BIRKHÄUSER

A.I. Shirshov

Contemporary Mathematicians

Gian-Carlo Rota[†]
Joseph P.S. Kung

Editors

Selected Works of A.I. Shirshov

Leonid A. Bokut
Victor Latyshev
Ivan Shestakov
Efim Zelmanov
Editors

Translated by
Murray Bremner and Mikhail V. Kotchetov

Birkhäuser
Basel · Boston · Berlin

Editors:

Leonid Bokut
Sobolev Institute of Mathematics
Koptyuga, 4
630090, Novosibirsk
Russia

Victor Latyshev
Mehmat
MGU im. Lomonosova
Vorob'evy Gory
119899 Moscow
Russia

Ivan Shestakov
IME-USP
Ruodo Matao, 1010
Cidade Universitaria
CEP 05508-090
Sao Paulo
SP, Brasil

Efim Zelmanov
Dep. of Mathematics
UCSD
9500 Gilman Drive # 0112
La Jolla, CA 92093-0112
USA

Translators:

Murray Bremner
University of Saskatchewan
Dept. Mathematics & Statistics
106 Wiggins Road
Saskatoon SK S7N 5E6
Canada

Mikhail V. Kotchetov
Department of Mathematics and Statistics
Memorial University of Newfoundland
St. John's, NL A1C 5S7
Canada

Library of Congress Control Number: 2009925469

Bibliographic information published by Die Deutsche Bibliothek
Die Deutsche Bibliothek lists this publication in the Deutsche Nationalbiographie;
detailed bibliographic data is available in the internet at http://dnb.ddb.de

ISBN 978-3-7643-8857-7 Birkhäuser Verlag, Basel – Boston – Berlin

Photo on page iii: From the family archive. With the friendly permission of Shirshov's daughter Trofimova Nina Anatolevna.

Printed on acid-free paper produced from chlorine-free pulp. TCF ∞
Printed in Germany

ISBN 978-3-7643-8857-7 e-ISBN 978-3-7643-8858-4

9 8 7 6 5 4 3 2 1 www.birkhauser.ch

Contents

Commentaries

Preface

Anatolii Illarionovich Shirshov (1921–1981) was an outstanding Russian mathematician whose works essentially influenced the theories of associative, Lie, Jordan and alternative rings. Many Shirshov's students and students of his students had a successful research career in mathematics.

Anatolii Shirshov was born on the 8th of August of 1921 in the village Kolyvan near Novosibirsk. Before the II World War he started to study mathematics at Tomsk university but then went to the front to fight as a volunteer. In 1946 he continued his study at Voroshilovgrad (now Lugansk) Pedagogical Institute and at the same time taught mathematics at a secondary school. In 1950 Shirshov was accepted as a graduate student at the Moscow State University under the supervision of A.G. Kurosh. In 1953 he has successfully defended his Candidate of Science thesis (analog of a Ph.D.) "Some problems in the theory of nonassociative rings and algebras" and joined the Department of Higher Algebra at the Moscow State University. In 1958 Shirshov was awarded the Doctor of Science degree for the thesis "On some classes of rings that are nearly associative".

In 1960 Shirshov moved to Novosibirsk (at the invitations of S.L. Sobolev and A.I. Malcev) to become one of the founders of the new mathematical institute of the Academy of Sciences (now Sobolev Institute of Mathematics) and to help the formation of the new Novosibirsk State University. From 1960 to 1973 he was a deputy director of the Institute and till his last days he led the research in the theory of algebras at the Institute.

The present collection contains English translations (by M. Bremner and M. Kochetov) of all the published scientific works of A.I. Shirshov with the exception of his book Rings that are nearly associative, Moscow: Nauka, 1978 (with K.A. Zhevlakov, A.M. Slinko and I.P. Shestakov) (translated by H.F. Smith, New York: Academic Press, 1982) and some articles whose content is included in later more extensive publications. The works are ordered chronologically.

The volume also includes commentaries on the works of Shirshov written (largely) by his students.

We are grateful to Bernd Wegner for his support and encouragement and to Karin Neihart for her invaluable help.

February 2009

L.A. Bokut, V. Latyshev
I.P. Shestakov, E.I. Zelmanov

Publications of A.I. Shirshov

Subalgebras of Free Lie Algebras

A.I. Shirshov

1. Introduction

In the work of A.G. Kurosh [2] it is proved that every subalgebra of a free nonassociative algebra is free. It would be natural to investigate the possibility of transferring this theorem to the most important classes of relatively free algebras whose general definition was given in the work of A.I. Malcev [3].

The widest class of such algebras that includes all classes of algebras that have been studied sufficiently deeply is the class of power associative algebras, i.e., the algebras in which each element generates an associative subalgebra. However, the corresponding theorem for this class of algebras is false, because the free associative algebra with one generator already contains subalgebras that are not free (see A.G. Kurosh [2]). For the same reason, this theorem does not hold for Jordan algebras, for alternative algebras, and also for right or left alternative algebras. It is not difficult to convince oneself that this theorem does not hold for power-commutative or flexible algebras either, for reasons similar to those stated above.

These considerations, however, are not valid for free Lie algebras, since in them a single element generates a one-dimensional subspace with zero multiplication, for which the theorem on subalgebras holds trivially. In the present work, it is proved that every subalgebra of every free Lie algebra is free.

This work was carried out under the supervision of A.G. Kurosh, to whom I find it my pleasant duty to express deep gratitude.

2. Preliminary concepts

Let $R = \{a_\alpha\}$ be a set of symbols where α ranges over some nonempty set of indices. From elements of R one can form nonassociative words of various lengths as is done in the work of A.G. Kurosh [2].

Mat. Sbornik N.S. 33 (75), (1953), no. 2, 441–452.

Definition 1. We will call words of length 1, i.e., elements of R, *regular words*, and we will order them arbitrarily. Assuming that regular words of length less than n, $n > 1$, are already defined and ordered by the relation $\leq$ in such a way that shorter words precede longer words, we call a word w of length n *regular* if the following conditions are satisfied:

1) $w = uv$ where u and v are regular words and $u > v$;
2) if $u = u_1 u_2$ then $u_2 \leq v$.

We will order arbitrarily the regular words of length n defined in this way, and declare that they are greater than shorter words.

Definition 2. Suppose we have a regular word d. We will call a regular word w, $w > d$, *d-reducible* if $w = uv$, $v > d$, and *d-irreducible* otherwise.

Obviously, for each regular word w, $w > d$, one can determine if it is d-reducible or d-irreducible. If it turns out that w is d-reducible, then $w = uv$ where each word u, v is regular and greater than d, and thus one can determine if each is d-reducible or d-irreducible. Continuing this process, we will clearly arrive at a unique representation of the word w as a product (with some arrangement of brackets) of d-irreducible words. We will call this representation a *d-factorization* of w.

Definition 3. We will say that two nonassociative words u and v *have the same content relative to* R if each element $a_\alpha \in R$ occurs in u and v the same number of times.

Clearly, the words that have the same content relative to R also have the same length.

Let $\mathcal{A}$ be a free Lie algebra over a field P with the same set R of free generators. The elements of $\mathcal{A}$ are linear combinations of nonassociative words formed from elements of R with coefficients from the field P; in this case, two elements are considered equal if one can be obtained from the other by a finite number of applications of the distributive laws and the identical relations:

$$x^2 = 0, \tag{1}$$

$$(xy)z + (yz)x + (zx)y = 0, \tag{2}$$

or identical transformations in the additive group.

Hall [1] proved:

Theorem 1. *Regular words, for any fixed choice of ordering in the definition, form a basis of the algebra $\mathcal{A}$.*

The proof of this theorem can found in the cited work of Hall. (It is easy to see that Hall's assumption of finiteness of the number of generators of the algebra $\mathcal{A}$ is not essential.) In the following, it is important that the process used in that proof allows one to express each word in the algebra $\mathcal{A}$ as a linear combination of regular words of the same content relative to R.

Theorem 1 and the above remark imply the following result of a combinatorial nature:

Corollary 1. *The number of regular words of the same given content relative to R does not depend on the choice of ordering in the definition of regular words.*

Indeed, let regular words be defined in two different ways, and let M_i $(i = 1, 2)$ be the sets of all words which are regular according to the first (respectively second) sense and have the same given content relative to R. By Theorem 1 the elements of each set M_i in $\mathcal{A}$ are linearly independent over P, and any element of each of these sets is a linear combination of the elements of the other set, which proves the corollary.

Given an arbitrary Lie algebra $\mathcal{L}$, one can speak of a *regular form* of its elements. For this, one must fix some set $M = \{v_\gamma\}$ of generators and consider the homomorphism of the free Lie algebra $\overline{\mathcal{L}}$, with the set $\overline{M} = \{\overline{v_\gamma}\}$ of free generators which are in one-to-one correspondence with the elements of M, onto $\mathcal{L}$.

An M-word, i.e., an element of $\mathcal{L}$ of the form $w = v_{\gamma_1} v_{\gamma_2} \cdots v_{\gamma_k}$ where $v_{\gamma_j} \in M$ with some arrangement of brackets, will be called M_τ*-regular* if, for the set $\overline{M}$ the regular words have been defined in some way τ and the word $\overline{w} = \overline{v_{\gamma_1}}\,\overline{v_{\gamma_2}} \cdots \overline{v_{\gamma_k}}$ in elements of $\overline{M}$ is regular. Generally speaking, for an element of $\mathcal{L}$, an M_τ*-regular form*, i.e., a representation as a linear combination of M_τ-regular words, is not uniquely defined, but for any M-word w there exists an expression as a linear combination of M_τ-regular words with the same content relative to M as w. To find such an expression, one must find an analogous expression for the word $\overline{w}$ and then pass to the homomorphic image.

For consistency of notation in what follows, we will denote by $\overline{\mathcal{D}}$ the free Lie algebra on the set of free generators that are in one-to-one correspondence with the generators of the given Lie algebra $\mathcal{D}$.

Definition 4. We will say that a set $\mathcal{R}$ of elements of the free Lie algebra $\mathcal{A}$ is *independent* if $\mathcal{R}$ generates a free subalgebra of $\mathcal{A}$ and is a system of free generators of that subalgebra.

For example, the set R itself is independent. In what follows we will assume that for the set R the regular words are defined in some fixed way and we will call those words *R-regular.*

Let d be a fixed R-regular word, and K_d the set of d-irreducible words. The set K_d generates some subalgebra $\mathcal{A}_d$ of $\mathcal{A}$. The set K_d consists of R-regular words, and thus it is already ordered by the fixed order of R-regular words. We will transfer this order to the set $\overline{K_d}$ of free generators of the free Lie algebra $\overline{\mathcal{A}_d}$, and starting with this order we will define in some fixed way $\overline{K_d}$-regular $\overline{K_d}$-words. After that, it also makes sense to speak of K_d-regular K_d-words. As was shown above, there exists a representation of each K_d-word as a linear combination of regular K_d words of the same content relative to K_d.

Lemma 1. *Every K_d-word can be represented as a linear combination of K_d-words of the same content relative to K_d which are in fact R-regular.*

This lemma is obvious for K_d-words whose K_d-length (i.e., length relative to K_d) is 1, since the elements of K_d are in fact R-regular.

Suppose the lemma has been proved for K_d-words whose K_d-length is less than n, $n > 1$. A word w whose K_d-length is equal to n can be represented as a product of two K_d-words of smaller K_d-length which can, by the inductive hypothesis, be rewritten in R-regular form with the same content relative to K_d. Therefore, we can assume that $w = uv$ where u and v are R-regular K_d-words; we can also assume that $u > v$ in the sense of the ordering of R-regular words because in the contrary case we would have written $w = -vu$. If u is a K_d-word of K_d-length 1, then w is already R-regular because u and v are R-regular, $u > v$, and if $u = u_1u_2$ then $u_2 \leq d < v$ by definition of d-irreducibility. If the K_d-length of u is greater than 1, then it suffices to consider the case when $u = u_1u_2$ and $u_2 > v$, since in the contrary case w would already be R-regular.

So let $w = (u_1u_2)v$ where u_1, u_2, v are R-regular K_d-words, $u_1 > u_2 > v$. By relation (2),

$$w = (u_1u_2)v = (u_1v)u_2 + u_1(u_2v). \tag{3}$$

Since the lengths of the words u_1v and u_2v are greater than the length of v, rewriting u_1v and u_2v in R-regular form we obtain K_d-words that are greater than v relative to the ordering of words in R. Applying distributivity and removing words of the form uu if they appear, and using anticommutativity to make the right factor less than the left factor, we obtain an expression of w as a linear combination of words, each of which, as w itself, consists of two R-regular factors with the right factor less than the left factor but now greater than v. We do the same with each of these words as with w. Because of the finiteness of the number of words with a given content, this process will terminate after a finite number of steps; this means that we have obtained the required expression for w.

Lemma 2. *K_d-regular K_d-words are linearly independent in $\mathcal{A}$.*

For the proof of Lemma 2 it suffices to prove linear independence of K_d-regular K_d-words with the same content relative to K_d, since by Lemma 1 each K_d-regular K_d-word is a linear combination of R-regular K_d-words of the same content which are linearly independent by Theorem 1.

For K_d-words of K_d-length 1, the statement of Lemma 2 is obvious. Assume by induction that, in any free Lie algebra $\mathcal{A}_0$, for any R_0-regular word d_0, K_{d_0}-regular K_{d_0}-words of K_{d_0}-length less than n are linearly independent.

Suppose there exists a linear dependence between K_d-regular K_d-words of K_d-length n, $n > 1$, that have given content relative to K_d. Now let w be the smallest element of K_d that appears in these linearly dependent words. Subject the K_d-regular K_d-words under consideration to w-factorization, which makes sense in $\overline{\mathcal{A}_d}$ and also in $\mathcal{A}_d$ by the homomorphism $\overline{\mathcal{A}_d} \to \mathcal{A}_d$. All w-irreducible words that can appear here will have the form u or $[\cdots(uw)\cdots]w$ where $u \in K_d$, $u \neq w$. Therefore they will be R-regular, i.e., belong to the set K_w of R-regular w-irreducible words.

The elements K_w will be ordered in a different way depending on whether we consider them as R-words or as K_d-words. Thus we introduce two definitions of regular words in $\overline{\mathcal{A}_w}$ and we will distinguish $\overline{K_{wR}}$-regular $\overline{K_w}$-words and $\overline{K_{wd}}$-regular $\overline{K_w}$-words, depending on whether the ordering in K_w is induced by the ordering of the regular words of $\mathcal{A}$ or the ordering of the regular words of $\overline{\mathcal{A}_d}$. In this sense we will speak of K_{wR}-regular and K_{wd}-regular K_w-words in the subalgebra $\mathcal{A}_w$ generated by the set K_w.

In view of the fact that w by assumption occurs in each of our linearly dependent K_d-regular K_d-words, and since for w itself w-reducibility or w-irreducibility does not make sense, it follows that the K_w-length of the K_d-regular K_d-words under consideration will be less than n, and thus the assumed linear dependence is at the same time a linear dependence between K_d-regular K_w-words of K_w-length less than n. By the inductive hypothesis, K_{wR}-regular K_w-words of length less than n are linearly independent. By Corollary 1 the number of K_{wR}-regular K_w-words of a fixed content is equal to the number of K_{wd}-regular K_w-words of the same content. From the possibility of representing a K_{wR}-regular K_w-word as a linear combination of K_{wd}-regular K_w-words of the same content, and vice versa, it follows that the K_{wd}-regular K_w-words of K_w-length less than n are linearly independent.

Applying Lemma 1 to the algebra $\overline{\mathcal{A}_d}$ it is possible to express any $\overline{K_{wd}}$-regular word as a linear combination of $\overline{K_d}$-regular words of the same content relative to $\overline{K_w}$. On the other hand, it is obvious that every $\overline{K_w}$-word is a linear combination of $\overline{K_{wd}}$-regular $\overline{K_w}$-words of the same content. Passing to the homomorphic images we obtain the corresponding statement for the subalgebra $\mathcal{A}_d$.

By the inductive hypothesis, $\overline{K_{wd}}$-regular $\overline{K_{wd}}$-words of $\overline{K_w}$-length less than n are linearly independent in the algebra $\overline{\mathcal{A}_d}$; therefore the numbers of $\overline{K_{wd}}$-regular and $\overline{K_d}$-regular $\overline{K_w}$-words of $\overline{K_w}$-length less than n and the same content are equal.

An analogous statement holds also for K_w-words. Therefore the K_w-words of K_w-length less than n that are K_d-regular are linearly independent, which however contradicts the above-mentioned linear dependence of these words. This proves Lemma 2.

Lemma 3. *The set K_d is independent.*

The homomorphism $\overline{\mathcal{A}_d} \to \mathcal{A}_d$ is, by Lemma 2, an isomorphism, since only the zero element of $\overline{\mathcal{A}_d}$ is mapped to the zero element of $\mathcal{A}_d$. The existence of an isomorphism between $\mathcal{A}_d$ and the free Lie algebra $\overline{\mathcal{A}_d}$ proves Lemma 3.

Corollary 2. *In the free Lie algebra with two generators there exists a subalgebra that is a free Lie algebra with a countably infinite set of generators.*

Let a and b be the generators of the free Lie algebra. Then the countable set of words of the form ab, $(ab)b$, $[(ab)b)b]$, $\ldots$ is independent since each of these words belongs to the independent set K_b of b-irreducible words. From this the desired conclusion follows.

In the free Lie algebra $\mathcal{A}$ with the set of free generators R, to each element w there corresponds uniquely a natural number $n(w)$, the *degree of the element* w. The degree of w can be defined as the greatest length of regular words in the representation of w in terms of the basis of regular words. Obviously, this does not depend on the definition of regular words. The sum of the terms in this representation of w whose length is equal to $n(w)$ will be called the *highest part* of w. The element w will be called *homogeneous* if it coincides with its highest part. In an analogous sense, we can define degree, highest part, and homogeneity relative to one of the free generators of the algebra $\mathcal{A}$.

3. Main theorem

Let $\mathcal{B}$ be an arbitrary subalgebra of the free Lie algebra $\mathcal{A}$. We will construct a finite or countably infinite increasing sequence of integers k_n $(n = 0, 1, 2, \ldots)$ and a sequence of subalgebras $\mathcal{B}_n \subset \mathcal{B}$ similarly to the way it is done in the work of A.G. Kurosh [2]: define $k_0 = 0$ and $\mathcal{B}_0 = 0$; if k_m and $\mathcal{B}_m$ are already defined for all $m = 0, 1, \ldots, n-1$, let k_n be the least degree of elements in $\mathcal{B}$ that do not belong to $\mathcal{B}_{n-1}$, and let $\mathcal{B}_n$ be the subalgebra of $\mathcal{B}$ generated by all elements whose degree does not exceed k_n.

Lemma 4. *In $\mathcal{B}$ it is possible to choose a subset $\mathcal{M}$ such that*

(1) *no element $a \in \mathcal{M}$ has its highest part in the subalgebra generated by the highest parts of the elements of $\mathcal{M} \setminus \{a\}$, and*
(2) *the subalgebra $\mathcal{B}$ is generated by the set $\mathcal{M}$.*

The set $\mathcal{K}_n$ of elements of the subalgebra $\mathcal{B}_n$ whose degree does not exceed k_n is a linear subspace and the set $\mathcal{K}'_n$ of elements of the subalgebra $\mathcal{B}_{n-1}$ whose degree does not exceed k_n is a linear subspace of $\mathcal{K}_n$.

Choose arbitrarily one representative for each coset in a basis of the linear space $\mathcal{K}_n/\mathcal{K}'_n$ and let $\mathcal{M}_n$ be this set. Now let $\mathcal{M} = \bigcup_{n\geq 1} \mathcal{M}_n$. We will prove that the set $\mathcal{M}$ satisfies the requirements of Lemma 4.

We will denote the elements of $\mathcal{M}$ by b_β and their highest parts by b'_β. Suppose that for $b_\beta \in \mathcal{M}_n$ the following equality holds:

$$b'_\beta = \sum_{\gamma\neq\beta} \alpha_\gamma b'_\gamma + \sum_{\gamma,\delta\neq\beta} \alpha_{\gamma\delta} b'_\gamma b'_\delta + \cdots + \sum_{\gamma,\delta,\ldots,\nu\neq\beta} \alpha_{\gamma\delta\cdots\nu} b'_\gamma b'_\delta \cdots b'_\nu, \tag{4}$$

where some bracket arrangement is assumed for each summand with more than two factors, and the α's with subscripts are elements of the field P.

The second and following summations on the right-hand side of equation (4) may contain factors of degree greater than the degree of b'_β. Then, when we rewrite these products in the regular form, they will either become zero or will keep the same degree. In view of the linear independence of regular words, all such terms must cancel each other, and hence we may assume that the first summation contains only the elements of the same degree as b'_β, and that the remaining elements

b' appearing on the right-hand side of equation (4) have degree strictly less than the degree of b'_β, but their products have the same degree as b'_β.

The highest part of the element

$$b_\beta - \sum_{\gamma\neq\beta} \alpha_\gamma b_\gamma - \sum_{\gamma,\delta\neq\beta} \alpha_{\gamma\delta} b_\gamma b_\delta - \cdots - \sum_{\gamma,\delta,\ldots,\nu\neq\beta} \alpha_{\gamma\delta\ldots\nu} b_\gamma b_\delta \cdots b_\nu$$

of the subalgebra $\mathcal{B}_n$, has degree less than k_n, and thus this element already belongs to the subalgebra $\mathcal{B}_{n-1}$, which leads to a contradiction with the linear independence of the cosets from which we chose the elements of $\mathcal{M}_n$. Requirement (1) for the set $\mathcal{M}$ has been proved.

To prove that requirement (2) holds, we observe that the subalgebra $\mathcal{B}_n$ is generated by the subalgebra $\mathcal{B}_{n-1}$ and the set $\mathcal{M}_n$, from which it follows by induction that the subalgebra $\mathcal{B}_n$ is generated by the set $\bigcup_{k=1}^n \mathcal{M}_k$ for all n. Since for each $c \in \mathcal{B}$ there exists a natural number q such that $c \in \mathcal{B}_q$, requirement (2) has been proved.

By a *nonassociative polynomial* we mean an element of the free nonassociative algebra S over the field P with a countably infinite set of free generators x_1, x_2, ... Let $\mathcal{S}$ be the free Lie algebra over the same field with free generators a_1, a_2, ..., where regular words in $\mathcal{S}$ have been defined in some way. There exists a natural homomorphism of S onto $\mathcal{S}$ that sends the polynomial $f(x_{i_1}, x_{i_2}, \ldots)$ to the element $f(a_{i_1}, a_{i_2}, \ldots)$. We will call two polynomials in S *equivalent* if their images in $\mathcal{S}$ are equal. We will call a polynomial $f(x_{i_1}, x_{i_2}, \ldots)$ *non-trivial* if its image $f(a_{i_1}, a_{i_2}, \ldots)$ is nonzero. Let $\varphi(a_{i_1}, a_{i_2}, \ldots)$ be the regular form of this image. Then the polynomial $\varphi(x_{i_1}, x_{i_2}, \ldots)$ equivalent to the polynomial $f(x_{i_1}, x_{i_2}, \ldots)$ will be called *regular*. Clearly, any part of a regular polynomial is non-trivial.

Theorem 2. *Any subalgebra $\mathcal{B}$ of a free Lie algebra $\mathcal{A}$ is free.*

Suppose we are given a free Lie algebra $\mathcal{A}$ over the field P with the set R of free generators, and a subalgebra $\mathcal{B}$. According to Lemma 4, we choose a set $\mathcal{M}$ and we will prove that it is independent.

Assume that for some finite system of elements b_1, b_2, ..., b_q in $\mathcal{M}$, there exists a non-trivial relation $F(b_1, b_2, \ldots, b_q) = 0$, i.e., $F(x_1, x_2, \ldots, x_q)$ is a non-trivial polynomial which we may take to be regular; from this we will derive a contradiction. We may assume that $n(b_i) \leq n(b_j)$ for $i < j$.

Lemma 5. *Under the above assumption, there exists a finite set $\mathcal{M}_1$ of homogeneous elements of the algebra $\mathcal{A}$ that satisfies requirement* (1) *of Lemma* 4, *and some non-trivial relation $F_1 = 0$ among the elements of $\mathcal{M}_1$.*

The regular polynomial $F(x_1, x_2, \ldots, x_q)$ can be represented as the following sum of two polynomials:

$$F(x_1, x_2, \ldots, x_q) = F_1(x_1, x_2, \ldots, x_q) + F'_2(x_1, x_2, \ldots, x_q).$$

To each term of the polynomial F under the substitution of b_i for x_i $(i = 1, 2, \ldots, q)$ there corresponds a natural number, namely the sum of the degrees relative to R

of all factors of the form b_i that occur in the given term. Then, we denote by F_1 the sum of all terms for which this sum of degrees is maximal.

Let $b_i = b'_i + b''_i$ where b'_i is the leading term of b_i $(i = 1, 2, \ldots, q)$. Then, from the relation

$$\begin{aligned} F(b_1, \ldots, b_q) &= F(b'_1 + b''_1, \ldots, b'_q + b''_q) \\ &= F(b'_1, \ldots, b'_q) + F'(b'_1, \ldots, b'_q, b''_1, \ldots, b''_q) \\ &= F_1(b'_1, \ldots, b'_q) + F'_2(b'_1, \ldots, b'_q) + F'(b'_1, \ldots, b'_q, b''_1, \ldots, b''_q) \\ &= 0, \end{aligned}$$

it follows that $F_1(b'_1, \ldots, b'_q) = 0$ by the definition of the polynomial F_1. The non-triviality of the polynomial F_1 follows from the fact that it is regular as part of the regular polynomial F. The required set $\mathcal{M}_1$ is b'_1, b'_2, …, b'_q.

Lemma 6. *Suppose there exists a set $\mathcal{M}_1 = \{b'_i\}$ $(i = 1, 2, \ldots, q)$ and a non-trivial relation*

$$F_1(b'_1, \ldots, b'_q) = 0,$$

that satisfy the conditions of Lemma 5. *Suppose that the elements of the set $\mathcal{M}'_2 = \{c_i\}$ $(i = 1, 2, \ldots, q)$ are in one-to-one correspondence with the elements of the set $\mathcal{M}_1$ and have the form $c_i = b'_i + v_i$ $(i = 1, 2, \ldots, q)$ where v_i is an element of the subalgebra generated by the elements b'_k with $k < i$, and v_i either is zero or has the same degree relative to R as b'_i. Then there exists a non-trivial relation $F_2(c_1, \ldots, c_q) = 0$ and the set $\mathcal{M}'_2$ satisfies the same conditions as the set $\mathcal{M}_1$.*

First of all, let us prove that there exists a representation $b_i = c_i + v'_i$ $(i = 1, 2, \ldots, q)$ where v'_i is zero or an element of the subalgebra generated by the elements c_j $(j < i)$ whose degree is equal to the degree of v_i. We set $b'_1 = c_1$. Suppose we have found the required representation for all b'_k with $k < m$. Then, from the equality $b'_m = c_m - v_m$, after replacing all b'_j $(j < m)$ in v_m by the already found expressions, it follows that there exists the required expression for b'_m.

We separate, from the non-trivial polynomial $F_1(b'_1, \ldots, b'_q)$ which we may suppose regular, the part F_{11} that has the highest degree relative to b'_q, and then from F_{11} we separate the part F_{12} that has the highest degree relative to b'_{q-1}, and so on; finally, from $F_{1,q-1}$ we separate the part F_{1q} that has the highest degree relative to b'_1. Let us substitute the expressions we have found for b'_k into the relation $f_1 = 0$:

$$\begin{aligned} F(b'_1, \ldots, b'_q) &= F_{1q}(b'_1, \ldots, b'_q) + \overline{F}_1(b'_1, \ldots, b'_q) \\ &= F_{1q}(c_1 + v'_1, \ldots, c_q + v'_q) + \overline{F}_1(c_1 + v'_1, \ldots, c_q + v'_q) \\ &= F_{1q}(c_1, \ldots, c_q) + \varphi(c_1, \ldots, c_q) \\ &= F_2(c_1, \ldots, c_q) \\ &= 0. \end{aligned}$$

The polynomial F_{1q} is non-trivial since it is regular; and obviously it does not have terms of the same content relative to $\mathcal{M}_2'$ as any term of the polynomial φ. It follows that the polynomial F_2 is non-trivial.

Now we prove that the element $c_j \in \mathcal{M}_2'$ does not belong to the subalgebra generated by the set $\mathcal{M}_2' \setminus c_j$. Assuming the contrary, we obtain the equation

$$c_j = \sum_{k_1 \neq j} \alpha_{k_1} c_{k_1} + \sum_{k_1, k_2 \neq j} \alpha_{k_1 k_2} c_{k_1} c_{k_2} + \cdots + \sum_{k_1, \ldots, k_n \neq j} \alpha_{k_1 \cdots k_n} c_{k_1} c_{k_2} \cdots c_{k_n},$$

where we assume for each product with $n > 2$ there is some arrangement of brackets.

Repeating verbatim what was said above about equation (4), we will assume that the element c_j and all elements c_{k_1} that occur in the first summation have the same degree, and all factors in the second and following summations on the right-hand side have strictly smaller degrees. Let c_ℓ have the greatest index among the elements c_j, c_{k_1}. Then, replacing all c_i by their expressions in terms of b_i', we obtain that b_i' belongs to the subalgebra generated by the other elements of the set $\mathcal{M}_1$, which contradicts Lemma 5. This completes the proof.

Lemma 7. *Under the conditions of Lemma* 6*, there exists a set* $\mathcal{M}_2$ *of elements which satisfy requirement* (1) *of Lemma* 4*, are homogeneous in each element of* R*, and satisfy some non-trivial relation.*

We choose arbitrarily some generator $a_\alpha \in R$ from among the elements of the set $\mathcal{M}_1$. Each element $b_i' \in \mathcal{M}_1$ can be written in the form

$$b_i' = b_{i1} + b_{i2} + \cdots + b_{in_i},$$

where b_{ik} is the part of the element b_i' that has degree k relative to a_α ($i = 1, 2, \ldots, q$; $k = 0, 1, \ldots, n_i$). If b_{2n_2} belongs to the subalgebra generated by the element b_{1n_1}, i.e., $b_{2n_2} = \gamma b_{1n_1}$, $\gamma \in P$, then we replace the element b_2' in $\mathcal{M}_1$ by the element $b_2' - \gamma b_1'$ and denote the resulting set $\mathcal{M}_{12}$, using for symmetry the notation $\mathcal{M}_{11} = \mathcal{M}_1$; otherwise, we set $\mathcal{M}_{12} = \mathcal{M}_{11}$. Suppose the sets $\mathcal{M}_{1r}$ ($r = 1, 2, \ldots, \ell$; $\ell < q$) have already been constructed. If, in the set $\mathcal{M}_{1\ell}$ the element $b_{\ell+1, n_{\ell+1}}$, that is a part of the element $b_{\ell+1}'$, does not belong to the subalgebra generated by the highest parts, relative to a_α, of the preceding elements of $\mathcal{M}_{1\ell}$, then we will set $\mathcal{M}_{1,\ell+1} = \mathcal{M}_{1\ell}$. If, on the other hand, $b_{\ell+1, n_{\ell+1}}$ belongs to that subalgebra, then we replace the element $b_{\ell+1}'$ by the element $b_{\ell+1}' - v_{\ell+1}$ where $v_{\ell+1}$ is an element of the subalgebra generated by the elements of $\mathcal{M}_{1\ell}$ preceding the element $b_{\ell+1}'$, whose highest part relative to a_α is the same as for $b_{\ell+1}'$. We denote the resulting set by $\mathcal{M}_{1,\ell+1}$. We may assume that the highest part relative to a_α of the element $b_{\ell+1}' - v_{\ell+1}$ does not belong to the subalgebra generated by the highest parts relative to a_α of the elements of $\mathcal{M}_{1\ell}$ that precede $b_{\ell+1}'$, because this can be easily achieved by an appropriate choice of $v_{\ell+1}$. Finally, we will obtain a set $\mathcal{M}_{1q} = \mathcal{M}'$ such that the highest part of each element relative to a_α does not belong to the subalgebra generated by the highest parts (relative to a_α) of the preceding elements. In fact, the highest part relative to a_α of each element of

$\mathcal{M}'$ does not belong to the subalgebra generated by the similar parts of the other elements, since assuming the contrary immediately leads to a contradiction as in the proof of Lemma 6.

Applying Lemma 6 at each step of the above construction we obtain that no element of the set $\mathcal{M}'$ belongs to the subalgebra generated by the other elements, and we also obtain a certain non-trivial relation $F'' = 0$ for the elements of this set. We write each element $c'_k \in \mathcal{M}$ in the form $c'_k = c'_{k1} + c'_{k2}$ where c'_{k1} is the highest part of the element c'_k relative to a_α, and separate in each polynomial F'' the highest part F''_1 relative to a_α. Then we will have

$$\begin{aligned} F''(c'_1, \dots, c'_q) &= F''_1(c'_1, \dots, c'_q) + F''_2(c'_1, \dots, c'_q) \\ &= F''_1(c'_{11}, \dots, c'_{q1}) + \varphi''(c'_{11}, \dots, c'_{q1}, c'_{12}, \dots, c'_{q2}) \\ &= 0. \end{aligned}$$

In view of the fact that each term of $F''_1(c'_{11}, \dots, c'_{q1})$ has the highest degree in a_α, these terms cannot cancel with the terms of the polynomial φ''; moreover, F''_1 is non-trivial as a part of a regular polynomial.

Thus we have obtained the set $\mathcal{M}'' = \{c'_{i1}\}$ of elements which are homogeneous in a_α, and a non-trivial relation $F''_1 = 0$ satisfied by these elements. Enumerating one by one all the generators that occur in the elements of the set $\mathcal{M}_1$ we find obtain the desired set $\mathcal{M}_2$ and some non-trivial relation for its elements.

Lemmas 5, 6 and 7 allow us to assume that the set $\mathcal{M}_1 = \{b'_i\}$ $(i = 1, 2, \dots, q)$ consists of elements that are homogeneous in each generator and satisfy requirement (1) of Lemma 4.

If $\mathcal{M}_1$ contains elements of degree 1, then by homogeneity they must have the form γa_μ where $\gamma \in P$, $a_\mu \in R$. Therefore we can assume that such elements have the form $a_\mu \in R$, i.e., they are simply free generators.

The ordered q-tuple $(\nu_1; \nu_2; \dots; \nu_q)$ of natural numbers, where ν_k is the degree of b'_k, will be called the *height* of the set $\mathcal{M}_1$. We order the set of all possible heights lexicographically, and assume that for the sets with smaller height there are no non-trivial relations if those sets satisfy requirement (1) of Lemma 4. This assumption is justified by considering the sets of height $\varepsilon = (1; 1; \dots; 1)$ that consist only of free generators.

Assume $(\nu_1; \nu_2; \dots; \nu_q) > (1; 1; \dots; 1)$; this means that some $\nu_k > 1$. Then, in the element b'_k, we can find a generator a_λ that is not one of the b'_m, since otherwise requirement (1) of Lemma 4 would be violated.

Let us reorder the generators to make a_λ the smallest if this is not already the case, and rewrite all b'_i in regular form relative to some new definition of regular words that depends on this order. After this, we subject the words in the elements of the set $\mathcal{M}_1$ to a_λ-factorization. By Lemma 3, a_λ-irreducible words form an independent set; thus all our considerations can be transferred to the free Lie algebra $\mathcal{A}_{a_\lambda}$ generated by the set K_{a_λ} of a_λ-irreducible words. Since a_λ is the smallest of the generators, all other generators will be a_λ-irreducible; therefore, the degree of each word relative to the new system of free generators of $\mathcal{A}_{a_\lambda}$

will be equal to the difference between its degree relative to the old system of free generators of the algebra $\mathcal{A}$ and its degree relative to a_λ. It follows that the elements of $\mathcal{M}_1$ which are homogeneous in each of the old generators will also be homogeneous relative to the new systems of generators, but the set $\mathcal{M}_1$ itself will have a smaller height. Obviously, the height will not become zero and also the set will retain a non-trivial relation. This contradicts the inductive hypothesis and consequently proves the theorem.

The theorem on subalgebras of free Lie algebras proved above cannot be transferred to rings, since for example the subring, of the free Lie ring with generators a and b, generated by the elements $2a$, b, ab is not free because the generators $2a$, b, ab satisfy the relation

$$(2a)b - 2(ab) = 0,$$

and as can be easily seen there is no other system of generators for this subring that would not satisfy a non-trivial relation.

References

[1] M. Hall, *A basis for free Lie rings and higher commutators in free groups*, Proc. Amer. Math. Soc. 1 (1950) 575–581.

[2] A.G. Kurosh, *Nonassociative free algebras and free products of algebras*, Mat. Sbornik N.S. 20 (1947) 239–262.

[3] A.I. Malcev, *On algebras defined by identical relations*, Mat. Sbornik N.S. 26 (1950) 19–33.