Quasigroups and Related Systems **34** (2026), 229 – 245

https://doi.org/10.56415/qrs.v34.17

On associative subloops of loops connected with the octonion algebras over commutative rings

Evgenii L. Bashkirov

Abstract. Let k be an associative and commutative ring with 1. Let $\mathbb{O}(k)$ be the alternative non-associative split octonion (Cayley–Dickson) algebra over k. Let $G(k)$ be the Moufang loop of invertible elements of $\mathbb{O}(k)$. In the paper, associative subloops (subgroups) of $G(k)$ are studied. Isomorphisms between subloops of this class and groups related to the group of 3×3 unitriangular matrices over k have been established.

1. Introduction

The present paper is devoted to the study of Moufang loops related to the split alternative non-associative octonion (Cayley–Dickson) algebras over associative and commutative rings with identity. The aim of the paper is to generalize isomorphisms arising in these algebras over fields between some subloops of invertible elements of the algebras and groups. In particular, there is a phenomenon when these isomorphisms, which are isomorphisms between non-abelian groups in the case of fields of characteristic not 2 (cf. [1]), become, in the case of fields of characteristic 2, isomorphisms between abelian groups [2]. In the paper, the phenomenon receives its explanation being considered within the framework of the octonion algebras over associative and commutative rings. The main results of the paper are contained in Propositions 5.1, 6.3, 8.2 and Corollary 8.3. The formulation all of these results requires a rather long preliminary work which includes introducing necessary notation and terminology. This will be accomplished in Sections 2, 3, 4.

2010 Mathematics Subject Classification: 20N05

Keywords: Moufang loops, alternative algebras, commutative and associative rings, groups of triangular matrices

2. Notation

Throughout the paper k denotes an associative and commutative ring with 1, and $k^\times$ is the multiplicative group of all invertible elements of k.

If n is a natural number, then the element $n1$ of k is identified with n itself.

If A is an $m \times n$ matrix over k, then the transpose of A is denoted ${}^tA$.

Every k-module M is considered as left, right and two-sided simultaneously via $a\beta = \beta a$ for all $a \in k$ and $\beta \in M$, the records $a\beta$ and βa being equal in their rights. If $n \geqslant 1, \beta_1, \beta_2, \ldots, \beta_n \in M$, and $S_1, S_2, \ldots, S_n$ are subsets of k, then $S_1\beta_1 + S_2\beta_2 + \cdots + S_n\beta_n = \beta_1 S_1 + \beta_2 S_2 + \cdots + \beta_n S_n$ denotes the set of all elements of M having the form $s_1\beta_1 + s_2\beta_2 + \cdots + s_n\beta_n$ with $s_1 \in S_1, s_2 \in S_2, \ldots, s_n \in S_n$.

If $\beta \in M$, then $\mathrm{Ann}_k(\beta)$, or simply $\mathrm{Ann}(\beta)$, is an ideal of k formed by all $r \in k$ that annihilate β, i. e., $\mathrm{Ann}(\beta) = \{r \in k \mid r\beta = 0\}$.

k^3 is the free k-module of column vectors of length 3 with components in k. The standard free module basis of k^3 is the ordered triple e_1, e_2, e_3, where

$$e_1 = {}^t(1,0,0), \quad e_2 = {}^t(0,1,0), \quad e_3 = {}^t(0,0,1).$$

The zero element of k^3 is designated as $\bar{0}$.

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

$\mathbb{O}(k)$ 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 $\mathbb{O}(k)$, 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 $\mathbb{O}(k)$ is an alternative non-associative k-algebra called the split octonion or Cayley-Dickson algebra ([4],[5]). The symbol 1_2 is used to denote the identity of the algebra $\mathbb{O}(k)$,

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

whereas 0_2 designates the zero of $\mathbb{O}(k)$,

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

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

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

The norm $n(x)$ of the element

$$x = \begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix} \in \mathbb{O}(k) \quad (a, b \in k, \alpha, \beta \in k^3)$$

is defined to be $n(x) = ab - \alpha \cdot \beta$. The element x is invertible in $\mathbb{O}(k)$ if and only if $n(x) \in k^\times$.

$G(k)$ denotes the Moufang loop of all invertible elements of $\mathbb{O}(k)$.

$S(k)$ is the subloop of $G(k)$ of all elements with norm 1.

If $\beta_1, \beta_2 \in k^3$, then the element of $\mathbb{O}(k)$ having the form

$$\begin{pmatrix} 1 & s\beta_1 + t\beta_2 \\ r(\beta_1 \times \beta_2) & 1 \end{pmatrix}, \qquad s, t, r \in k,$$

is written as $\big\|\beta_1, \beta_2; s, t, r\big\|$.

Let Y be a loop and X a subloop of Y. If X is isomorphic to a group, i. e., if the restriction of multiplication in Y to X is associative, then X is referred to as a subgroup of Y. If, in addition, X is isomorphic to an abelian group, then X is called an abelian subgroup of Y.

$UT_3(k)$ is the group of all 3×3 upper unitriangular matrices over k, i. e., upper triangular matrices all of whose diagonal elements are equal to 1.

If n is an integer, $n \geqslant 1$, then $M_n(k)$ denotes the associative ring of all $n \times n$ matrices with entries in k.

$GL_n(k)$ is the general linear group of all invertible matrices of $M_n(k)$.

3. Certain groups related to the group of unitriangular matrices of degree 3

The present section covers the family of groups that provide a way for the construction of homomorphisms from some subloops of the loop $S(k)$.

Suppose that I_1, I_2, I_3 are ideals of k such that $I_1 \subseteq I_3, I_2 \subseteq I_3$. Any triple of ideals with this property will be called a *net triple*. This name is dictated for the following reasons.

Let $\sigma = (\sigma_{ij})_{1\leqslant i,j\leqslant 3}$ be a 3×3 array, where

$$\begin{aligned} &\sigma_{11} = 0, \quad \sigma_{12} = I_1, \quad \sigma_{13} = I_3, \\ &\sigma_{21} = 0, \quad \sigma_{22} = 0, \quad \sigma_{23} = I_2, \\ &\sigma_{31} = 0, \quad \sigma_{32} = 0, \quad \sigma_{33} = 0. \end{aligned} \tag{1}$$

Then $\sigma_{it}\sigma_{tj} \subseteq \sigma_{ij}$ for all $i, j, t \in \{1, 2, 3\}$. This means that σ is a net of ideals in the sense of [3]. The set $M(\sigma) = \{a \in M_3(k) \mid a = (a_{ij})_{1\leqslant i,j\leqslant 3}, a_{ij} \in \sigma_{ij}\}$ is a subring of $M_3(k)$, and therefore the set $G(\sigma) = 1_3 + M(\sigma)$ is a multiplicatively closed subset of $M_3(k)$. Since every matrix of $M(\sigma)$ is nilpotent, every matrix of $G(\sigma)$ is invertible, and so $G(\sigma)$ is a subgroup of $GL_3(k)$. Moreover, $G(\sigma)$ is a normal subgroup of $UT_3(k)$.

Henceforth, any upper unitriangular matrix

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$$

is denoted $[a, b, c]$. Two matrices $[a_1, a_3, a_2]$ and $[b_1, b_3, b_2]$ of $UT_3(k)$ belong to one and the same coset of $G(\sigma)$ in $UT_3(k)$ if and only if for each $j \in \{1, 2, 3\}$, the elements a_j and b_j belong to one and the same coset of the subgroup I_j in the additive group of k. Therefore, the coset of $G(\sigma)$ in $UT_3(k)$ that contains the matrix $[s, r, t]$ can be denoted by the array

$$[s + I_1, r + I_3, t + I_2] = \begin{pmatrix} 1 & s + I_1 & r + I_3 \\ 0 & 1 & t + I_2 \\ 0 & 0 & 1 \end{pmatrix}. \tag{2}$$

Here each of the elements $s + I_1, r + I_3, t + I_2$ is considered as an element of the corresponding residue class ring k/I_j of k. In this manner, the quotient group $UT_3(k)/G(\sigma)$ can be identified with the group $UT_3(k, I_1, I_2, I_3)$ formed by all arrays (2) with $s, r, t \in k$, the operation of multiplication being given by the rule

$$\begin{aligned} &[s_1 + I_1, r_1 + I_3, t_1 + I_2][s_2 + I_1, r_2 + I_3, t_2 + I_2] = \\ &[s_1 + s_2 + I_1, r_1 + r_2 + s_1t_2 + I_3, t_1 + t_2 + I_2](s_i, t_i, r_i \in k). \end{aligned}$$

If n is a positive integer, then $UT_3(k, I_1, I_2, I_3)$ has the subgroups

$$\begin{aligned} UT_3^{(1)}(k, I_1, I_2, I_3, n) &= \big\{[sn + I_1, r + I_3, t + I_2] \mid s, r, t \in k\big\}, \\ UT_3^{(2)}(k, I_1, I_2, I_3, n) &= \big\{[sn + I_1, rn + I_3, t + I_2] \mid s, r, t \in k\big\}. \end{aligned}$$

Note that the correspondence

$$[s + I_1, r + I_3, t + I_2] \mapsto [sn + I_1, rn + I_3, t + I_2]$$

determines a homomorphism of the group $UT_3(k, I_1, I_2, I_3)$ onto the subgroup $UT_3^{(2)}(k, I_1, I_2, I_3, n)$ with kernel

$$\big\{[s + I_1, r + I_3, 0 + I_2] \mid s \in (I_1 : n), r \in (I_3 : n)\big\}$$

isomorphic to the direct sum $(I_1 : n)/I_1 \oplus (I_3 : n)/I_3$ of additive abelian groups. This shows that

$$UT_3^{(2)}(k, I_1, I_2, I_3, n) \cong UT_3(k, I_1, I_2, I_3)/\big((I_1 : n)/I_1 \oplus (I_3 : n)/I_3\big). \quad (3)$$

To clarify the nature of the subgroups $UT_3^{(j)}(k, I_1, I_2, I_3, n)(j = 1, 2)$, one should introduce the following subgroups of $UT_3(k)$:

$$UT_3^{(1)}(k, n) = \{[sn, r, t] \mid s, t, r \in k\},$$
$$UT_3^{(2)}(k, n) = \{[sn, rn, t] \mid s, t, r \in k\}.$$

These can be treated as $UT_3^{(j)}(k, I_1, I_2, I_3, n)$, where all I_1, I_2, I_3 are the zero ideals.

Example 3.1. If the additive group of k has no n-torsion, and if $I_1 = I_3 = (0)$ (hence I_2 is the zero ideal too), then (3) gives $UT_3^{(2)}(k, n) \cong UT_3(k)$.

Now let φ be the canonical homomorphism of $UT_3(k)$ onto $UT_3(k)/G(\sigma)$ when the latter is regarded as $UT_3(k, I_1, I_2, I_3)$. In other words, let

$$\varphi([s, r, t]) = [s + I_1, r + I_3, t + I_2], \quad s, t, r \in k.$$

The image of $UT_3^{(1)}(k, n)$ under φ is $UT_3^{(1)}(k, n)G(\sigma)/G(\sigma)$. But $UT_3^{(1)}(k, n)G(\sigma) = UT_3^{(1)}(k, n) + M(\sigma)$. Therefore, the restriction of φ to $UT_3^{(1)}(k, n)G(\sigma)$ yields the group homomorphism of $UT_3^{(1)}(k, n)G(\sigma)$ onto $UT_3^{(1)}(k, I_1, I_2, I_3, n)$ with kernel $G(\sigma)$. So, $UT_3^{(1)}(k, I_1, I_2, I_3, n) \cong UT_3^{(1)}(k, n)G(\sigma)/G(\sigma)$. Similarly, $UT_3^{(2)}(k, n)G(\sigma) = UT_3^{(2)}(k, n) + M(\sigma)$, and $UT_3^{(2)}(k, I_1, I_2, I_3, n) \cong UT_3^{(2)}(k, n)G(\sigma)/G(\sigma)$.

The center of $UT_3(k, I_1, I_2, I_3)$ is the subgroup of all elements of the form $[s + I_1, r + I_3, t + I_2] \in UT_3(k, I_1, I_2, I_3)$ with $s, t \in I_3$. Thus

$UT_3(k, I_1, I_2, I_3)$ is abelian if and only if $I_3 = k$. The commutator subgroup of $UT_3(k, I_1, I_2, I_3)$ is formed by all elements $[0 + I_1, r + I_3, 0 + I_2], r \in k$. Hence if $I_3 \neq k$, then $UT_3(k, I_1, I_2, I_3)$ is class-2 nilpotent. The groups $UT_3^{(j)}(k, I_1, I_2, I_3, n)(j = 1, 2)$ are abelian if and only if $n \in I_3$. Thus if $n \notin I_3$, then both $UT_3^{(j)}(k, I_1, I_2, I_3, n)$ are class-2 nilpotent.

4. On pairs of elements in modules

This section contains another piece of information which is necessary for formulating and proving the main results of the paper.

Let M be a k-module and $\beta_1, \beta_2 \in M$.

Denote by $I_1(\beta_1, \beta_2)$ the set of all $a_1 \in k$ such that there exists $a_2 \in k$ with $a_1\beta_1 + a_2\beta_2 = 0$. Then $I_1(\beta_1, \beta_2)$ is an ideal in k such that $\mathrm{Ann}(\beta_1) \subseteq I_1(\beta_1, \beta_2)$. Hence the residue class ring $Q_1 = I_1(\beta_1, \beta_2)/\mathrm{Ann}(\beta_1)$ is defined. Further, denote by $I_2(\beta_1, \beta_2)$ the set of all $a_2 \in k$ such that there exists $a_1 \in k$ with $a_1\beta_1 + a_2\beta_2 = 0$. Noting that $I_2(\beta_1, \beta_2) = I_1(\beta_2, \beta_1)$, one concludes that $I_2(\beta_1, \beta_2)$ is an ideal in k containing $\mathrm{Ann}(\beta_2)$. So the residue class ring $Q_2 = I_2(\beta_1, \beta_2)/\mathrm{Ann}(\beta_2)$ is defined. Observe that both residue class rings $Q_j(j = 1, 2)$ can be considered as k-modules. Now given $a_1 \in I_1(\beta_1, \beta_2)$ let $\gamma(a_1)$ be the set of all $a_2 \in k$ with $a_1\beta_1 + a_2\beta_2 = 0$. Note that $\gamma(a_1) \subseteq I_2(\beta_1, \beta_2)$. So if $a_2 \in \gamma(a_1)$, then the whole of the coset $a_2 + \mathrm{Ann}(\beta_2) \in Q_2$ is contained in $\gamma(a_1)$. Denoting this coset by $\overline{\gamma}(a_1 + \mathrm{Ann}(\beta_1))$, one gets that $\overline{\gamma}$ is a well defined function from Q_1 to Q_2. Furthermore, $\overline{\gamma}$ establishes an isomorphism of the k-module $I_1(\beta_1, \beta_2)/\mathrm{Ann}(\beta_1)$ onto the k-module $I_2(\beta_1, \beta_2)/\mathrm{Ann}(\beta_2)$.

Now specify the module M and consider the situation where $M = k^3$. Here the cross product $\beta_1 \times \beta_2$ is defined and the following assertion is valid.

Lemma 4.1. *For each,* $j = 1, 2$, $I_j(\beta_1, \beta_2) \subseteq \mathrm{Ann}(\beta_1 \times \beta_2)$.

Proof. Suppose that $a_1 \in I_1(\beta_1, \beta_2)$. This means that there exists $a_2 \in k$ with $a_1\beta_1 + a_2\beta_2 = \bar{0}$. Now $a_1(\beta_1 \times \beta_2) = (a_1\beta_1) \times \beta_2 = (-a_2\beta_2) \times \beta_2 = \bar{0}$, hence $a_1 \in \mathrm{Ann}(\beta_1 \times \beta_2)$. So $I_1(\beta_1, \beta_2) \subseteq \mathrm{Ann}(\beta_1 \times \beta_2)$. Using this, one gets $I_2(\beta_1, \beta_2) = I_1(\beta_2, \beta_1) \subseteq \mathrm{Ann}(\beta_2 \times \beta_1) = \mathrm{Ann}(\beta_1 \times \beta_2)$. □

Example 4.2. Let $\mathbb{Z}$ be the ring of rational integers, and $\mathbb{Z}[v]$ be the ring of dual numbers, i. e., $\mathbb{Z}[v] = \mathbb{Z} \oplus \mathbb{Z}v$, $v^2 = 0$. Let $k = \mathbb{Z}[v] \times \mathbb{Z} \times \mathbb{Z}$, the direct product of rings, and

$$\beta_1 = {}^t((v, 2, 2), (0, 2, 1), (0, 0, 0)), \quad \beta_2 = {}^t((0, 3, 3), (0, 3, 2), (0, 0, 0)) \in k^3.$$

Then $\beta_1 \times \beta_2 = {}^t((0,0,0),(0,0,0),(0,0,1))$. So

$$\begin{aligned} \mathrm{Ann}(\beta_1) &= \mathbb{Z}v \times \{0\} \times \{0\}, \quad \mathrm{Ann}(\beta_2) = \mathbb{Z}[v] \times \{0\} \times \{0\}, \\ \mathrm{Ann}(\beta_1 \times \beta_2) &= \mathbb{Z}[v] \times \mathbb{Z} \times \{0\}, \\ I_1(\beta_1,\beta_2) &= \mathbb{Z}v \times 3\mathbb{Z} \times \{0\}, \quad I_2(\beta_1,\beta_2) = \mathbb{Z}[v] \times 2\mathbb{Z} \times \{0\}.. \end{aligned}$$

This gives an example of a ring k and elements $\beta_1, \beta_2 \in k^3$ such that all of the five ideals $\mathrm{Ann}(\beta_1), \mathrm{Ann}(\beta_2), \mathrm{Ann}(\beta_1 \times \beta_2), I_1(\beta_1,\beta_2), I_2(\beta_1,\beta_2)$ in the ring k are proper, non-trivial and pairwise distinct in the set-theoretical sense. Every coset of $\mathrm{Ann}(\beta_1)$ in $I_1(\beta_1,\beta_2)$ has a representative of the form $(0,3m,0)$, where $m \in \mathbb{Z}$, and every coset of $\mathrm{Ann}(\beta_2)$ in $I_2(\beta_1,\beta_2)$ has a representative $(0,2n,0), n \in \mathbb{Z}$. Since $(0,3m,0)\beta_1 + (0,-2m,0)\beta_2 = \bar{0}$, the isomorphism $\overline{\gamma}\colon I_1(\beta_1,\beta_2)/\mathrm{Ann}(\beta_1) \to I_2(\beta_1,\beta_2)/\mathrm{Ann}(\beta_2)$ is

$$\overline{\gamma}\big((0,3m,0) + (\mathbb{Z}v \times \{0\} \times \{0\})\big) = (0,-2m,0) + (\mathbb{Z}[v] \times \{0\} \times \{0\}).$$

Lemma 4.1 implies that if $I_1 = I_1(\beta_1,\beta_2), I_2 = I_2(\beta_1,\beta_2)$ and $I_3 = \mathrm{Ann}(\beta_1 \times \beta_2)$, then I_1, I_2, I_3 is a net triple of ideals in k. So, the groups $UT_3(k, I_1, I_2, I_3)$ and $UT_3^{(j)}(k, I_1, I_2, I_3, 2)(j = 1, 2)$ are defined. Henceforth these groups will be denoted by $UT_3(k, \beta_1, \beta_2), UT_3^{(j)}(k, \beta_1, \beta_2)$, respectively.

5. Subloops $E^{(1)}(k, \beta_1, \beta_2)$

The preliminary work from the previous two sections makes it possible to formulate and prove the main results of the paper.

Again let k be an associative and commutative ring with 1, and $\beta_1, \beta_2 \in k^3$. Then the ideals $I_1(\beta_1,\beta_2), I_2(\beta_1,\beta_2), \mathrm{Ann}(\beta_1 \times \beta_2)$ that have been introduced in Section 4 can be defined. For short, these are denoted by I_1, I_2, I_3, respectively.

Let $E^{(1)}(k, \beta_1, \beta_2)$ be the set of all elements

$$\big\|\beta_1, \beta_2; s, t, r\big\| = \begin{pmatrix} 1 & s\beta_1 + t\beta_2 \\ r(\beta_1 \times \beta_2) & 1 \end{pmatrix} \in \mathbb{O}(k)(s, t, r \in k).$$

In the present section, whenever the symbol $E^{(1)}$ is used, the set $E^{(1)}(k, \beta_1, \beta_2)$ is meant. A direct calculation shows that $E^{(1)}$ is closed under multiplication:

$$\begin{aligned} &\big\|\beta_1, \beta_2; s_1, t_1, r_1\big\| \, \big\|\beta_1, \beta_2; s_2, t_2, r_2\big\| = \\ &\big\|\beta_1, \beta_2; s_1 + s_2, t_1 + t_2, r_1 + r_2 + s_1 t_2 - s_2 t_1\big\|. \end{aligned} \tag{4}$$

Also $E^{(1)}$ is closed under taking inverses. So $E^{(1)}$ is a subloop of the loop $S(k)$. Moreover, the restriction of multiplication in $\mathbb{O}(k)$ to $E^{(1)}$ is associative. Therefore, $E^{(1)}$ is a subgroup of $S(k)$. Several properties of $E^{(1)}$ are collected in the following proposition.

Proposition 5.1.

(*i*) *The subloop* (*subgroup*) $E^{(1)}(k,\beta_1,\beta_2)$ *is generated by the set* $S^{(1)} = t_{12}(k\beta_1 + k\beta_2)$.

(*ii*) $E^{(1)}(k,\beta_1,\beta_2)$ *contains the normal subgroup* $t_{12}((I_1:2)\beta_1 + I_2\beta_2)$ *which, in turn, is isomorphic to the subgroup* $(I_1:2)\beta_1 + I_2\beta_2$ *of the additive abelian group* $k^3 = (k^3,+)$, *and*

$$E^{(1)}(k,\beta_1,\beta_2)/t_{12}((I_1:2)\beta_1 + I_2\beta_2) \cong UT_3^{(1)}(k,\beta_1,\beta_2).$$

In other words, $E^{(1)}(k,\beta_1,\beta_2)$ *is isomorphic to a group which is an extension of the abelian group* $(I_1:2)\beta_1 + I_2\beta_2 \leqslant (k^3,+)$ *by the group* $UT_3^{(1)}(k,\beta_1,\beta_2)$ *which, in turn, is the subgroup* $UT_3^{(1)}(k,2)G(\sigma)/G(\sigma)$ *of the quotient group* $UT_3(k)$ *by the net subgroup* $G(\sigma)$, *where* σ *is the net*

$$\begin{pmatrix} 0 & I_1 & I_3 \\ 0 & 0 & I_2 \\ 0 & 0 & 0 \end{pmatrix}$$

of ideals in k.

(*iii*) $E^{(1)}(k,\beta_1,\beta_2)$ *is an abelian group if and only if* $2 \in I_3$. *If the subgroup* $E^{(1)}(k,\beta_1,\beta_2)$ *is not abelian, then it is a class-*2 *nilpotent group.*

Proof. (*i*). Denote $H^{(1)}$ the subloop generated by $S^{(1)}$. For any $r \in k$, one has

$$t_{21}(r(\beta_1 \times \beta_2)) = (t_{12}(r\beta_1)t_{12}(\beta_2))t_{12}(-r\beta_1 - \beta_2).$$

This shows that $t_{21}(k(\beta_1 \times \beta_2)) \subseteq H^{(1)}$. Now if $x \in E^{(1)}, x = \left\|\beta_1,\beta_2; s,t,r\right\|$ for some $s,t,r \in k$, then $x = t_{21}(r(\beta_1 \times \beta_2))t_{12}(s\beta_1 + t\beta_2)$, and so $x \in H^{(1)}$. Thus $E^{(1)} \subseteq H^{(1)}$. On the other hand, every element of $S^{(1)}$ lies in $E^{(1)}$, and since $E^{(1)}$ is a subloop, $H^{(1)} \subseteq E^{(1)}$, so $E^{(1)} = H^{(1)}$.

(*ii*). For any $s,t,r \in k$, denote the element $[-2s+I_1, st+r+I_3, -t+I_2] \in UT_3^{(1)}(k,\beta_1,\beta_2)$ by $\chi\big(\left\|\beta_1,\beta_2; s,t,r\right\|\big)$. The condition of equality in $\mathbb{O}(k)$ together with the relations $I_1 \subseteq I_3, I_2 \subseteq I_3$ show that χ is a well defined function from $E^{(1)}$ to $UT_3^{(1)}(k,\beta_1,\beta_2)$. Moreover, χ preserves multiplication and taking inverses. So χ is a group homomorphism. If y is an element

of $UT_3^{(1)}(k,\beta_1,\beta_2)$, $y = [2a + I_1, b + I_3, c + I_2]$, where $a, b, c \in k$, then $\chi\big(\big\|\beta_1,\beta_2;-a,-c,b-ac\big\|\big) = y$. Hence χ is surjective. Using the condition $I_2 \subseteq I_3$, one obtains $\ker\chi = E$, where $E = t_{12}((I_1 : 2)\beta_1 + I_2\beta_2)$. But the mapping $t_{12}(s\beta_1 + t\beta_2) \mapsto s\beta_1 + t\beta_2$, where $s \in (I_1 : 2), t \in I_2$, is an isomorphism of E onto the subgroup $(I_1 : 2)\beta_1 + I_2\beta_2$ of $(k^3, +)$. This proves (ii).

(iii). Suppose that $x = \big\|\beta_1,\beta_2;s_0,t_0,r_0\big\|$ $(s_0,t_0,r_0 \in k)$ is an element of the center $Z(E^{(1)})$ of the subgroup $E^{(1)}$. Then the equation $xt_{12}(\beta_1) = t_{12}(\beta_1)x$ gives $t_0 \in (I_3 : 2)$, whereas the equation $xt_{12}(\beta_2) = t_{12}(\beta_2)x$ gives $s_0 \in (I_3 : 2)$. Conversely, if r_0 is an arbitrary element of k, and $s_0, t_0 \in (I_3 : 2)$, then $ts_0(\beta_1 \times \beta_2) = -ts_0(\beta_1 \times \beta_2)$ for all $t \in k$, and $st_0(\beta_1 \times \beta_2) = -st_0(\beta_1 \times \beta_2)$ for all $s \in k$. It follows that x is permutable with all elements of $E^{(1)}$, and hence

$$\begin{pmatrix} 1 & (I_3 : 2)\beta_1 + (I_3 : 2)\beta_2 \\ k(\beta_1 \times \beta_2) & 1 \end{pmatrix} = Z(E^{(1)}).$$

Thus $E^{(1)}$ is an abelian group if and only if $(I_3 : 2) = k$, that is if and only if $2 \in I_3$.

Now if $i = 1, 2$ and $x_i = \big\|\beta_1,\beta_2;s_i,t_i,r_i\big\|$ $(s_i,t_i,r_i \in k)$, then $x_1^{-1}x_2^{-1}x_1x_2 = t_{21}(2(s_1t_2 - s_2t_1)(\beta_1 \times \beta_2))$. Since the set $t_{21}(2k(\beta_1 \times \beta_2))$ is closed under multiplication and taking inverses, it follows that the commutator subgroup $[E^{(1)}, E^{(1)}]$ of $E^{(1)}$ is contained in $t_{21}(2k(\beta_1 \times \beta_2))$. For any $r \in k$, one has

$$t_{21}(2r(\beta_1 \times \beta_2)) = t_{12}(r\beta_1)^{-1}t_{12}(\beta_2)^{-1}t_{12}(r\beta_1)t_{12}(\beta_2). \tag{5}$$

This shows that $t_{21}(2k(\beta_1 \times \beta_2)) = [E^{(1)}, E^{(1)}]$. Noting that $t_{21}(2k(\beta_1 \times \beta_2))$ is contained in $Z(E^{(1)})$, one concludes that if $E^{(1)}$ is not an abelian group, which is the case exactly when $2 \notin I_3$, then $E^{(1)}$ is a class-2 nilpotent group. This completes the proof of the proposition. □

Remark 5.2. If k is a field of characteristic 2, then $2 = 0$, and hence 2 lies in I_3. Thus in this case $E^{(1)}(k,\beta_1,\beta_2)$ is an abelian group which gives the explanation promised in Introduction.

6. Subloops $E^{(2)}(k,\beta_1,\beta_2)$

Denote by $E^{(2)}(k,\beta_1,\beta_2)$ the set of all $x \in E^{(1)}(k,\beta_1,\beta_2)$ that can be written as $x = \big\|\beta_1,\beta_2;s,t,r\big\|$ with $st + r \in 2k$. In this section, by $E^{(j)}(j = 1, 2)$ the subset $E^{(j)}(k,\beta_1,\beta_2)$ will be understood.

Note that the fact that an element $x \in E^{(1)}$ has a record $x = \|\beta_1, \beta_2; s, t, r\|$ with $st + r \notin 2k$ does not testify yet that $x \notin E^{(2)}$. Indeed, sometimes it is possible to find another representation for x, namely, $x = \|\beta_1, \beta_2; s', t', r'\|$, where $s', t', r' \in k$ are such that $s't' + r' \in 2k$, and therefore $x \in E^{(2)}$.

Example 6.1. Let $k = \mathbb{Z}/18\mathbb{Z}$ and the elements of k are designated as $0' = 0, 1', \ldots, 17'$. Let $\beta_1 = 2'e_1, \beta_2 = e_1 + 3'e_2 \in k^3$, and $x = t_{12}(\beta_1 + \beta_2)$. Here $x = \|\beta_1, \beta_2; s, t, r\|$, where $s = 1', t = 1', r = 0$, and $st + r = 1' \notin 2'k$. However, $\beta_1 \times \beta_2 = 6'e_3$, and hence $3'(\beta_1 \times \beta_2) = \bar{0}$. So $x = \|\beta_1, \beta_2; 1', 1', 3'\|$. Here $s' = 1', t' = 1', r' = 3'$, and $s't' + r' = 4' \in 2'k$ showing $x \in E^{(2)}(k, \beta_1, \beta_2)$.

A criterion on whether or not a given element of $E^{(1)}$ belongs to $E^{(2)}$ can be stated in terms of the ideals $I_j (j \in \{1, 2, 3\})$ and the isomorphism $\overline{\gamma}$ from Section 4 as follows.

Lemma 6.2. *An element $x = \|\beta_1, \beta_2; a, b, c\| \in E^{(1)}(k, \beta_1, \beta_2)$ belongs to $E^{(2)}(k, \beta_1, \beta_2)$ if and only if the cosets $a + I_1, b + I_2, c + I_3$ contain elements $a_0, b_0, c_0 \in k$, respectively, such that*

(*a*) $b_0 - b + \mathrm{Ann}(\beta_2) = \overline{\gamma}(a_0 - a + \mathrm{Ann}(\beta_1))$.

(*b*) $a_0 b_0 + c_0 \in 2k$.

Proof. Suppose that $x \in E^{(2)}$. This means that there exist $a_0, b_0, c_0 \in k$ such that $a_0 b_0 + c_0 \in 2k$ and $x = \|\beta_1, \beta_2; a_0, b_0, c_0\|$. The equality condition in $\mathbb{O}(k)$ gives then that

$$(a_0 - a)\beta_1 + (b_0 - b)\beta_2 = \bar{0}, \tag{6}$$

$$(c_0 - c)(\beta_1 \times \beta_2) = \bar{0}. \tag{7}$$

Equation (7) means that $c_0 - c \in I_3$, whereas by (6) $a_0 - a \in I_1, b_0 - b \in I_2$. Furthemore, the definition of $\overline{\gamma}$ shows that (a) is true. Thus both (a) and (b) hold.

Conversely, suppose that for some $a_0, b_0, c_0 \in k$ such that $a_0 \in a + I_1, b_0 \in b + I_2, c_0 \in c + I_3$, conditions (a) and (b) hold. By the definition of $\overline{\gamma}$, there exists $a_1 \in \mathrm{Ann}(\beta_1), b_1 \in \mathrm{Ann}(\beta_2)$ satisfying $b_0 - b + b_1 \in \gamma(a_0 - a + a_1)$. In other words, $(a_0 - a + a_1)\beta_1 + (b_0 - b + b_1)\beta_2 = \bar{0}$. Since $a_1 \in \mathrm{Ann}(\beta_1), b_1 \in \mathrm{Ann}(\beta_2)$, the latter equation can be rewritten as

$$a_0\beta_1 + b_0\beta_2 = a\beta_1 + b\beta_2. \tag{8}$$

Also the relation $c_0 - c_1 \in I_3$ means that

$$c_0(\beta_1 \times \beta_2) = c(\beta_1 \times \beta_2). \tag{9}$$

Combining (8), (9), yields $x = \big\|\beta_1, \beta_2; a_0, b_0, c_0\big\|$. Since $a_0b_0 + c_0 \in 2k$, the element $\big\|\beta_1, \beta_2; a_0, b_0, c_0\big\|$ lies in $E^{(2)}$. Hence $x \in E^{(2)}$. □

Equation (4) implies that $E^{(2)}$ is closed under multiplication. Moreover, $E^{(2)}$ is closed under taking inverses. Hence $E^{(2)}$ is a subloop of $E^{(1)}$. Some of the properties of $E^{(2)}$ are listed in the following proposition.

Proposition 6.3.

(*i*) *The subloop* $E^{(2)}(k, \beta_1, \beta_2)$ *is generated by* $S^{(2)} = t_{12}(k\beta_1) \cup t_{12}(k\beta_2)$.

(*ii*) *The subloop* $E^{(2)}(k, \beta_1, \beta_2)$ *contains a normal subloop* $t_{12}((I_1 : 2)\beta_1)$ *isomorphic to the abelian group* $(I_1 : 2)\beta_1 \leqslant (k^3, +)$, *and*

$$E^{(2)}(k, \beta_1, \beta_2)/t_{12}((I_1 : 2)\beta_1) \cong UT_3^{(2)}(k, \beta_1, \beta_2).$$

Thus $E^{(2)}(k, \beta_1, \beta_2)$ *is a group which is an extension of the abelian group* $(I_1 : 2) \leqslant (k^3, +)$ *by the group* $UT_3^{(2)}(k, \beta_1, \beta_2)$.

(*iii*) $E^{(2)}(k, \beta_1, \beta_2) = E^{(1)}(k, \beta_1, \beta_2)$ *if and only if for every* $a, b \in k$, *there exist* $a_0 \in a + I_1, b_0 \in b + I_2$ *and* $c_0 \in I_3$ *such that* $b_0 - b + \mathrm{Ann}(\beta_2) = \overline{\gamma}(a_0 - a + \mathrm{Ann}(\beta_1))$ *and* $a_0b_0 + c_0 \in 2k$.

(*iv*) *The subloop* $E^{(2)}(k, \beta_1, \beta_2)$ *is an abelian group if and only if* $2 \in I_3$. *If* $2 \notin I_3$, *then* $E^{(2)}(k, \beta_1, \beta_2)$ *is a class-2 nilpotent group.*

Proof. (*i*). Let $H^{(2)}$ denote the subloop generated by $S^{(2)}$. By (5), $t_{21}(2k(\beta_1 \times \beta_2)) \subseteq H^{(2)}$. Now if $x \in E^{(2)}$, then x can be represented as $\big\|\beta_1, \beta_2; s, t, r\big\|$ with $s, t, r \in k$ such that $st + r \in 2k$. So $t_{21}((st + r)(\beta_1 \times \beta_2)) \in H^{(2)}$. Therefore, $x \in H^{(2)}$ in view of the equality

$$x = \big(t_{21}((st + r)(\beta_1 \times \beta_2))t_{12}(t\beta_2)\big)t_{12}(s\beta_1).$$

Thus $E^{(2)} \subseteq H^{(2)}$. But $S^{(2)} \subseteq E^{(2)}$, and since $E^{(2)}$ is closed under multiplication, $H^{(2)} \subseteq E^{(2)}$. Consequently, $H^{(2)} = E^{(2)}$.

(*ii*). Let χ_0 denote the restriction of the homomorphism χ (see Section 5) to $E^{(2)}$. The definition of χ shows that χ_0 maps $E^{(2)}$ into $UT_3^{(2)}(k, \beta_1, \beta_2)$. If $y = [2a + I_1, 2b_1 + I_3, c + I_2]$ is an element of $UT_3^{(2)}(k, \beta_1, \beta_2)$, then $x = \big\|\beta_1, \beta_2; -a, -c, 2b_1 - ac\big\|$ belongs to $E^{(2)}$. Thus $\chi_0(x)$ is defined and $\chi_0(x) = y$. So χ_0 is a surjective homomorphism of

$E^{(2)}$ onto $UT_3^{(2)}(k, \beta_1, \beta_2)$. Since $\ker \chi = t_{12}((I_1 : 2)\beta_1 + I_2\beta_2)$, it remains to show that

$$t_{12}((I_1 : 2)\beta_1 + I_2\beta_2) \cap E^{(2)} = t_{12}((I_1 : 2)\beta_1). \tag{10}$$

The inclusion $t_{12}((I_1 : 2)\beta_1) \leqslant t_{12}((I_1 : 2)\beta_1 + I_2\beta_2) \cap E^{(2)}$ follows from the definition of $E^{(2)}$. To prove the reverse inclusion suppose that $x \in t_{12}((I_1 : 2)\beta_1 + I_2\beta_2) \cap E^{(2)}$. Since $x \in t_{12}((I_1 : 2)\beta_1 + I_2\beta_2), x = t_{12}(a\beta_1 + b\beta_2)$, where $a \in (I_1 : 2), b \in I_2$. On the other hand, x belongs to $E^{(2)}$ and hence x can be written as $x = \big\|\beta_1, \beta_2; a_0, b_0, c_0\big\|$, where the elements a_0, b_0, c_0 of k are subject to the constraint $a_0b_0 + c_0 \in 2k$. The equality condition in $\mathbb{O}(k)$ gives then

$$(a - a_0)\beta_1 + (b - b_0)\beta_2 = \bar{0}. \tag{11}$$

This means that $b - b_0 \in I_2$ and since $b \in I_2$, one has $b_0 \in I_2$. In turn, the latter means that there exists $a_0' \in k$ with

$$a_0'\beta_1 + b_0\beta_2 = \bar{0}. \tag{12}$$

Adding (11) and (12) yields $(a - a_0 + a_0')\beta_1 + b\beta_2 = \bar{0}$ whence it follows that $b\beta_2 = (-a + a_0 - a_0')\beta_1$, and so $a\beta_1 + b\beta_2 = (a_0 - a_0')\beta_1$. The condition $a \in (I_1 : 2)$ together with equation (11) imply $a_0 \in (I_1 : 2)$. By (12), $a_0' \in I_1$, and therefore $a_0' \in (I_1 : 2)$. So $a_0 - a_0' \in (I_1 : 2)$. Thus $x = t_{12}(a\beta_1 + b\beta_2) = t_{12}((a_0 - a_0')\beta_1) \in t_{12}((I_1 : 2)\beta_1)$. Hence $t_{12}((I_1 : 2)\beta_1 + I_2\beta_2) \cap E^{(2)} \subseteq t_{12}((I_1 : 2)\beta_1)$ and equality (10) is established.

(*iii*). This follows from Lemma 6.2 and Part (*i*) of Proposition 5.1.

(*iv*). Suppose that $E^{(2)}$ is an abelian group. Then, in particular, $t_{12}(\beta_1)t_{12}(\beta_2) = t_{12}(\beta_2)t_{12}(\beta_1)$. It follows that $\beta_1 \times \beta_2 = \beta_2 \times \beta_1$, and hence $2 \in I_3$. On the other hand, if $2 \in I_3$, then $E^{(1)}$ is an abelian group, and hence $E^{(2)} \subseteq E^{(1)}$ is an abelian group too.

Now if $2 \notin I_3$, then the group $E^{(2)}$ is nonabelian, and it is class-2 nilpotent as a nonabelian subgroup of the class-2 nilpotent group $E^{(1)}$. □

7. Further examples

To illustrate the content of Section 6, a few examples are in order.

Example 7.1. If $2 \in k^\times$, then

$$E^{(2)}(k, \beta_1, \beta_2) = E^{(1)}(k, \beta_1, \beta_2). \tag{13}$$

However, it is possible that $2 \notin k^\times$ but (13) still holds. To see this one can consider the situation from Example 6.1. By Part (i) of Proposition 5.1 to establish (13) it is sufficient to show that for all $a, b \in k, t_{12}(a\beta_1 + b\beta_2) \in E^{(2)} = E^{(2)}(k, \beta_1, \beta_2)$. This is certainly true when either $a \in 2'k$ or $b \in 2'k$. Now suppose that $a \notin 2'k$ and $b \notin 2'k$. Then $a, b \in \{0', 1', 3', \ldots, 17'\}$ and hence $ab \in \{0', 1', 3', \ldots, 17'\}$. But then $ab + 3' \in 2'k$, and since $t_{12}(a\beta_1 + b\beta_2) = \left\|\beta_1, \beta_2, a, b, 3'\right\| ; t_{12}(a\beta_1 + b\beta_2) \in E^{(2)}$.

Example 7.2. Most probably, the simplest example of the situation when

$$E^{(2)}(k, \beta_1, \beta_2) \subsetneqq E^{(1)}(k, \beta_1, \beta_2)$$

is that with $k = \mathbb{Z}, \beta_1 = e_1, \beta_2 = e_2$. The family $e_1, e_2, e_1 \times e_2 = e_3$ is a free module basis of $\mathbb{Z}^3$. So every $x \in E^{(1)}(\mathbb{Z}, e_1, e_2)$ can be written uniquely as $x = \left\|e_1, e_2, a, b, c\right\| ; a, b, c \in \mathbb{Z}$. Thus

$$E^{(2)}(\mathbb{Z}, e_1, e_2) =$$
$$\left\{ \left\|e_1, e_2, a, b, c\right\| \mid a, b, c \in \mathbb{Z}, ab + c \text{ is an even integer number} \right\}.$$

So $E^{(2)}(\mathbb{Z}, e_1, e_2) \subsetneqq E^{(1)}(\mathbb{Z}, e_1, e_2)$ because, for instance, $t_{12}(e_1 + e_2)$ does not belong to $E^{(2)}(\mathbb{Z}, e_1, e_2)$. Furthermore, all the ideals $I_1 = I_1(e_1, e_2), I_2 = I_2(e_1, e_2), I_3 = \mathrm{Ann}(e_1 \times e_2)$ are zero. Therefore, using Part (ii) of Proposition 6.3 and the isomorphism from Example 3.1, one has

$$\begin{aligned} E^{(2)}(\mathbb{Z}, e_1, e_2) &\cong UT_3^{(2)}(\mathbb{Z}, e_1, e_2) = \{[2s, 2r, t] \mid s, t, r \in \mathbb{Z}\} \\ &= UT_3^{(2)}(\mathbb{Z}, 2) \cong UT_3(\mathbb{Z}). \end{aligned}$$

By Part (ii) of Proposition 5.1,

$$E^{(1)}(\mathbb{Z}, e_1, e_2) \cong UT_3^{(1)}(\mathbb{Z}, e_1, e_2) = \{[2s, r, t] \mid s, t, r \in \mathbb{Z}\}$$

which is not isomorphic to $UT_3(\mathbb{Z})$. Thus $E^{(1)}(\mathbb{Z}, e_1, e_2)$ and $E^{(2)}(\mathbb{Z}, e_1, e_2)$ are not only distinct but also not isomorphic subloops of $S(\mathbb{Z})$.

8. Some maximal associative subloops of $G(k)$

Along with the subloops $E^{(j)}(k, \beta_1, \beta_2)(j = 1, 2)$ of the loop $S(k)$, the subloops

$$k^\times E^{(j)}(k, \beta_1, \beta_2) = (k^\times 1_2) E^{(j)}(k, \beta_1, \beta_2) =$$
$$\{ax \mid a \in k^\times, x \in E^{(j)}(k, \beta_1, \beta_2)\}$$

of $G(k)$ can be considered. Both of these are associative subloops of $G(k)$, i. e., subgroups of $G(k)$, and $k^\times E^{(j)}(k,\beta_1,\beta_2)$ is isomorphic to the group direct product $k^\times \times E^{(j)}(k,\beta_1,\beta_2)$. An application of Propositions 5.1 and 6.3 shows immediately that the following facts are true.

Proposition 8.1. *The subloop $k^\times E^{(j)}(k,\beta_1,\beta_2)$ is an abelian subgroup if and only if $2 \in \mathrm{Ann}(\beta_1 \times \beta_2)$. If $k^\times E^{(j)}(k,\beta_1,\beta_2)$ is not abelian, that is if $2 \notin \mathrm{Ann}(\beta_1 \times \beta_2)$, then $k^\times E^{(j)}(k,\beta_1,\beta_2)$ is isomorphic to a class-2 nilpotent group.*

The study of $k^\times E^{(1)}(k,\beta_1,\beta_2)$ is interesting in connection with the fact that under some restriction it gives examples of some maximal associative subloops of $G(k)$.

Namely, let $\beta_1, \beta_2 \in k^3$ and

$$\beta_1 = {}^t(b_{11}, b_{21}, b_{31}), \quad \beta_2 = {}^t(b_{12}, b_{22}, b_{32}), \qquad b_{ij} \in k.$$

Then

$$\beta_1 \times \beta_2 = {}^t(b_{21}b_{32} - b_{31}b_{22}, -b_{11}b_{32} + b_{31}b_{12}, b_{11}b_{22} - b_{21}b_{12}).$$

Form the matrix $B = (\beta_1|\beta_2|\beta_1 \times \beta_2)$ whose columns are $\beta_1, \beta_2, \beta_1 \times \beta_2$. In other words,

$$B = \begin{pmatrix} b_{11} & b_{12} & b_{21}b_{32} - b_{31}b_{22} \\ b_{21} & b_{22} & -b_{11}b_{32} + b_{31}b_{12} \\ b_{31} & b_{32} & b_{11}b_{22} - b_{21}b_{12} \end{pmatrix}.$$

If $d = \det B$, then

$$\begin{aligned} d &= (b_{21}b_{32} - b_{31}b_{22})^2 + (-b_{11}b_{32} + b_{31}b_{12})^2 + (b_{11}b_{22} - b_{21}b_{12})^2 \\ &= (\beta_1 \times \beta_2) \cdot (\beta_1 \times \beta_2) = (\beta_1 \cdot \beta_1)(\beta_2 \cdot \beta_2) - (\beta_1 \cdot \beta_2)^2. \end{aligned}$$

Now if f is an element of k, then the set $S = \{f^l \mid l \geqslant 0\}$ is a multiplicatively closed subset of k. So the ring of quotients $S^{-1}k = k_f$ is defined. Note that k_f is nontrivial if and only if f is not nilpotent. In particular, $k_f \neq 0$ when f is not a zero divisor in k.

The following assertion is true.

Proposition 8.2. *Let $\beta_1, \beta_2 \in k^3$. Suppose that $\beta_1, \beta_2, \beta_1 \times \beta_2$ are linearly independent. Let $B = (\beta_1|\beta_2|\beta_1 \times \beta_2)$ and $d = \det B$. If R is any associative and commutative ring with identity that contains k as a subring and such that $d \in R^\times$, then $R^\times E^{(1)}(R,\beta_1,\beta_2) \cap G(k)$ is a maximal associative subloop of $G(k)$ that contains $k^\times E^{(1)}(k,\beta_1,\beta_2)$. Moreover, the intersection $E^{(1)}(R,\beta_1,\beta_2) \cap G(k)$ is isomorphic to the subloop $k_d^\times E^{(1)}(k_d,\beta_1,\beta_2) \cap G(k)$.*

Proof. The assumption on linear independence of $\beta_1, \beta_2, \beta_1 \times \beta_2$ means that d is not a zero divisor of k. Therefore, the collection of all associative and commutative rings K with identity containing k as a subring and such that $d \in K^\times$ is nonempty. It contains, for instance, the ring of quotients k_d. Now if R is any associative and commutative ring with identity containing k as a subring and such that $d \in R^\times$, then the elements $\beta_1, \beta_2, \beta_1 \times \beta_2$ being considered as elements of R^3, form a free module basis of R^3.

Let H be an associative subloop of $G(k)$ such that $k^\times E^{(1)}(k, \beta_1, \beta_2) \leqslant H$ and $x \in H$. Then x can be viewed as an element of $G(R)$. Since $\beta_1, \beta_2, \beta_1 \times \beta_2$ is a free module basis for R^3, x can be written as

$$x = \begin{pmatrix} a_1 & a_2\beta_1 + a_3\beta_2 + a_4(\beta_1 \times \beta_2) \\ a_5\beta_1 + a_6\beta_2 + a_7(\beta_1 \times \beta_2) & a_8 \end{pmatrix}, \quad a_i \in R. \tag{14}$$

Since $t_{12}(\beta_1)$ and $t_{12}(\beta_2)$ belong to $E^{(1)}(k, \beta_1, \beta_2)$, hence to H, one has

$$(t_{12}(\beta_1)t_{12}(\beta_2))x = t_{12}(\beta_1)(t_{12}(\beta_2)x). \tag{15}$$

Explicitly, the left hand side of (15) is equal to

$$\left(\begin{array}{c|c} \begin{array}{c} a_1 + a_5(\beta_1 \cdot \beta_1) + \\ a_5(\beta_1 \cdot \beta_2) + a_6(\beta_2 \cdot \beta_2) + \\ a_6(\beta_1 \cdot \beta_2) \end{array} & \begin{array}{c} a_2\beta_1 + a_3\beta_2 + a_4(\beta_1 \times \beta_2) + \\ a_5(\beta_2 \cdot \beta_1)\beta_1 - a_5(\beta_1 \cdot \beta_1)\beta_2 + \\ a_6(\beta_2 \cdot \beta_2)\beta_1 - a_6(\beta_2 \cdot \beta_1)\beta_2 + \\ a_8\beta_2 + a_8\beta_1 \end{array} \\ \hline \begin{array}{c} a_1(\beta_1 \times \beta_2) + a_2(\beta_2 \times \beta_1) + \\ a_3(\beta_1 \times \beta_2) + a_4(\beta_2 \cdot \beta_2)\beta_1 - \\ a_4(\beta_2 \cdot \beta_1)\beta_2 + a_4(\beta_2 \cdot \beta_1)\beta_1 - \\ a_4(\beta_1 \cdot \beta_1)\beta_2 + a_5\beta_1 + \\ a_6\beta_2 + a_7(\beta_1 \times \beta_2) \end{array} & a_4\big((\beta_1 \times \beta_2) \cdot (\beta_1 \times \beta_2)\big) + a_8 \end{array}\right), \tag{16}$$

and the right hand side of (15) is equal to

$$\left(\begin{array}{c|c} \begin{array}{c} a_1 + a_4(\beta_1 \cdot \beta_1)(\beta_2 \cdot \beta_2) - \\ a_4(\beta_1 \cdot \beta_2)^2 + a_5(\beta_1 \cdot \beta_2) + \\ a_5(\beta_1 \cdot \beta_1) + a_6(\beta_2 \cdot \beta_2) + \\ a_6(\beta_1 \cdot \beta_2) \end{array} & \begin{array}{c} a_2\beta_1 + a_3\beta_2 + \\ a_4(\beta_1 \times \beta_2) + \\ a_8\beta_1 + a_8\beta_2 \end{array} \\ \hline \begin{array}{c} a_2(\beta_2 \times \beta_1) + a_3(\beta_1 \times \beta_2) + \\ a_4(\beta_2 \cdot \beta_2)\beta_1 - a_4(\beta_1 \cdot \beta_2)\beta_2 + \\ a_4(\beta_1 \cdot \beta_2)\beta_1 - a_4(\beta_1 \cdot \beta_1)\beta_2 + \\ a_5\beta_1 + a_6\beta_2 + \\ a_7(\beta_1 \times \beta_2) + a_8(\beta_1 \times \beta_2) \end{array} & a_8 \end{array}\right). \tag{17}$$

Equating elements of k occupying the upper left position in (16) and (17), respectively, one gets $a_4 d = 0$. This implies $a_4 = 0$ since d is an invertible element in R. Taking into account that a_4 is 0 and equating elements of R^3 occupying the right upper position in (16) and (17), respectively, one obtains

$$a_5(\beta_2 \cdot \beta_1)\beta_1 - a_5(\beta_1 \cdot \beta_1)\beta_2 + a_6(\beta_2 \cdot \beta_2)\beta_1 - a_6(\beta_2 \cdot \beta_1)\beta_2 = \bar{0}. \tag{18}$$

Since β_1, β_2 are linearly independent, (18) shows that

$$\begin{aligned} a_5(\beta_2 \cdot \beta_1) + a_6(\beta_2 \cdot \beta_2) &= 0, \\ a_5(\beta_1 \cdot \beta_1) + a_6(\beta_2 \cdot \beta_1) &= 0. \end{aligned}$$

This system of equations, considered as equations in a_5, a_6 as unknowns, has a unique trivial solution because the determinant of its matrix of coefficiens is $-d \in R^\times$. Therefore, equating the elements of R^3 occupying the left lower position in (16) and (17), respectively, yields $a_1(\beta_1 \times \beta_2) = a_8(\beta_1 \times \beta_2)$, whence it follows that $a_1 = a_8$. Thus

$$x = \begin{pmatrix} a_1 & a_2\beta_1 + a_3\beta_2 \\ a_7(\beta_1 \times \beta_2) & a_1 \end{pmatrix} \in R^\times E^{(1)}(R, \beta_1, \beta_2).$$

On the other hand, $x \in H \leqslant G(k)$, and so $x \in R^\times E^{(1)}(R, \beta_1, \beta_2) \cap G(k)$. Thus $H \subseteq R^\times E^{(1)}(R, \beta_1, \beta_2) \cap G(k)$. Since $R^\times E^{(1)}(R, \beta_1, \beta_2)$ is associative, the intersection $R^\times E^{(1)}(R, \beta_1, \beta_2) \cap G(k)$ is an associative subloop too.

Finally, consider the subset R_0 of R of all elements of the form yc^{-1}, where $y \in k$ and c a non-negative integer power of d. Then R_0 is a subring of R, and R_0 is isomorphic to the ring of quotients k_d. Since $\{\beta_1, \beta_2, \beta_1 \times \beta_2\}$ is a free module basis of the free R_0-module R_0^3, the above introduced $x \in H$ belongs to the subloop $G(R_0)$ of the loop $G(R)$, and hence it can be written as

$$x = \begin{pmatrix} a_1' & a_2'\beta_1 + a_3'\beta_2 + a_4'(\beta_1 \times \beta_2) \\ a_5'\beta_1 + a_6'\beta_2 + a_7'(\beta_1 \times \beta_2) & a_8' \end{pmatrix}, \tag{19}$$

where all $a_i' \in R_0$. But $\{\beta_1, \beta_2, \beta_1 \times \beta_2\}$ is a free module basis of R^3 too. So comparing (19) with (14) shows that $a_i' = a_i$ for all $i = 1, 2, \ldots, 8$. In particular, $a_4' = a_5' = a_6' = 0, a_1' = a_8'$, and hence $x \in R_0^\times E^{(1)}(R_0, \beta_1, \beta_2) \cap G(k)$. It follows that $R_0^\times E^{(1)}(R_0, \beta_1, \beta_2) \cap G(k) = R^\times E^{(1)}(R, \beta_1, \beta_2) \cap G(k)$. To complete the proof of the proposition it remains to notice that the subloop $R_0^\times E^{(1)}(R_0, \beta_1, \beta_2)$ of $G(k)$ is isomorphic to $k_d^\times E^{(1)}(k_d, \beta_1, \beta_2)$. □

The proof of Proposition 8.2 admits the following extraction.

Corollary 8.3. *Suppose that $\beta_1, \beta_2 \in k^3$ are such that $\{\beta_1, \beta_2, \beta_1 \times \beta_2\}$ is a free module basis for k^3. Then $k^\times E^{(1)}(k, \beta_1, \beta_2)$ is a maximal associative subloop of the loop $G(k)$.*

The situation when $\beta_1, \beta_2, \beta_1 \times \beta_2$ are not linearly independent is not clear for the author, though the following example shows that Corrollary 8.3 is not true in general.

Example 8.4. Let F be a field and $k = F \oplus F$, the direct sum of two copies of F. Let

$$H = \left\{ \begin{pmatrix} (c_1, c_2) & (c_3, 0)e_1 + (c_4, 0)e_2 + (0, c_5)e_3 \\ (c_6, 0)e_3 & (c_1, c_2) \end{pmatrix} \right\}$$

where $c_1, c_2 \in F^\times, c_3, c_4, c_5, c_6 \in F$ and $\beta_1 = (1, 0)e_1, \beta_2 = (1, 0)e_2$. Then H is a subloop of $G(k)$ that is associative and contains $k^\times E^{(1)}(k, \beta_1, \beta_2)$ properly.

References

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

[2] **E.L. Bashkirov**, *On commutative subloops of the loop of invertible elements in the split octonion algebra over a field of characteristic* 2, Quasigroups Related systems **32** (2024), 2, 191 – 206.

[3] **Z.I. Borevich**, *A description of the subgroups of the complete linear group that contain the group of diagonal matrices*, J. Soviet Math. (1981), 1718 – 1730.

[4] **S. Pumplün**, *A note on Moufang loops arising from octonion algebras over rings*, Beitr. Algebra Geom. **55** (2014), 33-42.

[5] **A. Wells**, *Moufang loops arising from Zorn matrix algebra*, Comment. Math. Univ. Carolin. **51** (2010), no. 2, 371 – 388.

Received October 17, 2025
Revised September 28, 2026

Kalinina str 25, ap. 24
Minsk 220012
Belarus

E-mail: zh.bash@mail.ru bashkirov.e@gmail.com