Two remarks on Lie rings of 2×2 matrices over commutative associative rings

Evgenii L. Bashkirov

Abstract. Let C be an associative commutative ring with 1. If $a \in C$, then aC denotes the principal ideal generated by a. Let l, m, n be nonzero elements of C such that $mn \in lC$. The set of matrices $\left(\begin{smallmatrix} a_{11} & a_{12} \\ a_{21} & -a_{11} \end{smallmatrix}\right)$, where $a_{11} \in lC$, $a_{12} \in mC$, $a_{21} \in nC$, forms a Lie ring under Lie multiplication and matrix addition. The paper studies properties of these Lie rings.

Keywords: Lie ring; associative commutative ring; matrix

Classification: 17B05

1. Introduction and the statement of main results

The present paper is a part of a large project devoted to the classification of Lie rings lying between two given matrix Lie rings over various commutative associative rings. In the course of doing preceding stages of the project, it has been noted, see [2], that some of the laws which govern the structure of matrix Lie rings over a commutative associative ring C with 1 fail when C has a noninvertible element $2 = 1 + 1$, and a Lie ring in question is formed by 2×2 matrices. More generally, these laws are violated when $2C = \{c + c \colon c \in C\}$ is a proper ideal of C (in this case, C may not possess 1). In particular, the subring structure of the Lie ring of traceless 2×2 matrices over such C is, in itself, but little susceptible of analysis. This obstacle leads naturally to the necessity to extend a family of Lie rings under investigation to overcome difficulties thus arising. One of possible ways for such an extension is the consideration of net Lie rings formed by matrices introduced one way or another by several authors under different names in different situations, see for instance [5], [6]. As an application of this concept, the description of Lie rings contained between $sl_2(\mathbb{Z})$ and $sl_2(K)$, K an integral quadratic extension of $\mathbb{Z}$, has been given, see [1]. Thus the class of net Lie rings being a central tool of this description is of importance in itself. For no other reason it is interesting to investigate interior properties of this class, and it is this investigation which is the main purpose of the present paper. Here

DOI 10.14712/1213-7243.2020.010

continuing our study from [1], we develop some further aspects of this concept in the situation where Lie nets consist of principal ideals of the ring C. At first, let us recall the definitions of the concepts mentioned. To this end, it is appropriate to list main notation to be used throughout.

Let Q be a ring. If $A, B \subseteq Q$, then AB is the subset of Q formed by finite sums $\sum a_i b_i$ with $a_i \in A$, $b_i \in B$. Given $q \in Q$, put

$$Aq = \{aq\colon a \in A\}, \qquad qA = \{qa\colon a \in A\}.$$

Also if m is a positive integer, then Am denotes the set of all elements

$$am = \underbrace{a + \cdots + a}_{m \text{ times}},$$

where $a \in A$ (this definition makes sense because we do not insist that Q has an identity element). In the case when Q is a ring with an identity element, Q^* denotes the multiplicative group of invertible elements of Q.

If S is a commutative multiplicative semigroup, and $a, b \in S$, we write $a \mid b$ to express the fact that a divides b, that is, there is $c \in S$ such that $b = ac$.

Given an additive abelian group A and subsets $A_1, A_2, \ldots, A_n$ of A, $n \geq 2$, we define $A_1 + A_2 + \cdots + A_n$ to be the set of the elements $a_1 + a_2 + \cdots + a_n$ with $a_i \in A_i$ for each $i = 1, 2, \ldots, n$.

Returning to our initial commutative associative ring C, we say that a triple $\mathcal{A} = (A_{11}, A_{12}, A_{21})$ of additive subgroups A_{11}, A_{12}, A_{21} of C is a *Lie net* (over C) if

$$2A_{11}A_{12} \subseteq A_{12}, \qquad 2A_{11}A_{21} \subseteq A_{21}, \qquad A_{12}A_{21} \subseteq A_{11}.$$

For this $\mathcal{A}$, the collection $sl_2(\mathcal{A})$ of matrices $\left(\begin{smallmatrix} a_{11} & a_{12} \\ a_{21} & -a_{11} \end{smallmatrix}\right)$ with $a_{ij} \in A_{ij}$ is a Lie ring under usual matrix addition and the operation of Lie multiplication $[a, b] = ab - ba$, where ab denotes the row by column product of a and b. This Lie ring $sl_2(\mathcal{A})$ is termed a *net Lie ring* (corresponding to the Lie net $\mathcal{A}$). If the net Lie ring carries a structure of a module over C, it is called a *net Lie algebra* over C. Notice in passing that if l, m, n are fixed elements of C, then the triple (lC, mC, nC) is a Lie net provided $l \mid mn$ and, moreover, this condition is not only necessary but also sufficient for C possessing an identity element.

The aim of the present paper is to establish two properties of net Lie algebras over a commutative associative ring C with 1. The first property deals with conditions under which two net Lie algebras over C corresponding to Lie nets formed by principal ideals of C are isomorphic provided C is a domain that has a theory of divisors (background related to this concept can be found in [3, Chapter 3]).

Theorem 1.1. *Suppose that a commutative associative ring C is a domain that has a theory of divisors, and let l, m, n, l_1, m_1, n_1 be nonzero elements of C such that $\mathcal{A} = (lC, mC, nC)$, $\mathcal{A}_1 = (l_1C, m_1C, n_1C)$ are Lie nets. Then the net Lie C-algebras $sl_2(\mathcal{A})$ and $sl_2(\mathcal{A}_1)$ are isomorphic if and only if $l_1 = l\varepsilon$, $m_1n_1 = mn\eta$ for some $\varepsilon, \eta \in C^*$.*

Our second result is concerned with the number of matrices that generate the net Lie C-algebra $sl_2(lC, mC, nC)$ provided m, n are not zero divisors in a commutative associative ring C with 1. The result asserts that this number can be determined by means of solving a quadratic congruence equation. More precisely, we have:

Theorem 1.2. *Let C be an arbitrary commutative associative ring with 1, and let $l, m, n \in C$ be such that m, n are not zero divisors in C and $mn = lq$ for some $q \in C$. Then the net Lie C-algebra $sl_2(lC, mC, nC)$ is generated by two matrices if and only if the following two conditions are satisfied:*

(G1) $qC + 4lC = C$.
(G2) *For some $u \in C^*$, the congruence equation*

$$x^2 \equiv uq \pmod{4lC} \tag{1.1}$$

has a solution within C.

Specializing C to the ring of integers $\mathbb{Z}$ and recalling the necessary and sufficient conditions for the quadratic congruence equation $x^2 \equiv \pm q \pmod{4l}$, $q, l \in \mathbb{Z}$, to have a solution, see [4, Proposition 5.1.1], we make use of Theorem 1.2 to obtain the following rather curious criterion, in terms of the Jacobi symbol $(\frac{a}{b})$, [4, page 56], for the net Lie ring $sl_2(l\mathbb{Z}, m\mathbb{Z}, n\mathbb{Z})$ to be generated by two matrices.

Theorem 1.3. *Let l, m, n be positive integers such that $l \mid mn$. Let $q = mn/l$ and $4l = 2^\alpha p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, where $p_1, p_2, \dots, p_k$ are distinct odd primes and all α_i are positive integers. The net Lie ring $sl_2(l\mathbb{Z}, m\mathbb{Z}, n\mathbb{Z})$ is generated by two matrices if and only if q is an odd number relatively prime to l, and one of the following conditions holds:*

(Z1) $\alpha = 2$, $q \equiv 1 \pmod 4$, $(\frac{q}{p_i}) = 1$ *for all* $i = 1, 2, \dots, k$.
(Z2) $\alpha \geq 3$, $q \equiv 1 \pmod 8$, $(\frac{q}{p_i}) = 1$ *for all* $i = 1, 2, \dots, k$.
(Z3) $\alpha = 2$, $q \equiv 3 \pmod 4$, $(\frac{p_i}{q}) = 1$ *for all* $i = 1, 2, \dots, k$.
(Z4) $\alpha \geq 3$, $q \equiv 7 \pmod 8$, $(\frac{p_i}{q}) = 1$ *for all* $i = 1, 2, \dots, k$.

In Section 5, we use Theorem 1.3 to provide a source of examples illustrating Theorem 1.2.

2. Restatements of the results

In this section, we slightly formalize the Lie algebras under investigation to arrive at more convenient forms of the formulations of Theorems 1.1 and 1.2 as well as of their proofs.

Namely, let C be a commutative associative ring, and let M be a left free C-module with free basis of three elements a_0, a_+, a_-. By this we mean that every element of M can be uniquely written as $c_1a_0 + c_2a_+ + c_3a_-$ with $c_i \in C$. Let l, q be fixed elements of C. Define products of a_0, a_+, a_- by

(2.1)

	a_0	a_+	a_-
a_0	0	$2la_+$	$-2la_-$
a_+	$-2la_+$	0	qa_0
a_-	$2la_-$	$-qa_0$	0

and extend this by linearity to the whole of M. This makes M into a C-algebra which is denoted by $\mathfrak{l}(l, q)$, the ordered basis $\{a_0, a_+, a_-\}$ being called the *standard basis* of $\mathfrak{l}(l, q)$. Clearly $x^2 = 0$ for all $x \in \mathfrak{l}(l, q)$. Moreover,

$$(a_0a_+)a_- + (a_+a_-)a_0 + (a_-a_0)a_+ = 0.$$

This shows that $\mathfrak{l}(l, q)$ is a Lie algebra over C, and henceforth the operation of multiplication on any $\mathfrak{l}(l, q)$ is designated by Lie brackets $[x, y]$. Furthermore, let m, n be elements of C such that $mn = lq$ (these always do exist for one can put $m = l, n = q$), and suppose that m, n are not zero divisors in C. Then the Lie C-algebra $\mathfrak{s} = sl_2(lC, mC, nC)$ exists, the elements l, q are also not zero divisors and the matrices

$$\begin{pmatrix} l & 0 \\ 0 & -l \end{pmatrix}, \qquad \begin{pmatrix} 0 & m \\ 0 & 0 \end{pmatrix}, \qquad \begin{pmatrix} 0 & 0 \\ n & 0 \end{pmatrix} \tag{2.2}$$

form a free basis of $\mathfrak{s}$ as a module over C. By inspection, the table for Lie multiplication of (2.2) is exactly the same as (2.1). In other words, the Lie C-algebras $sl_2(lC, mC, nC)$ and $\mathfrak{l}(l, q)$ are isomorphic, and in order to demonstrate Theorems 1.1 and 1.2 it is enough to proof the following two assertions.

Proposition 2.1. *Let C be a domain that has a theory of divisors, and let l, q, l_1, q_1 be nonzero elements of C. Then the Lie C-algebras $\mathfrak{l}(l, q)$, $\mathfrak{l}(l_1, q_1)$ are isomorphic if and only if $l_1 = l\varepsilon$, $q_1 = q\eta$ for some $\varepsilon, \eta \in C^*$.*

Proposition 2.2. *Let C be a commutative associative ring with 1, and $l, q \in C$ are not zero divisors. Then the Lie C-algebra $\mathfrak{l}(l, q)$ is generated by two elements if and only if conditions* (G1), (G2) *are satisfied.*

3. Proof of Proposition 2.1

That $\mathfrak{l}(l\varepsilon, q\eta) \cong \mathfrak{l}(l, q)$ for all $\varepsilon, \eta \in C^*$ is quite evident.

Conversely, let us suppose that $\mathfrak{l}(l, q) \cong \mathfrak{l}(l_1, q_1)$, and let $\varphi\colon \mathfrak{l}(l_1, q_1) \to \mathfrak{l}(l, q)$ be an isomorphism. Choosing standard bases $\{a_0, a_+, a_-\}$, $\{b_0, b_+, b_-\}$ for $\mathfrak{l}(l, q)$, $\mathfrak{l}(l_1, q_1)$, respectively, we put

$$\begin{aligned} \varphi(b_0) &= a_1 a_0 + a_2 a_+ + a_3 a_-, \\ \varphi(b_+) &= b_1 a_0 + b_2 a_+ + b_3 a_-, \\ \varphi(b_-) &= c_1 a_0 + c_2 a_+ + c_3 a_-, \qquad a_i, b_i, c_i \in C,\ 1 \le i \le 3. \end{aligned} \tag{3.1}$$

Since φ is a C-linear map preserving multiplication,

$$[\varphi(b_0), \varphi(b_\pm)] = \pm 2 l_1 \varphi(b_\pm), \qquad [\varphi(b_+), \varphi(b_-)] = q_1 \varphi(b_0),$$

and in view of (3.1), we get

$$q(a_2 b_3 - a_3 b_2) = 2 l_1 b_1, \tag{3.2}$$

$$l(a_1 b_2 - a_2 b_1) = l_1 b_2, \tag{3.3}$$

$$l(a_3 b_1 - a_1 b_3) = l_1 b_3, \tag{3.4}$$

$$q(a_3 c_2 - a_2 c_3) = 2 l_1 c_1, \tag{3.5}$$

$$l(a_2 c_1 - a_1 c_2) = l_1 c_2, \tag{3.6}$$

$$l(a_1 c_3 - a_3 c_1) = l_1 c_3, \tag{3.7}$$

$$q(b_2 c_3 - b_3 c_2) = q_1 a_1, \tag{3.8}$$

$$2l(b_1 c_2 - b_2 c_1) = q_1 a_2, \tag{3.9}$$

$$2l(b_3 c_1 - b_1 c_3) = q_1 a_3. \tag{3.10}$$

The requirement C to have a theory of divisors means that we are given a commutative semigroup $\mathfrak{D}$, with identity $\mathfrak{e}$, and with unique factorization such that there is a homomorphism $\alpha \to (\alpha)$ of the semigroup $C \setminus \{0\}$ into $\mathfrak{D}$ satisfying, among others, the following conditions:

(1) $\alpha \in C \setminus \{0\}$ is divisible by $\beta \in C \setminus \{0\}$ (in C) if and only if (α) is divisible by (β) in $\mathfrak{D}$.

(2) If $\alpha, \beta \in C$ are divisible by $\mathfrak{a} \in \mathfrak{D}$, then $\alpha \pm \beta$ are also divisible by $\mathfrak{a}$.

(See [3, page 178].)

Applying the homomorphism $\alpha \to (\alpha)$ to (3.3) shows that

$$(l)((a_1 b_2 - a_2 b_1)) = (l_1)(b_2).$$

Since $\mathfrak{D}$ is a unique factorization semigroup, (l) and (l_1) have a greatest common divisor which we denote by $\mathfrak{d}$. Thus $(l) = \mathfrak{a}\mathfrak{d}$, $(l_1) = \mathfrak{a}_1\mathfrak{d}$ for some $\mathfrak{a}, \mathfrak{a}_1 \in \mathfrak{D}$, and hence $\mathfrak{a}\mathfrak{d}((a_1b_2-a_2b_1))=\mathfrak{a}_1\mathfrak{d}(b_2)$, or after cancelling $\mathfrak{d}$, $\mathfrak{a}((a_1b_2-a_2b_1))=\mathfrak{a}_1(b_2)$. It follows that $\mathfrak{a}$ divides the product $\mathfrak{a}_1(b_2)$, and since $\mathfrak{a}$ and $\mathfrak{a}_1$ are relatively prime, $\mathfrak{a}$ must divide (b_2), or in other words, $\mathfrak{a}$ divides b_2. Similarly, (3.4), (3.6), (3.7) imply that $\mathfrak{a}$ divides b_3, c_2, c_3. Therefore, using row 1 to expand the determinant

$$D=\begin{vmatrix} a_1 & b_1 & c_1\\ a_2 & b_2 & c_2\\ a_3 & b_3 & c_3\end{vmatrix}, \tag{3.11}$$

and employing condition (2) imposing on the theory of divisor, we conclude that $\mathfrak{a}$ divides D. On the other hand, D is the determinant of the matrix of the isomorphism φ relative to the ordered free bases

$$\{b_0, b_+, b_-\}, \qquad \{a_0, a_+, a_-\},$$

and so $D\in C^*$. This implies that (D) is the unit element $\mathfrak{e}\in\mathfrak{D}$ and hence $(l)=\mathfrak{d}$. Since $l_1=\mathfrak{a}_1\mathfrak{d}$, we see that (l) divides (l_1) which by (1) amounts to saying $l\mid l_1$.

A similar reasoning being applied to the inverse isomorphism $\varphi^{-1}\colon \mathfrak{l}(l,q)\to\mathfrak{l}(l_1,q_1)$ yields $l_1\mid l$, and hence $l_1=l\varepsilon$ for some $\varepsilon\in C^*$. So $\mathfrak{l}(l_1,q_1)=\mathfrak{l}(l\varepsilon,q_1)$, and since $\mathfrak{l}(l\varepsilon,q_1)\cong\mathfrak{l}(l,q_1)$, one may assume $l=l_1$. Then (3.3), (3.4), (3.6), (3.7) give

$$\begin{aligned} b_2&=a_1b_2-a_2b_1,\\ b_3&=a_3b_1-a_1b_3,\\ c_2&=a_2c_1-a_1c_2,\\ c_3&=a_1c_3-a_3c_1,\end{aligned} \tag{3.12}$$

and so

$$b_2c_3-b_3c_2=a_1D,$$

where D is determined in (3.11). Thus (3.8) becomes

$$qa_1D=q_1a_1. \tag{3.13}$$

If $a_1\neq 0$, (3.13) implies that $q\mid q_1$. Suppose that $a_1=0$. Then equations (3.12) become

$$b_2=-a_2b_1, \qquad b_3=a_3b_1, \qquad c_2=a_2c_1, \qquad c_3=-a_3c_1,$$

and so (3.2) shows that $qa_2a_3b_1=lb_1$, whereas by (3.5), $qa_2a_3c_1=lc_1$. According to the bijectivity of φ, at least one of b_1, c_1 must be nonzero (because $a_1=0$), and hence $l=qa_2a_3$. Substituting this result in (3.9) and (3.10), we arrive at

$$4qa_2^2a_3b_1c_1=q_1a_2, \tag{3.14}$$

$$4qa_2a_3^2b_1c_1=q_1a_3, \tag{3.15}$$

respectively. Again, since $a_1 = 0$, either $a_2 \neq 0$ or $a_3 \neq 0$ and therefore, either (3.14) or (3.15) shows that $q \mid q_1$ and thus this relation holds in any case. The consideration of φ^{-1} gives $q_1 \mid q$, whence $q_1 = q\eta$ for some $\eta \in C^*$.

4. Proof of Proposition 2.2

We begin with several preliminary observations.

Let R be an associative ring with involution J. Let C be the set of J-symmetric elements of R, $C = \{x \in R\colon x^J = x\}$, and L the set of J-skew elements of R, $L = \{x \in R\colon x^J = -x\}$. Suppose that C is contained in the center of R, and therefore, C is a commutative subring of R. The Lie subring L of R can and will be treated as a Lie algebra over C (relative to the Lie multiplication $[a,b] = ab - ba$, $a, b \in L$).

Lemma 4.1. *The subalgera N of the Lie C-algebra L generated by two elements $a, b \in L$ equals to*

$$T = Ca + Cb + C \cdot [a,b] + \mathbb{Z}a + \mathbb{Z}b + \mathbb{Z} \cdot [a,b].$$

Proof: The relations a, b, $[a,b] \in N$ imply $T \subseteq N$. On the other hand, for any $l \in L$, $l^2 = -ll^J$ lies in the center of R and therefore, $[a,[a,b]] = 2a^2b - 2aba$. Further, $aba = (ab + (ab)^J)a + (aa^J)b$ which shows that $[a,[a,b]] \in T$. Interchanging a and b yields $[b,[a,b]] \in T$, and thus T is a subalgebra of the Lie C-algebra L. Since N is the intersection of all subalgebras of L that contain a, b, we obtain $N \subseteq T$, whence $N = T$. $\square$

Now we specialize R and J. Namely, let R be the associative ring $M_2(C)$ of $2{\times}2$ matrices over a commutative associative ring C, and J be the symplectic involution on $M_2(C)$:

$$\begin{pmatrix} x & y \\ z & t \end{pmatrix}^J = \begin{pmatrix} t & -y \\ -z & x \end{pmatrix}, \qquad x, y, z, t \in C.$$

Then L is interpreted as the Lie C-algebra $sl_2(C)$ formed by all matrices of $M_2(C)$ with trace 0, and Lemma 4.1 can be restated as follows.

Lemma 4.2. *The subalgebra N of the C-algebra $sl_2(C)$ generated by two matrices $a, b \in sl_2(C)$ coincides with*

$$Ca + Cb + C \cdot [a,b] + \mathbb{Z}a + \mathbb{Z}b + \mathbb{Z} \cdot [a,b].$$

If C contains 1, then $N = Ca + Cb + C \cdot [a,b]$.

Now we are ready to prove Proposition 2.2.

Proof of Proposition 2.2: Choose a standard basis a_0, a_+, a_- of $\mathfrak{l}(l,q)$. Suppose that $\mathfrak{l}(l,q)$ is generated by two elements

$$a = a_1a_0 + a_2a_+ + a_3a_-, \qquad b = b_1a_0 + b_2a_+ + b_3a_-.$$

The coefficient of a_- in any element of the subalgebra generated by a, b belongs to the ideal $I = Ca_3 + Cb_3$ of the ring C. This shows that $I = C$, and so $z_1a_3 + z_2b_3 = 1$ for some $z_1, z_2 \in C$. Therefore, one may replace the pair a, b by $z_1a + z_2b, -b_3a + a_3b$ and assume from the very beginning that $a_3 = 1$, $b_3 = 0$. Viewing a_0, a_+, a_- as the matrices (2.2) of $M_2(C)$ (it is this place in which we use the assumption that l, q are not zero divisors), we use Lemma 4.2 to conclude that the elements

$$\begin{aligned} a &= a_1a_0 + a_2a_+ + a_-, \\ b &= b_1a_0 + b_2a_+, \\ [a,b] &= -qb_2a_0 + 2l(a_1b_2 - a_2b_1)a_+ + 2lb_1a_- \end{aligned} \tag{4.1}$$

generate C-module $\mathfrak{l}(l,q)$ and hence form a basis of it. It follows that the determinant of the transition matrix from the ordered basis $\{a_0, a_+, a_-\}$ to the ordered system (4.1) lies in C^*, or explicitly,

$$4lb_1(a_1b_2 - a_2b_1) + qb_2^2 = u, \tag{4.2}$$

where $u \in C^*$. This shows at once that condition (G1) holds. Moreover, according to (4.2), $qb_2^2 \equiv u \pmod{4lC}$ which implies $(qb_2)^2 \equiv uq \pmod{4lC}$.

Now let us assume that (G1) and (G2) are valid. So the congruence equation (1.1) has a solution for some $u \in C^*$. Call this solution x_0 and note that condition (G1) implies that the image of q under the canonical epimorphism $C \to C/(4lC)$ is an invertible element of the quotient ring $C/(4lC)$. Hence $q(q^{-1}x_0)^2 \equiv u \pmod{4lC}$ and denoting $q^{-1}x_0$ by b_2, we get $qb_2^2 + 4lb_1 = u$ for some $b_1 \in C$. This shows that $b_1C + b_2C = C$, and therefore one can find $a_1, a_2 \in C$ such that $a_1b_2 - a_2b_1 = 1$. This yields

$$u = qb_2^2 + 4lb_1 \cdot 1 = \begin{vmatrix} a_1 & b_1 & -qb_2 \\ a_2 & b_2 & 2l \\ 1 & 0 & 2lb_1 \end{vmatrix},$$

which, in turn, means that the elements

$$g = a_1a_0 + a_2a_+ + a_-, \qquad h = b_1a_0 + b_2a_+, \qquad f = -qb_2a_0 + 2la_+ + 2lb_1a_-$$

form a basis of the C-module $\mathfrak{l}(l,q)$. But $[g,h] = f$, and so g and h generate $\mathfrak{l}(l,q)$ as a Lie C-algebra. $\square$

5. Examples

This section is devoted to several examples illustrating Proposition 2.2 and Theorem 1.2.

Example 5.1. First of all, it is worthwhile to note that if C is an associative commutative ring with 1 and this 1 is taken as q, then both conditions (G1), (G2) of Theorem 1.2 are obviously true. This completely agrees with the evident fact that the Lie C-algebra $sl_2(mnC, mC, nC)$ is generated by the matrices

$$\begin{pmatrix} 0 & m \\ 0 & 0 \end{pmatrix}, \qquad \begin{pmatrix} 0 & 0 \\ n & 0 \end{pmatrix}.$$

Example 5.2. This series of examples addresses the ring $C = \mathbb{Z}$, where one can refer to Lie rings rather than Lie C-algebras. Here we refer to conditions (Z1)–(Z4) from Theorem 1.3.

Certainly the elementary theory of congruence equations implies that all of the possibilities (Z1)–(Z4) can be realized, thus giving Lie rings $\mathfrak{l}(l, q)$, $l, q \in \mathbb{Z}$ generated by two elements. For concreteness, each of the Lie rings

$$\mathfrak{g}_1 = \mathfrak{l}(3^2, 5\cdot 17), \qquad \mathfrak{g}_2 = \mathfrak{l}(2^2\cdot 5, 3^2), \qquad \mathfrak{g}_3 = \mathfrak{l}(29\cdot 37, 7), \qquad \mathfrak{g}_4 = \mathfrak{l}(2\cdot 29\cdot 37, 7),$$

is generated by two elements because $\mathfrak{g}_i$ satisfies (Zi). For instance, using the process described in the second part of the Proposition 2.2 proof, one can find that $\mathfrak{g}_1$ is generated by $366a_0 - 5a_+ + a_-$, $-2269a_0 + 31a_+$, where $\{a_0, a_+, a_-\}$ means a standard basis for $\mathfrak{g}_1$.

On the other hand, let us take $l = 2 \cdot 29 \cdot 31 \cdot 37$, $q = 7$. Here $\left(\frac{31}{7}\right) = -1$, and so condition (Z4) does not hold. Further, conditions (Z1), (Z3) are not satisfied because $\alpha = 3$, and (Z2) is not valid for $q \not\equiv 1 \pmod 8$. Thus though l, q are relatively prime, the corresponding Lie ring $\mathfrak{l}(l, q)$ cannot be generated by two elements.

Now $\mathfrak{g}_5 = \mathfrak{l}(6, 2)$, $\mathfrak{g}_6 = \mathfrak{l}(5 \cdot 7, 3^2 \cdot 5)$ are not generated by two elements since for $\mathfrak{g}_5$, $q = 2$, is even, while in the case of $\mathfrak{g}_6$, $l = 5 \cdot 7$ and $q = 3^2 \cdot 5$ are not relatively prime.

Translating the aforementioned examples into the language of matrices, we obtain that the Lie rings

$$sl_2(9\mathbb{Z}, 15\mathbb{Z}, 51\mathbb{Z}), \qquad sl_2(20\mathbb{Z}, 12\mathbb{Z}, 15\mathbb{Z}), \qquad sl_2(29 \cdot 37\mathbb{Z}, 7 \cdot 29\mathbb{Z}, 37\mathbb{Z}),$$
$$sl_2(2 \cdot 29 \cdot 37\mathbb{Z}, 7 \cdot 29\mathbb{Z}, 2 \cdot 37\mathbb{Z})$$

are generated by two matrices, whereas

$$sl_2(2 \cdot 29 \cdot 31 \cdot 37\mathbb{Z}, 7 \cdot 29\mathbb{Z}, 2 \cdot 31 \cdot 37\mathbb{Z}),$$
$$sl_2(6\mathbb{Z}, 3\mathbb{Z}, 4\mathbb{Z}), \qquad sl_2(5 \cdot 7\mathbb{Z}, 3 \cdot 5^2\mathbb{Z}, 3 \cdot 7\mathbb{Z})$$

are not.

Example 5.3. Letting C be the ring $\mathbb{Q}[\lambda]$ of polynomials in the indeterminate λ with coefficients from the field $\mathbb{Q}$ of rational numbers, we take $l = \lambda^2 - 2$, $q = \lambda$. Since $2 \in C^*$, condition (G1) is reduced to $qC + lC = C$ which is evidently true, whereas (1.1) becomes $x^2 \equiv u\lambda \pmod{(\lambda^2 - 2)C}$, where u is a rational number. However, this congruence equation has no solution within C because for any rational u, $u\sqrt{2}$ is not a square in the field $\mathbb{Q}(\sqrt{2})$. Thus the Lie C-algebra $\mathfrak{l}(\lambda^2 - 2, \lambda)$ is not generated by two elements.

References

[1] Bashkirov E. L., *On a class of Lie rings of* 2×2 *matrices over associative commutative rings*, Linear Multilinear Algebra **67** (2019), no. 3, 456–478.

[2] Bashkirov E. L., Pekönür E., *On matrix Lie rings over a commutative ring that contain the special linear Lie ring*, Comment. Math. Univ. Carolin. **57** (2016), no. 1, 1–6.

[3] Borevich, A. I., Shafarevich I. R., *Number Theory*, Pure and Applied Mathematics, 20, Academic Press, New York, 1966.

[4] Ireland K., Rosen M., *A Classical Introduction to Modern Number Theory*, Graduate Texts in Mathematics, 84, Springer, New York, 1990.

[5] Koibaev V. A., Nuzhin Ya. N., *Subgroups of Chevalley groups and Lie rings of definable by a collection of additive subgroups of the original ring*, Fundam. Prikl. Mat. **18** (2013), no. 1, 75–84 (Russian. English, Russian summary); translated in J. Math. Sci. (NY) **201** (2014), no. 4, 458–464.

[6] Nuzhin Ya. N., *Lie rings defined by the root system and family of additive subgroups of the initial ring*, Proc. Steklov Inst. Math. **283** (2013), suppl. 1, S119–S125.

E. L. Bashkirov:

United Arab Emirates University, P. O. Box 15551, Al Ain, Abu Dhabi, United Arab Emirate

E-mail: zh.bash@mail.ru

(*Received* November 21, 2018, *revised* March 5, 2019)