Quasigroups and Related Systems **32** (2024), 191 – 206

https://doi.org/10.56415/qrs.v32.15

On commutative subloops of the loop of invertible elements in the split octonion algebra over a field of characteristic 2

Evgenii L. Bashkirov

Abstract. A loop X is said to be commutative if $x^2(yz) = (xy)(xz)$ for all $x, y, z \in X$. In the paper, commutative subloops of the Moufang loop of invertible elements in the split octonion algebra over a field of characteristic 2 are described.

1. Introduction

Let k be an associative and commutative ring with an identity 1, $O(k)$ the split octonion algebra over k and $G(k)$ the Moufang loop of all invertible elements of $O(k)$. The present paper deals with the case in which k is a field of characteristic 2. For this family of fields, as has been shown in Proposition 2 [2], the loop $G(k)$ has no subloop isomorphic to a class-2 nilpotent group. However, if k is a field of arbitrary characteristic (including characteristic 2), $G(k)$ possesses an ample quantity of subloops isomorphic to abelian groups, i.e. to class-1 nilpotent groups. For example, if x is a fixed element of $G(k)$, then x, being a member of the power associative algebra $O(k)$, has well-defined powers $x^0 = 1, x^1 = x, x^2, \dots, x^{-1}, x^{-2}, \dots$ which form a subloop isomorphic to a cyclic group that is certainly abelian. The present paper concerns a more general algebraic structure, namely, that of commutative loops. Recall that a loop X is called commutative if it satisfies the identity

$$x^2(yz) = (xy)(xz). \qquad (1)$$

It is known that if a loop X satisfies (1), then the operation of multiplication in X is commutative in the sense that $xy = yx$ for all $x, y \in X$, and the

2010 Mathematics Subject Classification:20N05
Keywords:Moufang loops, commutative loops, alternative algebras

loop X is Moufang ([3], pp. 99, 100; [6], p. 112, exercise IV 5.A). Speaking somewhat loosely, the content of the paper can be summed up as follows.

Theorem 1.1. *If k is a field of characteristic 2 and G is a commutative subloop of $G(k)$, that is, if $x^2(yz) = (xy)(xz)$ for all $x, y, z \in G$, then the operation of multiplication in $O(k)$, being restricted to G, is associative and commutative.*

In fact, the proof of Theorem 1.1 is deduced from the proof of Theorem 3.3 which classifies commutative subloops of $G(k)$. In turn the proof of Theorem 3.3 is accomplished by an investigation of subalgebras of $O(k)$ that are linear k-hulls of the corresponding commutative subloops. Since the list of these subalgebras, and as a consequence, that of the corresponding subloops is rather long, the formulation of Theorem 3.3 requires a quite cumbersome preliminary work.

2. Preliminaries

Let k be an associative and commutative ring with 1. The multiplicative group of invertible elements of k is denoted $k^\times$, and $(k, +)$ is the additive group of k.

If $a \in k$ and $S, T \subseteq k$, then $aS = Sa = \{as \mid s \in S\}$, $S + T = \{s + t \mid s \in S, t \in T\}$. The set of all elements that are squares in k is denoted $k^\square$, i.e. $k^\square = \{b^2 \mid b \in k\}$.

k^3 is the standard free k-module of column vectors of length 3 with components in k. The standard basis of k^3 is obtained, as usual, by specifying the elements

$$e_1 = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \quad e_2 = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}, \quad e_3 = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}.$$

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 in k^3, respectively.

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

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

where $a, b, c, d \in k, \alpha, \beta, \gamma, \delta \in k^3$. Under the operations just defined, $O(k)$ is an alternative non-associative k-algebra termed the split octonion or split Cayley-Dickson algebra (see, for instance, [8]). One should specify the elements

$$e_{11} = \begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{0} & 0 \end{pmatrix}, \quad e_{22} = \begin{pmatrix} 0 & \mathbf{0} \\ \mathbf{0} & 1 \end{pmatrix}, \quad e_{12}^{(m)} = \begin{pmatrix} 0 & e_m \\ \mathbf{0} & 0 \end{pmatrix}, \quad e_{21}^{(m)} = \begin{pmatrix} 0 & \mathbf{0} \\ e_m & 0 \end{pmatrix}$$
$$(m = 1, 2, 3)$$

which form a basis for the free k-module $O(k)$.

The symbol 1_2 is used to denote the identity element of the algebra $O(k)$,

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

The symbol 0_2 designates the zero octonion

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

If $\alpha \in k^3$, then

$$t_{12}(\alpha) = \begin{pmatrix} 1 & \alpha \\ \mathbf{0} & 1 \end{pmatrix}, \quad t_{21}(\alpha) = \begin{pmatrix} 1 & \mathbf{0} \\ \alpha & 1 \end{pmatrix}.$$

For any $m \in \{1, 2, 3\}$,

$$M_{[m]}(k) = \left\{ \begin{pmatrix} a & be_m \\ ce_m & d \end{pmatrix} \,\middle|\, a, b, c, d \in k \right\} \subseteq O(k).$$

$M_{[m]}(k)$ is an associative subalgebra of $O(k)$, and $M_{[m]}(k)$ is isomorphic to the algebra of 2×2 matrices over k.

The algebra $O(k)$ admits an involution $^-: O(k) \to O(k)$ such that

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

The trace $\mathrm{tr}(x)$ and the norm $n(x)$ of the x are defined by

$$x + \bar{x} = \mathrm{tr}(x) 1_2, \quad x\bar{x} = n(x) 1_2,$$

and so $\mathrm{tr}(x) = a + b, n(x) = ab - \alpha \cdot \beta$.

$G(k)$ denotes the Moufang loop of elements of $O(k)$ whose norm lies in $k^\times$, i.e. elements invertible in $O(k)$.

The norm n determines the bilinear form $(x, y) = n(x+y) - n(x) - n(y) = x\bar{y} + y\bar{x}$ on the k-module $O(k)(x, y \in O(k))$. Throughout the paper, all metric concepts mentioned are related to the bilinear form (,) determined by the norm mapping $n\colon O(k) \to k$.

The automorphism group of the algebra $O(k)$ is denoted $G_2(k)$.

If k is a subring of an associative and commutative ring S having the same 1 as k, then the set

$$ZT_2(k, S) = \left\{ \begin{pmatrix} r & s \\ 0 & r \end{pmatrix} =: [r, s] \middle| \; r \in k, s \in S \right\}$$

is a subring of the ring of 2×2 matrices over S. The group $ZT_2(k, S)^\times$ which is formed by all matrices $[r, s]$ with $r \in k^\times, s \in S$, is isomorphic to the group direct product $k^\times \times (S, +)$, an isomorphism of $ZT_2(k, S)^\times$ onto $k^\times \times (S, +)$ being given by $[r, s] \mapsto (r, sr^{-1})$.

3. Results

Assume that k is an associative and commutative ring with identity and taking $m', t \in k, m \in k^\times$ denote by

$$C_1(k, m, m'),\ C_{20}(k, m),\ C_{30}(k, m),\ C_{40}(k, m, t),\ C_5(k),\ C_6(k),\ C_7(k)$$

the following seven subsets of $O(k)$:

$C_1(k, m, m') = \left\{ \begin{pmatrix} c & \frac{c+d}{m} e_1 \\ \frac{c+d}{m} m' e_1 & d \end{pmatrix} \middle| \; c, d \in k \right\},$

$C_{20}(k, m) = k1_2 + k\left(e_{12}^{(1)} + m e_{21}^{(1)}\right),$

$C_{30}(k, m) = k1_2 + ke_{12}^{(1)} + ke_{21}^{(2)} + k\left(e_{12}^{(3)} + m e_{21}^{(3)}\right),$

$C_{40}(k, m, t) = k1_2 + k\left(e_{12}^{(1)} + m e_{21}^{(1)}\right) + k\left(e_{12}^{(2)} + t e_{21}^{(2)}\right) + k\left(-mte_{12}^{(3)} + e_{21}^{(3)}\right),$

$C_5(k) = C_{20}(k, 0),$

$C_6(k) = k1_2 + ke_{12}^{(1)} + ke_{21}^{(3)},$

$C_7(k) = k1_2 + ke_{12}^{(1)} + ke_{21}^{(2)} + ke_{21}^{(3)}.$

The subsets $C_{20}(k, m),\ C_{30}(k, m),\ C_{40}(k, m, t),\ C_5(k),\ C_6(k),\ C_7(k)$ are subalgebras of $O(k)$, and, furthermore, they are associative because all of these are generated by at most two elements. In addition, for any such k, the subalgebras $C_{20}(k,m)$, hence $C_5(k)$, and $C_6(k)$ are commutative. On the other hand, the associative subalgebra $A \in \{C_{30}(k,m), C_{40}(k,m,t), C_7(k)\}$ is commutative if and only if $2 = 0$. To see this, it is enough to consider the equation $xy = yx$ for $x = e_{12}^{(1)}, y = e_{12}^{(3)} + me_{21}^{(3)}$ if $A = C_{30}(k,m)$, for $x = e_{12}^{(1)} + me_{21}^{(1)}, y = e_{12}^{(2)} + te_{21}^{(2)}$ if $A = C_{40}(k,m,t)$ and for $x = e_{21}^{(2)}, y = e_{21}^{(3)}$ if $A = C_7(k)$.

As to $C_1(k,m,m')$, it is immediate that this is a submodule of the k-module $O(k)$. The sufficient and necessary condition for $C_1(k,m,m')$ to be a subalgebra of $O(k)$ is $2 = 0$ as can be seen from the following assertion.

Lemma 3.1. *The following conditions are equivalent for* $C_1 = C_1(k,m,m')$.

(*a*) $2 = 0$.

(*b*) C_1 *contains* 1_2.

(*c*) C_1 *is closed under the multiplication in* $O(k)$.

Proof. For the sake of brevity, it is convenient to write $u(c,d)$ instead of

$$\begin{pmatrix} c & \frac{c+d}{m}e_1 \\ \frac{c+d}{m}m'e_1 & d \end{pmatrix}.$$

(*a*) $\Rightarrow$ (*b*). If $2 = 0$, then $u(1,1) = 1_2 \in C_1$.

(*b*) $\Rightarrow$ (*c*). Suppose that C_1 contains 1_2. This means that $1_2 = u(c,d)$ for some $c,d \in k$. Thus $c = d = 1$, so $\mathbf{0} = \frac{1+1}{m}e_1$, whence $2 = 0$. Now the latter equality shows that $u(c,d) = d1_2 + \frac{c+d}{m}\iota$ for all $c,d \in k$, where $\iota = u(m,0)$. It follows that $1_2, \iota$ form a basis for C_1. Moreover, $\iota^2 = m'1_2 + m\iota$ which means that C_1 is a quadratic k-algebra of type (m',m) ([4], p. 433), and hence it is closed under multiplication.

(*c*) $\Rightarrow$ (*a*). Suppose that C_1 is closed under multiplication. Then

$$C_1 \ni u(m,0)^2 = \begin{pmatrix} m^2 + m' & me_1 \\ m'me_1 & m' \end{pmatrix},$$

whence $m = (m^2 + m' + m')m^{-1}$, and so $2m' = 0$. It follows that $u(1,1)$, being an element of C_1, is equal to $t_{12}(2m^{-1}e_1)$. Therefore, $C_1 \ni t_{12}(2m^{-1}e_1)^2 = t_{12}(4m^{-1}e_1)$, and thus $t_{12}(4m^{-1}e_1) = u(c,d)$ for some $c,d \in k$. This implies $c = d = 1$, and so $4m^{-1} = (1+1)m^{-1} = 2m^{-1}$, whence $2 = 0$. The lemma is proved completely. $\square$

From now on, k is assumed to be a field of characteristic 2, and hence all

$$C_1(k,m,m'),\ C_{20}(k,m),\ C_{30}(k,m),\ C_{40}(k,m,t),\ C_5(k),\ C_6(k),\ C_7(k)$$

are associative and commutative subalgebras of $O(k)$. It should be noted that some of these subalgebras are isomorphic to each other. The following lemma lists the isomorphisms and indicates conditions under which they exist. Note that all of these isomorphisms are induced by automorphisms of the algebra $O(k)$.

Lemma 3.2.
(I) *If* $m \in k^{\square}$, *then* $C_{20}(k,m)^{\sigma_1} = C_5(k)$ *and* $C_{30}(k,m)^{\sigma_2} = C_7(k)$ *for some* $\sigma_1, \sigma_2 \in G_2(k)$.
(II) (a) *If either* $m \in k^{\square}$ *and* $t \notin k^{\square} + k^{\square}m$ *or* $m \notin k^{\square}$ *and* $t \in k^{\square} + k^{\square}m$, *then* $C_{40}(k,m,t)^{\sigma} = C_{30}(k,m')$ *for some* $\sigma \in G_2(k)$ *and* $m' \in k \setminus k^{\square}$.
(b) *If* $m \in k^{\square}$ *and* $t \in k^{\square} + k^{\square}m$, *then* $C_{40}(k,m,t)^{\sigma} = C_7(k)$ *for some* $\sigma \in G_2(k)$.

Proof. (I) Suppose that $m = a^2, a \in k$. The subalgebra $C_{20}(k,m)$ contains the element $y_1 = a1_2 + (e_{12}^{(1)} + e_{21}^{(1)}a^2)$ for which $y_1^2 = 0_2$. Therefore, there exists $\sigma_1 \in G_2(k)$ with $y_1^{\sigma_1} = e_{12}^{(1)}$, and hence $C_{20}(k,m)^{\sigma_1} = (k1_2 + ky_1)^{\sigma_1} = C_5(k)$. Now consider $C_{30}(k,m)$. It contains the subspace Y spanned by $e_{12}^{(1)}, e_{21}^{(2)}, y_1$, where $y_1 = a1_2 + (e_{12}^{(3)} + e_{21}^{(3)}a^2)$. This Y is a 3-dimensional totally singular subspace ([5], p. 114) of $O(k)$ and all elements of Y are of trace 0. Moreover, the elements $e_{12}^{(1)}, e_{21}^{(2)} \in Y$ form, in the terminology of [1], an extra-special pair. By Lemma 5.2 [1], $Y^{\sigma_2} = e_{12}^{(1)}k + e_{21}^{(2)}k + e_{21}^{(3)}k$ for some $\sigma_2 \in G_2(k)$. So $C_{30}(k,m)^{\sigma_2} = (k1_2 + Y)^{\sigma_2} = C_7(k)$.

(II) (a) Let $m = a^2, a \in k$. Suppose that $t \notin k^{\square} + k^{\square}m$ which implies $t \notin k^{\square}$. Then $C_{40}(k,m,t)$ contains the extra-special pair y_1, y_2, where $y_1 = a1_2 + (e_{12}^{(1)} + e_{21}^{(1)}a^2), y_2 = y_1(e_{12}^{(2)} + e_{21}^{(2)}t)$. By Lemma 5.1 [1], there exists $\sigma \in G_2(k)$ with $y_1^{\sigma} = e_{12}^{(1)}, y_2^{\sigma} = e_{21}^{(2)}$. Set $y_3 = (e_{12}^{(2)} + e_{21}^{(2)}t)^{\sigma}$ and write

$$y_3 = \begin{pmatrix} r & e_1r_1 + e_2r_2 + e_3r_3 \\ e_1t_1 + e_2t_2 + e_3t_3 & r \end{pmatrix}, \quad r, r_i, t_i \in k.$$

Since y_3 commutes with $e_{12}^{(1)}$ and with $e_{21}^{(2)}, t_1 = r_2 = 0$. Thus, $C_{40}(k,m,t)^{\sigma}$ contains $y_4 = r_3e_{12}^{(3)} + t_3e_{21}^{(3)}$ because $y_4 = y_3 - r1_2 - e_{12}^{(1)}r_1 - e_{21}^{(2)}t_2$. Since $y_3^2 = t1_2, r^2 + r_3t_3 = t$ which shows that $r_3t_3 \notin k^{\square}$. In particular, $r_3 \neq 0$, and hence $m' = r_3^{-1}t_3 \notin k^\Box$. Now observe that $y_4 = r_3(e_{12}^{(3)} + m'e_{21}^{(3)})$, and so $C_{40}(k,m,t)^\sigma = C_{30}(k,m')$.

Suppose further that $m \notin k^\Box$ but $t \in k^\Box + k^\Box m$. Thus $t = a^2 + b^2 m$, where $a, b \in k$. First consider the case $b = 0$, and so $t = a^2 \in k^\Box$. The group $G_2(k)$ contains an element τ such that

$$\left(e_{12}^{(1)}\right)^\tau = e_{12}^{(2)}, \quad \left(e_{12}^{(2)}\right)^\tau = e_{12}^{(1)}, \quad \left(e_{12}^{(3)}\right)^\tau = e_{12}^{(3)},$$
$$\left(e_{21}^{(1)}\right)^\tau = e_{21}^{(2)}, \quad \left(e_{21}^{(2)}\right)^\tau = e_{21}^{(1)}, \quad \left(e_{21}^{(3)}\right)^\tau = e_{21}^{(3)}.$$

Then $C_{40}(k,m,t)^\tau = C_{40}(k,t,m)$ and since $t \in k^\Box$ and $m \notin k^\Box$, the case already considered shows that $C_{40}(k,t,m)^\phi = C_{30}(k,m')$ for some $\phi \in G_2(k)$ and $m' \in k \setminus k^\Box$. Therefore, $C_{40}(k,m,t)^{\tau\phi} = C_{30}(k,m')$ and hence $\tau\phi$ can serve as a required σ.

Next suppose that $b \neq 0$. Now the elements

$$y_1 = a1_2 + b\left(e_{12}^{(1)} + me_{21}^{(1)}\right) + \left(e_{12}^{(2)} + te_{21}^{(2)}\right), \quad y_2 = y_1\left(e_{12}^{(1)} + me_{21}^{(1)}\right),$$

both belonging to $C_{40}(k,m,t)$, form an extra-special pair. Again arguing as at the beginning of the Part (II) proof, one concludes that for some $\sigma \in G_2(k)$ and $m' \in k \setminus k^\Box, C_{40}(k,m,t)^\sigma = C_{30}(k,m')$.

(b). Suppose that $m \in k^\Box$ and $t \in k^\Box + k^\Box m$. This means that both a and t are squares in k, i.e. $m = a^2, t = d^2, a, d \in k$. Then $C_{40}(k,m,t)$ contains the elements

$$y_1 = \begin{pmatrix} a & e_1 \\ me_1 & a \end{pmatrix}, \quad y_2 = \begin{pmatrix} d & e_2 \\ te_2 & d \end{pmatrix},$$
$$y_3 = \begin{pmatrix} ad & e_1 d + e_2 a + e_3 mt \\ e_1 md + e_2 at + e_3 & ad \end{pmatrix}$$

because

$$y_1 = a1_2 + \left(e_{12}^{(1)} + e_{21}^{(1)}m\right), \quad y_2 = d1_2 + \left(e_{12}^{(2)} + e_{21}^{(2)}t\right), \quad y_3 = y_1 y_2.$$

Let Y be the subspace spanned by y_1, y_2, y_3. Then Y is a 3-dimensional totally singular subspace that contains the extra-special pair y_1, y_3 and is formed by elements of trace 0. Lemma 5.2 [1] shows then that there exists $\sigma \in G_2(k)$ with $Y^\sigma = e_{12}^{(1)}k + e_{21}^{(2)}k + e_{21}^{(3)}k$. So $C_{40}(k,m,t)^\sigma = k1_2 + Y^\sigma = C_7(k)$ which completes the proof of the lemma. $\Box$

Lemma 3.2 makes it reasonable to consider $C_{20}(k,m), C_{30}(k,m)$ and $C_{40}(k,m,t)$ under the following additional assumptions.

(a) For $C_{20}(k,m)$ and $C_{30}(k,m)$, it is assumed that $m \notin k^{\square}$.

(b) For $C_{40}(k,m,t)$, it is assumed that $m \notin k^{\square}$ and $t \notin k^{\square} + k^{\square}m$.

When (a) and (b) hold, $C_{20}(k,m), C_{30}(k,m), C_{40}(k,m,t)$ are denoted

$$C_2(k,m),\ C_3(k,m),\ C_4(k,m,t),$$

respectively. It should be noted, however, that for certain fields k,

$$C_2(k,m),\ C_3(k,m),\ C_4(k,m,t)$$

can not arise (this will be the case, for instance, if k is algebraically closed), whereas $C_5(k), C_6(k), C_7(k)$ exist for all fields of characteristic 2.

So, under the assumptions made, all

$$C_1(k,m,m'),\ C_2(k,m),\ C_3(k,m),\ C_4(k,m,t),\ C_5(k),\ C_6(k),\ C_7(k)$$

are associative and commutative subalgebras of $O(k)$, and hence their multiplicative groups

$$C_1(k,m,m')^{\times},\ C_2(k,m)^{\times},\ C_3(k,m)^{\times},\ C_4(k,m,t)^{\times},\ C_5(k)^{\times},\ C_6(k)^{\times},\ C_7(k)^{\times}$$

are abelian.

The subalgebra $C_1(k,m,m')$ is isomorphic to a quadratic k-algebra of type (m',m), and therefore $C_1(k,m,m')^{\times}$ is isomorphic to either the multiplicative group of a separable quadratic field extension $k(\theta)$ of k, where θ is a root of the irreducible (over k) polynomial $\lambda^2 + m\lambda + m'$ belonging to the polynomial ring $k[\lambda]$ in a transcendental element λ, or to the direct product $k^{\times} \times k^{\times}$ of two copies of the group $k^{\times}$.

$C_2(k,m)$ is isomorphic to a purely inseparable quadratic field extension $k(\sqrt{m})$ of k, and hence $C_2(k,m)^{\times} \cong k(\sqrt{m})^{\times}$.

$C_3(k,m)$ is isomorphic to the k-algebra $ZT_2(k(\sqrt{m}), k(\sqrt{m}))$. The isomorphism $C_3(k,m) \to ZT_2(k(\sqrt{m}), k(\sqrt{m}))$ is given by

$$\begin{pmatrix} x_0 & x_1e_1 + x_3e_3 \\ x_2e_2 + x_3me_3 & x_0 \end{pmatrix} \mapsto \begin{pmatrix} x_0 + x_3\sqrt{m} & x_1 + x_2\sqrt{m} \\ 0 & x_0 + x_3\sqrt{m} \end{pmatrix}.$$

Hence $C_3(k,m)^{\times} \cong k(\sqrt{m})^{\times} \times (k(\sqrt{m}), +) \cong k(\sqrt{m})^{\times} \times (k,+) \times (k,+)$.

Now let $k[q]$ be a quadratic k-algebra of type $(0,0)$ for which $1, q$ is a basis such that $q^2 = 0$. Then $C_6(k)$ is isomorphic to the k-algebra $ZT_2(k, k[q])$, the isomorphism between $C_6(k)$ and $ZT_2(k, k[q])$ being

$$\begin{pmatrix} x_0 & x_1e_1 \\ x_2e_3 & x_0 \end{pmatrix} \mapsto \begin{pmatrix} x_0 & x_1 + x_2q \\ 0 & x_0 \end{pmatrix}.$$

So $C_6(k)^\times \cong k^\times \times (k[q], +) \cong k^\times \times (k, +) \times (k, +)$ and an explicit form of the group isomorphism of $C_6(k)^\times$ onto $k^\times \times (k, +) \times (k, +)$ is

$$\begin{pmatrix} x_0 & x_1e_1 \\ x_2e_3 & x_0 \end{pmatrix} \mapsto (x_0, x_1x_0^{-1}, x_2x_0^{-1}).$$

Finally, $C_7(k)$ is isomorphic to the k-algebra $ZT_2(k[q], k[q])$. So $C_7(k)^\times \cong k[q]^\times \times (k[q], +) \cong k^\times \times (k, +) \times (k, +) \times (k, +)$. An explicit form of an k-algebra isomorphism between $C_7(k)$ and $ZT_2(k[q], k[q])$ is

$$\begin{pmatrix} x_0 & x_1e_1 \\ x_2e_2 + x_3e_3 & x_0 \end{pmatrix} \mapsto \begin{pmatrix} x_0 + x_3q & x_2 + x_1q \\ 0 & x_0 + x_3q \end{pmatrix},$$

and hence an explicit form of a group isomorphism between $C_7(k)^\times$ and $k^\times \times (k, +) \times (k, +) \times (k, +)$ is

$$\begin{pmatrix} x_0 & x_1e_1 \\ x_2e_2 + x_3e_3 & x_0 \end{pmatrix} \mapsto (x_0, x_3x_0^{-1}, x_2x_0^{-1}, x_2x_3x_0^{-2} + x_1x_0^{-1}).$$

Now it will be proved that subgroups of the listed above abelian groups

$$C_1(k, m, m')^\times,\ C_2(k, m)^\times,\ C_3(k, m)^\times,\ C_4(k, m, t)^\times,\ C_5(k)^\times,\ C_6(k)^\times,\ C_7(k)^\times$$

exhaust in fact all commutative subloops of $G(k)$.

Theorem 3.3. *Let k be a field of characteristic 2 and G a commutative subloop of $G(k)$ in the sense that $x^2(yz) = (xy)(xz)$ for all $x, y, z \in G$. Then for some $\sigma \in G_2(k)$, one of the following holds.*

(i) $G^\sigma \leqslant C_1(k, m, m')$ for some $m \in k^\times, m' \in k$ and $G \nsubseteq k1_2$ so that G is isomorphic to either a subgroup of the multiplicative group of a separable field quadratic extension of k, or to the subgroup of the group direct product $k^\times \times k^\times$.

(ii) $G^\sigma \leqslant k^\times 1_2$, and so G is isomorphic to a subgroup of $k^\times$.

(*iii*) $G^\sigma \leqslant C_2(k,m)^\times$, *and thus G is isomorphic to a subgroup of the multiplicative group of the purely inseparable quadraic field extension $k(\sqrt{m})$, the subloop G containing two elements linearly independent over k.*

(*iv*) $G^\sigma \leqslant C_3(k,m)^\times$, *and thus G is isomorphic to a subgroup of the direct product $k(\sqrt{m})^\times \times (k,+) \times (k,+)$, G containing four elements linearly independent over k.*

(*v*) $G^\sigma \leqslant C_4(k,m,t)^\times$, *and so G is isomorphic to a subgroup of the multiplicative group of the purely inseparable field extension $k(\sqrt{m},\sqrt{t})$ of degree 4 over k, G containing four elements linearly independent over k.*

(*vi*) $G^\sigma \leqslant C_5(k)^\times$, *and so G is isomorphic to a subgroup of $k^\times \times (k,+)$, and G contains two elements linearly independent over k.*

(*vii*) *G contains three elements linearly independent over k and $G^\sigma \leqslant C_6(k)^\times$ so that G is isomorphic to a subgroup of $k^\times \times (k,+) \times (k,+)$.*

(*viii*) *G contains four elements linearly independent over k and $G^\sigma \leqslant C_7(k)^\times$ so that G is isomorphic to a subgroup of $k^\times \times (k,+) \times (k,+) \times (k,+)$.*

Proof. The proof is divided in two parts, the first of which deals with the case when G contains an element of nonzero trace, whereas the second is devoted to loops all of whose elements have zero trace.

Part 1. Several preliminaries are needed before a direct consideration of the case will be given.

Let m be a fixed element of $k^\times$ and α_0, β_0 be fixed vectors of k^3. For any $c, d \in k$, the octonion

$$\begin{pmatrix} c & \frac{c+d}{m}\alpha_0 \\ \frac{c+d}{m}\beta_0 & d \end{pmatrix}$$

is denoted $u(m,\alpha_0,\beta_0;c,d)$ and let

$$U(m,\alpha_0,\beta_0) = \{u(m,\alpha_0,\beta_0;c,d) \mid c,d \in k\}.$$

Observe that $1_2 = u(m,\alpha_0,\beta_0;1,1) \in U(m,\alpha_0,\beta_0)$. If $\iota = u(m,\alpha_0,\beta_0;m,0)$, then $1_2, \iota$ is a basis of $U(m,\alpha_0,\beta_0)$. Moreover, if $m' = \alpha_0 \cdot \beta_0$, then $\iota^2 = \iota m + m' 1_2$ which can be expressed by saying that $U(m,\alpha_0,\beta_0)$ is a quadratic k-algebra of type (m',m). By Proposition 3 ([4], p. 441), $U(m,\alpha_0,\beta_0)$ is isomorphic to a field (when the polynomial $f(\lambda) = \lambda^2 + m\lambda + m'$ in an indeterminate λ is irreducible over k), or to the direct product $k \times k$ of two copies of the field k (if $f(\lambda)$ has a root in k). Since $(1_2, \iota) = m \neq 0$, the subspace $U(m, \alpha_0, \beta_0)$ of the k-vector space $O(k)$ together with the restriction of the bilinear form $(\ ,\ )$ to $U(m, \alpha_0, \beta_0)$ is non-defective (see, [5], p. 114). Hence $U(m, \alpha_0, \beta_0)$ is a subalgebra of the composition algebra $O(k)$ in the sense of [7], p. 4.

The correspondence $1_2 \mapsto 1_2$, $\iota \mapsto u(m, e_1, e_1 m'; m, 0)$ determines a k-linear isomorphism $\hat{\sigma}$ of the subalgebra $U(m, \alpha_0, \beta_0)$ onto the k-algebra $C_1(k, m, m')$. By Corollary 1.7.3 [7], p. 17, $\hat{\sigma}$ can be extended to an element of $G_2(k)$. In other words, there is $\sigma \in G_2(k)$ with $U(m, \alpha_0, \beta_0)^\sigma = C_1(k, m, m')$.

Now choose and fix $x \in G$ with nonzero trace, and let y be an element of G. Writing

$$x = \begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix} (a, b \in k, \alpha, \beta \in k^3), \quad y = \begin{pmatrix} c & \gamma \\ \delta & d \end{pmatrix} (c, d \in k, \gamma, \delta \in k^3),$$

one obtains that the equation $xy = yx$ together with the condition $a + b \neq 0$ yields

$$\gamma = \frac{c+d}{a+b}\alpha, \quad \delta = \frac{c+d}{a+b}\beta.$$

Thus $y \in U(m, \alpha, \beta)$ with $m = a + b$. So $G \subseteq U(m, \alpha, \beta)$ and as has been noted above, if $m' = \alpha \cdot \beta$, then there is $\sigma \in G_2(k)$ with $G^\sigma \subseteq C_1(k, m, m')$. Hence $G^\sigma \leqslant C_1(k, m, m')^\times$. It remains to note that since G contains the element x with non-zero trace, G can not be contained in $k1_2$, and so G is as in Item (i) of the theorem.

Part 2. Suppose that all elements of G are of trace 0. Hereafter L denotes the linear k-hull of G. As a subspace of the k-vector space $O(k), L$ is totally isotropic relative to the alternating bilinear form $(\ ,\ )$. Since the Witt index of the space $O(k)$ (equipped with $(\ ,\ )$) is 4, $\dim L \leqslant 4$. So the further proof is divided into four cases in accordance of the dimension of L.

(I) $\dim L = 1$. Since $1_2 \in L$, here $L = k1_2$, and so G is isomorphic to a subgroup of $k^\times$ falling in Item (ii) of the theorem.

(II) $\dim L = 2$. One can choose $g \in G \setminus k1_2$. This g together with 1_2 form a basis for L. One has $g^2 = e1_2$ with $e \in k^\times$. There are two possibilities to consider.

(a) $e \in k^\square, e = f^2, f \in k^\times$. If $g_1 = f1_2 + g$, then $1_2, g_1$ is a basis of L and $g_1^2 = 0_2$. Hence there is $\sigma \in G_2(k)$ with $g_1^\sigma = e_{12}^{(1)}$ and so $L^\sigma = C_5(k)$.

Thus G, being isomorphic to a subgroup of $k^{\times} \times (k,+)$, falls in Item (vi) of the theorem.

(b) $e \notin k^{\square}$. Writing

$$g = \begin{pmatrix} a & \alpha \\ \beta & a \end{pmatrix}, \quad a \in k, \alpha, \beta \in k^3,$$

and denoting $m = \alpha \cdot \beta$, one has $g^2 = (a^2 + m)1_2$. If $g_1 = g + a1_2$, then $g_1 = x + y$, where

$$x = \begin{pmatrix} 0 & \alpha \\ \mathbf{0} & 0 \end{pmatrix}, \quad y = \begin{pmatrix} 0 & \mathbf{0} \\ \beta & 0 \end{pmatrix}.$$

Observe that $m \neq 0$ due to the condition $e \notin k^{\square}$. It follows that the correspondence

$$x \mapsto e_{12}^{(1)}, \quad y \mapsto me_{21}^{(1)}, \quad xy \mapsto me_{11}, \quad yx \mapsto me_{22}$$

determines a k-linear isomorphism of the k-algebra $C = kx + ky + kxy + kyx$ onto $M_{[1]}(k)$. Therefore, one can find $\sigma \in G_2(k)$ such that $C^{\sigma} = M_{[1]}(k)$ and $x^{\sigma} = e_{12}^{(1)}, y^{\sigma} = me_{21}^{(1)}$. Then $g_1^{\sigma} = e_{12}^{(1)} + me_{21}^{(1)}$, and so $L^{\sigma} = C_2(k,m)$. Thus G falls in Item (iii) of the theorem.

(III) $\dim L = 3$. Choose elements $g_1, g_2 \in G$ so that $1_2, g_1, g_2$ is a basis for L. Then $g_1 g_2 \in G \subseteq L$, and hence

$$g_1 g_2 = r_0 1_2 + r_1 g_1 + r_2 g_2 \tag{2}$$

for some $r_i \in k$. Since for each $i = 1, 2$, g_i is of trace 0,

$$g_i^2 = a_i 1_2 \tag{3}$$

for some $a_i \in k^{\times}$. Therefore, by (3)

$$(g_1 g_2) g_1 = g_1^2 g_2 = a_1 g_2. \tag{4}$$

On the other hand, using (2), one has

$$\begin{aligned}(g_1 g_2) g_1 = (r_0 1_2 + r_1 g_1 + r_2 g_2) g_1 &= r_0 g_1 + r_1 a_1 1_2 + r_2 (r_0 1_2 + r_1 g_1 + r_2 g_2) \\ &= (r_1 a_1 + r_0 r_2) 1_2 + (r_0 + r_1 r_2) g_1 + r_2^2 g_2.\end{aligned} \tag{5}$$

Comparing (4) and (5) gives

$$r_2^2 = a_1, \tag{6}$$

$$r_0 + r_1 r_2 = 0. \tag{7}$$

Similarly, a calculation of $(g_1g_2)g_2$ in two ways shows that

$$r_1^2 = a_2. \tag{8}$$

Now set $u_1 = g_1 + r_2 1_2, u_2 = g_2 + r_1 1_2$. Then employing (6), (8), (2), (7) yields $u_1^2 = u_2^2 = u_1u_2 = 0_2$. This, together with linear independence of u_1, u_2, means that u_1, u_2 form an extra-special pair. According to Lemma 5.1 [1], there is $\sigma \in G_2(k)$ with $u_1^\sigma = e_{12}^{(1)}, u_2^\sigma = e_{21}^{(3)}$. Consequently, $L^\sigma = C_6(k)$ and so G, being isomorphic to a subgroup of $k^\times \times (k,+) \times (k,+)$, falls into Item (vii) of the theorem.

(IV) $\dim L = 4$. Suppose that any nonzero element of L has a nonzero square. Let $g \in G \setminus k1_2$ and write

$$g = \begin{pmatrix} a & \alpha \\ \beta & a \end{pmatrix}, \quad a \in k, \alpha, \beta \in k^3.$$

If $m = \alpha \cdot \beta$, then $m \notin k^\square$, in particular, $m \neq 0$. As has been shown while considering the case $\dim L = 2$, replacing G by G^ϕ with a suitable $\phi \in G_2(k)$, one may assume $\alpha = e_1, \beta = me_1$. It follows that $g_1 = e_{12}^{(1)} + me_{21}^{(1)} \in L$. Since $\dim L = 4$, one can find $h \in G \setminus (k1_2 + kg_1)$. Write

$$h = \begin{pmatrix} r & r_1e_1 + r_2e_2 + r_3e_3 \\ t_1e_1 + t_2e_2 + t_3e_3 & r \end{pmatrix}, \quad r, r_i, t_i \in k.$$

The condition $g_1h = hg_1$ gives $t_1 = mr_1$. Then L contains

$$h_1 = h - r1_2 - r_1g_1 = \begin{pmatrix} 0 & r_2e_2 + r_3e_3 \\ t_2e_2 + t_3e_3 & 0 \end{pmatrix}.$$

The choice of h shows that $h_1 \neq 0_2$, hence $h_1^2 \neq 0_2$ which, in turn implies that $t = r_2t_2 + r_3t_3 \neq 0$. Suppose $t = t_0^2 + s^2m$ where $t_0, s \in k$. Let

$$h_2 = t_0 1_2 + sg_1 + h_1 = \begin{pmatrix} t_0 & s_1e_1 + r_2e_2 + r_3e_3 \\ sme_1 + t_2e_2 + t_3e_3 & t_0 \end{pmatrix}.$$

Then $h_2^2 = 0_2$, hence $h_2 = 0_2$, so $r_2 = r_3 = t_2 = t_3 = 0$ which is impossible in view of the condition $t \neq 0$. Thus $t \notin k^\square + k^\square m$. Set

$$u_{11} = e_{11}, \quad u_{22} = e_{22},$$

$$u_{12}^{(1)} = e_{12}^{(1)}, \quad u_{12}^{(2)} = \begin{pmatrix} 0 & r_2e_2 + r_3e_3 \\ \mathbf{0} & 0 \end{pmatrix}, \qquad u_{12}^{(3)} = t^{-1}\begin{pmatrix} 0 & t_3e_2 + t_2e_3 \\ \mathbf{0} & 0 \end{pmatrix},$$

$$u_{21}^{(1)} = e_{21}^{(1)}, \quad u_{21}^{(2)} = t^{-1}\begin{pmatrix} 0 & \mathbf{0} \\ t_2e_2 + t_3e_3 & 0 \end{pmatrix}, \quad u_{21}^{(3)} = \begin{pmatrix} 0 & \mathbf{0} \\ r_3e_2 + r_2e_3 & 0 \end{pmatrix}.$$

The correspondence

$$u_{jj} \mapsto e_{jj}(j=1,2), \quad u_{12}^{(i)} \mapsto e_{12}^{(i)}, \quad u_{21}^{(i)} \mapsto e_{21}^{(i)}(i=1,2,3)$$

determines an element σ of the group $G_2(k)$ such that

$$g_1^\sigma = g_1, \quad h_1^\sigma = e_{12}^{(2)} + te_{21}^{(2)}.$$

So L^σ contains the product $g_1^\sigma h_1^\sigma = e_{21}^{(3)} + e_{12}^{(3)}mt$.

The elements $1_2, g_1^\sigma, h_1^\sigma, g_1^\sigma h_1^\sigma$ are linearly independent. Recalling that $m \notin k^\square$ and $t \notin k^\square + k^\square m$, one has $L^\sigma = C_4(k,m,t)$ and G is as in Item (v) of the theorem.

Suppose now that L contains a nonzero nilpotent element u. There is $\varphi \in G_2(k)$ such that $u^\varphi = e_{12}^{(1)}$. Thus replacing G by G^φ, one may assume that $e_{12}^{(1)} \in L$. Since $\dim L = 4$, one can find $g \in G \setminus (k1_2 + ke_{12}^{(1)})$. Let

$$g = \begin{pmatrix} r & r_1e_1 + r_2e_2 + r_3e_3 \\ t_1e_1 + t_2e_2 + t_3e_3 & r \end{pmatrix}, \quad r, r_i, t_i \in k.$$

Since $ge_{12}^{(1)} = e_{12}^{(1)}g, t_1 = 0$. Hence L contains $g_1 = r_2e_{12}^{(2)} + r_3e_{12}^{(3)} + t_2e_{21}^{(2)} + t_3e_{21}^{(3)}$ because $g_1 = g - r1_2 - r_1e_{12}^{(1)}$. Note also that g_1 is nonzero in view of the choice of g. If $r_2 = r_3 = 0$, then $e_{12}^{(1)}$ and g_1 form an extra-special pair. If $r_2e_2 + r_3e_3 \neq \mathbf{0}$, then $L \ni e_{12}^{(1)}g_1 = r_2e_{21}^{(3)} + r_3e_{21}^{(2)}$ which, together with $e_{12}^{(1)}$, gives an extra-special pair again. Thus if L contains a nonzero nilpotent element, then L contains an extra-special pair. By Lemma 5.1 [1] replacing G by G^σ with an appropriate $\sigma \in G_2(k)$, one may assume that $e_{12}^{(1)}, e_{21}^{(2)} \in L$. Using again the condition $\dim L = 4$, one can find $h \in L \setminus (k1_2 + ke_{12}^{(1)} + ke_{21}^{(2)})$. Since h commutes with $e_{12}^{(1)}$ and with $e_{21}^{(2)}$,

$$h = \begin{pmatrix} b & s_1e_1 + s_3e_3 \\ q_2e_2 + q_3e_3 & b \end{pmatrix} \quad b, s_1, s_3, q_2, q_3 \in k.$$

Therefore L contains $h_1 = s_3e_{12}^{(3)} + q_3e_{21}^{(3)}$ because $h_1 = h - b1_2 - s_1e_{12}^{(1)} - q_2e_{21}^{(2)}$. If $s_3q_3 \notin k^\square$, then $s_3 \neq 0$ and $h_1 = s_3(e_{12}^{(3)} + me_{21}^{(3)})$, where $m = q_3s_3^{-1} \notin k^\square$. Thus L contains the octonions $1_2, e_{12}^{(1)}, e_{21}^{(2)}, e_{12}^{(3)} + me_{21}^{(3)}$, and therefore $L = C_3(k,m)$. So, in this case G is isomorphic to a subgroup of $k(\sqrt{m})^\times \times (k,+) \times (k,+)$. But G contains four linearly independent elements, and consequently it falls into Item (iv) of the theorem.

Finally suppose that $s_3 q_3 = t_0 \in k^{\square}$. Then L contains $h_2 = t_0 1_2 + h_1 = t_0 1_2 + s_3 e_{12}^{(3)} + q_3 e_{21}^{(3)}$, and hence L contains the subspace Y spanned by $e_{12}^{(1)}, e_{21}^{(2)}, h_2$. A direct calculation shows that Y is a totally singular subspace of $O(k)$ and $\dim Y = 3$. Furthermore, every element of Y is of trace 0 and according to Lemma 5.2 [1], one can find $\sigma \in G_2(k)$ such that $Y^\sigma = ke_{12}^{(1)} + ke_{21}^{(2)} + ke_{21}^{(3)}$. So $L^\sigma = k1_2 + Y^\sigma = C_7(k)$. Thus, in this case, G is isomorphic to a subgroup $k^\times \times (k,+) \times (k,+) \times (k,+)$. Since G contains four linearly independent elements, G falls in Item (viii) of the theorem. The theorem is proved completely. □

The proof of Theorem 3.3 shows that this theorem admits the following restatement in the language of maximal commutative subloops of $G(k)$.

Theorem 3.4. *Let k be a field of characteristic 2. If G is a maximal commutative subloop of $G(k)$, then for some $\sigma \in G_2(k)$, G^σ coincides with one of the following subloops:*

$C_1(k,m,m')^\times$, $C_2(k,m)^\times$, $C_3(k,m)^\times$, $C_4(k,m,t)^\times$, $C_5(k)^\times$, $C_6(k)^\times$, $C_7(k)^\times$.

It is instructive also to see how the example of a commutative subloop isomorphic to a cyclic group considered at the beginning of the paper is consistent with Theorem 3.3. So, let x be a fixed element of $G(k)$ and let $G = \{x^n \mid n \in \mathbb{Z}\}$. Though G is a cyclic, hence abelian group, it may fall into different parts of Theorem 3.3 depending on the form of x. Let

$$x = \begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix}, \quad a, b \in k, \alpha, \beta \in k^3. \tag{9}$$

If $\mathrm{tr}(x) \neq 0$, then $G^\sigma \leqslant C_1(a+b, e_1, e_1(\alpha\cdot\beta))^\times$ for some $\sigma \in G_2(k)$. If $\mathrm{tr}(x) = 0$ and $\alpha\cdot\beta \notin k^{\square}$, then $G^\sigma \leqslant C_3(k, \sqrt{\alpha\cdot\beta})^\times$ for some $\sigma \in G_2(k)$. If, finally, $\mathrm{tr}(x) = 0$ and $\alpha\cdot\beta \in k^{\square}$, then $G^\sigma \leqslant C_5(k)^\times$, and thus G is isomorphic to a subgroup of $k^\times \times (k,+)$. To construct a more concrete example one can take in (9) the octonion x with $a = b = 1, \beta = \mathbf{0}$ and α a nonzero vector of k^3. In this case, G is isomorphic to a cyclic group of order 2. As a subgroup of $k^\times \times (k,+)$, this cyclic group is realized as $1 \times \{1, a_0\}$, where a_0 is a nonzero element of k. The first component of any element of this subgroup of $k^\times \times (k,+)$ must be trivial, since the group $k^\times$ does not contain any element of order 2.

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), 2083–2108.

[2] **E.L. Bashkirov**, *On nonexistence of certain associative subloops in the loop of invertible elements of the split alterative Cayley–Dickson algebra*, Quasigroups and Related Systems, **31** (2023), 185–200.

[3] **V.D. Belousov**, *Foundations of the theory of quasigroups and loops* (Russian) Izdat. Nauka, Moscow, 1967.

[4] **N. Bourbaki**, *Algebra I Chapters 1–13*, Addison-Wesley Publishing Company, Reading Massachusets, 1974.

[5] **L. Grove**, *Classical groups and geometric algebra*, Graduate Texts in Mathematics, Volume 39, Am. Math. Soc., Providence, Phode Island, 2002.

[6] **H.O. Pflugfelder**, *Quasigroups and loops. Introduction* (Sigma Series in Pure Mathematics), Heldermann, Berlin, 1990.

[7] **T.A. Springer, F.D. Veldkamp**, *Octonions, Jordan Algebras and Exceptional Groups*, Springer Verlag, Berlin, Heidelberg, New York, 2002.

[8] **A. Wells**, *Moufang loops arising from Zorn matrix algebra*, Comment. Math. Univ. Carol., **51** (2010), 371–388.

Received March 20, 2024

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