Quasigroups and Related Systems **31** (2023), 185 – 200

https://doi.org/10.56415/qrs.v31.14

On the nonexistence of certain associative subloops in the loop of invertible elements of the split alternative Cayley-Dickson algebra

Evgenii L. Bashkirov

Abstract. Let $O(k)$ be the octonion Cayley–Dickson algebra over a commutative associative ring k with 1. Let $G(k)$ be the Moufang loop of invertible elements of $O(k)$. Let $\mathcal{H}$ be a class of groups such that a group G is a member of $\mathcal{H}$ if and only if G satisfies the following three conditions: (a) G is not class-2 nilpotent. (b) G has a proper class-2 nilpotent subgroup. (c) G is not isomorphic to any subgroup of the group $GL_2(F)$ for any field F. The theorem proved in the paper states that if k is an integral domain with $1+1 \neq 0$, then $G(k)$ does not contain any subloop isomorphic to a group of class $\mathcal{H}$, while if k is an integral domain such that $1+1=0$, then $G(k)$ contains no subloop isomorphic to a class-2 nilpotent group at all.

Let $G(k)$ denote the loop of invertible elements in the split alternative Cayley-Dickson algebra over a field k. If the characteristic of k is not 2, then $G(k)$ has a subloop isomorphic to the group $UT_3(k)$ of all 3×3 upper unitriangular matrices over k ([1]). A natural question arises then, namely, whether $G(k)$ contains a subloop isomorphic to a group which is, in a sense, more larger than $UT_3(k)$. The present paper answers this question, actually, in the negative using as a working tool a class of groups that contain a class-2 nilpotent group as a proper subgroup. More precisely,

Definition. A group G belongs to the class $\mathcal{H}$ if and only if G satisfies the following three conditions:

(a) G is not class-2 nilpotent.

2010 Mathematics Subject Classification: 20N05, 17D05, 20F18
Keywords: Moufang loops, Alternative algebras, Nilponent groups

(b) G has a proper class-2 nilpotent subgroup.

(c) G is not isomorphic to any subgroup of the group $GL_2(F)$ for every field F.

The main purpose of the paper is to prove the following theorem which demonstrates, in particular, a distinction between the case involving fields of characteristic not 2 and that in which fields of characteristic 2 appear.

Theorem 1. *Let k be an associative and commutative integral domain with 1, $O(k)$ the alternative split Cayley-Dickson algebra over k and $G(k)$ a Moufang loop of invertible elements in $O(k)$.*

(*i*) *If $1+1 \neq 0$, then the loop $G(k)$ does not contain any subloop isomorphic to a group of class $\mathcal{H}$.*

(*ii*) *If $1+1=0$, then the loop $G(k)$ contains no subloop isomorphic to a class-2 nilpotent subgroup.*

Before exposing proof of the theorem a notational system will be established.

Let k be a commutative associative ring with 1. Then k^* is the multiplicative group of all invertible elements of k.

If $a \in k$ and $S, T \subseteq k$, then $aS = \{as \mid s \in S\}$ and $S+T = \{s+t \mid s \in S, t \in T\}$.

Let n be an integer, $n \geqslant 2$. Then $M_n(k)$ is the associative ring of $n \times n$ matrices with entries in k. As usual, $GL_n(k)$ denotes the group $M_n(k)^*$, the general linear group of degree n over k.

If 1_n is the identity matrix of degree n and $a \in k$, then $t_{ij}(a)$ denotes the matrix $1_n + ae_{ij}$, where e_{ij} is the $n \times n$ matrix which has 1 in its (i,j) position and zeros elsewhere. If $S \subseteq k$, then $t_{ij}(S) = \{t_{ij}(a) \mid a \in S\}$.

k^3 is the standard free k-module formed by column vectors of length 3 with components in k. The elements

$$\begin{bmatrix}1\\0\\0\end{bmatrix}, \quad \begin{bmatrix}0\\1\\0\end{bmatrix}, \quad \begin{bmatrix}0\\0\\1\end{bmatrix}$$

of k^3 are denoted by e_1, e_2, e_3, respectively. The zero element of k^3 is designated as $\mathbf{0}$.

If $\alpha, \beta \in k^3$, then $\alpha \cdot \beta$ and $\alpha \times \beta$ denote the usual dot product and cross product, respectively.

$O(k)$ is the set of all symbols of the form $\left(\begin{smallmatrix} a & \alpha \\ \beta & b \end{smallmatrix}\right)$ with $a, b \in k, \alpha, \beta \in k^3$. In $O(k)$, equality, addition and multiplication by elements of k are defined componentwise, whereas the operation of multiplication is given by

$$\begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix} \begin{pmatrix} c & \gamma \\ \delta & d \end{pmatrix} = \begin{pmatrix} ac + \alpha \cdot \delta & a\gamma + \alpha d - \beta \times \delta \\ \beta c + b\delta + \alpha \times \gamma & \beta \cdot \gamma + bd \end{pmatrix}, \quad a, b, c, d \in k, \quad \alpha, \beta, \gamma, \delta \in k^3.$$

Under the operations just defined $O(k)$ is an alternative nonassociative k-algebra termed the split Cayley-Dickson algebra (or the octonion one). Elements of $O(k)$ are called octonions.

To avoid a proliferation of symbols, it is convenient to adopt the following convention. The symbol 1_2 is used to denote the identity of the algebra $O(k)$,

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

as well as the identity 2×2 matrix. Also the symbol 0_2 is used to designate two things: the zero octonion

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

and the zero 2×2 matrix. The convention should lead to no ambiguity if one attends closely to the context in which the notation is employed.

The trace $\operatorname{tr}(x)$ and the norm $n(x)$ of the octonion

$$x = \begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix} \in O(k)$$

are defined to be $a + b$ and $ab - \alpha \cdot \beta$, respectively.

$G(k)$ is the (Moufang) loop of octonions of $O(k)$ whose norms lie in k^*. The norm n determines the bilinear form $(x, y) = n(x+y) - n(x) - n(y)$ on the k-module $O(k)$. Throughout the article, all metric concepts mentioned are related to the bilinear form (x, y) determined by the norm mapping $n\colon O(k) \to k$. In particular, if $Y \subseteq O(k)$, then the orthogonal complement $Y^\perp$ is defined to be the set $\{x \in O(k) \mid (x, y) = 0 \text{ for all } y \in Y\}$.

The algebra $O(k)$ admits an involution $^-\colon O(k) \to O(k)$ given by

$$\bar{x} = \begin{pmatrix} b & -\alpha \\ -\beta & a \end{pmatrix}, \text{ whenever } x = \begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix} \qquad a, b \in k, \quad \alpha, \beta \in k^3.$$

Borrowing the notation from the theory of algebraic groups, the automorphism group of the algebra $O(k)$ is denoted by $G_2(k)$.

Let $UT(k)$ and $ZUT(k)$ be the subloops of $G(k)$ defined by

$$UT(k) = \left\{ \begin{pmatrix} 1 & a_2e_1 \\ a_3e_2 + a_4e_3 & 1 \end{pmatrix} \,\middle|\, a_i \in k \right\},$$
$$ZUT(k) = \left\{ \begin{pmatrix} a_1 & a_2e_1 \\ a_3e_2 + a_4e_3 & a_1 \end{pmatrix} \,\middle|\, a_1 \in k^*, a_2, a_3, a_4 \in k \right\},$$

and let $N_0(k)$ and $N(k)$ be the subgroups of $GL_3(k)$ such that

$$N_0(k) = \left\{ \begin{pmatrix} r & 2a & b \\ 0 & r & c \\ 0 & 0 & r \end{pmatrix} \,\middle|\, r \in k^*, a, b, c \in k \right\},$$
$$N(k) = \left\{ \begin{pmatrix} 1 & 2a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \,\middle|\, a, b, c \in k \right\}.$$

A direct calculation shows that the restriction of multiplication in $O(k)$ to $ZUT(k)$ is associative, and since $UT(k) \subseteq ZUT(k)$, this is true also for $UT(k)$. Moreover, the mapping $\eta\colon ZUT(k) \to N_0(k)$ defined by

$$\begin{pmatrix} a_1 & a_2e_1 \\ a_3e_2 + a_4e_3 & a_1 \end{pmatrix} \mapsto \begin{pmatrix} a_1 & 2a_3 & a_3a_4a_1^{-1} - a_2 \\ 0 & a_1 & a_4 \\ 0 & 0 & a_1 \end{pmatrix},$$

satisfies for all $x, y \in ZUT(k)$ the condition $(xy)^\eta = x^\eta y^\eta$, where the multiplication on the right-hand side is performed in the group $GL_3(k)$. This means that η is a group homomorphism from $ZUT(k)$ onto $N_0(k)$. The kernel of η is isomorphic to the subgroup $k[2]$ of the additive group of k formed by all $a \in k$ with $2a = 0$. Thus $N_0(k)$ is isomorphic to the quotient $ZUT(k)/k[2]$ and the restriction of η to $UT(k)$ determines an isomorphism of $UT(k)/k[2]$ onto $N(k)$. If $2 \in k^*$, then $k[2] = 0, 2k = k$, and hence $ZUT(k)$ is isomorphic to the direct product $k^* \times UT_3(k)$ of the groups k^* and $UT_3(k)$, whereas $UT(k) \cong UT_3(k)$.

If X is a group and $x, x_1 \in X$, then $x_1^x = x^{-1}x_1x$, ${}^x x_1 = xx_1x^{-1}$, $[x_1, x] = x_1^{-1}x_1^x$. If $R \subseteq X$, then ${}^x R = \{ {}^x r \mid r \in R\}$.

If X is a loop and M is a subset of X, then $\langle M \rangle$ denotes the subloop of X generated by M.

A series of auxiliary results must be established before giving a direct proof of Theorem 1. The first of these is concerned with the following situation related to general alternative algebras.

Let k be a field of characteristic $\neq 2$ and L an alternative k-algebra with 1. Choose $a_1, a_2, a \in k$ and suppose that L contains elements y_1, y_2 such that

$$y_1^2 = a_1, \quad y_2^2 = a_2, \quad y_1y_2 + y_2y_1 = a. \tag{1}$$

It is straightforward to check that the subspace $A = k + ky_1 + ky_2 + ky_1y_2$ of the k-vector space L is a subalgebra of L which is denoted as

$$\Big(\frac{a_1, a_2, a}{k}, y_1, y_2\Big). \tag{2}$$

A description of noncommutative algebras (2) is a constituent of the proof of Theorem 1. Certainly, some parts of this description can be extracted from the usual classification of quaternion algebras exposed, for example, in [2], pp. 13–20. However, the full list of subalgebras (2) can not be given within the framework of [2] (mainly, due to the fact that the case $a_1a_2 = a = 0$ is excluded in [2]). Therefore, it is desirable to have, at least as a sketch, an argument leading to a full description of subalgebras (2). This is done in Lemma 1 below. The proof of that lemma requires, in turn, the following notations in which some algebras of 2×2 matrices appear.

If x_0, x_1, x_2 are indeterminates and $b, c \in k$ are such that the quadratic form $x_0^2 - x_1^2 b - x_2^2 c$ does not represent zero in k, then

$$D(b,c,k) = \left\{ \begin{pmatrix} r_0 + r_1\sqrt{b} & r_2 + r_3\sqrt{b} \\ c(r_2 - r_3\sqrt{b}) & r_0 - r_1\sqrt{b} \end{pmatrix} \,\middle|\, r_i \in k \right\}.$$

In other words, $D(b,c,k)$ is the quaternion division algebra $\left(\frac{b,c}{k}\right)$ realized by matrices of degree 2 over the field $k(\sqrt{b})$.

If $b \in k$ is not a square in the field k, then

$$T_0(k(\sqrt{b})) = \left\{ \begin{pmatrix} r_0 + r_1\sqrt{b} & r_2 + r_3\sqrt{b} \\ 0 & r_0 - r_1\sqrt{b} \end{pmatrix} \,\middle|\, r_i \in k \right\}.$$

Finally, $T(k)$ denotes the k-algebra of 2×2 upper triangular matrices over k:

$$T(k) = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \,\middle|\, a, b, c \in k \right\}.$$

Now the above mentioned description runs as follows.

Lemma 1. *Let k be a field of characteristic not 2, L an alternative algebra over k with 1, and $a_1, a_2, a \in k$. Suppose that L contains elements y_1, y_2 satisfying* (1) *and let A be the subalgebra of L defined by* (2). *Suppose that A is noncommutative. Then one of the following holds:*

(*i*) $A \cong M_2(k)$.

(*ii*) $A \cong D(b, c, k)$, *where the quadratic form $x_0^2 - x_1^2 b - x_2^2 c$ in x_0, x_1, x_2 does not represent 0 in k.*

(*iii*) $A \cong T_0(k(\sqrt{b}))$, *where b is not a square in k.*

(*iv*) $A \cong T(k)$.

(*v*) $\dim_k A = 4$ *and* $A \cong \left(\frac{1,0,0}{k}, z_1, z_2\right)$ *for some $z_1, z_2 \in L$.*

(*vi*) $A \cong \left(\frac{0,0,0}{k}, z_1, z_2\right)$ *for some $z_1, z_2 \in L$.*

Proof. Part one. Consider first the case $a = 0$. There are the following three possibilities for a_1:

(a) a_1 is not a square in k,

(b) a_1 is a nonzero square in k,

(c) $a_1 = 0$.

The corresponding possibilities exist for a_2 and exchanging, if necessary, y_1 and y_2, one obtains the following six possibilities for the ordered pair (a_1, a_2):

(1) Both a_1, a_2 are not squares in k.

(2) a_1 is not a square in k, a_2 is a nonzero square in k.

(3) a_1 is not a square in k, $a_2 = 0$.

(4) Both a_1, a_2 are nonzero squares in k.

(5) a_1 is a nonzero square in k, $a_2 = 0$.

(6) $a_1 = a_2 = 0$.

These cases are considered separately.

(1) Here $\dim_k A = 4$ and A is a quaternion algebra in the sense of [2], p. 14. So A is either a division algebra and $A \cong D(a_1, a_2, k)$ or $A \cong M_2(k)$.
(2) Again A is a quaternion algebra, and since a_2 is a square in k^*, $A \cong M_2(k)$.
(3) In this case, $\dim_k A = 4$ and $A \cong T_0(k(\sqrt{a_1}))$.
(4) Here again A is a quaternion algebra, A being isomorphic to $M_2(k)$.
(5) In this case, the following two possibilities arise for the dimension of A over k: this dimension is equal either to 3 or to 4. If $\dim_k A = 3$, then $A \cong T(k)$. If $\dim_k A = 4$, then setting $z_1 = y_1 b_1^{-1}$, where $a_1 = b_1^2, b_1 \in k$, and $z_2 = y_2$, one obtains $A \cong \left(\frac{1,0,0}{k}, z_1, z_2\right)$.
(6) Here A corresponds to the algebra listed in (vi).

Part two. Now consider the case $a \neq 0$. If, under this assumption, $a_1 = a_2 = 0$, then $\dim_k A = 4$ and the correspondence $y_1 \mapsto \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right), y_2 \mapsto \left(\begin{smallmatrix} 0 & 0 \\ a & 0 \end{smallmatrix}\right)$ determines an isomorphism of A upon $M_2(k)$. If $(a_1, a_2) \neq (0, 0)$, then exchanging, if necessary, y_1 and y_2, one may suppose that $a_1 \neq 0$ and

$$A = \left(\frac{a_1, a_1(-1 + 4a_1 a_2 a^{-2}), 0}{k}, y_1, y_1 - 2a_1 a^{-1} y_2\right).$$

In particular, if $a_2 = 0$, then $A \cong M_2(k)$. If both a_1, a_2 are nonzero, then A is as in $(i) - (v)$ by part one of the proof. The lemma is proved. □

The next lemma adjusts Suprunenko's results on class-2 nilpotent linear groups over algebraically closed fields (see, [5], pp.210, 211) to the situation of fields which are not necessarily algebraically closed. For the needs of Theorem 1 proof, the case of linear groups of degree 2 is considered only.

Lemma 2. *Let k be a field of characteristic $\neq 2$ and X a class-2 nilpotent subgroup of $GL_2(k)$. Then*

$$X = B1_2 \cup Bx_1 \cup Bx_2 \cup Bx_1x_2,$$

where $B \leqslant k^*$ with $-1 \in B$, and $x_1, x_2 \in GL_2(k)$ are such that $x_1^2, x_2^2 \in B1_2$ and $x_2x_1 = -x_1x_2$.

Proof. Let Ω be an algebraic closure of k. For every field F, the group $GL_2(F)$ does not possess any reducible class-2 nilpotent subgroup. Therefore X, being a class-2 nilpotent subgroup of $GL_2(\Omega)$, is an irreducible subgroup of $GL_2(\Omega)$. If M is a maximal irreducible class-2 nilpotent subgroup of $GL_2(\Omega)$ with $M \geqslant X$, then according to Theorem 7 [5], pp. 210, 211, M is conjugate by an element $q \in GL_2(\Omega)$ to the group Γ formed by all elements $\lambda a_1^{\alpha_1} a_2^{\alpha_2}$, where $\lambda \in \Omega^*, \alpha_1, \alpha_2$ integers, and

$$a_1 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad a_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

In other words, $\Gamma = \Omega_0 \cup \Omega_1 \cup \Omega_2 \cup \Omega_3$, where $\Omega_0 = \Omega^* 1_2$, $\Omega_i = \Omega^* a_i$ $(i = 1, 2)$, $\Omega_3 = \Omega^* a_1 a_2$. Choose not permutable $x_1, x_2 \in X$ and let $q_i = x_i^q (i = 1, 2)$. Then neither q_1 nor q_2 can lie in Ω_0 and also q_1, q_2 can not belong to one and the same set Ω_i with $i \in \{1, 2, 3\}$. Interchanging, if necessary, x_1 and x_2 and replacing (again if necessary) the ordered pair x_1, x_2 either by that of $x_1, x_1 x_2$ or by $x_1 x_2, x_1$, one may assume that $q_1 \in \Omega_1, q_2 \in \Omega_2$. So

$$q_1 = \begin{pmatrix} \omega_1 & 0 \\ 0 & -\omega_1 \end{pmatrix}, \quad q_2 = \begin{pmatrix} 0 & \omega_2 \\ \omega_2 & 0 \end{pmatrix}$$

for some $\omega_1, \omega_2 \in \Omega$. Denote X^q by C. Put then

$$B_0 = \{b \in \Omega^* \mid b1_2 \in C\}, \quad B_1 = \{b \in \Omega^* \mid bq_1 \in C\},$$
$$B_2 = \{b \in \Omega^* \mid bq_2 \in C\}, \quad B_3 = \{b \in \Omega^* \mid bq_1 q_2 \in C\},$$

and let U be the union $B_0 1_2 \cup B_1 q_1 \cup B_2 q_2 \cup B_3 q_1 q_2$. Clearly $U \subseteq C$. The definition of B_0 implies that $B_0 \leqslant \Omega^*$. Squaring q_1, q_2 and $q_1 q_2$, one gets that ω_1^2, ω_2^2 and -1 are in B_0. Observe also that all B_i contain 1. Therefore, since $B_0 B_i \subseteq B_i (i = 1, 2, 3)$, $B_0 \subseteq B_i$. On the other hand, $B_i B_i \subseteq B_0$ and again the relation $1 \in B_i$ shows that $B_i \subseteq B_0$ giving then $B_i = B_0 (i = 1, 2, 3)$. Denoting the common value of B_i by B, one has

$$U = B1_2 \cup Bq_1 \cup Bq_2 \cup Bq_1 q_2.$$

Now let h be an element of C. Writing

$$h = \begin{pmatrix} x & y \\ z & t \end{pmatrix}, \quad x, y, z, t \in \Omega,$$

and denoting $[q_1, h] = q_1^{-1} h^{-1} q_1 h$ by q_3, one has

$$q_3 = (\det h)^{-1} \begin{pmatrix} tx + yz & 2ty \\ 2xz & tx + yz \end{pmatrix}.$$

Since q_3 commutes with q_1 which is diagonal but not scalar, q_3 must be diagonal itself. It follows that $ty = xz = 0$ because char $k \neq 2$. If $x \neq 0$, then

$$h = \begin{pmatrix} x & 0 \\ 0 & t \end{pmatrix}.$$

Since $[q_2, h]$ commutes with q_2, one obtains $t = \pm x$. If $t = x$, then $h = x1_2$, and $h \in B1_2 \subseteq U$. If $t = -x$, then $hq_1 = x\omega_1 1_2 \in C$, so $x\omega_1 = b_0 \in B$. Thus $h = q_1 b_0 \omega_1^{-2} \in q_1 B \subseteq U$. Next let $x = 0$ and so

$$h = \begin{pmatrix} 0 & y \\ z & 0 \end{pmatrix}.$$

Since C contains the diagonal matrix

$$hq_2 = \begin{pmatrix} y\omega_2 & 0 \\ 0 & z\omega_2 \end{pmatrix},$$

$z = \pm y$. If $z = y$, then $hq_2 = y\omega_2 1_2$ and hence $y = z = b_1\omega_2^{-1}$ with $b_1 \in B$. This shows $h = q_2 b_1 \omega_2^{-2} \in q_2 B \subseteq U$. If $z = -y$, then $hq_2q_1 = y\omega_2\omega_1 1_2$, whence $y = b_2\omega_1^{-1}\omega_2^{-1}$ with $b_2 \in B$ and $h = q_1q_2b_2\omega_1^{-2}\omega_2^{-2} \in q_1q_2B \subseteq U$. Thus $h \in U$ in any case and consequently $C = U$. It follows that $X = B1_2 \cup Bx_1 \cup Bx_2 \cup Bx_1x_2$. But $X \leqslant GL_2(k)$, so $B \leqslant k^*$. Also $x_i^2 = ({}^{q}q_i)^2 = {}^{q}(q_i^2) = \omega_i^2 1_2$, that is, $x_i^2 \in B1_2 (i = 1, 2)$. Finally, $x_1x_2 + x_2x_1 = q(q_1q_2 + q_2q_1)q^{-1} = 0_2$ which completes the proof of the lemma. □

The following assertion has a technical character and is used in the subsequent description of subloops of $G(k)$ that are isomorphic to class-2 nilpotent groups.

Lemma 3. *Let*

$$x_1 = \begin{pmatrix} r & \mathbf{0} \\ \mathbf{0} & s \end{pmatrix}, \quad x_2 = \begin{pmatrix} u & \rho \\ \pi & v \end{pmatrix}$$

be elements of $G(k)$ such that $\rho \cdot \pi = 0$ with both ρ and π nonzero. If x_1 and x_2 are not permutable, then $[x_1, x_2]$ does not commute with x_1.

Proof. A straightforward calculation gives

$$[x_1, x_2] = \begin{pmatrix} 1 & e\rho \\ f\pi & 1 \end{pmatrix}$$

with $e = u^{-1}(1 - sr^{-1}), f = v^{-1}(1 - rs^{-1})$. If this commutes with x_1, then $es\rho = er\rho$ and $fr\pi = fs\pi$. Since ρ and π are both nonzero, $es = er, fr = fs$. But either $e \neq 0$ or $f \neq 0$ for $[x_1, x_2] \neq 1_2$. Therefore, $r = s$, hence x_1 commutes with x_2 which is impossible. □

Now the description of subloops of $G(k)$ that are isomorphic to class-2 nilpotent groups can be given for fields k of characteristic $\neq 2$.

Lemma 4. *Let k be a field of characteristic $\neq 2$ and $X \leqslant G(k)$. Suppose that X is isomorphic to a class-2 nilpotent group. Then one of the following holds:*

(i) *X is isomorphic to a subgroup of $GL_2(k_1)$ where either $k_1 = k$ or k_1 is a quadratic field extension of k.*

(ii) *There is $\psi \in G_2(k)$ such that $X^\psi \leqslant ZUT(k)$.*

Proof. Choose not permutable $x_1, x_2 \in X$. Since $x_i \in O(k)$, $x_i^2 = x_i t_i + n_i 1_2$ for some $t_i \in k$ and $n_i \in k^*$. As char $k \neq 2$, one can put $y_i = x_i - 2^{-1} t_i 1_2$, $a_i = 4^{-1} t_i^2 + n_i$ so that $y_i^2 = a_i 1_2$. This implies $\bar{y}_i = -y_i$ and $y_1 y_2 + y_2 y_1 = a 1_2$ with $a \in k$. Let $A = k1_2 + ky_1 + ky_2 + ky_1 y_2$. By Lemma 1, one of Possibilities (i) – (vi) listed in that lemma can arise for A.

Suppose first that Possibility (iv) arises. Then there is a ring isomorphism $\chi_0 \colon (A, +, \cdot) \to (T(k), +, \cdot)$. Considering A and $T(k)$ as semigroups (under corresponding multiplications), one obtains a semigroup isomorphism $\tilde{\chi}_0 \colon (A, \cdot) \to (T(k), \cdot)$. Restricting $\tilde{\chi}_0$ on A^*, the set of invertible elements of A, one has a group homomorphism χ of $(A^*, \cdot)$ into the group of all 2×2 invertible upper triangular matrices over k. Due to the equation $x_i = y_i + 2^{-1} t_i 1_2$ and since $k1_2 \subseteq A$, both x_1 and x_2 are in A. Hence $\langle x_1, x_2 \rangle^\chi$ is a reducible class-2 nilpotent subgroup of $GL_2(k)$ which is false. Thus Possibility (iv) is in fact impossible. A similar argument shows that Possibility (iii) from Lemma 1 also can not arise.

Now suppose that Possibility (v) from Lemma 1 takes place for A. Assume first that $a \neq 0$. Then if (v) takes place, one may suppose without loss of generality that $a_1 = b_1^2, b_1 \in k^*$ and $(y_1 - 2a_1 a^{-1} y_2)^2 = 0_2$. So replacing X by X^φ with a suitable $\varphi \in G_2(k)$, one may suppose that

$$y_1 = \begin{pmatrix} b_1 & \mathbf{0} \\ \mathbf{0} & -b_1 \end{pmatrix}.$$

Putting then

$$y_1 - 2a_1a^{-1}y_2 = \begin{pmatrix} c & \gamma \\ \delta & d \end{pmatrix}, \quad c, d \in k, \quad \gamma, \delta \in k^3,$$

one has $c = d = 0$ in view of the equation $y_1(y_1 - 2a_1a^{-1}y_2) + (y_1 - 2a_1a^{-1}y_2)y_1 = 0_2$. The condition $(y_1 - 2a_1a^{-1}y_2)^2 = 0_2$ gives $\gamma \cdot \delta = 0$, where γ and δ are both nonzero because $\dim_k A = 4$. It follows that

$$y_2 = \left[y_1 - (y_1 - 2a_1a^{-1}y_2)\right] \frac{a}{2a_1} = \begin{pmatrix} \frac{a}{2b_1} & -\gamma\frac{a}{2b_1^2} \\ -\delta\frac{a}{2b_1^2} & -\frac{a}{2b_1} \end{pmatrix}.$$

Therefore,

$$x_1 = y_1 + \frac{t_1}{2}1_2 = \begin{pmatrix} r & \mathbf{0} \\ \mathbf{0} & s \end{pmatrix},$$

where $r = b_1 + 2^{-1}t_1, s = -b_1 + 2^{-1}t_1$, and

$$x_2 = y_2 + \frac{t_2}{2}1_2 = \begin{pmatrix} u & \rho \\ \pi & v \end{pmatrix},$$

for some $u, v \in k$ and $\rho = -2^{-1}\gamma ab_1^{-2}, \pi = -2^{-1}\delta ab_1^{-2}$. Now observe that both γ and δ are nonzero because $\dim_k A = 4$. So $\rho \neq 0, \pi \neq 0$ and applying Lemma 3 one obtains a contradiction. A similar argument leads to a contradiction when $a = 0$, so Possibility (v) is impossible at all.

Suppose Case (ii) takes place. This means that A is isomorphic to a quaternion division k-algebra $(\frac{b,c}{k})$. In particular, the subalgebra A contains 1_2, and the restriction of the bilinear form $(,)$ to A is nondegenerate. Thus the subspace $A^{\perp}$ is nondegenerate too and hence it contains v with $n(v) \neq 0$ so that $O(k) = A \oplus vA$. Now let x be an arbitrary element of X. Then $x = a + vb$ with $a, b \in A$ and $(xx_1)x_2 = x(x_1x_2)$. But $(xx_1)x_2 = ax_1x_2 + v(x_2x_1b)$ and $x(x_1x_2) = ax_1x_2 + v(x_1x_2b)$ (see, [3], p. 26), whence it follows that $v(x_2x_1b) = v(x_1x_2b)$, and since v is invertible, $x_2x_1b = x_1x_2b$. Note that x_1 and x_2 are not permutable elements of the class-2 nilpotent group $\langle x_1, x_2\rangle$. According to Lemma 2, x_1 and x_2 must anticommute. So $-x_1x_2b = x_1x_2b$, and since x_1x_2 is invertible and char $k \neq 2$, one gets $b = 0$, hence $x \in A$. Thus $X \subseteq A$, that is, X is isomorphic to a subgroup of $GL_2(k(\sqrt{b}))$. In a similar fashion, one can show that X is isomorphic to a subgroup of $GL_2(k)$ if Case (i) of Lemma 1 takes place.

It remains to consider the situation when A is as in Possibility (vi) of Lemma 1. Using the terminology of [1], this can be expressed by saying that y_1 and y_2 form a half extra-special pair. According to Lemma 5.3 [1], there is $\psi \in G_2(k)$ such that

$$x_1^\psi = \begin{pmatrix} r_1 & \mathbf{0} \\ e_2 & r_1 \end{pmatrix}, \quad x_2^\psi = \begin{pmatrix} r_2 & \mathbf{0} \\ e_3 & r_2 \end{pmatrix}, \quad r_i = \frac{t_i}{2}.$$

Now let

$$x^\psi = \begin{pmatrix} f & \gamma \\ \delta & d \end{pmatrix}, \quad f, d \in k, \quad \gamma, \delta \in k^3$$

be an element of X^ψ. Then $(x_1^\psi x_2^\psi)x^\psi = x_1^\psi(x_2^\psi x^\psi)$ which leads to the equality

$$\begin{pmatrix} r_1r_2f - e_1 \cdot \delta & r_1r_2\gamma - e_1d - (e_2r_2 + e_3r_1) \times \delta \\ (e_2r_2 + e_3r_1)f + \delta r_1r_2 - e_1 \times \gamma & * \end{pmatrix}$$
$$= \begin{pmatrix} r_1r_2f & r_1(r_2\gamma - e_3 \times \delta) - e_2 \times (e_3f + \delta r_2) \\ e_2r_2f + r_1(e_3f + \delta r_2) & * \end{pmatrix}. \tag{3}$$

Comparing the corresponding entries in the position (11) shows that $e_1 \cdot \delta = 0$. This means exactly that $\delta \in e_2k + e_3k$. Further, comparing the vectors in the position (12) leads to the equality $d = f$. Finally, comparing vectors in the position (21) yields $e_1 \times \gamma = \mathbf{0}$ which means that $\gamma \in ke_1$. Collecting all this information, one concludes $x^\psi \in ZUT(k)$ which completes the proof of the lemma. □

After all these preparations, Part (i) of Theorem 1 can be proved. This will be done as the demonstration of the following proposition.

Proposition 1. *Let k be an associative and commutative integral domain with* 1. *If* $1+1 \neq 0$, *then the loop $G(k)$ does not have any subloop isomorphic to a group of class $\mathcal{H}$.*

Proof. The ring k can be considered as a subring of a field which, due to the condition $1 + 1 \neq 0$, must have characteristic $\neq 2$. So from the very beginning one can assume that k is a field and char $k \neq 2$. Suppose that $G(k)$ has a subloop G isomorphic to a group of class $\mathcal{H}$. By Item (b) in Definition, G contains a proper subloop X isomorphic to a class-2 nilpotent subgroup. By Lemma 4, X is either isomorphic to a subgroup of the group $GL_2(k_1)$, where k_1 is a field extension of k with $[k_1 : k] \leqslant 2$ or there is $\psi \in G_2(k)$ such that $X^\psi \leqslant ZUT(k)$.

Suppose that X is isomorphic to a subgroup of $GL_2(k_1)$. Consider the k_1-algebra $O(k_1) = O(k) \otimes_k k_1$. One has $X \leqslant G \leqslant G(k) \leqslant G(k_1)$, and following the line of Lemma 4 proof, namely, those places of the proof which address Possibilities (i) and (ii) of Lemma 1, it is readily seen that X is a subset of the subalgebra A' of $O(k_1)$ such that A' is isomorphic to $M_2(k_1)$. So there is $\varphi \in G_2(k_1)$ with $X^\varphi \leqslant G_{[1]}(k_1)$, where

$$G_{[1]}(k_1) = \left\{ \begin{pmatrix} a & be_1 \\ ce_1 & d \end{pmatrix} \,\middle|\, a, b, c, d \in k_1, ad - bc \neq 0 \right\}$$

([4], p. 17, Corollary 1.7). Using again the proof of Lemma 4, one can deduce that $G \leqslant G_{[1]}(k_1)$, that is, that G is isomorphic to a subgroup of $GL_2(k_1)$. But this contradicts Item (c) in Definition. Hence $X^\psi \leqslant ZUT(k)$ for some $\psi \in G_2(k)$, and the argument employing equation (3) shows that $G^\psi \leqslant ZUT(k)$. Therefore, G is isomorphic to a class-2 nilpotent group which contradicts Item (a) in Definition. This final contradiction proves the proposition completely. □

Now an example that illustrates the result just proved will be given.

Example 1. Let $\mathbb{Q}$ be the field of all rational numbers, and B the subset of $\mathbb{Q}$ consisted of all numbers $\pm 11^n, n \in \mathbb{Z}$. Let θ be a root of the polynomial $\lambda^2 + 11 \in \mathbb{Q}[\lambda]$. Clearly B is a subgroup of $\mathbb{Q}(\theta)^*$. Let

$$h_1 = \begin{pmatrix} \theta & 0 \\ 0 & -\theta \end{pmatrix}, \quad h_2 = \begin{pmatrix} 0 & \theta \\ \theta & 0 \end{pmatrix}.$$

Then $H = B1_2 \cup Bh_1 \cup Bh_2 \cup Bh_1h_2$ is a class-2 nilpotent subgroup of $GL_2(\mathbb{Q}(\theta))$. Though H is not isomorphic to any subgroup of $GL_2(\mathbb{Q})$, H can be realized as a subloop of $G(\mathbb{Q})$. Indeed, if

$$x_1 = \begin{pmatrix} 1 & e_1 + 3e_2 + 2e_3 \\ e_1 - 3e_2 - 2e_3 & -1 \end{pmatrix}, \quad x_2 = \begin{pmatrix} 0 & e_1 \\ -e_1 & 0 \end{pmatrix},$$

and $X = \langle x_1, x_2 \rangle$, then the correspondence $x_1 \mapsto h_1, x_2 \mapsto (-11)^{-1}h_1h_2$ and $b \mapsto b$ for every $b \in B$, determines an isomorphism of X onto H. The subalgebra $A_0 = \mathbb{Q}1_2 + \mathbb{Q}x_1 + \mathbb{Q}x_2 + \mathbb{Q}x_1x_2$ of $O(\mathbb{Q})$ is isomorphic to the quaternion division algebra $\left(\frac{-11,-1}{\mathbb{Q}}\right)$ and is of the type $\left(\frac{-11,-1,0}{\mathbb{Q}}, x_1, x_2\right)$. One has $A_0 \otimes_{\mathbb{Q}} \mathbb{Q}(\theta) \cong M_2(\mathbb{Q}(\theta))$. By [4], Corollary 1.7 on p. 17, there is an automorphism φ of the algebra $O(\mathbb{Q}(\theta)) \cong O(\mathbb{Q}) \otimes_{\mathbb{Q}} \mathbb{Q}(\theta)$ such that $X^\varphi \leqslant G_{[1]}(\mathbb{Q}(\theta))$.

The following situation can serve as an application of Proposition 1.

Let R be an associative and commutative ring with 1 and let $EAff_{2+1}(R)$ denote the subgroup of $GL_3(R)$ generated by the set $t_{12}(R) \cup t_{21}(R) \cup t_{13}(1)$. It is claimed that $EAff_{2+1}(R)$ is a group of class $\mathcal{H}$.

The center of $EAff_{2+1}(R)$ is trivial. Therefore, Item (a) of Definition is satisfied. Since $UT_3(R) \leqslant EAff_{2+1}(R)$, Item (b) in Definition also holds. Now suppose that there exists a field F such that $EAff_{2+1}(R)$ is isomorphic to subgroup H of $GL_2(F)$. Then $GL_2(F)$ must have a subgroup H_0 isomorphic to $UT_3(R)$. In particular, H_0 is class-2 nilpotent. If Ω is an algebraic closure of F, then H_0, being a class-2 nilpotent subgroup of $GL_2(\Omega)$, is an irreducible subgroup of $GL_2(\Omega)$. Therefore, by Corollary 2 [5], p. 209, char $\Omega \neq 2$, hence char $F \neq 2$ too. By Lemma 2, H_0 contains the matrix -1_2 which commutes with all elements of $GL_2(F)$, in particular, with all elements of H. Since char $F \neq 2$, $-1_2 \neq 1_2$ which means that the center of H is nontrivial. This contradiction shows that Item (c) in Definition holds, and consequently $EAff_{2+1}(R) \in \mathcal{H}$. Now Proposition 1 shows that the following assertion is valid.

Corollary 1. *Let k and R be associative and commutative rings with identities, the identity of k being designated by* 1. *Suppose that k is an integral domain and that $1+1 \neq 0$. Then the loop $G(k)$ does not contain any subloop isomorphic to the group $EAff_{2+1}(R)$.*

Note that it is this corollary that has been the initial point for writing the present paper.

The proof of Part (*ii*) of Theorem 1 is given as the proof of the following proposition.

Proposition 2. *Let k be an associative and commutative integral domain with* 1. *Suppose that $1+1=0$. Then $G(k)$ contains no subloop isomorphic to a class-*2 *nilpotent group.*

Proof. One may assume that k is a field of characteristic 2. Suppose that $G(k)$ has a subloop G which is isomorphic to a class-2 nilpotent group. Then G contains not permutable elements g_1, g_2 such that both of them commutes with their group commutator $[g_1, g_2]$ or, which is equivalent, with $\bar{g}_1\bar{g}_2g_1g_2$. Note that to satisfy the latter condition each g_i can be replaced by any of its scalar multiples. So if $\mathrm{tr}(g_i) \neq 0$, one may assume that $\mathrm{tr}(g_i) = 1$. Thus interchanging, if necessary, g_1 and g_2, there are three cases to consider each to be handled separately.

(i) $\mathrm{tr}(g_1) = \mathrm{tr}(g_2) = 1$.

(ii) $\mathrm{tr}(g_1) = 1, \mathrm{tr}(g_2) = 0$.

(iii) $\mathrm{tr}(g_1) = \mathrm{tr}(g_2) = 0$.

Case (i). Here $g_i^2 = g_i + r_i 1_2$ for some $r_i \in k^*$ and $\bar{g}_i = 1_2 + g_i (i = 1, 2)$. Therefore,

$$\bar{g}_1 \bar{g}_2 g_1 g_2 = r_1 g_2 + g_2 g_1 g_2 + g_1 g_2 g_1 g_2. \tag{4}$$

Denoting by r the trace of the product $g_1 g_2$, one obtains

$$g_2 g_1 = (r + 1)1_2 + g_1 + g_2 + g_1 g_2.$$

So

$$g_2 g_1 g_2 = r g_2 + r_2 g_1 + r_2 1_2, \tag{5}$$

hence

$$g_1 g_2 g_1 g_2 = r g_1 g_2 + r_1 r_2 1_2. \tag{6}$$

Substituting (5) and (6) into (4), one gets

$$\bar{g}_1 \bar{g}_2 g_1 g_2 = r_1 g_2 + r g_2 + r_2 g_1 + r_2 1_2 + r g_1 g_2 + r_1 r_2 1_2.$$

Since g_2 commutes with $\bar{g}_1 \bar{g}_2 g_1 g_2$,

$$g_2 g_1 (r_2 1_2 + r g_2) = g_1 (r_2 1_2 + r g_2) g_2 = g_1 g_2 (r_2 1_2 + r g_2).$$

This shows that if $r_2 1_2 + r g_2$ were invertible, then g_2 would commute with g_1 which is impossible. Thus $n(r_2 1_2 + r g_2) = 0$ whence it follows that $r^2 + r + r_2 = 0$. Observe further that the roles of g_1 and g_2 are completely symmetric which implies that $r^2 + r + r_1 = 0$, and so $r_1 = r_2 = r^2 + r$. It follows that if $h_i = g_i + r 1_2 (i = 1, 2)$, then h_i is an idempotent of $O(k)$. Therefore, if $h_3 = (r + 1)1_2 + h_1 + h_2$, then $h_3 \in (k 1_2 + k h_1)^{\perp}$ and the subalgebra $A = k 1_2 + k h_1 + h_3 (k 1_2 + k h_1)$ of $O(k)$ is isomorphic to the associative algebra $M_2(k)$ (see, [6], pp. 43–45). Since $g_1, g_2 \in A$, the subloop $\langle g_1, g_2 \rangle$ of G is isomorphic to a class-2 nilpotent subgroup of $GL_2(k)$. According to [5], Corollary 2, p. 209, this is false. So Case (i) is impossible.

Case (ii). Here $\bar{g}_1 = 1_2 + g_1, \bar{g}_2 = g_2, g_1^2 = g_1 + r_1 1_2, g_2^2 = r_2 1_2, r_1, r_2 \in k^*$. Following the line of the consideration in the previous case, one obtains

$$\bar{g}_1 \bar{g}_2 g_1 g_2 = r g_2 + g_1 r_2 + r_2 1_2 + r g_1 g_2 + r_1 r_2 1_2,$$

where r is the trace of g_1g_2. Since g_2 commutes with $\bar{g}_1\bar{g}_2g_1g_2$, $g_2(g_1r_2 + rg_1g_2) = (g_1r_2 + rg_1g_2)g_2$, whence $r_2 = r^2$, and in particular $r \neq 0$. This, together with the fact that g_1 and $\bar{g}_1\bar{g}_2g_1g_2$ commute, implies $g_1(g_2+g_1g_2) = (g_2+g_1g_2)g_1$ which can be written as $(1_2+g_1)g_1g_2 = (1_2+g_1)g_2g_1$. It follows that $n(1_2 + g_1) = 0$, or $(1_2 + g_1)(1_2 + g_1 + 1_2) = (1_2 + g_1)g_1 = 0_2$. But $g_1 \in G(k)$, and so $g_1 = 1_2$ which is false. So Case (ii) is impossible.

Case (iii). Here $g_i^2 = r_i1_2$ with $r_i \in k^*$ and $\bar{g}_i = g_i(i = 1, 2)$. The condition that g_1 commutes with $\bar{g}_1\bar{g}_2g_1g_2 = g_1g_2g_1g_2$ leads to the equation

$$r_1g_2g_1g_2 = g_1g_2g_1g_2g_1. \tag{7}$$

Denoting the trace of g_1g_2 by r, one has $g_2g_1g_2 = rg_2 + g_1r_2, g_1g_2g_1g_2g_1 = r^2g_1+rr_1g_2+r_1r_2g_1$. Then (7) becomes $r_1(rg_2+g_1r_2) = r^2g_1+rr_1g_2+r_1r_2g_1$, whence $r^2g_1 = 0_2$ which is false. Case (iii) is impossible. This completes the proof of the proposition. □

Corollary 2. *Let k and R be associative commutative rings with identity elements. Suppose that 1 is the identity of k and that $1 + 1 = 0$. Suppose also that k is an integral domain. Then the loop $G(k)$ does not contain any subloop isomorphic to the group $UT_3(R)$.*

References

[1] **E.L. Bashkirov**, *On subloops of the loop of invertible elements of the split Cayley-Dickson algebra over a field that contain a subloop of transvections*, Commun. Algebra, **50** (2022), no. 4, 2083–2108.

[2] **R.S. Pierce**, *Associative algebras*. Graduate Texts in Mathematics, **88**, Springer Verlag, New York, Berlin (1988).

[3] **R. D. Shafer**, *An introduction to nonassociative algebras*, Academic Press, New York (1966).

[4] **T.A. Springer, F.D. Veldkamp**, *Octonions, Jordan algebras and exceptional groups*, Springer Verlag, Berlin, Heidelberg, New York (2000).

[5] **D.A. Suprunenko**, *Matrix groups*, Transl. Math. Monogr., **45**, Amer. Math. Soc., Providence, Rhode Island (1976).

[6] **K.A. Zhevlakov, A. M.Slin'ko, I.P. Shestakov, A.I. Shirshov**, *Rings that are nearly associative*, Academic Press, New York (1982).

Received March 21, 2023

Kalinina str 25, ap. 24
Minsk 220012
Belarus
E-mail: zh.bash@mail.ru