S_{0,n}^{(4)}$ when char $\mathbb{F} \neq 2$.

Proposition 4.5. *Assume* char $\mathbb{F} \neq 2$. *Then* $S_{0,n}^{(4)}$ *and* $S_n^{(4)}$ *are minimal separating sets for* $K_{0,n}^{G_2}$ *and* $K_n^{G_2}$ (*respectively*) *for all* $n > 0$.

Proof. By Proposition 4.3 and Remark 4.4, the sets $S_{0,n}^{(4)}$ and $S_n^{(4)}$ are separating for $K_{0,n}^{G_2}$ and $K_n^{G_2}$ (respectively). For $a = 0$, $b = \boldsymbol{u}_1 + \boldsymbol{v}_1$ we have $\mathrm{tr}(a) = n(a) = \mathrm{tr}(b) = 0$, but $n(b) = -1$. For $a = 0$, $b = e_1$ we have $\mathrm{tr}(a) = n(a) = n(b) = 0$, but $\mathrm{tr}(b) = 1$. Hence, S_1 is a minimal separating set for $K_1^{G_2}$. Claims 1, 2, 3 (see below) imply that $S_{0,n}^{(4)}$ is a *minimal* separating set for $K_{0,n}^{G_2}$. Therefore, $S_n^{(4)}$ is also a minimal separating set for $K_n^{G_2}$.

Claim 1. Let $n = 2$. Then $S_{0,2} \backslash \{\mathrm{tr}(X_1X_2)\}$ is not separating $K_{0,2}^{G_2}$.

To prove this claim consider $\underline{a} = (0, 0)$ and $\underline{b} = (\boldsymbol{u}_1, \boldsymbol{v}_1)$ from $\boldsymbol{O}_0^2$. Then $\mathrm{tr}(a_1a_2) \neq \mathrm{tr}(b_1b_2)$.

Claim 2. Let $n = 3$. Then $S_{0,3} \backslash \{\mathrm{tr}((X_1X_2)X_3)\}$ is not separating for $K_{0,3}^{G_2}$.

To prove this claim we consider $\underline{a} = (0, 0, 0)$ and $\underline{b} = (\boldsymbol{v}_1, \boldsymbol{v}_2, \boldsymbol{v}_3)$ from $\boldsymbol{O}_0^3$. Then $\mathrm{tr}(a_ia_j) = \mathrm{tr}(b_ib_j) = 0$ for all $1 \le i < j \le 3$, but $\mathrm{tr}(a_1a_2a_3) \neq \mathrm{tr}(b_1b_2b_3)$.

Claim 3. Let $n = 4$. Then $S_{0,4} \backslash \big\{\mathrm{tr}\big(((X_1X_2)X_3)X_4\big)\big\}$ is not separating for $K_{0,4}^{G_2}$.

To prove this claim we consider $\underline{a} = (\boldsymbol{u}_1, \boldsymbol{v}_1, c, \boldsymbol{u}_2)$ and $\underline{b} = (\boldsymbol{u}_1, \boldsymbol{v}_1, c, -\boldsymbol{v}_2)$ from $\boldsymbol{O}_0^4$, where $c = e_1 + \boldsymbol{u}_2 - \boldsymbol{v}_2 - e_2$. Then $\mathrm{tr}(a_ia_4) = \mathrm{tr}(b_ib_4)$ for $1 \le i \le 3$ and $\mathrm{tr}((a_ia_j)a_4) = \mathrm{tr}((b_ib_j)b_4)$ for $1 \le i < j \le 3$, but $\mathrm{tr}\big(((a_1a_2)a_3)a_4\big) = 0$ and $\mathrm{tr}\big(((b_1b_2)b_3)b_4\big) = -1$. □

5. Trace invariants

The group $\mathrm{GL}_2 = \mathrm{GL}_2(\mathbb{F})$ acts on $M_2^n = M_2(\mathbb{F})^{\oplus n}$ diagonally by conjugation. The coordinate ring $\mathbb{F}[M_2^n] = \mathbb{F}[z_{i1}, z_{i2}, z_{i5}, z_{i8} \mid 1 \le i \le n]$ is also a GL_2-module, where the *generic matrices* are

$$\widehat{Z}_i = \begin{pmatrix} z_{i1} & z_{i2} \\ z_{i5} & z_{i8} \end{pmatrix}.$$

We consider $\mathbb{F}[M_2^n]$ as a subalgebra of K_n. In [6] it was shown that

$$\{\det(\widehat{Z}_i) \mid 1 \le i \le n\} \cup \{\mathrm{tr}(\widehat{Z}_{i_1} \cdots \widehat{Z}_{i_k}) \mid 1 \le i_1 < \cdots < i_k \le n,\ k > 0\}, \tag{5-1}$$

is a minimal generating set for $\mathbb{F}[M_2^n]^{\mathrm{GL}_2}$, where $k \le 3$ in case $\mathrm{char}\,\mathbb{F} \ne 2$. In particular, all elements from set (5-1) are indecomposable. A minimal separating set for $\mathbb{F}[M_2^n]^{\mathrm{GL}_2}$ was obtained in [11].

Define a surjective homomorphism of $\mathbb{F}$-algebras $\Psi : K_n \to \mathbb{F}[M_2^n]$ as follows: $z_{i3} \to 0$, $z_{i4} \to 0$, $z_{i6} \to 0$, $z_{i7} \to 0$ for all i. We can naturally extend Ψ to the linear map $\widehat{\Psi} : \boldsymbol{O}(K_n) \to \boldsymbol{O}(\mathbb{F}[M_2^n])$ by

$$\widehat{\Psi}\begin{pmatrix} f_1 & (f_2, f_3, f_4) \\ (f_5, f_6, f_7) & f_8 \end{pmatrix} = \begin{pmatrix} \Psi(f_1) & (\Psi(f_2), \Psi(f_3), \Psi(f_4)) \\ (\Psi(f_5), \Psi(f_6), \Psi(f_7)) & \Psi(f_8) \end{pmatrix}$$

for $f_1, \ldots, f_8 \in K_n$.

For an associative commutative $\mathbb{F}$-algebra $\mathcal{A}$ define a map $\mathcal{F} : M_2(\mathcal{A}) \to \boldsymbol{O}(\mathcal{A})$ by

$$\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \to \begin{pmatrix} a_1 & (a_2, 0, 0) \\ (a_3, 0, 0) & a_4 \end{pmatrix}$$

for $a_1, \ldots, a_4 \in \mathcal{A}$. It is easy to see that $\mathcal{F}$ is an injective homomorphism of algebras preserving the trace, since $(a, 0, 0) \times (b, 0, 0) = 0$ for all $a, b \in \mathcal{A}$. In what follows, we consider $\mathcal{A} = K_n$. Since the homomorphism $\widehat{\Psi}$ commutes with the trace and the norm, we obtain the following lemma.

Lemma 5.1. *For all* $1 \le i, i_1, \ldots, i_k \le n$ *we have*

(a) $\widehat{\Psi}\big(\cdots((Z_{i_1}Z_{i_2})Z_{i_3})\cdots\big)Z_{i_k}) = \mathcal{F}(\widehat{Z}_{i_1} \cdots \widehat{Z}_{i_k})$;

(b) $\Psi\big(\mathrm{tr}\big(\big(\cdots((Z_{i_1}Z_{i_2})Z_{i_3})\cdots\big)Z_{i_k}\big)\big) = \mathrm{tr}(\widehat{Z}_{i_1} \cdots \widehat{Z}_{i_k})$;

(c) $\Psi(n(Z_i)) = \det(\widehat{Z}_i)$.

Lemmas 2.1, 5.1 and the description of generators of $\mathbb{F}[M_2^n]^{\mathrm{GL}_2}$ imply that

$$\mathbb{F}[M_2^n]^{\mathrm{GL}_2} \subset \Psi(K_n^{G_2}), \tag{5-2}$$

where we have equality in case $\mathrm{char}\,\mathbb{F} \ne 2$.

Theorem 5.2. *In case* $\mathrm{char}\,\mathbb{F} = 2$ *the algebra of trace* G_2*-invariants* T_n *is minimally generated by* S_n.

Proof. By Lemma 4.2 and formula (2-8), the algebra T_n is generated by S_n. To show that S_n is a minimal generating set, it is enough to prove that every element $f \in S_n$ is indecomposable in T_n. Assume the contrary. If $f = \mathrm{tr}\big(\big(\cdots((Z_{i_1}Z_{i_2})Z_{i_3})\cdots\big)Z_{i_k}\big)$ from S_n were decomposable in T_n, then by parts (b), (c) of Lemma 5.1, $\Psi(f) = \mathrm{tr}(\widehat{Z}_{i_1} \cdots \widehat{Z}_{i_k})$ would be decomposable in $\mathbb{F}[M_2^n]^{\mathrm{GL}_2}$; a contradiction. Similarly, if $f = n(Z_i)$ were decomposable in T_n, then $\Psi(f) = \det(\widehat{Z}_i)$ would be decomposable in $\mathbb{F}[M_2^n]^{\mathrm{GL}_2}$; a contradiction. □

6. Subalgebras of $\boldsymbol{O}$ of low dimension

The group G_2 acts naturally on the set of subalgebras of $\boldsymbol{O}$. For a subalgebra $\mathcal{A}$ of $\boldsymbol{O}$ we denote by $[\mathcal{A}]$ the G_2-orbit of $\mathcal{A}$ and we say that $[\mathcal{A}]$ is the equivalence class of $\mathcal{A}$. Obviously, all algebras in $[\mathcal{A}]$ are isomorphic to $\mathcal{A}$. Denote by $\Omega(\boldsymbol{O})$ the set of G_2-orbits (i.e., equivalence classes) in the set of subalgebras of $\boldsymbol{O}$. Since all algebras from a given equivalence class $\mathfrak{A} \in \Omega(\boldsymbol{O})$ have the same dimension, we call it the *dimension* of $\mathfrak{A}$. A set of (linearly independent) octonions is said to be a *basis* of $\mathfrak{A}$, provided they form a basis of an algebra from $\mathfrak{A}$. An equivalence class $\mathfrak{A} \in \Omega(\boldsymbol{O})$ is called *closed* if there exists a subalgebra $\mathcal{A}$ of $\boldsymbol{O}$ with $[\mathcal{A}] = \mathfrak{A}$ and there is an $\mathbb{F}$-basis $a_1, \dots, a_n$ of $\mathcal{A}$ such that the G_2-orbit of $(a_1, \dots, a_n)$ is closed in $\boldsymbol{O}^n$. More details on the definition of a closed equivalence class can be found in Remark 7.3 (see below). Denote by

$$\mathbb{M} = \begin{pmatrix} * & (*,0,0) \\ (*,0,0) & * \end{pmatrix} \quad \text{and} \quad \mathbb{S} = \begin{pmatrix} * & (*,*,0) \\ (*,0,*) & * \end{pmatrix},$$

the subalgebra of *quaternions* and *sextonions* of $\boldsymbol{O}$, respectively, where the term *sextonions* was introduced in [15]. Note that $\mathcal{F} : M_2(\mathbb{F}) \to \mathbb{M}$ is an isomorphism of $\mathbb{F}$-algebras (see Section 5 for the details).

The main result of this section is the following statement.

Proposition 6.1. *Assume* $\mathrm{char}\,\mathbb{F} = 2$ *and an equivalence class* $\mathfrak{A} \in \Omega(\boldsymbol{O})$ *has dimension* $d \le 3$. *Then one of the following sets is a basis for* $\mathfrak{A}$:

$d = 1$: $\{1_{\boldsymbol{O}}\}$, $\{\boldsymbol{u}_1\}$, $\{e_1\}$;

$d = 2$: $\{1_{\boldsymbol{O}}, \boldsymbol{u}_1\}$, $\{\boldsymbol{u}_1, \boldsymbol{v}_2\}$, $\{e_1, \boldsymbol{u}_1\}$, $\{e_1, \boldsymbol{v}_1\}$, $\{e_1, e_2\}$;

$d = 3$: $\{1_{\boldsymbol{O}}, \boldsymbol{u}_1, \boldsymbol{v}_2\}$, $\{e_1, e_2, \boldsymbol{u}_1\}$, $\{e_1, \boldsymbol{u}_1, \boldsymbol{v}_2\}$, $\{\boldsymbol{u}_1, \boldsymbol{v}_2, \boldsymbol{v}_3\}$.

We do not require for a subalgebra of $\boldsymbol{O}$ to be unital. The proof of Proposition 6.1 will be given in a series of propositions and lemmas, which are interesting on their own.

Proposition 6.2 [17, Proposition 3.3]. *For each* $a \in \boldsymbol{O}$ *there exists* $g \in G_2$ *such that* ga *is a canonical octonion of one of the following types*:

(D) $\left(\begin{smallmatrix} \alpha_1 & \mathbf{0} \\ \mathbf{0} & \alpha_8 \end{smallmatrix}\right)$,

(K$_1$) $\left(\begin{smallmatrix} \alpha_1 & (1,0,0) \\ \mathbf{0} & \alpha_1 \end{smallmatrix}\right)$,

for some $\alpha_1, \alpha_8 \in \mathbb{F}$. *These canonical octonions are unique modulo permutation* $\alpha_1 \leftrightarrow \alpha_8$ *for type* (D).

Proposition 6.3 [17, Theorem 4.4]. *Assume* $\mathrm{char}\,\mathbb{F} = 2$. *For each* $(a, b) \in \boldsymbol{O}_0^2$ *there exists* $g \in G_2$ *such that* $g(a, b)$ *is a pair of one of the following types*:

(EE) $(\alpha_1 1_{\boldsymbol{O}}, \beta_1 1_{\boldsymbol{O}})$,

(EK$_1$) $\left(\alpha_1 1_{\boldsymbol{O}}, \left(\begin{smallmatrix} \beta_1 & (1,0,0) \\ \mathbf{0} & \beta_1 \end{smallmatrix}\right)\right)$, (K$_1$E) $\left(\left(\begin{smallmatrix}\alpha_1 & (1,0,0)\\ \mathbf{0} & \alpha_1\end{smallmatrix}\right), \beta_1 1_{\boldsymbol{O}}\right)$,

(K$_1$L$_1$) $\left(\left(\begin{smallmatrix}\alpha_1 & (1,0,0)\\ \mathbf{0} & \alpha_1\end{smallmatrix}\right), \left(\begin{smallmatrix}\beta_1 & (\beta_2,0,0)\\ \mathbf{0} & \beta_1\end{smallmatrix}\right)\right)$ *with* $\beta_2 \neq 0$,

(K$_1$L$_1^\top$) $\left(\left(\begin{smallmatrix}\alpha_1 & (1,0,0)\\ \mathbf{0} & \alpha_1\end{smallmatrix}\right), \left(\begin{smallmatrix}\beta_1 & \mathbf{0}\\ (\beta_5,0,0) & \beta_1\end{smallmatrix}\right)\right)$ *with* $\beta_5 \neq 0$,

(K$_1$M$_1$) $\left(\left(\begin{smallmatrix}\alpha_1 & (1,0,0)\\ \mathbf{0} & \alpha_1\end{smallmatrix}\right), \left(\begin{smallmatrix}\beta_1 & (0,1,0)\\ \mathbf{0} & \beta_1\end{smallmatrix}\right)\right)$,

(K$_1$M$_1^\top$) $\left(\left(\begin{smallmatrix}\alpha_1 & (1,0,0)\\ \mathbf{0} & \alpha_1\end{smallmatrix}\right), \left(\begin{smallmatrix}\beta_1 & \mathbf{0}\\ (0,1,0) & \beta_1\end{smallmatrix}\right)\right)$,

where $\alpha_1, \beta_1, \beta_2, \beta_5 \in \mathbb{F}$.

Remark 6.4 [17, Lemma 3.2]. Assume $a = \left(\begin{smallmatrix}\alpha & \boldsymbol{u}\\ \boldsymbol{v} & \beta\end{smallmatrix}\right) \in \boldsymbol{O}$. Then:

(a) If $\boldsymbol{u} \neq 0$, then there exists $g \in \mathrm{SL}_3$ such that $ga = \left(\begin{smallmatrix}\alpha & (1,0,0)\\ \boldsymbol{v}' & \beta\end{smallmatrix}\right)$, where $\boldsymbol{v}' = (*, 0, 0)$ or $\boldsymbol{v}' = (0, 1, 0)$.

(b) If $\boldsymbol{v} \neq 0$, then there exists $g \in \mathrm{SL}_3$ such that $ga = \left(\begin{smallmatrix}\alpha & \boldsymbol{u}'\\ (1,0,0) & \beta\end{smallmatrix}\right)$, where $\boldsymbol{u}' = (*, 0, 0)$ or $\boldsymbol{u}' = (0, 1, 0)$.

(c) There exist $g, g', g'' \in \mathrm{SL}_3$ such that

$$g(\boldsymbol{u}_1, \boldsymbol{v}_1, \boldsymbol{u}_2, \boldsymbol{v}_3) = (\boldsymbol{u}_1, \boldsymbol{v}_1, \boldsymbol{u}_3, -\boldsymbol{v}_2),$$
$$g'(\boldsymbol{u}_2, \boldsymbol{v}_2, \boldsymbol{u}_1, \boldsymbol{v}_3) = (\boldsymbol{u}_2, \boldsymbol{v}_2, \boldsymbol{u}_3, -\boldsymbol{v}_1),$$
$$g''(\boldsymbol{u}_3, \boldsymbol{v}_3, \boldsymbol{u}_1, \boldsymbol{v}_2) = (\boldsymbol{u}_3, \boldsymbol{v}_3, \boldsymbol{u}_2, -\boldsymbol{v}_1).$$

(d) If $\boldsymbol{u} = (\gamma_1, \gamma_2, \gamma_3)$ with $\gamma_2 \neq 0$ or $\gamma_3 \neq 0$ and $\boldsymbol{v} = (\delta, 0, 0)$, then there exists $g \in \mathrm{SL}_3$ such that $ga = \left(\begin{smallmatrix}\alpha & (\gamma_1,1,0)\\ (\delta,0,0) & \beta\end{smallmatrix}\right)$ and $g(\boldsymbol{u}_1, \boldsymbol{v}_1) = (\boldsymbol{u}_1, \boldsymbol{v}_1)$.

(e) If $\boldsymbol{v} = (\gamma_1, \gamma_2, \gamma_3)$ with $\gamma_2 \neq 0$ or $\gamma_3 \neq 0$ and $\boldsymbol{u} = (\delta, 0, 0)$, then there exists $g \in \mathrm{SL}_3$ such that $ga = \left(\begin{smallmatrix}\alpha & (\delta,0,0)\\ (\gamma_1,1,0) & \beta\end{smallmatrix}\right)$ and $g(\boldsymbol{u}_1, \boldsymbol{v}_1) = (\boldsymbol{u}_1, \boldsymbol{v}_1)$.

The following lemma is an immediate consequence of the Cayley–Dickson doubling process (see also Section 2.1 of [22]). Its analogue over a finite field is part (ii) of Lemma 3.3 from [9].

Lemma 6.5. *Every automorphism of the* $\mathbb{F}$*-algebra* $\mathbb{M}$ *can be extended to an automorphism of the algebra* $\boldsymbol{O}$.

Lemma 6.6. *If* $\mathcal{A} \subset \boldsymbol{O}$ *is a nonzero subalgebra, then there exists* $g \in G_2$ *such that* $1_{\boldsymbol{O}} \in g\mathcal{A}$ *or* $\boldsymbol{u}_1 \in g\mathcal{A}$ *or* $e_1 \in g\mathcal{A}$. *In particular, if* $\operatorname{char}\mathbb{F} = 2$ *and* $\mathcal{A} \not\subset \boldsymbol{O}_0$ *is a nonzero subalgebra of* $\boldsymbol{O}$, *then there exists* $g \in G_2$ *such that* $e_1 \in g\mathcal{A}$.

Proof. This follows from Proposition 6.2, the known corresponding statement for the algebra $\mathbb{M} \simeq M_2(\mathbb{F})$ and Lemma 6.5. □

6A. *The case of traceless subalgebra.* In this section we assume that $\operatorname{char}\mathbb{F} = 2$ and $\mathcal{A} \subset \boldsymbol{O}$ is a subalgebra of traceless octonions, that is, $\mathcal{A} \subset \boldsymbol{O}_0$.

Remark 6.7. If $a = \left(\begin{smallmatrix}\alpha & \boldsymbol{u}\\ \boldsymbol{v} & \beta\end{smallmatrix}\right) \in \mathcal{A}$ is *triangular* (i.e., $\boldsymbol{u} = \mathbf{0}$ or $\boldsymbol{v} = \mathbf{0}$), and $\alpha \neq 0$ or $\beta \neq 0$, then $1_{\boldsymbol{O}} \in \mathcal{A}$.

Proof. Since $\alpha = \beta$ is nonzero, considering $a^2 = \alpha^2 1_{\boldsymbol{O}}$ completes the proof. □

Lemma 6.8. *If* $\dim \mathcal{A} \geq 2$, *then there exists* $g \in G_2$ *such that one of the following possibilities holds*:

(a) $\{1_{\boldsymbol{O}}, \boldsymbol{u}_1\} \subset g\mathcal{A}$;

(b) $\{\boldsymbol{u}_1, \boldsymbol{v}_2\} \subset g\mathcal{A}$ *and* $1_{\boldsymbol{O}} \notin g\mathcal{A}$.

Proof. By Lemma 6.6, we assume that one of the following alternatives holds:

1. $1_{\boldsymbol{O}} \in \mathcal{A}$. There exists $a \in \mathcal{A}$ such that $\{1_{\boldsymbol{O}}, a\}$ are linearly independent. Since $G_2 1_{\boldsymbol{O}} = 1_{\boldsymbol{O}}$, by Proposition 6.2, we can assume that $a = \alpha e_1 + \beta e_2$ or $a = \alpha 1_{\boldsymbol{O}} + \boldsymbol{u}_1$ for some $\alpha, \beta \in \mathbb{F}$. In the first case we have $\alpha = \beta$ and $\{1_{\boldsymbol{O}}, a\}$ are linearly dependent; a contradiction. In the second case we obtain that $\boldsymbol{u}_1 = a - \alpha 1_{\boldsymbol{O}}$ lies in $\mathcal{A}$.

2. $\boldsymbol{u}_1 \in \mathcal{A}$ and $1_{\boldsymbol{O}} \notin \mathcal{A}$. There exists $b \in \mathcal{A}$ such that $\{\boldsymbol{u}_1, b\}$ are linearly independent. Consider $g \in G_2$ such that $g(\boldsymbol{u}_1, b) = (a', b')$ is one of the pairs from Proposition 6.3. Since $\mathrm{tr}(a') = n(a') = 0$ and $a' \neq 0$, one easily sees that $a' = \boldsymbol{u}_1$. By Remark 6.7 and the fact that $1_{\boldsymbol{O}} \notin \mathcal{A}$ one sees that both diagonal entries of b' are equal to zero. Using the fact that $\{\boldsymbol{u}_1, b'\}$ are linearly independent, we obtain that the pair $(\boldsymbol{u}_1, b')$ has one of the following types:

($\mathrm{K}_1\mathrm{L}_1^{\top}$) $b' = \beta \boldsymbol{v}_1$, where $\beta \in \mathbb{F} \setminus \{0\}$. Since $\boldsymbol{u}_1 b' = \beta e_1$ and $\mathrm{tr}(e_1) \neq 0$, we obtain a contradiction.

($\mathrm{K}_1\mathrm{M}_1$) $b' = \boldsymbol{u}_2$. Since $\boldsymbol{u}_1 b' = \boldsymbol{v}_3$, acting by a suitable element of SL_3 and using part (c) of Remark 6.4, we obtain case (b).

($\mathrm{K}_1\mathrm{M}_1^{\top}$) $b' = \boldsymbol{v}_2$, i.e., we have case (b). □

Lemma 6.9. *If* $\dim \mathcal{A} \geq 3$, *then there exists* $g \in G_2$ *such that one of the following possibilities holds*:

(a) $\{1_{\boldsymbol{O}}, \boldsymbol{u}_1, \boldsymbol{v}_2\} \subset g\mathcal{A}$;

(b) $\{\boldsymbol{u}_1, \boldsymbol{v}_2, \boldsymbol{v}_3\} \subset g\mathcal{A}$ *and* $1_{\boldsymbol{O}} \notin g\mathcal{A}$.

Proof. By Lemma 6.8, one can assume that one of the following possibilities holds:

1. $\{1_{\boldsymbol{O}}, \boldsymbol{u}_1\} \subset \mathcal{A}$. There exists $b \in \mathcal{A}$ such that $\{1_{\boldsymbol{O}}, \boldsymbol{u}_1, b\}$ are linearly independent. Consider $g \in G_2$ such that $g(\boldsymbol{u}_1, b) = (a', b')$ is one of the pairs from Proposition 6.3. Since $\mathrm{tr}(a') = n(a') = 0$ and $a' \neq 0$, one easily sees that $a' = \boldsymbol{u}_1$. Let β' be the diagonal element of b'. Since $G_2 1_{\boldsymbol{O}} = 1_{\boldsymbol{O}}$, taking $b'' = b' - \beta' 1_{\boldsymbol{O}}$ instead of b', we can assume that $\{1_{\boldsymbol{O}}, \boldsymbol{u}_1, b''\} \subset \mathcal{A}$ are linearly independent and $(\boldsymbol{u}_1, b'')$ has one of types from Proposition 6.3, where the diagonal elements of b'' are zeros. Consider the possible types for $(\boldsymbol{u}_1, b'')$:

($\mathrm{K}_1\mathrm{L}_1^{\top}$) $\{1_{\boldsymbol{O}}, \boldsymbol{u}_1, \beta \boldsymbol{v}_1\} \subset \mathcal{A}$ for some nonzero $\beta \in \mathbb{F}$. Since $\boldsymbol{u}_1 \boldsymbol{v}_1 = e_1$, we obtain a contradiction.

($\mathrm{K}_1\mathrm{M}_1$) $\{1_{\boldsymbol{O}}, \boldsymbol{u}_1, \boldsymbol{u}_2\} \subset \mathcal{A}$. Since $\boldsymbol{u}_1 \boldsymbol{u}_2 = \boldsymbol{v}_3$, acting by a suitable element of SL_3 from part (c) of Remark 6.4 we obtain case (a).

($\mathrm{K}_1\mathrm{M}_1^{\top}$) $\{1_{\boldsymbol{O}}, \boldsymbol{u}_1, \boldsymbol{v}_2\} \subset \mathcal{A}$, i.e., we have case (a).

2. $\{\boldsymbol{u}_1, \boldsymbol{v}_2\} \subset \mathcal{A}$ and $1_{\boldsymbol{O}} \notin \mathcal{A}$. Consider $b \in \mathcal{A}$ such that $\{\boldsymbol{u}_1, \boldsymbol{v}_2, b\}$ are linearly independent. One can assume that $b = \begin{pmatrix} \beta_1 & (0,\beta_3,\beta_4) \\ (\beta_5,0,\beta_7) & \beta_1 \end{pmatrix}$ for some $\beta_i \in \mathbb{F}$. Since

$$\boldsymbol{u}_1 b = \begin{pmatrix} \beta_5 & (\beta_1, 0, 0) \\ (0, -\beta_4, \beta_3) & 0 \end{pmatrix} \quad \text{and} \quad \boldsymbol{v}_2 b = \begin{pmatrix} 0 & (-\beta_7, 0, \beta_5) \\ (0, \beta_1, 0) & \beta_3 \end{pmatrix},$$

we have $\beta_3=\beta_5=0$. The equality $b^2=(\beta_1^2+\beta_4\beta_7)1_{\boldsymbol{O}}$ implies that $\{\boldsymbol{u}_1, \boldsymbol{v}_2, b\}\subset\mathcal{A}$, where the element $b=\beta_1 1_{\boldsymbol{O}}+\beta_4\boldsymbol{u}_3+\beta_7\boldsymbol{v}_3$ is nonzero and $\beta_1^2=\beta_4\beta_7$.

Let $\beta_1=0$. Then $\boldsymbol{u}_3$ lies in $\mathcal{A}$ or case (b) holds. If $\boldsymbol{u}_3\in\mathcal{A}$, then $\{\boldsymbol{u}_1, \boldsymbol{v}_2, \boldsymbol{u}_3\}\subset\mathcal{A}$; thus, $\{\boldsymbol{v}_1, \boldsymbol{u}_2, \boldsymbol{v}_3\}\subset\hbar\,\mathcal{A}$ and part (c) of Remark 6.4 implies that case (b) holds.

Let $\beta_1\neq 0$. Then $\beta_4, \beta_7\neq 0$ and for $g=\delta_1(0, 0, \beta_1/\beta_7)$ from G_2 we have

$$g(\boldsymbol{u}_1, \boldsymbol{v}_2, b)=\left(\boldsymbol{u}_1+\frac{\beta_1}{\beta_7}\boldsymbol{v}_2, \boldsymbol{v}_2, \beta_7\boldsymbol{u}_3\right).$$

Therefore, $\{\boldsymbol{u}_1, \boldsymbol{v}_2, \boldsymbol{u}_3\}\subset g\mathcal{A}$ and case (b) holds (see above). □

6B. *The case of nontraceless subalgebra.* In this section we assume that $\operatorname{char}\mathbb{F}=2$ and $\mathcal{A}\not\subset\boldsymbol{O}_0$ is a subalgebra of $\boldsymbol{O}$.

Lemma 6.10. *If* $\dim\mathcal{A}\geq 2$, *then there exists* $g\in G_2$ *such that one of the following possibilities holds*:

(a) $\{e_1, \boldsymbol{u}_1\}\subset g\mathcal{A}$;

(b) $\{e_1, \boldsymbol{v}_1\}\subset g\mathcal{A}$;

(c) $\{e_1, e_2\}\subset g\mathcal{A}$.

Proof. By Lemma 6.6 we can assume that $e_1\in\mathcal{A}$. There exists $b\in\mathcal{A}$ such that $\{e_1, b\}$ are linearly independent. One can also assume that $b=\left(\begin{smallmatrix}0 & \boldsymbol{u}\\ \boldsymbol{v} & \beta\end{smallmatrix}\right)$ for some $\boldsymbol{u}, \boldsymbol{v}\in\mathbb{F}^3$ and $\beta\in\mathbb{F}$.

Assume $\boldsymbol{u}\neq\boldsymbol{0}$. Since $e_1b=\left(\begin{smallmatrix}0 & \boldsymbol{u}\\ \boldsymbol{0} & 0\end{smallmatrix}\right)$, by part (a) of Remark 6.4 there exists $g\in\mathrm{SL}_3$ such that $g(e_1, e_1b)=(e_1, \boldsymbol{u}_1)$, i.e., the case (a) holds.

Assume $\boldsymbol{v}\neq\boldsymbol{0}$. Since $b\,e_1=\left(\begin{smallmatrix}0 & \boldsymbol{0}\\ \boldsymbol{v} & 0\end{smallmatrix}\right)$, by part (b) of Remark 6.4 there exists $g\in\mathrm{SL}_3$ such that $g(e_1, b\,e_1)=(e_1, \boldsymbol{v}_1)$, i.e., the case (b) holds.

In case $\boldsymbol{u}=\boldsymbol{v}=\boldsymbol{0}$ we have $\beta\neq 0$, i.e., the case (c) holds. □

Lemma 6.11. *If* $\dim\mathcal{A}\geq 3$, *then there exists* $g\in G_2$ *such that one of the following possibilities holds*:

(a) $\{e_1, e_2, \boldsymbol{u}_1\}\subset g\mathcal{A}$;

(b) $\{e_1, \boldsymbol{u}_1, \boldsymbol{v}_2\}\subset g\mathcal{A}$.

Before the proof of this lemma we formulate the following remark.

Remark 6.12. (a) $\{e_1, e_2, \boldsymbol{u}_1\}\subset\mathcal{A}$ if and only if $\{e_1, e_2, \boldsymbol{v}_1\}\subset\hbar\,\mathcal{A}$.

(b) $\{e_1, \boldsymbol{u}_1, \boldsymbol{v}_2\}\subset\mathcal{A}$ if and only if $\{e_1, \boldsymbol{u}_2, \boldsymbol{v}_1\}\subset g\mathcal{A}$ for some $g\in G_2$ (see part (c) of Remark 6.4).

Proof of Lemma 6.11. By Lemma 6.10, we assume that one of the following possibilities holds:

1. $\{e_1, \boldsymbol{u}_1\}\subset\mathcal{A}$. There exists $b\in\mathcal{A}$ such that $\{e_1, \boldsymbol{u}_1, b\}$ are linearly independent. We can assume that $b=\left(\begin{smallmatrix}0 & \boldsymbol{u}\\ \boldsymbol{v} & \beta\end{smallmatrix}\right)$ for some $\boldsymbol{u}=(0, *, *)\in\mathbb{F}^3$, $\boldsymbol{v}=(\gamma_1, \gamma_2, \gamma_3)\in\mathbb{F}^3$ and $\beta\in\mathbb{F}$.

Assume $\boldsymbol{u}\neq\boldsymbol{0}$. Since $e_1b=\left(\begin{smallmatrix}0 & \boldsymbol{u}\\ \boldsymbol{0} & 0\end{smallmatrix}\right)$, by part (d) of Remark 6.4 there exists $g\in\mathrm{SL}_3$ such that $g(e_1, \boldsymbol{u}_1, e_1b)=(e_1, \boldsymbol{u}_1, \boldsymbol{u}_2)$. By part (c) of Remark 6.4 there exists $g'\in\mathrm{SL}_3$ such that $g'(e_1, \boldsymbol{u}_1, e_1b)=(e_1, \boldsymbol{u}_1, \boldsymbol{u}_3)$. The equality $\boldsymbol{u}_1\boldsymbol{u}_3=-\boldsymbol{v}_2$ implies that the case (b) holds.

Assume $\boldsymbol{u} = \mathbf{0}$. Note that $b\, e_1 = \left(\begin{smallmatrix} 0 & \mathbf{0} \\ \boldsymbol{v} & 0 \end{smallmatrix}\right)$ lies in $\mathcal{A}$.

Let $\gamma_1 \neq 0$. The equality $b\, \boldsymbol{u}_1 = \gamma_1 e_2$ implies that the case (a) holds.

Otherwise, $\gamma_1 = 0$. In case $\gamma_2 \neq 0$ or $\gamma_3 \neq 0$, by part (e) of Remark 6.4 there exists $g \in \mathrm{SL}_3$ such that $g(e_1, \boldsymbol{u}_1, b\, e_1) = (e_1, \boldsymbol{u}_1, \boldsymbol{v}_2)$, that is, the case (b) holds. If $\gamma_2 = \gamma_3 = 0$, then $\beta \neq 0$ and $e_2 \in \mathcal{A}$, that is, the case (a) holds.

2. The case $\{e_1, \boldsymbol{v}_1\} \subset \mathcal{A}$ is similar to case 1.

3. $\{e_1, e_2\} \subset \mathcal{A}$. There exists $b = \left(\begin{smallmatrix} \alpha & \boldsymbol{u} \\ \boldsymbol{v} & \beta \end{smallmatrix}\right)$ in $\mathcal{A}$ such that $\{e_1, e_2, b\}$ are linearly independent. We can assume that $\alpha = \beta = 0$.

Assume $\boldsymbol{u} \neq \mathbf{0}$. Since $e_1 b = \left(\begin{smallmatrix} 0 & \boldsymbol{u} \\ \mathbf{0} & 0 \end{smallmatrix}\right)$, by part (a) of Remark 6.4 there exists $g \in \mathrm{SL}_3$ such that $g(e_1, e_2, e_1 b) = (e_1, e_2, \boldsymbol{u}_1)$, equivalently, the case (a) holds.

Otherwise, $\boldsymbol{v} \neq \mathbf{0}$. Since $b = \left(\begin{smallmatrix} 0 & \mathbf{0} \\ \boldsymbol{v} & 0 \end{smallmatrix}\right)$ by part (b) of Remark 6.4 there exists $g \in \mathrm{SL}_3$ such that $g(e_1, e_2, b) = (e_1, e_2, \boldsymbol{v}_1)$. By part (a) of Remark 6.12 we obtain that case (a) holds. □

6C. ***Proof of Proposition 6.1.*** Assume $\mathfrak{A} = [\mathcal{A}]$ for some subalgebra $\mathcal{A}$ of $\boldsymbol{O}$. Lemmas 6.6, 6.8, 6.9, 6.10, 6.11 imply that there exist $g \in G_2$ such that $g\mathcal{A}$ contains one of the sets from the formulation of Proposition 6.1. Since the $\mathbb{F}$-span of each of these sets is an algebra, the proof is completed.

7. Separating invariants in case char $\mathbb{F} = 2$

In this section we assume that char $\mathbb{F} = 2$. We introduce some notation for $\underline{a} \in \boldsymbol{O}^n$:

- the *rank* $\mathrm{rk}(\underline{a})$ is the dimension of the subspace of $\boldsymbol{O}$ spanned by $a_1, \dots, a_n$;
- $\mathrm{alg}(\underline{a})$ is the $\mathbb{F}$-algebra (in general, nonunital) generated by $a_1, \dots, a_n$.

Obviously, $\mathrm{rk}(g\underline{a}) = \mathrm{rk}(\underline{a})$ for every $g \in G_2$. The following remark is well-known (for example, see Corollary 2.3.6 of [2]).

Remark 7.1. Assume $\underline{a} \in \boldsymbol{O}^n$. Then there exists a unique closed G_2-orbit $O = O_{\underline{a}}$ in the closure of $G_2\underline{a}$, and $O_{\underline{a}}$ is the only closed orbit in the fiber

$$\{\underline{c} \in \boldsymbol{O}^n \mid f(\underline{a}) = f(\underline{c}) \text{ for all } f \in K_n^{G_2}\}.$$

In particular, $f(\underline{a}) = f(\underline{c})$ for every $f \in K_n^{G_2}$ and $\underline{c} \in O_a$.

Observe that the group GL_n acts naturally on $\boldsymbol{O}^n$ on the right as follows: for any $A = (\alpha_{ij}) \in \mathrm{GL}_n$ and $\underline{a} \in \boldsymbol{O}^n$ we set

$$(\underline{a}A)_i = \sum_{1 \le k \le n} \alpha_{ki} a_k \quad \text{for } 1 \le i \le n.$$

This action commutes with the left G_2-action.

Lemma 7.2. *Given $\underline{a}, \underline{b} \in \boldsymbol{O}^n$, define $\underline{a}' = \underline{a}A$ and $\underline{b}' = \underline{b}A$ for some $A \in \mathrm{GL}_n$. Then*:

(a) *$G_2\underline{a} = G_2\underline{b}$ if and only if $G_2\underline{a}' = G_2\underline{b}'$.*

(b) *Given some* $d \geq 2$, *we have that* $\underline{a}$ *and* $\underline{b}$ *are not separated by* $S_n^{(d)}$ *if and only if* $\underline{a}'$ *and* $\underline{b}'$ *are not separated by* $S_n^{(d)}$.

(c) $G_2\underline{a}$ *is closed if and only if* $G_2\underline{a}'$ *is closed.*

Proof. Since A is invertible, for each part of this lemma it is sufficient to prove the "only if" implication.

(a) For each $g \in G_2$ the equality $g\underline{a} = \underline{b}$ implies $g\underline{a}' = \underline{b}'$, hence our claim follows.

(b) Assume that $\underline{a}$ and $\underline{b}$ are not separated by $S_n^{(d)}$, i.e., $f(\underline{a}) = f(\underline{b})$ for all $f \in S_n^{(d)}$. The linearity of the trace together with Lemma 4.2 and formulas (2-3), (2-8) imply that $h(\underline{a}') = h(\underline{b}')$ for all $h \in S_n^{(d)}$.

(c) The right action by A on $\boldsymbol{O}^n$ gives a homeomorphism of $\boldsymbol{O}^n$ with respect to the Zariski topology. Hence it sends closed subsets to closed subsets. Moreover, it maps G_2-orbits to G_2-orbits. □

The following remark is a consequence of part (c) of Lemma 7.2.

Remark 7.3. An equivalence class $\mathfrak{A} \in \Omega(\boldsymbol{O})$ is closed if and only if for every subalgebra $\mathcal{A}$ of $\boldsymbol{O}$ with $[\mathcal{A}] = \mathfrak{A}$ we have that if $\mathcal{A}$ is the $\mathbb{F}$-span of some $a_1, \ldots, a_n$, then the G_2-orbit of $(a_1, \ldots, a_n)$ is closed in $\boldsymbol{O}^n$.

Proposition 7.4. *The set* $S_m^{(8)} \subset K_m^{G_2}$ *is separating for every* $m > 0$ *if and only if* $S_n^{(8)}$ *separates different closed* G_2*-orbits of* $\underline{a} = (a_1, \ldots, a_l, 0, \ldots, 0) \in \boldsymbol{O}^n$ *and* $\underline{b} \in \boldsymbol{O}^n$ *for all* $n > 0$, *where*

- $a_1, \ldots, a_l$ *is a basis of some subalgebra* $\mathcal{A}$ *of* $\boldsymbol{O}$,
- $b_1, \ldots, b_n$ *of* $\boldsymbol{O}$ *linearly generate some subalgebra* $\mathcal{B}$ *of* $\boldsymbol{O}$,
- $\dim \mathcal{A} \geq \dim \mathcal{B}$.

Proof. We only have to prove the "if" part of the statement. Assume that $\underline{a}, \underline{b} \in \boldsymbol{O}^n$ are not separated by $S_n^{(8)}$ for some $n > 0$. To obtain the required, we will show that $G_2\underline{a} = G_2\underline{b}$.

By Remark 7.1 we can assume that $G_2\underline{a}$ and $G_2\underline{b}$ are closed.

Claim 1. Given an $\mathbb{F}$-basis $a_1', \ldots, a_l'$ of $\mathbb{F}$-span of $a_1, \ldots, a_n$, without loss of generality, we can assume that $\underline{a} = (a_1', \ldots, a_l', 0, \ldots, 0) \in \boldsymbol{O}^n$.

To prove claim 1, we consider $A \in \mathrm{GL}_n$ such that $\underline{a}A = (a_1', \ldots, a_l', 0, \ldots, 0)$. Parts (a), (b), (c) of Lemma 7.2 imply that we can consider $\underline{a}A, \underline{b}A$ instead of $\underline{a}, \underline{b}$ and claim 1 is proven.

Denote by $\mathcal{A}$ the algebra generated by $a_1, \ldots, a_n$ and by $\mathcal{B}$ the algebra generated by $b_1, \ldots, b_n$. Without loss of generality we can assume that $\dim \mathcal{A} \geq \dim \mathcal{B}$.

Claim 2. Without loss of generality, we can assume that $\mathbb{F}$-span of $a_1, \ldots, a_n$ is $\mathcal{A}$ and $\mathbb{F}$-span of $b_1, \ldots, b_n$ is $\mathcal{B}$.

Let us prove claim 2. It is an easy exercise in linear algebra to show that there exists $A \in \mathrm{GL}_n$ such that $\underline{a}A = (a_1', \ldots, a_l', 0, \ldots, 0)$ and $\underline{b}A = (0, \ldots, 0, b_d', \ldots, b_t', 0, \ldots, 0)$, where $a_1', \ldots, a_l'$ is a basis for $\mathbb{F}$-span of $a_1, \ldots, a_n$ and $b_d', \ldots, b_t'$ is a basis for $b_1, \ldots, b_n$. Similarly to claim 1, without loss of generality, we can take $\underline{a}A, \underline{b}A$ instead of $\underline{a}, \underline{b}$, that is, we assume that

$$\underline{a} = (a_1, \ldots, a_l, 0, \ldots, 0) \quad \text{and} \quad \underline{b} = (0, \ldots, 0, b_d, \ldots, b_t, 0, \ldots, 0),$$

where $l \le 8 = \dim \boldsymbol{O}$ and $t-d+1 \le 8$. There exist words $v_1, \dots, v_r$ of $\mathbb{F}\{\mathbb{X}\}_n$ such that the $\mathbb{F}$-span of the set $a_1, \dots, a_n, v_1(\underline{a}), \dots, v_r(\underline{a})$ is $\mathcal{A}$. Similarly, there exist words $w_1, \dots, w_s$ of $\mathbb{F}\{\mathbb{X}\}_n$ such that the $\mathbb{F}$-span of the set $b_1, \dots, b_n, w_1(\underline{b}), \dots, w_s(\underline{b})$ is $\mathcal{B}$.

Since the map $\boldsymbol{O}^n \to \boldsymbol{O}^{r+s}$ given by $\underline{x} \to (v_1(\underline{x}), \dots, v_r(\underline{x}), w_1(\underline{x}), \dots, w_s(\underline{x}))$ is a morphism of affine algebraic varieties, the G_2-orbits of

$$\underline{c}_1 = (a_1, \dots, a_n, v_1(\underline{a}), \dots, v_r(\underline{a}), w_1(\underline{a}), \dots, w_s(\underline{a})),$$
$$\underline{c}_2 = (b_1, \dots, b_n, v_1(\underline{b}), \dots, v_r(\underline{b}), w_1(\underline{b}), \dots, w_s(\underline{b}))$$

are closed. Obviously, $G_2\underline{a} = G_2\underline{b}$ if and only if $G_2\underline{c}_1 = G_2\underline{c}_2$. By Lemma 4.2 and formula (2-8), for any $f \in S^{(8)}_{n+r+s}$ we have that $f(\underline{c}_1)$ is a nonassociative polynomial in $\mathrm{tr}\big((\dots(a_{i_1}a_{i_2})\dots)a_{i_k}\big)$ and $n(a_i)$ for $1 \le i_1 < \dots < i_k \le n$ and $1 \le i \le n$. But this trace is zero in case $k > 8$ by the construction of $\underline{a}$. The same fact holds also for $f(\underline{c}_2)$. Thus, $\underline{a}$ and $\underline{b}$ are not separated by $S^{(8)}_n$ if and only if $\underline{c}_1$ and $\underline{c}_2$ are not separated by $S^{(8)}_{n+r+s}$. Therefore, we can consider $\underline{c}_1, \underline{c}_2$ instead of $\underline{a}, \underline{b}$ and claim 2 is proven.

Since claims 1 and 2 imply that $\underline{a}, \underline{b}$ satisfy conditions from the formulation of the lemma, we obtain that $G_2\underline{a} = G_2\underline{b}$. □

Lemma 7.5. 1. *For every $a \in \mathbb{M}$ with $\mathrm{tr}(a) = 1$ and $n(a) = 0$ there exists g from the stabilizer $\mathrm{Stab}_{G_2}(\mathbb{M}) = \{g \in G_2 \mid g\,\mathbb{M} \subset \mathbb{M}\}$ such that $ga = e_1$.*

2. *For every $a \in \mathbb{M}$ with $\mathrm{tr}(a) = 0$ and $n(a) = 1$ there exists $g \in \mathrm{Stab}_{G_2}(\mathbb{M})$ such that $ga \in \{1_{\boldsymbol{O}}, 1_{\boldsymbol{O}} + \boldsymbol{u}_1\}$.*

3. *Given nonzero $\gamma \in \mathbb{F}$, there exists $\xi_\gamma \in \mathrm{Stab}_{G_2}(\mathbb{M})$ such that for every $\alpha_1, \dots, \alpha_4 \in \mathbb{F}$ we have*

$$\xi_\gamma \begin{pmatrix} \alpha_1 & (\alpha_2, 0, 0) \\ (\alpha_3, 0, 0) & \alpha_4 \end{pmatrix} = \begin{pmatrix} \alpha_1 & (\gamma\alpha_2, 0, 0) \\ (\gamma^{-1}\alpha_3, 0, 0) & \alpha_4 \end{pmatrix}.$$

4. *Assume that $\underline{a} = (e_1, e_2)$ and $\underline{b} \in \mathbb{M}^2$ satisfy $S^{(2)}_n(\underline{a}) = S^{(2)}_n(\underline{b})$. Then there exists $g \in \mathrm{Stab}_{G_2}(\mathbb{M})$ such that $gb_1 = e_1$ and $gb_2 \in \{e_2, e_2 + \boldsymbol{u}_1, e_2 + \boldsymbol{v}_1\}$.*

5. *If $b \in \mathbb{M}$ satisfies $\mathrm{tr}(b) = n(b) = \mathrm{tr}(e_1 b) = 0$, then $b \in \mathbb{F}\boldsymbol{u}_1$ or $b \in \mathbb{F}\boldsymbol{v}_1$.*

Proof. **1.** For $A = \mathcal{F}^{-1}(a)$ we have $\mathrm{tr}(A) = 1$ and $\det(A) = 0$. Hence there exists $g \in \mathrm{GL}_2$ such that $g^{-1}Ag = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$ and Lemma 6.5 completes the proof.

2. For $A = \mathcal{F}^{-1}(a)$ we have $\mathrm{tr}(A) = 0$ and $\det(A) = 1$. Hence there exists $g \in \mathrm{GL}_2$ such that $g^{-1}Ag = \left(\begin{smallmatrix} \lambda & 1 \\ 0 & \lambda \end{smallmatrix}\right)$ or $g^{-1}Ag = \left(\begin{smallmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{smallmatrix}\right)$ for some $\lambda, \lambda_1, \lambda_2$ and Lemma 6.5 completes the proof.

3. Given $g = \left(\begin{smallmatrix} 1 & 0 \\ 0 & \gamma \end{smallmatrix}\right) \in \mathrm{GL}_2$, we have

$$g^{-1}\begin{pmatrix} \alpha_1 & \alpha_2 \\ \alpha_3 & \alpha_4 \end{pmatrix} g = \begin{pmatrix} \alpha_1 & \gamma\alpha_2 \\ \gamma^{-1}\alpha_3 & \alpha_4 \end{pmatrix}.$$

Lemma 6.5 concludes the proof.

4. By part 1 we assume that $b_1 = e_1$. Define $\mathcal{F}^{-1}(b_2) = B_2 = \left(\begin{smallmatrix} \beta_1 & \beta_2 \\ \beta_3 & \beta_4 \end{smallmatrix}\right)$. Since $0 = \mathrm{tr}(a_1 a_2) = \mathrm{tr}(b_1 b_2)$, we obtain $\beta_1 = 0$. The equalities $\mathrm{tr}(b_2) = 1$ and $n(b_2) = 0$ imply $\beta_4 = 1$ and $\beta_2\beta_3 = 0$. Part 3 concludes the proof.

5. Define $\mathcal{F}^{-1}(b) = B = \left(\begin{smallmatrix}\beta_1 & \beta_2\\ \beta_3 & \beta_4\end{smallmatrix}\right)$. Since $0 = \mathrm{tr}(e_1 b) = \beta_1$, the equalities $\mathrm{tr}(b) = n(b) = 0$ conclude the proof. □

Lemma 7.6. *Assume that* $\underline{a} = (a_1, 0, \dots, 0) \in \mathbb{M}^n$ *and* $\underline{b} \in \mathbb{M}^n$ *are not separated by* $S_n^{(2)}$, *where* $a_1 \in \{1_{\boldsymbol{O}}, e_1\}$ *and* $\dim(\mathrm{alg}(\underline{b})) \leq 1$. *Then* $G_2\, \underline{a} = G_2\, \underline{b}$.

Proof. **1.** Let $a_1 = 1_{\boldsymbol{O}}$. Since $\mathrm{tr}(b_1) = 0$ and $n(b_1) = 1$, by part 2 of Lemma 7.5 we can assume that $b_1 = 1_{\boldsymbol{O}}$ or $b_1 = 1_{\boldsymbol{O}} + \boldsymbol{u}_1$.

In the first case, $\dim(\mathrm{alg}(\underline{b})) \leq 1$ implies $\underline{b} = (1_{\boldsymbol{O}}, \beta_2 1_{\boldsymbol{O}}, \dots, \beta_n 1_{\boldsymbol{O}})$ for some $\beta_2, \dots, \beta_n \in \mathbb{F}$. Since $0 = n(b_i) = \beta_i^2$ for all $1 < i \leq n$, we have $\underline{a} = \underline{b}$.

In the second case we have that b_1 and $b_1^2 = 1_{\boldsymbol{O}}$ are linearly independent; a contradiction.

2. Let $a_1 = e_1$. Since $\mathrm{tr}(b_1) = 1$ and $n(b_1) = 0$, by part 1 of Lemma 7.5 we can assume that $b_1 = e_1$. Then the condition $\dim(\mathrm{alg}(\underline{b})) \leq 1$ implies that $\underline{b} = (e_1, \beta_2 e_1, \dots, \beta_n e_1)$ for some $\beta_2, \dots, \beta_n \in \mathbb{F}$. For each $1 < i \leq n$ we have $0 = \mathrm{tr}(a_1 0) = \mathrm{tr}(b_1 b_i) = \beta_i$. Therefore, $\underline{a} = \underline{b}$. □

Lemma 7.7. *Assume that* $\underline{a} = (e_1, e_2, 0, \dots, 0) \in \mathbb{M}^n$ *and* $\underline{b} \in \mathbb{M}^n$ *are not separated by* $S_n^{(2)}$ *and* $\dim(\mathrm{alg}(\underline{b})) \leq 2$. *Then* $G_2\, \underline{a} = G_2\, \underline{b}$.

Proof. By part 4 of Lemma 7.5 we can assume that $b_1 = e_1$ and $b_2 \in \{e_2, e_2 + \boldsymbol{u}_1, e_2 + \boldsymbol{v}_1\}$.

Let $b_2 = e_2$. For $3 \leq i \leq n$ part 5 of Lemma 7.5 implies that $b_i \in \mathbb{F}\boldsymbol{u}_1$ or $b_i \in \mathbb{F}\boldsymbol{v}_1$, since $\mathrm{tr}(b_i) = n(b_i) = \mathrm{tr}(b_1 b_i) = 0$. It follows from $\dim(\mathrm{alg}(\underline{b})) \leq 2$ that $b_i = 0$ for all $3 \leq i \leq n$. Therefore, $\underline{a} = \underline{b}$.

In case $b_2 = e_2 + \boldsymbol{u}_1$ we consider $b_1 b_2 = \boldsymbol{u}_1$ and obtain that $\{e_1, \boldsymbol{u}_1, e_2\} \subset \mathrm{alg}(\underline{b})$; a contradiction.

In case $b_2 = e_2 + \boldsymbol{v}_1$ we consider $b_2 b_1 = \boldsymbol{v}_1$ and obtain that $\{e_1, \boldsymbol{v}_1, e_2\} \subset \mathrm{alg}(\underline{b})$; a contradiction. □

Lemma 7.8. *If* $\underline{a} = (e_1, e_2, \boldsymbol{u}_1, \boldsymbol{v}_1, 0, \dots, 0) \in \mathbb{M}^n$ *and* $\underline{b} \in \mathbb{M}^n$ *are not separated by* $S_n^{(3)}$, *then* $G_2\, \underline{a} = G_2\, \underline{b}$.

Proof. By part 4 of Lemma 7.5 we can assume that $b_1 = e_1$ and $b_2 \in \{e_2, e_2 + \boldsymbol{u}_1, e_2 + \boldsymbol{v}_1\}$. Assume $3 \leq i \leq n$. We have $\mathrm{tr}(b_i) = n(b_i) = \mathrm{tr}(b_1 b_i) = 0$, since $\mathrm{tr}(a_1 a_3) = \mathrm{tr}(a_1 a_4) = 0$. Thus part 5 of Lemma 7.5 implies that $b_i = \beta_i \boldsymbol{u}_1$ or $b_i = \beta_i \boldsymbol{v}_1$ for some $\beta_i \in \mathbb{F}$. Since $\mathrm{tr}(b_3 b_4) = \mathrm{tr}(a_3 a_4) = 1$, we obtain that $\beta_3 \beta_4 = 1$ and either $b_3 = \beta_3 \boldsymbol{u}_1$, $b_4 = \beta_4 \boldsymbol{v}_1$ or $b_3 = \beta_3 \boldsymbol{v}_1$, $b_4 = \beta_4 \boldsymbol{u}_1$ for some nonzero $\beta_3, \beta_4 \in \mathbb{F}$ with $\beta_3 \beta_4 = 1$. Hence equalities $\mathrm{tr}(b_3 b_2) = \mathrm{tr}(b_4 b_2) = 0$ imply that $b_2 = e_2$.

1. Let $b_3 = \beta_3 \boldsymbol{u}_1$, $b_4 = \beta_3^{-1} \boldsymbol{v}_1$. By part 3 of Lemma 7.5 we can assume that $\beta_3 = 1$.

Consider $5 \leq i \leq n$. If $b_i = \beta_i \boldsymbol{u}_1$, then $0 = \mathrm{tr}(a_4 a_i) = \mathrm{tr}(b_4 b_i) = \beta_i$. If $b_i = \beta_i \boldsymbol{v}_1$, then $0 = \mathrm{tr}(a_3 a_i) = \mathrm{tr}(b_3 b_i) = \beta_i$. Therefore, $\underline{a} = \underline{b}$.

2. If $b_3 = \beta_3 \boldsymbol{v}_1$, $b_4 = \beta_3^{-1} \boldsymbol{u}_1$, we have $0 = \mathrm{tr}((b_1 b_3) b_4) = \mathrm{tr}((a_1 a_3) a_4) = \mathrm{tr}(\boldsymbol{u}_1 \boldsymbol{v}_1) = 1$; a contradiction. □

Lemma 7.9. *If* $\underline{a} = (e_1, e_2, \boldsymbol{u}_1, \boldsymbol{v}_1, \boldsymbol{u}_2, \boldsymbol{v}_2, \boldsymbol{u}_3, \boldsymbol{v}_3, 0, \dots, 0) \in \boldsymbol{O}^n$ *and* $\underline{b} \in \boldsymbol{O}^n$ *are not separated by* $S_n^{(3)}$, *then* $G_2\, \underline{a} = G_2\, \underline{b}$.

Proof. Given $c_1, \dots, c_8$, denote by $M_{c_1,\dots,c_8}$ the Gram matrix $(\mathrm{tr}(c_i c_j))_{1 \leq i,j \leq 8}$. Since the trace is a bilinear nondegenerate form on $\boldsymbol{O}$ and $a_1, \dots, a_8$ are linearly independent, we obtain that $\det(G_{a_1,\dots,a_8}) = \det(G_{b_1,\dots,b_8})$ is nonzero. Hence, $b_1, \dots, b_8$ are also linearly independent. In particular, $\mathbb{F}$-span of $b_1, \dots, b_8$ is $\boldsymbol{O}$.

For every $1 \le i \le 8$ and $8 < j \le n$ we have that $\mathrm{tr}(a_i a_j) = \mathrm{tr}(b_i b_j)$ is zero. Therefore, $\mathrm{tr}(b b_j) = 0$ for all $b \in \boldsymbol{O}$. Since tr is nondegenerate on $\boldsymbol{O}$, we obtain $\underline{b} = (b_1, \dots, b_8, 0, \dots, 0)$.

For every $1 \le i, j \le 8$ there exists $1 \le k_{ij} \le 8$ and $\eta_{ij} \in \mathbb{F}$ such that $a_i a_j = \eta_{ij} a_{k_{ij}}$. Therefore, for each $1 \le l \le 8$ we have that $\mathrm{tr}((a_i a_j - \eta_{ij} a_{k_{ij}}) a_l) = \mathrm{tr}((b_i b_j - \eta_{ij} b_{k_{ij}}) b_l)$ is zero. Hence, $b_i b_j = \eta_{ij} b_{k_{ij}}$. Consider a linear map $f : \boldsymbol{O} \to \boldsymbol{O}$ defined on the basis of $\boldsymbol{O}$ by $f(a_i) = b_i$ for all $1 \le i \le 8$. Since the multiplication table for $a_1, \dots, a_8$ is the same as for $b_1, \dots, b_8$, we can see that $f \in G_2$. The required is proven. □

The following statement is a corollary of Proposition 6.1.

Corollary 7.10. *Assume* $\mathrm{char}\,\mathbb{F} = 2$ *and a closed equivalence class* $\mathfrak{A} \in \Omega(\boldsymbol{O})$ *has the dimension* $d \le 3$. *Then one of the following sets is a basis for* $\mathfrak{A}$:

$d = 1$: $\{1_{\boldsymbol{O}}\}, \{e_1\}$;

$d = 2$: $\{e_1, e_2\}$.

Proof. We need to show that any basis $\{a_1, \dots, a_n\}$ from Proposition 6.1, different from the above bases, generates nonclosed equivalence class. For each $\underline{a} = (a_1, \dots, a_n)$ the arguments are the same: we find an element $\underline{a}'$ in the closure of $G_2\underline{a}$ such that $\mathrm{rk}(\underline{a}') < \mathrm{rk}(\underline{a})$, which obviously implies that $G_2\underline{a}$ is not closed.

- If $\underline{a} = (\boldsymbol{u}_1) \in \boldsymbol{O}^1$, then for the standard one-parameter subgroup $\theta_{\underline{\lambda}}$ with $\underline{\lambda} = (1, -1, 0)$ the element $\underline{a}' = \lim_{t\to 0} \theta_{\underline{\lambda}}(t)\underline{a} = (0)$ lies in $\overline{G_2\underline{a}}$ (see Section 3B for more details).
- If $\underline{a} = (1_{\boldsymbol{O}}, \boldsymbol{u}_1)$, then $\underline{a}' = \lim_{t\to 0} \theta_{(1,-1,0)}(t)\underline{a} = (1_{\boldsymbol{O}}, 0)$ lies in $\overline{G_2\underline{a}}$.
- If $\underline{a} = (\boldsymbol{u}_1, \boldsymbol{v}_2)$, then $\underline{a}' = \lim_{t\to 0} \theta_{(1,-1,0)}(t)\underline{a} = (0, 0)$ lies in $\overline{G_2\underline{a}}$.
- If $\underline{a} = (e_1, \boldsymbol{u}_1)$, then $\underline{a}' = \lim_{t\to 0} \theta_{(1,-1,0)}(t)\underline{a} = (e_1, 0)$ lies in $\overline{G_2\underline{a}}$.
- If $\underline{a} = (e_1, \boldsymbol{v}_1)$, then $\underline{a}' = \lim_{t\to 0} \theta_{(-1,1,0)}(t)\underline{a} = (e_1, 0)$ lies in $\overline{G_2\underline{a}}$.
- If $\underline{a} = (1_{\boldsymbol{O}}, \boldsymbol{u}_1, \boldsymbol{v}_2)$, then $\underline{a}' = \lim_{t\to 0} \theta_{(1,-1,0)}(t)\underline{a} = (1_{\boldsymbol{O}}, 0, 0)$ lies in $\overline{G_2\underline{a}}$.
- If $\underline{a} = (e_1, e_2, \boldsymbol{u}_1)$, then $\underline{a}' = \lim_{t\to 0} \theta_{(1,-1,0)}(t)\underline{a} = (e_1, e_2, 0)$ lies in $\overline{G_2\underline{a}}$.
- If $\underline{a} = (e_1, \boldsymbol{u}_1, \boldsymbol{v}_2)$, then $\underline{a}' = \lim_{t\to 0} \theta_{(1,-1,0)}(t)\underline{a} = (e_1, 0, 0)$ lies in $\overline{G_2\underline{a}}$.
- If $\underline{a} = (\boldsymbol{u}_1, \boldsymbol{v}_2, \boldsymbol{v}_3)$, then $\underline{a}' = \lim_{t\to 0} \theta_{(1,-1,0)}(t)\underline{a} = (0, 0, \boldsymbol{v}_3)$ lies in $\overline{G_2\underline{a}}$. □

Theorem 7.11. *The set* $S_n^{(8)}$ *is a separating set for* $K_n^{G_2}$ *in case* $\mathrm{char}\,\mathbb{F} = 2$.

Proof. We will apply Proposition 7.4 to obtain the required statement. Assume that G_2-orbits of $\underline{a} = (a_1, \dots, a_l, 0, \dots, 0) \in \boldsymbol{O}^n$, $\underline{b} \in \boldsymbol{O}^n$ are closed, $a_1, \dots, a_l$ is a basis of some subalgebra $\mathcal{A}$ of $\boldsymbol{O}$, octonions $b_1, \dots, b_n$ linearly generate some subalgebra $\mathcal{B}$ of $\boldsymbol{O}$, and $\dim \mathcal{A} \ge \dim \mathcal{B}$. We assume that $\underline{a}$ and $\underline{b}$ are not separated by $S_n^{(8)}$.

Let $\dim \mathcal{A} = 8$. We may choose that $\underline{a} = (e_1, e_2, \boldsymbol{u}_1, \boldsymbol{v}_1, \boldsymbol{u}_2, \boldsymbol{v}_2, \boldsymbol{u}_3, \boldsymbol{v}_3, 0, \dots, 0)$ by Lemma 7.2. Then Lemma 7.9 implies that $G_2\,\underline{a} = G_2\,\underline{b}$.

Let $\dim \mathcal{A} < 8$. Then $\mathcal{A}$ lies in a maximal proper subalgebra of $\boldsymbol{O}$. By Theorem 5 of [19], the algebra of sextonions $\mathbb{S}$ is the unique maximal proper subalgebra of $\boldsymbol{O}$ modulo G_2-action (see also Remark 7.12

below). So $\mathcal{A} \subset \mathbb{S}$, that is, for all $1 \le i \le l$ we have

$$a_i = \begin{pmatrix} \alpha_{i1} & (\alpha_{i2}, \alpha_{i3}, 0) \\ (\alpha_{i4}, 0, \alpha_{i5}) & \alpha_{i6} \end{pmatrix}$$

for some $\alpha_{ij} \in \mathbb{F}$. Similarly, we can assume that $\mathcal{B} \subset \mathbb{S}$.

Since for the standard one-parameter subgroup $\theta_{\underline{\lambda}}$ with $\underline{\lambda} = (0, 1, -1)$ we have

$$\theta_{\underline{\lambda}}(t) a_i = \begin{pmatrix} \alpha_{i1} & (\alpha_{i2}, t\alpha_{i3}, 0) \\ (\alpha_{i4}, 0, t\alpha_{i5}) & \alpha_{i6} \end{pmatrix},$$

the limit $\underline{a}' = \lim_{t \to 0} \theta_{\underline{\lambda}}(t)\underline{a}$ exists (see Section 3B for more details). Obviously, $\underline{a}' = (a_1', \dots, a_l', 0, \dots, 0)$ lies in $\mathbb{M}^n$. The orbit $G_2\underline{a}$ is closed, therefore, $\underline{a}' \in G_2\,\underline{a}$. Replacing $\underline{a}$ by $\underline{a}'$ we may assume that $\underline{a} \subset \mathbb{M}^n$. Therefore, $\mathcal{A} \subset \mathbb{M}$. In the same manner we can assume that $\mathcal{B} \subset \mathbb{M}$.

In case $\dim \mathcal{A} = 4$ by Lemma 7.2 we may choose that $\underline{a} = (e_1, e_2, \boldsymbol{u}_1, \boldsymbol{v}_1, 0, \dots, 0)$ and Lemma 7.8 implies that $G_2\,\underline{a} = G_2\,\underline{b}$.

Let $\dim \mathcal{A} \le 3$. By Corollary 7.10 and Lemma 7.2 we can assume that $\underline{a}$ is one of the next elements: $(1_{\boldsymbol{O}})$, (e_1), (e_1, e_2). If $\underline{a} = (1_{\boldsymbol{O}})$ or $\underline{a} = (e_1)$, then Lemma 7.6 implies that $G_2\,\underline{a} = G_2\,\underline{b}$. If $\underline{a} = (e_1, e_2)$, then Lemma 7.7 implies that $G_2\,\underline{a} = G_2\,\underline{b}$.

Finally, by Proposition 7.4 the set $S_n^{(8)}$ is separating for $K_n^{G_2}$. □

Remark 7.12. In the proof of Theorem 5 of [19], which claims that $\mathbb{S}$ is the unique maximal proper subalgebra of $\boldsymbol{O}$ modulo G_2-action, there is a small error, but this does not interfere with the case of an algebraically closed field. See [8; 18] for more details.

Remark 7.13. It follows from Theorem 7.11 that the set $S_{0,n}^{(8)}$ is a separating set for $K_{0,n}^{G_2}$ in case $\operatorname{char} \mathbb{F} = 2$.

Acknowledgement

We are very grateful to the anonymous referees for helpful comments.

References

[1] F. B. Cavalcante and A. Lopatin, "Separating invariants of three nilpotent 3×3 matrices", *Linear Algebra Appl.* **607** (2020), 9–28. MR Zbl

[2] H. Derksen and G. Kemper, *Computational invariant theory*, Invariant Theory Algebr. Transform. Groups **1**, Springer, 2002. MR Zbl

[3] H. Derksen and V. Makam, "Algorithms for orbit closure separation for invariants and semi-invariants of matrices", *Algebra Number Theory* **14**:10 (2020), 2791–2813. MR Zbl

[4] M. Domokos, "Degree bound for separating invariants of abelian groups", *Proc. Amer. Math. Soc.* **145**:9 (2017), 3695–3708. MR Zbl

[5] M. Domokos, "Characteristic free description of semi-invariants of 2×2 matrices", *J. Pure Appl. Algebra* **224**:5 (2020), art. id. 106220. Addendum in **224**:6 (2020), art. id. 106270. MR Zbl

[6] M. Domokos, S. G. Kuzmin, and A. N. Zubkov, "Rings of matrix invariants in positive characteristic", *J. Pure Appl. Algebra* **176**:1 (2002), 61–80. MR Zbl

[7] E. Dufresne, J. Elmer, and M. Sezer, "Separating invariants for arbitrary linear actions of the additive group", *Manuscripta Math.* **143**:1-2 (2014), 207–219. MR Zbl

[8] S. M. Gagola, III, "Maximal subalgebras of the octonions", *J. Pure Appl. Algebra* **217**:1 (2013), 20–21. MR Zbl

[9] A. N. Grishkov, M. d. L. M. Giuliani, and A. V. Zavarnitsine, "Classification of subalgebras of the Cayley algebra over a finite field", *J. Algebra Appl.* **9**:5 (2010), 791–808. MR Zbl

[10] A. V. Iltyakov and I. P. Shestakov, "On invariants of F_4 and the center of the Albert algebra", *J. Algebra* **179**:3 (1996), 838–851. MR Zbl

[11] I. Kaygorodov, A. Lopatin, and Y. Popov, "Separating invariants for 2×2 matrices", *Linear Algebra Appl.* **559** (2018), 114–124. MR Zbl

[12] G. Kemper, A. Lopatin, and F. Reimers, "Separating invariants over finite fields", *J. Pure Appl. Algebra* **226**:4 (2022), art. id. 106904. MR Zbl

[13] G. R. Kempf, "Instability in invariant theory", *Ann. of Math.* (2) **108**:2 (1978), 299–316. MR Zbl

[14] M. Kohls and M. Sezer, "Separating invariants for the Klein four group and cyclic groups", *Int. J. Math.* **24**:6 (2013), art. id. 1350046. MR Zbl

[15] J. M. Landsberg and L. Manivel, "The sextonions and $E_{7\frac{1}{2}}$", *Adv. Math.* **201**:1 (2006), 143–179. MR Zbl

[16] A. Lopatin and F. Reimers, "Separating invariants for multisymmetric polynomials", *Proc. Amer. Math. Soc.* **149**:2 (2021), 497–508. MR Zbl

[17] A. Lopatin and A. N. Zubkov, "Classification of G_2-orbits for pairs of octonions", preprint, 2022. arXiv 2208.08122

[18] H. P. Petersson, "Maximal subalgebras of octonions", *J. Pure Appl. Algebra* **217**:9 (2013), 1700–1701. MR Zbl

[19] M. L. Racine, "On maximal subalgebras", *J. Algebra* **30** (1974), 155–180. MR Zbl

[20] G. W. Schwarz, "Invariant theory of G_2 and Spin_7", *Comment. Math. Helv.* **63**:4 (1988), 624–663. MR Zbl

[21] R. J. Sousa Ferreira and A. Lopatin, "Minimal generating and separating sets for $O(3)$-invariants of several matrices", *Oper. Matrices* **17**:3 (2023), 639–651. MR Zbl

[22] T. A. Springer and F. D. Veldkamp, *Octonions, Jordan algebras and exceptional groups*, Springer, 2000. MR Zbl

[23] A. N. Zubkov and I. P. Shestakov, "Invariants of G_2 and $\mathrm{Spin}(7)$ in positive characteristic", *Transform. Groups* **23**:2 (2018), 555–588. MR Zbl

Communicated by Gavril Farkas
Received 2022-08-29 Revised 2023-08-19 Accepted 2023-12-18

dr.artem.lopatin@gmail.com *Departamento de Matemática, Universidade Estadual de Campinas (UNICAMP), Campinas, Brazil*

a.zubkov@yahoo.com *Department of Mathematical Sciences, United Arab Emirates University, Abu Dhabi, United Arab Emirates*

Sobolev Institute of Mathematics, Omsk Branch, Omsk, Russia

Algebra & Number Theory

msp.org/ant

PRODUCTION

production@msp.org

Silvio Levy, Scientific Editor

See inside back cover or msp.org/ant for submission instructions.

The subscription price for 2024 is US $525/year for the electronic version, and $770/year (+$65, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online.

ANT peer review and production are managed by EditFLOW® from MSP.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

Algebra & Number Theory

Volume 18 No. 12 2024