Contents

Preface

Anatolii Illarionovich Shirshov (1921–1981) was an outstanding Russian mathematician whose works made a decisive contribution to the theory of associative, Lie, Jordan, and alternative rings. He created a large scientific school whose representatives have worked successfully in many different areas of algebra. For a period of fifteen years (1959–1973), A.I. Shirshov was Deputy Director of the (now Sobolev) Institute of Mathematics of the Siberian Branch of the Russian Academy of Sciences (the Director was S.L. Sobolev) and in this and other positions he made a substantial contribution to the organization and early development of both the Sobolev Institute and the entire Siberian Branch of the Academy.

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*, M: Nauka, 1978 (With K.A. Zhevlakov, A.M. Slinko and I.P. Shestakov) (translated by H.F. Smith, N.Y.: Academic Press, 1982) and some articles whose content is included in later more extensive publications. The works are ordered chronologically.

February 2009

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

Commentaries

Perspectives on Shirshov's Height Theorem

Alexei Kanel-Belov and Louis H. Rowen

In this survey we consider the impact of Shirshov's Height Theorem on algebra. In order to avoid duplication, we often refer to Kemer's survey article [Kem09] in this volume for further details. Proofs of various quoted results are given in the book [BBL97], and in the authors' book [BR05].

1. Historical background to Shirshov's Theorem

Let F denote a field. An F-algebra is called *affine* if it is finitely generated as an algebra. An F-algebra is *algebraic* if each element a satisfies an algebraic equation over F; i.e., if the dimension $[F[a] : F] < \infty$. We say that an algebra A has PI-*degree* n if A satisfies a multilinear polynomial identity (PI) of degree n. One of the early tests of the utility of PI-theory was whether it could provide a framework for a positive solution of the following famous problem of Kurosh:

Are affine algebraic algebras necessarily finite dimensional?

Although now known to be false for associative algebras in general (cf. [Gol64]), Kurosh's problem was solved for associative PI-algebras by Kaplansky [Kap50], building on work of Jacobson and Levitzki, as described in [Kem09]. However, Kaplansky's elegant proof, relying on topology and structure theory, is not constructive.

Digression. In hindsight, Kurosh's problem for PI-algebras has an easy solution using standard results from structure theory. Here is a modification of the argument given in [Pro73]. By [Pro73, Lemma 2.6], if A is not finite-dimensional, there is a prime ideal P maximal with respect to A/P not being finite-dimensional, so we may assume that A is a prime affine algebraic PI-algebra. But then the center C of A is a field, so A is simple, by [Row88, Corollary 6.1.29], and thus

This research was supported by the Israel Science Foundation, grant #1178/06. The authors would like to thank L. Bokut, A. Kemer, E. Zelmanov, and U. Vishne for helpful comments on drafts of this survey.

finite-dimensional over C, by Kaplansky's Theorem. Then a version of the Artin-Tate Lemma [Row88, Proposition 6.2.5] says the field C is affine and thus finite-dimensional over F, implying R is finite-dimensional over F. (This argument also works more generally for affine algebras integral over a commutative Noetherian ring.)

A different approach to Kurosh's problem, taken by A.I. Shirshov [Shir57a], [Shir57b], involves the detailed analysis of words and their relations, as given in *Shirshov's Height Theorem*:

Let A be a finitely generated algebra of PI-degree d. Then there exists a finite set $Y \subset A$ and an integer $\tilde{h} \in \mathbb{N}$ such that A is linearly spanned by the set of elements of the form

$$v_1^{k_1} v_2^{k_2} \cdots v_h^{k_h} \quad \text{where} \quad h \leq \tilde{h}, \quad v_i \in Y.$$

For Y we may take the set of words of length $\leq d$. Such Y is called a *Shirshov base* of the algebra A, and $\tilde{h}$ is called the *Shirshov height* $h(A)$.

The object of this survey is to describe the impact of this pioneering theorem. Shirshov's theorem immediately yields an independent positive solution of Kurosh's problem and of other related problems for PI-algebras. Specifically, if Y is a Shirshov base consisting of algebraic elements, then the algebra A is finite-dimensional. Thus, Shirshov's theorem explicitly determines the set of elements whose algebraicity implies algebraicity of the whole algebra. (It is worth noting that Procesi [Pro73] later discovered a structural proof of Shirshov's theorem also, by means of reducing first to prime rings and then utilizing traces.) We also have

Corollary 1.1. *If A is a PI-algebra of PI-degree d and all words in its generators of length $\leq d$ are algebraic, then A is locally finite.*

Let us briefly sketch the proof of Shirshov's Theorem. Suppose that $A = F\{a_1, \ldots, a_\ell\}$ is an affine algebra. Ordering the letters $a_1 < \cdots < a_\ell$ induces the *lexicographic* order on the set Ω^* of words in the generators $\{a_1, \ldots, a_\ell\}$. We consider this as a total order, where a proper initial subword v of a word w is defined to precede w. But note that this order is not preserved under multiplication; for example $a_2 \prec a_2 a_1$ but $a_2^2 \succ (a_2 a_1)^2$. A word w is *reducible* if it can be written as a linear combination of smaller words.

Definition 1.2. *A word w is called* d-decomposable *if it contains a subword $w_1 \cdots w_d$ such that $w_1 \cdots w_d \succ w_{\pi(1)} \cdots w_{\pi(d)}$ for any permutation π of $\{1, \ldots, d\}$.*

A (multilinear) PI of degree d can be used to rewrite any d-decomposable word as a sum of smaller words; thus, the irreducible words are d-indecomposable. Shirshov proved *Shirshov's Lemma*, which asserts that, for any given $r > 0$, any long enough d-indecomposable word must contain a nonempty word u^r where $|u| \leq d$. Shirshov's height theorem follows from an algorithmic argument given in [BR05, p. 50].

Shirshov's Height Theorem also yields a result about the *Gelfand-Kirillov dimension* $\mathrm{GK}(A)$ of an affine algebra A. Recall that

$$\mathrm{GK}(A) = \lim_{n\to\infty} \frac{\ln \dim(V_A(n))}{\ln(n)},$$

where $V_A(n)$ is the vector space generated by the words of length $\leq n$ in the generators of A. A related concept is the (*Poincaré-*)*Hilbert Series*

$$H_A = 1 + \sum d_n \lambda^n,$$

where $d_n = \dim(V_A(n)/V_A(n-1))$, the number of irreducible words of length n. (Strictly speaking, H_A depends on the given set of generators of A, whereas $\mathrm{GK}(A)$ is independent of the choice of generators.)

Corollary 1.3 (Berele [Ber93]**).** $\mathrm{GK}(A) < \infty$*, for any affine PI-algebra* A*.*

To prove the corollary, it suffices to observe that the number of solutions of the inequality $k_1|v_1| + \cdots + k_h|v_h| \leq n$ with $h \leq \tilde{h}$ does not exceed $N^{\tilde{h}}$, and therefore $\mathrm{GK}(A) \leq h(A)$.

Shirshov's beautiful theorem, which also is formulated for algebras over arbitrary commutative rings, opened the way to the combinatoric school of PI-theory, which has led to many breakthroughs in recent years. (Ironically, Shirshov's work was unknown in the West until Amitsur brought it to attention in 1973. Thus, for many years, there was a parallel development of PI-theory on both sides of the former "iron curtain," along mostly combinatoric lines in the former Soviet Union and along structural lines in the West. Although our focus in this survey is on Shirshov's influence, and thus on the Russian school, we also describe parallel results in the West.)

1.1. The radical of an affine PI-algebra and the Nagata-Higman Theorem

One of the early applications of Shirshov's Theorem was in a seemingly unrelated direction. Using structure theory, Amitsur [Am57] showed that the Jacobson radical $J(A)$ of an affine PI-algebra is nil. This led to the question of whether $J(A)$ is nilpotent, which was formally raised by Latyshev in his dissertation. Shirshov's Theorem is a key tool in verifying this assertion when R satisfies the PI's of $n \times n$ matrices, as shown by Razmyslov [Raz74a], who also proved that a complete solution is equivalent to the conjecture that every affine PI-algebra satisfies the *standard* PI. Kemer[Kem80] verified this latter conjecture in characteristic 0. Braun [Br84] was the first to prove the nilpotence of $J(A)$ for arbitrary affine A, using the structure of Azumaya algebras. A nice exposition of Braun's theorem can also be found in Lvov [Lv83].

Incidentally, much earlier, Dubnov and Ivanov, and independently, Nagata and Higman [Hig56] showed that in characteristic 0, any nil algebra of bounded index n is nilpotent. The original bounds for the nilpotence index were exponential in n. Better bounds have been obtained as an outgrowth of Shirshov's work.

Razmyslov [Raz74b] showed that n^2 is an upper bound, and Kuzmin obtained the lower bound $\frac{n^2+n-2}{2}$, described in [BR05, p. 341].

1.2. Representable algebras

An F-algebra is called *representable* if it can be embedded into $M_n(K)$ for some field extension $K \supset F$ and some n. (More generally, we can take K commutative Noetherian, in view of [An92].) Shirshov's Theorem implies that for any representable affine PI-algebra A, one may adjoin the characteristic coefficients of finitely many words of the generators, to obtain a PI-algebra $\hat{A}$, called the *trace ring* or *characteristic closure*, which is finite over its center but also possesses a nonzero ideal contained in A. The use of this *conductor ideal*, discovered by Razmyslov [Raz74a] (and later, independently, by Schelter [Sch76]) is one of the keys to the structure of affine PI-algebras, and is used in Razmyslov's work on the Jacobson radical described above.

Another application of the characteristic closure is to the *Hilbert series* of an algebra; Answering a question raised by Procesi [Pro73], Belov proved that any relatively free, affine PI-algebra has a rational Hilbert series (with respect to a suitable set of generators); cf. [BR05, Chapter 9] for this and related results. On the other hand, Theorem 3.5 below provides examples of representable algebras with non-rational Hilbert series.

1.3. Specht's conjecture

One of the most famous problems in PI-theory was Specht's conjecture, that every set of identities is a consequence of a finite set of identities. (More formally, every T-ideal of the free algebra is finitely generated as a T-ideal.) As described in [Kem09], this question was settled affirmatively by Kemer [Kem87], [Kem90b] whenever the base field F is infinite, and later by Belov for arbitrary affine PI-algebras. The characteristic closure is one component of the proofs, and the nilpotence of the radical is another important aspect, so Shirshov's theorem plays an important role. The key step of Kemer's theorem is that each affine PI-algebra over an infinite field satisfies the same PI's as a suitable finite-dimensional algebra; it follows at once that the corresponding relatively free algebra is representable. (Belov extended this fact to affine algebras over arbitrary commutative Noetherian rings.)

2. Generalizations to nonassociative algebras

Shirshov's Height Theorem has been extended to various classes of nonassociative algebras. In his original paper, Shirshov applied his theorem to special Jordan algebras. Zelmanov [Zel91] obtained the following analog for ad-identities of Lie algebras:

Say an associative word in X is *special* if it is the leading word appearing in some Lie word (i.e., word with respect to the Lie multiplication). The word w is *Zelmanov d-decomposable* if it can be written as a product of subwords $w = w'w_1w_1'w_2w_2' \cdots w_dw_d'w''$ with each w_i special and $w_1 \succ w_2 \cdots \succ w_d$. Then, for

any ℓ, k, d, there is $\beta = \beta(\ell, k, d)$ such that any Zelmanov d-indecomposable word w of length $\geq \beta$ in ℓ letters must contain a nonempty subword of the form u^k, with u special.

Zelmanov's result is a major ingredient in his celebrated solution of the restricted Burnside problem. S.P. Mishchenko [Mis90] obtained an analogue of Shirshov's Height Theorem for Lie algebras with a "sparse" identity. S.V. Pchelintsev [Pch84] proved an analog for alternative and $(-1, 1)$ cases. Belov [Bel88b] proved a version for a certain class of rings asymptotically close to associative rings, including alternative and Jordan PI-algebras.

3. Questions arising in connection with Shirshov's Theorem

Shirshov's Height Theorem also gives rise to various notions, which we examine in turn.

3.1. d-decomposable words

We start with d-decomposable words; cf. Definiton 1.2. An equivalent formulation: A word w is d-decomposable if it can be written in the form $s_0 v_1 s_1 v_2 \dots s_{-1} v_d s_d$ where $v_1 \succ v_2 \succ \cdots \succ v_d$. The next proposition below demonstrates the importance of the notion of d-decomposability.

Proposition 3.1 (A.I. Shirshov).

a) *Suppose that a word w is d-decomposable. Then any word obtained from w by means of a nonidentical permutation is lexicographically less than w.*

b) *If an algebra A satisfies a PI*

$$x_1 \cdots x_d = \sum_{\sigma \neq id \in S_d} \alpha_\sigma x_{\sigma(1)} \cdots x_{\sigma(d)}$$

of degree d, then any d-decomposable word w can be written as a linear combination of words of lower order.

Thus in an algebra of PI-degree d, any word not representable as a linear combination of lower-order words is not d-decomposable, and it suffices to check that the set of d-indecomposable words has bounded height.

3.1.1. d-decomposable words and codimensions. Regev [Reg72] introduced the *codimension sequence* in order to prove that the tensor product of PI-algebras is a PI-algebra. Namely, let W_n denote the F-space of multilinear polynomials in $x_1, \dots, x_n$, and

$$c_n = \dim_F(W_n/(W_n \cap \mathrm{id}(A));$$

then c_n is exponentially bounded, for any PI-degree n.

A theorem of Dilworth enables one to bound the number of d-indecomposable words of length n by $n^{2(d-1)}$. Latyshev [Lat72] discovered a quicker proof of Regev's tensor product theorem by using Dilworth's Theorem, and showing that $c_n(A)$ is bounded by the number of d-indecomposable multilinear words. This estimate of

the codimension series led to the result of Kemer, Regev, and Amitsur that any polynomial identity whose Young tableau contains a rectangle (whose size is a suitably large function of n) is a consequence of any given polynomial identity of degree n. (This is the basis of Kemer's "super-trick" to pass from identities of nonaffine algebras to identities of affine superalgebras.)

On the other hand, there is an interesting refinement of the Hilbert series. The *multivariate Poincaré-Hilbert series* of an affine algebra $A = F\{a_1, \dots, a_\ell\}$ is defined as

$$H(A) = \sum d_{\mathbf{i}} \lambda_1^{i_1} \cdots \lambda_\ell^{i_\ell},$$

where

$$d_{\mathbf{i}} = \dim_F \left(\bar{V}_A(\mathbf{i})\right);$$

here $\mathbf{i} = (i_1, \dots, i_\ell)$, and $\bar{V}_A(\mathbf{i})$ is the vector space spanned by irreducible words of length $\leq i_u$ in the generator a_i of A, for $1 \leq u \leq \ell$.

Kemer [Kem95, §2] proved that the number of d-indecomposable multilinear words of length n equals the codimension of the space of multilinear polynomials of degree n, with traces, of $M_d(F)$. By Formanek [For84], this codimension sequence can be calculated precisely, using the multivariate Hilbert series.

Thus, Shirshov's approach motivates the use of combinatorics to compute codimensions, and to introduce the use of invariants of matrices. In this regard, Razmyslov [Raz74b], Helling[Hel74], and Procesi[Pro76], independently showed in characteristic 0 that every PI is a consequence of the Hamilton-Cayley equation (which can be written as a trace identity). This follows from the two *Fundamental Theorems of Invariant Theory*, which respectively are as follows:

- All invariants can be expressed in terms of traces.
- All relations between invariants are consequences of the Hamilton-Cayley trace identity.

In characteristic $p > 0$ one must study all of the coefficients of the Hamilton-Cayley equation as individual functions, arising from homogeneous forms (not necessarily linear), since they cannot be computed in terms of the trace. Kemer [Kem90b] developed the theory of identities involving these forms. Donkin[Do94] proved the analog of the First Fundamental Theorem of Invariant Theory, and Zubkov [Zubk96] proved the analog of the Second Fundamental Theorem.

In a similar vein, Razmyslov's student Zubrilin developed the technique of incorporating coefficients of the characteristic polynomial into Capelli polynomials, which leads to a combinatoric proof of the Razmyslov-Kemer-Braun theorem, as exposed in [BR05, §2.5].

Kemer [Kem95] showed that, unlike the situation in characteristic 0, any PI-algebra A (not necessarily affine) of characteristic $p > 0$ satisfies all the multilinear identities of a finite-dimensional algebra; combining this with the cited work of Donkin, Zubkov, and Zubrilin, yields that A satisfies all PI's of a finite-dimensional algebra; cf. [Bel00].

3.2. Estimates of Shirshov height

Shirshov's original proof was purely combinatorial (based on an elimination technique he developed for Lie algebras), but did not provide a reasonable estimate for the height. Kolotov [Kol81] obtained an estimate for $h(A) \leq s^{s^m}$ ($m = \text{PI-deg}(A)$, and s is the number of generators). In the Dniester Notebook (most recent version [Dne93]), Zelmanov asked for an exponential bound, which was obtained later by Belov [Bel88a]:

Theorem 3.1. *Suppose A is a PI-algebra of PI-degree d, generated by ℓ elements. Then the height of A over the set of words having length $\leq m$ is bounded by a function $h(m, \ell)$ where $h(m, \ell) < 2m\ell^{m+1}$.*

3.2.1. Burnside-type problems. A word $w = u^k$, for $k > 1$, is called *cyclic* or *periodic*. By problems of *Burnside type*, we mean problems related to periodic words. Combinatorics play an important role. The following basic lemma yields computational tools involving subwords which are described in [Bel07] and provide the bounds given in Theorem 3.1. The technique is illustrated in the slightly weaker result given in [BR05, Theorem 2.74].

Lemma 3.2 (on overlapping). *If two periodic words of respective periods m and n contain identical subwords having length $m+n-gcd(m, n)$ then they have identical periods.*

3.3. The essential height of an algebra

Definition 3.3. *An algebra A is said to have* essential height $\leq h$ *over a subset Y, if there is a finite set $S \subset A$ (which may depend on Y) such that A is spanned as a vector space by*

$$Y^{[h],S} = \{s_0 y_1^{m_1} s_1 \cdots s_{t-1} y_t^{m_t} s_t : \ m_i \in \mathbb{N}, \ y_i \in Y, \ s_i \in S, \ t \leq h\}.$$

In this case, Y is called an essential Shirshov base*, and S the* supplementary *set.*

Essential height is an estimate for GK-dimension; also, the converse is true for representable algebras.

Theorem 3.2 (A.Ya. Belov [BBL97]**).** *Suppose A is a finitely generated representable algebra and $H_{Ess_Y}(A) < \infty$. Then $H_{Ess_Y}(A) = \text{GK}(A)$.*

This equality is useful in both directions. First of all, it shows for a representable algebra A that $H_{Ess_Y}(A)$ is independent of the choice of Y. In the other direction, since $H_{Ess_Y}(A)$ must be an integer, one has:

Corollary 3.4 (V.T. Markov). *The Gelfand-Kirillov dimension of a representable affine algebra is an integer.*

Due to the representability of relatively free affine algebras (noted above), the Gelfand-Kirillov dimension of a relatively free algebra also equals the essential height.

Clearly, an essential Shirshov base is a Shirshov base iff it generates A as an algebra. Boundedness of essential height over Y implies a positive solution of "Kurosh's problem over Y." The converse is much less trivial.

Theorem 3.3 (A.Ya. Belov). *Suppose A is a graded PI-algebra, and Y is a finite set of homogeneous elements. Let $Y^{(n)}$ denote the ideal generated by all nth powers of elements of Y. If the algebra $A/Y^{(n)}$ is nilpotent for each n, then Y is an s-base for A. If in this situation Y generates A as an algebra, then Y is a Shirshov base for A.*

We proceed to formulate a generalization of this theorem for the non-graded case. We must confront the following counterexample to the straightforward converse of Kurosh's problem: Suppose $A = \mathbb{Q}[x, 1/x]$. Each projection π such that $\pi(x)$ is algebraic has finite-dimensional image. Nevertheless the set $\{x\}$ is not an s-base for A.

Thus we need a stronger definition:

Definition 3.5. *A set $M \subset A$ is called a Kurosh set if it satisfies the condition that for any projection $\pi\colon A \otimes K[X] \to A'$, if the image $\pi(M)$ is integral over $\pi(K[X])$, then $\pi(M)$ is finite over $\pi(K[X])$.*

Theorem 3.4 (A.Ya. Belov). *Let A be a PI-algebra, $M \subseteq A$ a Kurosh subset in A. Then M is an s-base for A.*

Thus, boundedness of essential height is a non-commutative generalization of integrality. The following proposition shows that Theorem 3.4 does generalize Theorem 3.3:

Proposition 3.6. *Let A be a graded algebra, Y a set of homogeneous elements. If the algebra $A/Y^{(n)}$ is locally nilpotent for all n, then Y is a Kurosh set.*

3.4. Normal bases and monomial algebras

Shirshov's combinatoric approach leads us to the combinatoric study of bases. Let $A = F\{a_1, \dots, a_\ell\}$ be an associative affine algebra. A word is called *reducible* if it can be written as a linear combination of lexicographically smaller words; the *normal base* of the algebra A is the set of all irreducible words in the generators; cf. [BBL97], [BRV06], [Dr00], [Lat88], [Ufn85].

A *monomial algebra* is an algebra that can be described in terms of relations that are monomials in the generators. Any affine algebra A has its *associated monomial algebra* possessing the same Hilbert series; namely one factors the free algebra by the set of reducible words in the generators of A, cf. [BR05, Proposition 9.8]. The associated monomial algebra of an algebra A also has the same Shirshov base, although it may not satisfy the same PI's. Nevertheless, their easier relations make monomial algebras a useful tool in studying Shirshov bases. This discussion follows [BRV06]; the reader should also consult [BBL97].

In case an affine monomial algebra A is PI, it has bounded essential height over a (finite) Shirshov base Y, which we may assume to be a set of words in

the generators. Take a supplementary set S as in Definition 3.3 that contains Y. Choose a subset of $Y^{[h],S}$ that spans A. Given

$$w = s_0 y_1^{m_1} s_1 \cdots s_{t-1} y_t^{m_t} s_t \tag{1}$$

(with $y_i \in Y$ and $s_i \in S$, and t bounded by the height), we rewrite it in the same manner with $s_0 \in S$ of maximal possible length, then with $y_1^{m_1}$ of maximal possible length, and so on. $(s_0, y_1, s_1, \ldots, s_{t-1}, y_t, s_t)$ is called the *type* of w. The type of a subword of a w of type θ is called a *subtype* of θ.

By an *exponential polynomial* in the variables $m_1, \ldots, m_t$ we mean an expression of the form

$$\sum f_j(m_1, \ldots, m_t) \alpha_{1j}^{m_1} \cdots \alpha_{tj}^{m_t}$$

where f_j are polynomials over a finite algebraic extension K of F, and $\alpha_{ij} \in K$. For example,

$$P(m_1, \ldots, m_t) = (5 - \sqrt{2})^{m_1} - m_2^4 \cdot 3^{m_1}$$

is an exponential polynomial over $\mathbb{Q}$.

Theorem 3.5. *A monomial algebra A over F is representable iff:*

1. *A has essential height over a finite set Y (with a supplementary set S), such that every word in the generators of A has a unique type, and there are finitely many types.*
2. *For each type $\theta = (s_0, y_1, s_1, y_2, \ldots, y_t, s_t)$, there is a finite system $P_{\theta,j}$ of exponential equations over k, in the variables $m_1, \ldots, m_t$, such that*

$$\bigcup_\theta \{ s_0 y_1^{m_1} s_1 \cdots y_t^{m_t} s_t : \quad \exists j \ P_{\theta,j}(m_1, \ldots, m_t) \neq 0 \}$$

is a normal base.

The construction of monomial algebras is thus equivalent to the solution of arbitrary exponential polynomials. But this is algorithmically unsolvable by the celebrated theorem of Davis-Putnam-Robinson [DPR61]. Thus there is no algorithm to determine whether there is an isomorphism (given in terms of the generators) for two monomial subalgebras of the matrix algebra over a polynomial ring of characteristic 0. On the other hand, this isomorphism problem is algorithmically solvable in characteristic $p > 0$. More precisely, Belov and Chilikov [BC00], [BRV06] proved over a field of characteristic p that the set of p-adic representations of exponential equations (with unknowns in $\mathbb{N}$) forms a "regular language." Thus, an inaccessible problem in characteristic 0 becomes algorithmically solvable in positive characteristic.

3.5. The conjecture of Amitsur and Shestakov

S. Amitsur and I.P. Shestakov conjectured that if the algebra A satisfies the identities of $M_n(F)$ and all words having length not exceeding n are algebraic, then A is finite-dimensional. I.V. Lvov reduced this assertion to the following:

Let $A = F\{a_1, \dots, a_\ell\}$ be a finite-dimensional subalgebra (without 1) of a matrix algebra of order n. If all words in $a_1, \dots, a_\ell$ of length $\leq n$ are nilpotent, then the algebra A is nilpotent.

Shestakov's conjecture was proved by V.A. Ufnarovsky [Ufn85] and by G.P. Chekanu [Che88]. Their *Independence Theorem* may be formulated as follows [Che88], [Ufn90]:

Theorem 3.6 (Independence Theorem). *Suppose the following is true:*

1. *a word $w = a_{i_1} \cdots a_{i_n}$ is minimal under the lexicographical order in the set of all nonzero products of length n;*
2. *all terminal subwords of w are nilpotent.*

Then the initial subwords of w are linearly independent.

Here is a key step. A word is called *extremal* if it does not lexicographically precede any nonzero word.

Lemma 3.7. *Any set of pairwise incomparable subwords of an extremal word is independent.*

To deduce I.P. Shestakov's conjecture (or, equivalently, I.V. L'vov's assertion) from this theorem, we consider the following construction:

Remark 3.8. *Given an algebra A and a right module V, the algebra $\widetilde{A}$ is defined additively as $A \oplus V$, with multiplication defined as follows: $V \cdot V = A \cdot V = 0$, and the product of elements from V and A is given by the module multiplication.*

We take a faithful representation of A acting on an n-dimensional right vector space V. Taking a base $v_1, \dots, v_n$ of this space, then, for some v_i we have $v_i w \neq 0$. Viewing V as a right A-module, we form the algebra $\tilde{A}$ of Remark 3.8, ordering the generators by $v_1 \succ \cdots \succ v_n \succ a_1 \succ \cdots \succ a_s$, and apply the Independence Theorem. Later, Belov and Chekanu showed that we may take the $\{v_i\}$ to be the set of words from Shestakov's conjecture. Another proof of this fact was obtained by V. Drensky.

The original proofs of the Independence Theorem were rather complicated. Application of *hyperwords*, described below, allow a considerable simplification.

Subsequent papers of these authors contained various refinements and generalizations of these theorems. Here is another elegant result of Chekanu [Che96]:

Theorem 3.7. *Suppose a word w is extremal and non-periodic, of length n. If $w^n \neq 0$, then the algebra generated by the letters of w contains a nilpotent element of index exactly n.*

3.6. Hyperwords in algebras

Many of the combinatorial results in this survey are most easily proved using infinite words, or *hyperwords*, so we conclude with a discussion of basic auxiliary facts and constructions related to hyperwords in algebras.

Definition 3.9. *A hyperword is a word infinite in both directions; a word infinite only to the left (resp. right) is called a left* (resp. *right*) *hyperword.*

u^∞ denotes the hyperword having period u, and $u^{\infty/2}$ the left (resp. right) hyperword having period u and terminal (resp. initial) subword u.

The context will always make clear whether we consider a left or right hyperword, so we do not distinguish the notation between them. For example, the expression $u^{\infty/2}wv^{\infty/2}$ indicates that $u^{\infty/2}$ is a left hyperword and $v^{\infty/2}$ is a right hyperword.

Right hyperwords form a linearly ordered set with respect to the lexicographical order. For a right hyperword w, we let $(w)_k$ denote the initial subword of w having length k.

Lemma 3.10 ([BBL97]**).** *Let C be an arbitrary collection of words having unbounded length. Then there exists a hyperword w such that each of its subwords is a subword of a word from C.*

Although evaluating a hyperword in an algebra does not make sense, we can define whether or not it equals 0 (according to whether some subword equals 0), and this leads to the notion of linear independence of hyperwords in A:

Definition 3.11.

a) *A hyperword w is called a zero hyperword if it includes a subword of finite length equal to 0, and a nonzero hyperword otherwise.*
b) *A finite set of right hyperwords $\{w_i\}$ is called linearly dependent if there exist $\{\alpha_i\}$ such that some of them are not zero and for all sufficiently large k we have*
$$\sum \alpha_i (w_i)_k = 0.$$
c) *Suppose w is a right hyperword in an algebra A, M is a right A-module, and $m \in M$. We say that $mw \neq 0$ if $m(w)_k \neq 0$ for all k. Otherwise $Mw = 0$.*
d) *Suppose $\{w_1, \ldots, w_n\}$ is a set of right hyperwords in an algebra A, and M is a right A-module. We say that $\sum m_i w_i = 0$ for $m_i \in M$ if $\sum m_i (w_i)_k = 0$ for all sufficiently large k.*

Proposition 3.12.

a) *A finitely generated non-nilpotent algebra A contains non-zero hyperwords.*
b) *Suppose A is a finitely generated algebra, M is a finitely generated right A-module. If $MA^k \neq 0$ for all $k > 0$, then there exist $m \in M$ and a right hyperword w such that $mw \neq 0$.*

The existence of a least upper bound and of a greatest lower bound for any set of right hyperwords implies the following

Proposition 3.13.

a) *Let w be a hyperword. Then the set of right hyperwords whose subwords are all subwords of w contains maximal and minimal hyperwords.*
b) *Suppose $\forall k \quad mA^k \neq 0$. Then the set of right hyperwords w such that $mw \neq 0$ contains a maximal and a minimal hyperword.*

c) *If A is non-nilpotent, then the set of nonzero right hyperwords in A contains a maximal and a minimal hyperword.*

Let u be the maximal word in an algebra A among all nonzero words in A having length $\leq n$. Unfortunately u may have no extension to a word of greater length. Thus, to utilize hyperwords, we need the following construction:

Construction 1. Let A be an algebra having generators $a_s \succ \cdots \succ a_1$. Put $a_1 \succ x$ and consider the free product $A' = A * F\langle x\rangle$.

Each word u in A is an initial subword of some hyperword in A'. If u is the maximal word in A among all words having length at most $|u|$, then the maximal hyperword in A' beginning with u is a hyperword in A. If $\tilde{u}$ is a hyperword in A for which each initial subword has this property, then the maximal hyperword in A' is $\tilde{u}$.

The following construction is useful for treating modules.

Construction 2. Suppose A is an algebra having generators $a_s \succ \cdots \succ a_1$, and V is a finitely generated right A-module having generators $m_k \succ \cdots \succ m_1$. Put $m_1 \succ a_s$, $a_1 \succ x$, and $\widetilde{A}$ as in Remark 3.8. Define $A'' = \widetilde{A} * F\langle x\rangle / I$ where the ideal I is generated by elements of the form xm_i.

In the algebra A'', the maximal right hyperword begins with m_k, and each word in $\widetilde{A}$ may be extended to a hyperword in A''; if $MA^k \neq 0$ for all k, then the maximal hyperword in $\widetilde{A}$ begins with some m_i.

If u is the maximal word in A among all words having length at most $|u|$ that act nontrivially on the generators of the module, then after renumbering the m_i suitably, the maximal hyperword in A'' is a hyperword in $\widetilde{A}$. If u is a hyperword in $\widetilde{A}$ such that each of its initial subwords has the above property, then the maximal hyperword in A'' is u.

Note that if an algebra has no nonzero nilpotent ideals, then any word may be extended to a hyperword. The following observation is useful.

Proposition 3.14. *If an algebra contains no nonzero periodic hyperword, then all of its words are nilpotent.*

The technique of hyperwords seems to lie rather close to the lines of structure theory, as illustrated in the following theorem and its proof, cf. [Bel07].

Theorem 3.8. *The set of irreducible words in a* PI*-algebra A has bounded height over the set of words whose degree does not exceed the PI-degree of A.*

Proof. Suppose m is the minimal degree of identities holding in an algebra A of PI-degree d. Since A has bounded height over the set of words having degree $\leq m$, it suffices to show that if $|u|$ is a nonperiodic word of length $> n$ then the word u^k for sufficiently large k is a linear combination of words of smaller lexicographic order.

Step 1. Consider the right A-module M defined by a generator v and by the relations $vw = 0$ whenever $w \prec u^{\infty/2}$. Our goal is to show that $Mu^k = 0$ for some k. Indeed, some power u^k is spanned by smaller lexicographic words. By

virtue of Shirshov's Height Theorem, the set of irreducible words has bounded height over Y_m, the set of words of degree $\leq m$. But if each sufficiently large power of a nonperiodic word having length d may be linearly represented by smaller words, then the words having length $> d$ may be excluded from Y_m.

Step 2. The correspondence $\lambda : vs \to vus$ defines a well-defined endomorphism of the module M, hence M may be considered as an $A[\lambda]$-module. Our goal is to show that $M\lambda^k = 0$ for some k, or equivalently that $\overline{M} = M \otimes \mathbb{F}[\lambda, \lambda^{-1}] = 0$.

Step 3. If $M\lambda^k \in M \cdot J(\operatorname{Ann} M)$ where $J(\operatorname{Ann} M)$ is the Jacobson radical of the annihilator of M, then $M\lambda^{\ell k} \in M \cdot J(\operatorname{Ann} M)^\ell$, and by the nilpotence of the radical, $M\lambda^{\ell k} = 0$ for sufficiently large ℓ. Hence, we may assume that $J(\operatorname{Ann} M) = 0$.

Step 4. Using primary decomposition, we reduce to the case for which M is a faithful module over a primary ring B.

Step 5. Elements of the center $Z(B)$ have trivial annihilator, so we may localize relative to them; replacing $Z(B)$ by an algebraic extension, we reduce to the case for which B is the algebra of some dimension $k \leq n$ over a field, and $\overline{M}$ is a k-dimensional vector space.

Step 6. Since M is a vector space of dimension $< |u|$, the vectors $\vec{v}u_0$, $\vec{v}u_1$, $\ldots$, $\vec{v}u_{n-1}$ are linearly dependent (where u_i is the initial subword of length i in the word u, and $u_0 = 1$). Thus we have the equality

$$\sum_{i \in I} \lambda_i \vec{v}_i u_i = 0 \tag{2}$$

where $I \subseteq \{0, \ldots, n-1\}$, $\lambda_i \in \mathbb{F}\backslash 0$. To each u_i we attach a word $u^{(i)}$ so that $u_i u^{(i)} = u^{|u|}$. Let $u^{(j)}$ be the least of those $u^{(i)}$ which are involved in the formula (2). Write the equality (2) in the form

$$\vec{v}_j u_j = \sum_{i \in I \backslash \{j\}} \beta_i \vec{v}_i u_i \tag{3}$$

where $\beta_i = -\alpha_i/\alpha_j$. But then

$$\vec{v}u^{|u|} = \vec{v}_j u_j u^{(j)} = \sum_{i \in I \backslash \{j\}} \beta_i \vec{v}_i u_i u^{(j)}. \tag{4}$$

If $i \in I\backslash\{j\}$, then $u^{(j)} \prec u^{(i)}$ and $u_i u^{(j)} \prec u_i u^{(i)} = u^{|u|}$; hence $v u_i u^{(j)} = 0$. Thus all terms in the right side of (4) are zero. Hence $\vec{v}u^{|u|} = 0$, as desired. □

Hyperwords facilitate proofs of the Independence Theorem, Shirshov's Height Theorem, nilpotence of the Lie algebra generated by sandwiches [Ufn90], proof of the *Bergman Gap Theorem*, (that any algebra of GK dimension greater than 1, has GK dimension at least 2, together with a description of the base having growth function $V_A(n) = \frac{n(n+3)}{2}$), and also describe various properties of monomial algebras [BBL97] as well as other combinatorial results for semigroups and rings.

References

[Am57] Amitsur, S.A., *A generalization of Hilbert's Nullstellensatz*, Proc. Amer. Math. Soc. **8** (1957), 649–656.

[An92] Anan'in, A.Z., *The representability of finitely generated algebras with chain condition*, Arch. Math. **59** (1992), 1–5.

[Ba87] Bakhturin, Yu.A., Identical relations in Lie algebras. Translated from the Russian by Bakhturin. VNU Science Press, b.v., Utrecht, (1987).

[Bel88a] Belov, A.Ya., *On Shirshov bases in relatively free algebras of complexity n*, Mat. Sb. **135** (1988), no. 3, 373–384.

[Bel88b] Belov, A.Ya., *The height theorem for Jordan and Lie PI-algebras*, in: Tez. Dokl. Sib. Shkoly po Mnogoobr. Algebraicheskih Sistem, Barnaul (1988), pp. 12–13.

[Bel89] Belov, A.Ya., *Estimations of the height and Gelfand-Kirillov dimension of associative PI-algebras*, In: Tez. Dokl. po Teorii Koletz, Algebr i Modulei. Mezhdunar. Konf. po Algebre Pamyati A.I.Mal'tzeva, Novosibirsk (1989), p. 21.

[Bel92] Belov, A.Ya., *Some estimations for nilpotency of nil-algebras over a field of an arbitrary characteristic and height theorem*, Commun. Algebra **20** (1992), no. 10, 2919–2922.

[Bel97] Belov, A.Ya., *Rationality of Hilbert series with respect to free algebras*, Russian Math. Surveys **52** (1997), no. 10, 394–395.

[Bel00] Belov, A.Ya., *Counterexamples to the Specht problem*, Sb. Math. **191** (3–4) (2000), 329–340.

[Bel02] Belov, A.Ya., *Algebras with polynomial idenitities: Representations and combinatorial methods*, Doctor of Science Dissertation, Moscow (2002).

[Bel07] Belov, A.Ya., *Burnside-type problems, and theorems on height and independence* (Russian), Fundam. Prikl. Mat. 13 (2007), no. 5, 19–79.

[BBL97] Belov, A.Ya., Borisenko, V.V., and Latyshev, V.N., *Monomial algebras. Algebra 4*, J. Math. Sci. (New York) **87** (1997), no. 3, 3463–3575.

[BC00] Belov, A.Ya. and Chilikov, A.A., *Exponential Diophantine equations in rings of positive characteristic* (Russian) Fundam. Prikl. Mat. **6**(3), 649–668, (2000).

[BR05] Belov, A.Ya. and Rowen, L.H. *Computational aspects of polynomial identities*. Research Notes in Mathematics **9**. AK Peters, Ltd., Wellesley, MA, 2005.

[BRV06] Kanel-Belov, A.Ya., Rowen, L.H., and Vishne, U., *Normal bases of PI-algebras*, Adv. in Appl. Math. 37 (2006), no. 3, 378–389.

[Ber93] Berele, A., *Generic verbally prime PI-algebras and their GK-dimensions*, Comm. Algebra **21** (1993), no. 5, 1487–1504.

[Bog01] Bogdanov I., *Nagata-Higman's theorem for hemirings*, Fundam. Prikl. Mat. **7** (2001), no. 3, 651–658 (in Russian).

[BLH88] Bokut', L.A., L'vov, I.V., and Harchenko, V.K., *Noncommutative rings*, In: Sovrem. Probl. Mat. Fundam. Napravl. Vol. 18, Itogi Nauki i Tekhn., All-Union Institute for Scientificand Technical Information (VINITI), Akad. Nauk SSSR, Moscow (1988), 5–116.

[Br82] Braun, A., *The radical in a finitely generated PI-algebra*, Bull. Amer. Math. Soc. **7** (1982), no. 2, 385–386.

[Br84] Braun, A., *The nilpotence of the radical in a finitely generated PI-ring*, J. Algebra **89** (1984), 375–396.

[Che88] Chekanu, G.P., *Local finiteness of algebras*. (Russian) Mat. Issled. **105**, Moduli, Algebry, Topol. (1988), 153–171, 198.

[Che95] Chekanu, G.P., *Independence and quasiregularity in algebras*, Dokl. Akad. Nauk **337** (1994), no. 3, 316–319; translation: Russian Acad. Sci. Dokl. Math. **50** (1995), no. 1, 84–89.

[Che96] Chekanu, G.P., *Independence and quasiregularity in algebras. I.* (Moldavian) Izv. Akad. Nauk Respub. Moldova Mat. 1996, no. 3, 29–39, 120, 122.

[ChUf85] Chekanu, G.P., and Ufnarovski'i, V.A., *Nilpotent matrices*, Mat. Issled. no. 85, Algebry, Kotsa i Topologi (1985), 130–141, 155.

[DPR61] Davis M., Putnam, H., and Robsinson, J. *The decision problem for exponential differential equations*, Annals of Math. **74**, 425–436, (1961).

[Dne93] Dniester Notebook (Dnestrovskaya tetrad), Sobolev Institute of Mathematics, Novosibirsk, 1993.

[Do94] Donkin, S., *Polynomial invariants of representations of quivers*, Comment. Math. Helv. **69** (1994), no. 1, 137–141.

[Dr84a] Drensky, V., *On the Hilbert series of relatively free algebras*, Comm. in Algebra, **12** no. 19 (1984), 2335–2347.

[Dr84b] Drensky, V., *Codimensions of T-ideals and Hilbert series of relatively free algebras*, J. Algebra **91** no. 1 (1984), 1–17.

[Dr00] Drensky, V., *Free Algebras and PI-algebras: Graduate Course in Algebra*, Springer-Verlag, Singapore (2000).

[DrFor04] Drensky, V. and Formanek, E., *Polynomials Identity Rings*, CRM Advanced Courses in Mathematics, Birkhäuser, Basel (2004).

[For84] Formanek, E., *Invariants and the ring of generic matrices*, J. Algebra **89** (1984), no. 1, 178–223.

[Gol64] Golod, E.S., *On nil-algebras and residually finite p-groups*, Izv. Akad. Nauk SSSR **28** (1964), no. 2, 273–276.

[Gri99] Grishin, A.V., *Examples of T-spaces and T-ideals in Characteristic 2 without the Finite Basis Property*, Fundam. Prikl. Mat. **5** (1) (1999), no. 6, 101–118 (in Russian).

[GuKr02] Gupta, C.K., and Krasilnikov, A.N., *A simple example of a non-finitely based system of polynomial identities*, Comm. Algebra **36** (2002), 4851–4866.

[Hel74] Helling, H., *Eine Kennzeichnung von Charakteren auf Gruppen und Assoziativen Algebren*, Comm. in Alg. **1** (1974), 491–501.

[Hig56] Higman, G., *On a conjecture of Nagata*, Proc. Cam. Phil. Soc. **52** (1956), 1–4.

[Ilt91] Iltyakov, A.V., *Finiteness of basis identities of a finitely generated alternative PI-algebra*, Sibir. Mat. Zh. **31** (1991), no. 6, 87–99; English translation: Sib. Math. J. **31** (1991), 948–961.

[Ilt03] Iltyakov, A.V., *Polynomial identities of Finite Dimensional Lie Algebras*, monograph (2003).

[Kap49] Kaplansky, I., *Groups with representations of bounded degree*, Canadian J. Math. **1** (1949), 105–112.

[Kap50] Kaplansky, I., *Topological representation of algebras. II*, Trans. Amer. Math. Soc. **66** (1949), 464–491.

[Kem80] Kemer, A.R., *Capelli identities and the nilpotence of the radical of a finitely generated PI-algebra*, Soviet Math. Dokl. **22** (3) (1980), 750–753.

[Kem87] Kemer, A.R., *Finite basability of identities of associative algebras* (Russian), Algebra i Logika **26** (1987), 597–641; English translation: Algebra and Logic **26** (1987), 362–397.

[Kem88] Kemer, A.R., *The representability of reduced-free algebras*, Algebra i Logika **27** (1988), no. 3, 274–294.

[Kem90a] Kemer, A.R., *Identities of Associative Algebras*, Transl. Math. Monogr., **87**, Amer. Math. Soc. (1991).

[Kem90b] Kemer, A.R. *Identities of finitely generated algebras over an infinite field* (Russian), Izv. Akad. Nauk SSSR Ser. Mat. **54** (1990), no. 4, 726–753; translation in Math. USSR-Izv. **37** (1991), no. 1, 69–96.

[Kem95] Kemer, A.R., *Multilinear identities of the algebras over a field of characteristic p*, Internat. J. Algebra Comput. **5** (1995), no. 2, 189–197.

[Kem09] Kemer, A.R., *Comments on the Shirshov's Height Theorem*, in this collection.

[Kol81] Kolotov, A.T., *Aperiodic sequences and growth functions in algebras*, Algebra i Logika **20** (1981), no. 2, 138–154.

[KrLe00] Krause, G.R., and Lenagan, T.H., *Growth of Algebras and Gelfand-Kirillov Dimension*, Amer. Math. Soc. Graduate Studies in Mathematics **22** (2000).

[Kuz75] Kuzmin, E.N., *About Nagata-Higman Theorem*, Proceedings dedicated to the 60th birthday of Academician Iliev, Sofia (1975), 101–107 (in Russian).

[Lat72] Latyshev, V.N., *On Regev's theorem on indentities in a tensor product of PI-algebras*, Uspehi Mat. Nauk. **27** (1972), 213–214.

[Lat88] Latyshev, V.N., *Combinatorial Ring Theory. Standard Bases*, Moscow University Press, Moscow (1988), (in Russian).

[Lev46] Levitzki, J., *On a problem of Kurosch*, Bull. Amer. Math. Soc. **52** (1946), 1033–1035.

[Lv83] Lvov, I.V., *Braun's theorem on the radical of PI-algebras*, Institute of Mathematics, Novosibirsk (1983), preprint.

[Mar88] Markov, V.T., *Gelfand-Kirillov dimension: nilpotence, representability, nonmatrix varieties*, In: Tez.Dokl. Sib. Shkola po Mnogoobr. Algebraicheskih Sistem, Barnaul (1988), 43–45.

[Mis90] Mishchenko, S.P. *A variant of a theorem on height for Lie algebras*. (Russian) Mat. Zametki **47** (1990), no. 4, 83–89; translation in Math. Notes **47** (1990), no. 3–4, 368–372.

[Pch84] Pchelintzev, S.V., *The height theorem for alternate algebras*, Mat. Sb. **124** (1984), no. 4, 557–567.

[Pro73] Procesi, C., *Rings with polynomial identities*, Research Notes in Mathematics **917**. Marcel Dekker, New York, 1973.

[Pro76] Procesi, C., *The invariant theory of $n \times n$ matrices*, Advances in Math. **19** (1976), 306–381.

[Raz74a] Razmyslov, Yu.P., Algebra and Logic **13** (1974), no. 3, 192–204.

[Raz74b] Razmyslov, Yu.P., *Trace identities of full matrix algebras over a field of characteristic zero*, Math. USSR Izv. **8** (1974), 724–760.

[Raz89] Razmyslov, Yu.P., *Identities of Algbras and their Representations*, Nauka, Moscow (1989).

[Reg72] Regev, A., *Existence of identities in $A \otimes B$*, Israel J. Math. 11 (1972), 131–152.

[Reg84] Regev, A., *Codimensions and trace codimensions of matrices are asymptotically equal*, Israel J. Math. **47** (1984), 246–250.

[Row88] Rowen, L.H., *Ring Theory II*, Pure and Applied Mathematics **128** Academic Press, New York, 1988.

[Sch76] Schelter, W., *Integral extensions of rings satisfying a polynomial identity*, J. Algebra **40** (1976), 245–257; errata op. cit. **44** (1977), 576.

[Sch78] Schelter, W., *Noncommutative affine PI-algebras are catenary*, J. Algebra **51** (1978), 12–18.

[Shch01] Shchigolev, V.V., *Finite basis property of T-spaces over fields of characteristic zero*, Izv. Ross. Akad. Nauk Ser. Mat. **65** (2001), no. 5, 191–224; translation: Izv. Math. **65** (2001), no. 5, 1041–1071.

[Shir57a] Shirshov, A.I., *On some nonassociative nil-rings and algebraic algebras*, Mat. Sb. **41** (1957), no. 3, 381–394.

[Shir57b] Shirshov, A.I., *On rings with identity relations*, Mat. Sb. **43**, (1957), no. 2, 277–283.

[Sp50] Specht, W., *Gesetze in Ringen I*, Math. Z. **52** (1950), 557–589.

[Ufn80] Ufnarovski'i, V.A., *On Poincaré series of graded algebras*, Mat. Zametki **27** (1980), no. 1, 21–32.

[Ufn85] Ufnarovski'i, V.A., *The independency theorem and its consequences*, Mat. Sb., **128** (1985), no. 1, 124–13.

[Ufn89] Ufnarovski'i, V.A., *On regular words in Shirshov sense*, In: Tez. Dokl. po Teorii Koletz, Algebr i Modulei. Mezhd. Konf. po Algebre Pamyati A.I. Mal'tzeva, Novosibirsk (1989), 140.

[Ufn90] Ufnarovski'i, V.A., *On using graphs for computing bases, growth functions and Hilbert series of associative algebras*, Mat. Sb. **180** (1990), no. 11, 1548–1550.

[VaZel89] Vais, A.Ja., and Zelmanov, E.I., *Kemer's theorem for finitely generated Jordan algebras*, Izv. Vyssh. Uchebn. Zved. Mat. (1989), no. 6, 42–51; translation: Soviet Math. (Iz. VUZ) **33** (1989), no. 6, 38–47.

[Zel91] Zelmanov, E.I., *The solution of the restricted Burnside problem for groups of prime power*, Mimeographed notes, Yale University (1991)

[ZelKos88] Zelmanov, E.I., *On nilpotence of nilalgebras*, Lect. Notes Math. **1352** (1988), 227–240.

[Zubk96] Zubkov, A.N., *On a generalization of the Razmyslov-Procesi theorem.* (Russian) Algebra i Logika **35** (1996), no. 4, 433–457, 498; translation in Algebra and Logic **35** (1996), no. 4, 241–254.

[Zubk00] Zubkov, A.N., *Modules with good filtration and invariant theory.* Algebra – representation theory (Constanta, 2000), 439–460, NATO Sci. Ser. II Math. Phys. Chem. **28** Kluwer Acad. Publ., Dordrecht, 2001.

[Zubr97] Zubrilin, K.A., *On the largest nilpotent ideal in algebras satisfying Capelli identities*, Sb. Math. **188** (1997), 1203–1211.

On Shirshov's Papers for Lie Algebras

Leonid Bokut

Shirshov published six papers on Lie algebras in which he found the following results (in order of publication, 1953–1962):

- Some years before Witt [84], the "Shirshov-Witt theorem" [1].
- Some years before Lazard [62], the "Lazard-Shirshov elimination process" [1]. This is often called "Lazard elimination"; see for example [79].
- The first example of a Lie ring that is not representable into any associative ring [2]; see also P. Cartier [37] and P.M. Cohn [43].
- In the same year as Chen-Fox-Lyndon [38], the "Lyndon-Shirshov basis" of a free Lie algebra (Lyndon-Shirshov Lie words) [6]. This is often called the "Lyndon basis"; see for example [63], [79], [64].
- Independently of Lyndon [65], the "Lyndon-Shirshov (associative) words" [6]. They are often called "Lyndon words"; see for example [63]. In the literature they are also often called "(Shirshov's) regular words" or "Lyndon-Shirshov words"; see for example [42], [24], [13], [32], [85], [76], [14].
- The algorithmic criterion to recognize Lie polynomials in a free associative algebra over any commutative ring [6]. The algorithm is based on the property that the maximal (in deg-lex ordering) associative word of any Lie polynomial is an associative Lyndon-Shirshov word. The Friedrichs criterion [45] follows from the Shirshov algorithmic criterion (see [6]).
- In the same year as Chen-Fox-Lyndon [38], the "central result on Lyndon-Shirshov words": any word is a unique non-decreasing product of Lyndon-Shirshov words [6]. This is often called the "Lyndon theorem" or the "Chen-Fox-Lyndon theorem".
- The reduction algorithm for Lie polynomials: the elimination of the maximal Lyndon-Shirshov Lie word of a Lie polynomial in a Lyndon-Shirshov Lie word [6]. The algorithm based on the Special Bracketing Lemma [6, Lemma 4], which in turn depends on the "central result on Lyndon-Shirshov words" above.
- The theorem that any Lie algebra of countable dimension is embeddable into two-generated Lie algebra with the same number of defining relations [6].

- Some years before Viennot [82], the "Hall-Shirshov bases" of a free Lie algebra [7]: a series of bases that contains the Hall basis and the Lyndon-Shirshov basis and depends on an ordering of basic Lie words such that $[w] = [[u][v]] > [v]$. They are often called "Hall sets"; see for example [79].
- Some years before Hironaka [53] and Buchberger [35], [36], the "Gröbner-Shirshov basis theory" for Lie polynomials (Lie algebras) explicitly and for noncommutative polynomials (associative algebras) implicitly [9]. This theory includes the definition of composition (s-polynomial), reduction algorithm, algorithm for producing a Gröbner-Shirshov basis (this is an infinite algorithm of Knuth-Bendix types [55]; see also the software implementations in [48], [87], [15]), and "Composition-Diamond Lemma". The Shirshov's "Composition-Diamond Lemma" for associative algebras was formulated explicitly in [25] and rediscovered by G. Bergman [16] under the name "Diamond Lemma for ring theory". The "Gröbner-Shirshov basis theory" for associative algebras was rediscovered by T. Mora [78] under the name "non-commutative Gröbner basis theory". The analogous theory for polynomials (commutative algebras) was found by B. Buchberger [35], [36] under the name "Gröbner basis theory"; similar ideas for (commutative) formal series were found by H. Hironaka [53] under the name "standard basis theory".
- The "Freiheitssatz" and the decidability of the word problem for one-relator Lie algebras [9].
- The first linear basis of the free product of Lie algebras [10].
- The first example showing that an analogue of the Kurosh subgroup theorem is not valid for subalgebras of the free product of Lie algebras [10].

Let us give some comments on these papers and further developments. See also V.K. Kharchenko's comments to some of these papers elsewhere in this volume.

In the paper [1], A.I. Shirshov, an aspirant (Ph.D. student) of A.G. Kurosh, proved that any subalgebra of a free Lie algebra is also free. This result was inspired by Kurosh's theorem [60] that any subalgebra of free non-associative algebra is also free. The former result was independently proved by E. Witt [84] three years later and is now called the Shirshov-Witt theorem. In this paper, Shirshov used the "K_d-lemma" to rewrite, in particular, a basic Lie word on a set $X = \{x_i : i = 1, 2, \ldots\}$ as a basic Lie word on the independent set $[x_i x_1^k] = [\ldots [x_i x_1] \ldots x_1]$ $(i > 1, k \geq 0)$; see Lemma 3 and Corollary 2 in [1]. This is often called the "Lazard elimination process" (Lazard [62]); see Theorem 0.6 of [79], cf. [34].

In the paper [2], Shirshov constructed the first example showing that the PBW theorem is not valid in general for Lie algebras over a commutative ring Σ (Σ-algebras). In this paper, Shirshov was able to construct a Lie Σ-algebra L with an element a in the center of L such that a belongs to the center of any Lie Σ-algebra extension of L. On the other hand, he gives a construction showing that the analogous extension result is not valid in general for associative Σ-algebras. Other counter-examples to the PBW theorem for Lie rings were constructed by P. Cartier [37] and P.M. Cohn [43].

In the paper [4], Shirshov proved that any subalgebra of a free commutative (anti-commutative) non-associative algebra is also free. He established linear bases of free (anti)commutative algebras, and later he used these bases for his "Gröbner-Shirshov basis theory" for (anti)commutative algebras, namely, for "Composition-Diamond Lemmas" for these algebras (see below [8]).

In the paper [5], Shirshov proves that any countably generated special Jordan (non-associative, (anti)commutative) algebra over a commutative ring can be embedded into a two-generated special Jordan (non-associative, (anti)commutative) algebra with the same number of defining relations. For groups, this is the famous Higman-Neumann-Neumann theorem [51]. A.I. Malcev [72] proved an analogous result for associative algebras. The analogous problem for Lie algebras was open until Shirshov's next paper [6].

Speaking about Shirshov's paper [6], I cannot help but cite P.M. Cohn's review (Zbl 0080.25503): "The author varies the usual construction of basic commutators in Lie rings by ordering words lexicographically and not by length [the "Lyndon-Shirshov basis", see also Chen-Fox-Lyndon [38]; in [42], P.M. Cohn credited this basis together with "Lyndon-Shirshov words" to Shirshov alone – L.B.]. This is used to give a very short proof of the theorem (Magnus, this Zbl. 16, 194 [see [69] – L.B.]; Witt, this Zbl 16, 244 [see [83] – L.B.]) that the Lie algebra obtained from a free associative algebra is free, with appropriate modification for the case of restricted Lie algebras. Secondly he derives the Friedrichs criterion (this Zbl. 52, 45 [see [45] – L.B.]) for Lie elements (see also P.M. Cohn [44] and R. Lyndon [66] – L.B.). As the third application he proves that every Lie algebra L can be embedded in a Lie algebra M such that in M any subalgebra of countable dimension is contained in a two-generated subalgebra. This is proved by showing that in the free associative algebra on two generators a, b (over a field), the elements

$$d_k = [[a, [a, b^k]], [a, b]], \quad k = 1, 2, \dots \quad ([x, y] = xy - yx),$$

form a distinguished set in the Lie algebra on two generators a, b (cf. Shirshov, this Zbl 71, 257 [see [5] – L.B.]).

Let us formulate the last statement, Lemma 10 of [6], explicitly. Let $k\langle a, b\rangle$ be the free associative algebra over a field k on two generators a, b, let $\mathrm{Lie}(a, b)$ be the Lie algebra of Lie polynomials of $k\langle a, b\rangle$ (the free Lie algebra on $\{a, b\}$), and let $L_\infty = \mathrm{Lie}(d_k : k = 1, 2, \dots)$ be the Lie subalgebra of $Lie(a, b)$, generated by $\{d_k : k = 1, 2, \dots\}$ above. By the K_d-lemma [1] (the Lazard-Shirshov elimination process), L_∞ is the free Lie algebra on the countable set $\{d_k : k \geq 1\}$. Let S be a subset of L_∞. Then

$$\mathrm{AssoId}_{k\langle a,b\rangle}(S) \cap L_\infty = \mathrm{LieId}_{L_\infty}(S),$$

where the former is the associative ideal (in $k\langle a, b\rangle$) generated by S, and the latter is the Lie ideal (in L_∞) generated by S. Shirshov also noticed that from the last statement the PBW theorem follows. In the proof of Lemma 10, Shirshov used the leading (maximal in the deg-lex order) associative monomials of Lie and associative

polynomials, and Lemma 4 on the "special bracketing" of a Lyndon-Shirshov word with a fixed Lyndon-Shirshov subword. The Special Bracketing Lemma is crucial: it allows him to define the reduction algorithm for Lie polynomials (he used this algorithm in the proof of Lemma 10), and to define later in [9] the notion of composition of two Lie polynomials (an analog of Buchberger's s-polynomial in Gröbner basis theory). By the way, in the proof of the Special Bracketing Lemma, he used the fact that any word c can be uniquely expressed as the product of a non-decreasing series of Lyndon-Shirshov words, $c = c_1 c_2 \dots c_k$ with $c_1 \le c_2 \le \dots \le c_k$ ($k \ge 0$). Actually, this remark is an important theorem often called the Lyndon theorem or the Chen-Fox-Lyndon theorem (see [38]). For example, this result is cited in the following way by Springer Online, Encyclopedia of Mathematics (edited by Michiel Hazewinkel): *Lyndon words – "The central result on Lyndon words is the following Chen-Fox-Lyndon theorem: any word can be expressed as a unique non-decreasing product of Lyndon words".*

All in all, Shirshov's paper [6] can be viewed, in particular, as an important step toward the Gröbner-Shirshov basis theory for associative and Lie algebras [9].

A.I. Shirshov [7] "varies the usual construction of basic commutators" [P. Hall [49] for groups and M. Hall [50] for Lie algebras – L.B.] in a free Lie algebra by ordering basic Lie words $\{[w]\}$ in any way such that $[w] > [v]$ if $[w] = [[u][v]]$. For example, an ordering based on the length (the Hall words), or an ordering based on lexicographical ordering (the Lyndon-Shirshov basis), both enjoy this property. He proves that any ordering of this kind leads to a linear basis of a free Lie algebra. Actually, this paper is a part of Shirshov's Thesis [3]. As mentioned above, Shirshov's series of bases were rediscovered later by Viennot [82] and are now often called "Hall bases" (see [79]). There is another example of "Hall-Shirshov bases", that give bases of free solvable Lie algebras ([18], see also [80] and [79], Ch. 5.3). In the paper [41], a first example of right normed basis of a free Lie algebra is found. Though it is not a Hall-Shirshov basis, it is closely connected to Lyndon–Shirshov words.

In the paper [8], Shirshov invented the "Gröbner-Shirshov basis theory" for (anti)commutative non-associative algebras based on the "Composition-Diamond Lemmas" for those algebras (see Lemma 2 in [8]). In particular, it implies the decidability of the word problem for any finitely presented (anti)commutative non-associative algebra. Also, the reduction algorithm is defined in order to find a "Gröbner-Shirshov basis" of any finitely generated ideal in a free (anti)commutative algebra. Shirshov also mentioned that the same results are valid for non-associative algebras. The decidability of the word problem for non-associative algebras was proved by A.I. Zhukov [86], another student of A.G. Kurosh. Actually, Zhukov invented a kind of "Gröbner-Shirshov basis theory" for non-associative algebras. The difference is that he did not use any linear ordering of non-associative words; for a non-associative polynomial f, he chose any non-associative word of maximal length from f as a "leading monomial" of f.

Shirshov's paper [9] is truly a pioneering paper in the subject. He starts with the definition of the composition of two Lie polynomials f, g (explicitly) and two

associative polynomials (implicitly) via the leading associative words $\bar{f}$, $\bar{g}$ of polynomials in the deg-lex ordering: Let $w = \bar{f}b = a\bar{g}$ for some associative words a, b such that $\bar{f} = ac$, $\bar{g} = cb$ and $c \neq 1$ (where 1 is the empty word). Then the associative composition $(f, g)_c$ (this is Shirshov's original notation; we now use $(f, g)_w$) is defined as follows: $(f, g)_c = fb - ag$. For Lie polynomials f, g, one needs to put extra Lie brackets on fb and ga. This is done according to the above mentioned Special Bracketing Lemma 4 [6]. This is a really important and crucial notion for the Gröbner-Shirshov basis theory for both Lie and associative algebras. Together with the above definition of reduction of one Lie polynomial modulo another (see the same paper [6]), it leads to an infinite algorithm to construct the Gröbner-Shirshov basis S^c starting with any set of Lie (associative) polynomials S. He proves Lemma 3, which is now called the Composition Lemma, or the Composition-Diamond Lemma, for Lie polynomials: if $f \in \text{Ideal}(S)$ then the leading associative word $\bar{f}$ contains as a subword $\bar{s}$ for some $s \in S^c$ (see also [32], [27]). Actually, he assumes the extra condition that S should be stable in some sense (see below), but he did not use the stability condition in the proof of the lemma (this condition is essential in order that S^c should be a recursive set for, say, finite S; he kips the stability condition having in mind the application of his theory to the word problem for Lie algebras). In [24], Shirshov's Composition Lemma for Lie polynomials was formulated in the modern form: Let S be a set of Lie polynomials that is closed under compositions (i.e., a Gröbner-Shirshov basis). If $f \in \text{Ideal}(S)$ then $\bar{f} = a\bar{s}b$ for some $s \in S$ and some associative words a, b. Closure means that any composition (i.e., composition of inclusion and composition of intersection) $(f, g)_w$ of polynomials f, g from S is trivial, i.e., it is zero after the reduction leading words of S. One may use a weaker form of the triviality that $(f, g)_w = \sum \alpha_i(a_i s_i b_i)$ for some $s_i \in S$, $\alpha_i \in k$ (the ground field) and some associative words a_i, b_i (with extra Lie bracketing), such that the leading associative words $a_i\bar{s}_i b_i$ of each expression are strictly less than w. The same Composition Lemma is valid for non-commutative associative polynomials with a much easier proof.

A.I. Shirshov gives three applications of his Composition Lemma for Lie algebras.

Theorem 1. *For any Lie polynomial f, there is no non-zero composition $(f, f)_w$. Then the reduction algorithm gives a solution of the word problem for any one-relator Lie algebra $Lie(X|f = 0)$.*

This is because any one-element set in a free Lie algebra is Gröbner-Shirshov basis. One may apply Shirshov's reduction algorithm for Lie polynomials. For groups, it is the famous result of W. Magnus [67]. S.I. Adjan [12] proved it for any semigroup with one defining relation of the form $u = 1$. V.N. Gerasimov [47] proved the decidability result for an associative one-relator algebra $k\langle X|f(X) = 0\rangle$ over a field k where the maximal homogeneous part $\widetilde{f}$ of $f(X)$ has no a proper two-sided divisor (from $\widetilde{f} = gh = h'g$ it follows $g \in k$).

In the paper [18], there is an application of the Shirshov's theorem: Any Lie algebra L is embeddable into an algebraically closed Lie algebra M (in the sense that any equation $f(x_1, \dots, x_n) = 0$ in the variables $X = \{x_1, x_2, \dots\}$ with coefficients in M has a solution in M; here f belongs to a free Lie product (see [10] below) of a free Lie algebra $\mathrm{Lie}(X)$ and M, $f \notin M$).

Theorem 2. *The word problem is decidable for any Lie algebra with a finite number of homogeneous defining relations.*

This is because any finite homogeneous set of Lie (associative) polynomials is a stable set in the sense of this paper. So, one may find all elements of S^c up to some fixed degree, and then apply Shirshov's reduction algorithm to the polynomial under consideration.

Theorem 3. (Freeness Theorem). *Let L be a Lie algebra with one defining relation $s = 0$. Then any subalgebra of L, generated by all but one letter involved in s, is the free Lie algebra on these free generators.*

For groups, this is the famous "Freiheitssatz" by W. Magnus [68]. The Freeness Theorem is also valid for an associative algebra with one defining relation (L.G. Makar-Limanov [71]). The proof does not use the Gröbner-Shirshov basis theory for associative algebras, but rather the existence of algebraically closed associative algebras (L.G. Makar-Limanov [70]). The Freeness theorem is proved for a pre-Lie (or right-symmetric) one-relator algebra (D. Kozybaev, L. Makar-Limanov, U. Umirbaev [56]).

Shirshov's paper [9] implicitly contains the Gröbner-Shirshov basis theory for associative algebras too, because he constantly used the fact that any Lie polynomial is at the same time a non-commutative polynomial. For example, the maximal term of a Lie polynomial is defined to be its maximal word as a non-commutative polynomial, the definition of the Lie composition (the Lie s-polynomial) of two Lie polynomials begins with their composition as non-commutative polynomials and then puts some special Lie brackets on it, and so on. The main Composition-Diamond Lemma for associative polynomials is actually proved in the paper: we need only to "forget" about the Lie brackets in the proof of this lemma for Lie polynomials (Lemma 3 [9]). The Composition-Diamond Lemma was explicitly formulated much later in papers L.A. Bokut [25] and G. Bergman [16].

We formulate Shirshov's Composition-Diamond Lemma for associative algebras following his paper [9] by "forgetting" the brackets, i.e., with only the change of "Lie polynomials" to "non-commutative polynomials". Let $k\langle X\rangle$ be the free associative algebra over a field k on a set X, such that the free monoid X^* is well-ordered by the deg-lex ordering. For a polynomial f, Shirshov [9] denotes by $\overline{f}$ the maximal word of f. Let f, g be two monic polynomials (possibly equal), let $w \in X^*$ be such that $w = acb$, where $\overline{f} = ac$, $\overline{g} = cb$ and a, b, c are words with c nonempty. Then $(f, g)_c = fb - ag$ is called an (associative) composition of f, g (this is Shirshov's original notation, now we use $(f, g)_w$); for Lie polynomials f, g, Shirshov puts some special brackets into $[fb] - [ag]$ such that $\overline{[fb] - [ag]} < w$.

Let S be a reduced set in $k\langle X\rangle$ and let S^c be a reduced set obtained from S by (transfinite) induction applying the following elementary operations: joining to S a composition of two elements of S and applying the reduction algorithm to the resulting set (until one gets a reduced set with only trivial compositions after the reduction). In current terminology, S^c is a Gröbner-Shirshov basis of the ideal generated by S, and the process of adding compositions is Shirshov's algorithm. He calls S a *stable* set if, at each step, the degree of the composition $(f,g)_w$, after the reduction, is bigger than the degree of f, g (or $(f,g)_w$ is zero after the reduction). Of course, if S is a finite (or recursive) stable set, then S^c is a recursive set and from the next lemma the word problem is solvable in the algebra with defining relations S. Now suppose that S is a Gröbner-Shirshov basis in the sense that S is a reduced set and any composition of intersection of elements of S is zero after the reduction (S is complete or closed under compositions). Hence S is a stable set in the sense of Shirshov. Then Lemma 3 of [9] has the following "forgetting brackets" form (see [25]).

Shirshov's Composition-Diamond Lemma for Associative Algebras. *Let $S \subset k\langle X\rangle$ be a Gröbner-Shirshov basis of the ideal* $\mathrm{Id}(S)$*. If $f \in \mathrm{Id}(S)$, then $\overline{f} = a\overline{s}b$, for some $s \in S$ and $a, b \in X^*$. Hence the set of S-irreducible words* $\mathrm{Irr}(S)$*, that do not contain maximal words of polynomials from S as subwords, is a k-basis of the algebra $k\langle X|S\rangle$.*

It is easy to see that the converse is also true (see [16]).

In the paper [10], Shirshov found a linear basis of a free product of Lie algebras with an amalgamation as an application of his Composition-Diamond Lemma for Lie algebras. Then he found an example proving that an analog of the Kurosh subgroup theorem [61] for a free product of groups, as well as Kurosh's [60] and Gainov's [46] theorems for subalgebras of free products of non-associative or (anti)commutative non-associative algebras, are not valid for subalgebras of free products of Lie algebras. Kukin [59], [58] found a description of subalgebras of free (amalgamated) products of Lie algebras.

In the paper [24], Shirshov's Composition-Diamond Lemma was systematically used in order to prove the following embedding theorem: Let M be any recursively enumerable set of natural numbers. Let

$$L_M = \mathrm{Lie}(a, b, c, a_1, b_1, c_1 \mid [ab^k c] = [a_1 b_1^k c_1], k \in M)$$

be a recursively presented Lie algebra. Then L_M is embeddable into a finitely presented Lie algebra L. If M is not recursive, then the word problem is undecidable in L_M and hence in L.

This gave the negative solution of the word problem for Lie algebras. An explicit example of a finitely presented Lie algebra with undecidable word problem was given by Kukin [57]. The proof in [24] used Matiyasevich's solution of Hilbert's 10th problem [73] and some ideas of the Higman theorem [52] that any recursively presented group is embeddable into a finitely presented group. There remained the problem of whether any recursively presented Lie (associative) algebra can be

embedded into a finitely presented Lie (associative) algebra. V. Belyaev [17] solved positively the problem for associative algebras.

In the paper [25], Shirshov's Composition-Diamond Lemma for associative algebras was used to prove an embedding theorem for associative algebras: For any associative algebras A, A_i $(i = 1, 2, 3, 4)$ with appropriate cardinality conditions, for example, all of them are algebras of countable dimension and A_i $(i = 1, 2, 3, 4)$ is the union of a countable increasing series of subalgebras with factors of countable dimension. Then A can be embedded into a simple associative algebra which is a sum of A_i $(i = 1, 2, 3, 4)$; in particular, A can be embedded into a finitely generated simple associative algebra. By the way, answering a question raised by [25], Shelah [81] constructed an example of an associative algebra of uncountable dimension which is not a union of a countable increasing series of subalgebras with factors of uncountable dimension.

In the paper [26], Shirshov's Composition-Diamond Lemma for Lie algebras was used to prove an embedding theorem for Lie algebras: Any Lie algebra is embeddable into an algebraically closed (in particular simple) Lie algebra which is a sum of four prescribed Lie subalgebras with the same cardinality conditions as in [25] above.

In the papers [20], [21], [23], there were found normal forms of elements of Novikov's and Boone's groups, as well as relative normal forms of some groups of quotients of multiplicative semigroups of some rings. Actually, those normal forms are the (relative) irreducible words for (relative) Gröbner-Shirshov bases of the groups, see [33], [39].

In the papers [74], [75], there were proved Composition-Diamond Lemmas for colore Lie superalgebras, Lie p-algebras and Lie p-superalgebras.

In the papers [54], [40], there were proved Composition-Diamond Lemmas for modules.

In the paper [28], it was proved Composition-Diamond Lemma for associative conformal algebras.

Some other papers on Gröbner–Shirshov bases one may found in surveys [29], [30], [31].

References

[1] Shirshov, A.I., *Subalgebras of free Lie algebras*. (Russian) Mat. Sb., N. Ser. **33(75)**, 441–452 (1953).

[2] Shirshov, A.I. *On representation of Lie rings in associative rings.* (Russian) Usp. Mat. Nauk **8**, No.5 (57), 173–175 (1953).

[3] Shirshov, A.I. *Certain problems of the theory of non-associative algebras.* Thesis, Moscow State University, 1953.

[4] Shirshov, A.I. *Subalgebras of free commutative and free anti-commutative algebras. Mat. Sbornik.*, **34(76)** (1954), 81–88.

[5] Shirshov, A.I., *Some theorems on embedding for rings*. (Russian) Mat. Sb., N. Ser. **40(82)**, 65–72 (1956).

[6] Shirshov, A.I., *On free Lie rings.* (Russian) Mat. Sb., N. Ser. **45(87)**, 113–122 (1958).

[7] Shirshov, A.I., *On bases of a free Lie algebra.* (Russian) Algebra Logika **1**, No.1, 14–19 (1962).

[8] Shirshov, A.I., *Certain algorithmic problems for ϵ-algebras.* (Russian) Sib. Mat. Zh. **3**, 132–137 (1962).

[9] Shirshov, A.I., *Certain algorithmic problems for Lie algebras.* (Russian) Sib. Mat. Zh. **3**, 292–296 (1962). English translation: Shirshov, A.I., *Certain algorithmic problems for Lie algebras.* (English) ACM SIGSAM Bull. **33**, No. 2, 3–6 (1999).

[10] Shirshov, A.I., *On the conjecture of the theory of Lie algebras.* (Russian) Sib. Mat. Zh. **3**, 297–301 (1962).

[11] A.I. Shirshov, *Collected Works. Rings and Algebras*. Nauka, Moscow, 1984.

[12] Adjan, S.I. Defining relations and algorithmic problems for groups and semigroups. (English. Russian original) Proc. Steklov Inst. Math. **85**, 152 p. (1966); translation from Tr. Mat. Inst. Steklov **85**, 123 p. (1966).

[13] Yu.A. Bahturin, A.A. Mikhalev, M.V. Zaicev, and V.M. Petrogradsky, *Infinite Dimensional Lie Superalgebras*. Walter de Gruyter Publ., Berlin, New York, 1992.

[14] Bahturin, Yuri; Mikhalev, Alexander A.; Zaicev, Mikhail Infinite-dimensional Lie superalgebras. (English) Hazewinkel, M. (ed.), Handbook of algebra. Volume 2. Amsterdam: North-Holland. 579–614 (2000).

[15] Backelin, Jörgen; Cojocaru, Svetlana; Ufnarovski, Victor *The computer algebra package Bergman: Current state.* (English) Herzog, Jürgen (ed.) et al., commutative algebra, singularities and computer algebra. Proceedings of the NATO advanced research workshop, Sinaia, Romania, September 17–22, 2002. Dordrecht: Kluwer Academic Publishers. NATO Sci. Ser. II, Math. Phys. Chem. 115, 75–100 (2003).

[16] G.M. Bergman, *The Diamond Lemma for ring theory. Adv. in Math.*, **29**(1978), 178–218.

[17] Belyaev, V. Ya. *Subrings of finitely presented associative rings.* (English) Algebra Logika **17**, 627–638 (1978).

[18] Bokut, L.A., *Embedding of Lie algebras into algebraically closed Lie algebras.* (Russian) Algebra Logika **1**, No.2, 47–53 (1962).

[19] Bokut, L.A., *Bases of free poly-nilpotent Lie algebras.* (Russian) Algebra Logika **2**, No.4, 13–19 (1963).

[20] L.A. Bokut, *On a property of the Boone groups.* Algebra i Logika Sem., **5** (1966), 5, 5–23; **6** (1967), 1, 15–24.

[21] L.A. Bokut, *On Novikov's groups.* Algebra i Logika Sem., **6** (1967), 1, 25–38.

[22] Bokut, L.A., *Degrees of insolvability of the conjugacy problem for finitely presented groups.* (Russian) Algebra Logika **7**, No.5, 4–70; No.6, 4–52 (1968).

[23] L.A. Bokut, *Groups of fractions of multiplication semigroups of certain rings. I–III, Malcev's problem.* Sibir. Math.J., **10**, 2, 246–286; 4, 744–799; 4, 800–819; 5, 965–1005.

[24] L.A. Bokut, *Unsolvability of the word problem, and subalgebras of finitely presented Lie algebras.* Izv. Akad. Nauk SSSR Ser. Mat. **36** (1972), 1173–1219.

[25] L.A. Bokut, *Imbeddings into simple associative algebras.* Algebra i Logika Sem., **15** (1976), 117–142.

[26] Bokut', L.A., *On algebraically closed and simple Lie algebras.* (Russian, English) Proc. Steklov Inst. Math. **148**, 30–42 (1978).

[27] L.A. Bokut, Yuqun Chen, *Gröbner-Shirshov bases for Lie algebras: after A.I. Shirshov. SEA Bull Math.,* **31** (2007), 811–831.

[28] L.A. Bokut, Y. Fong, W.- F. Ke, *Composition Diamond Lemma for associative conformal algebras. J. Algebra*, **272**(2004), 739–774.

[29] L.A. Bokut, Y. Fong, W.-F. Ke, P.S. Kolesnikov, *Gröbner and Gröbner-Shirshov bases in Algebra and Conformal algebras. Fundamental and Applied Mathematics*, **6**(2000), N3, 669–706 (in Russian).

[30] L.A. Bokut, P.S. Kolesnikov, *Gröbner-Shirshov bases: From Incipient to Nowdays*, *Proceedings of the POMI*, **272**(2000), 26–67.

[31] L.A. Bokut, P.S. Kolesnikov, *Gröbner-Shirshov bases: conformal algebras and pseudoalgebras*, *Journal of Mathematicfal Sciences*, **131**(5)(2005), 5962–6003.

[32] L.A. Bokut, and G.P. Kukin, Algorithmic and combinatorial algebra. Mathematics and its Applications, 255. Kluwer Academic Publishers Group, Dordrecht, 1994.

[33] L.A. Bokut, K.P. Shum, *Relative Gröbner-Shirshov bases for algebras and groups.* Algebra i Analiz **19** (2007), no. 6, 1–21.

[34] Bourbaki, N. Elements de mathematique. Fasc. XXXVII: Groupes et algèbres de Lie. Chap. II: Algèbres de Lie libres. Chap. III: Groupes de Lie. (French) Actualites scientifiques et industrielles 1349. Paris: Hermann. 320 p. (1972)

[35] B. Buchberger, An algorithm for finding a basis for the residue class ring of a zero-dimensional polynomial ideal. (German). Ph.D. thesis, University of Innsbruck, Austria, 1965.

[36] B. Buchberger, *An algorithmical criteria for the solvability of algebraic systems of equations.* (German). Aequationes Math. **4** (1970), 374–383.

[37] Cartier, P. *Remarques sur le theore me de Birkhoff-Witt.* (French) Ann. Sc. Norm. Super. Pisa, Sci. Fis. Mat., III. Ser. **12**, 1–4 (1958).

[38] K.T. Chen, R.H. Fox, and R.C. Lyndon, *Free differential calculus, IV: the quotient groups of the lower central series. Annals of Mathematics* **68** (1958), pp. 81–95.

[39] Yuqun Chen, Wenshu Chen and Runai Luo, *Word problem for Novikov's and Boone's group via Gröbner-Shirshov bases.*, SEA Bull Math., **32**(2008), 5.

[40] E.S. Chibrikov, *On free Lie conformal algebras.* Vestnik Novosib. State Univ., Ser. "Math, Mech, Inform.", **4** (2004), No 1, 65–83 (in Russian).

[41] Chibrikov, E.S. *A right normed basis for free Lie algebras and Lyndon–Shirshov words.* J. Algebra **302**, No. 2, 593–612 (2006).

[42] Cohn, P.M. Universal algebra. (English) Harper's Series in Modern Mathematics. New York-Evanston-London: Harper and Row, Publishers 1965, XV, 333 p. (1965).

[43] Cohn, P.M. *A remark on the Birkhoff-Witt theorem.* (English) J. Lond. Math. Soc. **38**, 197–203 (1963).

[44] Cohn, P.M. *Sur le critère de Friedrichs pour les commutateurs dans une algèbre asociative libre.* Comptes Rendus Acad. Science Paris, **239**, 743–745 (1954).

[45] Friedrichs, K.O. *Mathematical aspects of the quantum theory of fields. V.* (English) Commun. Pure Appl. Math. **6**, 1–72 (1953).

[46] Gainov, A.T. *Free commutative and free anticommutative products of algebras.* (Russian) Sib. Mat. Zh. **3**, 805–833 (1962).

[47] Gerasimov, V.N. *Distributive lattices of subspaces and the equality problem for algebras with a single relation.* Algebra Logic **15** (1976), 238–274 (1977); translation from Algebra Logika **15**, 384–435 (1976).

[48] Gerdt, V.P.; Kornyak, V.V. *Program for constructing a complete system of relations, basis elements, and commutator table for finitely presented Lie algebras and superalgebras.* (English. Russian original) Program. Comput. Softw. **23**, No. 3, 164–172 (1997); translation from Programmirovanie 1997, No.3, 58–71 (1997).

[49] P. Hall, *A contribution to the theory of groups of prime power order. Proc. London Math. Soc. Ser.* 2, **36** (1933), pp. 29–95.

[50] M. Hall, *A basis for free Lie rings and higher commutators in free groups. Proc. Amer. Math. Soc.* **3**(1950), pp. 575–581.

[51] G. Higman, B.H. Neumann, H. Neumann, *Embedding theorems for groups. J. London Math. Soc.* **24** (1949) 247–254.

[52] Higman, G. *Subgroups of finitely presented groups.* (English) Proc. R. Soc. Lond., Ser. A **262**, 455–475 (1961).

[53] H. Hironaka, *Resolution of singularities of an algebraic variety over a field of characteristic zero, I, II. Ann. Math.*, **79**(2) (1964), pp. 109–203, 205–326.

[54] S.-J. Kang, K.-H. Lee, Gröbner–Shirshov bases for irreducible sl_{n+1}-modules, *Journal of Algebra*, **232** (2000), 1–20.

[55] Knuth, D.E.; Bendix, P.B. *Simple word problems in universal algebras.* Comput. Probl. abstract Algebra, Proc. Conf. Oxford 1967, 263–297 (1970).

[56] D. Kozybaev, L. Makar-Limanov, U. Umirbaev, *The Freiheitssatz and the automorphisms of free right-symmetric algebras*, *Asian-European J. Math.* **1** (2008), 2, 243–252.

[57] G.P. Kukin, *On the word problem for Lie algebras.* Sibirsk. Math. Zh. **18** (1977), 1194–1197.

[58] Kukin, G.P. *Subalgebras of a free Lie sum of Lie algebras with an amalgamated subalgebra.* Algebra Logic **11**(1972), 59–86.

[59] Kukin, G.P. *On the Cartesian subalgebras of a free Lie sum of Lie algebras.* Algebra Logika **9**, 701–713 (1970).

[60] Kurosh, A., *Nonassociative free algebras and free products of algebras.* (Russian. English summary) Mat. Sb., N. Ser. **20(62)**, 239–262 (1947).

[61] Kurosch, A. *Die Untergruppen der freien Produkte von beliebigen Gruppen.* (German) Math. Ann. **109**, 647–660 (1934)

[62] Lazard, M. Groupes, anneaux de Lie et problème de Burnside. C.I.M.E., Gruppi, Anelli di Lie e Teoria della Coomologia 60 p. (1960). The same in: Instituto Matematico dell'Universita di Roma (1960).

[63] Lothaire, M. Combinatorics on words. Foreword by Roger Lyndon. Encyclopedia of Mathematics and Its Applications, Vol. 17. Reading, Massachusetts, etc.: Addison-Wesley Publishing Company, Advanced Book Program/World Science Division. XIX, 238 p. (1983).

[64] Lothaire, M. Combinatorics on words. Foreword by Roger Lyndon. 2nd ed. Encyclopedia of Mathematics and Its Applications. 17. Cambridge: Cambridge University Press. xvii, 238 p.(1997).

[65] Lyndon, R.C. *On Burnside's problem.* Trans. Am. Math. Soc. **77**, 202–215 (1954).

[66] Lyndon, R.C. *A theorem of Friedrichs.* Mich. Math. J. **3**, 27–29 (1956).

[67] Magnus, W. *Über diskontinuierliche Gruppen mit einer definierenden Relation* (*Der Freiheitssatz*). *J. Reine Angew. Math* **163***(1930), pp. 141–165.*

[68] Magnus, *W. Das Identitätsproblem für Gruppen mit einer definierenden Relation.* (German) Math. Ann. **106**, 295–307 (1932).,

[69] W. Magnus, *Über Beziehungen zwischen höheren Kommutatoren. J. Reine Angew. Math* **177***(1937), pp. 105–115.*

[70] Makar-Limanov, L. *Algebraically closed skew fields.* J. Algebra 93, 117–135 (1985).

[71] Makar-Limanov, L.G. *On algebras with one relation.* Usp. Mat. Nauk **30**, No.2(182), 217 (1975).

[72] Malcev, A.I.,*On representation of nonassociative rings.* Uspehi Mat. Nauk N.S. **7** (1952), 181–185.

[73] Matiyasevich, Yu.V. *Enumerable sets are diophantine.* Russian original) Sov. Math., Dokl. 11, 354–358 (1970); translation from Dokl. Akad. Nauk SSSR 191, 279–282 (1970).

[74] Mikhalev, A.A., *The junction lemma and the equality problem for color Lie superalgebras.* Vestnik Moskov. Univ. Ser. 1. Mat. Mekh. 1989, no. 5, 88–91. English translation: Moscow Univ. Math. Bull. 44 (1989), 87–90.

[75] A.A. Mikhalev, *Shirshov's composition techniques in Lie superalgebras* (*non-commutative Gröbner bases*). Trudy Sem. Petrovsk. **18** (1995), 277–289.

[76] A.A. Mikhalev and A.A. Zolotykh, *Combinatorial Aspects of Lie Superalgebras*. CRC Press, Boca Raton, New York, 1995.

[77] V.N. Latyshev, *Combinatorial Theory of Rings. Standard Bases*. Moscow State Univ. Publ. House, Moscow, 1988.

[78] T. Mora, *Gröbner bases for non-commutative polynomial rings.* Lecture Notes in Comput. Sci. **229** (1986), 353–362.

[79] C. Reutenauer. Free Lie algebras. London Mathematical Society Monographs. New Series, 7. Oxford Science Publications. The Clarendon Press, Oxford University Press, New York, 1993.

[80] C. Reutenauer. *Dimensions and characters of the derived series of the free Lie algebra.* In M. Lothaire, Mots, Melanges offerts a M.-P. Schützenberger, pp. 171–184. Hermes, Paris.

[81] Shelah, Saharon *On a problem of Kurosh, Jonsson groups, and applications.* (English) Word problems II, Stud. Logic Found. Math. Vol. 95, 373–394 (1980).

[82] Viennot, Gerard. Algèbres de Lie libres et monoides libres. Bases des algèbres de Lie libres et factorisations des monoides libres. (French) Lecture Notes in Mathematics. 691. Berlin-Heidelberg-New York: Springer-Verlag. 124 p. (1978)

[83] E. Witt, *Treue Darstellungen Lieschen Ringe. J. Reine Angew. Math.* **177**(1937), pp. 152–160.

[84] E. Witt, *Subrings of free Lie rings Math. Zeit.*, 64(1956), 195–216.

[85] V.A. Ufnarovski, *Combinatorial and Asymptotic Methods in Algebra*. Encyclopaedia Math. Sci. **57** (1995), 1–196.

[86] A.I. Zhukov, *Reduced systems of defining relations in non-associative algebras Mat. Sb., N. Ser.*, 27(69) (1950), 267–280.

[87] Zolotykh, A.A.; Mikhalev, A.A. *Algorithms for construction of standard Gröbner-Shirshov bases of ideals of free algebras over commutative rings.* (English. Russian original) Program. Comput. Softw. 24, No. 6, 271–272 (1998); translation from Programmirovanie 1998, No.6, 10–11 (1998).

Some of A.I. Shirshov Works

V.K. Kharchenko

In his first published paper "Subalgebras of free Lie algebras" A.I. Shirshov proved for Lie algebras an analog of the famous Nielsen-Schreier theorem: every subalgebra of a free Lie algebra is free. Three years later this theorem was independently proved and extended to restricted Lie algebras by E. Witt [38]. Much later this result was generalized to Lie superalgebras (A.S. Shtern [29]), and to colored Lie superalgebras (A.A. Mikhalev [20, 21, 22]). These results went through further development in the field of quantum algebra as follows. The Shirshov–Witt theorem for Lie algebras over fields of characteristic zero admits an equivalent formulation in terms of a free associative algebra: Every Hopf subalgebra of a free algebra $\mathbf{k}\langle y_i\rangle$ with the coproduct set up by $\Delta(y_i) = y_i \otimes 1 + 1 \otimes y_i$ is free. If we consider the free algebra as a braided Hopf algebra with a very special braiding ($\tau(y_i \otimes y_j) = p_{ij}y_j \otimes y_i,\ p_{ij}p_{ji} = 1$), then we get a reformulation of the Mikhalev-Shtern generalization as well. We may consider the free associative algebra $\mathbf{k}\langle V\rangle$ as a braided Hopf algebra provided that V is a braided space with arbitrary braiding (not necessary invertible). In this setting the braided version of the Shirshov-Witt theorem takes up the following form [12]. If a subalgebra $U \subseteq \mathbf{k}\langle V\rangle$ is a right categorical right coideal, that is $\Delta(U) \subseteq U\underline{\otimes}\mathbf{k}\langle V\rangle,\ \tau(\mathbf{k}\langle V\rangle \otimes U) \subseteq U\otimes\mathbf{k}\langle V\rangle$, then U is a free subalgebra.

A detailed investigation of free generators for subalgebras of a free Lie algebra and their ranks can be found in the papers [15, 23, 25]. An analogue of Schreier's formula was found by V. Petrogradsky for free Lie (super)algebras in terms of formal power series [27, 28]. Description of automorphism groups of free Lie algebras is closely related to the theorem of A.I. Shirshov on subalgebras. In 1964 P. Cohn [4] proved that the automorphisms of free Lie algebras of a finite rank are tame, i.e., the automorphism group is generated by elementary automorpisms. Defining relations of the automorphism group were described in 2007 by U.U. Umirbaev [36]. A detailed investigation of automorphisms of free Lie algebras and their applications can be found in the papers [15, 26, 23, 34, 35, 24, 25, 27]. The Shirshov-Witt theorem on subalgebras gives also the decidability of the occurrence problem for free Lie algebras (see, also [15]). In 1990 U.U. Umirbaev proved

[32] that finitely generated subalgebras of free Lie algebras are finitely separable. The occurrence problem for free Lie algebras and for relatively free algebras was studied in [33, 6, 7].

In a small note "On representation of Lie rings in associative rings" A.I. Shirshov constructed an example of a Lie ring that has no faithful representations in associative rings. This example shows that the Poincare-Birkhoff-Witt theorem may not be extended to Lie algebras over arbitrary commutative rings. Recall that the original proof of the PBW-theorem for Lie algebras over fields remains valid for Lie algebras over commutative rings, provided that the algebra is a free module over the ring of scalars [1, 37]. However it is not evident if a free Lie algebra over any commutative ring indeed is a free module over the ring of scalars. A.I. Shirshov in his fundamental paper "On free Lie rings" showed in particular that this question has an affirmative answer. Independently M. Lazard [17] and P. Cartier [2] proved that every Lie algebra over a Dedekind domain has a representation in an associative ring. If the ring of scalars itself is an algebra over the rationals, the representation exists as well (P. Cohn [3]). Later H.-J. Higgins in [8] found necessary and sufficient conditions for the module structure for a Lie algebra over a commutative ring to have a representation in an associative ring. It should be emphasized that the embedding problems are the most subtle problems located at the interfaces between algebra and logic. Sometimes in this area deep and extensive investigations trace back to publications with serious gaps and errors, see for example the historical notes [30]. Even in our time there appear such publications concerning the representation of generalizations of Lie algebras in associative rings in serious mathematical journals (see a discussion in [12, Section 5]).

In the paper "On free Lie rings" in order to construct a basis of a free Lie algebra (over a commutative ring) A.I. Shirshov introduced a class of words that is fundamental for modern combinatorial theory. This class of words was independently discovered by R. Lyndon several years before [19]. Now these words are called *Lyndon words* or *Lyndon-Shirshov words*, see M. Lothaire [18].

The method of Lyndon-Shirshov words remains a very effective tool for modern investigations in algebra. This allows one to construct a PBW-basis in arbitrary Hopf algebra generated by skew-primitive semi-invariants, [11], or in a braided Hopf algebra with a so-called triangular set of primitive generators [31]. In a more general setting, [5], it is possible to find some kind of factorization of graded Hopf algebras using Lyndon-Shirshov words. An interesting development is due to P. Lalonde and A. Ram. They found an elegant representation of the Lyndon-Shirshov basis for classical finite-dimensional simple Lie algebras, see [16, Figure 1]. More recently the method of Lyndon-Shirshov words has proved to be an extremely important tool for classification of right coideal subalgebras in quantum groups [13, 14].

One more result from the paper "On free Lie rings" that has a reflection to contemporaneity, the Freiderich criterion (Theorem 3 in that paper), shows that the elements of a given free Lie algebra (over a commutative ring Σ) can be distinguished in the enveloping free associative algebra (over Σ) as primitive

elements with respect to the diagonal coproduct. Even though A.I. Shirshov did not introduce the very same coproduct, in Theorem 3 one may replace the commuting variables a_i, a_i' with $a_i \otimes 1$ and $1 \otimes a_i$ respectively. Then the condition

$$f(a_1 + a_1', \ldots, a_n + a_n') = f(a_1, \ldots, a_n) + f(a_1', \ldots, a_n')$$

reduces to $\Delta(f) = f \otimes 1 + 1 \otimes f$, where Δ is the diagonal coproduct defined on the generators via $\Delta(a_i) = a_i \otimes 1 + 1 \otimes a_i$ and extended to the enveloping free algebra as an algebra homomorphism $\Delta : \mathfrak{A}_{\Sigma R} \to \mathfrak{A}_{\Sigma R} \otimes \mathfrak{A}_{\Sigma R}$.

In the paper "On rings with identity relations" A.I. Shirshov in particular proves that every associative PI-ring algebraic over a central subring Z_1 is in some sense finite over Z_1 (Theorem 4 in the paper). This new notion of finiteness is close to but not identical with the notion of finitely generated module. It is interesting that essentially the same notion over a not necessarily central subring appears in the modern noncommutative Galois theory. More precisely a subring $A \subseteq R$ is called (right) *Shirshov finite* over a subring $D \subseteq R$ if there exists a finite number of elements $r_1, r_2, \ldots, r_k$ such that $A \subseteq r_1 D + r_2 D + \cdots + r_k D$. The Shirshov theorem (Theorem 4 in the paper) says that R^n is Shirshov finite over Z_1, where n is the degree of PI-identity of the finitely generated ring R. The same finiteness relation in local form exists between a given semiprime ring R and its Galois subring R^G with respect to a finite group G of automorphisms, [9, 10, Theorem 5.10.1]. In more detail, suppose that semiprime associative ring R has no additive $|G|$-torsion (or more generally G is a Maschke group, [9, 10, Definition 5.4.13]). Then R has an essential two-sided ideal I that is locally finite in the Shirshov sense over the fixed ring $R^G = \{r \in R \mid \forall g \in G,\ g(r) = r\}$. Here the *local finiteness* means that each finitely generated right ideal $A \subseteq I$ is Shirshov finite over R^G as a subring.

References

[1] G. Birkhoff, Representability of Lie algebras and Lie groups by matrices, Annals Math., v.38(1937), 526–532.

[2] P. Cartier, Remarques sur le théorème de Birkhoff–Witt, Ann. Scuola norm sup. Pisa, Sci. fis. mat. v.3, Ser. 12(1958), 1–4.

[3] P.M. Cohn, A remark on the Birkhoff–Witt theorem, J. London Math. Soc., v. 38(1963), 197–203.

[4] P.M. Cohn, Subalgebras of free associative algebras, Proc. London Math. Soc. (3) 14, (1964), 618–632.

[5] M. Graña, I. Heckenberger, On a factorization of graded Hopf algebras using Lyndon words, Journal of Algebra, v. 314, N1(2007), 324–343.

[6] C.K. Gupta and U.U. Umirbaev, Systems of linear equations over associative algebras and the occurence problem for Lie algebras, Commun. Algebra, 27(1999), 411–427.

[7] C.K. Gupta and U.U. Umirbaev, The occurence problem for free metanilpotent Lie algebras, Commun. Algebra, 27(1999), 5857–5876.

[8] H.-J. Higgins, Baer invariants and the Birkhoff–Witt theorem, Journal of Algebra, v. 11(1969), 469–482.

[9] V.K. Kharchenko, Automorphisms and Derivations of Associative Rings, Kluwer Academic Publishers, Dordrecht-Boston-London, 1991.

[10] V.K. Kharchenko, Noncommutative Galois Theory, Nauchnaja Kniga, Novosibirsk, 1996.

[11] V.K. Kharchenko, A quantum analog of the Poincaré-Birkhoff-Witt theorem, Algebra i Logika, 38, N4(1999), 476–507. English translation: Algebra and Logic, 38, N4(1999), 259–276 (QA/0005101).

[12] V.K. Kharchenko, Braided version of Shirshov–Witt theorem, Journal of Algebra, 294, N1(2005), 196–225.

[13] V.K. Kharchenko, PBW-bases of coideal subalgebras and a freeness theorem, Transactions of the American Mmathematical Society, v. 360, N10(2008), 5121–5143.

[14] V.K. Kharchenko, A.V. Lara Sagahon, Right coideal subalgebras in $U_q(\mathfrak{sl}_{n+1})$, Journal of Algebra, v. 319 (2008), 2571–2625.

[15] G.P. Kukin, Primitive elements of free algebras, Algebra i Logika, v. 9, N4(1970), 458–472. English translation: Algebra and Logic, v. 9 (1970), 275–284.

[16] P. Lalonde, A. Ram, Standard Lyndon bases of Lie algebras and enveloping algebras, Transactions of the American Mathematical Society, v. 347, N5(1995), 1821–1830.

[17] M. Lazard, Sur les algèbres enveloppantes universelles de certaines algèbres de Lie, Publ. Sci. Univ. Alger, Sér. A. v. 1(1954), 281–294.

[18] M. Lothaire, Algebraic Combinatorics on Words,Cambridge Univ. Press, 2002.

[19] Lyndon, R.C. On Burnside's problem, Trans. Am. Math. Soc., 77(1954), 202–215.

[20] A.A. Mikhalev, Subalgebras of free color Lie superalgebras, Mat. Zametki 37 N5 (1985) 653–661. English translation: Math. Notes 37 (1985) 356–360.

[21] A.A. Mikhalev, Free color Lie superalgebras, Dokl. Akad. Nauk SSSR, 286, N3 (1986) 551–554. English translation: Soviet Math. Dokl. 33 (1986) 136–139.

[22] A.A. Mikhalev, Subalgebras of free Lie p-superalgebras, Mat. Zametki 43 N2 (1988) 178–191. English translation: Math. Notes 43 (1988) 99–106.

[23] A.A. Mikhalev, Primitive elements and automorphisms of free algebras of Schreier varieties, J. Math. Sci., 102, N6(2000), 4628–4640.

[24] A.A. Mikhalev, U.U. Umirbaev, J.-T. Yu, Automorphic orbits of elements of free nonassociative algebras, Journal of Algebra, 243(2001), 198–223.

[25] A.A. Mikhalev, U. Umirbaev, Jie-Tai Yu, Generic, almost primitive and test elements of free Lie algebras, Proc. Amer. Math. Soc., 130(2002), 1303–1310.

[26] A.A. Mikhalev, A.A. Zolotykh, Rank and primitivity of elements of free color Lie (p-)superalgebras, Intern. J. Algebra and Computation, 4(1994), 617–656.

[27] V.M. Petrogradsky, Schreier's formulae for free Lie algebras, their Applications and Asymptotics, Proceedings of International Algebraic Conference on 90th Birthday of A.G. Kurosh, Moscow, 1998, Ed. by Y. Bahturin, and de Gruyter, Berlin, 2000.

[28] V.M. Petrogradsky, Schreier's formula for free Lie algebras. Arch. Math. (Basel), 75(2000), no. 1, 16–28.

[29] A.S. Shtern, Free Lie superalgebras, Siberian Math. J. 27 (1986) 551–554.

[30] W. Schmid, Poincare and Lie groups, Bull. (N.S.) Amer. Math. Soc. v.6(1982), 175–186.

[31] S. Ufer, PBW bases for a class of braided Hopf algebras, Journal of Algebra, 280, N1(2004), 84–119.

[32] U.U. Umirbaev, On the approximation of free Lie algebras with respect to entry, Monoids, rings and algebras, Tartu: Tartuskij Universitet, Tartu Uelik. Toim., Mat.-Meh.-Alaseid Toeid, 878(1990), 147–152.

[33] U.U. Umirbaev, The occurrence problem for Lie algebras, Algebra Logic, 32 (1993), No. 3, 173–181 ; translation from Algebra Logika, 32(1993), No. 3, 326–340.

[34] U.U. Umirbaev, Partial derivations and endomorphisms of some relatively free Lie algebras, Sib. Math. J., 34(1993), No. 6, 1161–1170; translation from Sib. Mat. Zh. 34(1993), No. 6, 179–188.

[35] U.U. Umirbaev, On Schreier varieties of algebras, Algebra Logic, 33(1994), No. 3, 180–193; translation from Algebra Logika, 33 (1994), No. 3, 317–340 .

[36] U.U. Umirbaev, Definig relations for automorphism groups of free algebras, J. Algebra, 314 (2007), 209–225.

[37] E. Witt, Treue Darstellung Liescher Ringe, J. reine angew. Math. v. 177(1937), 152–160.

[38] E. Witt, Die Unterringe der freien Lieschen Ringe, Math. Zeitschr. Bd. 64 (1956) 195–216.

Comments on Shirshov's Height Theorem

Alexander Kemer

In 1941 A.G. Kurosh [1] posed the problem: Is every finitely-generated algebraic associative algebra finite-dimensional? In 1964 E.S. Golod and I.R. Shafarevich [2, 3] constructed a counterexample: they presented an infinite-dimensional finitely-generated nil-algebra. This counterexample shows that in general finitely-generated algebraic associative algebras are very far from being finite-dimensional.

Every problem can be considered not only as an explicit problem but as a direction of research. In the case of Kurosh's problem such a direction can be formulated in the following way: Find the conditions which imply that a finitely generated algebra is finite-dimensional.

Before the counterexample of Golod-Shafarevich was constructed, many positive results on Kurosh's problem were obtained. In 1945 N. Jacobson [4] solved the problem of Kurosh for algebraic algebras of bounded index. In 1946 J. Levitzky [5] proved that for a finitely generated PI-algebra over a commutative ring, if each element is nilpotent then the algebra is nilpotent. Finally, in 1948 I. Kaplansky [6] solved Kurosh's problem for PI-algebras over a field. All of these results became classical and are included in textbooks on ring theory. The great role of these results in ring theory is well known. In fact, the structure theory of rings developed around the problem of A.G. Kurosh.

In 1957 A.I. Shirshov proved his famous theorem on height:

Theorem (A.I. Shirshov [7]**).** *For any finitely-generated associative PI-algebra A over a commutative ring R with* 1*, there exist a natural number h and elements $a_1, \dots, a_n \in A$ such that any element of A can be represented as an R-linear combination of elements of the form*

$$a_{i_1}^{\alpha_1} \cdots a_{i_k}^{\alpha_k},$$

where $k < h$.

We note that an algebra A over a commutative ring R with 1 is called a PI-algebra if A satisfies some polynomial identity $f = 0$ such that the ideal of the ring R generated by the coefficients of the highest-degree terms of the polynomial f contains 1.

The positive solution of Kurosh's problem for PI-algebras over a ring follows immediately from Shirshov's theorem. Indeed, since the elements $a_1, \ldots, a_n \in A$ are algebraic (the elements $a_1, \ldots, a_n$ are taken from the conclusion of the theorem on height), the degrees α_i are bounded. Hence the algebra A is a finitely-generated R-module.

Comparing the solutions of Kurosh's problem obtained by I. Kaplansky and A.I. Shirshov one notes that the solution of I. Kaplansky is based on the well-developed structure theory of rings, but makes little use of the PI-condition. In fact, the PI-condition is used in two statements: (1) The radical of a finitely-generated algebraic PI-algebra is nilpotent; (2) A matrix algebra of order n does not satisfy a polynomial identity of degree less than $2n$. These statements are quite easy from the contemporary point of view.

The solution of A.I. Shirshov does not use the structure theory at all. Moreover A.I. Shirshov also made little use of algebraicity. It follows from the above that it is sufficient to require algebraicity only for some finite set of elements. But the most important merit of the theorem on height is that it was proved for algebras over a commutative ring. Many of the results in ring theory concerning PI-algebras would not have been obtained if the theorem on height were true only for algebras over fields.

With the first results about PI-algebras it became clear that the PI-condition is a peculiar finiteness condition. In 1957 S. Amitsur [8] proved a remarkable theorem: The radical of a finitely-generated PI-algebra is a nil-ideal. This theorem once again corroborated that the PI-condition is a finiteness condition, and allowed V.N. Latyshev at that time to formulate rather boldly the problem: Is the radical of a finitely-generated PI-algebra nilpotent? (See [9].) A great contribution to the solution of this problem was made by Yu.P. Razmyslov [10] who proved that the radical of finitely-generated PI-algebra over a field is nilpotent if and only if the algebra satisfies some standard identity. To prove this statement, Yu.P. Razmyslov constructed an embedding of certain algebras into algebras which are algebraic over the center and then applied the theorem on height. Yu.P. Razmyslov was the first algebraist to apply the theorem on height very often and deeply. For algebras over a field of characteristic zero, Latyshev's problem was solved by A.R. Kemer [11] who proved that every finitely-generated PI-algebra over a field of characteristic zero satisfies a standard identity of some order. Indeed this result and the theorem of Razmyslov mentioned above imply the positive solution of Latyshev's problem in the case of characteristic zero. In 1982, A. Braun [12] solved Latyshev's problem positively for algebras over a commutative Noetherian ring. At present the theorem on the nilpotency of the radical of a finitely-generated PI-algebra is known as the theorem of Braun-Kemer-Razmyslov.

In 1974, Yu.P. Razmyslov introduced a new concept of trace identity, and proved that each trace identity of the matrix algebra of order n over a field of characteristic 0 follows from the Cayley-Hamilton trace identity of degree n and the identity $\mathrm{Tr}(1) = n$ [13]. Little later C. Procesi [14] proved actually the same result in the terms of invariants.

The Cayley-Hamilton identity of degree n has the form

$$X_n(x) = x^n + b_1(x)x^{n-1} + \cdots + b_n(x) = 0,$$

where the coefficient $b_m(x)$ is a form of degree m. In the case of characteristic zero the coefficients $b_m(x)$ can be represented as linear combinations of trace monomials of the form

$$\mathrm{Tr}(x^{i_1})^{\alpha_1}\mathrm{Tr}(x^{i_2})^{\alpha_2}\cdots\mathrm{Tr}(x^{i_k})^{\alpha_k}.$$

Of course this theorem of Yu.P. Razmyslov does not concern the theorem on height directly, but the idea of trace identities gives a way of embedding (if possible) a finitely-generated PI-algebra over a field into a finite-dimensional algebra (a matrix algebra) over a larger field (such algebras are called representable). Indeed, let a finitely-generated algebra A over a field F be embeddable into the matrix algebra $M_n(K)$, $F \subseteq K$. Consider the F-subalgebra $C = SA$, where S is the F-subalgebra (with unity) of the field K generated by all the elements $b_m(a)$ $(a \in A)$ where the elements $b_m(a)$ are the coefficients of the Cayley-Hamilton identity of degree n. It follows from this that in the case of characteristic zero the algebra A is embeddable into the algebra

$$D = A \otimes T\langle A\rangle / J,$$

where $T\langle A\rangle$ is the commutative algebra generated by the symbols $\mathrm{Tr}(a), a \in A$, the trace on the algebra $A \otimes T\langle A\rangle$ is defined by the formula

$$\mathrm{Tr}\Big(\sum a_k \otimes t_k\Big) = \sum \mathrm{Tr}(a_k)t_k,$$

and the ideal J is generated by the elements $X_n(d)$ $(d \in A \otimes T\langle A\rangle)$. In the case of characteristic p the algebra $A \otimes T\langle A\rangle$ is generated by the symbols $b_m(a)$ $(a \in A)$. The forms $b_m(x)$ are defined in the same manner but with more complicated formulas.

Assume that the algebra A is embeddable into the algebra D. Then the algebra A is embeddable into the algebra

$$D' = A \otimes T'\langle A\rangle / J \cap A \otimes T'\langle A\rangle,$$

where $T'\langle A\rangle$ is the subalgebra of $A \otimes T\langle A\rangle$ generated by the elements $b_m(a_i)$ (the elements a_i are taken from the conclusion of the theorem on height). The algebra D' is finitely-generated and algebraic over the commutative algebra $T'\langle A\rangle$ because it satisfies the Cayley-Hamilton identity. By the theorem on height the algebra D' is a finitely-generated $T'\langle A\rangle$-module. Since the algebra $T'\langle A\rangle$ is noetherian, by a theorem of K. Beidar [15] the algebras D' and A are representable. In 1995 the theorem of Razmyslov in the case of characteristic p was proved by A.R. Kemer at the multilinear level [16] and little later A.N. Zubkov proved this theorem at the homogeneous level [17].

A very important problem in the theory of PI-algebras was posed by W. Specht [18] in 1950: Does every associative algebra over a field of characteristic zero have a finite basis of identities? The finite basis problem makes sense for algebras over any field, and even for rings, groups and arbitrary general algebraic systems.

A positive solution of the finite basis problem for a given class of algebraic systems is a sort of classification of these algebraic systems in the language of identities.

A rather large number of papers have been devoted to Specht's problem for associative algebras over a field of characteristic zero. We note the most important results. In 1977 V.N. Latyshev [19] proved that any associative algebra over a field of characteristic zero satisfying a polynomial identity of the form

$$[x_1, \dots, x_n] \cdots [y_1, \dots, y_n] = 0,$$

has a finite basis of identities. This result was also obtained independently by G. Genov [20] and A. Popov [21].

In 1982 A.R. Kemer reduced the Specht problem to the finite basis problem for graded identities of finitely-generated associative PI-superalgebras [22] and in 1986 he solved the Specht problem positively [23]. The first proof of the theorem on the finite basis of identities was rather complicated. A little later in 1987 A.R. Kemer [24] proved that relatively free finitely-generated associative PI-superalgebras over a field of characteristic zero are representable. This theorem implies the theorem on the finite basis, and explains the reason why the Specht problem has a positive solution. This reason is that finite-generated PI-algebras over a field of characteristic zero cannot be distinguished in the language of identities from finite-dimensional algebras. More precisely, for every finitely-generated PI-algebra A there exists a finitely-dimensional algebra C such that the ideals of identities of these algebras are equal. In 1988 A.R. Kemer proved the same result for algebras over an infinite field of characteristic p [25].

The main idea of the proof of this theorem is to approach step-by-step the given T-ideal Γ by the ideals of identities of finite-dimensional algebras. At the first step there is constructed a finite-dimensional algebra C_0 such that

$$T[C_0] \subseteq \Gamma.$$

The existence of this algebra follows from the theorem on nilpotency of Braun-Kemer-Razmyslov and the theorem of J. Lewin [33]. The most difficult part of the proof is the following statement: If $T[C] \subseteq \Gamma$, $T[C] \neq \Gamma$ (C is finite-dimensional) then there exists a finite-dimensional algebra C' such that

$$T[C] \subseteq T[C'] \subseteq \Gamma, \qquad T[C] \neq T[C'].$$

The proof of this statement uses identities with forms and the standard application of the theorem on height which was described above.

Examples of infinitely-based algebras in the case of characteristic p were constructed in 1999 by V.V. Schigolev [26] and A.Ya. Belov [27].

In 1998 A.Ya. Belov [28] announced a positive solution of the local finite basis problem for algebras over a commutative noetherian ring, and announced a result about the representability of the relatively free algebra over a commutative noetherian ring in some weak sense: The relatively free finitely-generated PI-algebra A over a commutative noetherian ring R is embeddable into some algebra

A' over a commutative noetherian ring R' such that A' is a finitely-generated R'-module ($R \subseteq R'$). In other words the algebra A is embeddable into the algebra of endomorphisms of some finitely generated R'-module.

Regarding the methods of A.Ya. Belov we should note that most of the ideas of A.Ya. Belov are combinatorial, and come from the theorem on height and other results of A.I. Shirshov. A.Ya. Belov developed the combinatorial ideas of A.I. Shirshov which made it possible to consider more complicated combinatorial situations than in the theorem on height. In this sense one can call A.Ya. Belov a successor of A.I. Shirshov.

Another nice idea is applying Zariski closure. This idea was new for PI-theory. The algebras of endomorphisms of finitely generated modules over a ring have a more complicated structure than finite-dimensional algebras, but applying Zariski closure A.Ya. Belov proved that a finitely-generated PI-algebra A over a commutative noetherian ring R has the same identities as some algebra C over a commutative noetherian ring R', $R \subseteq R'$, satisfying the property that the radical of the algebra C splits off and is nilpotent, i.e., $C = P + \operatorname{Rad} C$, where the subalgebra C is semisimple. Applying Zariski closure A.Ya. Belov also obtained a lot of information about the semiprime part P. We note that the main results of A.Ya. Belov are not yet published.

We also mention the results devoted to the estimation of height in the theorem of A.I. Shirshov. The height $h(A)$ of an algebra A depends on the number of generators s and the minimal degree of identities $m = \deg(A)$. The estimate for the height which follows from the proof of the theorem on height is not satisfactory. In 1982 A.G. Kolotov [29] obtained the estimate

$$h(a) \leq s^{s^m}.$$

In [30] E.I. Zelmanov raised a question about the exponential estimate of the height. The positive answer was obtained by A. Ya. Belov in 1988 [31, 32].

References

[1] A.G. Kurosh, Ringtheoretische Probleme, die mit dem Burnsideschen Problem uber periodische Gruppen in Zusammenhang stehen, Izv. Akad. Nauk SSSR. Ser. Mat., v. 5(1941), 233–240. (Russian)

[2] E.S. Golod, On nil-algebras and residually finite p-groups, Izv. Akad. Nauk SSSR. Ser. Mat., v. 28(1964), 273–276; English transl. in Amer. Math. Soc. Transl., v. 48(1965).

[3] E.S. Golod, I.R. Shafarevich, On class field towers, Izv. Akad. Nauk SSSR. Ser. Mat., v. 28(1964), 261–272; English transl. in Amer. Math. Soc. Transl., v. 48(1965).

[4] N. Jacobson, Structure theory for algebraic algebras of bounded degree, Ann. of Math., v. 2(1945), 695–707.

[5] J. Levitzky, On a blem of A. Kurosh, Bull. Amer. Math. Soc., v. 52(1946), 1033–1035.

[6] I. Kaplansky, Rings with a polynomial identity, Bull. Amer. Math. Soc., v. 54(1948), 575–580.

[7] A.I. Shirshov, On rings with polynomial identities, Mat. Sb., v. 43(1957), 277–283; English transl. in Amer. Math. Soc. Transl., v. 119(1983).

[8] S.A. Amitsur, A generalization of Hilbert's Nullstellensatz, Proc. Amer. Math. Soc., v. 8(1957), 649–656.

[9] The Dniester notebook: unsolved problems in the theory of rings and modules, 3rd ed. (V.A. Andrunakievich, editor), Inst. Mat. Sibirsk. Otdel. Akad. Nauk SSSR, Novosibirsk, (1982) (Russian).

[10] Yu.P. Razmyslov, On the Jacobson radical in PI-algebras, Algebra i logika, v. 13(1974), 337–360; English transl. in Algebra and logic, 13(1974).

[11] A.R. Kemer, Capelli identities and the nilpotence of the radical of a finitely-generated PI-algebra, Dokl. Akad. Nauk SSSR, v. 255(1980), 793–797; English transl. in Soviet Math. Dokl., v. 22(1980).

[12] A. Braun, The radical in finitely-generated $P.I.$ algebra, Bull. (New Ser.) Amer. Math. Soc., v. 7(1982), 385–386.

[13] Yu.P. Razmyslov, Trace identities of full matrix algebras over field of characteristic zero, Izv. Akad. Nauk SSSR Ser. Mat., v. 38(1974), 723–756; English transl. in Math. USSR Izv. v. 8.(1974)

[14] C. Procesi, The invariant theory of $n \times n$-matrices, Adv. in Math., v. 19(1076), 306–381.

[15] K.I. Beidar, On theorems of A.I. Mal'tsev concerning matrix representations of algebras, Uspekhi Mat. Nauk, v. 41(1986), 161–162; English transl. in Ruusian Math. Sueveys., v. 41(1986).

[16] A.R. Kemer, Multilinear identities of the algebras over a field of characteristic p, Int. J. of Alg. and Comp., v. 5(1995), 189–197.

[17] A.N. Zubkov, On the generalization of the theorem of Procesi-Razmyslov, Algebra i Logika, v. 35(1996), 433–457. English transl. in Algebra and logic, 35(1996).

[18] W. Specht, Gesetze in Ringen. I, Math. Z., v. 52(1950), 557–589.

[19] V.N. Latyshev, On the finite basis property for the identities of certain rings, Uspekhi Mat. Nauk v. 32(1977), 259–260. (Russian)

[20] G.K. Genov, Some Specht varieties of associative algebras, Pliska Stud. Math. Bulgar v. 2(1981), 30–40. (Russian)

[21] A.P. Popov, On the Specht property for some varieties of assocuative algebras, Pliska Stud. Math. Bulgar v. 2(1981), 41–53. (Russian)

[22] A.R. Kemer, Varieties and Z_2-graded algebras, Izv. Akad. Nauk SSSR. Ser. Mat., v. 48(1982), 1042–1059; English transl. in Math. USSR Izv. v. 25(1985).

[23] A.R. Kemer, Finite bases for identities of associative algebras, Algebra i Logika v. 26(1987), 597–641; English transl. in Algebra and logic, 26(1987).

[24] A.R. Kemer, Representation of relatively free algebras, Algebra i Logika v. 27(1988), 274–294; English transl. in Algebra and logic, 27(1988).

[25] A.R. Kemer, Identities of finitely generated algebras over an infinite field, Izv. Akad. Nauk SSSR. Ser. Mat., v. 54(1990), 726–753; English transl. in Math. USSR Izv. v. 29(1990).

[26] V.V. Schigolev, Examples of infinitely-based T-ideals, Fund. and Appl. Math., v. 5(1999), 307–312.

[27] A.Ya. Belov, On non-spechtian varieties, Fund. and Appl. Math., v. 5(1999), 47–66.

[28] A.Ya. Belov, Local representability of relatively free associative algebras, Kurosh Algebraic conference – 98. Abstracts of talks. Ed. by Yu.A. Bahturin, A.I. Kostrikin, A. Yu. Ol'shansky. Moscow, 1998, 143–144.

[29] A.G. Kolotov, On the upper estimation of the height in finitely-generated PI-algebras, Sibirsk. Mat. Zh., v. 23(1982), 187–189; English transl. in Siberian Math. J. v. 23(1982).

[30] The Dniester notebook: unsolved problems in the theory of rings and modules, 3rd ed. (V.A. Andrunakievich, editor), Inst. Mat. Sibirsk. Otdel. Akad. Nauk SSSR, Novosibirsk, (1993)(Russian).

[31] A.Ya. Belov, Estimations for the height and Gelfand-Kirillov dimension of associative PI-algebras, Abstracts of Int. alg. Maltsev's conf. Novosibirsk, 1989. (Russian)

[32] A.Ya. Belov, Some estimations for nilpotence og nil-algebras over field of an arbitrary characteristic and height theorem, Comm. in algebra. v. 20(1992), 2919–2922.

[33] J. Lewin, A matrix representation for associative algebras. I, II, Trans. Amer. Math. Soc., v. 188(1974), 293–308, 309–317.

Brief Review of the Life and Work of A.I. Shirshov

Evgenii Kuzmin

An outstanding Russian mathematician, Anatoliĭ Illarionovich Shirshov was born on the 8th of August 1921 in the village of Kolyvan in the Novosibirsk Region. Before the war he started his studies in Tomsk University and then went to the front as a volunteer, and after demobilization in 1946 he continued his studies in Voroshilovgrad (now Lugansk) Pedagogical Institute. He combined his studies at the Institute with working as a mathematics teacher at a secondary school.

In 1950, A.I. Shirshov entered the Graduate School of the Faculty of Mechanics and Mathematics at Moscow State University (MSU) where he studied under the supervision of Professor A.G. Kurosh. After successful defence in 1953 of his Candidate of Science thesis, *Some problems in the theory of nonassociative rings and algebras*, he started working at the Department of Higher Algebra at MSU, first as Assistant, and starting in 1955, as Docent. In 1957–1960, A.I. Shirshov worked as the First Deputy Dean of the Faculty (the Dean was A.N. Kolmogorov). These years witnessed the blossoming of his creative scientific activity: in rapid succession he published works in which he laid the foundation for a new direction in modern algebra, the theory of rings that are nearly associative. In 1958, A.I. Shirshov defended his Doctor of Science thesis, *On some classes of rings that are nearly associative*, and in 1961 he was promoted to the rank of Professor.

In 1960, A.I. Shirshov, upon the invitation of Academicians S.L. Sobolev, I.N. Vekua and A.I. Malcev, decided to participate in the realization of an important national program: raising the level of scientific activity in his native region of Siberia. Like many other scientists of the time, who answered the call of the Government, he took an active part in the organization of the Siberian Branch of the Academy of Sciences of the USSR. Together with Academician A.I. Malcev, he became one of the founders of the Siberian school of algebra and logic. By his scientific, administrative and public activities, he made a great contribution to the foundation and development of the Mathematical Institute and the entire Siberian Branch. From 1960 to 1973, he was Deputy Director of the Mathematical

Institute of the Siberian Branch, and from 1967 to his last days, he was the Head of Division of Ring Theory of the Mathematical Institute. Simultaneously he conducted extensive pedagogical work as a Professor of the Department of Algebra and Mathematical Logic of Novosibirsk State University.

In 1964, A.I. Shirshov was elected a Corresponding Member of the Academy of Sciences of the USSR. He became a member of the Bureau of the Mathematical Division of the Academy of Sciences, a member of the National Committee of Soviet Mathematicians, Chairman of the Committee on Algebra of the Academy of Sciences, and also a member of several scientific councils and editorial boards.

The circle of scientific interests of A.I. Shirshov was rather extensive: algebra, mathematical logic, number theory, and projective geometry. However, his creative activity was concentrated mostly on ring theory and problems of algebra on the border with mathematical logic. When A.I. Shirshov started his research in the theory of rings that are nearly associative (1953), this theory simply did not exist: there were merely definitions of various classes of nonassociative rings and some isolated results about these rings. Now, it is a well-developed branch of algebra that includes as its components the theories of infinite-dimensional Lie algebras, the theory of alternative algebras, the theory of Jordan algebras, and also the theories of wider classes of algebras: Malcev algebras, binary-Lie algebras, right-alternative algebras, and others. The theory of rings that are nearly associative owes its modern development largely to the works of A.I. Shirshov and his students.

Already in the first works of A.I. Shirshov on ring theory we find brilliant results that have become classical: the theorem on freeness of subalgebras of free Lie algebras, and the theorem on embedding of an arbitrary Lie algebra with a countable number of generators into a Lie algebra with two generators. The bases of the free Lie algebra constructed by A.I. Shirshov (the Lyndon-Shirshov basis, the Hall-Shirshov bases) have played an important role in the solution of various types of algorithmic problems in the theory of Lie algebras, and also find applications in group theory. The attention of specialists was attracted by A.I. Shirshov's beautiful example of a Lie algebra over a ring which does not have an enveloping associative algebra over the same ring.

In group theory as well as ring theory an important role is played by problems of Burnside type; one of the best-known problems of this kind is the problem posed by A.G. Kurosh: is an associative algebraic algebra necessarily locally finite? As is well known, in the general case this problem of Kurosh was given a negative answer by E.S. Golod: on the other hand, this problem was given a positive answer by Kaplansky in the class of associative algebras which satisfy a polynomial identity. A.I. Shirshov suggested a general combinatorial approach that provides a positive solution to the problem of Kurosh for alternative and special Jordan algebras of bounded degree, and proves local nilpotency in the particular case of nil rings of bounded index. Turning his attention to associative rings with identical relations, A.I. Shirshov proved a theorem on local boundedness of their heights which is an essential strengthening of the theorem of Kaplansky. Introducing natural definitions of algebraicity and local finiteness over a subring of the center, he

obtained another generalization of Kaplansky's theorem: an alternative ring with a non-trivial identity, which is algebraic over a subring of its center, is locally finite over that subring.

Perhaps the most beautiful and difficult theorem of A.I. Shirshov is the statement that any Jordan algebra with two generators is special. This served as the starting point of a long series of works by American authors on Jordan algebras with two and three generators and on identities of Jordan algebras.

An important event for algebra was the publication of the monograph *Rings that are nearly associative* (Moscow, Nauka, 1978) written by A.I. Shirshov in collaboration with his students K.A. Zhevlakov, A.M. Slinko and I.P. Shestakov.

Among the algorithmic problems of algebra, to A.I. Shirshov belongs the solution of the word problem and the proof of the freeness theorem in the classes of commutative and anticommutative algebras and Lie algebras with one defining relation (using what is now called Gröbner-Shirshov basis theory). He also solved the word problem for solvable Lie algebras of index 2.

The works of A.I. Shirshov in the theory of rings that are nearly associative have cleared the way for further investigations in this area. In the works of his students and followers, many problems stated by A.I. Shirshov were solved: decidability of the word problem in the class of all Lie algebras and in the class of solvable Lie algebras; the problem of computing the basis rank of the varieties of alternative and Malcev algebras; the problem of describing the subalgebras of the free product of Lie algebras; the problem of local nilpotency of Jordan nil-algebras of bounded index; and others.

In the last years of his life, A.I. Shirshov was actively engaged in theory of projective planes. He developed a new algebraic approach to the study of projective planes; in particular he constructed a simple explicit "base" of a free projective plane. This approach allowed the formulation of a series of problems and a new viewpoint on the known results and problems in the theory of projective planes. To these problems A.I. Shirshov devoted an extended plenary report at the 14th All-Union Algebra Conference in Novosibirsk in 1977.

A.I. Shirshov devoted much attention and care to the training of the next generation of young scientists; he considered this the duty of a scientist. The school of algebra created by him was an object of personal pride.

A.I. Shirshov died on the 28th of February 1981 after a prolonged serious illness. The profound ideas of his works remain alive.

A Word about the Teacher

Evgenii Kuzmin

Strict and attentive, but at the same time fatherly and warm – a glance above the glasses (in a simple thin frame). He walked through the rows of students looking into notebooks, checking how the problem written on the blackboard was being solved. September 1955: a seminar in higher algebra is in progress for the students of the 104th section of the first year in the Faculty of Mechanics and Mathematics [Mehmat] at MSU. The seminar is run by the Teacher, Anatoly Illarionovich Shirshov, a young assistant in the Department of Higher Algebra at MSU. The Department is headed by Alexander Gennadievich Kurosh, the author of the textbook "A Course in Higher Algebra" and the monograph "Group Theory". A.I. stops next to me, nods with satisfaction and calls me to the blackboard: "Kuzmin, come and tell us how to solve this problem". I go up and explain it. Stopping me before I finish, A.I. asks the audience: "Who knows how to complete the solution? Vinogradov, come to the blackboard."

To be called to the blackboard is an honour; it must be earned. We have some rather strong folks in our class, future doctors of science Sasha Vinogradov, Borya Vainberg, Dima Fuks, Galina Turina (a talented mathematician who, unfortunately, was killed in an untimely accident rafting on northern rivers), Valera Kudryavtsev, Galina Blohina, Vitya Ivnitsky and your humble servant Zhenya (Evgenii) Kuzmin. The studies at Mehmat came easily to me, and I especially enjoyed algebra, with its strict logic of calculations and somewhat dry beauty of algebraic structures and abstract theories. We could not imagine how different higher mathematics is from school mathematics! And it was rare luck to meet your life-long Teacher during the first few days of university studies. A.I. noticed me, started to give me separate, more difficult and interesting homework assignments, and once offered a completely unusual problem:

"There is a theorem of Shirokov which gives a positive answer to the conjecture of Kaplansky on the quasi-nilpotency of the commutator in an associative valuation ring under one extra condition of an algebraic nature. Shirokov proved his theorem using methods of functional analysis. But Kaplansky himself is an

algebraist, and his problem is also formulated algebraically. So I think that there must exist a purely algebraic proof of this theorem. Try to find such a proof!"

After some time I managed to do it! (Later in my diploma thesis I extended Shirokov's theorem to flexible valuation rings, which are a wide generalization of associative rings.) The reaction of Shirshov was unexpected. He brought me to his seminar, where the participants were students one or two years older than me, and said: "Look at this boy. He solved a problem of Kaplansky!" Of course, it was Shirokov who solved the problem of Kaplansky; I merely re-proved his theorem. A.I. simply wanted to praise me, and his words gave me wings. I began to attend his seminar and then his special course in ring theory, where he explained his ideas, amazing in their beauty and complexity, related to alternative, Jordan and Lie rings – the ideas that created a new direction in ring theory and were the basis of Shirshov's doctoral thesis.

The core of Shirshov's seminar consisted of five people: L. A. Bokut, G.V. Dorofeev, E.N. Kuzmin, V.N. Latyshev, and K.A. Zhevlakov, whom somebody called the "magnificent five". These five direct students of A.I. became the basis on which the school of Shirshov emerged; in the framework of this school the well-known doctors of science were formed: V.T. Filippov, A.Ya. Kanel-Belov, A.V. Iltyakov, A.R. Kemer, V.K. Kharchenko, P.S. Kolesnikov, G.P. Kukin, Yu.N. Malcev, Yu.A. Medvedev, A.A. Nikitin, S.V. Pchelintsev, V.V. Shchigolev, I.P. Shestakov, A.M. Slinko, S.R. Sverchkov, U.U. Umirbaev, E.I. Zelmanov, V.N. Zhelyabin – not to mention numerous candidates of science (like members of Shirshov's Ring Theory Department at Sobolev Institute A.Z. Ananin, V.N. Gerasimov, A.T. Kolotov, I.V. Lvov, A.N. Koryukin, V.A. Parfenov, A.P. Pojidaev, V.G. Skosyrskii, O.N. Smirnov, A.I. Valitskas, S.Yu. Vasilovskii).

A distinguishing trait of Shirshov's creative work was its exceptional individuality: he wrote all his main works by himself, without co-authors. This trait was largely inherited by his students. One day, after a regular session of the Academy of Sciences, he recounted that, during a break between meetings, he was approached by I.M. Gelfand, a well-known "co-authorizer", who said, holding Shirshov by a button of his jacket, that he had some ideas about Jordan algebras: "Would you like, Anatoly Illarionovich, to think about them?" A.I. refused; he did not want to join the numerous ranks of co-authors of Izrail Moiseevich.

Something similar also happened to me. After struggling with the problem of existence of an analytic Moufang loop with a given tangent Malcev algebra, I ventured to ask A.I. for help. The answer was like a cold shower: "If you don't want to work on this problem yourself, I will give it to somebody else". In a few years it dawned upon me how to make use of the Campbell-Hausdorff series, and the proof was found! How happy was A.I. for me! He used to say: "This is your second doctoral thesis".

Shirshov's treatment of his students was truly fatherly. He was happy for our successes as a father would be – and what were our successes compared to his truly outstanding achievements?! – and he looked after us even in everyday life. It was impossible not to feel a grateful love for this Man, our great Teacher.

A.I. Shirshov's Works on Alternative and Jordan Algebras

Ivan Shestakov and Efim Zelmanov

This survey is an extended version of Section 3 of the paper [3] by L.A. Bokut and the first author, which was based on the report delivered at the Second International Conference on Algebra in memory of A.I. Shirshov, held in Barnaul, Russia in August 1991.

We consider here the contribution of A.I. Shirshov to the theories of alternative and Jordan algebras. In the middle of the 1950s, when A.I. Shirshov began to investigate these algebras, there was no general structure theory. Only the structure theory of finite-dimensional algebras had been developed in the works of M. Zorn, A.A. Albert, N. Jacobson, R.D. Schafer, and others [9, 20]. As to the infinite-dimensional case, only some isolated results, such as the Bruck-Kleinfeld-Skornyakov theorem on alternative division rings [2, 27], had begun to appear. The results of A.I. Shirshov and, more importantly, the ideas and methods developed in his papers, provided a basis for the creation of structure theories for alternative and Jordan algebras in the general case.

Recall that at that time the structure theory of associative rings was already well-developed. One of its main achievements was I. Kaplansky's solution [11] of the A.G. Kurosh problem for algebraic PI-algebras. Although the Kurosh problem is easily reformulated for alternative or Jordan algebras, the proof of I. Kaplansky could not be translated to these classes of algebras since they lacked any structure theory. As has already been mentioned in other surveys in this volume, A.I. Shirshov looked at the Kurosh problem from the combinatorial point of view, and this approach permitted him not only to obtain more profound results in the associative case, but also to solve the problem for alternative and special Jordan algebras. Furthermore, these works were of fundamental significance for the entire development of the theory of alternative rings. They clearly demonstrated the intrinsic unity of the theories of Jordan and alternative algebras.

Recall that an algebra A is said to be *alternative* if, for all $a, b \in A$, the subalgebra generated by a, b is associative. An algebra J is said to be *Jordan* if it satisfies the identities $xy = yx$ and $(x^2y)x = x^2(yx)$.

The best-known example of an alternative algebra is the algebra of Cayley numbers. The typical example of a Jordan algebra is the algebra $A^{(+)} = \langle A, +, \circ \rangle$, where A is an associative algebra and $a \circ b = \frac{1}{2}(ab + ba)$. If a Jordan algebra J is embeddable into the algebra $A^{(+)}$ for a suitable associative algebra A, then J is called a *special* Jordan algebra; in this case we denote by $A(J) = \mathrm{alg}_A(J)$ the enveloping algebra of J.

A.I. Shirshov proved that if J is an algebraic special Jordan PI-algebra, then the algebra $A(J)$ is locally finite. In particular, the algebra J itself is locally finite in this case. The proof of this striking result should be considered together with the proof of the celebrated Height Theorem (see the other surveys in this volume). Both proofs are based on a Ramsey-type combinatorial statement which has implications far beyond algebra.

A word v is said to be *n-divisible* if it can be represented as $v = v_1 \dots v_n$ where $v > v_{\sigma(1)} \dots v_{\sigma(n)}$ lexicographically for an arbitrary nonidentical permutation σ.

The Shirshov $N(k,s,n)$-lemma. *For arbitrary integers $k, s, n \geq 1$ there exists an integer $N(k,s,n)$ such that an arbitrary word in $x_1, \dots x_k$ of length $N(k,s,n)$ contains a subword u^s or an n-divisible subword.*

The proof of this lemma involves induction on k. Let $k \geq 2$. Modulo the induction assumption it is sufficient to consider only words in the finite set

$$T = \{\, x_k^i x_{i_1} \dots x_{i_r} \mid 1 \leq i < s, 1 \leq i_1, \dots, i_r \leq k-1, r < N(k-1,s,n) \,\}.$$

An $(n-1)$-divisible word in T gives rise to an n-divisible word in the alphabet $x_1, \dots, x_k$. The key observation of Shirshov that allowed him to apply this combinatorics to special Jordan algebras is that an arbitrary T-word is a Jordan word; that is, a lexicographically greatest monomial in a homogeneous Jordan expression in $x_1, \dots, x_k$.

Shirshov's result works for alternative algebras as well. If B is an alternative algebra, then $B^{(+)}$ is a special Jordan algebra, and moreover, an enveloping algebra $A(B^{(+)})$ is isomorphic to the algebra of right multiplications,

$$R(B) = \mathrm{alg}\langle R_b \mid b \in B \rangle, \quad R_b \colon x \mapsto xb.$$

Thus, we have the transitions,

$$\begin{array}{l} B \text{ is an} \\ \text{algebraic} \\ \text{alternative} \\ \text{PI-algebra} \end{array} \Longrightarrow \begin{array}{l} B^{(+)} \text{ is an} \\ \text{algebraic} \\ \text{Jordan} \\ \text{PI-algebra} \end{array} \Longrightarrow \begin{array}{l} A(B^{(+)}) \\ \cong R(B) \text{ is} \\ \text{locally} \\ \text{finite} \end{array} \Longrightarrow \begin{array}{l} B \text{ is} \\ \text{locally} \\ \text{finite,} \end{array}$$

which give a solution to the Kurosh problem for alternative algebras. The idea of the transition from associative algebras to alternative algebras via Jordan algebras,

$$\text{Associative algebras} \overset{\text{Jordan algebras}}{\Longrightarrow} \text{Alternative algebras,}$$

plays a crucial role in many further investigations.

We remark that the reduction of the Restricted Burnside Problem [36, 37, 38] to Engel Lie algebras [35] was based on the Lie analogue of Shirshov's $N(k,s,n)$-lemma. A word in $x_1,\dots,x_k$ is said to be a *Lie word* if it is the lexicographically greatest word in a homogeneous linear combination of commutators in $x_1,\dots,x_k$.

Theorem. *For arbitrary integers $k,s,n\geq 1$, there exists an integer $L(k,s,n)$ such that an arbitrary word in $x_1,\dots,x_k$ of length $L(k,s,n)$ contains a subword u^s where u is a Lie word, or a subword $v_1u_1v_2u_2\dots u_{n-1}v_n$ where $v_1,\dots,v_n$ are Lie words, such that*

$$v_1u_1v_2\dots u_{n-1}v_n > v_{\sigma(1)}u_1v_{\sigma(2)}u_2\dots u_{n-1}v_{\sigma(n)},$$

lexicographically, for any nonidentical permutation σ.

In [34] the Kurosh problem for arbitrary (not necessarily special) Jordan PI-algebras was solved. It is a typical situation for Jordan algebras, when a theorem is first proved for special algebras and then extended to the class of all algebras. In this connection, it is very important to determine conditions sufficient for speciality of an algebra. In this direction, A.I. Shirshov proved the fundamental theorem that *the free Jordan algebra with two generators is special.* Combined with the earlier result by P. Cohn [4], the theorem implies that *every Jordan algebra with two generators is special.* A.I. Shirshov considered this theorem as one of his best results. The claim is quite simple whereas the proof is difficult and sophisticated. The theorem served as a source of diverse research in several directions. The first of them relates to the investigation of the structure of free Jordan algebras $J[x,y,z,\dots]$ with more than two generators.

We ought to say that A.I. Shirshov was always interested in studying problems related to the structure of free algebras. His first works are devoted to free Lie algebras. His last results are concerned with the structure of free projective planes. He also formulated a series of questions on the structure of free Jordan, alternative, Malcev, and other algebras [5].

The first result on the structure of the free Jordan algebra $J[X]$, $|X|\geq 3$, was obtained in 1959 by A.A. Albert and L.J. Paige [1]. They proved that this algebra is neither special nor even a homomorphic image of a special Jordan algebra. (Earlier P. Cohn in [4] showed that the class of special Jordan algebras is not closed under homomorphic images.) This implies that the algebra $J[x,y,z]$ contains nonzero elements vanishing in every special Jordan algebra (such elements are called *s-identities*). In 1966, C.M. Glennie [7] presented a concrete s-identity of degree 8. Until now, no essentially new s-identities have been found, and the question of their description is still open. Moreover, he proved that there are no s-identities of degree ≤ 7 and no homogeneous s-identities in three variables, which are linear in one of them. It is curious that these two facts provided all the identities that are needed for the structure theory [33].

In the case of special algebras, the role of a free algebra is played by the *free special Jordan algebra* $SJ[X]$, which is defined as the minimal subspace of the free associative algebra $\mathrm{Assoc}[X]$ that contains X and is closed with respect to

the Jordan product $a \circ b$. The elements of $SJ[X]$ are called *Jordan elements*. It is easy to see that $SJ[X] \subseteq H(\mathrm{Assoc}[X], *)$, where $H(\mathrm{Assoc}[X], *)$ is the subspace of symmetric elements of $\mathrm{Assoc}[X]$ with respect to the involution $*$ which is the identity on X: $(x_1 x_2 \cdots x_n)^* = x_n \cdots x_2 x_1$. The subspace $H(\mathrm{Assoc}[X], *)$ is closed with respect to the Jordan product and hence may be considered as a Jordan algebra. It is generated as an algebra by the set X and by all *tetrads* $\{x_i x_j x_k x_l\} = x_i x_j x_k x_l + x_l x_k x_j x_i$; when $|X| \leq 3$ then $H(\mathrm{Assoc}[X], *) = SJ[X]$, and when $|X| > 3$ then $H(\mathrm{Assoc}[X], *)$ strictly contains $SJ[X]$ (since tetrads in general are not Jordan elements).

An important tool to "diminish the gap" between $H(\mathrm{Assoc}[X], *)$ and $SJ[X]$ was invented by E. Zelmanov [33]. An element $n \in SJ[X]$ is called a *tetrad-eater* if the tetrad $\{nabc\}$ is a Jordan element for any $a, b, c \in SJ[X]$. E. Zelmanov constructed an ideal I in $SJ[X]$ which consists of tetrad-eaters; it satisfies the condition $I = H(A(I), *)$, that is, I coincides with the subspace of symmetric elements in its enveloping algebra. The tetrad-eater ideal I is essential to the classification of prime Jordan algebras [33]. Among various corollaries of the classification, it was proved that the algebra $J[X]$ is not prime for $|X| > 3$. The generators of I in [33] are of quite large degree. The following example, due to V. Skosyrsky [28], presents a tetrad-eater of minimal known degree:

$$\lambda(x, y, z, t, u) = [[[x, y]^2, x], [[[z, t]^2, z], u]].$$

One can easily check that this is a Jordan element; moreover, the ideal of $SJ[X]$ generated by all homogeneous elements of this type consists of tetrad-eaters.

As of now there are no known criteria to determine when an element of $\mathrm{Assoc}[X]$ is a Jordan element.

A series of interesting results on the structure of the free Jordan algebra $J[X]$ was obtained by Yu.A. Medvedev [16, 17]. He proved in particular that

(1) If $|X| \geq 3$, then the algebra $J[X]$ has nontrivial center and contains Albert subrings (central orders in 27-dimensional exceptional simple Jordan algebras).
(2) If $|X| \geq 32$, then $J[X]$ contains nonzero nilpotent elements and nontrivial nil ideals.

In the joint paper by Yu.A. Medvedev and E. Zelmanov [18], it was proved that

(3) If $|X|$ is infinite, then the nil radical of $J[X]$ is neither nilpotent nor solvable.

The first two results had their analogues in the theory of free alternative algebras [32]. The third is specific for Jordan algebras. As E.I. Zelmanov and I.P. Shestakov showed [39], the nil radical of a free alternative algebra over a field of characteristic zero is nilpotent. It is interesting that nilpotency of the radical in the alternative case as well as nonnilpotency of the radical in the Jordan case was proved by analyzing the structure of simple superalgebras and their identities.

Another direction stemming from the Shirshov theorem on two-generated Jordan algebras relates to investigating the problems of speciality, finding certain criteria of speciality, and studying the influence of identities of an algebra on its

speciality. Together with A.I. Shirshov, P. M. Cohn was a pioneer in this direction [4]. The direction was further developed in the works by A.M. Slin'ko [29] and S.R. Sverchkov [30, 31]. In the papers [14, 22, 19, 13, 8, 23, 24] this approach was extended to Jordan superalgebras and to other classes of algebras. We present one of the results of S.R. Sverchkov [30]: The class of special Jordan algebras regarded as a quasivariety cannot be determined by a set of quasi-identities (that is, expressions of the type "$f(x) = 0 \Rightarrow g(x) = 0$") in finitely many variables.

One of the important and difficult problems in the theory of nonassociative algebras is the construction of effective bases of free algebras. A.I. Shirshov constructed bases for free Lie algebras, and free commutative and anticommutative algebras, and formulated this problem for free alternative, free Jordan, free Malcev, and other free algebras [5, problem 1.160]. In the case of free Jordan algebras, no effective bases are known for $J[X]$, $|X| > 2$ and $SJ[X]$, $|X| > 3$. In the case of alternative algebras, a base for the free algebra $Alt[x, y, z]$ was constructed by A. Iltiakov [10] who also proved that this algebra has no nilpotent elements, contrary to $Alt[X]$ for $|X| > 3$. In [25, 26] bases of free Malcev and alternative superalgebras on one odd generator are constructed.

The structure of the free alternative algebras $Alt[X]$ for $|X| > 3$ was studied by I.P. Shestakov (see [32]). In particular, in [21] he solved the following problem of A.I. Shirshov [5, problem 1.159]: *Let Alt_n denote the variety generated by a free alternative algebra with n generators. Does the chain of varieties*

$$Alt_1 \subseteq Alt_2 \subseteq \cdots \subseteq Alt_n \subseteq Alt_{n+1} \subseteq \cdots ,$$

stabilize after a finite number of steps? The answer turned out to be negative. It was proved in [21] that $Alt_n \subset Alt_{2^n+1}$ strictly for any n. Later, V. T. Filippov [6] showed that if the base field has characteristic different from 2 and 3 then $Alt_n \subset Alt_{n+1}$ strictly for any n.

A.I. Shirshov posed the analogous problem for free Jordan, free Malcev, and other free algebras. A negative answer for the variety Mal of Malcev algebras was obtained in [21] by I.P. Shestakov; later V.T. Filippov refined this result in [6] by proving that $Mal_n \subset Mal_{n+1}$ strictly for any $n \neq 3$. For $n = 3$ the question is still open. The corresponding problem for the variety Jor of Jordan algebras remains open; it is known only that $Jor_1 \subset Jor_2 \subset Jor_3$ strictly. In the light of the above results, it seems very interesting to construct bases of the free Jordan and free Malcev algebras on three generators. In particular, are these algebras semiprime like $Alt[x, y, z]$?

It seems natural to reformulate the problem above on the chain of varieties in the framework of superalgebras. Recall that a variety of algebras $\mathcal{M}$ is said to have finite *basic rank* if it can be generated by a finitely generated algebra; the minimal number of generators in this case is called the basic rank of $\mathcal{M}$. For example, the varieties of all associative and all Lie algebras have basic rank 2, the varieties Alt and Mal, or the variety generated by a Grassmann algebra on an infinite number of generators, have infinite basic rank. Similarly, we will say that a variety $\mathcal{M}$ has a finite *basic superrank* if the corresponding variety of $\mathcal{M}$-superalgebras is

generated by a finitely generated superalgebra; a pair (m, n) of m even and n odd generators of such a superalgebra we call a basic superrank of $\mathcal{M}$ if it is minimal right lexicographically.

The notion of basic superrank is a more refined characteristic of a variety; this fact is evidenced by the following theorem by A.R. Kemer [12] which played a crucial role in his solution of the Specht problem: *Every variety of associative algebras over a field of characteristic 0 has a finite basic superrank*. The variety of alternative algebras which are solvable of index 2 provides a nonassociative example: it has infinite basic rank but its basic superrank is $(0, 1)$. In this connection, the following question arises: *What is the value of basic superrank for the variety Alt of alternative alebras? Is it finite?*

Finally, we want to mention one work by A.I. Shirshov which greatly influenced the development of the theory of nonassociative algebras. This is the survey *Some questions of the theory of rings that are nearly associative*. Many students of A.I. Shirshov, and the students of his students, began their acquaintance with ring theory while perusing this article. On the one hand, it is accessible for beginners, on the other hand, it contains a whole program of further study, and a series of attractive and still open problems.

In recent years, the theory of nonassociative algebras has gained wide recognition; its methods penetrate deeply into other domains of mathematics, not only into algebra but also into geometry, analysis, and theoretical physics. A great part of the merit for this belongs to A.I. Shirshov, who was a harbinger of the theory and whose marvelous theorems will adorn it forever.

References

[1] A.A. Albert and L.J. Paige, On a homomorphism property of certain Jordan algebras, Trans. Amer. Math. Soc. 92 (1959), 20–29.

[2] R.H. Bruck and E. Kleinfeld, The structure of alternative division rings, Proc. Amer. Math. Soc. 2, no. 6 (1951), 878–890.

[3] L.A. Bokut' and I.P. Shestakov, Some results by A.I. Shirshov and his school, Contemporary Mathematics, 184, 1995, 1–12.

[4] P. Cohn, On homomorphic images of special Jordan algebras, Canad. J. Math. 6 (1954), 253–264.

[5] Dnestrovskaya Tetrad', Open problems in the theory of rings and modules, Institute of Mathematics, Novosibirsk, 1993 (in Russian). English translation: Lect. Notes Pure Appl. Math., 246, Non-associative algebra and its applications, 461–516, Chapman & Hall / CRC, Boca Raton, FL, 2006.

[6] V.T. Filippov, On varieties of Malcev and alternative algebras generated by algebras of finite rank, Trudy Inst. Mat. SOAN SSSR, Novosibirsk, v. 4, 1984, 139–156.

[7] C.M. Glennie, Some identities valid in special Jordan algebras but not valid in all Jordan algebras, Pacific J. Math. 16, no. 1 (1966), 47–59.

[8] A.N. Grishkov, I.P. Shestakov, Speciality of Lie-Jordan Algebras, J. Algebra, 237 (2001), 621–636.

[9] N. Jacobson, Structure and Representations of Jordan Algebras, AMS colloquium Publ., vol. 39, Providence, R.I., 1968.

[10] A.V. Iltiakov, Free alternative algebras of rank 3. Algebra i Logika 23, No. 2 (1984), 136–158.

[11] I. Kaplansky, Topological representations of algebras. II, Trans. Amer. Math. Soc. 68, no. 1 (1950), 62–75.

[12] A.R. Kemer, Varieties and Z_2-graded algebras, Izv. Akad. Nauk SSSR, Ser. Mat. 48(1984), 1042–1059.

[13] M.C. López Díaz, I.P. Shestakov and S.R. Sverchkov, On speciality of Bernstein Jordan algebras, Communications in Algebra, 28 (2000), no. 9, 4375–4387.

[14] K. McCrimmon, Speciality and nonspeciality of two Jordan superalgebras, J. Algebra 149 (1992), no. 2, 326–351.

[15] K. McCrimmon, Taste of Jordan Algebras, Springer Berlin Heidelberg, 2004.

[16] Yu.A. Medvedev, Free Jordan algebras, Algebra i Logika, 27, no. 2 (1988), 172–200.

[17] Yu.A. Medvedev, On nilpotent elements of a free Jordan algebra, Sibirsk. Mat. Zh. 26, no.2 (1985), 1402–1408.

[18] Yu.A. Medvedev, E.I. Zelmanov, Some counterexamples in the theory of Jordan algebras. Nonassociative algebraic models (Zaragoza, 1989), 1–16, Nova Sci. Publ., Commack, NY, 1992.

[19] C. Martínez, I. Shestakov and E. Zelmanov, Jordan superalgebras defined by brackets, J. London Math. Soc. (2) 64 (2001), no. 2, 357–368.

[20] R.D. Schafer, An Introduction to Nonassociative Algebras, Acad. Press., New York, 1966.

[21] I.P. Shestakov, On a problem by Shirshov, Algebra i Logika 16, no. 2 (1977), 227–246.

[22] I.P. Shestakov, A quantization of Poisson superalgebras and a speciality of Jordan Poisson superalgebras, Algebra i Logika, 32, N 5 (1993), 572–585.

[23] I.P. Shestakov, The speciality problem for Malcev algebras and deformations of Malcev Poisson algebras, in "Non-Associative Algebra and Its Applications", Proceedings of the IV International Conference on Non-Associative Algebra and Its Applications, July 1998, São Paulo, 365–371, Marcel Dekker, NY; Series Name: Lecture Notes in Pure and Applied Mathematics, v. 211, 2000.

[24] I.P. Shestakov, Every Akivis algebra is linear, Geometriae dedicata, 77 (1999), no. 2, 215–223.

[25] I.P. Shestakov, Free Malcev superalgebra on one odd generator, Algebra and Applications, 2 (2003), no. 4, 451–461.

[26] I. Shestakov, N. Zhukavets, The free alternative superalgebra on one odd generator, International Journal of Algebra and Computation (IJAC) 17, no. 5/6 (2007), 1215–1247.

[27] L.A. Skornyakov, Alternative skew fields, Ukrain. Mat. Zh. 2, no. 1 (1950), 70–85.

[28] V.G. Skosyrsky, Strongly prime noncommutative Jordan algebras, Trudy Inst. Mat. SOAN SSSR, Novosibirsk, v. 16, 1989, 131–164.

[29] A.M. Slin'ko, On special varieties of Jordan algebras, Mat. Zametki 26, no. 3 (1979), 337–344.

[30] S.R. Sverchkov, On the quasivariety of special Jordan algebras, Algebra i Logika 24, no. 5 (1983), 563–573.

[31] S.R. Sverchkov, Varieties of special algebras, Comm. in Algebra 16, no. 9 (1988), 1877–1920.

[32] K.A. Zhevlakov, A.M. Slin'ko, I.P. Shestakov, A.I. Shirshov, Rings that are nearly associative, Nauka, Moscow, 1978.

[33] E.I. Zelmanov, On prime Jordan algebras. II, Sibirsk. Mat. Zh. 24 (1983), 83–104.

[34] E.I. Zelmanov, Absolute zero divisors and algebraic Jordan algebras, Sibirsk. Mat. Zh. 23, no. 6 (1982), 100–116.

[35] E.I. Zelmanov, Some problems in the theory of groups and Lie algebras, Math. Ussr-Sb. 66 (1990), no. 1, 159–168

[36] E.I. Zelmanov, Solution of the restricted Burnside problem for groups of odd exponent, Izv. Akad. Nauk SSSR, Ser. Mat. 54, no. 1 (1991), 41–60.

[37] E.I. Zelmanov, Solution of the restricted Burnside problem for 2-groups, Mat. Sb. 182, no. 4 (1991), 568–592.

[38] E.I. Zelmanov, On the restricted Burnside problem. Proceedings of the International Congress of Mathematicians, Vol. I, II (Kyoto, 1990), 395–402, Math. Soc. Japan, Tokyo, 1991.

[39] E.I. Zelmanov and I.P. Shestakov, Prime alternative superalgebras and nilpotency of the radical of a free alternative algebra, Izv. Akad. Nauk SSSR, Ser. Mat. 53, no. 1 (1990), 42–59.

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 $u = u_1u_2$ 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, $(ab)b$, $[(ab)b)b]$, ... 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:

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

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, $\ldots$, 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

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

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.

On the Representation of Lie Rings in Associative Rings

A.I. Shirshov

V.M. Kurochkin [1] has formulated the following theorem: *Every* Σ*-operator Lie ring* L *has a faithful representation in an associative* Σ*-operator ring* $\mathcal{A}$*, where* Σ *is an arbitrary domain of operators for the ring* L*.* In a subsequent note [2], V.M. Kurochkin pointed out the insufficient rigor of the proof he proposed for this theorem.

In the present paper, an example is constructed which demonstrates that, for the above formulation, the theorem is not valid.

Consider a linear space A with basis elements a_i $(i = 1, 2, \ldots, 13)$ over the field $GF(2)$. We make the space A into a ring by defining multiplication according to the following formulas:

$$a_1a_2 = a_2a_1 = a_{11}; \qquad a_1a_3 = a_3a_1 = a_{13}; \qquad a_2a_3 = a_3a_2 = a_{12};$$
$$a_1a_8 = a_8a_1 = a_2a_6 = a_6a_2 = a_3a_5 = a_5a_3 = a_{10};$$

and in all remaining cases $a_ia_j = 0$. Since the following equations hold identically as a consequence of the multiplication table,

$$x^2 = 0; \qquad (xy)z = 0;$$

the ring A is a Lie ring.

Now let Σ be the linear space over the same field with basis elements e_i $(i = 0, 1, 2, 3)$. Define a multiplication in Σ as follows:

$$e_ie_0 = e_0e_i = e_i,\ i = 0, 1, 2, 3; \qquad e_ie_j = 0,\ i, j \neq 0.$$

Define an action of the elements of Σ on the elements of A in the following way:

$e_0a_i = a_i$, $i = 1, 2, \ldots, 13$;

$e_1a_1 = a_4$; $e_1a_2 = a_5$; $e_1a_3 = a_6$; $e_1a_{12} = a_{10}$; $e_1a_k = 0$, $3 < k < 12$, $k = 13$;

$e_2a_1 = a_5$; $e_2a_2 = a_7$; $e_2a_3 = a_8$; $e_2a_{13} = a_{10}$; $e_2a_t = 0$, $3 < t < 13$;

Uspekhi Mat. Nauk N.S. 8, (1953), no. 5 (57), 173–175.

$$e_3a_1 = a_6;\ e_3a_2 = a_8;\ e_3a_3 = a_9;\ e_3a_{11} = a_{10};\ e_3a_\ell = 0,\ 3 < \ell < 11,\ \ell = 12, 13.$$

By distributivity we define the action of any element of Σ on any element of A.

In this way, the ring A becomes a Σ-operator Lie ring. Indeed, from the displayed table it follows that $(e_ie_j)a_k = e_i(e_ja_k)$ for $i \neq 0$, $j \neq 0$. Obviously, for $i = 0$ and $j = 0$ this equation also holds. Therefore, $(\sigma_1\sigma_2)b = \sigma_1(\sigma_2 b)$ where $\sigma_1, \sigma_2 \in \Sigma$ and $b \in A$. Further, if $a_ia_j = a_k$ then $k = 10, 11, 12, 13$. Suppose $k = 10$; then the equation $(e_ra_i)a_j = a_i(e_ra_j) = e_ra_{10}$ can be easily verified directly. For $k = 11$, it is sufficient to consider the equation $a_1a_2 = a_{11}$. In this case also, $(e_ra_1)a_2 = a_1(e_ra_2) = e_ra_{11}$, where a nonzero result is possible only for $r = 0$ and $r = 3$. The situation is similar for $k = 12$ and $k = 13$. Now, if $a_ia_j = 0$ then, for example, for $i = 1$ we will have $j = 1, 4, \ldots, 7, 9, 13$ and $(e_ra_1)a_j = a_1(e_ra_j) = 0$. Similarly for $i = 2$ and $i = 3$. From this it easily follows that $(\sigma b_1)b_2 = b_1(\sigma b_2) = \sigma(b_1b_2)$ where $\sigma \in \Sigma$, $b_1, b_2 \in A$, which completes the proof of the fact that A is a Σ-operator ring.

We now show that, in no matter which Σ-operator Lie ring $\mathcal{A}$ we embed the ring A, the element a_{10} will always be an absolute zero-divisor[1] of $\mathcal{A}$.

Indeed, let x be an arbitrary element of $\mathcal{A}$. Then,

$$\begin{aligned}
0 &= [x(e_1a_2 + a_5)]a_3 + (xa_1)(e_2a_3 + a_8) + [x(a_6 + e_1a_3)]a_2 \\
&= [x(e_1a_2)]a_3 + (xa_5)a_3 + (xa_1)(e_2a_3) + (xa_1)a_8 + (xa_6)a_2 + [x(e_1a_3)]a_2 \\
&= (xa_3)(e_1a_2) + x[(e_1a_2)a_3] + [x(e_2a_1)]a_3 + [x(e_2a_1)]a_3 + (xa_1)(e_3a_2) \\
&\quad + [x(e_3a_1)]a_2 + (xa_3)(e_1a_2) \\
&= x[(e_1a_2)a_3] \\
&= xa_{10},
\end{aligned}$$

where we have used the Jacobi identity, the fact that $\mathcal{A}$ is a Σ-operator ring, and the fact that all elements of the additive group of A have order 2.

Suppose there exists an associative Σ-operator ring $\mathcal{B}$ whose commutator Lie ring $\mathcal{B}^-$ contains A as a Σ-admissible subring. Then it is obvious that to the element a_{10} there corresponds some element of the center of $\mathcal{B}$, such that for any embedding of the ring $\mathcal{B}$ into any other associative Σ-operator ring $\overline{\mathcal{B}}$, this element is mapped to the center of $\overline{\mathcal{B}}$.

We now obtain a contradiction from the following result:

Lemma 1. *Any associative Σ-operator ring $\mathcal{B}$, such that $e_0\ell = \ell$ for any $\ell \in \mathcal{B}$, can be embedded into some associative Σ-operator ring $\overline{\mathcal{B}}$ such that the intersection of the center Z of $\overline{\mathcal{B}}$ with $\mathcal{B}$ equals zero*[2].

For the proof it suffices to consider the case in which Σ is a commutative associative ring with identity element e_0 acting on $\mathcal{B}$ as the identity automorphism.

[1] That is, a central element. [Translators]

[2] To make the condition of the lemma hold in our case, it suffices to consider, instead of the ring $\mathcal{B}$, the Σ-admissible subring generated by all elements of A.

Consider the collection $\overline{\mathcal{B}}$ of symbols of the form $(\sigma_i, b_{i1}, b_{i2}, b_{i3})$ where $\sigma_i \in \Sigma$, and $b_{ik} \in \mathcal{B}$, $k = 1, 2, 3$. We will regard two symbols $(\sigma_i, b_{i1}, b_{i2}, b_{i3})$ and $(\sigma_j, b_{j1}, b_{j2}, b_{j3})$ as equal if and only if $\sigma_i = \sigma_j$, $b_{ik} = b_{jk}$, $k = 1, 2, 3$.

We make the collection $\overline{\mathcal{B}}$ into a Σ-operator ring by defining addition, multiplication, and the action of $\sigma \in \Sigma$ on an element $\overline{b} \in \overline{\mathcal{B}}$ by the following formulas:

$$(\sigma_i, b_{i1}, b_{i2}, b_{i3}) + (\sigma_j, b_{j1}, b_{j2}, b_{j3}) = (\sigma_i + \sigma_j, b_{i1} + b_{j1}, b_{i2} + b_{j2}, b_{i3} + b_{j3});$$

$$(\sigma_i, b_{i1}, b_{i2}, b_{i3}) \cdot (\sigma_j, b_{j1}, b_{j2}, b_{j3}) = (0, \sigma_j b_{i3} + b_{i3} b_{j1}, \sigma_i b_{j3} + b_{i2} b_{j3}, b_{i3} b_{j3});$$

$$\sigma(\sigma_i, b_{i1}, b_{i2}, b_{i3}) = (\sigma\sigma_i, \sigma b_{i1}, \sigma b_{i2}, \sigma b_{i3}).$$

It is easy to verify that all the axioms of a Σ-operator ring are satisfied.

The ring $\overline{\mathcal{B}}$ is an associative ring, since

$$\begin{aligned}
&[(\sigma_i, b_{i1}, b_{i2}, b_{i3}) \cdot (\sigma_j, b_{j1}, b_{j2}, b_{j3})] \cdot (\sigma_k, b_{k1}, b_{k2}, b_{k3}) \\
&= (\sigma_i, b_{i1}, b_{i2}, b_{i3}) \cdot [(\sigma_j, b_{j1}, b_{j2}, b_{j3}) \cdot (\sigma_k, b_{k1}, b_{k2}, b_{k3})] \\
&= (0, \sigma_k b_{i3} b_{j3} + b_{i3} b_{j3} b_{k1}, \sigma_i b_{j3} b_{k3} + b_{i2} b_{j3} b_{k3}, b_{i3} b_{j3} b_{k3}),
\end{aligned}$$

and it contains a subring of symbols $(0, 0, 0, b_{i3})$ that is isomorphic to the ring $\mathcal{B}$.

On the other hand, for $b_{i3} \neq 0$, from the equations

$$(e_0, 0, 0, 0) \cdot (0, 0, 0, b_{i3}) = (0, 0, b_{i3}, 0), \text{ and}$$

$$(0, 0, 0, b_{i3}) \cdot (e_0, 0, 0, 0) = (0, b_{i3}, 0, 0),$$

it follows that

$$(e_0, 0, 0, 0) \cdot (0, 0, 0, b_{i3}) \neq (0, 0, 0, b_{i3}) \cdot (e_0, 0, 0, 0),$$

which completes the proof of the lemma.

From the contradiction just obtained, it follows that the Σ-operator ring A cannot be faithfully represented in any associative Σ-operator ring. This example also shows that Ado's theorem cannot be generalized to rings over an arbitrary ring of operators.

It would be interesting to find necessary and sufficient conditions for the existence of a faithful representation of a given Σ-operator Lie ring R. Lazard [3] proved that if Σ is a principal ideal ring, then such a representation exists for any R. One can also prove the following theorem: *If no element $\sigma \in \Sigma$, $\sigma \neq 0$, annihilates an absolute zero-divisor of R, then a faithful representation always exists.*

References

[1] V.M. Kurochkin, *The representation of Lie rings by associative rings*, Mat. Sbornik N.S. 28 (1951) 467–472.

[2] V.M. Kurochkin, *Correction to the paper "The representation of Lie rings by associative rings"*, Mat. Sbornik N.S. 30 (1952) 463.

[3] M. Lazard, *Sur les algèbres enveloppantes universelles de certaines algèbres de Lie*, C. R. Acad. Sci. Paris 234 (1952) 788–791.

Subalgebras of Free Commutative and Free Anticommutative Algebras

A.I. Shirshov

1. It is known (see A.G. Kurosh [2]) that any subalgebra of the free nonassociative algebra is free. It is natural to ask the corresponding question for relatively free algebras (see A.I. Malcev [3]), of course restricting oneself to the most important classes of algebras.

In the work of the present author [4], it is proved that every subalgebra of a free Lie algebra is also free. In the same paper it is pointed out that the analogous theorem is not valid for free associative, alternative, right- or left-alternative, or Jordan algebras, and also for flexible algebras, and power-associative or power-commutative algebras. It is easy to see that this theorem is valid for free nilpotent algebras of class 1, and not valid for free nilpotent algebras of class k, $k > 1$.

Among the most important classes of algebras, there remain only the commutative and anticommutative algebras. In the present paper, it is proved that for the free algebras of these two classes, the corresponding problem has a positive solution. For brevity and convenience of exposition, we will call commutative algebras C-algebras and anticommutative algebras AC-algebras.

Analogously to the definitions of A.I. Malcev [3] we call an algebra $\mathcal{A}$ over a field P a *free ε-algebra* where $\varepsilon = C$ or $\varepsilon = AC$ if it is defined by some set R of generators and by the identical relation

$$xy + \delta yx = 0, \tag{1}$$

where $\delta = -1$ for $\varepsilon = C$ and $\delta = +1$ for $\varepsilon = AC$, and also for $\varepsilon = AC$ we will assume[1] that the characteristic of P is not 2 since this case will be included in the case $\varepsilon = C$.

In the proof of Theorem 1 below, we use a method that is similar to Hall's method in [1], and in the proof of Theorem 2 below, we partially use the methods

Mat. Sbornik N.S. 34 (76), (1954), no. 1, 81–88.

[1]According to current terminology, an anticommutative algebra in characteristic 2 should also satisfy $x^2 = 0$ for all x, and this case is not included in the author's considerations. [Translators]

of A.G. Kurosh [2] and of the present author [4]. The present work can be studied independently of the above-mentioned papers, although it can be regarded as a sequel to the present author's work [4].

The present work was carried out under the supervision of A.G. Kurosh, to whom the author expresses his deep gratitude.

2. Let $R = \{a_\alpha\}$ be some set of symbols where α takes values in some non-empty set of indices.

Consider nonassociative words of various lengths formed from these symbols, in the sense of the definitions given in the work of A.G. Kurosh [2]; we will call them *R-words* or simply *words*.

Definition. Words of length 1 will be called *ε-regular* and ordered arbitrarily. Assuming that ε-regular words of length less than n, $n > 1$, have been already defined and ordered in such a way that words of smaller length precede words of greater length, a word w of length n will be called *ε-regular* if

1) $w = uv$ where u and v are ε-regular words;
2) $u \geq v$ for $\varepsilon = C$ and $u > v$ for $\varepsilon = AC$.

We order arbitrarily the ε-regular words of length n defined in this way, and declare them to be greater than regular words of smaller length.

The symbols $<, >, \leq, \geq$ as applied to ε-regular words in the above definition, as well as in the remainder of this paper, will be understood in the sense of the ordering of these words.

Theorem 1. *The collection of all ε-regular words for $\varepsilon = C, AC$ forms a basis of the free ε-algebra $\mathcal{A}$ with the system of free generators R.*

We demonstrate a method that allows us to assign uniquely, to each word w of the free ε-algebra $\mathcal{A}$, some element w^* of the same algebra such that

$$w^* = w \text{ in the algebra } \mathcal{A}, \tag{2}$$

where w^* is either an ε-regular word with coefficient $+1$ or -1, or 0. For words of length 1, we set $w^* = w$.

Suppose such a method is already defined for words of length less than n, and let w be a word of length n, $n > 1$. Then $w = uv$. We set

$$w^* = u^*v^*, \text{ if } u^* \geq v^* \text{ in case } \varepsilon = C, \text{ or } u^* > v^* \text{ in case } \varepsilon = AC;$$
$$w^* = 0 \text{ if } u^* = v^* \text{ in case } \varepsilon = AC;$$
$$w^* = -\delta v^*u^* \text{ if } u^* < v^*.$$

Obviously, all the conditions imposed on w^* are satisfied.

Each element $a \in \mathcal{A}$ has the form

$$a = \sum_{i=1}^{k} \alpha_i w_i, \tag{3}$$

where α_i are elements of the base field, and w_i are some words, not necessarily distinct. Clearly, the element a can be written in the form

$$a = \sum_{i=1}^{k} \alpha_i w_i^*, \tag{4}$$

from which it follows that every element of the free ε-algebra can be represented as a linear combination of ε-regular words.

The zero element of the algebra $\mathcal{A}$ only admits a representation of the form

$$0 = \sum_i \alpha_i a_{i1} a_{i2} \cdots a_{in_i} [c_i d_i + \delta d_i c_i] b_{i1} b_{i2} \cdots b_{im_i},$$

where $\alpha \in P$, and a, b, c, d are some words, and an appropriate arrangement of parentheses is assumed. One immediately sees that the ε-regular expression of the right-hand side obtained after applying distributivity and replacing each of the resulting words by the corresponding starred word, gives zero. Since for an ε-regular word w we have $w^* = w$, it follows that there do not exist two distinct ε-regular expressions for the same element, which is equivalent to the linear independence of ε-regular words. The theorem is proved.

The unique expression of an element a as a linear combination of ε-regular words will be denoted by a^*.

In the free ε-algebra $\mathcal{A}$, to each element a there corresponds a natural number $n(a)$, the *degree* of a, defined as the greatest length of the ε-regular words occurring in a^*.

The sum of the terms of the element a^*, i.e., ε-regular words with coefficients in P, whose degree is equal to $n(a)$, will be called the *highest part* of the element a.

3. The purpose of the present work is the proof of the following theorem.

Theorem 2. *Every subalgebra $\mathcal{B}$ of a free ε-algebra $\mathcal{A}$ (where $\varepsilon = C$ or $\varepsilon = AC$) is also free.*

Thanks to the existence of the concept of degree, we can use the method of A.G. Kurosh [2] to construct, for each subalgebra $\mathcal{B}$ of the free ε-algebra $\mathcal{A}$, a finite or countably infinite sequence of integers k_n and subalgebras $\mathcal{B}_n$ $(n = 1, 2, \ldots)$, where $k_0 = 0$, $\mathcal{B}_0 = 0$, k_n is the smallest degree of elements of the subalgebra $\mathcal{B}$ which have not been included in $\mathcal{B}_{n-1}$, and $\mathcal{B}_n$ is the subalgebra generated in $\mathcal{B}$ by the elements whose degree does not exceed k_n.

The set $\mathcal{K}_n$ of elements of $\mathcal{B}_n$ whose degree does not exceed k_n is a linear subspace, and the set $\mathcal{K}'_n$ of elements of $\mathcal{B}_{n-1}$ whose degree does not exceed k_n is a subspace of $\mathcal{K}_n$. We arbitrarily choose one representative from each coset in a basis of the linear space $\mathcal{K}_n/\mathcal{K}'_n$ and denote the resulting set by $\mathcal{M}_n$. Now let $\mathcal{M} = \bigcup_{n\geq 1} \mathcal{M}_n$. We prove that the set $\mathcal{M}$ has the following properties:

A. *The highest part of each element a, $a \in \mathcal{M}$, does not belong to the subalgebra generated by the highest parts of the elements of the set $\mathcal{M} \setminus \{a\}$;*

B. *The subalgebra $\mathcal{B}$ is generated by the set $\mathcal{M}$.*

Suppose, contrary to property A, that the highest part $\overline{a}$ of some element $a \in \mathcal{M}$ belongs to the subalgebra generated by the highest parts of the elements of the set $\mathcal{M} \setminus \{a\}$, i.e.,

$$\overline{a} = \sum_i \alpha_i \overline{a_i} + \sum_{i,j} \alpha_{ij} \overline{b_i}\,\overline{b_j} + \cdots + \sum_{i,j,\ldots,k} \alpha_{ij\ldots k} \overline{c_i}\,\overline{c_j} \cdots \overline{c_k},$$

where $\alpha \in P$, and parentheses are placed appropriately. Then all $\overline{b}, \ldots, \overline{c}$ that occur in the second and following summations can obviously be assumed to have degree less than the degree of $\overline{a}$, and all $\overline{a_i}$ that occur in the first summation can be assumed to be distinct from $\overline{a}$ and to have degree equal to the degree of $\overline{a}$, i.e., all corresponding elements a, a_i must belong to the same set $\mathcal{M}_n$. It follows that for the cosets A, A_i represented by the elements a, a_i there exists a linear dependence relation $A - \sum_i \alpha_i A_i = 0$, which contradicts the choice of these cosets. Thus, property A has been proved.

To prove property B, it suffices to observe that the subalgebra $\mathcal{B}_n$ is generated by the set $\bigcup_{k=1}^{n} \mathcal{M}_k$.

4. We will call any element of the free nonassociative algebra S, with the set $X = \{x_1, x_2, \ldots\}$ of free generators, a *nonassociative polynomial*. Let $\mathcal{S}$ be the free ε-algebra with generators $a_1, a_2, \ldots$ over the same field P. 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 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 is nonzero. If in $\mathcal{S}$, regular words are defined and $\varphi(a_{i_1}, a_{i_2}, \ldots)$ is the ε-regular form of the element $f(a_{i_1}, a_{i_2}, \ldots)$, then the polynomials $f(x_{i_1}, x_{i_2}, \ldots)$ and $\varphi(x_{i_1}, x_{i_2}, \ldots)$ are equivalent. In this case, we will call the polynomial $\varphi(x_{i_1}, x_{i_2}, \ldots)$ *ε-regular*, and then obviously any part of φ will also be ε-regular.

We now assume that there exists some non-trivial relation $f(b_1, b_2, \ldots, b_q) = 0$ for the elements of $\mathcal{M}$, i.e., $f(x_1, x_2, \ldots, x_q)$ is a non-trivial polynomial which can in fact be taken to be regular, and we derive a contradiction from this assumption.

Lemma. *If, in the free ε-algebra $\mathcal{A}$ there exists a finite set of elements b_i (where $i = 1, 2, \ldots, q$, and $n(b_i) \geq n(b_j)$ for $i > j$) which satisfy property A and some non-trivial relation $f(b_1, b_2, \ldots, b_q) = 0$, then the elements of the finite set $\mathcal{M} = \{c_i\}$ $(i = 1, 2, \ldots, q)$ that have the form $c_i = b_i + w_i$, where w_i is an element of the subalgebra generated by the elements b_k $(k < i)$ and either $w_i = 0$ or $n(w_i) = n(b_i)$, also satisfy property A and some non-trivial relation $f'(c_1, c_2, \ldots, c_q) = 0$.*

We will first prove that there exist expressions

$$b_i = c_i + w_i' \ (i = 1, 2, \ldots, q)$$

where w_i' is an element (possibly zero) of the subalgebra generated by the elements c_k $(k < i)$. Indeed, $b_1 = c_1$. Assuming that for all $i < k$ the desired expression has been found, we can replace, in the equation

$$b_k = c_k - w_k,$$

all b_j $(j < k)$ that occur in w_k by the already found expressions in terms of c_i, after which we obtain the desired expression for b_k.

We will prove that property A holds for the elements of the set $\overline{\mathcal{M}}$. If the highest part $\overline{c_j}$ of some element $c_j \in \mathcal{M}$ belongs to the subalgebra generated by the highest parts of the elements of $\mathcal{M} \setminus \{c_j\}$, then analogously to what was done in the proof of property A for the set $\mathcal{M}$, we may assume that $\overline{c_j}$ belongs to the subalgebra generated by $\overline{c_k}$, $k < j$. But then, using the obvious equations

$$\overline{c_i} = \overline{b_i} + \overline{w_i}\ (i = 1, 2, \ldots, q),$$

where $\overline{w_i}$ is the highest part of w_i, to replace all $\overline{c_i}$ by their expressions in terms of $\overline{b_i}$ $(i = 1, 2, \ldots, q)$, we obtain an expression of the element $\overline{b_j}$ in terms of $\overline{b_\ell}$, $\ell < j$, which contradicts the assumption.

Now we prove that the elements of the set $\overline{\mathcal{M}}$ satisfy some non-trivial relation. Separate, in the polynomial $f(x_1, x_2, \ldots, x_q)$, the highest part relative to x_q, i.e., the collection of the terms that contain the factor x_q the maximal number of times. Denote this part by f_q. Now separate in f_q the highest part f_{q-1} relative to x_{q-1}, and so on, and finally separate in f_2 the highest part f_1 relative to x_1. After this we have:

$$\begin{aligned} f(b_1, b_2, \ldots, b_q) &= f_1(b_1, b_2, \ldots, b_q) + f_1'(b_1, b_2, \ldots, b_q) \\ &= f_1(c_1 + w_1', \ldots, c_q + w_q') + f_1'(c_1 + w_1', \ldots, c_q + w_q') \\ &= f_1(c_1, \ldots, c_q) + \varphi(c_1, \ldots, c_q) \\ &= f'(c_1, \ldots, c_q) \\ &= 0. \end{aligned}$$

The polynomial $f'(c_1, \ldots, c_q)$ cannot be trivial because the polynomials f_1 and φ do not have terms of the same content and f_1 is a non-trivial polynomial. This completes the proof of the lemma.

Based on the lemma, one can easily prove that the assumption of the existence of a non-trivial relation among the elements of $\mathcal{M}$ implies the existence of a finite set $\mathcal{N}$ of elements, that satisfy property A and some non-trivial relation, such that in each of them any term included in the highest part is not the product of *leading terms* (relative to the fixed ordering of ε-regular words) of the other elements of the set.

To prove this statement, we enumerate the finite subset of elements of $\mathcal{M}$ that occur in the non-trivial relation $f = 0$ and denote the resulting finite set by $\mathcal{M}_1$ where $\mathcal{M}_1 = \{b_i\}$ $(i = 1, 2, \ldots, q)$. Without loss of generality we assume that for $i > j$ either $n(b_i) > n(b_j)$ or $\overline{b_i} \geq \overline{b_j}$ where $\overline{b_i}$, $\overline{b_j}$ are the ε-regular words of the leading terms of the elements b_i, b_j. We will show that using the lemma we can obtain $\overline{b_i} > \overline{b_j}$ for $i > j$. Separate in $\mathcal{M}_1$ the subset $\mathcal{M}_{1k}$ of elements of degree k. Consider in $\mathcal{M}_{1k}$ the subset $\overline{\mathcal{M}_{1k}}$ of elements with the greatest leading terms (up to a coefficient from the field P). Let

$$\overline{\mathcal{M}_{1k}} = \{b_i\}\ (i = i_k, i_k + 1, \ldots, i_k + q_k).$$

Replacing in $\mathcal{M}_{1k}$ the subset $\overline{\mathcal{M}_{1k}}$ by the set of elements

$$b_{i_k},\ b_{i_k+1}-\alpha_1 b_{i_k},\ b_{i_k+2}-\alpha_2 b_{i_k},\ \ldots,\ b_{i_k+q_k}-\alpha_{q_k} b_{i_k},$$

where α_s $(s=1,2,\ldots,q_k)$ are the elements of the field P chosen such that in the differences above the leading terms cancel, we obtain that in the set $\mathcal{M}_{1k}$ there will be only one element with leading term $\overline{b_{i_k}}$ and the leading terms of all other elements will be less than $\overline{b_{i_k}}$. Doing the same with the set $\{b_{i_1+s}-\alpha_s b_{i_k}\}$ $(s=1,2,\ldots,q_k)$ and so on, we transform the set $\mathcal{M}_{1k}$ into a set in which all leading terms are distinct. We perform the same transformations for all possible k. Obviously, these transformations conform to the requirements of the lemma.

If it now turns out that some term $\overline{\overline{w}}$ of the highest part of some element w of the resulting set can be represented as a product of leading terms of other elements of the set, then obviously the latter terms will not have greater degree. Therefore we can eliminate the term $\overline{\overline{w}}$ in w by subtracting from w the product of the corresponding elements with the appropriate arrangement of parentheses. We assume by induction that the elements of the set under consideration that precede the element w are such that the terms of their highest parts can no longer be represented as products of leading terms of other elements. It is clear that, even if after performing the subtraction we obtain new terms that can be represented as products of leading terms of other elements, then the number of such factors in such terms is strictly less than the corresponding number for the term $\overline{\overline{w}}$. The proof can now be completed by a straightforward induction.

Let us now prove that the properties satisfied by the set $\mathcal{N}$ are contradictory. Indeed, let $\overline{f}=0$ be a non-trivial relation satisfied by the elements of the set $\mathcal{N}$, and let

$$e=\alpha b_{i_1} b_{i_2}\cdots b_{i_s},\ \alpha\in P,\ b_{i_k}\in\mathcal{N}\ (k=1,2,\ldots,s),$$

where parentheses are arranged in a certain way, be one of the terms of the regular polynomial $\overline{f}$; this term is chosen from among the terms for which the number $n=\sum_{k=1}^{s} n(b_{i_k})$ is maximal, in such a way that the number s is maximal. We show that, when the word

$$\overline{e}=\overline{b_{i_1}}\,\overline{b_{i_2}}\cdots\overline{b_{i_s}},$$

where $\overline{b_{i_k}}$ is the leading term of the element b_{i_k} and parentheses are arranged in the same way as before, is rewritten in ε-regular form $\overline{e}^*$, there will be no such term among the other ε-regular words obtained by representing the left-hand side of the non-trivial relation $\overline{f}=0$ as a linear combination of ε-regular R-words. Indeed, such a word could only appear after rewriting some product of terms of highest parts of elements of $\mathcal{N}$ in ε-regular form. Assume that there is a term,

$$\overline{\overline{m}}=\beta\overline{\overline{b_{j_1}}}\,\overline{\overline{b_{j_2}}}\cdots\overline{\overline{b_{j_r}}},$$

where $\overline{\overline{b_{j_k}}}$ is some term in the highest part of the element b_{j_k}, such that $\overline{\overline{m}}^*$ and $\overline{e}^*$ are similar terms. Then, since all $\overline{\overline{b_{j_k}}}$ and $\overline{b_{i_k}}$ are assumed to be ε-regular, from the process of constructing w^* from w it follows that $\overline{\overline{m}}^*$ can be represented as a product of the same words $\overline{\overline{b_{j_1}}},\ \ldots,\ \overline{\overline{b_{j_r}}}$ with possibly a different order and a

different arrangement of parentheses. The same applies to the term $\overline{e}^*$. If some term $\overline{\overline{b_{j_k}}}$ is not in fact the leading term of the element b_{j_k}, then it cannot be represented as a product of leading terms of the elements of $\mathcal{N}$ (we recall that analogous statements are made up to a factor from the field P); therefore, from the similarity of $\overline{e}^*$ and $\overline{\overline{m}}^*$, it follows that b_{j_k} taken in a product with other terms $\overline{b_{j_t}}$ must give the leading term $\overline{b_{i_g}}$; but from here it follows that $r > s$ which is impossible. Therefore, all $\overline{\overline{b_{j_k}}}$ are in fact the leading terms of the corresponding elements. On the other hand, from the equation

$$(\alpha\overline{e} - \overline{\overline{m}})^* = 0,\ \alpha \in P,$$

it follows that

$$(\alpha_1 e - m)^* = 0,\ \alpha_1 \in P,$$

where $m = \beta b_{j_1} b_{j_2} \cdots b_{j_r}$ is the term of the polynomial $\overline{f}$ from which the term $\overline{\overline{m}}$ could be obtained. Therefore, since the polynomial $\overline{f}$ is ε-regular, e and m are similar terms, which is a contradiction. This completes the proof of Theorem 2.

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.

[4] A.I. Shirshov, *Subalgebras of free Lie algebras*, Mat. Sbornik N.S. 33 (1953) 441–45.

On Special J-rings

A.I. Shirshov

1. Introduction

A commutative ring such that for every pair of elements a and b the following equation holds,

$$J_0\{a,b\} \equiv (a^2b)a - a^2(ba) = 0, \tag{1}$$

is called a *Jordan ring*[1]. In the first four sections of this paper, we will consider Jordan algebras[2] over an arbitrary ring of coefficients Σ, assuming only that Σ is a unital ring and that for each element a in the Jordan algebra there exists a unique element b such that $2b = a$. Clearly, in this case the equation $2a = 0$ implies $a = 0$. In such Jordan algebras, i.e., Jordan algebras without elements of order 2 in the additive group, the following equations hold:

$$J_1\{x,y,z,t\} \equiv$$
$$[(yz)x]t + [(ty)x]z + [(zt)x]y - (yz)(xt) - (ty)(xz) - (zt)(xy) = 0, \tag{2}$$
$$J_2\{x,y,z,t\} \equiv$$
$$[(yz)x]t + [(ty)x]z + [(zt)x]y - [(xz)y]t - [(tx)y]z - [(zt)y]x = 0. \tag{3}$$

The validity of equation (2) follows from the relation

$$J_0\{y+z+t,x\} - J_0\{-y+z+t,x\} - J_0\{y-z+t,x\} - J_0\{y+z-t,x\}$$
$$= 8J_1\{x,y,z,t\},$$

which can be verified by direct computation, and then equation (3) follows from (2) using the relation

$$J_2\{x,y,z,t\} = J_1\{x,y,z,t\} - J_1\{y,x,z,t\}.$$

Mat. Sbornik N.S. 38 (80), (1956), no. 2, 149–166.

[1]Literally, "J-ring". We adopt the modern terminology, "Jordan ring". [Translators]
[2]Literally, "Jordan rings with an arbitrary ring Σ of operators". [Translators]

Jordan algebras also satisfy the relation

$$(ba^s)a^t = (ba^t)a^s, \tag{4}$$

which generalizes equation (1). Indeed, suppose that relation (4) holds for exponents s_1 and t_1 such that $s_1 + t_1 < s + t$. Then, from the equation

$$J_1\{a^{s+t-3}, a, a, ba\} - aJ_1\{a^{s+t-3}, a, a, b\} = a^{s+t-1}(ba) - (ba^{s+t-1})a = 0,$$

which is implied by the inductive hypothesis, the validity of equation (4) follows in the case when one of s or t equals 1. For $s = t$ there is nothing to prove. If $1 < s < t$, then from the equation

$$\begin{aligned} &J_1\{b, a, a^{s-1}, a^t\} \\ &= [(ba^s)a^t - (ba^t)a^s] + [(ba^{t+1})a^{s-1} - (ba^{s-1})a^{t+1}] + [(ba^{s+t-1})a - (ba)a^{s+t-1}] \\ &= 0 \end{aligned}$$

it easily follows that the proof can be completed by induction on $\min(s, t)$. From equation (4) it is easy to obtain associativity for the powers of one element.

It is known that if $\mathcal{A}$ is an associative algebra over Σ which admits unique division by 2, then introducing in $\mathcal{A}$ the new multiplication

$$a \cdot b = \frac{1}{2}(ab + ba),$$

we obtain a Jordan algebra $\mathcal{A}^{(+)}$ with the same additive group and new multiplication. A Jordan algebra I over Σ is called *special* if there exists an associative algebra $\mathcal{A}$ over Σ such that the Jordan algebra $\mathcal{A}^{(+)}$ contains a subalgebra isomorphic to I. Even in the case of algebras over a field, it is known [1] that not every Jordan algebra is special.

In the case of algebras over a field, Cohn [2] proved that a homomorphic image of a special Jordan algebra is not necessarily special. It follows that the class of special Jordan algebras cannot be defined by identical relations. In the present paper, it is proved that a Jordan algebra over Σ that has a finite or countably infinite set of generators is special if and only if it can be embedded into a Jordan algebra over Σ with two generators.

In the last section of this paper, we remove the requirement that for every element a there exists an element b such that $2b = a$. This condition will be replaced by the weaker condition that there are no elements of order 2 in the additive group. It is clear that in this case we will be forced to consider the operation $a \circ b = ab + ba$.

2. An embedding theorem

Consider the free associative algebra A over Σ (see the definition in [3]) with two generators a and b. We will assume that the ring Σ admits unique division by 2. Let A' be the subalgebra of A generated by the elements of the set $T = \{bab, ba^2b, \ldots, ba^nb, \ldots\}$.

Lemma 1. *The subalgebra A' is a free associative algebra over Σ with the set T of free generators.*

Proof. We introduce the notation: $ba^nb = c_n$. Let $f(x_1, x_2, \ldots, x_k)$ be an associative polynomial with coefficients in Σ (with all similar terms combined) such that $f(c_1, c_2, \ldots, c_k) = 0$. Clearly,

$$x_{i_1}^{n_1} x_{i_2}^{n_2} \cdots x_{i_s}^{n_s} \neq x_{j_1}^{m_1} x_{j_2}^{m_2} \cdots x_{j_t}^{m_t} \quad \text{implies} \quad c_{i_1}^{n_1} c_{i_2}^{n_2} \cdots c_{i_s}^{n_s} \neq c_{j_1}^{m_1} c_{j_2}^{m_2} \cdots c_{j_t}^{m_t}.$$

Hence it follows that $f \equiv 0$, and this proves the lemma. □

Let N' be an ideal of the algebra A' over Σ. Then N' generates in A some ideal N.

Lemma 2. *For any ideal N' of the algebra A', the following equality holds: $N \cap A' = N'$.*

Proof. Obviously, $N \cap A' \supseteq N'$. Let n be an element of the ideal N; then $n = \sum_i c_i n_i' d_i$ where $n_i' \in N'$ and c_i, d_i are monomials of A. Let $n \in A'$. This means that all terms that occur in the expression of n such that c_i or d_i does not belong to A' must cancel each other. This implies that $n \in N'$, and this proves the lemma. □

Theorem 1. *Every special Jordan algebra I over Σ that has a finite or countably infinite number of generators can be embedded into a special Jordan algebra over Σ with two generators.*

Proof. Obviously, the associative algebra B over Σ in which the algebra I can be represented can be assumed to have a finite or countably infinite number of generators. It is also clear that the algebra B is isomorphic to a quotient algebra $\overline{A'}$ of the algebra A' by some ideal N'. From Lemma 2 it follows that the quotient algebra $\overline{A}$, of the algebra A with respect to the corresponding ideal N, contains a subalgebra isomorphic to $\overline{A'}$, and therefore also isomorphic to B. Since $ba^kb = 2b \cdot (b \cdot a^k) - a^k \cdot b^2$ it follows that the algebra I is isomorphic to the subalgebra generated in $\overline{A}^{(+)}$ by the two generators $\overline{a}$ and $\overline{b}$ that are the images of the elements a and b. This proves the theorem. □

Clearly, as a byproduct we have reproved the theorem of A.I. Malcev [3] that states that any associative algebra over Σ with a finite or countably infinite number of generators can be embedded into an associative algebra over Σ with two generators.

Remark. From the proof of Theorem 1 it follows that the generators of the algebra I can be expressed in terms of the generators $\overline{a}$ and $\overline{b}$ using only the algebra product without scalar multiplication.

3. Main theorem

Consider the set S of associative words in two generators a and b. The degree of an associative word will be understood in the usual sense; in addition, we will introduce the notion of *height*. The heights of the associative words

$$a^{n_1}b^{m_1}a^{n_2}b^{m_2}\cdots a^{n_k}b^{m_k} \quad \text{and} \quad a^{n_1}b^{m_1}a^{n_2}b^{m_2}\cdots a^{n_k}b^{m_k}a^{n_{k+1}},$$

and also of the words obtained from these by interchanging a and b, will be respectively $2k$ and $2k+1$. The words of the form a^s and b^r have height 1, the words a^sb^r and b^ra^s have height 2, and so on.

We define a mapping $\alpha \to \overline{\alpha}$ of the set S onto itself as follows: for $\alpha \in S$ we set $\overline{\alpha} = \alpha$ if α has height 1, and $\overline{\alpha} = d^m\overline{c}$ if $\alpha = cd^m$ where d is one of the generators a and b.

To each associative word α in S we assign an element α^* of the free Jordan algebra I over Σ with two generators a and b as follows:

$$\alpha^* = \begin{cases} \alpha \text{ if } \alpha \text{ has height 1,} \\ a^s \circ b^r \text{ if } \alpha = a^sb^r \text{ or } \alpha = b^ra^s, \\ a^m \circ (ca^n)^* + (a^mc)^* \circ a^n - c^* \circ a^{m+n} \text{ if } \alpha = a^mca^n, \\ 2a^m \circ (b^n \circ c^*) + 2b^n \circ (a^m \circ c^*) - 2(a^m \circ b^n) \circ c^* - (b^nca^m)^* \\ \qquad \text{if } \alpha = a^mcb^n. \end{cases} \tag{5}$$

Interchanging a and b in the third and fourth cases, we obtain two more formulas. The symbol $\circ$ in the right-hand side means the multiplication in the free Jordan algebra; in the fourth case one should also take into account that the height of the word b^nca^m is smaller than the height of the word $\alpha = a^mcb^n$.

For two associative words α and β we introduce the operation

$$\alpha \circ \beta = \frac{1}{4}\big(\alpha\beta + \alpha\overline{\beta} + \beta\alpha + \overline{\beta}\alpha\big), \tag{6}$$

where in the right-hand side we have an element of the free associative algebra A over Σ on two generators a and b. The two meanings of the operation $\circ$ should not cause confusion, as can be seen from the Main Lemma stated below.

The next two formulas follow immediately from the definition:

$$(\overline{\alpha})^* = \alpha^* \quad \text{and} \quad (\alpha \circ \beta)^* = (\beta \circ \alpha)^*. \tag{7}$$

By straightforward computation, one can verify the equation

$$J_1(\alpha, \beta, \gamma, \delta) = 0, \tag{8}$$

where α, β, γ, δ are words from S and the multiplication is performed in the sense of the operation $\circ$. Clearly, from this it follows that

$$J_2(\alpha, \beta, \gamma, \delta) = 0. \tag{9}$$

The validity of equations (8) and (9) will also be clear from what follows.

We extend the operations $*, \overline{\ }, \circ$ linearly to the elements of the free associative algebra over Σ with generators a and b.

Main Lemma. *For associative words α and β in two generators a and b, the following equation holds:*

$$(\alpha \circ \beta)^* = \alpha^* \circ \beta^*.$$

The proof of the Main Lemma, owing to its complexity, will be given in the next section; now we will consider its consequences.

Let A be the free associative algebra over Σ with two generators a and b. In the Jordan algebra $A^{(+)}$, the elements a and b generate a subalgebra $A_0^{(+)}$.

Lemma 3. *Every element of the algebra $A_0^{(+)}$ can be represented as a linear combination (with coefficients from Σ) of elements of the form $\alpha + \overline{\alpha}$ where α is an associative word in a and b.*

Proof. Obviously, it suffices to prove Lemma 3 for monomials relative to the operation $\cdot$ of the algebra $A_0^{(+)}$. For monomials of the form a^r or b^s, the lemma is obvious. Suppose we have some monomial $M = N \cdot P$ of the algebra $A_0^{(+)}$ where N and P are monomials of lower degree for which we assume that Lemma 3 is valid. Then the validity of Lemma 3 follows from the equation:

$$\begin{aligned}&(\alpha + \overline{\alpha}) \cdot \left(\beta + \overline{\beta}\right)\\ &= \frac{1}{2}\left(\alpha\beta + \overline{\alpha\beta}\right) + \frac{1}{2}\left(\alpha\overline{\beta} + \beta\overline{\alpha}\right) + \frac{1}{2}\left(\overline{\alpha}\beta + \overline{\beta}\alpha\right) + \frac{1}{2}\left(\overline{\alpha}\,\overline{\beta} + \beta\alpha\right).\end{aligned}$$

This completes the proof. □

Theorem 2. *The algebra $A_0^{(+)}$ is isomorphic to the free Jordan algebra I over Σ with generators a and b.*

Proof. To each element of the form $(\alpha + \overline{\alpha})/2$ of the algebra $A_0^{(+)}$ where $\alpha \in S$, we assign the element α^* of I. By Lemma 3 this mapping can be extended to the entire additive group of the algebra $A_0^{(+)}$.

We show that this mapping is a homomorphism from $A_0^{(+)}$ to I. It follows from the definition that this mapping is Σ-linear (it preserves addition, and multiplication by elements of Σ). From the equation

$$\begin{aligned}&\left[\frac{1}{2}(\alpha + \overline{\alpha})\right] \cdot \left[\frac{1}{2}\left(\beta + \overline{\beta}\right)\right] = \frac{1}{8}\left(\alpha\beta + \alpha\overline{\beta} + \overline{\alpha}\beta + \overline{\alpha}\overline{\beta} + \beta\alpha + \overline{\beta}\alpha + \beta\overline{\alpha} + \overline{\beta}\overline{\alpha}\right)\\ &= \frac{1}{4}\left(\frac{\alpha\beta + \overline{\beta}\overline{\alpha}}{2}\right) + \frac{1}{4}\left(\frac{\alpha\overline{\beta} + \beta\overline{\alpha}}{2}\right) + \frac{1}{4}\left(\frac{\overline{\alpha}\beta + \overline{\beta}\alpha}{2}\right) + \frac{1}{4}\left(\frac{\overline{\alpha}\,\overline{\beta} + \beta\alpha}{2}\right),\end{aligned}$$

it follows that to the product of the elements $(\alpha + \overline{\alpha})/2$ and $(\beta + \overline{\beta})/2$ there corresponds the following element of I:

$$\frac{1}{4}\left[(\alpha\beta)^* + \left(\alpha\overline{\beta}\right)^* + (\beta\alpha)^* + \left(\overline{\beta}\alpha\right)^*\right] = (\alpha \circ \beta)^* = \alpha^* \circ \beta^*,$$

where we have used the Main Lemma and the bilinearity of the operation $*$. This implies that the image of the product equals the product of the images.

We now show that each element of the algebra I is the image of some element of the algebra $A_0^{(+)}$. Indeed, the elements of I of the form a^s and b^r have obvious pre-images; if we now assume the existence of pre-images for elements n and p of the algebra I, then clearly there exists a pre-image for $m = n \circ p$. The proof can now be completed by induction and the passage from monomials to polynomials.

Since the Jordan algebra I is free, it is clear that the mapping just constructed is an isomorphism, and this completes the proof. □

Every ideal I_1 of the algebra $A_0^{(+)}$, being a subset of the algebra A, generates in it some ideal $\overline{I_1}$.

Lemma 4. *For every ideal I_1 of the algebra $A_0^{(+)}$, the following equality holds:*

$$\overline{I_1} \cap A_0^{(+)} = I_1.$$

Proof. From Lemma 3 it follows that each element s of the algebra $A_0^{(+)}$, considered as an associative polynomial, satisfies the relation $s = \overline{s}$. Let v be an element of the intersection $\overline{I_1} \cap A_0^{(+)}$. Then v, being an element of the ideal $\overline{I_1}$, can be written as

$$v = \sum_k c_k i_k d_k,$$

where $i_k \in I_1$ and c_k, d_k are associative words. Since v is an element of the algebra $A_0^{(+)}$, we have

$$v = \frac{1}{2}(v + \overline{v}) = \sum_k \frac{c_k\, i_k\, d_k + \overline{d_k}\, i_k\, \overline{c_k}}{2}.$$

We show that each summand

$$e_k = \frac{c_k\, i_k\, d_k + \overline{d_k}\, i_k\, \overline{c_k}}{2}$$

belongs to the ideal I_1. We carry out an induction on the sum of the heights of the words c_k and d_k. If this sum is equal to 1, i.e., one of the words has the form a^r or b^s and the other is empty, then the statement is obvious. Suppose the statement has been proved for all smaller sums. We show that in this case the statement is true if both words c_k and d_k are nonempty. Then, up to interchanging the generators a and b, there are two possible cases:

(1) $e_k = \dfrac{a^m c a^n + a^n \overline{c} a^m}{2}$, and so

$$e_k = a^m \cdot \frac{c a^n + a^n \overline{c}}{2} + a^n \cdot \frac{a^m c + \overline{c} a^m}{2} - a^{m+n} \cdot \frac{c + \overline{c}}{2},$$

(2) $e_k = \dfrac{a^m c b^n + b^n \overline{c} a^m}{2}$, and so

$$e_k = 2a^m \cdot \left(b^n \cdot \frac{c + \overline{c}}{2}\right) + 2b^n \cdot \left(a^m \cdot \frac{c + \overline{c}}{2}\right) - 2\,(b^n \cdot a^m) \cdot \frac{c + \overline{c}}{2} - \frac{b^n c a^m + a^m \overline{c} b^n}{2}.$$

Clearly, in both cases, the conditions of the inductive hypothesis are satisfied, provided that

$$e_k \neq \frac{a^m i_k b^n + b^n i_k a^m}{2},$$

and in the remaining case,

$$e_k = a^m \cdot (b^n \cdot i_k) + b^n \cdot (a^m \cdot i_k) - (b^n \cdot a^m) \cdot i_k.$$

It remains to consider the case when

$$e_k = \frac{i_k CD + \overline{D}\,\overline{C}\,i_k}{2}.$$

This case can be reduced to a previous case using the inductive hypothesis and the equation

$$e_k = 2D \cdot \frac{i_k C + \overline{C} i_k}{2} - \frac{D i_k C + \overline{C} i_k D}{2},$$

if we assume that $D = \overline{D}$. We are permitted to make this assumption by separating as D a factor of height 1. Therefore, we have proved that $\overline{I_1} \cap A_0^{(+)} \subseteq I_1$. The reverse inclusion is obvious, and this completes the proof of the lemma. □

Theorem 3. *Every Jordan algebra $\mathcal{N}$ over Σ with two generators is special.*

Proof. From Theorem 1 it follows that the algebra $\mathcal{N}$ is isomorphic to a quotient algebra of $A_0^{(+)}$ by some ideal I_1. Lemma 4 implies that, in the quotient algebra $A/\overline{I_1}$, distinct elements of the algebra $A_0^{(+)}/I_1$ have distinct images. From here it follows that the Jordan algebra $\mathcal{N} \cong A_0^{(+)}/I_1$ is isomorphic to a subalgebra of the Jordan algebra $(A/\overline{I_1})^{(+)}$. This completes the proof. □

Remark. The statements of Lemmas 3 and 4 for algebras over a field are contained in the results of Cohn [2], where a special case of Theorem 3 is also proved, stating that a homomorphic image of a special Jordan algebra (over a field) with two generators is a special Jordan algebra.

4. Main lemma

We start the proof of the Main Lemma. In the course of the proof, for associative words α and β, we will assume the following inductive hypotheses:

1) *The lemma holds for pairs of words for which the sum of the heights is less than the corresponding sum for α and β.*
2) *The lemma holds for pairs of words for which the sum of the heights is equal to the corresponding sum for α and β, but the sum of the degrees is less than the corresponding sum for α and β.*

The basis of the induction is the obvious validity of the lemma when the sum of heights equals 2.

3) *The lemma holds for pairs of words for which the sum of the heights as well as the sum of the degrees are equal to the corresponding sums for α and β, but the smaller of the heights is less than the smaller of the heights of α and β.*

The basis of the induction for the last hypothesis will be justified below, where it will be shown that the lemma holds if one of the heights of α and β is less than 3.

Suppose now that β has height greater than 2, and the height of α is not less than the height of β. Then,

$$\beta^* = \sum_i \sigma_i \left(c_i^* \circ d_i^*\right) \circ e_i^* + \sum_j \sigma_j a^{k_j} \circ b^{s_j},$$

where σ_k are some coefficients. By the bilinearity of all the operations, to prove the lemma it suffices to consider in place of β^* the elements $\beta_1 = (c^* \circ d^*) \circ e^*$ and $\beta_2 = a^k \circ b^s$.

From inductive hypothesis 3) it follows that

$$\alpha^* \circ \beta_2^* = \alpha^* \circ \left(a^k \circ b^s\right) = \left[\alpha \circ \left(a^k \circ b^s\right)\right]^* = (\alpha \circ \beta_2)^*.$$

From equation (2) it follows that

$$\begin{aligned}
&\alpha^* \circ \beta_1^* = \alpha^* \circ [(c^* \circ d^*) \circ e^*] \\
&= J_1\{e^*, c^*, d^*, \alpha^*\} - [(\alpha^* \circ c^*) \circ e^*] \circ d^* - [(\alpha^* \circ d^*) \circ e^*] \circ c^* \\
&\quad + (\alpha^* \circ e^*) \circ (c^* \circ d^*) + (\alpha^* \circ c^*) \circ (d^* \circ e^*) + (\alpha^* \circ d^*) \circ (c^* \circ e^*),
\end{aligned}$$

but according to inductive hypothesis 3) and equation (8) we have

$$\alpha^* \circ \beta_1^* = [\alpha \circ \beta_1 - J_1\{e, c, d, a\}]^* = (\alpha \circ \beta_1)^*.$$

This completes the proof of the lemma.

It will be far more difficult to justify the basis for inductive hypothesis 3). Here the proof will consist of a number of cases.

4.1. Case 1: $\alpha = a^m b^s D b^r$, $\beta = a^n$

From the definitions of $*$ and $\circ$, and equation (2), it follows that

$$\begin{aligned}
&(\alpha \circ \beta)^* - \alpha^* \circ \beta^* = \frac{1}{2}\left(a^m b^s D b^r a^n\right)^* + \frac{1}{2}\left(a^{m+n} b^s D b^r\right)^* - \left(a^m b^s D b^r\right)^* \circ a^n \\
&= \frac{1}{2} a^m \circ \left(b^s D b^r a^n\right)^* - \frac{1}{2} a^n \circ \left(a^m b^s D b^r\right)^* - \frac{1}{2} a^{m+n} \circ \left(b^s D b^r\right)^* \\
&\quad + \frac{1}{2}\left(a^{m+n} b^s D b^r\right)^* \\
&= a^m \circ \{b^s \circ [a^n \circ (D b^r)^*]\} + a^m \circ \{a^n \circ [b^s \circ (D b^r)^*]\} \\
&\quad - a^m \circ \{(a^n \circ b^s) \circ (D b^r)^*]\} - \frac{1}{2} a^m \circ \left(a^n D b^{r+s}\right)^* - \frac{1}{2} a^n \circ \left(a^m b^s D b^r\right)^* \\
&\quad - \frac{1}{2} a^{m+n} \circ \left(b^s D b^r\right)^* + \frac{1}{2}\left(a^{m+n} b^s D b^r\right)^*
\end{aligned}$$

$$
\begin{aligned}
&= J_2\{b^s, (Db^r)^*, a^m, a^n\} - a^n \circ \{b^s \circ [a^m \circ (Db^r)^*]\} - (a^{m+n} \circ b^s) \circ (Db^r)^* \\
&\quad + b^s \circ [a^{m+n} \circ (Db^r)^*] + a^n \circ [(a^m \circ b^s) \circ (Db^r)^*] \\
&\quad + a^m \circ \{a^n \circ [b^s \circ (Db^r)^*]\} - \frac{1}{2} a^m \circ (a^n Db^{r+s})^* - \frac{1}{2} a^n \circ (a^m b^s Db^r)^* \\
&\quad - \frac{1}{2} a^{m+n} \circ (b^s Db^r)^* + \frac{1}{2} (a^{m+n} b^s Db^r)^*.
\end{aligned}
$$

Using inductive hypothesis 1), we can write the following equations:

$$
\begin{aligned}
&a^n \circ \{b^s \circ [a^m \circ (Db^r)^*]\} = \qquad (10)\\
&\frac{1}{4}\Big[a^n \circ (b^s a^m Db^r)^* + a^n \circ (b^s Db^r a^m)^* + a^n \circ (a^m Db^{r+s})^* + a^n \circ (Db^r a^m b^s)^*\Big],\\
&(a^{m+n} \circ b^s) \circ (Db^r)^* = \qquad (11)\\
&\frac{1}{4}\Big[(a^{m+n} b^s Db^r)^* + (b^s a^{m+n} Db^r)^* + (Db^r a^{m+n} b^s)^* + (Db^{r+s} a^{m+n})^*\Big],\\
&b^s \circ [a^{m+n} \circ (Db^r)^*] = \qquad (12)\\
&\frac{1}{4}\Big[(b^s a^{m+n} Db^r)^* + (b^s Db^r a^{m+n})^* + (a^{m+n} Db^{r+s})^* + (Db^r a^{m+n} b^s)^*\Big],\\
&a^n \circ [(a^m \circ b^s) \circ (Db^r)^*] = \qquad (13)\\
&\frac{1}{4}\Big[a^n \circ (a^m b^s Db^r)^* + a^n \circ (b^s a^m Db^r)^* + a^n \circ (Db^r a^m b^s)^* + a^n \circ (Db^{r+s} a^m)^*\Big],\\
&\frac{1}{2} a^m \circ (a^n Db^{r+s})^* = \frac{1}{4}\Big[(a^{m+n} Db^{r+s})^* + (a^n Db^{r+s} a^m)^*\Big], \qquad (14)\\
&\frac{1}{2} a^{m+n} \circ (b^s Db^r)^* = \frac{1}{4}\Big[(a^{m+n} b^s Db^r)^* + (b^s Db^r a^{m+n})^*\Big]. \qquad (15)
\end{aligned}
$$

Using equation (4), and inductive hypothesis 1), we obtain the equation

$$
\begin{aligned}
a^m \circ \{a^n \circ [b^s \circ (Db^r)^*]\} &= a^n \circ \{a^m \circ [b^s \circ (Db^r)^*]\} \qquad (16)\\
&= \frac{1}{4}\Big[a^n \circ (a^m b^s Db^r)^* + a^n \circ (a^m Db^{r+s})^* \\
&\qquad + a^n \circ (b^s Db^r a^m)^* + a^n \circ (Db^{r+s} a^m)^*\Big].
\end{aligned}
$$

Substituting the right-hand sides of equations (10–16) for the corresponding terms in the preceding expression for $(\alpha \circ \beta)^* - \alpha^* \circ \beta^*$, and combining like terms, we obtain:

$$
\begin{aligned}
&(\alpha \circ \beta)^* - \alpha^* \circ \beta^* = \\
&\frac{1}{2} a^n \circ \left(Db^{r+s} a^m\right)^* - \frac{1}{4}\left(Db^{r+s} a^{m+n}\right)^* - \frac{1}{4}\left(a^n Db^{r+s} a^m\right)^* = 0,
\end{aligned}
$$

by inductive hypothesis 1).

4.2. Case 2: $\alpha = a^s D a^m$, $\beta = a^t$

First we prove the validity of the lemma for $s = m$. In this case, it follows from the definitions of the operations, inductive hypothesis 1), and equation (4), that

$$\begin{aligned}(\alpha\circ\beta)^* &= \left(a^sDa^s\circ a^t\right)^* = \frac{1}{2}\left(a^sDa^{s+t}\right)^* + \frac{1}{2}\left(a^{s+t}Da^s\right)^* \\ &= \frac{1}{2}a^s\circ\left(Da^{s+t}\right)^* + \frac{1}{2}a^{s+t}\circ(a^sD)^* + \frac{1}{2}a^{s+t}\circ(Da^s)^* + \frac{1}{2}a^s\circ\left(a^{s+t}D\right)^* \\ &\quad - a^{2s+t}\circ D^* \\ &= a^s\circ\left(D^*\circ a^{s+t}\right) + a^{s+t}\circ(a^s\circ D^*) - a^{2s+t}\circ D^* \\ &= 2a^{s+t}\circ(a^s\circ D^*) - a^{2s+t}\circ D^*.\end{aligned} \tag{17}$$

By inductive hypothesis 2) we have:

$$\begin{aligned}\alpha^*\circ\beta^* &= (a^sDa^s)^*\circ a^t = a^t\circ[2a^s\circ(a^s\circ D) - a^{2s}\circ D]^* \\ &= 2a^t\circ[a^s\circ(a^s\circ D^*)] - a^t\circ(a^{2s}\circ D^*).\end{aligned} \tag{18}$$

From equations (17) and (18) it follows that:

$$\begin{aligned}&(\alpha\circ\beta)^* - \alpha^*\circ\beta^* \\ &= 2a^{s+t}\circ(a^s\circ D^*) + a^t\circ\left(a^{2s}\circ D^*\right) - 2a^t\circ[a^s\circ(a^s\circ D^*)] - a^{2s+r}\circ D^* \\ &= -J_1\{a^s, a^s, a^t, D^*\} = 0.\end{aligned}$$

In the proof of the general case, we will assume that $s > m$. We can do this without loss of generality, because in the contrary case, we can consider $\overline{\alpha}$ instead of α. Using hypothesis 2) we obtain:

$$\begin{aligned}\alpha^*\circ\beta^* &= (a^sDa^m)^*\circ a^t \\ &= a^t\circ\{2a^m\circ[a^m\circ(a^{s-m}D)] - a^{2m}\circ(a^{s-m}D)]\}^* \\ &= 2a^t\circ\{a^m\circ[a^m\circ(a^{s-m}D)^*]\} - a^t\circ[a^{2m}\circ(a^{s-m}D)^*] \\ &= J_2\{a^m, (a^{s-m}D)^*, a^t, a^m\} + 2a^{m+t}\circ[a^m\circ(a^{s-m}D)^*] - a^{2m+t}\circ(a^{s-m}D)^* \\ &= (a^sD)^*\circ a^{m+t} + (a^{s-m}Da^m)^*\circ a^{m+t} - a^{2m+t}\circ(a^{s-m}D)^*.\end{aligned} \tag{19}$$

From equation (19) it follows that the proof can be completed by induction on the degree of β, with constant sums of heights and degrees of α and β.

Assuming that the lemma holds for $t' > t$, we have:

$$(a^{s-m}Da^m)^*\circ a^{m+t} = \frac{1}{2}(a^{s+t}Da^m)^* + \frac{1}{2}(a^{s-m}Da^{2m+t})^*. \tag{20}$$

From inductive hypothesis 1) it follows that:

$$(a^sD)^*\circ a^{m+t} = \frac{1}{2}(a^{m+t+s}D)^* + \frac{1}{2}(a^sDa^{m+t})^*, \tag{21}$$

and

$$a^{2m+t}\circ(a^{s-m}D)^* = \frac{1}{2}(a^{m+t+s}D)^* + \frac{1}{2}(a^{s-m}Da^{2m+t})^*. \tag{22}$$

Using equations (20), (21) and (22), we obtain from (19):

$$\alpha^* \circ \beta^* = \frac{1}{2}(a^{s+t}Da^m)^* + \frac{1}{2}(a^sDa^{m+t})^* = (\alpha \circ \beta)^*,$$

as desired.

Remark. The sum of heights in Case 1 is odd, and in Case 2 is even. From transformations (17) through (22) it is clear that the proof in Case 2 reduces to Case 1 with the sum of heights being smaller by 1. Therefore the validity of the Main Lemma for Case 2 with the sum of the heights of α and β equal to 2ℓ can be assumed as soon as the validity is assumed for Case 1 with the corresponding sum equal to $2\ell - 1$. This remark will be needed in the proof of Case 5.

4.3. Case 3: $\alpha = a^mb^sDb^ra^t$**,** $\beta = b^n$

First we consider the easier special case when the word D is empty. Let $\alpha_1 = a^mb^sa^t$. Then from equations (2), (4), and the definitions of the operations, it follows that

$$\begin{aligned}
(\alpha_1 \circ \beta)^* &= \frac{1}{2}(a^mb^sa^tb^n)^* + \frac{1}{2}(b^na^mb^sa^t)^* \\
&= a^m \circ [b^n \circ (b^s \circ a^t)] + b^n \circ [a^m \circ (b^s \circ a^t)] - (b^n \circ a^m) \circ (b^s \circ a^t) \\
&\quad - \frac{1}{2}b^{n+s} \circ a^{m+t} + b^n \circ [a^t \circ (a^m \circ b^s)] + a^t \circ [b^n \circ (a^m \circ b^s)] \\
&\quad - (b^n \circ a^t) \circ (b^s \circ a^m) - \frac{1}{2}b^{n+s} \circ a^{m+t} \\
&= J_1\{b^n, b^s, a^t, a^m\} - b^s \circ (b^n \circ a^{t+m}) + 2b^n \circ [a^m \circ (b^s \circ a^t)] \\
&= 2[a^m \circ (b^s \circ a^t)] \circ b^n - (a^{t+m} \circ b^s) \circ b^n = \alpha_1^* \circ \beta^*,
\end{aligned}$$

as desired. In the general case, the proof is much longer.

Using inductive hypothesis 1), the definitions of the operations, and equation (4), we obtain

$$\begin{aligned}
(\alpha \circ \beta)^* - \alpha^* \circ \beta^* &= [(a^mb^sDb^ra^t) \circ b^n]^* - (a^mb^sDb^ra^t)^* \circ b^n \\
&= \frac{1}{2}(a^mb^sDb^ra^tb^n)^* + \frac{1}{2}(b^na^mb^sDb^ra^t)^* - (a^mb^sDb^ra^t)^* \circ b^n \\
&= a^m \circ [b^n \circ (b^sDb^ra^t)^*] + b^n \circ [a^m \circ (b^sDb^ra^t)^*] - (b^n \circ a^m) \circ (b^sDb^ra^t)^* \\
&\quad - \frac{1}{2}(b^{n+s}Db^ra^{t+m})^* + b^n \circ [a^t \circ (a^mb^sDb^r)^*] + a^t \circ [b^n \circ (a^mb^sDb^r)^*] \\
&\quad - (a^t \circ b^n) \circ (a^mb^sDb^r)^* - \frac{1}{2}(a^{m+t}b^sDb^{r+n})^* - b^n \circ [a^m \circ (b^sDb^ra^t)^*] \\
&\quad - b^n \circ [a^t \circ (a^mb^sDb^r)^*] + b^n \circ [a^{m+t} \circ (b^sDb^r)^*] \\
&= a^m \circ [b^n \circ (b^sDb^ra^t)^*] - (b^n \circ a^m) \circ (b^sDb^ra^t)^* + a^t \circ [b^n \circ (a^mb^sDb^r)^*] \\
&\quad - (a^t \circ b^n) \circ (a^mb^sDb^r)^* - \frac{1}{2}(b^{n+s}Db^ra^{t+m})^* - \frac{1}{2}(a^{m+t}b^sDb^{r+n})^* \\
&\quad + b^n \circ [a^{m+t} \circ (b^sDb^r)^*]
\end{aligned}$$

$$
\begin{aligned}
&= a^m \circ [b^n \circ (b^s D b^r a^t)^*] - (b^n \circ a^m) \circ (b^s D b^r a^t)^* \\
&\quad + 2a^t \circ \{b^n \circ [a^m \circ (b^s D b^r)^*]\} - a^t \circ [b^n \circ (b^s D b^r a^m)^*] \\
&\quad - 2(a^t \circ b^n) \circ [a^m \circ (b^s D b^r)^*] + (a^t \circ b^n) \circ (b^s D b^r a^m)^* \\
&\quad - \frac{1}{2}(b^{n+s} D b^r a^{t+m})^* - \frac{1}{2}(a^{m+t} b^s D b^{r+n})^* + b^n \circ [a^{m+t} \circ (b^s D b^r)^*] \\
&= 2a^m \circ \langle b^n \circ \{b^s \circ [a^t \circ (D b^r)^*]\}\rangle + 2a^m \circ \langle b^n \circ \{a^t \circ [b^s \circ (D b^r)^*]\}\rangle \\
&\quad - 2a^m \circ \{b^n \circ [(a^t \circ b^s) \circ (D b^r)^*]\} - 2(a^m \circ b^n) \circ \{b^s \circ [a^t \circ (D b^r)^*]\} \\
&\quad - 2(a^m \circ b^n) \circ \{a^t \circ [b^s \circ (D b^r)^*]\} + 2(a^m \circ b^n) \circ [(a^t \circ b^s) \circ (D b^r)^*] \\
&\quad - 2a^t \circ \langle b^n \circ \{b^s \circ [a^m \circ (D b^r)^*]\}\rangle - 2a^t \circ \langle b^n \circ \{a^m \circ [b^s \circ (D b^r)^*]\}\rangle \\
&\quad + 2a^t \circ \{b^n \circ [(a^m \circ b^s) \circ (D b^r)^*]\} + 2(a^t \circ b^n) \circ \{b^s \circ [a^m \circ (D b^r)^*]\} \\
&\quad + 2(a^t \circ b^n) \circ \{a^m \circ [b^s \circ (D b^r)^*]\} - 2(a^t \circ b^n) \circ [(a^m \circ b^s) \circ (D b^r)^*] \\
&\quad + 2a^t \circ \{b^n \circ [a^m \circ (b^s D b^r)^*]\} - 2(a^t \circ b^n) \circ [a^m \circ (b^s D b^r)^*] \\
&\quad - \frac{1}{2}(b^{n+s} D b^r a^{t+m})^* - \frac{1}{2}(a^{m+t} b^s D b^{r+n})^* + b^n \circ [a^{m+t} \circ (b^s D b^r)^*] \\
&\quad - a^m \circ [b^n \circ (a^t D b^{r+s})^*] + a^t \circ [b^n \circ (a^m D b^{r+s})^*] \\
&\quad + (a^m \circ b^n) \circ (a^t D b^{r+s})^* - (a^t \circ b^n) \circ (a^m D b^{r+s})^* \\
&= 2J_1\{b^n, a^m, b^s, a^t \circ (D b^r)^*\} - 2b^s \circ \langle b^n \circ \{a^m \circ [a^t \circ (D b^r)^*]\}\rangle \\
&\quad - 2[(a^m \circ b^s) \circ b^n] \circ [a^t \circ (D b^r)^*] + 2b^{n+s} \circ \{a^m \circ [a^t \circ (D b^r)^*]\} \\
&\quad + 2\{b^n \circ [a^t \circ (D b^r)^*]\} \circ (a^m \circ b^s) - 2a^t \circ \langle b^n \circ \{a^m \circ [b^s \circ (D b^r)^*]\} \\
&\quad + 2(a^t \circ b^n) \circ \{a^m \circ [b^s \circ (D b^r)^*]\} - 2J_1\{b^n, a^m, a^t \circ b^s, (D b^r)^*\} \\
&\quad + 2(a^t \circ b^s) \circ \{b^n \circ [a^m \circ (D b^r)^*]\} + 2\{b^n \circ [a^m \circ (a^t \circ b^s)]\} \circ (D b^r)^* \\
&\quad - 2[(a^t \circ b^s) \circ b^n] \circ [a^m \circ (D b^r)^*] - 2[a^m \circ (a^t \circ b^s)] \circ [b^n \circ (D b^r)^*] \\
&\quad - 2J_1\{b^n, a^t, b^s, a^m \circ (D b^r)^*\} + 2b^s \circ \langle b^n \circ \{a^t \circ [a^m \circ (D b^r)^*]\}\rangle \\
&\quad + 2[(a^t \circ b^s) \circ b^n] \circ [a^m \circ (D b^r)^*] - 2b^{n+s} \circ \{a^t \circ [a^m \circ (D b^r)^*]\} \\
&\quad - 2\{b^n \circ [a^m \circ (D b^r)^*]\} \circ (a^t \circ b^s) + 2a^m \circ \langle b^n \circ \{a^t \circ [b^s \circ (D b^r)^*]\}\rangle \\
&\quad - 2(a^m \circ b^n) \circ \{a^t \circ [b^s \circ (D b^r)^*]\} + 2J_1\{b^n, a^t, a^m \circ b^s, (D b^r)^*\} \\
&\quad - 2(a^m \circ b^s) \circ \{b^n \circ [a^t \circ (D b^r)^*]\} - 2\{b^n \circ [a^t \circ (a^m \circ b^s)]\} \circ (D b^r)^* \\
&\quad + 2[(a^m \circ b^s) \circ b^n] \circ [a^t \circ (D b^r)^*] + 2[a^t \circ (a^m \circ b^s)] \circ [b^n \circ (D b^r)^*] \\
&\quad + 2a^t \circ \{b^n \circ [a^m \circ (b^s D b^r)^*]\} - 2(a^t \circ b^n) \circ [a^m \circ (b^s D b^r)^*] \\
&\quad - \frac{1}{2}(b^{n+s} D b^r a^{t+m})^* - \frac{1}{2}(a^{m+t} b^s D b^{r+n})^* + b^n \circ [a^{m+t} \circ (b^s D b^r)^*] \\
&\quad - a^m \circ [b^n \circ (a^t D b^{r+s})^*] + (a^m \circ b^n) \circ (a^t D b^{r+s})^* \\
&\quad + a^t \circ [b^n \circ (a^m D b^{r+s})^*] - (a^t \circ b^n) \circ (a^m D b^{r+s})^*
\end{aligned}
$$

$$
\begin{aligned}
&= -2a^t \circ \langle b^n \circ \{a^m \circ [b^s \circ (Db^r)^*]\}\rangle + 2(a^t \circ b^n) \circ \{a^m \circ [b^s (Db^r)^*]\} \\
&\quad + 2a^m \circ \langle b^n \circ \{a^t \circ [b^s \circ (Db^r)^*]\}\rangle - 2(a^m \circ b^n) \circ \{a^t \circ [b^s \circ (Db^r)^*]\} \\
&\quad + 2a^t \circ \{b^n \circ [a^m \circ (b^s Db^r)^*]\} - 2(a^t \circ b^n) \circ [a^m \circ (b^s Db^r)^*] \\
&\quad - \frac{1}{2}(b^{n+s} Db^r a^{t+m})^* - \frac{1}{2}(a^{m+t} b^s Db^{r+n})^* + b^n \circ [a^{m+t} \circ (b^s Db^r)^*] \\
&\quad - a^m \circ [b^n \circ (a^t Db^{r+s})^*] + (a^m \circ b^n) \circ (a^t Db^{r+s})^* \\
&\quad + a^t \circ [b^n \circ (a^m Db^{r+s})^*] - (a^t \circ b^n) \circ (a^m Db^{r+s})^* \\
&= -2a^t \circ \langle b^n \circ \{a^m \circ [b^s \circ (Db^r)^*]\}\rangle + 2(a^t \circ b^n) \circ \{a^m \circ [b^s \circ (Db^r)^*]\} \\
&\quad + 2J_1\{b^n, a^t, a^m, b^s \circ (Db^r)^*\} - 2a^t \circ \langle b^n \circ \{a^m \circ [b^s \circ (Db^r)^*]\}\rangle \\
&\quad - 2(a^{m+t} \circ b^n) \circ [b^s \circ (Db^r)^*] + 2(a^t \circ b^n) \circ \{a^m \circ [b^s \circ (Db^r)^*]\} \\
&\quad + 2a^{m+t} \circ \{b^n \circ [b^s \circ (Db^r)^*]\} + 2a^t \circ \{b^n \circ [a^m \circ (b^s Db^r)^*]\} \\
&\quad - 2(a^t \circ b^n) \circ [a^m \circ (b^s Db^r)^*] - \frac{1}{2}(b^{n+s} Db^r a^{t+m})^* - \frac{1}{2}(a^{m+t} b^s Db^{r+n})^* \\
&\quad + b^n \circ [a^{m+t} \circ (b^s Db^r)^*] - a^m \circ [b^n \circ (a^t Db^{r+s})^*] + (a^m \circ b^n) \circ (a^t Db^{r+s})^* \\
&\quad + a^t \circ [b^n \circ (a^m Db^{r+s})^*] - (a^t \circ b^n) \circ (a^m Db^{r+s})^* \\
&= -2a^t \circ \{b^n \circ [a^m \circ (Db^{r+s})^*]\} + 2(a^t \circ b^n) \circ [a^m \circ (Db^{r+s})^*] \\
&\quad - 2(a^{m+t} \circ b^n) \circ [b^s \circ (Db^r)^*] + 2(a^{m+t} \circ \{b^n \circ [b^s \circ (Db^r)^*]\} \\
&\quad - \frac{1}{2}(b^{n+s} Db^r a^{t+m})^* - \frac{1}{2}(a^{m+t} b^s Db^{r+m})^* + b^n \circ [a^{m+t} \circ (b^s Db^r)^*] \\
&\quad - a^m \circ [b^n \circ (a^t Db^{r+s})^*] + (a^m \circ b^n) \circ (a^t Db^{r+s})^* \\
&\quad + a^t \circ [b^n \circ (a^m Db^{r+s})^*] - (a^t \circ b^n) \circ (a^m Db^{r+s})^* \\
&= \frac{1}{4}\Big[- (a^t b^n a^m Db^{r+s})^* - (a^t b^n Db^{s+r} a^m)^* - (a^{t+m} Db^{r+s+n})^* \\
&\qquad - (a^t Db^{r+s} a^m b^n)^* - (b^n a^m Db^{r+s} a^t)^* - (b^n Db^{r+s} a^{m+t})^* \\
&\qquad - (a^m Db^{r+s+n} a^t)^* - (Db^{r+s} a^m b^n a^t)^* + (a^t b^n a^m Db^{r+s})^* \\
&\qquad + (a^t b^n Db^{r+s} a^m)^* + (b^n a^{t+m} Db^{r+s})^* + (b^n a^t Db^{r+s} a^m)^* \\
&\qquad + (a^m Db^{r+s} a^t b^n)^* + (Db^{r+s} a^{m+t} b^n)^* + (a^m Db^{r+s+n} a^t)^* \\
&\qquad + (Db^{r+s} a^m b^n a^t)^* - (a^{m+t} b^{n+s} Db^r)^* - (b^n a^{m+t} b^s Db^r)^* \\
&\qquad - (a^{m+t} b^n Db^{r+s})^* - (b^n a^{m+t} Db^{r+s})^* - (b^s Db^r a^{m+t} b^n)^* \\
&\qquad - (b^s Db^{r+n} a^{m+t})^* - (Db^{r+s} a^{m+t} b^n)^* - (Db^{r+s+n} a^{m+t})^* \\
&\qquad + (a^{m+t} b^{n+s} Db^r)^* + (a^{m+t} b^n Db^{r+s})^* + (a^{m+t} b^s Db^{r+n})^* \\
&\qquad + (a^{m+t} Db^{r+s+n})^* + (b^{n+s} Db^r a^{m+t})^* + (b^n Db^{r+s} a^{m+t})^* \\
&\qquad + (b^s Db^{r+n} a^{m+t})^* + (Db^{r+s+n} a^{m+t})^* - 2(b^{n+s} Db^r a^{t+m})^* \\
&\qquad - 2(a^{m+t} b^s Db^{r+n})^* + (b^n a^{m+t} b^s Db^r)^* + (b^{n+s} Db^r a^{m+t})^*
\end{aligned}
$$

$$
\begin{aligned}
&+ (a^{m+t}b^sDb^{r+n})^* + (b^sDb^ra^{m+t}b^n)^* - (a^mb^na^tDb^{r+s})^* \\
&- (a^{m+t}Db^{r+s+n})^* - (b^na^tDb^{r+s}a^m)^* - (a^tDb^{r+s+n}a^m)^* \\
&+ (a^mb^na^tDb^{r+s})^* + (b^na^{m+t}Db^{r+s})^* + (a^tDb^{r+s}a^mb^n)^* \\
&+ (a^tDb^{r+s+n}a^m)^* + (a^tb^na^mDb^{r+s})^* + (a^{t+m}Db^{r+s+n})^* \\
&+ (b^na^mDb^{r+s}a^t)^* + (a^mDb^{r+s+n}a^t)^* - (a^tb^na^mDb^{r+s})^* \\
&- (b^na^{t+m}Db^{r+s})^* - (a^mDb^{r+s}a^tb^n)^* - (a^mDb^{r+s+n}a^t)^* \Big] \\
&= 0,
\end{aligned}
$$

as was to be established.

4.4. Case 4: $\alpha = a^mDb^n$, $\beta = a^tb^q$

From the definition of operation $*$ it follows that

$$
\begin{aligned}
(b^qa^mDb^na^t)^* = {} & 2b^q \circ [a^t \circ (a^mDb^n)^*] + 2a^t \circ [b^q \circ (a^mDb^n)^*] \\
& - 2(a^t \circ b^q) \circ (a^mDb^n)^* - (a^{m+t}Db^{n+q})^*.
\end{aligned}
$$

From this equation we have:

$$
\begin{aligned}
\alpha^* \circ \beta^* &= (a^mDb^n)^* \circ (a^t \circ b^q) \\
&= b^q \circ [a^t \circ (a^mDb^n)^*] + a^t \circ [b^q \circ (a^mDb^n)^*] \\
&\quad - \frac{1}{2}(a^{m+t}Db^{n+q})^* - \frac{1}{2}(b^qa^mDb^na^t)^*.
\end{aligned} \tag{23}
$$

Using inductive hypothesis 1), and the relation proved in Case 3, we obtain the equations

$$
\begin{aligned}
&b^q \circ [a^t \circ (a^mDb^n)^*] = b^q \circ (a^t \circ a^mDb^n)^* = [b^q \circ (a^t \circ a^mDb^n)]^* \qquad (24) \\
&= \frac{1}{4}(b^qa^{t+m}Db^n)^* + \frac{1}{4}(b^qa^mDb^na^t)^* + \frac{1}{4}(a^{t+m}Db^{n+q})^* + \frac{1}{4}(a^mDb^na^tb^q)^*, \\
&a^t \circ [b^q \circ (a^mDb^n)^*] = [a^t \circ (b^q \circ a^mDb^n)]^* \qquad (25) \\
&= \frac{1}{4}(a^tb^qa^mDb^n)^* + \frac{1}{4}(a^{t+m}Db^{n+q})^* + \frac{1}{4}(b^qa^mDb^na^t)^* + \frac{1}{4}(a^mDb^{n+q}a^t)^*.
\end{aligned}
$$

From equations (23), (24) and (25) it follows that

$$
\begin{aligned}
\alpha^* \circ \beta^* &= \frac{1}{4}\Big[(b^qa^{t+m}Db^n)^* + (a^mDb^na^tb^q)^* + (a^tb^qa^mDb^n)^* + (a^mDb^{n+q}a^t)^*\Big] \\
&= (\alpha \circ \beta)^*.
\end{aligned}
$$

Clearly, the same proof is valid if the word D is empty.

4.5. Case 5: $\alpha = a^mDa^n$, $\beta = a^pb^q$

4.5.1. Step 1. First of all we prove that the lemma holds if $m = n$. Using inductive hypothesis 1) and the relation proved in Case 1, we have:

$$
\alpha^* \circ \beta^* = (a^nDa^n)^* \circ (a^p \circ b^q) = [a^n \circ (a^nD + Da^n) - a^{2n} \circ D]^* \circ (a^p \circ b^q)
$$

$$
\begin{aligned}
&= [a^n \circ (a^n D + Da^n)^*] \circ (a^p \circ b^q) - (a^{2n} \circ D^*) \circ (a^p \circ b^q)\\
&= 2[a^n \circ (a^n \circ D^*)] \circ (a^p \circ b^q) - (a^{2n} \circ D^*) \circ (a^p \circ b^q)\\
&= 2J_2\{a^n, D^*, a^n, a^p \circ b^q\} - 2\{a^n \circ [a^n \circ (a^p \circ b^q)]\} \circ D^*\\
&\quad - 2\{a^n \circ [D^* \circ (a^p \circ b^q)]\} \circ a^n + 4\{D^* \circ [a^n \circ (a^p \circ b^q)]\} \circ a^n\\
&\quad + (a^{2n} \circ D^*) \circ (a^p \circ b^q)\\
&= -2\{a^n \circ [D^* \circ (a^p \circ b^q)]\} \circ a^n + 4\{D^* \circ [a^n \circ (a^p \circ b^q)]\} \circ a^n\\
&\quad + (a^{2n} \circ D^*) \circ (a^p \circ b^a) - J_1\{a^n, a^n, a^p, b^q\} \circ D^* + (b^q \circ a^{2n+p}) \circ D^*\\
&\quad - 2[a^{n+p} \circ (a^n \circ b^q)] \circ D^* - [a^{2n} \circ (a^p \circ b^q)] \circ D^*\\
&= \big[- 2\{a^n \circ [D \circ (a^p \circ b^q)] \circ a^n + 4\{D \circ [a^n \circ (a^p \circ b^q)]\} \circ a^n\\
&\qquad + (a^{2n} \circ D) \circ (a^p \circ b^q) - J_1\{a^n, a^n, a^p, b^q\} \circ D\\
&\qquad + (b^q \circ a^{2n+p}) \circ D - 2[a^{n+p} \circ (a^n \circ b^q)] \circ D - [a^{2n} \circ (a^p \circ b^q)] \circ D \big]^*\\
&= \big[- 2\{a^n \circ [a^n \circ (a^p \circ b^q)]\} \circ D - 2\{a^n \circ [D \circ (a^p \circ b^q)]\} \circ a^n\\
&\quad + 4\{D \circ [a^n \circ (a^p \circ b^q)]\} \circ a^n + (a^{2n} \circ D) \circ (a^p \circ b^q) \big]^*\\
&= \big[- 2J_2\{a^n, D, a^n, a^p \circ b^q\} + 2[a^n \circ (a^n \circ D)] \circ (a^p \circ b^q)\\
&\quad - (a^{2n} \circ D) \circ (a^p \circ b^q) \big]^*\\
&= \big\{ [2a^n \circ (a^n \circ D) - a^{2n} \circ D] \circ (a^p \circ b^q) \big\}^* = \big[a^n D a^n \circ (a^p \circ b^q)\big]^*\\
&= (\alpha \circ a^p b^q)^* = (\alpha \circ \beta)^*.
\end{aligned}
$$

4.5.2. Step 2. Now suppose that the lemma holds for some pair of words $\alpha_1 = a^t D a^r$, $\beta_1 = a^k b^s$. We will show that in this case the lemma also holds for the words $\alpha_2 = a^t D a^k$, $\beta_2 = a^r b^s$. Indeed,

$$
\begin{aligned}
&\alpha_2^* \circ \beta_2^* = (a^t D a^k)^* \circ (a^r \circ b^s)\\
&= 2[(a^t D)^* \circ a^k] \circ (a^r \circ b^s) - (a^{t+k} D)^* \circ (a^r \circ b^s)\\
&= -2J_1\{(a^t D)^*, a^k, a^r, b^s\} + 2[(a^t D)^* \circ a^{k+r}] \circ b^s + 2[(a^t D)^* \circ (a^k \circ a^s)] \circ a^r\\
&\quad + 2[(a^t D)^* \circ (a^r \circ b^s)] \circ a^k - 2[(a^t D)^* \circ b^s] \circ a^{k+r}\\
&\quad - 2[(a^t D)^* \circ a^r] \circ (a^k \circ b^s) - (a^{t+k} D)^* \circ (a^r \circ b^s)\\
&= \big[- 2J_1\{a^t D, a^k, a^r, b^s\} + 2(a^t D \circ a^{k+r}) \circ b^s + 2[a^t D \circ (a^k \circ b^s)] \circ a^r\\
&\quad + 2[a^t D \circ (a^r \circ b^s)] \circ a^k - 2(a^t D \circ b^s) \circ a^{k+r} - (a^{t+r} D) \circ (a^k \circ b^s)\\
&\quad - (a^{t+k} D) \circ (a^r \circ b^s) \big]^* - (a^t D a^r)^* \circ (a^k \circ b^s)\\
&= -\alpha_1^* \circ \beta_1^* + \big[2(a^t D \circ a^r) \circ (a^k \circ b^s) + 2(a^t D \circ a^k) \circ (a^r \circ b^s)\\
&\quad - (a^{t+r} D) \circ (a^k \circ b^s) - (a^{t+k} D) \circ (a^r \circ b^s) \big]^*\\
&= -\alpha_1^* \circ \beta_1^* + \big[a^t D a^r \circ (a^k \circ b^s) + a^t D a^k \circ (a^r \circ b^s)\big]^*\\
&= -\alpha_1^* \circ \beta_1^* + (\alpha_1 \circ \beta_1)^* + (\alpha_2 \circ \beta_2)^* = (\alpha_2 \circ \beta_2)^*.
\end{aligned}
$$

The claim is proved.

4.5.3. Step 3. Finally we prove that if the lemma holds for some words $\alpha_3 = a^{2s}Da^r$, $\beta_3 = a^pb^q$ then it also holds for the words $\alpha_4 = a^sDa^{r+s}$ and β_3. Indeed,

$$\begin{aligned}
\alpha_4^* \circ \beta_3^* &= (a^sDa^{r+s})^* \circ (a^p \circ b^q) = 2\{a^s \circ [a^s \circ (Da^r)^*]\} \circ (a^p \circ b^q) \qquad (26)\\
&= 2J_2\{a^s, a^p \circ b^q, a^s, (Da^r)^*\} - 2\{a^s \circ [(a^p \circ b^q) \circ (Da^r)^*]\} \circ a^s\\
&\quad - 2\{a^s \circ [a^s \circ (a^p \circ b^q)]\} \circ (Da^r)^* + 4\{(a^p \circ b^q) \circ [a^s \circ (Da^r)^*]\} \circ a^s\\
&\quad + 2[(a^p \circ b^q) \circ a^{2s}] \circ (Da^r)^* - [a^{2s} \circ (Da^r)^*] \circ (a^p \circ b^q)\\
&= -2\{a^s \circ [(a^p \circ b^q) \circ (Da^r)^*]\} \circ a^s + 4\{(a^p \circ b^q) \circ [a^s \circ (Da^r)^*]\} \circ a^s\\
&\quad - [a^{2s} \circ (Da^r)^*] \circ (a^p \circ b^q) - J_1\{a^s, a^s, a^p, b^q\} \circ (Da^r)^*\\
&\quad + (b^q \circ a^{2s+p}) \circ (Da^r)^* - 2[(a^s \circ b^q) \circ a^{s+p}] \circ (Da^r)^*\\
&\quad + [(a^p \circ b^q) \circ a^{2s}] \circ (Da^r)^*\\
&= -2\{a^s \circ [(a^p \circ b^q) \circ (Da^r)^*]\} \circ a^s + 4\{(a^p \circ b^q) \circ [a^s \circ (Da^r)^*]\} \circ a^s\\
&\quad - [a^{2s} \circ (Da^r)^*] \circ (a^p \circ b^q) + (b^q \circ a^{2s+p}) \circ (Da^r)^*\\
&\quad - 2J_2\{a^{s+p}, b^q, a^s, (Da^r)^*\} + J_2\{a^{2s}, b^q, a^p, (Da^r)^*\}\\
&\quad + 2\{a^{s+p} \circ [b^q \circ (Da^r)^*]\} \circ a^s + 2\{a^{s+p} \circ [a^s \circ (Da^r)^*]\} \circ b^q\\
&\quad - 2(b^q \circ a^{2s+p}) \circ (Da^r)^* - 2\{b^q \circ [a^{s+p} \circ (Da^r)^*]\} \circ a^s\\
&\quad - 2\{b^q \circ [a^s \circ (Da^r)^*]\} \circ a^{s+p} - \{a^{2s} \circ [b^q \circ (Da^r)^*]\} \circ a^p\\
&\quad - \{a^{2s} \circ [a^p \circ (Da^r)^*]\} \circ b^q + (b^q \circ a^{2s+p}) \circ (Da^r)^*\\
&\quad + \{b^q \circ [a^{2s} \circ (Da^r)^*]\} \circ a^p + \{b^q \circ [a^p \circ (Da^r)^*]\} \circ a^{2s}.
\end{aligned}$$

Using inductive hypothesis 2) we can move the symbol $*$ outside the braces in the first two monomials of the right-hand side of equation (26). As a result we obtain the monomials

$$\{a^s \circ [(a^p \circ b^q) \circ (Da^r)]\}^* \circ a^s \quad \text{and} \quad \{(a^p \circ b^q) \circ [a^s \circ (Da^r)]\}^* \circ a^s. \qquad (27)$$

After performing all the $\circ$ operations inside the braces, we obtain, either monomials whose heights will not exceed one less than the sum of the heights of α and β, or words whose heights are equal to the sum of the heights of the words α and β but which together with the word a^s form a pair of the form considered in Case 2. Using the cases already established, and the remark in Case 2, we conclude that the monomials (27) are equal respectively to the monomials

$$\langle\{a^s \circ [(a^p \circ b^q) \circ Da^r]\} \circ a^s\rangle^* \quad \text{and} \quad \langle\{(a^p \circ b^q) \circ [a^s \circ Da^r]\} \circ a^s\rangle^*. \qquad (28)$$

Since it is obvious that

$$\begin{aligned}
[a^{2s} \circ (Da^r)^*] \circ (a^p \circ b^q) &= [a^{2s} \circ Da^r]^* \circ (a^p \circ b^q)\\
&= \frac{1}{2}(a^{2s}Da^r)^* \circ (a^p \circ^q) + \frac{1}{2}(Da^{2s+r})^* \circ (a^p \circ b^q),
\end{aligned}$$

for the right-hand side of equation (26), using the cases established earlier or inductive hypothesis 1), we can move the operation $*$ outside the parentheses everywhere except in the term

$$\frac{1}{2}(a^{2s}Da^r)^* \circ (a^p b^q).$$

We do this, and then perform the transformations done in (26) in the reverse order:

$$\begin{aligned}
\alpha_4^* \circ \beta_3^* = \Big\langle & -2\{a^s \circ [(a^p \circ b^q) \circ (Da^r)]\} \circ a^s + 4\{(a^p \circ b^q) \circ [a^s \circ Da^r]\} \circ a^s \\
& - \frac{1}{2} Da^{2s+r} \circ (a^p \circ b^q) + (b^q \circ a^{2s+p}) \circ Da^r - 2J_2\{a^{s+p}, b^q, a^s, Da^r\} \\
& + J_2\{a^{2s}, b^q, a^p, Da^r\} + 2\{a^{s+p} \circ [b^q \circ Da^r]\} \circ a^s + 2\{a^{s+p} \circ [a^s \circ Da^r]\} \circ b^q \\
& - 2(b^q \circ a^{2s+p}) \circ Da^r - 2[b^q \circ (a^{s+p} \circ Da^r)] \circ a^s - 2[b^q \circ (a^s \circ Da^r)] \circ a^{s+p} \\
& - [a^{2s} \circ (b^q \circ Da^r)] \circ a^p - [a^{2s} \circ (a^p \circ Da^r)] \circ b^q + (b^q \circ a^{2s+p}) \circ Da^r \\
& + [b^q \circ (a^{2s} \circ Da^r)] \circ a^p + [b^q \circ (a^p \circ Da^r)] \circ a^{2s} \Big\rangle^* - \frac{1}{2}(a^{2s}Da^r)^* \circ (a^p \circ b^q) \\
= \Big\langle & -2\{a^s \circ [(a^p \circ b^q) \circ Da^r]\} \circ a^s + 4[(a^p \circ b^q) \circ (a^s \circ Da^r)] \circ a^s \\
& - \frac{1}{2} Da^{2s+r} \circ (a^p \circ b^q) + (b^q \circ a^{2s+p}) \circ Da^r - 2[a^{s+p} \circ (b^q \circ a^s)] \circ Da^r \\
& + [a^{2s} \circ (b^q \circ a^p)] \circ Da^r \Big\rangle^* - \frac{1}{2}\,\alpha_3^* \circ \beta_3^* \\
= \Big\langle & -2\{a^s \circ [(a^p \circ b^q) \circ Da^r]\} \circ a^s + 4[(a^p \circ b^q) \circ (a^s \circ Da^r)] \circ a^s \\
& - \frac{1}{2} Da^{2s+r} \circ (a^p \circ b^q) + J_1\{a^s, a^s, a^p, b^q\} \circ Da^r \\
& - 2\{a^s \circ [a^s \circ (a^p \circ b^q)]\} \circ Da^r + 2[a^{2s} \circ (b^q \circ a^p)] \circ Da^r \Big\rangle^* - \frac{1}{2}\,\alpha_3^* \circ \beta_3^* \\
= \Big\langle & -2J_2\{a^s, a^p \circ b^q, a^s, Da^r\} + 2[a^s \circ (a^s \circ Da^r)] \circ (a^p \circ b^q) \\
& - \frac{1}{2} Da^{2s+r} \circ (a^p \circ b^q) \Big\rangle^* - \frac{1}{2}\,\alpha_3^* \circ \beta_3^* \\
= & \frac{1}{2}[a^{2s}Da^r \circ (a^p \circ b^q)]^* + [a^s Da^{r+s} \circ (a^p \circ b^q)]^* - \frac{1}{2}\,\alpha_3^* \circ \beta_3^* \\
= & \frac{1}{2}(\alpha_3 \circ \beta_3)^* + (\alpha_4 \circ \beta_3)^* - \frac{1}{2}\,\alpha_3^* \circ \beta_3^* = (\alpha_4 \circ \beta_3)^*.
\end{aligned}$$

4.5.4. Step 4.

Definition. By the *δ-transformation* of a pair of natural numbers t and s, $t > s$, we will mean the transformation that replaces this pair by the pair $t - s, 2s$.

Lemma 5. *Starting with an arbitrary triple n, p, q of natural numbers, and using a finite number of δ-transformations, we can pass to another triple of natural numbers at least two of which are equal.*

Proof. Let γ be the greatest natural number such that at least one of the numbers $n+p$, $n+q$, $p+q$ is divisible by 2^γ. The proof will be complete if we can show that, in the case where n, p, q are pairwise distinct, the number γ can be increased by one by δ-transformations.

Obviously, $\gamma > 0$. First we show that if the sum of n and p is divisible by 2^γ then by δ-transformations we can replace them by a pair of numbers such that either they are equal or they are both are divisible by 2^γ. Let

$$n + p = 2^\gamma(2s-1), \quad n > p, \quad p = 2^\mu(2q-1), \quad \mu < \gamma.$$

Then after one δ-transformation both resulting numbers will be divisible by $2^{\mu+1}$. Clearly, for this argument we need simultaneously $n \neq p$ and $\mu < \gamma$. It is therefore obvious that after a finite number of steps we will arrive at a pair of numbers that are either equal or both divisible by 2^γ.

On the basis of the preceding argument, we may assume that two of the given three numbers, say n and p, are divisible by 2^γ. Clearly, one of the numbers n and p is divisible by $2^{\gamma+1}$ since otherwise their sum would be divisible by $2^{\gamma+1}$. Without loss of generality, we may assume that the greater of the numbers n and p is divisible by $2^{\gamma+1}$, since in the contrary case this can be easily obtained by doubling the smaller of the numbers n and p sufficiently many times at the expense of the greater. On the basis of the above arguments, we may assume that

$$n > p, \quad n + p = 2^\gamma(2s-1), \quad n = 2^{\gamma+1}k.$$

As to the number q, there are two possible cases:

1) $q > p$: Then, replacing the pair q, p by the pair $2p$, $q-p$ we see that the number $2p$ is divisible by $2^{\gamma+1}$ and therefore the sum $n+2p$ is also divisible by $2^{\gamma+1}$.
2) $q < p$: Then, the δ-transformations

$$(n,p,q) \longrightarrow (n,p-q,2q) \longrightarrow (n-p+q, 2p-2q, 2q)$$

lead to a triple of natural numbers, for two of which, $2p-2q$ and $2q$, the sum is divisible by $2^{\gamma+1}$.

This completes the proof of Lemma 5. □

Now let us complete the proof of Case 5.

The natural numbers m, n, p that occur in the expressions for α and β can be subjected to arbitrary permutations because of Step 2 and the possibility of replacing α by $\overline{\alpha}$. Step 3 allows us to perform δ-transformations on them. Because of Lemma 5, we can obtain after a finite number of steps the equality of two of these natural numbers. The proof can be completed by Step 1. Case 5 is finished.

The cases considered above together with the cases that can be obtained from them by interchanging a and b or by replacing α by $\overline{\alpha}$ justify the basis of inductive hypothesis 3). This completes the proof of the Main Lemma.

5. The operation $ab + ba$

In the preceding sections, we assumed everywhere that the associative ring Σ admits division by 2. Suppose that we have an associative algebra $\mathcal{B}$ over Σ such that for some elements a and b in $\mathcal{B}$ there does not exist an element c for which $2c = ab + ba$, but the characteristic of the algebra is not 2. Then in the algebra $\mathcal{B}$ we can introduce the operation $a \circ b = ab + ba$, relative to which the additive group of $\mathcal{B}$ will again be a Jordan algebra over Σ. We show that in this case also the main results of this article are valid.

Lemma 6. *Any associative ring Σ with characteristic different from 2 can be embedded in a ring $\overline{\Sigma}$ that admits unique division by 2.*

Proof. Consider the set $\overline{\Sigma}$ of pairs $(\sigma, 2^k)$ where $\sigma \in \Sigma$, and $k \geq 0$ is an integer. We will consider the pairs $(\sigma_1, 2^{k_1})$ and $(\sigma_2, 2^{k_2})$ to be *equivalent* if $2^{k_2}\sigma_1 = 2^{k_1}\sigma_2$. We define addition and multiplication of the pairs in the familiar way:

$$(\sigma_1, 2^{k_1}) + (\sigma_2, 2^{k_2}) = \left(2^{k_2}\sigma_1 + 2^{k_1}\sigma_2, 2^{k_1+k_2}\right),$$
$$(\sigma_1, 2^{k_1})(\sigma_2, 2^{k_2}) = \left(\sigma_1\sigma_2, 2^{k_1+k_2}\right).$$

Obviously, the ring $\overline{\Sigma}$ satisfies the requirements of Lemma 6. □

Suppose we have a Jordan algebra $\mathcal{M}$ over Σ with a finite or countably infinite set of generators, which is special in the new sense, i.e., there exists an associative algebra $\mathcal{B}$ over Σ whose Jordan algebra $\mathcal{B}^{(+)}_{(2)}$ with respect to the operation $\circ$ contains a subalgebra isomorphic to $\mathcal{M}$. Such algebras will be called *semispecial*.

We introduce a new multiplication $\times$ on $\mathcal{B}$ by the equation $a \times b = 2ab$ for $a, b \in \mathcal{B}$. The additive group of $\mathcal{B}$ relative to the old addition and the new multiplication $\times$ will be an associative algebra $\mathcal{B}^{(\times)}$ over Σ. This algebra can be embedded into the algebra $\overline{\mathcal{B}^{(\times)}}$ over $\overline{\Sigma}$ of pairs $(b, 2^k)$ in the way described for Σ. If the action of the elements of $\overline{\Sigma}$ is defined by $(\sigma, 2^s)(b, 2^k) = (\sigma b, 2^{k+s})$, then the subset of $\overline{\mathcal{B}^{(\times)}}$ consisting of the pairs $(m, 2^t)$, where m belongs to the subset of elements of the additive group of $\mathcal{B}$ that correspond to the elements of $\mathcal{M}$, will obviously be a special Jordan algebra over $\overline{\Sigma}$. By Theorem 1, it can be embedded into a special Jordan algebra over $\overline{\Sigma}$ with two generators.

Each element of the algebra $\overline{\mathcal{B}^{(\times)}}$ under this embedding can be expressed in terms of the generators using only the operation $\times$ without the action of $\overline{\Sigma}$, as can be seen from the remark to Theorem 1. If we now return from the multiplication $\times$ to the multiplication $ab = \frac{1}{2}a \times b$, then relative to this operation, the algebra $\mathcal{M}$ will be embedded into a semispecial Jordan algebra with two generators over $\overline{\Sigma}$, which can also be considered as an algebra over Σ. Clearly, the subalgebra over Σ generated by the two generators will be smaller than the corresponding subalgebra over $\overline{\Sigma}$, but it will still contain the algebra $\mathcal{M}$ as can be easily verified. Thus, we have proved the following theorem:

Theorem 4. *Every semispecial Jordan algebra $\mathcal{M}$ over Σ with a finite or countably infinite number of generators, and without elements of order 2 in the additive group, can be embedded into a semispecial Jordan algebra with two generators over Σ.*

Suppose we have a Jordan algebra $\mathcal{N}$ with two generators over Σ; regarding $\mathcal{N}$ we now assume only that its additive group does not have elements of order 2. Since the construction of Lemma 6 applies in this case, we may assume that the algebra $\mathcal{N}$ is embedded into the algebra $\overline{\mathcal{N}}$ of pairs of the form $(n, 2^k)$ for $n \in \mathcal{N}$ $(k = 0, 1, 2, \ldots)$ which is a Jordan algebra over $\overline{\Sigma}$. By Theorem 3, $\overline{\mathcal{N}}$ is a special Jordan algebra over $\overline{\Sigma}$. If we now introduce a new operation $a * b = \frac{1}{2}ab$ on the corresponding associative algebra $\mathcal{A}$ over $\overline{\Sigma}$, then it is obvious that with respect to the algebra $\mathcal{A}^{(*)}$ the Jordan algebra $\overline{\mathcal{N}}$ will be a semispecial Jordan algebra over $\overline{\Sigma}$. If we regard the algebra $\mathcal{A}^{(*)}$ as an algebra over Σ, then the subalgebra $\mathcal{N}$ (over Σ) of the algebra $\left(\mathcal{A}^{(*)}\right)^{(+)}_{(2)}$ will be semispecial. Thus, we have proved the following theorem:

Theorem 5. *Every Jordan algebra $\mathcal{N}$ over Σ with two generators and without elements of order 2 in the additive group is semispecial.*

References

[1] A.A. Albert, *A note on the exceptional Jordan algebra*, Proc. Nat. Acad. Sci. U.S.A. 36 (1950) 372–374.

[2] P.M. Cohn, *On homomorphic images of special Jordan algebras*, Canadian J. Math. 6 (1954) 253–264.

[3] A.I. Malcev, *On a representation of nonassociative rings*, Uspekhi Mat. Nauk N.S. 7 (1952) 181–185.

Some Theorems on Embedding of Rings

A.I. Shirshov

1. Introduction

The present work is a sequel to the author's article [4]. The main topic is special Jordan algebras over rings, but the methods employed also allow us to obtain new results for other classes of algebras. The main result of the present article concerning special Jordan algebras is a necessary and sufficient condition for speciality (or semispeciality) of a Jordan algebra formulated in terms of the algebra itself (Theorems 8 and 9). Other new theorems deal with the general theory of nonassociative rings (Theorems 2, 3, 4, 5).

2. Some embedding theorems

Suppose we have a commutative[1] associative ring Σ and a set Ω of (nonassociative) multilinear polynomials in the independent variables x, y, z, ... with coefficients in Σ. Then we can speak of Ω-*algebras over* Σ, i.e., algebras over Σ in which the polynomials in Ω vanish identically after substituting elements of the algebra for the variables x, y, z, ... In the usual sense we will speak of free Ω-algebras over Σ. Generally speaking, all algebras considered here will be nonassociative.

Definition 1. Let S_k be the free Ω-algebra over Σ with k generators. A countably infinite subset $\mathcal{N}$ of S_k, which is a free generating set for the subalgebra T it generates in S_k, will be called *distinguished* if any ideal I of T is the intersection of the ideal $\overline{I}$ generated by I in S_k with the subalgebra T.

Definition 2. The smallest natural number k (if it exists) for which S_k contains a distinguished subset will be called the *basis rank*[2] of the set Ω over Σ.

Mat. Sbornik N.S. 40 (82), (1956), no. 1, 65–72.

[1]The word "commutative" is omitted in the Russian. [Translators]
[2]Literally, the "dimension". [Translators]

Theorem 1. *If a set of identical relations Ω has basis rank k over the ring Σ, then any Ω-algebra R over Σ that has a finite or countably infinite set of generators can be isomorphically embedded into some Ω-algebra with k generators.*

Proof. Suppose that we have a distinguished subset $\mathcal{N}$ in the free Ω-algebra S_k, and as before let T be the Ω-subalgebra generated by $\mathcal{N}$ in S_k. Then the algebra R is isomorphic to the quotient of T by some ideal I. The ideal I generates in S_k an ideal $\overline{I}$ such that $I = \overline{I} \cap T$. Therefore the quotient algebra $S_k/\overline{I}$ contains a subalgebra isomorphic to T/I and hence to R. □

Theorem 2. *If some set Ω of identical relations has basis rank k over Σ, then any Ω-algebra K over Σ can be isomorphically embedded into an Ω-algebra N over Σ each of whose countable subsets is contained in a subalgebra generated by k elements.*

Proof. We will assume that the collection $\{B_\alpha\}$ of countably infinite subsets of K is well-ordered by the index variable α which ranges over some well-ordered set. Suppose we have already constructed an Ω-algebra K_α over Σ that is an extension of the algebra K such that each subset B_β, $\beta < \alpha$, is already contained in a subalgebra generated by k elements. If B_α itself lies in a subalgebra with k generators then we set $K_{\alpha+1} = K_\alpha$. Now suppose that B_α does not lie in any subalgebra of K_α with k generators. We extend the set B_α to some set Λ_α of generators of K_α. Consider the free Ω-algebra Q_α over Σ with the set of generators Λ'_α of the same cardinality as Λ_α. Then we arbitrarily select k elements a_1, a_2, $\ldots$, a_k in the set Λ'_α, and a distinguished set T_α in the free Ω-algebra $Q_{\alpha k}$ over Σ that is generated in the algebra Q_α by the elements a_i $(i = 1, 2, \ldots, k)$. Select a countably infinite subset $t_1^\alpha, \ldots, t_r^\alpha, \ldots$ of the set T_α that has a countably infinite complement in T_α. Clearly, the subalgebra $\overline{K}_\alpha$ generated in Q_α by the set

$$\overline{\Lambda}_\alpha = \{t_s^\alpha \mid s = 1, 2, \ldots\} \cup \big(\Lambda'_\alpha \setminus \{a_i \mid i = 1, \ldots, k\}\big),$$

is a free Ω-algebra, since from any relation which is non-trivial (i.e., not a consequence of Ω) we could obtain a non-trivial relation for the elements of the set T_α by replacing the generators from $\overline{\Lambda}_\alpha$ that are not in T_α by arbitrary elements of T_α. From this it follows that the algebra K_α is isomorphic to the quotient algebra of $\overline{K}_\alpha$ by some ideal I_α, where I_α can be chosen such that the images of the elements t_i^α $(i = 1, 2, \ldots, r, \ldots)$ correspond to the elements of B_α. The ideal I_α generates in Q_α some ideal $\overline{I}_\alpha$. We will prove that $\overline{I}_\alpha \cap \overline{K}_\alpha = I_\alpha$.

Let d be an arbitrary element of this intersection. Since $d \in I_\alpha$, it can be written as a (nonassociative) polynomial each of whose terms contains a factor from I_α; and since $d \in K_\alpha$, it can be written as a polynomial in elements of $\overline{\Lambda}_\alpha$. Comparing these two expressions, we obtain an equation in the free Ω-algebra Q_α over Σ, which obviously will still be valid if the free generators from the set $\Lambda'_\alpha \setminus \{a_i \mid i = 1, \ldots, k\}$ which occur in it are replaced by (distinct) elements of the set $T_\alpha \setminus \{t_s^\alpha \mid s = 1, 2, \ldots\}$. Let $\overline{I}_\alpha^0$ be the ideal of $Q_{\alpha k}$ generated by the finite set of elements obtained as a result of this replacement of the elements I_α that occur

in the expression for d, and let I_α^0 be the ideal generated by the same elements in the subalgebra generated by T_α. From the fact that T_α is a distinguished set, it follows that, after this replacement, the element d becomes an element of the ideal I_α^0. Using the fact that T_α is a set of free generators for the subalgebra it generates, we can perform the reverse replacement which gives us an expression for d as an element of I_α.

From the claim just proved it follows that the quotient algebra $Q_\alpha/\overline{I}_\alpha$ contains a subalgebra isomorphic to the algebra K_α, and under the natural embedding the set B_α is contained in a subring generated by k elements, namely the images of the elements of the set $\{a_i \mid i = 1, \ldots, k\}$. We extend the algebra K_α to the algebra isomorphic to $Q_\alpha/\overline{I}_\alpha$ and denote the extended algebra by $K_{\alpha+1}$.

If γ is a limit ordinal then by K_γ we denote the union of the increasing chain of algebras $\bigcup_{\delta<\gamma} K_\delta$.

By an obvious transfinite induction, it follows that the algebra K can be extended to an Ω-algebra K' over Σ such that every countably infinite subset of K is contained in a subalgebra of K' generated by k elements. Analogously, the algebra K' can be extended to K'' and so on. The union $N = \bigcup K^{(\gamma)}$ of this increasing chain of algebras will obviously satisfy the conditions of the theorem if γ ranges over all ordinals of the first two classes. This completes the proof. □

We now consider applications of Theorem 2 to some particular cases.

1) The set Ω is empty and Σ is an arbitrary ring.

Lemma 1. *The set* $T = \{aa^2, a^2a^2, (a^2a)a^2, [(a^2a)a]a^2, \ldots\}$ *is a distinguished subset of the free algebra* S *over* Σ *on one generator* a.

Proof. Let S_0 be the subring of S generated by T, let I_0 be an ideal of S_0, and let I be the ideal of S generated by I_0. If q is an element of the intersection $S_0 \cap I$, then q can be written as a polynomial, each of whose terms q_i is a product of an element of I_0 and some monomials in S. If at least one of the latter monomials does not belong to S_0, then from the definition of T it follows that none of the monomials obtained by expanding q_i belongs to S_0. Since $q \in S_0$, all such q_i must cancel each other, and thus $q \in I_0$. This completes the proof. □

2) The set Ω consists of the relation $xy - yx = 0$, and Σ is an arbitrary ring.

Lemma 2. *The set* $T_C = \{a^2a^2, (a^2a)a^2, [(a^2a)a]a^2, \ldots\}$ *is a distinguished subset of the free commutative algebra* S_C *over* Σ *on one generator* a.

Proof. From [3] it follows that the elements of S_C are linear combinations with coefficients from Σ of the so-called C-regular words. Taking this into account, we can complete the proof similarly to the proof of Lemma 1. □

3) The set Ω consists of the relation $xy + yx = 0$, and Σ is an arbitrary ring.

Lemma 3. *The set* $T_{AC} = \{[(ab)b](ab), \{[(ab)b]b\}(ab), \ldots\}$ *is a distinguished subset of the free anticommutative algebra* S_{AC} *over* Σ *on two generators* a *and* b.

The proof is similar, using the results of [3]. Obviously, in the general case the basis rank here is 2, but in the case when all elements of Σ have additive order 2 we will obtain a commutative algebra and thus the basis rank will be 1.

4) The set Ω consists of the relation $(xy)z - x(yz) = 0$, and Σ is an arbitrary ring.

Lemma 4. *The set $T_A = \{bab, ba^2b, ba^3b, \ldots\}$ is a distinguished subset of the free associative algebra S_A over Σ on two generators a and b.*

See the proof of this lemma in [4].

Theorem 2 and Lemmas 1–4 imply the following Theorems:

Theorem 3. *Every algebra over Σ can be embedded into an algebra over Σ in which every countably infinite subset is contained in a subalgebra generated by one element.*

This theorem generalizes a result of A.I. Zhukov [5].

Theorem 4. *Every commutative (resp. anticommutative) algebra over Σ can be embedded into a commutative (resp. anticommutative) algebra over Σ in which every countably infinite subset is contained in a subalgebra generated by one element (resp. by two elements).*

Theorem 5. *Every associative algebra over Σ can be embedded into an associative algebra over Σ in which every countably infinite subset is contained in a subalgebra generated by two elements.*

Theorem 5 generalizes a result of A.I. Malcev [2].

3. Applications to special Jordan algebras

Special Jordan rings cannot be immediately included into the scheme explained in Section 1 because there does not exist a set of identical relations defining this class of algebras (see [1], [4]). Suppose we have some algebra J over Σ. In the case when J is generated by a finite or countably infinite set is considered in [4], where it is shown that J can be embedded into a Jordan algebra with two generators. First we will assume that Σ admits division by 2.

Theorem 6. *Any special Jordan algebra J over Σ can be isomorphically embedded into a special Jordan algebra $\overline{J}$ each of whose countable subsets is contained in a subalgebra generated by two elements.*

Proof. Since the algebra J is special, it can be represented isomorphically in some associative algebra K over Σ. By Theorem 5, the algebra K is embeddable in an associative algebra N over Σ, each of whose countable subsets is contained in a subalgebra generated by two elements. Since the set T_A of Lemma 4 consists of the Jordan polynomials $t_s = ba^sb = 2b \circ (b \circ a^s) - a^s \circ b^2$, it is clear that, upon extending the algebra K, each countably infinite subset B_α that appears in the

proof of Theorem 2 will be contained in a special Jordan subalgebra generated by two elements, namely the images of the elements a and b. Obviously, we will also have to carry out this construction for the countably infinite subsets B_α that are contained in a subalgebra generated by two elements but do not consist of Jordan polynomials in these two elements. It follows that each countably infinite subset of the algebra N will be contained in a special Jordan subalgebra generated by two elements. To the associative algebra N there corresponds the special Jordan algebra $N^{(+)}$. This completes the proof. □

A question arises regarding the validity of the converse to Theorem 6: Is a Jordan algebra special if each of its countable subsets is contained in a subalgebra with two generators, that is, in a special Jordan algebra [4]? A positive answer to this question will be given in a somewhat more general form.

We will call a Jordan algebra *locally special* if each of its finitely generated subalgebras is special.

Theorem 7. *Any locally special Jordan algebra J is special.*

Proof. By $\overline{J}$ we will denote a set of elements that is in one-to-one correspondence with the algebra J. Consider the free associative algebra $\mathcal{A}$ over Σ with the set $\overline{J}$ of free generators, and its ideal $\overline{I}_1$ generated by all elements of the form[3]

$$\alpha_i = \overline{a}_{1i} + \overline{b}_{1i} - \overline{c}_{1i}, \qquad \beta_j = \frac{1}{2}\left(\overline{a}_{2j}\overline{b}_{2j} + \overline{b}_{2j}\overline{a}_{2j}\right) - \overline{c}_{2j}, \qquad \gamma_k = \sigma_k \overline{a}_{3k} - \overline{c}_{3k},$$

whenever the following equations hold in the algebra J:

$$a_{1i} + b_{1i} = c_{1i}, \qquad a_{2j} \circ b_{2j} = c_{2j}, \qquad \sigma_k a_{3k} = c_{3k}.$$

We will prove that the Jordan algebra J is isomorphically represented in the quotient algebra $\mathcal{A}/\overline{I}_1$. For this it suffices to show that $\overline{I}_1 \cap \overline{J}$ equals zero. Assume to the contrary that we have the following relation:

$$\sum_i d_i \alpha_i s_i + \sum_j r_j \beta_j t_j + \sum_k n_k \gamma_k m_k = q, \tag{1}$$

where $q \in \overline{J}$ and d, s, r, t, n, m may be absent[4]. Since (1) is a relation among the generators of a free associative algebra over Σ, it must hold in any associative algebra over Σ for arbitrary elements in one-to-one correspondence with the elements under consideration. However, to the finite set $\overline{T}$ of elements of $\overline{J}$ that occur in relation (1), there corresponds a finite set of elements T in J. By local speciality of J, there exists an associative algebra $\mathcal{A}_1$ that represents the subalgebra of J generated by the finite set T. For the elements of the set T in $\mathcal{A}_1$, the relation (1) must hold, but obviously the left-hand side of (1) vanishes in $\mathcal{A}_1$, which gives a contradiction. □

The results of Theorems 6 and 7 can be formulated as follows:

[3]It is implicit that $\sigma_k \in \Sigma$. [Translators]
[4]It is implicit that $q \neq 0$. [Translators]

Theorem 8. *If the ring Σ admits unique division by 2, then a Jordan algebra J over Σ is special if and only if it is isomorphically embeddable in a Jordan algebra each of whose countable subsets is contained in a subalgebra generated by two elements.*

If we restrict ourselves to the assumption that the additive group of the algebra J has no elements of order 2, then we can consider semispecial Jordan algebras (see [4]).

Theorem 9. *If the additive group of the Jordan algebra J has no elements of order 2, then J is semispecial if and only if J is isomorphically embeddable in a Jordan algebra each of whose countable subsets is contained in a subalgebra generated by two elements.*

Proof. From semispeciality of J it follows that there exists an associative algebra K_1 in which the algebra J is isomorphically represented by the operation $a \circ b = ab + ba$. We may assume that the additive group of the algebra K_1 does not have elements of order 2, since the collection of elements of order 2^s in the additive group of a ring is an ideal for which the corresponding quotient ring does not contain elements a satisfying $2^s a = 0$ for some natural number s. The intersection of this ideal with the set that corresponds in K_1 to the algebra J will be zero. The algebra K_1 can be extended to an algebra K with unique division by 2 ([4], Lemma 6). At the same time, the base ring Σ will be extended to $\overline{\Sigma}$ with unique division by 2.

We introduce in K a new associative operation $a \times b = 2ab$. Then the special algebra $K^{(+)}$ considered relative to the operation $a \cdot b = \frac{1}{2}(a \times b + b \times a)$ can be embedded into a Jordan algebra N over $\overline{\Sigma}$, each of whose countable subsets is contained in a subalgebra generated by two elements. Returning to the original operation $ab = \frac{1}{2}(a \times b)$, we convince ourselves that the algebra J is embedded in the desired way, since an algebra over $\overline{\Sigma}$ is also an algebra over Σ.

Conversely, suppose that J is embedded into a corresponding algebra N. Then in N ([4], Theorem 5) each finite subset is contained in a semispecial algebra. The proof can be completed by repeating the proof of Theorem 7 but replacing β_j by $\beta'_j = \overline{a}_{2j}\overline{b}_{2j} + \overline{b}_{2j}\overline{a}_{2j} - \overline{c}_{2j}$. □

4. Algebras of finite dimension

In this section we consider a refinement of the previous results for algebras of finite dimension.

Let $\mathcal{A}$ be an associative algebra of finite dimension over some field F. Obviously, $\mathcal{A}$ has a finite system of generators $\{c_i\}$ $(i = 1, 2, \ldots, m)$. Consider the free associative algebra $\mathcal{B}$ with two generators a and b over F. The subalgebra $\mathcal{B}'$ generated in $\mathcal{B}$ by the elements $c'_i = ba^i b$ $(i = 1, 2, \ldots, m, \ldots)$ is a free associative algebra with a countably infinite set of generators. Let I' be the kernel of the homomorphism of $\mathcal{B}'$ onto $\mathcal{A}$, and let I be the ideal generated by I' in $\mathcal{B}$. We may

assume[5] that $c'_{m+i} \in I'$ $(i = 1, 2, \ldots)$. Further, let I_1 be the ideal of $\mathcal{B}$ generated by the elements of the form aba, b^k, a^{m+k-2} $(k = 3, 4, \ldots)$. We will prove the equality

$$(I + I_1) \cap \mathcal{B}' = I'.$$

Suppose that the element $i + i_1$ in the sum of ideals $I + I_1$ is an element of $\mathcal{B}'$. From the obvious relation $I_1 \cap \mathcal{B}' \subseteq I$ it follows that $i_1 \in I$, and thus $i + i_1 \in I$. The proof can be completed using the equality $I \cap \mathcal{B}' = I'$, which is proved in the work [4]. The quotient algebra $\overline{\mathcal{B}} = \mathcal{B}/(I + I')$ therefore contains a subalgebra isomorphic to $\mathcal{A}$, and is clearly an algebra with two generators. In addition to the cosets corresponding to the elements of $\mathcal{A}$, the algebra $\overline{\mathcal{B}}$ contains only a finite number of linearly independent cosets, and thus is an algebra of finite dimension. Thus, we have proved the following result:

Theorem 10. *Any associative algebra $\mathcal{A}$ of finite dimension over a field F is isomorphic to a subalgebra of an associative algebra $\mathcal{B}$ with two generators and finite dimension over F.*

Now consider a special Jordan algebra J of finite dimension with basis a_1, a_2, …, a_n. Let A be an associative algebra in which J is represented. It is easy to show that the subalgebra of A generated by the elements $a_1, a_2, \ldots, a_n$ has finite dimension. Indeed, any product of elements a_i that contains more than n factors can be represented as a linear combination of such products with a smaller number of factors. This follows from the equation $a_i \circ a_j = \frac{1}{2}(a_i a_j + a_j a_i) = \sum c_{ij}^k a_k$, because in the product under consideration there will be at least two equal factors, which by a sequence of transpositions can be moved next to each other, and then it will become possible to decrease the number of factors. From this, using the proof of Theorem 10, the next result follows.

Theorem 11. *Any special Jordan algebra J of finite dimension over the field F of characteristic $\neq 2$ is isomorphic to a subalgebra of a special Jordan algebra $\overline{J}$ with two generators and finite dimension over F.*

Remark 1. Special Jordan algebras over fields of characteristic 2 are Lie algebras. It is known that a Lie algebra of finite dimension can be represented in an associative algebra of finite dimension; the question of the number of generators has not been considered for this case.

Remark 2. Without changing the methods, it is easy to obtain analogues of Theorems 10 and 11 for finite algebras, or algebras of finite rank over some ring of coefficients.

References

[1] P.M. Cohn, *On homomorphic images of special Jordan algebras*, Canadian J. Math. 6 (1954) 253–264.

[5] It is also implicit that c'_i maps to c_i for $i = 1, \ldots, m$. [Translators]

[2] A.I. Malcev, *On a representation of nonassociative rings*, Uspekhi Mat. Nauk N.S. 7 (1952) 181–185.

[3] A.I. Shirshov, *Subalgebras of free commutative and free anticommutative algebras*, Mat. Sbornik 34 (1954) 81–88.

[4] A.I. Shirshov, *On special J-rings*, Mat. Sbornik 38 (1956) 149–166.

[5] A.I. Zhukov, *Reduced systems of defining relations for nonassociative algebras*, Mat. Sbornik 27 (1950) 267–280.

On some Nonassociative Nil-rings and Algebraic Algebras

A.I. Shirshov

1. Introduction

In the works of Levitzki [5] and Jacobson [3] devoted to the solution of the problem of Kurosh [4], it is proved that any associative algebraic algebra of bounded degree is locally finite, and that every associative nil-ring of bounded index is locally nilpotent. The problem of Kurosh can be stated for any class of power associative algebras [1], but already Lie algebras give an example showing that the problem does not have a positive solution for arbitrary power associative algebras.

In the present paper, a positive solution is given for the analogous problem (also in the bounded case) for special Jordan algebras and for alternative algebras, under a natural restriction on the characteristic of the base field (Theorems 4 and 8). For nil rings, results generalizing the theorem of Levitzki in the associative case are also obtained (Theorems 2 and 7).

2. Preliminary results

Consider the associative words formed from the elements of some finite ordered set of symbols:

$$R = \{a_i\}\ (i = 1, 2, \ldots, k), \qquad a_i > a_j \ \text{ if } \ i > j.$$

Definition 1. A word of the form[1] $\alpha = a_k \cdots a_k a_{i_1} a_{i_2} \cdots a_{i_s}$ where $i_t \neq k$ $(t = 1, 2, \ldots, s)$, $s \geq 1$ will be called a_k-*irreducible*.

Definition 2. A representation of the word β (if possible) as the product of a number of a_k-irreducible words will be called an a_k-*factorization* of the word β.

Mat. Sbornik N.S. 41 (83), (1957), no. 3, 381–394.

[1]It is implicit that a_k occurs at least once. [Translators]

It is easy to see that for a word β there exists an a_k-factorization, which is moreover unique, if and only if β starts with the symbol a_k and ends with a symbol different from a_k. The following is an example of an a_3-factorization of a word on three symbols:

$$(a_3a_3a_2a_1a_1a_2a_1)(a_3a_1)(a_3a_3a_3a_1a_1a_2)(a_3a_1a_2).$$

On the set of all associative words in the elements of the set R, we introduce a partial order: for words α and β of the same length we declare $\alpha > \beta$ if this relation holds in the lexicographical sense. We order lexicographically the set T of all a_k-irreducible words; when the word α is the beginning of the word β (i.e., $\beta = \alpha a_{i_1}a_{i_2}\cdots a_{i_m}$, $i_t \neq k$, $t = 1, 2, \ldots, m$) we declare $\alpha > \beta$.

Definition 3. The associative word γ will be called *n-decomposable* if it can be represented as the product of n subwords in such a way that, for any non-identity permutation of these subwords, the resulting associative word is strictly less than γ.

For example, the word $a_3a_1a_2a_2a_1a_1a_2a_1a_1a_1$ is 3-decomposable and admits several 3-decompositions:

$$(a_3a_1)(a_2a_2a_1a_1)(a_2a_1a_1a_1), \qquad (a_3a_1a_2)(a_2a_1a_1)(a_2a_1a_1a_1),$$
$$(a_3)(a_1a_2a_2a_1a_1a_2)(a_1a_1a_1), \qquad \text{etc.};$$

the word $a_1a_2a_1a_3a_2a_1a_2a_3a_2$ is not 2-decomposable.

The words that admit a_k-factorization can be considered as words formed from the elements of the set T. In this case also, it makes sense to consider n-decomposable words. In the rest of the paper, where it could lead to confusion, we will speak about n_R-decomposable or n_T-decomposable words, specifying which set of symbols is to be regarded as generators.

When we consider words formed from elements of the set T, we will call them *T-words* (as opposed to *R-words*); analogously, we will use the terms *T-length* and *R-length*.

Lemma 1. *For any associative T-word α, n_T-decomposability implies n_R-decomposability.*

Proof. Let $\alpha = \alpha_1\alpha_2\cdots\alpha_n$ be an n_T-decomposition of α; then α, α_1, …, α_n admit an a_k-factorization. From Definition 3 it follows that $\alpha > \alpha_{i_1}\alpha_{i_2}\cdots\alpha_{i_n}$ in the sense of the set T whenever $(i_1, i_2, \ldots, i_n)$ is a non-identity permutation of the symbols $1, 2, \ldots, n$. It is easy to see that this relation also holds in the sense of the set R. Therefore, this n_T-decomposition is also an n_R-decomposition. The lemma has been proved. □

Lemma 2. *If the word α is $(n-1)_T$-decomposable, then the word αa_k is n_R-decomposable.*

Proof. Lemma 1 implies the existence of the following $(n-1)_R$-decomposition of the word α:

$$\alpha = (a_k a_{i_1}\cdots a'_{i_1})(a_k a_{i_2}\cdots a'_{i_2})\cdots(a_k a_{i_{n-1}}\cdots a'_{i_{n-1}}),$$

where $a, a' \in R$, $a'_{i_t} \neq a_k$ $(t = 1, 2, \ldots, n-1)$. We will prove that for the word αa_k we have the following n_R-decomposition:

$$\alpha a_k = (a_k)(a_{i_1} \cdots a'_{i_1} a_k)(a_{i_2} \cdots a'_{i_2} a_k) \cdots (a_{i_{n-1}} \cdots a'_{i_{n-1}} a_k).$$

Indeed, any permutation of the factors of αa_k that fixes the first factor a_k, transforms αa_k into $\alpha' a_k$ where α' is obtained by some permutation of the factors in the given $(n-1)_T$-decomposition of α. Therefore, $\alpha > \alpha'$ and $\alpha a_k > \alpha' a_k$. Now, if we consider permutations that move the symbol a_k from the first position, then it is obvious that the result of applying such a permutation to αa_k will start with a strictly smaller number of symbols a_k as compared to αa_k. Thus, it will be strictly less than αa_k. The lemma has been proved. □

Lemma 3. *For any three natural numbers k, s, n there exists a natural number $N(k, s, n)$ such that in any associative word of length $N(k, s, n)$ in k ordered symbols there exists either a subword repeated s times consecutively or an n-decomposable subword (or both).*

Proof. It is easy to see that the natural numbers $N(k, s, 1)$ and $N(1, s, n)$ satisfying the conditions of the lemma exist for any k, s, n. Suppose we are given some natural numbers k and n. We make the inductive assumption that there exist natural numbers $N(k-1, s, n)$ and $N(k, s, n-1)$ satisfying the conditions of the lemma for all natural numbers k and s.

Consider an arbitrary associative word α of length

$$[s + N(k-1, s, n)] \left[N\left(k^{N(k-1,s,n)+s}, s, n-1\right) + 1 \right],$$

in elements of our familiar set R. If, at the beginning of α there is a number of the symbols a_i other than a_k, and their number is not less than $N(k-1, s, n)$, then we can apply the inductive hypothesis to the subword α' that is at the beginning of the word α and depends only on $k-1$ symbols. Therefore, we may assume that the length of the word α' (if it exists) is less than $N(k-1, s, n)$. At the end of the word α there may be a subword $\alpha'' = a_k a_k \cdots a_k$. We may suppose that if α'' exists then its length is less than s, for in the contrary case the conclusion of the lemma would hold. Removing the words α' and α'' (if they exist) we obtain a subword α_1 whose length is greater than

$$[s + N(k-1, s, n)] N\left(k^{N(k-1,s,n)+s}, s, n-1\right).$$

Having performed a_k-factorization of the word α_1, we may assume in addition that the length of each a_k-irreducible word that occurs in this a_k-factorization is less than the number $s + N(k-1, s, n)$, for in the contrary case such a word would contain either s consecutive symbols a_k or a subword of length $N(k-1, s, n)$ not containing the symbol a_k. It is easy to see that there exist no more than $k^{N(k-1,s,n)+s}$ distinct a_k-irreducible words with the above-mentioned restriction on length. We will regard the word α_1 as a T-word. Since its T-length is strictly greater than $N(k^{N(k-1,s,n)+s}, s, n-1)$, in α_1 there exists either a subword repeated s times consecutively or an $(n-1)_T$-decomposable subword β.

If this second alternative holds, then by the strict inequality for the length of α_1 we may assume that the subword β is immediately followed by the symbol a_k. By Lemma 2 the subword βa_k is n_R-decomposable. In this case, as well as obviously in the case when the first alternative holds, the conclusion of the lemma is true. Therefore we set

$$N(k,s,n) = [s + N(k-1,s,n)]\left[N\left(k^{N(k-1,s,n)+s}, s, n-1\right) + 1\right].$$

This completes the proof of Lemma 3. □

Definition 4. An element b of the free associative ring $\mathcal{A}$ with the set R of generators will be called a *Jordan polynomial* if there exists a natural number t such that the element $2^t b$ can be represented as a polynomial in the elements of R with respect to addition and the Jordan multiplication $a \circ b = ab + ba$.

For example, the element $a_1a_2a_1$ is a Jordan polynomial in the sense of Definition 4, because $2^2 a_1a_2a_1 = 2a_1 \circ (a_1 \circ a_2) - (a_1 \circ a_1) \circ a_2$.

Definition 5. An associative word α in the elements of R will be called *special* if there exists a homogeneous Jordan polynomial b_α such that the highest word of b_α is α, and this occurs in b_α with coefficient of the form 2^t $(t = 0, 1, \ldots)$.

Lemma 4. *Every T-word α is special (relative to the set R).*

Proof. If the T-length of α equals 1, i.e.,

$$\alpha = a_k a_k \cdots a_k a_{i_1} a_{i_2} \cdots a_{i_m} \ (i_r \neq k; r = 1, 2, \ldots, m),$$

then $b_\alpha = [\cdots[\cdots(a_k \circ a_k) \circ \cdots \circ a_k] \circ a_{i_1}] \circ \cdots a_{i_m}$.

Suppose the statement of the lemma has been proved for T-words whose T-length is strictly less than the T-length of α (which is greater than 1). Then,

$$\alpha = \beta a_k a_k \cdots a_k a_{i_1} a_{i_2} \cdots a_{i_m} \ (i_r \neq k; r = 1, 2, \ldots, m),$$

where β is a T-word to which the inductive hypothesis applies. Let b_β be a Jordan polynomial that corresponds to β. Then a simple calculation shows that we may take as b_α the Jordan polynomial

$$\begin{aligned}
&[\cdots[[b_\beta \circ [[\cdots(a_k \circ a_k) \circ \cdots \circ a_k] \circ a_{i_1}]] \circ a_{i_2}] \cdots] \circ a_{i_m} \\
+\ &[\cdots[[[b_\beta \circ [\cdots(a_k \circ a_k) \circ \cdots \circ a_k]] \circ a_{i_1}] \circ a_{i_2}] \cdots] \circ a_{i_m} \\
-\ &[\cdots[[(b_\beta \circ a_{i_1}) \circ [\cdots(a_k \circ a_k) \circ \cdots \circ a_k]] \circ a_{i_2}] \cdots] \circ a_{i_m}.
\end{aligned}$$

The lemma has been proved. □

Consider an arbitrary algebra K which will in general be nonassociative. Let Γ be a subsemigroup of the additive group of K, and suppose that the elements of Γ satisfy the following homogeneous identical relation (in K):

$$f(\gamma_1^{p_1}, \gamma_2^{p_2}, \ldots, \gamma_k^{p_k}) = 0, \text{ for all } \gamma_i \in \Gamma.$$

Here, $f(x_1^{p_1}, x_2^{p_2}, \ldots, x_k^{p_k})$ denotes a (nonassociative) homogeneous polynomial in the variables x_i $(i = 1, 2, \ldots, k)$, in each of whose monomials x_i occurs p_i times,

and whose coefficients can be taken to be elements of an arbitrary associative ring[2] Σ.

Definition 6. By the *multilinear polynomial*

$$\overline{f}(x_{11},\dots,x_{1p_1},x_{21},\dots,x_{2p_2},\dots,x_{k1},\dots,x_{kp_k}),$$

corresponding to the polynomial

$$f(x_1^{p_1},x_2^{p_2},\dots,x_k^{p_k}),$$

we mean the polynomial obtained from f by first replacing each variable x_i by one of the variables x_{is} so that in each monomial exactly one x_{is} occurs, and then summing over all permutations of the symbols $x_{i1},x_{i2},\dots,x_{ip_i}$ for all $i=1,2,\dots,k$.

For example, if

$$f(x_1^3,x_2^2)=[(x_1x_2)x_1](x_1x_2),$$

then

$$\begin{aligned}&\overline{f}(x_{11},x_{12},x_{13},x_{21},x_{22})=\\&[(x_{11}x_{21})x_{12}](x_{13}x_{22})+[(x_{11}x_{22})x_{12}](x_{13}x_{21})+[(x_{11}x_{21})x_{13}](x_{12}x_{22})\\&+[(x_{11}x_{22})x_{13}](x_{12}x_{21})+[(x_{12}x_{21})x_{11}](x_{13}x_{22})+[(x_{12}x_{22})x_{11}](x_{13}x_{21})\\&+[(x_{12}x_{21})x_{13}](x_{11}x_{22})+[(x_{12}x_{22})x_{13}](x_{11}x_{21})+[(x_{13}x_{21})x_{11}](x_{12}x_{22})\\&+[(x_{13}x_{22})x_{11}](x_{12}x_{21})+[(x_{13}x_{21})x_{12}](x_{11}x_{22})+[(x_{13}x_{22})x_{12}](x_{11}x_{21}).\end{aligned}$$

Lemma 5. *For arbitrary elements γ_{ij} $(i=1,2,\dots,k;j=1,2,\dots,p_i)$ of the semigroup Γ in K, the following relation holds:*

$$\overline{f}(\gamma_{11},\dots,\gamma_{1p_1},\gamma_{21},\dots,\gamma_{2p_2},\dots,\gamma_{k1},\dots,\gamma_{kp_k})=0.$$

Proof. Suppose that

$$p_1=p_2=\dots=p_{s-1}=1,\ p_s>1.$$

From the properties of the semigroup Γ it follows that the polynomial

$$\begin{aligned}&f\big(x_1,x_2,\dots,x_{s-1},(x_{s1}+x_{s2}+\dots+x_{sp_s})^{p_s},x_{s+1}^{p_{s+1}},\dots,x_k^{p_k}\big)\\&-\sum_{q=1}^{p_s}f\big(x_1,x_2,\dots,x_{s-1},\big[\big(\sum_{j=1}^{p_s}x_{sj}\big)-x_{sq}\big]^{p_s},x_{s+1}^{p_{s+1}},\dots,x_k^{p_k}\big)\\&+\sum_{p_s\ge q_1>q_2\ge 1}f\big(x_1,x_2,\dots,x_{s-1},\big[\big(\sum_{j=1}^{p_s}x_{sj}\big)-x_{sq_1}-x_{sq_2}\big]^{p_s},x_{s+1}^{p_{s+1}},\dots,x_k^{p_k}\big)\\&-\dots+(-1)^{p_s-1}\sum_{t=1}^{p_s}f\big(x_1,x_2,\dots,x_{s-1},x_t^{p_s},x_{s+1}^{p_{s+1}},\dots,x_k^{p_k}\big),\end{aligned}$$

vanishes, if the variables are replaced by arbitrary elements of Γ.

[2]It is implicit that Σ is also commutative. [Translators]

Now a simple calculation performed for each monomial of the polynomial f shows that the polynomial above is linear in each variable x_{si} $(i = 1, 2, \ldots, p_s)$, and can be obtained from f by first replacing each occurrence of the variable x_s in each term by one of the variables x_{si} so that in each monomial of f exactly one x_{si} occurs, and then summing over all permutations of the symbols $x_{s1}, x_{s2}, \ldots, x_{sp_s}$. Performing this construction consecutively for all s from 1 to k, we obtain the desired result. This completes the proof of the lemma. □

Remark. This rather simple statement, in a weaker formulation, has appeared many times already in algebraic papers, but usually it was proved for algebras over a field (see, for example, [6]) with some restrictions on the field.

3. Semispecial Jordan rings and algebras

Consider a semispecial Jordan ring I, i.e., a ring embeddable in some associative ring $A_0(I)$ such that the set of elements corresponding to the elements of I forms a Jordan ring isomorphic to I with respect to addition and the Jordan multiplication $a \circ b = ab + ba$. If, for some element c of I there exists a natural number $n(c)$ such that $c^{n(c)-1} \neq 0$ and $c^{n(c)} = 0$, then we will call c as usual a *nilpotent element of index* $n(c)$.

Definition 7. If all elements of the ring I are nilpotent, and their indices are uniformly bounded, then we will say that I is a *Jordan nil-ring of bounded index.*

Definition 8. An arbitrary ring S is called *nilpotent* if there exists a natural number $N(S)$ such that the product of any $N(S)$ elements of S, with any arrangement of brackets, is equal to zero.

Theorem 1. *Any semispecial Jordan nil-ring of bounded index with finitely many generators, and without elements of order* 2 *in the additive group, is nilpotent.*

Definition 9. The intersection of all subrings of $A_0(I)$ that contain I will be called an *enveloping associative ring* $A(I)$ of the semispecial Jordan ring I.

It is easy to see that the enveloping ring $A(I)$ is the subring generated in $A_0(I)$ by an arbitrary set of generators of I.

The validity of Theorem 1 will follow from Theorem 2, which generalizes a theorem of Levitzki [5] (generally speaking).

Theorem 2. *Any enveloping associative ring $A(I)$, without elements of order 2 in the additive group, of a semispecial Jordan nil-ring I of bounded index with a finite number of generators, is nilpotent.*

Proof. Suppose the ring I has $R = \{a_i\}$ $(i = 1, 2, \ldots, k)$ as a set of generators. We will regard the same set R as a set of generators of $A(I)$. We will carry out the proof of Theorem 2 by induction, assuming its validity in the case when the number of generators of I equals $k - 1$.

Consider an arbitrary R-word α of length $m[N(M,n,n)+2]$ where m is the maximal length of nonzero a_k-irreducible words (here we are using the inductive hypothesis), M is the number of such words, and n is a bound on the indices of the elements of I. Then, in the word α we can find a subword β that is a T-word and has T-length equal to $N(M,n,n)$.

By Lemma 3, in the word β there exists either a subword repeated n times consecutively, or an n-decomposable subword γ. We will consider both possibilities one after the other.

1. $\beta = \beta_1 \underbrace{\gamma\gamma\cdots\gamma}_{n \text{ times}} \beta_2$. By Lemma 4, the word γ is special. Thus, there exists a natural number p such that $2^p\gamma$ is the highest term of a Jordan polynomial b_γ. Since $b_\gamma^n = 0$, the element $2^{np}\beta$ can be written as a linear combination with integral coefficients of words of the same R-length that strictly precede the word β. Therefore $2^{np}\alpha$ can also be expressed in a similar way.

2. $\beta = \beta_1\gamma_1\gamma_2\cdots\gamma_n\beta_2$. The elements of I form a subgroup of the additive subgroup of $A(I)$. By Lemma 5, the relation $x_1^n = 0$ that holds in $A(I)$ for the elements of I, implies the relation $\sum_p x_{i_1}x_{i_2}\cdots x_{i_n} = 0$, where the summation extends over all permutations $(i_1, i_2, \ldots i_n)$ of the symbols $1, 2, \ldots, n$.

By Lemma 4, the elements γ_i are special, and thus, up to a factor of the form 2^s, each element γ_i is the highest term of a Jordan polynomial b_{γ_i}.

Using the definition of n-decomposition, and the defining property of the Jordan polynomials b_{γ_i}, we see that the relation $\sum_p b_{\gamma_{i_1}} b_{\gamma_{i_2}} \cdots b_{\gamma_{i_n}} = 0$ implies that the element $2^s\beta$, for some non-negative integer s, can be expressed as a linear combination with integral coefficients of words preceding β. Therefore, $2^s\alpha$ can also be expressed in a similar way.

Thus, we have arrived at the conclusion that either $\alpha = 0$ or the element $2^s\alpha$ can be expressed as a linear combination with integral coefficients of words that have the same R-length as α but precede α. Since a decreasing sequence of words of the same length must terminate, it follows that for some non-negative integer s_1, we have the equality $2^{s_1}\alpha = 0$; the absence of elements of order 2 in the additive group of $A(I)$ implies that $\alpha = 0$. Theorems 2 and 1 have been proved. □

Without changing the notation, we will now assume that I is a special algebraic Jordan algebra over a field F of characteristic different from 2 and that the degrees of the elements of I are bounded by n. In other words, each element of I is a root of some (associative) polynomial of degree n in one variable x with coefficients from F (compare [4]).

Let $P_t(x_1, x_2, \ldots, x_t) = \sum \pm x_{i_1}x_{i_2}\cdots x_{i_t}$ be the alternating sum of the $n!$ terms that are obtained from the product $x_1x_2\cdots x_t$ by all possible permutations of the factors; the sign of each term depends on the parity (even + or odd −) of the corresponding permutation.

Lemma 6. *For any elements $a, b_1, b_2, \ldots, b_{n-1}$ of the algebra I, the following equation holds in any enveloping associative algebra $A(I)$:*

$$P_{2n-1}(a, a^2, \ldots, a^n, b_1, b_2, \ldots, b_{n-1}) = 0.$$

Proof. It is easy to see that each alternating sum P_t of the above form equals zero if any two of the arguments are equal. On the other hand, by assumption, for each element $a \in I$ there exist elements $\delta_i(a) \in F$ such that

$$a^n = \delta_1(n)a^{n-1} + \delta_2(n)a^{n-2} + \cdots .$$

To complete the proof of Lemma 6, we substitute the above expression for a_n into the left-hand side of the desired equation. □

The equation just proved is not trivial, i.e., it does not hold in all associative algebras. Indeed, the term $ab_1a^2b_2 \cdots a^{n-1}b_{n-1}a^n$, for example, appears only once.

Theorem 3. *Any enveloping associative algebra $A(I)$ of a special algebraic Jordan algebra I of bounded degree over a field F of characteristic $\neq 2$, is locally finite, i.e., each finite subset of its elements generates a subalgebra of finite dimension.*

Proof. Any subalgebra $A_Q(I)$ of $A(I)$, that has a finite number of generators, is contained in a subalgebra $A_R(I)$ whose set of generators $R = \{a_i\}$ $(i = 1, 2, \ldots, k)$ consists of elements of I. We will prove the finiteness of the dimension of $A_R(I)$ by induction on k. Assume that subalgebras generated in $A(I)$ by $k-1$ elements of I have finite dimension. Then, there exists a natural number m such that each word of length $\geq m$ formed from elements of the set $R' = R \setminus \{a_k\}$ can be expressed as a linear combination of words of smaller length. Consider an R-word α of length

$$(m+n)\left[N\left(M, n, \frac{1}{2}(n^2+3n-2)\right)+1\right],$$

where M is the number of distinct a_k-irreducible words that cannot be represented as linear combinations of R-words of smaller R-length, and n is a bound on the degrees of the elements of I. Theorem 3 will be proved if we can show that α can be represented as a linear combination of words of smaller R-length.

If $\alpha = \alpha'\beta\alpha''$ where α' is an R'-word, β is a T-word, and $\alpha'' = a_k a_k \cdots a_k$, then we may assume that the R-lengths of the words α' and α'' are less than (respectively) m and n, because in the contrary case there would be nothing to prove. Then, the R-length of β is greater than

$$(m+n)N\left(M, n, \frac{1}{2}(n^2+3n-2)\right).$$

We may assume that each of the a_k-irreducible words that occur in β cannot be represented as a linear combination of R-words of smaller R-length. Each such word has R-length less than $m+n$. Thus, the T-length of β is greater than

$$N\left(M, n, \frac{1}{2}(n^2+3n-2)\right).$$

By Lemma 3 we can claim that in the word β there exists either a T-subword repeated n times consecutively or a $\frac{1}{2}(n^2+3n-2)$-decomposable T-subword. We will consider separately both possibilities.

1. $\beta = \beta_1\gamma_1\gamma_1\cdots\gamma_1\beta_2$. Using the algebraicity of the Jordan polynomial b_{γ_1} defined analogously to how it was done in the proof of Theorem 2, we obtain an expression of β (and thus also of α) as a linear combination of preceding words (in the sense of lexicographical order) and words of smaller R-length.

2. $\beta = \beta_1\gamma_1\gamma_2\cdots\gamma_{n'}\beta_2$ for $n' = \frac{1}{2}(n^2+3n-2)$. By Lemmas 6 and 5, for the Jordan polynomials $b_{\gamma_{i_s}}$ $(s = 1, 2, \ldots, n')$ we have a non-linear relation of degree $n' = (1+2+\cdots+n)+(n-1)$. From this it follows that the product $b_{\gamma_1}b_{\gamma_2}\cdots b_{\gamma_{n'}}$ can be expressed as a linear combination of products obtained from it by permuting the factors. As in the proof of Theorem 2, we conclude that it is possible to express the word β, and thus also α, as a linear combination of preceding words.

Applying the argument repeatedly to the words produced, we will obtain in the end an expression of α as a linear combination of words of smaller R-length. This completes the proof of the theorem. □

The following result is an obvious consequence of Theorem 3:

Theorem 4. *Any special algebraic Jordan algebra of bounded degree, over a field F of characteristic $\neq 2$, is locally finite.*

Remark 1. The question remains open, whether we can remove the hypotheses of semispeciality and speciality in Theorems 1 and 4. However, from the work of the present author [8] and Theorems 1 and 4, it follows that any two elements generate a nilpotent subring (respectively a subalgebra of finite dimension) in a Jordan nil-ring of bounded index (respectively in an algebraic Jordan algebra of bounded degree) under the same restriction on the additive group of the ring (respectively the characteristic of the base field of the algebra).

Remark 2. The restrictions on the additive group (respectively on the characteristic of the field) are essential, as shown already by the example of the free Lie algebra on two generators over a field of characteristic 2, which is a semispecial Jordan algebra by Birkhoff and Witt (see [2] and [9]) but has infinite dimension.

4. Right alternative and alternative rings and algebras

It is well known that a ring S is called *right alternative* (respectively, *left-alternative*) if for any two elements a and b we have $(ab)b = a(bb)$ (respectively, $b(ba) = (bb)a$). A ring that is simultaneously right and left alternative is called *alternative*. It is known [7] that, under the operation of addition and Jordan multiplication $a \circ b = ab + ba$, the elements of a right alternative ring form a semispecial Jordan ring. Lemma 5 implies the following well-known multilinear relation:

$$(ab)c + (ac)b = a(bc) + a(cb), \tag{1}$$

for all elements a, b and c of a right alternative ring S.

Fixing a set of generators R of the right alternative ring S and assuming that S has no elements of order 2 in its additive group, we transfer Definition 4 to the elements of the right alternative ring. For example, the element $(a_1a_2)a_1$ is a Jordan polynomial since using relation (1) we can easily verify that

$$2^2(a_1a_2)a_1 = 2a_1 \circ (a_2 \circ a_1) - (a_1 \circ a_1) \circ a_2;$$

on the other hand, the element $a_1(a_2a_1)$ is not a Jordan polynomial.

Definition 10. Let $a_{i_1}a_{i_2}\cdots a_{i_s}$ be an associative word in the elements of the set R. Then we set

$$\langle a_{i_1}a_{i_2}\cdots a_{i_s}\rangle = \{\cdots[(a_{i_1}a_{i_2})a_{i_3}]a_{i_4}\cdots\}a_{i_s}.$$

We extend the operation $\langle\ \rangle$ to nonassociative words by ignoring the existing arrangement of parentheses, and then to linear combinations of those words. For example,

$$\langle\,(ab)(cd) + m[n(pq)]\,\rangle = [(ab)c]d + [(mn)p]q.$$

We will indicate by a bar over some subword or element that this subword or element is considered as a generator and is not subjected to change. For example,

$$\langle\,[\,(ab)\,\overline{(cd)}\,]\,(mn)\,\rangle = \{[(ab)(cd)]m\}n = \langle\,\overline{[(ab)(cd)]}\,(mn)\,\rangle,$$

and

$$\langle\,[\,(ab)\,(cd)\,]\,\overline{(mn)}\,\rangle = \{[(ab)c]d\}(mn).$$

If an element q of the free nonassociative ring on the set of generators R lies in the ideal generated by the element of the form $(ab)b - a(bb)$, then obviously $\langle q\rangle = 0$.

Lemma 7. *If m is an element of a right alternative ring S that has no elements of order 2 in the additive group, and d is a Jordan polynomial, then we have the equation:*

$$md = \langle\overline{m}d\rangle.$$

Proof. By the last remark, it suffices to prove the lemma under the assumption that d is a Jordan monomial, i.e., it can be written as the Jordan product of some factors from R.

If d has degree 1, i.e., is an element of R, then there is nothing to prove. Suppose d has degree $n > 1$, and for lower degrees the statement has already been proved. Then $d = d_1 \circ d_2$, where d_1 and d_2 are Jordan monomials to which we can apply the inductive hypothesis. Then

$$\begin{aligned} md &= m(d_1d_2) + m(d_2d_1) = (md_1)d_2 + (md_2)d_1 = \langle\overline{m}d_1\rangle d_2 + \langle\overline{m}d_2\rangle d_1 \\ &= \langle(\overline{m}d_1)d_2\rangle + \langle(\overline{m}d_2)d_1\rangle = \langle\overline{m}(d_1 \circ d_2)\rangle = \langle\overline{m}\,d\rangle. \end{aligned}$$

Here we have used equation (1), the inductive hypothesis, and the linearity of the operation $\langle\ \rangle$. This completes the proof. □

Lemma 7 and the fact proved above that the element $(a_1a_2)a_1$ is a Jordan polynomial, imply under our assumptions the following well-known equation:

$$a[(bc)b] = [(ab)c]b, \tag{2}$$

for all elements a, b and c of S.

Lemma 8. *Under the assumptions of Lemma* 7*, we have* $d = \langle d \rangle$.

Proof. Using the method of the proof of Lemma 7 and the lemma itself, we obtain this series of equations:

$$d = d_1 \circ d_2 = d_1d_2 + d_2d_1 = \langle\, \overline{d_1}\, d_2 \,\rangle + \langle\, \overline{d_2}\, d_1 \,\rangle = \langle d_1d_2 \rangle + \langle d_2d_1 \rangle = \langle d \rangle,$$

which complete the proof. □

Definition 11. A monomial q of the free nonassociative ring with the set of generators $R = \{a_i\}$ $(i = 1, 2, \ldots, k)$ is called an r_1*-word* if $q = \langle q \rangle$. By induction we define an r_i*-word* to be an r_1-word in r_{i-1}-words. For example, the words

$$\{[(a_1a_2)a_3]a_4\}a_5 \quad \text{and} \quad (\{(a_1a_2)[(a_2a_1)a_3]\}a_4)(a_1a_3),$$

are respectively r_1- and r_2-words.

Lemma 9. *Every element* b*, of an alternative ring* C *that has no elements of order* 2 *in its additive group, can be represented as a linear combination with integer coefficients of* r_2*-words in any set* R *of generators of* C.

Proof. Obviously, it suffices to prove the lemma assuming that b is a monomial. For monomials of degree ≤ 3 the statement of the lemma is trivial. Suppose that the lemma has been proved for degrees $< n$, and the degree of the monomial b is n. Using this assumption we have:

$$b = b'b'' = \sum_i b_{2i}(c_{2i}d_{1i}), \text{ where } b_{ji}, c_{ji}, d_{ji} \text{ are } r_j\text{-words.}$$

It now suffices to prove the lemma for monomials of degree n of the form $b_{2i}(c_{2i}d_{1i})$. If the degree of the monomial $c_{2i}d_{1i}$ is less than or equal to 2, then our statement is trivially true. Let us perform a second induction, with the inductive hypothesis that the lemma is valid for monomials of degree n if the degree of the right factor is less than m.

Suppose now that the monomial $b_{2i}(c_{2i}d_{1i})$ has degree n, and that the monomial $c_{2i}d_{1i}$ has degree m where $3 \leq m < n$. First we assume that the monomial d_{1i} has degree 1. We will need these two well-known relations,

$$(ab)c + (ba)c = a(bc) + b(ac), \tag{3}$$

$$(ab)c + (cb)a = a(bc) + c(ba), \tag{4}$$

that hold for any elements a, b, c of an alternative ring. Relation (3) is the analogue of relation (1) and holds in any left alternative ring; relation (4) (flexibility) is an immediate consequence of the relations (1) and (3). Using consecutively relations

(4) and (1) we obtain:

$$b_{2i}(c_{2i}d_{1i}) = -d_{1i}(c_{2i}b_{2i}) + (b_{2i}c_{2i})d_{1i} + (d_{1i}c_{2i})b_{2i}$$
$$= d_{1i}(b_{2i}c_{2i}) - (d_{1i}b_{2i})c_{2i} + (b_{2i}c_{2i})d_{1i}.$$

We can apply the second inductive hypothesis to the monomials $(d_{1i}b_{2i})c_{2i}$ and $(b_{2i}c_{2i})d_{1i}$.

Consider the monomial $d_{1i}(b_{2i}c_{2i})$. Its factor $b_{2i}c_{2i}$ has degree $n-1$, so $b_{2i}c_{2i} = \sum_t \ell_{2t}p_{1t}$. Using consecutively relations (3) and (1), we have

$$d_{1i}(b_{2i}c_{2i}) = \sum_t d_{1i}(\ell_{2t}p_{1t}) = \sum_t [-\ell_{2t}(d_{1i}p_{1t}) + (d_{1i}\ell_{2t})p_{1t} + (\ell_{2t}d_{1i})p_{1t}]$$
$$= \sum_t [\ell_{2t}(p_{1t}d_{1i}) - (\ell_{2t}p_{1t})d_{1i} + (d_{1i}\ell_{2t})p_{1t}].$$

Since the monomial d_{1i} has degree 1, and ℓ_{jt} and p_{jt} are r_j-words, then obviously the inductive hypothesis applies to all the words that we obtain ($p_{1t}d_{1i}$ is an r_1-word, and $(d_{1i}\ell_{2t})p_{1t}$ can be expressed in terms of r_2-words, since when we right-multiply an r_2-word by an r_1-word we obtain an r_2-word by Definition 11).

Thus the lemma has been proved assuming the inductive hypotheses and making the additional assumption on d_{1i}. This provides the basis for a third induction with the hypothesis that the lemma is valid if we assume the second inductive hypothesis when the degree of d_{1i} is less than k. Suppose now that this degree is equal to k for $1 < k < m$.

Keeping the same meaning of the indices, we have

$$b_{2i}(c_{2i}d_{1i}) = b_{2i}[c_{2i}(d'_{1i}a_s)],$$

where the monomial d'_{1i} has degree $k-1$ and $a_s \in R$.

Applying Lemma 5 to relation (2), we obtain the relation

$$a[(b'c)b''] + a[(b''c)b'] = [(ab')c]b'' + [(ab'')c]b', \tag{5}$$

that holds for all elements a, b', b'', c of the ring C. Using consecutively relations (1) and (5) we obtain

$$b_{2i}[c_{2i}(d'_{1i}a_s)] = -b_{2i}[(d'_{1i}a_s)c_{2i}] + \omega_1 = b_{2i}[(c_{2i}a_s)d'_{i1}] + \omega_2 = \omega_3,$$

where the ω_i are linear combinations of monomials to which we can apply the inductive hypothesis. This completes the proof of Lemma 9. □

Definition 12. A ring S with a set of generators R is called *right nilpotent relative to* R if there exists a natural number m such that for any R-monomial d of degree $\geq m$ we have $\langle d \rangle = 0$.

Since any right alternative ring S is a power associative ring, Definition 7 of nil rings can be transferred without any change to right alternative rings.

Theorem 5. *Every right alternative nil-ring S of bounded index without elements of order 2 in the additive group is locally right-nilpotent relative to any set of generators.*

Theorem 5 is a consequence of the following result:

Theorem 6. *If the Jordan polynomials of a right alternative ring S, without elements of order 2 in the additive group and with a set of generators $R = \{a_i\}$ $(i = 1, 2, \ldots, k)$, are nilpotent of uniformly bounded index, then S is right-nilpotent relative to R.*

Proof. Let the number n be a bound on the indices of the Jordan polynomials of the ring S. In the free associative ring A with the set of generators R, we consider the ideal I_1 generated by the n-th powers of all Jordan polynomials. Theorem 2 implies that, for any monomial q of the ring A with degree $\geq m[N(M, n, n) + 2]$, there exists a natural number s_q such that $2^{s_q} q \in I_1$, i.e., $2^{s_q} q = \sum_r \ell_r c_r j_r^n d_r$, where the ℓ_r are integers, the c_r and d_r are monomials which may be absent, and the j_r are Jordan polynomials.

Since the last equation holds in the free associative ring, then in any (nonassociative) ring on the same set of generators, the following relation will be valid:

$$2^{s_q} \langle q \rangle = \sum_r \ell_r \langle c_r j_r^n d_r \rangle.$$

Using Lemma 7 and if necessary Lemma 8, we obtain that in the ring S,

$$2^{s_q} \langle q \rangle = \sum_r \ell_r \langle \langle c_r j_r^n \rangle d_r \rangle = \sum_r \ell_r \langle \langle c_r \rangle \overline{j_r^n} d_r \rangle = 0,$$

since any power of a Jordan polynomial is again a Jordan polynomial. This completes the proof of Theorems 5 and 6. □

Theorem 7. *Any alternative nil-ring S of bounded index, without elements of order 2 in the additive group, is locally nilpotent.*

Proof. Every finite set $R = \{a_i\}$ $(i = 1, 2, \ldots, k)$ in the ring S generates, by Theorem 6, a subring that is right-nilpotent relative to R. The finite set R_1 of nonzero r_1-words in S generates a subring S_1 that is right-nilpotent relative to R_1. From the proof of Lemma 9 it follows that any R-monomial q in the ring S can be written as a linear combination with integer coefficients of r_2-words of the same R-length. If q is an r_2-word of sufficiently large R-length, then from the right-nilpotency of the ring S_1 it follows that $q = 0$. This completes the proof. □

Lemma 10. *In any right alternative algebra S, which is algebraic of bounded degree over a field F of characteristic $\neq 2$ and is generated by a finite set R, there exist only finitely many linearly independent r_1-words (relative to R).*

Proof. For any Jordan polynomial j_s, the following equation holds:

$$f_s(j_s) = j_s^n + \delta_{s1} j_s^{n-1} + \delta_{s2} j_s^{n-2} + \cdots = 0,$$

where $\delta_{si} \in F$.

Consider the free associative algebra A over F with the set R of generators, and the ideal I_1 in A generated by all elements $f_s(j_s)$. From Theorem 3 it follows that the quotient algebra $\overline{A} = A/I_1$ is locally finite.

We will show that the linear dependence in $\overline{A}$ of the images of some words q_i $(i = 1, 2, \ldots, t)$ implies the linear dependence of the r_1-words $\langle q_i \rangle$ in the algebra S. The former linear dependence is equivalent to the following relation in the free associative algebra A:

$$\sum_{i=1}^{t} \mu_i q_i + \sum_s \rho_s c_s f_s(j_s) d_s = 0,$$

where $\mu, \rho \in F$ and c_s, d_s are some monomials. As in the proof of Theorem 6, we obtain that

$$\sum_{i=1}^{t} \mu_i \langle q_i \rangle + \sum_s \rho_s \langle \langle c_s \rangle \, \overline{f_s(j_s)} \, d_s \rangle = 0,$$

from which it follows that $\sum_{i=1}^{t} \mu_i \langle q_i \rangle = 0$ in the algebra A. This completes the proof. □

Theorem 8. *Any algebraic alternative algebra S of bounded degree over a field F of characteristic $\neq 2$ is locally finite.*

The validity of this theorem follows immediately from Lemmas 9 and 10.

References

[1] A.A. Albert, *Power associative rings*, Trans. Amer. Math. Soc. 64 (1948) 552–593.

[2] G. Birkhoff, *Representability of Lie algebras and Lie groups by matrices*, Annals of Math. 38 (1937) 526–632.

[3] N. Jacobson, *Structure theory for algebraic algebras of bounded degree*, Annals of Math. 46 (1945) 695–707.

[4] A.G. Kurosh, *Problems in the theory of rings related to the Burnside problem on periodic groups*, Izv. Akad. Nauk USSR, Ser. Mat. 5 (1941) 233–240.

[5] I. Levitzki, *On a problem of A. Kurosch*, Bull. Amer. Math. Soc. 52 (1946) 1033–1035.

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

[7] R.D. Schafer, *Representations of alternative algebras*, Trans. Amer. Math. Soc. 72 (1952) 1–17.

[8] A.I. Shirshov, *On special J-rings*, Mat. Sbornik 38 (1956) 149–166.

[9] E. Witt, *Treue Darstellung Liescher Ringe*, J. reine und angew. Math. 177 (1937) 152–160.

On Rings with Identical Relations

A.I. Shirshov

1. Introduction

The present work is a sequel to the author's paper [6]. In order to avoid repeating numerous definitions and explaining many notations, which would take up an unjustifiable amount of space, the author will limit himself to frequent references.

The first part of this work (§2) is devoted to associative rings with identical relations. In that section, Theorem 1 is proved, which establishes a local finiteness property for such rings, and consequences of that theorem which follow almost immediately are pointed out, including in particular the theorem of Kaplansky [2] on local finiteness of algebraic algebras with identical relations. In the last section (§3), a certain generalization of Kaplansky's theorem to the case of alternative rings (Theorem 5) is proved.

2. Associative rings with identical relations

First we consider associative algebras that satisfy one or more identical relations. Examples of such algebras are commutative algebras and algebras of finite dimension. These examples demonstrate the breadth of this class of associative algebras, and the importance of obtaining general theorems that hold for arbitrary associative algebras with identical relations.

It is known (see for example [4] and [6]) that one may assume that such an algebra satisfies a multilinear identity. Obviously, such an identity can always be written in the form

$$x_1 x_2 \cdots x_n = \sum_{(i_1,i_2,\ldots,i_n)} \alpha_{i_1 i_2 \cdots i_n} x_{i_1} x_{i_2} \cdots x_{i_n}, \tag{1}$$

Mat. Sbornik N.S. 43 (85), (1957), no. 2, 277–283.

where the summation on the right side is over all permutations $(i_1, i_2, \dots, i_n)$ of the symbols $1, 2, \dots, n$ other than the identity permutation $(1, 2, \dots, n)$, and all the coefficients $\alpha_{i_1 i_2 \dots i_n}$ belong to the base field.

Definition 1. If a word s in some symbols $v_1, v_2, \dots, v_r$ can be written in the form

$$s = v_{i_1}^{m_1} v_{i_2}^{m_2} \cdots v_{i_k}^{m_k} \text{ where } v_{i_\ell} \neq v_{i_{\ell+1}},$$

then the natural number k will be called the *height of the word s relative to the set $\{v_i\}$*.

Obviously, the word $s = v_1 v_1 v_2 v_1 v_1 v_2 v_1 v_1 v_2$, for example, has height 6 relative to the set $\{v_1, v_2\}$, and height 1 relative to the word $v_1 v_1 v_2$.

Definition 2. Let A be an algebra with a finite number of generators $a_1, a_2, \dots, a_\ell$. Suppose that there exists a set $t_1, t_2, \dots, t_k$ of elements which are homogeneous in each a_i such that each word s in the generators a_i is equal in A to some linear combination of words in the elements t_j that have the same content (relative to the set $\{a_i\}$) as the word s and have height (relative to the set $\{t_j\}$) less than or equal to some given number q. In this case, we will say that *the algebra A has bounded height*. If every finite subset of an algebra B generates a subalgebra of bounded height, then we will say that the algebra B has *locally bounded heights*.

Obviously, any commutative algebra has locally bounded heights.

Theorem 1. *Any associative algebra (over a field) which satisfies an identical relation of degree n has locally bounded heights (relative to some set of words whose degrees are less than n, with respect to any set of generators).*

Proof. Suppose the algebra A is generated by $a_1, a_2, \dots, a_k$. According to Lemma 3 of [6], there exists a natural number $N = N(n)$ such that for every word of length N in the generators a_i there exists either an n-decomposable subword [6, Definition 3] or a subword of the form b^{2^n}. First, we will prove that if b has length $m \geq n$ then some subword of the word b^{2^n} is itself n-decomposable; without loss of generality we may assume that the word b cannot be written in the form $\overline{b}^t$ for some $t > 1$. Using cyclic permutations of the generators, we can form m different words from the word b, namely $b = b_0$, b_1, …, b_{m-1}. We can order these words lexicographically: $b_{i_0} > b_{i_1} > \cdots > b_{i_{m-1}}$. Obviously, the word b^{2^n} can be written in the form $b^{2^n} = c b'_{i_0} b'_{i_1} \cdots b'_{i_{m-1}}$, where each of the words b'_i has b_i as an initial subword. Furthermore, it is obvious that the subword $b'_{i_0} b'_{i_1} \cdots b'_{i_{m-1}}$ is m-decomposable, and consequently, it contains an n-decomposable subword. By relation (1), every n-decomposable word can be represented as a linear combination of (lexicographically) smaller words. From this, it follows that every word of length N in the generators a_i is equal to a linear combination of words that have the same content relative to the generators but contain subwords of the form b^{2^n} where b has length $< n$.

The last remark implies that if the height of a word s is sufficiently large, and the word s does not contain n-decomposable subwords, then there exists a

subword s_1 of the form $s_1 = b^n b'$ where the lengths m, m' of the words b, b' satisfy the inequality $n > m \geq m'$ and the word b' is not an initial subword of b. Since the set of possibilities for the words b and b' is finite, it easily follows that there exists a sufficiently large natural number M such that every word $\overline{s}$ of height M relative to some set of words of length $< n$ is a linear combination of words of the same content which are lexicographically not greater than $\overline{s}$ and such that each of these words has n equal subwords of the form $s_1 = b^n b'$ (which are not necessarily consecutive). However, every such word has a subword that is n-decomposable in one of the following ways:

$$\alpha_0(b^n b'\alpha_1 b)(b^{n-1}b'\alpha_2 b^2)(b^{n-2}b'\alpha_3 b^3)\cdots(bb'\alpha_n),$$
$$\alpha_0 b^n(b'\alpha_1 b^{n-1})(bb'\alpha_2 b^{n-2})(b^2 b'\alpha_3 b^{n-3})\cdots(b^{n-1}b'\alpha_n),$$

depending on which of the words b and b' is lexicographically greater. Therefore, each word of height $\geq M$ can be written as a linear combination of words of smaller height. The proof is complete. □

Now we pass to associative algebras over an arbitrary commutative associative coefficient ring Σ.

Definition 3. An identical relation satisfied by an associative algebra over Σ will be called *admissible* if (after combining similar terms) at least one of the coefficients of a term of highest degree is equal to 1.

Theorem 2. *If an associative ring C over Σ satisfies an admissible identical relation of degree n, then the ring C has locally bounded heights (relative to some set of words whose degrees are less than n, with respect to any set of generators).*

Proof. Suppose that the distinguished term of degree n (with coefficient 1) of the identity involves the variables $x_1, x_2, \ldots, x_k$ to degrees $n_1, n_2, \ldots, n_k$ (respectively) with $\sum_{i=1}^{k} n_i = n$. Linearizing this term [6, Lemma 5] consecutively with respect to $x_1, x_2, \ldots, x_k$, we eliminate all the terms in which at least one of the x_i has degree less than n_i. (If $n_i = 1$ then we consider the relation

$$\phi(x_i, x_i') = f(x_i + x_i') - f(x_i') = 0,$$

where f is the left side of the original identity.) Since similar terms cannot appear as a result of this process, the multilinear identity thus obtained will have at least one term with coefficient 1. Performing, if necessary, a permutation of the variables, we obtain an identity of the form (1) which was used in the proof of Theorem 1. The remainder of the proof is a repetition of the proof of Theorem 1. □

We now consider some corollaries of the results already proved.

Theorem 3. *Let A be an associative ring over Σ with an admissible identical relation of degree n. If all products in A of fewer than n generators are nilpotent, then A is locally nilpotent.*

The proof of this theorem is obvious.

Corollary 1. *If all products of degree $\leq n$ of the generators of an associative algebra A of dimension n are nilpotent, then A is nilpotent.*

This statement follows from the known fact that any algebra of dimension n satisfies an identical relation of degree $n+1$: the alternating sum of all $(n+1)!$ distinct products of $n+1$ distinct variables is identically zero.

Definition 4. An element a of an associative ring A will be called *algebraic*[1] *over the subring Z_1 of the center Z of A* if there exist elements $z_i \in Z_1$ and a natural number m such that this equation holds:

$$a^m = \sum_{i=1}^{m-1} z_i a^{m-i}.$$

Definition 5. If the associative ring A has elements $b_1, b_2, \ldots, b_k$ such that for some natural number m every element $c \in A^m$ can be written in the form

$$c = \sum_{i=1}^{k} z_i b_i,$$

where the elements z_i belong to the subring Z_1 of the center Z, then A will be called *finite over Z_1*.

As in the case of algebras of finite dimension, it is obvious that a ring, which is finite over its center, satisfies an admissible identical relation. The following stronger result follows immediately from Theorem 2.

Theorem 4. *Let A be an associative ring with a finite number of generators and an admissible identical relation of degree n. If all products in A of fewer than n generators are algebraic over the subring Z_1 of the center of A, then A is finite over Z_1.*

In the special case where Z_1 is the zero subring, Theorem 4 includes Levitski's theorem [3]; it also contains a more general theorem of Kaplansky [2] (it suffices to adjoin a unit element).

3. Alternative and special Jordan rings with identical relations

In what follows, we will consider alternative rings without elements of order 2 in the additive group, satisfying some identical relation which is not a consequence of associativity.

Definition 6. An identical relation $f(x_1, x_2, \ldots, x_n) = 0$, satisfied by an alternative ring, will be called *essential* if at least one of the coefficients of the highest degree terms of the element $\langle f \rangle$ [6, Definition 9] of the free nonassociative ring in the generators x_i is equal to 1 (after combining similar terms).

[1] The current term is "integral". [Translators]

Definition 7. An identical relation $I = 0$ in a special Jordan ring will be called *admissible* if the relation $F = 0$ is admissible, where F is the associative polynomial obtained by expanding the Jordan polynomial I.

Lemma 1. *If an alternative ring K satisfies an essential identical relation, then the corresponding special Jordan ring K^+ satisfies an admissible identical relation.*

Proof. Let $f(x_1, x_2, \ldots, x_q) = 0$ be the identical relation that holds in K. If we substitute in f the monomial xy^i for x_i then we obtain an essential relation $\phi(x, y) = 0$. If $\overline{\phi}(x, y)$ is the polynomial obtained from ϕ by reversing the order of variables in each monomial, then [5, §3] the ring K satisfies the admissible essential identical relation $\psi(x, y) = \phi(x, y)\overline{\phi}(x, y) = 0$. However, the polynomial $\psi(x, y)$ is a Jordan polynomial, since $\overline{\psi} = \psi$ (see [1, 5]); we have also used the associativity of an alternative ring on two generators. Regarding $\psi(x, y) \equiv I(x, y)$ as a Jordan polynomial, we see that the Jordan polynomial $I(x, y)$ is identically zero in K^+. The proof of the lemma is complete. □

Definition 8. The *center* Z of a (nonassociative) ring T is the set of all elements $x \in T$ such that $xa = ax$ and $(xa)b = x(ab) = a(bx)$ for all elements $a, b \in T$.

It is easy to verify that Z is a subring.

Remark. When we consider the center of an alternative ring, we can, generally speaking, limit ourselves in Definition 8 to the condition $xa = ax$. We do not do this, because we do not wish to distract the reader from the main goal of this work by the details that arise.

We extend Definitions 4 and 5 to alternative rings.

Theorem 5. *Let K be an alternative ring with a finite number of generators and an essential identical relation. If Z_1 is any subring of the center for which all Jordan monomials in r_2-words of the generators are algebraic over Z_1, then K is finite over Z_1.*

Proof. Let λ be the maximal element of the set R of generators of the ring K. Consider an r_1-word w in the elements of the set R such that λ occurs consecutively fewer than $m(\lambda)$ times where $m(\lambda)$ is the degree of the element λ. We perform λ-factorization of the associative word $\overline{w}$ obtained from w by omitting parentheses, and denote by $d_\lambda(w)$ the number of λ-irreducible factors.

Suppose that in the word $\overline{w}$ there appear k distinct λ-irreducible words and $d_\lambda(w) > N(k, s, n)$ [6, Lemma 3], where n is the degree[2] of the identical relation that holds in K, and $s \geq 2n$ is the upper bound on the degrees of all r_1-words v that correspond to subwords $\overline{v}$ of $\overline{w}$ formed by λ-irreducible subwords for which $d_\lambda(v) < n$. From [6, Lemma 3] and the proof of Theorem 1 it follows that the word $\overline{w}$ has a subword u which has either the form $u = u_1 u_2 \cdots u_{n-1} u_n$ or the form

[2]The number n should denote not the degree of the identity in K but in K^+. In general it is not the same and much bigger. [Editors]

$u = (u')^s$ where u' and u_i are words formed by λ-irreducible words, $d_\lambda(u') < n$, and $u_1 u_2 \cdots u_{n-1} u_n$ is an n-decomposition of u.

In each of these cases, we can express the word w as a linear combination of r_1-words that are smaller than w, together with words with coefficients in the ring Z_1 such that the R-lengths of these latter words are strictly less than the R-length of w. Since the arguments are completely analogous, we will consider only the first case.

Let $\overline{w} = \alpha u \beta$ where $u = u_1 u_2 \cdots u_{n-1} u_n$. The words u_i (up to a scalar multiple of the form 2^t) are the maximal (associative) words of some Jordan monomials b_{u_i} [6, Lemma 4]. Thus the element

$$W = \langle \alpha b_{u_1} b_{u_2} \cdots b_{u_n} \beta \rangle = \langle \alpha \overline{b}_{u_1} \overline{b}_{u_2} \cdots \overline{b}_{u_n} \beta \rangle,$$

(recall the notation[3] from [6, §4]) has w as the leading term. According to the last lemma, there exists a Jordan polynomial $I(x_1, x_2, \ldots, x_n)$ that is identically zero in K and has the word $x_1 x_2 \cdots x_n$ as its maximal (associative) word. Since

$$\langle \overline{\alpha I(b_{u_1}, b_{u_2}, \ldots, b_{u_n})} \beta \rangle = 0, \quad \text{and}$$
$$\langle \overline{\alpha I(b_{u_1}, b_{u_2}, \ldots, b_{u_n})} \beta \rangle = \langle \alpha I(b_{u_1}, b_{u_2}, \ldots, b_{u_n}) \beta \rangle,$$

the word w is equal to a linear combination of (lexicographically) smaller r_1-words.

Using the above arguments, we carry out induction on the number of generators, and see that first, every sufficiently long λ-irreducible word is a linear combination of shorter λ-irreducible words, which justifies the introduction of the number k, and second, every sufficiently long r_1-word is a linear combination of shorter r_1-words with coefficients in Z_1. This statement immediately carries over to r_2-words which, by virtue of Lemma 9 of reference [6], completes the proof. □

Let us point out, for example, the following two corollaries of Theorem 5.

Corollary 2. *Any alternative algebraic algebra with an essential identical relation is locally finite.*

The proof of this statement follows from the sufficiently obvious fact that adjoining a unit element preserves algebraicity and also preserves the property of having an identical relation. (For example, the identical relation

$$f(x_1, x_2, \ldots, x_n) \sum (-1)^i \langle x_{i_1} x_{i_2} \cdots x_{i_n} \rangle = 0$$

holds[4], where $f(x_1, x_2, \ldots, x_n) = 0$ is the original relation and $i = (i_1, i_2, \ldots, i_n)$ ranges over all permutations of the symbols $1, 2, \ldots, n$, and $(-1)^i = \pm 1$ according to the parity of the permutation i.)

[3]The bar here has a different meaning from earlier in this proof, up to and including the first sentence of this paragraph. [Translators]

[4]In fact, this identical relation may not hold. For instance, if $f(x, y) = xxy = 0$ holds in A, then $xxy[x, y] = 0$ does not necessary hold in the algebra $A \oplus \mathbb{Z}1$ with an external unit element 1. We can consider instead the identical relation $f([x_1, y_1], \ldots, [x_n, y_n])$. [Editors]

Corollary 3. *The enveloping associative algebra, of an algebraic special Jordan algebra of characteristic* $\neq 2$ *with a finite number of generators and an identical relation, has finite dimension.*

The proof of this statement follows from the fact that the existence of an identical relation for the Jordan polynomials in the generators is sufficient to guarantee that the number of linearly independent r_1-words is finite.

References

[1] P.M. Cohn, *On homomorphic images of special Jordan algebras*, Canadian J. Math. 6 (1954) 253–264.

[2] I. Kaplansky, *Topological representation of algebras II*, Trans. Amer.Math. Soc. 68 (1950) 62–75.

[3] I. Levitski, *On a problem of A. Kurosch*, Bull. Amer. Math. Soc. 52 (1946) 1033–1035.

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

[5] A.I. Shirshov, *On special J-rings*, Mat. Sbornik 38 (1956) 149–166.

[6] A.I. Shirshov, *On some nonassociative nil-rings and algebraic algebras*, Mat. Sbornik 41 (1957) 381–394.

On Free Lie Rings

A.I. Shirshov

1. Introduction

Let Σ be a commutative associative ring with unit, let $R = \{a_\alpha\}$ be some set of symbols, and let $\mathfrak{A}_{\Sigma R}$ be the free associative algebra over Σ with free generating set R. In the ring $\mathfrak{A}_{\Sigma R}$, the set R generates a Lie subring $\mathfrak{A}_{\Sigma R}^{(-)}$ with respect to the operations $x \circ y = xy - yx$, addition, and scalar multiplication by elements of Σ.

If Σ is a field, then it is known that $\mathfrak{A}_{\Sigma R}^{(-)}$ is the free Lie algebra with free generating set R. This result can be derived as an immediate corollary of the Birkhoff-Witt theorem [1, 10]. Since the Birkhoff-Witt theorem cannot be generalized to algebras over an arbitrary coefficient ring [7], the question naturally arises whether the ring $\mathfrak{A}_{\Sigma R}^{(-)}$ is free for arbitrary Σ. In the present paper, a positive answer is given to this question.

For the cases when Σ is a field of characteristic 0 (and also for the case of the so-called restricted Lie algebras), a number of authors [2, 3, 4, 6, 9] concerned themselves with the problem of determining necessary and sufficient conditions under which a given element of $\mathfrak{A}_{\Sigma R}$ belongs to $\mathfrak{A}_{\Sigma R}^{(-)}$. In §3 this problem is resolved without any restrictions on the ring Σ.

Finally, in §4 it is proved that any Lie algebra over a field, with at most countable dimension, can be isomorphically embedded into a Lie algebra with two generators.

All the above-mentioned results are simultaneously proved for restricted Lie algebras.

2. Choice of basis in the ring $\mathfrak{A}_{\Sigma R}^{(-)}$

Consider the set $\mathfrak{R}$ of associative words generated by the elements of R.

Mat. Sbornik N.S. 45 (87), (1958), no. 2, 113–122.

Defining arbitrarily some total order on the set R, we partially order lexicographically the set $\mathfrak{R}$. The order relation will be undefined only for pairs of words in which one word is an initial subword of the other.

Definition 1. An associative word u is called *regular* if $u > u_2u_1$ for any factorization $u = u_1u_2$ where u_1 and u_2 are nonempty.

For example, the word $a_3a_3a_2a_3a_2a_1$ is regular because it is greater than the words $a_3a_2a_3a_2a_1a_3$, $a_2a_3a_2a_1a_3a_3$, $a_3a_2a_1a_3a_3a_2$, etc.

If u and v are regular words and $u = vv_1$, then we will define $v > u$.

Remark. If $u = vv_1$ is a regular word, then $u > v_1$ since v_1 cannot coincide with any initial subword of u.

Definition 2. A nonassociative R-word $[u]$ will be called *regular* if

(1) the associative word u, obtained by omitting the parentheses, is regular; and
(2) if $[u] = [v][w]$ then $[v]$ and $[w]$ are regular words; and
(3) if $[u] = [[v_1][v_2]][w]$ then $v_2 \leq w$.

It is easy to see that regular words are defined inductively, and that one can determine effectively whether a given nonassociative word is regular or not. We also remark that in Condition (2) it is implicit by Condition (1) that $v > w$.

Lemma 1. *In any regular associative word, one can place parentheses in one and only one way such that the resulting nonassociative word is regular.*

Proof. Suppose the lemma is proved for words whose lengths are less than n. Suppose that a given regular associative word u of length $n > 1$ contains an element $a_\beta \in R$ that is less than all the other elements of R occurring in u. Then it is obvious that the word u begins with an element of R that is greater than a_β. From Definition 2 it follows that for any placement of parentheses in the word u that results in a regular nonassociative word, only one placement of parenthesis is possible for subwords of the form $a_\gamma a_\beta a_\beta \cdots a_\beta$:

$$\{\cdots[(a_\gamma a_\beta)a_\beta]\cdots\}a_\beta \quad (a_\gamma > a_\beta).$$

Replacing in the word $[u]$ every subword of the form

$$[\cdots(a_\gamma \underbrace{a_\beta)a_\beta\cdots]a_\beta}_{k \text{ times}},$$

by the symbol a_γ^k, and setting $a_\gamma^k > a_\delta^\ell$ if either $a_\gamma > a_\delta$ or $\gamma = \delta$, $k < \ell$, we obtain a new regular word $[\overline{u}]$ in the symbols a_γ^k $(k = 0, 1, 2, \ldots)$, $a_\gamma^0 = a_\gamma$. If the conclusion of the lemma did not hold for the word $[u]$, then obviously it would not hold for the word $\overline{u}$ either. However, by the inductive hypothesis, this is impossible. The proof is complete. □

By virtue of the one-to-one correspondence between regular associative and nonassociative words that has just been established, we will retain the symbol $[u]$

to denote the regular nonassociative word corresponding to the regular associative word u.

We denote by $L_{\Sigma R}$ the free Lie algebra over Σ with free generating set R.

Lemma 2. *Every element of the free Lie algebra $L_{\Sigma R}$ over Σ with free generating set R can be represented as a linear combination of regular words with coefficients from Σ.*

Proof. Obviously, it suffices to prove the lemma only for words in the elements of the set R. Suppose a word v has length n, and that the lemma has been proved for words of smaller length. Then

$$v = uw = \sum_i \sum_k \sigma_{ik}[u_i][w_k],$$

where $\sigma_{ik} \in \Sigma$, and u_i and w_k are regular words with $u_i > w_k$. If

$$[u_i][w_k] = [[u_{i_1}][u_{i_2}]][w_k] \text{ and } u_{i_2} > w_k,$$

then obviously

$$[u_i][w_k] = [[u_{i_1}][w_k]][u_{i_2}] + [u_{i_1}][[u_{i_2}][w_k]].$$

If we now assume in addition that the associative words, obtained by omitting parentheses in the regular words that occur in the expressions for $[u_{i_1}][w_k]$ and $[u_{i_2}][w_k]$, are greater than w_k, then the proof will be complete by induction on the smallest factor. □

Lemma 3. *If we write the regular word $[v] \in \mathfrak{A}_{\Sigma R}^{(-)}$ as an element of the associative algebra $\mathfrak{A}_{\Sigma R}$, then in this expression v will appear with coefficient 1 and all other associative words that occur will be less than v.*

Proof. For words of length 1, Lemma 3 is trivially valid. Suppose it is valid for words of lengths less than n. If $[v]$ is a word of length $n > 1$ then $[v] = [u][w]$. If we denote by $\overline{t}$ the associative expression for a Lie word t, then obviously

$$\overline{[v]} = \overline{[u]}\,\overline{[w]} - \overline{[w]}\,\overline{[u]}.$$

Since $u > w$ and (by the inductive hypothesis) the maximal words in the expressions $\overline{[u]}\,\overline{[w]}$, $\overline{[w]}\,\overline{[u]}$ are equal respectively to the words uw, wu and have coefficient 1, it follows that the maximal word occurring in $\overline{[v]}$ is equal to $uw = v$ and has coefficient 1. The proof is complete. □

Theorem 1. *The rings $L_{\Sigma R}$ and $\mathfrak{A}_{\Sigma R}^{(-)}$ are isomorphic.*

Proof. Let the element $\ell \in L_{\Sigma R}$ be sent to the element $\overline{\ell}$, under the homomorphism φ of the ring $L_{\Sigma R}$ onto the ring $\mathfrak{A}_{\Sigma R}^{(-)}$ extending the correspondence between the generators. If $\ell \neq 0$, then by Lemma 2 we can assume that the element ℓ is written as a linear combination of regular words, and the coefficient σ of the maximal word $[\ell_1]$ is not zero. Then by Lemma 3, we have $\overline{\ell} \neq 0$ since the word ℓ_1 in the element $\overline{\ell}$ appears with the same coefficient σ. The proof is complete. □

In §4 we will need the following result.

Lemma 4. *Suppose that a regular associative R-word u has the form $u = \alpha\ell\beta$ where ℓ is a regular subword; the words α and β may be empty. Then in the placement of parentheses in the word $[u]$, one pair of parentheses will occur in the position $\alpha(\ell\beta_1)\beta_2$ where $\beta_1\beta_2 = \beta$ and each of the words β_1, β_2 may be empty. Furthermore, parentheses can be placed in the regular word $\ell\beta_1$ as follows:*

$$\{\cdots[(\ell\beta_1^{(1)})\beta_1^{(2)}]\cdots\}\beta_1^{(s)},$$

where $\beta_1^{(i)}$ are regular words with $\beta_1^{(1)} \leq \beta_1^{(2)} \leq \cdots \leq \beta_1^{(s)}$, and in each of the words ℓ, $\beta_1^{(i)}$ parentheses are placed in the unique way prescribed by Lemma 1, and[1] *the maximal (associative) word of the resulting expression*

$$\big(\alpha\{\cdots[(\ell\beta_1^{(1)})\beta_1^{(2)}]\cdots\}\beta_1^{(s)}\big)\beta_2,$$

is equal to u.

Proof. Let a_β be the smallest of the generators that occurs in u. If ℓ has length 1 then there is nothing to prove. Suppose that the lemma is valid if u has length less than n where $n > 1$.

If u has length n, then (as in the proof of Lemma 1) we represent it as a word in the symbols a_γ^k. Assuming that the length of ℓ is greater than 1, we note that it starts with a symbol other than a_β, and in the new representation it will be replaced by a new word ℓ_1 which, regarded as an R-word, can differ by several factors a_β appended on the right. It is easy to see that the R-word ℓ_1 will be regular. Considering the words u and ℓ_1 as words in the symbols a_γ^k, we find ourselves in a situation where we can apply the inductive hypothesis. The remainder of the argument is obvious, and this completes the proof. □

To conclude this section, we will show how Theorem 1 implies Witt's formula [10] for the rank of the homogeneous submodule of degree q in the free Lie algebra.

Definition 3. An associative word v is called *periodic* if it can be written as the product of k ($k > 1$) equal words. Two associative words u and w are called *cyclically comparable* if there exist representations $u = u_1u_2$, $w = w_1w_2$ such that $u_1 = w_2$, $u_2 = w_1$.

It is easy to see that the set of all associative words is partitioned into disjoint classes of cyclically comparable words. The following statements are trivial.

Lemma 5. *Each class of cyclically comparable non-periodic words contains one and only one regular word.*

Lemma 6. *No class of cyclically comparable periodic words contains a regular word.*

Let $\psi_q(n)$ be the rank of the submodule of homogeneous polynomials of degree q in the free Lie algebra on n generators. The number $\psi_q(n)$ coincides with

[1] The rest of this sentence has been added by the Editors.

the number of regular words of length q in n symbols. From Lemmas 5 and 6, we obtain the following equation:

$$n^q = q\,\psi_q(n) + d_1\psi_{d_1}(n) + \cdots + d_s\psi_{d_s}(n),$$

where n^q is the number of all associative words of length q in n symbols, and the d_i are the divisors of q (other than q itself). The Dedekind inversion principle[2] immediately gives Witt's formula:

$$\psi_n(q) = \frac{1}{q}\sum_{s|q}\mu(s)\,n^{q/s}$$

where $\mu(s)$ is the Möbius function.

3. Free restricted Lie rings

Suppose that the characteristic of the coefficient ring Σ is a prime number p. The associative ring $\mathfrak{A}_{\Sigma R}$ that was considered in §1 is obviously a ring of characteristic p. It is known [5] that in this case the element $(a+b)^p - a^p - b^p = \varphi(a,b)$ of the ring $\mathfrak{A}_{\Sigma R}$ is a Lie polynomial in the elements a and b.

Definition 4. A Lie algebra L over Σ in which a unary operation $x^{[p]}$ is defined is called a *restricted Lie algebra* if

$$(a+b)^{[p]} = a^{[p]} + b^{[p]} + \varphi(a,b), \quad a\cdot b^{[p]} = [\cdots(a\cdot\underbrace{b)\cdot b\cdots]b}_{p\text{ times}}, \quad (\sigma a)^{[p]} = \sigma^p a^{[p]},$$

for all elements $a, b \in L$ and $\sigma \in \Sigma$.

Obviously any associative algebra over Σ becomes a restricted Lie algebra with respect to addition and the operations $a \circ b = ab - ba$, $a^{[p]} = a^p$. In the free ring $\mathfrak{A}_{\Sigma R}$, the set R generates a restricted Lie algebra $\mathfrak{A}^{(p)}_{\Sigma R}$. We introduce the following notation:

$$x^{[p^k]} = [\cdots(x\underbrace{^{[p]})^{[p]}\cdots]^{[p]}}_{k\text{ times}}.$$

Lemma 7. *Every element of an arbitrary restricted Lie algebra A over Σ with generating set R can be written as a linear combination with coefficients in Σ of elements of the form $u^{[p^k]}$ $(k = 0, 1, 2, \ldots)$ where u is a regular nonassociative word.*

The proof of this result follows immediately from Definition 4 and Lemma 2.

Definition 5. An associative word v is called *p-regular* if it has the form u^{p^k} $(k = 0, 1, 2, \ldots)$ where u is a regular word.

[2]This is now usually called the Möbius inversion formula. [Translators]

Definition 6. Elements of the ring $\mathfrak{A}_{\Sigma R}^{(p)}$ that have the form $[u]^{p^k}$, where $[u]$ is a regular nonassociative R-word relative to the operation $a \circ b = ab - ba$, are called *p-regular elements.*

Lemma 8. *The set of p-regular elements of $\mathfrak{A}_{\Sigma R}^{(p)}$ is linearly independent over Σ.*

Proof. Obviously, the leading term of the polynomial which is the associative expansion of the p-regular element $[u]^{p^k}$ will be the p-regular associative word u^{p^k}. Therefore distinct p-regular elements correspond to distinct maximal words. From this the lemma follows. □

Lemmas 7 and 8 immediately imply the following result.

Theorem 2. *The algebra $\mathfrak{A}_{\Sigma R}^{(p)}$ is a free restricted Lie algebra over Σ with generating set R and a basis consisting of the p-regular elements.*

From the above constructions we immediately obtain an algorithm that allows us to determine, for a given element a of the algebra $\mathfrak{A}_{\Sigma R}$, whether or not it belongs to the algebras $\mathfrak{A}_{\Sigma R}^{(-)}$ or $\mathfrak{A}_{\Sigma R}^{(p)}$. For this determination, one should separate the lexicographically maximal monomial σu in the expression of the element a. If the word u is not regular (respectively, p-regular) then the corresponding membership question is answered in the negative. If the word is regular (respectively, p-regular) then subtracting from a the element $\sigma[u]$ (respectively, $\sigma[u_1]^{p^k}$) where $[u]$, $[u_1]$ are the corresponding regular nonassociative words, we obtain an element a_1 whose maximal monomial will be less than the monomial σu. After a finite number of steps this process will terminate. From this algorithm one can obtain the following criterion of Friedrichs [4].

Theorem 3. *An element $f(a_1, a_2, \ldots, a_s)$ of the algebra $\mathfrak{A}_{\Sigma R}$ belongs*[3] *to $\mathfrak{A}_{\Sigma R}^{(p)}$ if and only if the relations $a_i a'_j = a'_j a_i$ imply the equation*[4]

$$f(a_1 + a'_1, a_2 + a'_2, \ldots, a_s + a'_s) = f(a_1, a_2, \ldots, a_s) + f(a'_1, a'_2, \ldots, a'_s).$$

Proof. The proof of the necessity of the conditions is by induction and is almost trivial. Let us prove the sufficiency for the case of characteristic 0 (the proof of the general case is similar).

Let d be an element of $\mathfrak{A}_{\Sigma R}$ that does not belong to $\mathfrak{A}_{\Sigma R}^{(-)}$. Then, after a finite number of steps of the above-mentioned algorithm, we will obtain an element d_i whose leading term is σu_i where the word u_i is not regular. Then $u_i = vw$ where $wv \geq u_i$; and[5] wv is maximal among the words that are cyclically comparable with u_i. It is easy to see, however, that in the expression

$$d_i(a_1 + a'_1, a_2 + a'_2, \ldots, a_s + a'_s) - d_i(a_1, a_2, \ldots, a_s) - d_i(a'_1, a'_2, \ldots, a'_s),$$

[3] In the case of characteristic 0, one must replace $\mathfrak{A}_{\Sigma R}^{(p)}$ by $\mathfrak{A}_{\Sigma R}^{(-)}$. [Translators]
[4] Today this is expressed in terms of the coproduct on the algebra $\mathfrak{A}_{\Sigma R}$. [Translators]
[5] (without loss of generality). [Translators]

the element

$$v(a_1,\dots,a_s)\,w(a'_1,\dots,a'_s) = w(a'_1,\dots,a'_s)\,v(a_1,\dots,a_s),$$

occurs with coefficient $\sigma \neq 0$. The proof is complete. □

4. Theorems on embeddings of Lie algebras and restricted Lie algebras

In what follows we will denote by L a Lie algebra over an arbitrary field or a restricted Lie algebra over a field of characteristic $p > 0$. Our task is to demonstrate the possibility of embedding L into an appropriate algebra with two generators under certain assumptions of countability, and then to generalize this result. Let A be the free associative algebra on two generators a and b.

Lemma 9. *The elements*

$$d_k = [a \circ \{[\cdots(a \circ \underbrace{b) \circ b \cdots] \circ b\}]}_{k\ times} \circ (a \circ b) \qquad (k = 1, 2, \ldots),$$

of A generate (under the operations $a \circ b$ and $a^{[p]}$) a free Lie algebra (respectively a free restricted Lie algebra) $L(a,b)$, and constitute a set T of free generators.

Proof. We order the set T by setting $d_k > d_s$ for $k < s$. It is easy to verify that every regular nonassociative T-word (respectively, p-regular T-element) is a regular nonassociative R-word (respectively, p-regular R-element). From this follows the linear independence of regular nonassociative T-words (respectively, p-regular T-elements), and this proves the lemma. □

Lemma 10. *The set $T = \{d_k\}$ is distinguished (in the sense of Definition 1 of* [8]*).*

Proof. Let J be an ideal of $L(a,b)$ and J_1 the ideal generated by J in A. It suffices to prove the equality $J_1 \cap L(a,b) = J$ (in fact the definition of 'distinguished' demands that $J'_1 \cap L(a,b) = J$ where J'_1 is the ideal of the Lie algebra $A^{(-)}$ generated by J). Consider some element ℓ in J_1:

$$\ell = \sum_i m_i = \sum_i \alpha_i \ell_i \beta_i,$$

where the α_i and β_i are monomials (possibly empty) in a and b, and the ℓ_i are elements of J and thus of $L(a,b)$, that is, Lie polynomials in the elements of T. Let $\overline{\ell_i}$ be the maximal word among the words of highest degree that occur in the associative expansion of ℓ_i. Obviously, $\overline{\ell_i}$ is a regular (respectively p-regular) associative word. Among the words of the form $\alpha_i\overline{\ell_i}\beta_i$ that have highest degree, we choose one which is maximal in the lexicographical sense: $t = \alpha_j\overline{\ell_j}\beta_j$. Assume that $\ell \in L(a,b)$.

Case 1*:* Suppose that the word t does not occur[6] among the other associative words that occur in the expansion of ℓ. Then the word t is regular (respectively

[6]Literally, "does not have similars". [Translators]

p-regular) and contains a regular (respectively p-regular) subword $\overline{\ell_j}$. We place parentheses in the word t in the unique way which makes it a regular nonassociative word (p-regular element). By virtue of Lemma 4, one pair of these parentheses will be placed as follows[7]: $\alpha_j[\overline{\ell_j}\beta_{1j}]\beta_{2j}$ where $\beta_{1j}\beta_{2j} = \beta_j$ and each of the words β_{1j}, β_{2j} may be empty. Moreover, after the required placement of parentheses, the word $\overline{\ell_j}\beta_{1j}$ will take the form

$$\ell' = [\cdots(\overline{\ell_j} \circ \beta^{(1)}) \circ \beta^{(2)} \cdots] \circ \beta^{(k)},$$

where $\overline{\ell_j}$ and β_s are regular nonassociative words and $\beta^{(1)} \leq \beta^{(2)} \leq \cdots \leq \beta^{(k)}$.

The word t is the product of words of the form a^2b^kab $(k = 1, 2, \ldots)$ since otherwise, performing the algorithm of expressing ℓ as a linear combination of the basis elements of the algebra $A^{(-)}$ (respectively, the free restricted algebra $A^{(p)}$), we would obtain a leading term which is not a T-word; but it is obvious that every element of $L(a, b)$ contains only T-words in its expression in terms of the basis of regular words. From this it easily follows that each of the words $\beta^{(s)}$, as well as α_j and β_{2j}, is a T-word.

The element $\ell'' = \{\alpha_j[\overline{\ell_j}\beta_{1j}]\beta_{2j}\}$, in which the parentheses inside the square brackets are placed in the same way as in ℓ', and elsewhere in the way prescribed for regular words, will obviously be a nonassociative T-polynomial that belongs to the intersection $J_1 \cap L(a, b)$; from the proof of Lemma 4 it follows that its lexicographically maximal word, among the words of highest degree, coincides with t. Therefore, in the difference $\ell - \ell''$ the analogous word will be lexicographically smaller or will have lower degree.

Our argument does not apply only in the case when t is a p^k-th power of $\overline{\ell_j}$. Let

$$t = q^s\overline{\ell_j}q^{p^{k+k_1}-p^{k_1}-s},$$

where $\overline{\ell_j} = q^{p^{k_1}}$, and q is a regular word. The element $(\ell_j)^{p^k}$ of the ideal J can be written in the form

$$\left(\overline{\ell_j} + \omega\right)^{p^k} = \left(\overline{\ell_j} + \omega\right)^{p^k-1}\ell_j = q^{p^{k+k_1}-p^{k_1}}\ell_j + \sum_k \varepsilon_k\ell_j,$$

where ω stands for the terms smaller than $\overline{\ell_j}$, and the leading terms of the elements $\varepsilon_k\ell_j$ of the ideal J_1 are less than t. On the other hand, by virtue of the representation

$$\begin{aligned} q^s\ell_j q^{p^{k+k_1}-p^{k_1}-s} &= \sum_{t=1}^{p^{k+k_1}-p^{k_1}-s} q^{s+t-1}(\ell_j \circ q)q^{p^{k+k_1}-p^{k_1}-s-t} + q^{p^{k+k_1}-p^{k_1}}\ell_j \\ &= s_1 + q^{p^{k+k_1}-p^{k_1}}\ell_j = s_1 + (\ell_j)^{p^k} - \sum_k \varepsilon_k\ell_j, \end{aligned}$$

[7]We have added a bar over ℓ_j. [Translators]

where s_1 is also an element of J_1 with leading term less than t, we see that after subtracting from ℓ the element $(\ell_j)^{p^k}$ (that obviously belongs to the ideal J) we will obtain an element of J_1 with leading term less than t.

Case 2*:* Suppose that we have several maximal words: $t_1, t_2, \ldots, t_r$. Take any two of them:

$$t_1 = \alpha_j \overline{\ell_j} \beta_j, \qquad t_2 = \alpha_k \overline{\ell_k} \beta_k.$$

Again several subcases are possible.

(a) $t_1 = t_2 = \alpha_j \, \overline{\ell_j} \, \gamma_j \, \overline{\ell_k} \, \beta_k$. In this case m_j (the element to which the word t_1 belongs) can be written, up to a scalar coefficient, in the form

$$m_j = \alpha_j \, \ell_j \, \gamma_j \, \overline{\ell_k} \, \beta_k = \alpha_j \, \ell_j \, \gamma_j \, \ell_k \, \beta_k - \omega_j = m_k + \omega,$$

where ω and ω_j are polynomials whose terms are smaller than t_1 or have lower degree; and ω_j as well as ω belong to the ideal J_1. Combining similar terms reduces the number of distinct t_s.

(b) $t_1 = t_2 = \alpha_j \ell_{1j} \ell_{2j} \ell_{3j} \beta_k$ where $\ell_{1j} \ell_{2j} = \overline{\ell_j}$ and $\ell_{2j} \ell_{3j} = \overline{\ell_k}$; also $\overline{\ell_j}$ and $\overline{\ell_k}$ are regular words (one of the words ℓ_{1j} and ℓ_{3j} may be empty). From regularity of the words $\overline{\ell_j}$ and $\overline{\ell_k}$ and the Remark after Definition 1, it follows that the word $\ell_{1j} \ell_{2j} \ell_{3j}$ is regular. From Lemma 4 it follows that the placement of parentheses in the word $[\ell_{1j} \ell_{2j} \ell_{3j}]$ on the subword $\overline{\ell_k}$ coincides with the placement of parentheses in the word $[\overline{\ell_k}]$:

$$[\ell_{1j} \ell_{2j} \ell_{3j}] = \ell'_1 \{\ell'_2 \cdots (\ell'_s [\overline{\ell_k}]) \cdots \}.$$

The same lemma implies that we may place parentheses in the word $\ell_{1j} \ell_{2j} \ell_{3j}$ as follows:

$$\{([\overline{\ell_j}] \ell''_1) \ell''_2 \cdots \} \ell''_q,$$

where $\ell''_1 \le \ell''_2 \le \cdots \le \ell''_q$, and the ℓ''_r are regular words with the corresponding placement of parentheses. In this case each of the words ℓ_{tj} $(t = 1, 2, 3)$, ℓ'_p, ℓ''_r is a product of words of the form $a^2 b^k a b$ $(k = 1, 2, \ldots)$. Obviously, the element

$$\alpha_j \Big(\ell'_1 \circ \{\ell'_2 \circ \cdots (\ell'_s \circ \ell_k) \cdots \} + \{\cdots [(\ell_j \circ \ell''_1) \circ \ell''_2] \cdots \circ \ell''_q\} \Big) \beta_k,$$

of the ideal J_1, coincides up to some lower terms with the sum $m_j + m_k$. Therefore the words t_1 and t_2 in this case can be replaced by one word (or both can be omitted).

One can argue analogously using Lemma 4 in the case where $\overline{\ell_j} = \ell_{1j} \ell_{2j} \ell_{3j}$ and $\ell_{2j} = \overline{\ell_k}$.

(c) $t_1 = t_2 = \alpha_j \ell_{1j} \ell_{2j} \ell_{3j} \beta_k$ where $\ell_{1j} \ell_{2j} = \overline{\ell_j} = q^{p^r}$, $\ell_{2j} \ell_{3j} = \overline{\ell_k} = q^{p^s}$ $(s > r)$ and $\ell_{2j} = q^n$. Then we can reduce the number of the words t_s by using

the equations

$$\ell_j\ell_{3j} = \ell_j q^{p^s-n} = \sum_{t=0}^{p^s-n-1} q^t(\ell\circ q)q^{p^s-n-t-1} + q^{p^s-n}\ell_j = \omega_1 + q^{p^s-n}\ell_j$$
$$= \omega_1 + q^{p^s-n}\overline{\ell_j}^{p^{s-r}-1}\ell_j = \omega_1 + q^{p^r-n}\Big(\overline{\ell_j}^{p^{s-r}} - \sum_i \varepsilon_i\ell_j\Big)$$
$$= q^{p^r-n}\ell_j^{p^{s-r}} + \omega_2 = \ell_{1j}\ell_k + q^{p^r-n}\Big(\ell_j^{p^{s-r}} - \ell_k\Big) + \omega_2 = \ell_{1j}\ell_k + \omega_3,$$

where ω_i, as well as $\varepsilon_i\ell_j$, are elements of the ideal J_1 with smaller leading terms.

Considering the remaining possible cases, including those in which one of the words $\overline{\ell_j}$ or $\overline{\ell_k}$ is regular and the other is p-regular but not regular, by analogous arguments we can reduce the number of words t_s. Having reduced this number to 1, we will be under the conditions of Case 1. These arguments imply that after a finite number of steps we will express ℓ as an element of the ideal J. The proof is complete. □

Theorem 4. *Every Lie algebra or restricted Lie algebra of at most countable rank can be isomorphically embedded into an appropriate algebra with two generators over the same field.*

Theorem 5. *Any Lie algebra (respectively restricted Lie algebra) can be isomorphically embedded into a Lie algebra (respectively restricted Lie algebra) with the property that every subalgebra of countable rank is contained in a subalgebra with two generators.*

Theorems 4 and 5 are corollaries of Lemma 10 as well as Theorems 1 and 2 of [8]; it is necessary to remark that although the statements of the latter Theorems do not formally include the case of restricted Lie algebras, the given proofs also remain valid in this case without any changes.

It is easy to see that the algebras obtained here are automatically represented in an associative algebra. Therefore, the proof given here also contains a proof of the Birkhoff-Witt theorem [1], [10] and the theorem of Jacobson [5].

References

[1] G. Birkhoff: *Representability of Lie algebras and Lie groups by matrices.* Annals of Math. 38 (1937) 526–532.

[2] P.M. Cohn: *Sur le critère de Friedrichs pour les commutateurs dans une algèbre associative libre.* C. R. Acad. Sci. Paris 239 (1954) 743–745.

[3] E.B. Dynkin: *Evaluation of the coefficients in the Campbell-Hausdorff formula.* Doklady Akad. Nauk USSR 57 (1947) 323–326.

[4] K.O. Friedrichs: *Mathematical aspects of the quantum theory of fields, V.* Comm. Pure Appl. Math. 6 (1953) 1–72.

[5] N. Jacobson: *Restricted Lie algebras of characteristic p.* Trans. Amer. Math. Soc. 50 (1941) 15–25.

[6] R.C. Lyndon: *A theorem of Friedrichs*, Michigan Math. J. 3 (1955–56) 27–29.

[7] A.I. Shirshov: *On the representation of Lie rings in associative rings*. Uspekhi Mat. Nauk 8 (1953) 173–175.

[8] A.I. Shirshov: *Some theorems on embedding of rings*. Mat. Sbornik 40 (1956) 65–72.

[9] F. Wever: *Operatoren in Lieschen Ringen*. J. reine angew. Math. 189 (1947) 44–55.

[10] E. Witt: *Treue Darstellung Lieschen Ringen*. J. reine angew. Math. 177 (1937) 152–160.

On a Problem of Levitzki

A.I. Shirshov

An associative ring S is called a *nil-ring* if every element of S is nilpotent. Levitzki [4] posed the following problem: Is every nil-ring nilpotent? This problem was solved in the affirmative by Levitzki himself [5] for the case in which the elements of S have globally bounded indices of nilpotency. Later, Kaplansky [2], who was investigating the more general problem of Kurosh [3], extended the result of Levitzki to nil-rings with polynomial identities. In the present note an affirmative solution is given to Levitzki's problem for the wider class of rings introduced by Drazin [1].

Let $\Lambda = \{\lambda_i\}$, $i = 1, 2, \ldots, h$ be some set of variables, and let $\pi(\lambda) = \lambda_{i_1}\lambda_{i_2}\cdots\lambda_{i_k}$ be some monomial in these variables. Denote by $T_\pi(\lambda)$ the set of all monomials in Λ of degree $\geq k$ and distinct from $\pi(\lambda)$. For any sequence of elements $\{x_i\}$, $i = 1, 2, \ldots, h$, of the ring S, we denote by $\pi(x)$ the element $x_{i_1}x_{i_2}\cdots x_{i_k}$ and by $T_\pi(x)$ the set of all elements of S obtained by replacing the variables λ_i by the corresponding elements x_i in each monomial of $T_\pi(\lambda)$.

If there exists a monomial $\pi(\lambda)$, such that for any collection of elements x_i, $i = 1, 2, \ldots, h$, of the ring S the element $\pi(x)$ belongs to the right ideal generated by $T_\pi(x)$, then the monomial $\pi(\lambda)$ is called a *strongly pivotal monomial* of S, and S is called a *ring with strongly pivotal monomial*. For brevity, we will call such rings SP-rings.

Drazin [1] has shown that the class of SP-rings contains the rings with minimum condition on right ideals and the rings with polynomial identity. In the same paper it was shown that for any SP-ring the monomial $\pi(\lambda)$ can be assumed to be linear in each variable λ_i. Under some strong restrictions, Drazin, using essentially the methods of Kaplansky, gave an affirmative solution to the problem of Kurosh for SP-algebras, i.e., he proved local finiteness of algebraic SP-algebras of a particular type. However, Drazin himself points out the difficulties that did not allow him to solve even the Levitzki problem for SP-rings without additional restrictions.

Doklady Akad. Nauk SSSR 120, (1958), no. 1, 41–42.

If a strongly pivotal monomial $\pi(\lambda)$, which in the sequel will be assumed linear in each variable λ_i, has degree t, then the SP-ring S will be called *an SP-ring of degree t.*

Lemma. *Let S be a nil SP-ring of degree t, and let I be the ideal generated by the elements a_i^t where a_i, $i = 1, 2, \ldots, n$, is some fixed set of elements of S. Then for any natural number $q > t$ there exists a natural number $k = k(q)$ such that the ideal I^k is contained in the ideal generated by the elements a_i^q.*

Proof. Suppose that there exists a natural number r such that the ideal I^r is contained in the ideal generated by the elements a_i^m, $i = 1, 2, \ldots, n$, for some fixed $m \geq t$. In order to prove the lemma we will show that there exists a natural number r_1 such that the ideal I^{r_1} is contained in the ideal generated by the elements a_i^{m+1}.

Every element of the ideal $I^{r(nt+1)}$ can be written as a sum of products of $nt+1$ elements of the form $\alpha\, a_j^m \beta$ where α and β are monomials in the generators of S. In each such product there exists an element a_j^m that occurs at least $t+1$ times. Therefore, each such product can be written in the form

$$\begin{aligned} c_1 D c_{t+2} &= c_1 d_1 d_2 \cdots d_t c_{t+2} \\ &= c_1 (a_j^m c_2 a_j)(a_j^{m-1} c_3 a_j^2)(a_j^{m-2} c_4 a_j^3) \cdots (a_j^{m-t+1} c_{t+1} a_j^t) c_{t+2}. \end{aligned}$$

By assumption, the monomial D belongs to the right ideal generated by all possible products of its factors d_1, d_2, …, d_t which are distinct from D itself and have total degree (with respect to the elements d_i) greater than or equal to that of D.

For any other monomial of degree t in the elements d_i, there exist two adjacent elements d_{j_1} and d_{j_2} with $j_1 \geq j_2$. In each such case, in the corresponding segment, there is a word

$$\begin{aligned} d_{j_1} d_{j_2} &= a_j^{m-j_1+1} c_{j_1+1} a_j^{j_1} a_j^{m-j_2+1} c_{j_2+1} a_j^{j_2} \\ &= a_j^{m-j_1+1} c_{j_1+1} a_j^{m+1+(j_1-j_2)} c_{j_2+1} a_j^{j_2}. \end{aligned}$$

It is easy to see that all such elements belong to the ideal generated by a_j^{m+1}. From this it follows that $c_1 D = \omega_1 + c_1 D q$ where ω_1 is an element of the ideal generated by the element a_j^{m+1}. But then

$$\begin{aligned} c_1 D &= \omega_1 + \omega_1 q + c_1 D q^2 = \omega_1 + \omega_1 q + \omega_1 q^2 + c_1 D q^3 = \cdots \\ &= \omega_1 + \omega_1 q + \omega_1 q^2 + \cdots + \omega_1 a^\ell + c_1 D q^{\ell+1}, \end{aligned}$$

for any ℓ. The lemma now follows from nilpotency of the element q. For the number r_1 we can take $r(nt+1)$. □

Theorem. *Any nil SP-ring is locally nilpotent.*

Proof. Let S be a nil SP-ring of degree t with a finite number of generators, and let J be the ideal generated by all possible elements a^t, $a \in S$. The quotient ring S/J is nilpotent by Levitzki's theorem [5], and this means that there exists a natural number M such that any element of the form $b_{i_1} b_{i_2} \cdots b_{i_M}$, where the b_{i_s} are the generators of S, belongs to the ideal J. Since there is only a finite number

of elements of the form $b_{i_1} b_{i_2} \cdots b_{i_M}$, the ideal S^M is contained in some ideal J_1 which is contained in J and is generated by some finite set of elements a_i^t. The lemma implies nilpotency of the ideal J_1, and hence of the ring S. □

References

[1] M.P. Drazin, *A generalization of polynomial identities in rings*, Proc. Amer. Math. Soc. 8 (1957) 352–361.

[2] I. Kaplansky, *Topological representation of algebras II*, Trans. Amer. Math. Soc. 68 (1950) 62–75.

[3] A.G. Kurosh, *Ringtheoretische Probleme, die mit dem Burnsideschen Problem über periodische Gruppen in Zusammenhang stehen*, Izvestiya Akad. Nauk USSR Ser. Mat. 5 (1941) 233–240.

[4] J. Levitski, *On the radical of a general ring*, Bull. Amer. Math. Soc. 49 (1943) 462–466.

[5] J. Levitski, *On a problem of A. Kurosch*, Bull. Amer. Math. Soc. 52 (1946) 1033–1035.

Some Problems in the Theory of Rings that are Nearly Associative

A.I. Shirshov

The words "some problems" in the title of this article mean primarily that the article considers absolutely no results about algebras of finite dimension. Among other questions that remain outside the scope of the article, we mention, for example, various theorems about decomposition of algebras (see for example [47, 70]) which are closely related to the theory of algebras of finite dimension.

The author is grateful to A.G. Kurosh and L.A. Skornyakov who got acquainted with the first draft of the manuscript and made a series of very valuable comments.

1. Introduction

1. Until recently the theory of rings and algebras was regarded exclusively as the theory of *associative* rings and algebras. This was a result of the fact that the first rings encountered in the course of the development of mathematics were associative (and commutative) rings of numbers and rings of functions, and also associative rings of endomorphisms of Abelian groups, in particular, rings of linear transformations of vector spaces.

In the survey article by A.G. Kurosh [40] he persuasively argued that the contemporary theory of associative rings is only a part of a general theory of rings, although it continues to play a very important role in mathematics. The present article, in contrast to the article of A.G. Kurosh, is dedicated to a survey of one part of the theory of rings: precisely, the theory of rings, which although nonassociative, are more or less connected with associative rings. More precise connections will be mentioned during the discussion of particular classes of rings.

Uspekhi Mat. Nauk 13, (1958), no. 6 (84), 3–20.

Because the classes of rings that are studied in this article were mentioned to some extent in the article of A.G. Kurosh, there is some intersection in the content of these two articles. In what follows, the author assumes that the following notions are understood: rings, algebras, ideals, quotient rings, rings with a domain Σ of operators (or Σ-operator rings[1]). These notions and also some other main notions of the theory of rings can be found in the same article by A.G. Kurosh.

2. We briefly describe the origins of the theory of nonassociative rings. Examples of such rings were known a long time ago. The nonassociativity of the vector product of 3-dimensional vectors was known in mechanics. With this operation and vector addition the collection of vectors is a Lie ring. Another very beautiful example is the algebra of so-called Cayley numbers, which have been used in different parts of mathematics.

The development of the theory of continuous groups in general and Lie groups in particular contributed to the study of Lie algebras of finite dimension, which are closely connected to Lie groups. Another connection between Lie algebras and groups which appears to be very fruitful has been studied in the works of W. Magnus [45], I.N. Sanov [50], A.I. Kostrikin [35] and others.

There is an interesting relationship between associative rings on the one hand and Lie rings and Jordan rings[2] on the other hand, constructed by the introduction of a new operation on an associative ring. This relationship, in addition to giving certain information about Lie rings and Jordan rings, allows us to study associative rings themselves from some new directions.

3. Because there are differences between the properties of rings in different classes, there are few results which have a universal character. We will describe some of them.

Let A be an associative ring, and let a be some element of the ring A. It is possible to connect with this element a new operation of "multiplication" which is defined by $x \cdot y = axy$. It is easy to check that the set of elements of the ring A forms, under this operation and addition, a ring (in general, already nonassociative), which we will denote by $A(a)$. In [48] A.I. Malcev proved that any ring is isomorphic to some subring of a ring of the form $A(a)$.

Let the additive group of an associative ring be decomposed into the direct sum of subgroups A_1 and A_2. Then every element $a \in A$ allows a unique representation of the form $a = a_1 + a_2$. Under the operations of "multiplication" $x \cdot y = (xy)_1$ and addition the set of elements of the ring A is a ring (in general, nonassociative). We denote this ring by A'. In [66] L.A. Skornyakov proved that any ring is isomorphic to some subring of a ring of the form A'.

The preceding results of Malcev and Skornyakov indicate the possibility of developing the entire theory of rings in terms of associative rings. However, nobody until now has been able to get any precise theorems about rings of some class based

[1]That is, an algebra over the commutative associative coefficient ring Σ. [Translators]
[2]Literally, "J-rings". [Translators]

on this method. Among the reasons for this is the fact that we cannot transfer the properties of A to $A(a)$ and A'. So, for example, if A is a Lie ring, then the rings $A(a)$ and A' may not be Lie rings.

The results and problems that correspond to different classes of rings are formulated very differently and require specific methods, and because of this it is difficult to imagine the development of the entire theory of rings from the theory of one specific, sufficiently studied class.

4. In the theory of rings, as in the theory of groups and other algebraic systems, free systems play an important role: free rings, free associative rings, free Lie rings, etc.

Let ν be a cardinal number. The free ring (free associative ring, free Lie ring, etc.) on ν generators is a ring (associative ring, Lie ring, etc.) which has a system S of generators of cardinality ν such that any mapping from S onto any system of generators of any ring (associative ring, Lie ring, etc.) can be extended to a homomorphism of rings. The free ring A_ν with the set S of generators of cardinality ν can be built constructively by the following steps.

We will call the elements of the set S *words of length* 1. If α and β are words of lengths m and n (respectively) then the symbol $(\alpha)(\beta)$ will be called a *word of length* $m+n$; furthermore, we will consider two words $(\alpha)(\beta)$ and $(\alpha_1)(\beta_1)$ to be equal if and only if $\alpha=\alpha_1$ and $\beta=\beta_1$. The collection of finite sums of the form $\sum_s k_s\gamma_s$ where k_s is an integer and γ_s is a word (we assume $\gamma_s\neq\gamma_t$ when $s\neq t$) becomes a ring, which we will denote by A_ν, when we define the operations as follows:

$$\sum_s k_s\gamma_s+\sum_s l_s\gamma_s=\sum_s(k_s+l_s)\gamma_s,$$
$$\sum_s k_s\gamma_s\cdot\sum_t l_t\gamma_t=\sum_{s,t}k_sl_t(\gamma_s)(\gamma_t).$$

It is easy to check that the ring A_ν satisfies the above-formulated definition, and that any ring that satisfies that definition is isomorphic to A_ν.

If the symbols k_s are allowed to come from some associative ring Σ and we define

$$k\sum_s k_s\gamma_s=\sum_s(kk_s)\gamma_s,\ k\in\Sigma,$$

then the ring A_ν will be a free Σ-operator ring with ν generators in the sense of Σ-operator homomorphisms. If, furthermore, Σ is a field, then A_ν is a free algebra with ν generators over the field Σ.

In the works of Kurosh [39, 41] it was proved that any subalgebra of a free algebra is again free, and some generalizations of this result to free sums of algebras were given. A.I. Zhukov [74] solved positively the word problem[3] for algebras[4] with

[3]Literally, the "problem of equality". [Translators]
[4]That is, nonassociative algebras. [Translators]

a finite number of generators and a finite number of defining relations which is analogous to the famous word problem in the theory of groups.

5. With additional axioms, or so-called identical relations, we may define various classes of rings. The general method applied to this problem is as follows.

Let A_ω be the free ring with a countably infinite number of generators x_i $(i = 1, 2, \ldots)$. In the ring A_ω we consider a subset Q. Any ring C which satisfies the condition that any substitution of any elements of C into the generators x_i in any element of the set Q gives zero, will be regarded as belonging to the class defined by the set Q, or simply to the class of Q-rings. If in some free ring A_ν we take the ideal J generated by the elements obtained by substituting all the elements of A_ν into the generators x_i in the elements of Q, then the quotient ring $D = A_\nu/J$ will be isomorphic to the free Q-ring in the sense given earlier. For example, if the set Q consists of the single element $(x_1x_2)x_3 - x_1(x_2x_3)$ then we obtain the class of associative rings. If the set Q consists of elements q_α, then it is sometimes said that the class of Q-rings is defined by the identical relations $q_\alpha = 0$. The same concepts can be defined in a very similar way for Σ-operator Q-rings.

For the case when the set Q is finite, Yu.I. Sorkin [69] showed that the corresponding class of rings can be given with the help of one ternary operation (that is, defined on ordered triples of elements) and one relation which this operation must satisfy.

2. Alternative rings

1. It is known that the field of complex numbers can be represented as the collection of pairs of real numbers with the natural addition and the familiar definition of multiplication. If on the Abelian group of ordered pairs (p, q) of complex numbers with coordinate-wise addition is defined an operation of multiplication by the formula

$$(p_1, q_1) \cdot (p_2, q_2) = (p_1p_2 - \overline{q_2}q_1, q_2p_1 + q_1\overline{p_2}), \tag{1}$$

where $\overline{p_2}$ and $\overline{q_2}$ are the complex conjugates of the complex numbers p_2 and q_2, then one can easily check that with respect to these operations the set we are considering is a ring. In this ring it happens that the equations $AX = B$ and $XC = D$ have a uniquely determined solution when $A \neq 0$, $C \neq 0$ and so this ring is the (associative but not commutative) division ring of real quaternions. If in equation (1) we replace the symbols p_i and q_i by real quaternions, and we understand $\overline{p}$ to be the quaternion conjugate of the quaternion $p = (a, b)$ – that is, $\overline{p} = (\overline{a}, -b)$ – then the pairs of quaternions become a ring with respect to these operations, which in this case is a nonassociative division ring. If for every real number α and pair (p, q) we define $\alpha(p, q) = (\alpha p, \alpha q)$, then the additive groups of the above division rings become vector spaces over the field of real numbers with corresponding dimensions 4 and 8, and the division rings become algebras over the

field of real numbers. The constructed nonassociative algebra of dimension 8 over the field of real numbers is called the *algebra of Cayley numbers*. In what follows we will denote it by R_8.

2. The *associator* of the elements a, b, c in any ring is defined to be the element

$$[a, b, c] = (ab)c - a(bc).$$

The algebra R_8 satisfies the following identical relations,

$$[x, y, y] = 0, \tag{2}$$

$$[x, x, y] = 0, \tag{3}$$

$$[x, y, x] = 0, \tag{4}$$

each of which is implied by the other two. Rings in which the identical relations (2)–(4) are satisfied are called *alternative*. A more general class of 8-dimensional alternative algebras was studied by Dickson. These algebras received the name Cayley-Dickson algebras.

In this and the following section (if this is not stated explicitly) for simplicity of language we will assume that the additive groups of the rings do not contain elements of order 2.

We next list some identical relations that hold in every alternative ring:

$$[(xy)z]y = x[(yz)y], \tag{5}$$

$$y[z(yx)] = [y(zy)]x, \tag{6}$$

$$(xy)(zx) = x[(yz)x]. \tag{7}$$

To prove relation (5) we notice that substitution of $y + z$ for y in equation (2) leads to the equation

$$[x, y, z] = -[x, z, y]. \tag{8}$$

Using equations (2) and (8) gives

$$\begin{aligned}
2x[(yz)y] &= x\big[\,2(yz)y + [z, y, y] - [y, z, y] - [y, y, z]\,\big] \\
&= x\big[\,(yz)y + (zy)y - zy^2 + y(zy) - y^2z + y(yz)\,\big] \\
&= [x(yz)]y + (xy)(yz) - [x, yz, y] - [x, y, yz] + [x(zy)]y + (xy)(zy) \\
&\quad - [x, zy, y] - [x, y, zy] + [x, z, y^2] + [x, y^2, z] - (xz)y^2 - (xy^2)z \\
&= \big[\,x(yz) + x(zy)\,\big]y + (xy)(yz + zy) - [(xz)y]z - [(xy)y]z \\
&= 2[(xy)z]y.
\end{aligned}$$

Thus equation (5) is proved, and for its proof we used only equation (2). From this it follows that equation (5) holds in any ring which satisfies equation (2), that is, in any so-called *right alternative* ring. The proofs of equations (6) and (7) are left to the reader.

3. Let us notice one property of alternative rings, which makes them close to associative rings. Let a and b be two elements of some alternative ring A, and let

D be the subring of the ring A generated by the elements a and b. It happens that the ring D is associative. To prove this proposition it is enough to show that any two elements of the ring D obtained by different parenthesizations of an associative monomial in a and b are equal.

Let c be some associative monomial as described. We denote by $\langle c\rangle$ the nonassociative monomial obtained from the monomial c by the following parenthesization: when $c = c_1a$ or $c = c_1b$ we let $\langle c\rangle = (\langle c_1\rangle)a$ or $\langle c\rangle = (\langle c_1\rangle)b$, respectively; and $\langle a\rangle = a$, $\langle b\rangle = b$. For example, $\langle a^2bab^2\rangle = ((((aa)b)a)b)b$. If d is a nonassociative monomial with some parenthesization, then we will denote by $\overline{d}$ the associative monomial obtained by removing the parentheses from d. The associativity of the ring D is equivalent to the equation $d = \langle\overline{d}\rangle$ holding where d is any nonassociative monomial in the generators a and b. The last equality, which is obvious if the degree of the monomial d in a and b is less than or equal to 3, will be proved by induction on the degree of d.

Let the degree of the monomial d be greater than 3: $d = d_1d_2$, $d_1 = a\langle\overline{d_3}\rangle$, and we assume that the equality to be proved holds for monomials with lower degree. Then we have the following cases:

$$\text{(i)}\qquad d_2 = \langle\overline{d_4}\rangle a, \quad d = (a\langle\overline{d_3}\rangle)(\langle\overline{d_4}\rangle a) = [a(\langle\overline{d_3}\rangle\langle\overline{d_4}\rangle)]a = \langle\overline{d}\rangle,$$

where we have used equation (7). If the monomial $\langle\overline{d_3}\rangle$ is empty, then the proof works using equation (4).

$$\text{(ii)}\qquad d_2 = (b\langle\overline{d_4}\rangle)b, \quad d = (a\langle\overline{d_3}\rangle)[(b\langle\overline{d_4}\rangle)b] = [(d_1b)\langle\overline{d_4}\rangle]b = \langle\overline{d}\rangle,$$

where equation (5) was used. Finally,

$$\begin{aligned}\text{(iii)}\quad d_2 &= (a\langle\overline{d_4}\rangle)b,\\ d &= (a\langle\overline{d_3}\rangle)[(a\langle\overline{d_4}\rangle)b]\\ &= -(a\langle\overline{d_3}\rangle)[b(a\langle\overline{d_4}\rangle)] + [(a\langle\overline{d_3}\rangle)(a\langle\overline{d_4}\rangle)]b + [(a\langle\overline{d_3}\rangle)b](a\langle\overline{d_4}\rangle)\\ &= -\langle\overline{d_5}\rangle + \langle\overline{d}\rangle + d_5,\end{aligned}$$

where we have used equation (8) and also the above-proved identities from cases (i) and (ii). Repeating (if necessary) the same transformation on d_5 and so on, we come in a finite number of steps to the identity which we are proving.

4. In spite of the noted closeness of alternative rings to associative rings, as of now there is no general method which allows us to prove identities in alternative rings. Each of the presently known such identities requires a separate and in some cases very difficult proof. This happens because as of now there is no known method to build constructively free alternative rings, so there is no known algorithm which solves the word problem in free alternative rings; that is, an algorithm which allows us, for every element of this ring written in terms of the generators, to determine if it is zero or not.

We mention the following interesting identity:

$$[\,(ab-ba)^2,\, c,\, d\,]\,(ab-ba)=0,$$

which was proved by Kleinfeld (see for example [67]) and which shows that in the free alternative ring there are zero divisors.

5. The study of alternative rings in general began with the study of alternative division rings, which in the theory of projective planes play the role of the so-called natural division rings of alternative planes (see [65]); that is, planes for which the little Desargues theorem holds.

In the works of L.A. Skornyakov [62, 63] a full description is given of alternative but not associative division rings. It happens that every such division ring is an algebra of dimension 8 over some field (a Cayley-Dickson algebra). Later and independently of Skornyakov this statement was proved by Bruck and Kleinfeld [8], but Kleinfeld [29] proved that even simplicity (that is, not having two-sided ideals) of an alternative but not associative ring implies that the ring is a Cayley-Dickson algebra.

If for an element a of some ring A there exists a natural number $n(a)$ such that $a^{n(a)}=0$ (with any parenthesization of the expression $a^{n(a)}$), then this element is called a *nilpotent* element. If all the elements in a ring (resp. ideal) are nilpotent, it is called a *nil-ring* (resp. *nil-ideal*).

Recently Kleinfeld [30] strengthened his results by proving that any alternative but not associative ring, in which the intersection of all the two-sided ideals is not a nil-ideal, is a Cayley-Dickson algebra over some field. Hence the class of alternative rings is much larger than the class of associative rings, but only outside the limits of the above-mentioned classes of rings.

6. Some attention has been given to right alternative rings (rings which satisfy identity (2)). Skornyakov [64] proved that every right alternative division ring is alternative. Kleinfeld [28] proved that for the alternativity of a right alternative ring it is sufficient that $[x,y,z]^2=0$ implies $[x,y,z]=0$. Smiley [68] analyzed the proof of Kleinfeld and noticed that it is sufficient to check only these cases: $x=y$, $x=yz-zy$, $x=(yz-zy)y$, $x=[y,y,z]$, or $z=wy$ and $x=[y,y,w]$ for some w. We know about the structure of free right alternative rings as little as we know about the structure of free alternative rings. The study of these rings is one of the main tasks of the theory of alternative rings.

It would be interesting to find out whether there are any identical relations which are not implied by (2)–(4) and are satisfied in the free alternative ring with three generators as, for example, the relation $(xy)z-x(yz)=0$ is satisfied by the free alternative ring with two generators.

Because alternative rings are close relatives of associative rings, we may ask of any statement which holds for associative rings whether it also holds for alternative rings. One such problem (the Kurosh problem) will be discussed in the next section.

San Soucie [51, 52] studied alternative and right alternative rings in characteristic 2 ($2x = 0$).

3. Jordan rings

1. Let A be an associative ring. If we set $a \circ b = ab + ba$, then with respect to addition and the operation $\circ$ the set of elements of the ring A becomes a ring which is in general nonassociative. We denote this ring by $A^{(+)}$. For an associative algebra B (or a Σ-operator ring) it is possible in a similar way to define an algebra $B^{(+)}$ over the same field (or a Σ-operator ring); for an algebra it is more convenient to use the operation $a \circ b = \frac{1}{2}(ab + ba)$. It is easy to check that in the ring $A^{(+)}$ the following identities hold:

$$a \circ b = b \circ a, \tag{9}$$

$$((a \circ a) \circ b) \circ a = (a \circ a) \circ (b \circ a). \tag{10}$$

Rings in which the multiplication satisfies (9) and (10) are called *J-rings* or *Jordan rings*.

It can happen that some subset of a ring, which is not a subring, becomes a Jordan ring under the operation $\circ$. As an example, consider the set of all real symmetric matrices of some fixed degree n. A Jordan ring which is isomorphic to a subring of some ring of the form $A^{(+)}$ is called a *special* Jordan ring. Special Jordan algebras can be defined in a similar way.

2. Not every Jordan ring and not every Jordan algebra is special. The classical example, that will be discussed below, of a non-special (often called exceptional) Jordan algebra of finite dimension belongs to Albert [5].

In the algebra R_8, which was discussed at the beginning of Section 2, for any element $s = (p, q)$ we set $\overline{s} = (\overline{p}, -q)$. In the set of all matrices of degree 3 with elements from the algebra R_8 we consider the subspace C_{27} of self-conjugate matrices (that is, matrices which do not change when the elements are conjugated and the matrix is transposed). It is possible to check that the set C_{27} with respect to addition, the usual multiplication of real numbers, and the operation $s \circ t = \frac{1}{2}(s \cdot t + t \cdot s)$ is a Jordan algebra of dimension 27 over the field of real numbers.

Let x be an element of the algebra R_8. Denote by x_{ij} the matrix S from the algebra C_{27} in which $s_{ij} = \overline{x}$ and $s_{ji} = x$ and all other entries are zero; by e denote the identity of the algebra R_8.

Assume that there exists an associative algebra $\mathfrak{A}$, such that the Jordan algebra $\mathfrak{A}^{(+)}$ has a subalgebra C'_{27} isomorphic to the algebra C_{27}. For simplicity in what follows we will identify the algebra C'_{27} with the algebra C_{27}. If $s, t \in C_{27}$ then it is obvious that $s \cdot t + t \cdot s = st + ts$ where st is the product of the elements s and t in the algebra $\mathfrak{A}$. The last observation allows us to easily verify the following equations:

$$e_{ij}^2 = e_{ij}e_{ij} = e_{ij} \cdot e_{ij} = e_{ii} + e_{jj}, \tag{11}$$

$$e_{ii}x_{ij} + x_{ij}e_{ii} = e_{jj}x_{ij} + x_{ij}e_{jj} = x_{ij}, \tag{12}$$
$$e_{kk}x_{ij} + x_{ij}e_{kk} = 0 \text{ (for } k \neq i, j), \tag{13}$$
$$x_{12}y_{23} + y_{23}x_{12} = (x \cdot y)_{13}, \tag{14}$$
$$x_{12}y_{13} + y_{13}x_{12} = (\overline{x} \cdot y)_{23}, \tag{15}$$
$$x_{13}y_{23} + y_{23}x_{13} = (x \cdot \overline{y})_{12}. \tag{16}$$

From equation (13) we have

$$e_{kk}(e_{kk}x_{ij} + x_{ij}e_{kk}) = (e_{kk}x_{ij} + x_{ij}e_{kk})e_{kk} = 0,$$

and because of $e_{kk}^2 = e_{kk}$, it easily follows that

$$e_{kk}x_{ij} = x_{ij}e_{kk} = 0 \ (k \neq i, j). \tag{17}$$

Setting $f_{ij} = e_{ii} + e_{jj}$, from the obvious equalities

$$f_{ij}x_{ij} + x_{ij}f_{ij} = 2x_{ij}, \quad 2f_{ij}x_{ij} = f_{ij}x_{ij} + f_{ij}x_{ij}f_{ij},$$

we easily obtain

$$f_{ij}x_{ij} = f_{ij}x_{ij}f_{ij} = x_{ij}f_{ij} = x_{ij}. \tag{18}$$

Finally,

$$e_{ii}y_{ij}e_{ii} = e_{jj}y_{ij}e_{jj} = 0, \tag{19}$$

because, for example,

$$e_{ii}y_{ij}e_{ii} = e_{ii}(y_{ij} - e_{ii}y_{ij}) = 0,$$

(equation (12)).

If $x \in R_8$ then we set $x' = e_{11}x_{12}e_{12}$. We show that the map $x \to x'$ is a homomorphism of the algebra R_8 into the algebra $\mathfrak{A}$. Clearly $(x + y)' = x' + y'$. From equations (14)–(17) it follows that

$$\begin{aligned}(x \cdot y)' &= e_{11}(x \cdot y)_{12}e_{12} = e_{11}(x_{13}\overline{y}_{23} + \overline{y}_{23}x_{13})e_{12} = e_{11}x_{13}\overline{y}_{23}e_{12}\\ &= e_{11}(x_{12}e_{23} + e_{23}x_{12})\overline{y}_{23}e_{12} = e_{11}x_{12}e_{23}\overline{y}_{23}e_{12}\\ &= e_{11}x_{12}e_{23}(y_{12}e_{13} + e_{13}y_{12})e_{12}.\end{aligned}$$

On the other hand,

$$\begin{aligned}y_{12}e_{13}e_{12} &= y_{12}e_{13}f_{13}e_{12} = y_{12}e_{13}e_{11}e_{12} = (\overline{y}_{23} - e_{13}y_{12})e_{11}e_{12}\\ &= -e_{13}y_{12}e_{11}e_{12} = -e_{13}f_{13}y_{12}e_{11}e_{12} = -e_{13}e_{11}y_{12}e_{11}e_{12} = 0,\\ e_{23}e_{13}y_{12} &= e_{23}e_{13}f_{12}y_{12} = e_{23}e_{13}e_{11}y_{12} = (e_{12} - e_{13}e_{23})e_{11}y_{12} = e_{12}e_{11}y_{12}.\end{aligned}$$

Making the corresponding substitution in the expression $(x \cdot y)'$ we get

$$(x \cdot y)' = e_{11}x_{12}e_{12}e_{11}y_{12}e_{12} = x'y'.$$

Because of the absence of proper ideals in the algebra R_8, and also because $e' = e_{11}e_{12}e_{12} = e_{11}f_{12} = e_{11} \neq 0$, we conclude that the algebra R_8 is isomorphic to a subalgebra of the associative algebra $\mathfrak{A}$, which contradicts the nonassociativity of the algebra R_8. This contradiction shows that there is no associative algebra $\mathfrak{A}$ with the required properties.

3. It would be natural to assume that special Jordan algebras satisfy some system of identities which do not follow from (9) and (10).

At the present time such identities have not been found. Moreover, every attempt to characterize special Jordan rings with the help of any system of identities must be completely unsuccessful, because Cohn [9] gave many examples of *non-special Jordan algebras which are homomorphic images of special Jordan algebras*. It was also shown by Cohn that *any homomorphic image of a special Jordan algebra with two generators is also a special Jordan algebra*.

Let $\mathfrak{B}$ be some Jordan ring. We define by the formula

$$\{a, b, c\} = (ab)c + (bc)a - (ca)b,$$

a ternary operation on the set of elements of the ring $\mathfrak{B}$. It is easy to check that if $\mathfrak{B}$ is a special Jordan ring then we have the identity

$$\{a, b, a\}^2 = \{a, \{b, a^2, b\}, a\}. \tag{20}$$

Hall [15] and Harper [17] independently proved that (20) holds for any Jordan ring. In the author's work [58] it was proved that *every Jordan ring on two generators is special*. From this result it easily follows that any identity which involves, like (20), only two variables and which holds in any special Jordan ring, also holds in any Jordan ring. This result was recently reproved by Jacobson and Paige [26].

At present it is still not known whether the identities

$$\{\{a, x, a\}, x, \{a, x, b\}\} = \{\{\{a, x, a\}, x, b\}, x, a\}, \tag{21}$$

$$\{\{x, b, x\}, a, \{x, b, x\}\} = \{x, \{b, \{x, a, x\}, b\}, x\}, \tag{22}$$

which hold in any special Jordan ring, also hold in any Jordan ring. These identities were pointed out by Jacobson; he proved in [27] that they hold in C_{27}.

Jacobson proposed the question: Does there exist a Jordan algebra which is not a homomorphic image of a special Jordan algebra?

Albert [6] proved that the algebra C_{27} is not a homomorphic image of any special Jordan algebra *of finite dimension*.

The above-mentioned problem is equivalent to the following: Is the free Jordan ring on more than two generators special or not? A positive answer would trivially imply the solution of the word problem for a free Jordan ring, but still it would not imply a solution of the problem of finding a basis for the free Jordan algebra on three or more generators (see Cohn [9]).

4. If, on the set of elements of a right-alternative ring T, we define the operation $a \circ b = ab + ba$, then it is easy to show that in this case the ring $T^{(+)}$ will be a Jordan ring. However, it turns out that the class of all Jordan rings that can be obtained in this way is equal to the class of all special Jordan rings. Indeed, the mapping $f\colon x \to R_x$ of elements of the ring T to the associative ring, generated in the ring T^* of all endomorphisms of the additive group of the ring T by right multiplications R_x ($aR_x = ax$), is a homomorphism of the ring $T^{(+)}$ onto some subring of the special Jordan ring $T^{*(+)}$. The mapping f will be an isomorphism

if we initially extend the ring T by an identity element (after which the extended ring remains right alternative).

The possibility of associating with every right alternative ring an associative ring (in general, not unique), through the corresponding (special) Jordan ring, turns out to be very useful in the study of right alternative rings, and so also in the study of alternative rings.

Using this method, the author proved in [59, 60] that all the results obtained as of the present towards solving the Kurosh problem [38] (or its special case, the Levitzky problem) for associative algebras (or rings) also hold for alternative algebras (or rings) and for special Jordan algebras (or Jordan rings). Let us formulate one of them:

An alternative ring D with a finite number of generators and the identical relation $x^n = 0$ is nilpotent, that is, there exists a natural number N such that any product of N elements of D is zero.

The closest generalization of Jordan rings are the so-called noncommutative Jordan rings, the study of which was started by Schafer. The natural place for them in the present article is in the last section.

4. Lie rings

1. A ring which satisfies the identical relations

$$x^2 = 0, \tag{23}$$

$$(xy)z + (yz)x + (zx)y = 0, \tag{24}$$

is called a *Lie ring*.

In this article we completely avoid the discussion of Lie algebras of finite dimension, an exposition of which would be more natural in connection with the theory of Lie groups.

If, in an associative ring A we define a new operation by the equation $a \cdot b = ab - ba$, then the set of elements of A will be a Lie ring with this operation and addition. We denote this new ring by $A^{(-)}$. Birkhoff [7] and Witt [71] independently proved that *every Lie algebra is isomorphic to a subalgebra of some algebra of the form $A^{(-)}$*. If we use the terminology of Jordan rings, then we can say that every Lie ring is special.

Lazard [42] and Witt [72] studied representations of Σ-operator Lie rings in Σ-operator associative rings. The existence of such a representation was proved by them in the case when Σ is a principal ideal domain, and in particular for Lie rings without operators. The example constructed by the author in [57] shows that there exist non-representable Σ-operator Lie rings which do not have elements of finite order in the additive group.

I.D. Ado [1, 2] proved that any finite-dimensional Lie algebra over the field of complex numbers can be represented in a finite-dimensional associative algebra.

Later Harish-Chandra [16] and Iwasawa [24] proved that Ado's theorem holds for any finite-dimensional Lie algebra.

We mention the cycle of works of Herstein [19]–[21], which, in essence, belong to the theory of associative rings and are dedicated to studying the ring $A^{(-)}$ under various assumptions on the ring A.

2. There are interesting relations between the theory of Lie rings and the theory of groups.

Let K be the ring of formal power series with rational coefficients in the noncommutative variables x_i $(i = 1, 2, \ldots)$. Magnus [45] proved that the elements $y_i = 1 + x_i$ of the ring K generate a free subgroup G of the multiplicative group of the ring K, and that every element of the subgroup G_n (the n-th commutator subgroup[5]) has the form $1+\ell_n+\omega$, where ℓ_n is some homogeneous Lie polynomial (with respect to the operations $a \cdot b$ and $a + b$) of degree n in the generators x_i, and ω is a formal power series in which all the terms have degree greater than n. Then because of known criteria [11, 12, 44] which allow us to determine whether a given polynomial is a Lie polynomial, the above mentioned representation of the free group allows us to determine whether any given element lies in one term or another of the lower central series.

The elements $z_i = e^{x_i}$ of the ring K also generate a free group [46] and if $e^x e^y = e^t$ then t is a power series, the terms of which are homogeneous Lie polynomials in x and y [18].

The relations which exist between the theory of groups and the theory of Lie rings allow us to obtain group-theoretical results from statements proved for Lie rings. For example, Higman [23] proved nilpotency (see the definition below) of any Lie ring which has an automorphism of prime order without nonzero fixed points. This statement allowed him to prove nilpotency of finite solvable groups which have an automorphism satisfying the analogous conditions.

Earlier Lazard [43] studied nilpotent groups using extensively the apparatus of Lie ring theory.

3. We consider one more circle of questions which are relevant to the theory of groups.

A Lie ring L is called a ring satisfying the *n-th Engel condition* if for any elements x and y we have the relation

$$\{\cdots[(x\underbrace{y)y]\cdots\}y}_{n\ y\text{'s}} = 0.$$

We introduce the following notation:

$$L = L^1 = L^{(1)}, \qquad L^k = L^{k-1}L, \qquad L^{(k)} = L^{(k-1)}L^{(k-1)}.$$

A Lie ring is called *nilpotent* (resp. *solvable*) if there exists a natural number m such that $L^m = 0$ (resp. $L^{(m)} = 0$).

[5]That is, the n-th term of the lower central series. [Translators]

With some restrictions on the additive group, Higgins [22] proved that solvable rings satisfying the n-th Engel condition are nilpotent. Then Cohn [10] constructed an example of a solvable Lie ring whose additive group is a p-group and which satisfies the p-th Engel condition, but is not nilpotent. For Lie rings with a finite number of generators and some restrictions on the additive group, A.I. Kostrikin [37] proved that the Engel condition implies nilpotency. This result is especially interesting because from it follows the positive solution of the group-theoretical restricted Burnside problem for p-groups with elements of prime order [35, 36].

An element a in a Lie algebra L is called *algebraic* if the endomorphism $R_a : x \mapsto xa$ generates a finite-dimensional subalgebra in the (associative) algebra of all endomorphisms of the additive group of the algebra L.

It is not known whether there exists a Lie algebra with a finite number of generators and infinite dimension in which every element is algebraic. This problem is analogous to the famous Kurosh problem [38] for associative algebras.

We mention one easier but unsolved problem. Let the Lie algebra L be such that any two elements belong to a subalgebra, the dimension of which does not exceed some fixed number. Does it follow from this that every finite subset of the algebra L belongs to some subalgebra of finite dimension?

4. An important role in the theory of Lie rings is played by free Lie rings. In contrast to free alternative rings and free Jordan rings, free Lie rings have been thoroughly studied. M. Hall [14] pointed out a method for constructing a basis of a free Lie algebra; E. Witt [71] found a formula for computing the rank of the homogeneous modules in a free Lie algebra on a finite number of generators.

We briefly describe one constructive method of building a free Lie ring. Let $\mathfrak{A}$ be a free associative Σ-operator ring with some set $R = \{a_i\}$ $(i = 1, 2, \ldots, k)$ as a set of free generators. It turns out that [61] the elements of the set R generate in the Lie ring $\mathfrak{A}^{(-)}$ a free Lie ring L for which they are free generators. We order the elements of the set R in some way, and then we order lexicographically every set of (associative) monomials of the same degree in the elements of the set R. Let W be the set of all monomials w such that $w = w_1 w_2 > w_2 w_1$, for any representation of the monomial w as a product of two monomials w_1 and w_2. Let $v \in W$ with $v = v_1 v_2$ where v_1 is a monomial from W of minimal degree such that $v_2 \in W$. We parenthesize the monomial v in the following way: $v = (v_1)(v_2)$, and we repeat this method of parenthesization on the monomials v_1 and v_2. The set of nonassociative monomials obtained from the elements of the set W by this method of parenthesization with the operation interpreted as $a \cdot b = ab - ba$ will be a basis of the ring L.

The author in [56] and independently Witt in [73] proved that *any subalgebra of a free Lie algebra is again free*. This theorem is analogous to the theorem of Kurosh mentioned in Section 1 for subalgebras of free algebras.

Using the above method of constructing a free Lie algebra allowed the author in [61] to prove that *any Lie algebra of finite or countable dimension can be embedded in a Lie algebra with two generators.*

Analogous theorems about embedding of arbitrary algebras and of associative rings were proved respectively by A.I. Zhukov [74] and A.I. Malcev [48].

5. The study of Lie algebras over fields of prime characteristic has led to the discussion of so-called restricted Lie algebras.

In a restricted Lie algebra over a field of characteristic $p > 0$ an additional unary operation is defined with some natural axioms which are typical of the usual (associative) p-th power. Jacobson [25] proved a theorem for restricted Lie algebras analogous to the Birkhoff-Witt theorem, which in this case already includes a theorem similar to Ado's theorem.

6. Recently A.I. Malcev [49] considered a class of binary-Lie rings, which are related to Lie rings in a way analogous to the way alternative rings are related to associative rings. A ring is called *binary-Lie* if every two elements lie in some Lie subring.

A.T. Gainov [13] proved that in the case of a ring without elements of order 2 in the additive group, for a ring to be binary-Lie it is sufficient that these identities hold:

$$x^2 = [(xy)y]x + [(yx)x]y = 0.$$

If, on the set of elements of some alternative ring D, we define the above described operation $a \cdot b = ab - ba$, then in the ring $D^{(-)}$, as was shown by A.I. Malcev [49], these relations hold identically:

$$x^2 = [(x \cdot y) \cdot z] \cdot x + [(y \cdot z) \cdot x] \cdot x + [(z \cdot x) \cdot x] \cdot y - (x \cdot y) \cdot (x \cdot z) = 0. \quad (25)$$

Rings satisfying the identities (25) are called by A.I. Malcev *Moufang-Lie* rings, and he also showed that the class of Moufang-Lie rings[6] without elements of additive order 6 is properly contained in the class of binary-Lie rings.

Recently Kleinfeld [31] proved that *a Moufang-Lie ring M without elements of additive order 2 which has an element a such that $aM = M$ is a Lie ring.* A corresponding result can clearly be formulated in the language of alternative rings.

The problem of the truth of a theorem, similar to the Birkhoff-Witt theorem, connecting the theory of Moufang-Lie rings with the theory of alternative rings remains open.

5. Some wider classes of rings

1. As was shown earlier, a ring is alternative if and only if every two elements lie in some associative subring.

Algebraists working in the theory of rings have been attracted for a long time to the wider class of rings with associative powers. A ring is called *power-associative*

[6]Now called Malcev rings. [Translators]

if every element lies in some associative subring. It is not difficult to check that all the classes of rings discussed in the present article are power-associative.

In the case of rings for which the additive group has no torsion, Albert [3] has shown that the identities $x^2x = xx^2$ and $(x^2x)x = x^2x^2$ are sufficient to guarantee power-associativity. This result was recently given another proof by A.T. Gainov [13]. Albert proved in [4] that if in the additive group of a ring there are no elements of order 30 then power-associativity follows from the identities

$$(xy)x = x(yx) \quad \text{and} \quad (x^2x)x = x^2x^2.$$

For rings of small characteristic some sufficient conditions for power-associativity were found by Kokoris [32, 33].

2. We mention one method for studying power-associative rings which has been used extensively in the works of Albert.

Let A be a commutative power-associative ring in which the equation $2x = a$ has a unique solution for every $a \in A$ and which contains an idempotent e ($e^2 = e$). Then it turns out that every element $b \in A$ has a unique representation in the form $b = b_0 + b_1 + b_{1/2}$ where $b_\lambda e = \lambda b_\lambda$; that is, the ring A can be represented as the direct sum of three modules $A = A_0 + A_1 + A_{1/2}$, the study of which gives some information about the ring A. If the ring A is noncommutative, then we can study the commutative ring $A^{(+)}$ which is obtained from the ring A with the help of the new multiplication $a \circ b = \frac{1}{2}(ab + ba)$. It is obvious that the subrings generated by a single element in the rings A and $A^{(+)}$ are the same. Therefore the ring $A^{(+)}$ is again power-associative.

Another very wide class of rings is the class of flexible rings; that is, rings which satisfy the identical relation (4). All the rings discussed in this article, except for right alternative rings, are from this class.

No significant results, which would go beyond the class of algebras of finite dimension, have been obtained for flexible rings.

3. It would be natural to expect a deeper study of flexible power-associative rings.

However, comparatively recently Schafer [53] began the study of the class of so-called noncommutative Jordan rings, defined by identities (4) and (10), which is slightly narrower than the class of flexible power-associative rings, but contains most of the rings mentioned above.

The study of this class of rings at the present time is restricted to the theory of algebras of finite dimension (see [54, 55, 34]); however, we can hope that in the future a sufficiently interesting theory of this class of rings will be constructed.

In conclusion, we mention one very wide class, the so-called *power-commutative rings*; that is, rings in which every element belongs to a commutative (but not necessarily associative) subring. This class includes not only the flexible rings, but also the power-associative rings. Unfortunately, at this point in time, we do not even know whether this class can be defined by a finite system of identities.

References

[1] I.D. Ado, *On representations of finite continuous groups using linear substitutions*, Izv. Kaz. fiz.-matem. ob-va 7 (1934–35) 1–43.

[2] I.D. Ado, *Representation of Lie algebras by matrices*, Uspekhi Mat. Nauk II (1947) 159–173.

[3] A.A. Albert, *On the power-associativity of rings*, Summa Brasil. Math. 2 (1948) 21–33.

[4] A.A. Albert, *Power-associative rings*, Trans. Amer. Math. Soc. 64 (1948) 552–593.

[5] A.A. Albert, *A note on the exceptional Jordan algebra*, Proc. Nat. Acad. Sci. USA 36 (1950) 372–374.

[6] A.A. Albert, *A property of special Jordan algebras*, Proc. Nat. Acad. Sci. USA 42 (1956) 624–625.

[7] G. Birkhoff, *Representability of Lie algebras and Lie groups by matrices*, Ann. of Math. 38 (1937) 526–532.

[8] R.N. Bruck, E. Kleinfeld, *The structure of alternative division rings*, Proc. Amer. Math. Soc. 2 (1951) 878–890.

[9] P.M. Cohn, *On homomorphic images of special Jordan algebras*, Canad. Journ. Math. 6 (1954) 253–264.

[10] P.M. Cohn, *A non-nilpotent Lie ring satisfying the Engel condition and a non-nilpotent Engel group*, Proc. Cambridge Philos. Soc. 51 (1955) 401–405.

[11] E.B. Dynkin, *Computation of the coefficients in the Campbell-Hausdorf formula*, Doklady Akad. Nauk USSR 57 (1947) 323–326.

[12] K.O. Friedrichs, *Mathematical aspects of the quantum theory of fields, V*, Comm. Pure Appl. Math. 6 (1953) 1–72.

[13] A.T. Gainov, *Identitical relations for binary-Lie rings*, Uspekhi Mat. Nauk XII (1957) 141–146.

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

[15] M. Hall, *An identity in Jordan rings*, Proc. Amer. Math. Soc. 42 (1956) 990–998.

[16] Harish-Chandra, *Faithful representations of Lie algebras*, Ann. of Math. 50 (1949) 68–76.

[17] L.R. Harper, *A proof of an identity for Jordan algebras*, Proc. Nat. Acad. Sci. USA 42 (1956) 137–139.

[18] E. Hausdorf, *Die simbolische Exponentialformel in der Gruppentheorie*, Bericht d. König. Sächs. Ges. d. wiss. Math.-Phis. Klasse 58 (1906) 19–48.

[19] I.N. Herstein, *On the Lie and Jordan rings of a simple associative ring*, Amer. Journ. Math. 77 (1955) 279–285.

[20] I.N. Herstein, *The Lie ring of a simple associative ring*, Duke Math. Journ. 22 (1955) 471–476.

[21] I.N. Herstein, *Lie and Jordan systems in simple rings with involution*, Amer. Journ. Math. 78 (1956) 629–649.

[22] P.J. Higgins, *Lie rings satisfying the Engel condition*, Proc. Cambridge Philos. Soc. 50 (1954) 8–15.

[23] G. Higman, *Groups and rings having automorphisms without non-trivial fixed elements*, Journ. London Math. Soc. 32 (1957) 321–332.

[24] K. Iwasawa, *On the representation of Lie algebras*, Jap. Journ. Math. 19 (1948) 405–426.

[25] N. Jacobson, *Restricted Lie algebras of characteristic p*, Trans. Amer. Math. Soc. 50 (1941) 15–25.

[26] N. Jacobson, L.J. Paige, *On Jordan algebras with two generators*, Journ. Math. and Mech. 6 (1957) 895–906.

[27] N. Jacobson, *Jordan algebras*, Report of a Conference on Linear Algebras (1957) 12–19.

[28] E. Kleinfeld, *Right alternative rings*, Proc. Amer. Math. Soc. 4 (1953) 939–944.

[29] E. Kleinfeld, *Simple alternative rings*, Ann. of Math. 58 (1953) 544–547.

[30] E. Kleinfeld, *Generalization of a theorem on simple alternative rings*, Portugal. Math. 14, 3–4 (1955) 91–94.

[31] E. Kleinfeld, *A note on Moufang-Lie rings*, Proc. Amer. Math. Soc. (1958) 72–74.

[32] L.A. Kokoris, *New results on power-associative algebras*, Trans. Amer. Math. Soc. 77 (1954) 363–373.

[33] L.A. Kokoris, *Power-associative rings of characteristic two*, Proc. Amer. Math. Soc. 6 (1955) 705–710.

[34] L.A. Kokoris, *Some nodal noncommutative Jordan algebras*, Proc. Amer. Math. Soc. 9 (1958) 164–166.

[35] A.I. Kostrikin, *On the relation between periodic groups and Lie rings*, Izv. Akad. Nauk USSR 21 (1957) 289–310.

[36] A.I. Kostrikin, *Lie rings satisfying the Engel condition*, Izv. Akad. Nauk USSR 21 (1957) 515–540.

[37] A.I. Kostrikin, *On the Burnside problem*, Doklady Akad. Nauk USSR 119 (1958) 1081–1084.

[38] A.G. Kurosh, *Problems in the theory of rings related to the problem of Burnside on periodic groups*, Izv. Akad. Nauk USSR 5 (1941) 233–247.

[39] A.G. Kurosh, *Free nonassociative algebras and free products of algebras*, Matem. Sb. 20, 62 (1947) 239–262.

[40] A.G. Kurosh, *The current state of the theory of rings and algebras*, Uspekhi Mat. Nauk VI, 2 (1951) 3–15.

[41] A.G. Kurosh, *Nonassociative free sums of algebras*, Mat. Sbornik 37, 79 (1955) 251–264.

[42] M. Lazard, *Sur les algèbres enveloppantes universelles des certaines algèbres de Lie*, Publ. Sci. de l'Univ. d'Alger, Ser. A 1 (1954) 281–294.

[43] M. Lazard, *Sur les groupes nilpotents et les anneaux de Lie*, Ann. Sci. Ec. Norm. Sup. 71 (1954) 101–190.

[44] R.C. Lyndon, *A theorem of Friedrichs*, Michigan Math. Journ. 3 (1955–56) 27–29.

[45] W. Magnus, *Über Beziehungen zwischen höheren Kommutatoren*, Journ. reine und angew. Math. 177 (1937) 105–115.

[46] W. Magnus, *Über Gruppen und zugeordnete Liesche Ringe*, Journ. reine und angew. Math. 182 (1940) 142–149.

[47] A.I. Malcev, *On the decomposition of an algebra into the direct sum of the radical and a semi-simple subalgebra*, Doklady Akad. Nauk USSR 36 (1942) 46–50.

[48] A.I. Malcev, *On a representation of nonassociative rings*, Uspekhi Mat. Nauk VII, 1 (1952) 181–185.

[49] A.I. Malcev, *Analytic loops*, Mat. Sbornik 36 (1955) 569–576.

[50] I.N. Sanov, *Investigations into the relation between periodic groups of prime period and Lie rings*, Izv. Akad. Nauk USSR 16 (1952) 23–58.

[51] R.L. San Soucie, *Right alternative division rings of characteristic 2*, Proc. Amer. Math. Soc. 6 (1955) 291–296.

[52] R.L. San Soucie, *Right alternative rings of characteristic two*, Proc. Amer. Math. Soc. 6 (1955) 716–719.

[53] R.D. Schafer, *Non-commutative Jordan algebras of characteristic zero*, Proc. Amer. Math. Soc. 6 (1955) 472–475.

[54] R.D. Schafer, *On non-commutative Jordan algebras*, Proc. Amer. Math. Soc. 9 (1958) 110–117.

[55] R.D. Schafer, *Restricted non-commutative Jordan algebras of characteristic p*, Proc. Amer. Math. Soc. 9 (1958) 141–144.

[56] A.I. Shirshov, *Subalgebras of free Lie algebras*, Mat. Sbornik 33 (1953) 441–452.

[57] A.I. Shirshov, *On the representation of Lie rings in associative rings*, Uspekhi Mat. Nauk VIII (1953) 173–175.

[58] A.I. Shirshov, *On special J-rings*, Mat. Sbornik 38 (1956) 149–166.

[59] A.I. Shirshov, *On some nonassociative nilrings and algebraic algebras*, Mat. Sbornik 41 (1957) 381–394.

[60] A.I. Shirshov, *On rings with identical relations*, Mat. Sbornik 43 (1957) 277–283.

[61] A.I. Shirshov, *On free Lie rings*, Mat. Sbornik 45 (1958) 113–122.

[62] L.A. Skornyakov, *Alternative division rings*, Ukr. Matem. Zhurn. 2, 1 (1950) 70–85.

[63] L.A. Skornyakov, *Alternative division rings of characteristic* 2 *and* 3, Ukr. Matem. Zhurn. 2, 3 (1950) 94–99.

[64] L.A. Skornyakov, *Right-alternative division rings*, Izv. Akad. Nauk USSR 15 (1951) 177–184.

[65] L.A. Skornyakov, *Projective planes*, Uspekhi Mat. Nauk VI, 6 (1951) 112–154.

[66] L.A. Skornyakov, *Representation of nonassociative rings in associative rings*, Doklady Akad. Nauk USSR 102, 1 (1955) 33–35.

[67] M.F. Smiley, *Kleinfeld's proof of the Bruck-Kleinfeld-Skornyakov theorem*, Math. Ann. 134 (1957) 53–57.

[68] M.F. Smiley, *Jordan homomorphisms and right alternative rings*, Proc. Amer. Math. Soc. 8 (1957) 668–671.

[69] Yu.I. Sorkin, *Rings as sets with one operation which satisfy only one relation*, Uspekhi Mat. Nauk XII, 4 (1957) 357–362.

[70] Liu-Shao Syue, *On decomposition of locally finite algebras*, Mat. Sbornik 39 (1956) 385–396.

[71] E. Witt, *Treue Darstellung Liescher Ringe*, Journ. reine und angew. Math. 177 (1937) 152–160.

[72] E. Witt, *Treue Darstellung beliebiger Liescher Ringe*, Collect. Math. 6 (1953) 107–114.

[73] E. Witt, *Die Unterringe der freien Liescher Ringe*, Mat. Zeitschr. 64 (1956) 195–216.

[74] A.I. Zhukov, *Complete systems of defining relations in nonassociative algebras*, Mat. Sbornik 27, 69 (1950) 267–280.

Some Algorithmic Problems for ε-algebras

A.I. Shirshov

Introduction

The word problem[1], stated relative to one or another algebraic system, has attracted the attention of many mathematicians. In the works of A.A. Markov [1] and E. Post [3] it was proved for the first time that there exist algebraic systems (semigroups) with undecidable word problem. The most significant achievement in this direction is the result of P.S. Novikov [2] that establishes undecidability of the word problem for groups. In 1950, A.I. Zhukov [5], while studying free nonassociative algebras, established that in the case in which one does not assume that the algebra satisfies any identical relation (for instance, associativity) the word problem (as well as some other algorithmic problems) is decidable. From the results obtained for semigroups, it easily follows that the word problem is undecidable for associative algebras.

The above-mentioned facts show that it is of interest to discover classes of algebras defined by identical relations for which the word problem or some other algorithmic problems are decidable. In the present work, the word problem is solved for commutative and anticommutative algebras (ε-algebras). Moreover, in these cases, the more general membership problem is solved, and a theorem is proved that is analogous to a known theorem on freeness in group theory.

1. The word problem

In the study of commutative and anticommutative algebras, we will for brevity use the terminology introduced in the work [4]. Hence, commutative and anticommutative algebras will be called respectively C-algebras and AC-algebras. The term ε-algebras with $\varepsilon = C$ or $\varepsilon = AC$ will be used when there is no need to distinguish

Sibirsk Mat. Zh. 3, (1962), no. 1, 132–137.

[1]Literally, "the problem of identity". [Translators]

the two cases. In [4] the definition of ε-regular words is given, and it is shown that they form a basis of the free ε-algebra. This result will also be used in the sequel without further mention.

Let E be the free ε-algebra over some field P (fixed once and for all), and let $R = \{a_\alpha\}$, $\alpha \in I$, be a set of free generators. We choose in E an arbitrary finite set of elements S and denote by $\langle S\rangle$ the ideal generated in E by S. To solve the word problem in this case means to provide an algorithm that allows us, for an arbitrary finite set S and an arbitrary element $a \in E$, to determine whether or not a belongs to $\langle S\rangle$.

The definition of ε-regular words requires that some ordering be fixed. In the sequel we will make the convention that, given two ε-regular words $u = u_1u_2$ and $v = v_1v_2$ of equal length ≥ 2, the greater word is either the one with greater first factor (u_1 or v_1), or if these are equal, then the one with greater second factor (u_2 or v_2). With respect to this ordering, we will speak of the leading term $\overline{a}$ of any element a in the algebra E.

The concept of a subword of a nonassociative word is sufficiently well known. Formally, it can be defined (by induction) on the word length, for example as follows.

Definition 1. Let u be a word of length ≥ 2 with $u = u_1u_2$. Then u, u_1, u_2 and the subwords of u_1 and u_2 are called *subwords* of u.

Definition 2. A set S of elements of E is called *reduced* if no element of S has a leading term which is a subword of the leading term of another element of S, and all the coefficients of the leading terms are equal to 1.

We now prove a few auxiliary results.

Lemma 1. *Let S be a finite set of elements of E. Then there exists a reduced finite set S' such that $\langle S'\rangle = \langle S\rangle$.*

Proof. In the expression of the elements of S, there occurs only a finite subset R' of elements of R. Let s_i, $i = 1, 2, \ldots, n$, be the elements of S, and let $\overline{s}_i$ be the leading term of s_i; then obviously we may assume that the coefficients of the leading terms of the elements of S are equal to 1. The symbol $\Sigma = (\overline{s}_1, \overline{s}_2, \ldots, \overline{s}_n)$ where $\overline{s}_i \leq \overline{s}_j$ if $i > j$ will be called the *type* of the set S, and the number n will be called the *length* of the type.

The set of all possible types that correspond to finite subsets of E, the expressions of whose elements only involve elements from R', will be ordered as follows: if the lengths of the types are equal then the order is lexicographical, and shorter types precede longer types.

Suppose that the finite set S is not reduced, i.e., the leading term $\overline{s}_j$ of some element $s_j \in S$ is a subword of the leading term $\overline{s}_i$ of an element $s_i \in S$, $i \neq j$. Then obviously there exists an element t_j of the ideal $\langle s_j\rangle$ such that $\overline{s}_i = \overline{t}_j$ and hence the leading term $\overline{d}_i$ of the element $d_i = s_i - t_j$ will be smaller than the word $\overline{s}_i$. Denote by S_1 the set obtained from S by replacing the element s_i by the

element d_i. Obviously $\langle S\rangle = \langle S_1\rangle$ and the type of S_1 is smaller than the type of S. The proof is complete since any decreasing sequence of types must terminate. □

Lemma 2. *An element $t \in E$ lies in the ideal $\langle S\rangle$, where $S = \{s_i\}$, $i = 1, 2, \ldots, n$, is a finite reduced set, only if at least one of the words $\overline{s}_i$, $i = 1, 2, \ldots, n$, is a subword of $\overline{t}$.*

Proof. If $t \in \langle S\rangle$ then obviously t can be represented as a linear combination of products d_i, $i = 1, 2, \ldots, m$, of one of the elements[2] s_{k_i} of S and some number of ε-regular words. Here we may assume that each $\overline{d}_i$ is an ε-regular word that has a subword $\overline{s}_{k_i}$, and replacing this subword by s_{k_i} turns $\overline{d}_i$ into d_i.

The last statement is obvious if $\varepsilon = C$, but it requires additional considerations if $\varepsilon = AC$. In this second case, one should look at products of the form $s_i\overline{s}_i$. But then, by virtue of the equation

$$s_i\overline{s}_i = s_i[s_i - (s_i - \overline{s}_i)] = -s_i(s_i - \overline{s}_i),$$

it is clear that in this case also the required representation is possible. In the more general case of the expression $\sigma_i\overline{\sigma}_i$, where $\overline{\sigma}_i$ is an AC-regular word with a distinguished subword $\overline{s}_{k_i}$ satisfying the above conditions, the argument is similar.

Among the ε-regular words $\overline{d}_i$, $i = 1, 2, \ldots, m$, we select the maximal. If this word is unique, then the lemma is proved. Assume now that the maximal word $\overline{d}_i$ is equal to the word $\overline{d}_j$. Since S is reduced, each of the subwords $\overline{s}_{k_i}$, $\overline{s}_{k_j}$ of the word $\overline{d}_j$ does not occur as a subword of the other in the expression of the word $\overline{d}_j$ (although they can be equal[3]). Therefore, without loss of generality, we may assume that

$$\overline{d}_j = b_1b_2\cdots b_{p_j}\overline{s}_{k_i}c_1c_2\cdots c_{q_j}\overline{s}_{k_j}f_1f_2\cdots f_{r_j},$$

where parentheses are placed in a certain way and all b, c, f are ε-regular words. By virtue of the equation

$$\begin{aligned} d_j = {} & b_1b_2\cdots b_{p_j}s_{k_i}c_1c_2\cdots c_{q_j}\overline{s}_{k_j}f_1f_2\cdots f_{r_j} \\ & + b_1b_2\cdots b_{p_j}\overline{s}_{k_i}c_1c_2\cdots c_{q_j}(s_{k_j} - \overline{s}_{k_j})f_1f_2\cdots f_{r_j} \\ & + b_1b_2\cdots b_{p_j}(\overline{s}_{k_i} - s_{k_i})c_1c_2\cdots c_{q_j}s_{k_j}f_1f_2\cdots f_{r_j}, \end{aligned}$$

it is obvious that the element d_j can be written as a linear combination of the element d_i and some other elements formed in a similar way to the elements d_k, $k = 1, 2, \ldots, m$, but having smaller leading terms. After combining like terms, the number of elements d_k whose leading terms coincide and are maximal is reduced by 1. The proof is complete by an obvious induction. □

From Lemmas 1 and 2 we easily obtain the following algorithm which solves the word problem for ε-algebras as stated at the beginning of this section:

(a) In a finite number of steps one performs replacement of the set S by the reduced set S' (Lemma 1).

[2]In this proof, we have replaced $s_{i_{k(i)}}$, $s_{j_{k(j)}}$ by s_{k_i}, s_{k_j} respectively. [Translators]

[3]The original says "although they can be subwords of each other". [Translators]

(b) If the word $\overline{a}$ does not contain a subword that coincides with the leading term of one of the elements S', then Lemma 2 implies that $a \notin \langle S \rangle$. If to the contrary such a subword is found, then it is easy to construct an element $a_1 \in \langle S \rangle$ such that $\overline{a} = \overline{a}_1$ and hence $\overline{a - a_1}$ will be less that $\overline{a}$.

It is easy to see that the element a lies in the ideal $\langle S \rangle$ if and only if the element $b = a - a_1$ lies in $\langle S \rangle$. The rest is obvious.

For ε-algebras, as well as nonassociative algebras [5], we have the following result.

Theorem. (Freeness Theorem) *Suppose that the expression of an element $c \in E$, in terms of the elements of the basis of ε-regular words, contains the generating element $a_\alpha \in R$. Then the images of the elements of the set $R \setminus \{a_\alpha\}$ generate a free ε-algebra in the quotient $E/\langle c \rangle$.*

Proof. In the construction of the basis of ε-regular words, we make the convention that for two such words the greater is the one whose expression contains the generator a_α more times, regardless of the degrees of the words. The words that contain the generator a_α the same number of times will be ordered in the usual way. Obviously, any subword v of the word u will be smaller than this word u, and any decreasing sequence of words that are ε-regular (in this sense) must terminate.

The proof of Theorem 1 of the work [4] can be applied to this situation without essential changes. The above way of ordering ε-regular words guarantees that the leading term $\overline{c}$ of an element c contains the generator a_α. Lemma 2, whose proof is still valid, states in our case that the maximal word $\overline{v}$, of any element v in the ideal $\langle c \rangle$, contains a subword that coincides with $\overline{c}$. From this it follows that the (free) subalgebra E' of E generated by the set $R \setminus \{a_\alpha\}$ has zero intersection with the ideal $\langle c \rangle$. This is equivalent to the statement of the theorem. □

2. The membership problem

The word problem is a special case of the so-called membership problem, which for the case considered in this paper has the following formulation:

> An arbitrary finite set $V = \{v_j\}$, $j = 1, 2, \ldots, k$, of elements of the algebra E generates a subalgebra $[V]$. It is necessary to find an algorithm that allows us to determine whether or not the image of an arbitrary element $t \in E$, under the natural homomorphism of E onto the quotient algebra $E' = E/\langle S \rangle$ where $S = \{s_i\}$, $i = 1, 2, \ldots, n$, belongs to the image $[V]'$ of $[V]$ under this homomorphism.

Obviously, when considering the membership problem for sets S and V and elements t, one can make the following assumptions without loss of generality:

(1) The set S is reduced.
(2) None of the words $\overline{t}$ and $\overline{v}_j$, $j = 1, 2, \ldots, k$, contains any of the words $\overline{s}_i$ as a subword.

(3) The coefficients of the leading terms of the elements t and v_j, $j = 1, 2, \ldots, k$, are equal to 1.
(4) Each element $\overline{v}_j$ does not belong to the subalgebra of E generated by the leading terms of the elements of the set $V \setminus \{v_j\}$.

One can achieve Conditions (1)–(4) in a finite number of steps without changing the ideal $\langle S\rangle$, the subalgebra V, or the image t' of the element t. The proof of this fact essentially repeats the argument given in the proof of Lemma 1. For example, if it happens that some element $\overline{v}_j$ belongs to the subalgebra generated by the elements $\overline{v}_i$, $i \neq j$, then instead of the element v_j one should consider the difference $v'_j = v_j - u_j$ where $u_j \in [V]$ and $\overline{v}'_j < \overline{v}_j$.

Let λ be the maximum of the degrees of the elements of S. We will describe a process for modifying the set V. Suppose some element $\overline{s}_i$ has the form $\overline{s}_i = \overline{v}_{i_1}\overline{v}_{i_2}\cdots\overline{v}_{i_q}$ with some placement of parentheses. Then to the set V we adjoin the element $v' = v_{i_1}v_{i_2}\cdots v_{i_q} - s_i$ with the same placement of parentheses. Note that the degrees of the elements v_{i_k} that appear in the expression of the element v' are less than λ. If necessary, to the set $V' = V \cup \{v'\}$ we apply the transformations which ensure Conditions (2)–(4). We repeat this entire process as many times as required.

Since, after each step, the set of words of degree $\leq \lambda$, which can be obtained by multiplying the leading terms of the elements of the corresponding $V^{(i)}$, can only increase, and the number of ε-regular words of degree $\leq \lambda$ that occur in this process is finite, the process will lead in the end to a set V_1 satisfying the following conditions:

– Conditions (2)–(4) above;
– the images of the algebras $[V_1]$ and $[V]$, under the natural homomorphism of the algebra E onto the quotient algebra $E/\langle S\rangle$, coincide;
– if for some placement of parentheses $\overline{s}_j = \overline{v}_{j_1}\overline{v}_{j_2}\cdots\overline{v}_{j_p}$ for some j, j_1, j_2, …, j_p, then the element $s_j - v_{j_1}v_{j_2}\cdots v_{j_p}$ can be represented as the sum $w + \tau$ where $w \in [V_1]$, $\tau \in \langle S\rangle$, $\overline{w} < \overline{s}_j$ and $\overline{\tau} < \overline{s}_j$.

The totality of these conditions imposed on the sets S and V_1 and the element t will be called for brevity *Condition* (5).

Lemma 3. *The image of an element $t \in E$ belongs to the image of the subalgebra $[V_1]$ under the natural homomorphism of E onto the quotient algebra $E/\langle S\rangle$ only if $t \in [\overline{V}_1]$ where $\overline{V}_1$ is the set of leading terms of the elements of V_1; here we assume that Condition* (5) *is satisfied.*

Proof. Indeed, suppose that $t = u + \sigma$ where $u \in [V_1]$ and $\sigma \in \langle S\rangle$. The leading term $\overline{\sigma}$ of σ contains some word $\overline{s}_p$ as a subword where $s_p \in S$ (Lemma 2). Obviously, $\overline{u} \in [\overline{V}_1]$. If $\overline{\sigma} \neq \overline{u}$ (ignoring the coefficients) then the lemma is proved, since $\overline{t} \neq \overline{\sigma}$ by Condition (2) and therefore $\overline{t} = \overline{u}$.

Now assume that $\overline{u} = \overline{\sigma}$. Then for the element $\overline{s}_p$ that is a subword of $\overline{\sigma}$ we have the representation $\overline{s}_p = \overline{v}_{p_1}\overline{v}_{p_2}\cdots\overline{v}_{p_\ell}$ with some placement of parentheses. By Condition (5) we have $s_p - v_{p_1}v_{p_2}\cdots v_{p_\ell} = u' + \sigma'$ where $u' \in [V_1]$, $\sigma' \in \langle S\rangle$,

$\overline{u}' < \overline{s}_p$ and $\overline{\sigma}' < \overline{s}_p$. Thus $s_p = u'' + \sigma'$, $u'' \in [V_1]$. The element σ can be written in the form $\sigma = \sigma_1 + \sigma_2$ where σ_1 is obtained by replacing the subword $\overline{s}_p$ in $\overline{\sigma}$ by the element s_p, and also σ_2 is in $\langle S\rangle$ with $\overline{\sigma}_2 < \overline{\sigma}_1$. Obviously, $\overline{\sigma}_1 = \overline{\sigma} = \overline{u}$. Replacing the factor s_p in σ_1 by the expression $u'' + \sigma'$, we obtain the following expression for the element t: $t = u + u_1 + \sigma_3$ where $u_1 \in [V_1]$ and $\sigma_3 \in \langle S\rangle$ with $\overline{\sigma}_3 < \overline{\sigma}$. The process of decreasing the leading terms of the summands in $\langle S\rangle$ that occur in the expression for t cannot continue indefinitely. The proof is completed by the obvious remark that the condition $u \in [V_1]$ implies $\overline{u} \in [\overline{V}_1]$. The lemma is proved. □

Lemma 3 implies the following algorithm for solving the membership problem for ε-algebras as stated above:

(a) Rewrite the element t, and the elements of the sets V and S, so that they satisfy Conditions (1)–(4).
(b) Extend the set V to the set V_1 satisfying Condition (5).
(c) If $\overline{t} \in [V_1]$ then instead of the element t consider the difference $t_1 = t - w$, where $w \in [V_1]$ and $\overline{w} = \overline{t}$, so that the leading term of t_1 is smaller than $\overline{t}$.
(d) If at any step the current difference equals zero, then the result concerning t is affirmative; if the process terminates with a nonzero element t_r, then the result is negative.

Remark 1. The above stated algorithm also applies of course to the case of nonassociative algebras considered in the work [5] by A.I. Zhukov. Therefore, the membership problem is decidable also for algebras without any identical relations.

Remark 2. In the same way as in [5], the finiteness problem is decidable for ε-algebras.

References

[1] A.A. Markov, *On the impossibility of certain algorithms in the theory of associative systems*, Doklady Akad. Nauk USSR 55 (1947), no. 7, 587–591.

[2] P.S. Novikov, *On the algorithmic unsolvability of the problem of identity*, Doklady Akad. Nauk USSR 85 (1952), no. 4, 709–712.

[3] E. Post, *Recursive unsolvability of a problem of Thue*, J. Symbolic Logic 12 (1947) 1–11.

[4] A.I. Shirshov, *Subalgebras of free commutative and free anticommutative algebras*, Mat. Sbornik 34 (1954), no. 1, 81–88.

[5] A.I. Zhukov, *Reduced systems of defining relations in nonassociative algebras*, Mat. Sbornik 27 (1950), no. 2, 267–280.

Some Algorithmic Problems for Lie Algebras

A.I. Shirshov

1. Introduction

In a previous work [2] the author considered some algorithmic problems in the theory of ε-algebras. The same paper mentioned some literature relevant to these problems.

In the present paper, we consider the analogous problems for Lie algebras. Unfortunately, we cannot obtain the solution of the word problem in this case. However, the word problem can be solved for Lie algebras with one defining relation, and for Lie algebras with a homogeneous system of defining relations.

Moreover, for Lie algebras we will prove a freeness theorem analogous to the corresponding theorem in group theory.

2. Definition of composition

Let L be the free Lie algebra over a field P with the set $R = \{a_\alpha\}$, $\alpha \in I$, of free generators. For brevity of exposition, in what follows we will use the definitions and results of the author's work [1] without particular explanation.

Having fixed once and for all an ordering on the set R, we define regular associative and regular nonassociative words formed by the elements of this set. In the work [1], it is shown that the regular nonassociative words form a basis of L. In what follows, unless otherwise indicated, when we speak of some element of L, we will mean its representation as a linear combination of the elements of this basis. The regular associative word that corresponds to the leading term of an element $b \in L$ (without coefficient) will be denoted by $\overline{b}$.

Sibirsk Mat. Zh. 3, (1962), no. 2, 292–296.

We choose in L two arbitrary elements b and c such that $\overline{b} = b_1b_2$ and $\overline{c} = c_1c_2$ with $b_2 = c_1$, where b_1, b_2, c_2 are (nonempty associative) words and the coefficients of the leading terms of the elements b and c equal 1.

Lemma 1. *The associative word $u = b_1b_2c_2 = b_1c_1c_2$ is regular.*

Proof. Suppose $u = w_1w_2$ and w_1 is a subword of $\overline{b}$. Then $\overline{b} = w_1v$, $\overline{b} > v$, and hence $w_1w_2 > w_2w_1$. In the case when w_2 is a subword of c_2, i.e., $c_2 = c_2'w_2$, the inequality $w_1w_2 > w_2w_1$ follows from the obvious inequalities $w_2 < c_2 < \overline{c} < u$. The proof is complete. □

According to Lemma 4 of [1], we form nonassociative words u_1 and u_2 by placing parentheses in the word u in two different ways[1]:

$$u_1 = \{\cdots[(\widetilde{\overline{b}}q_1)q_2]\cdots\}q_s,$$

where the q_i are regular nonassociative words and $\overline{q}_1\overline{q}_2\cdots\overline{q}_s = c_2$, with $q_1 \le q_2 \le \cdots \le q_s$; and

$$u_2 = r_1\{r_2\cdots[r_{t-1}(r_t\widetilde{\overline{c}})]\cdots\},$$

where the r_j are regular nonassociative words and $\overline{r}_1\overline{r}_2\cdots\overline{r}_t = b_1$. Let

$$u_1' = \{\cdots[(bq_1)q_2]\cdots\}q_s, \qquad u_2' = r_1\{r_2\cdots[r_{t-1}(r_tc)]\cdots\}.$$

Definition 1. The element $t = \alpha(u_1' - u_2')$, where $\alpha \in P$ is the inverse of the coefficient of the leading term of $u_1' - u_2'$, will be called *the composition $(b, c)_{c_1}$ of the elements b and c relative to the word c_1.*

Therefore, the notion of composition is defined for some but not all pairs b and c of elements of L, and essentially depends on the word c_1.

Lemma 2. *No composition can be formed for the pair (b, b).*

Proof. It suffices to show that there cannot be two representations $\overline{b} = b_1b_2 = b_2b_3$ where b_2 is a nonempty associative word. Suppose that $\overline{b} = b_1b_2 = b_2b_3$. From the definition of regularity it follows that $\overline{b} > b_3b_2$, i.e., $b_1 > b_3$; on the other hand, $\overline{b} > b_2b_1$, i.e., $b_3 > b_1$: an obvious contradiction. □

Note that if the composition $(b, c)_{c_1}$ is defined for some word c_1, then the composition $(c, b)_{b_1}$ of the elements c and b cannot be formed, since the assumption of the existence of the composition $(b, c)_{c_1}$ implies the inequality $\overline{b} > \overline{c}$.

[1]We have added tildes over $\overline{b}$ and $\overline{c}$ in the following equations for u_1 and u_2; the tilde means the regular nonassociative word corresponding to a given regular associative word. See the proof of Lemma 3. [Translators]

3. Some word problems

We consider some definitions necessary for what follows.

Definition 2. A finite set $S = \{s_i\}$, $i = 1, 2, \ldots, k$, of elements of the algebra L is called *reduced* if none of the associative words $\overline{s}_i$ is a subword of another word $\overline{s}_j$ $(s_i, s_j \in S)$ and the coefficients of the leading terms of the elements equal 1.

Let S be a reduced set of elements of L, and let S^* be the set of the leading terms of the elements of S and the elements obtained from S by all possible compositions (repeated any number of times).

Definition 3. A reduced set S of elements of L will be called *stable* if

(i) the degree of the composition $(s', s'')_c$ of two elements s' and s'', belonging to S or obtained from S by any number of compositions, is greater than the degree of each of the elements s' and s'', and
(ii) no element of S^* contains another element of S^* as a subword (in particular, the elements of S^* are distinct).

Theorem 1. *Let S be a stable set of elements of L. Then there exists an algorithm that allows us to determine, in a finite number of steps, whether or not an arbitrary element $t \in L$ belongs to the ideal $\langle S \rangle$ generated by S in L.*

We will obtain Theorem 1 from the following lemma.

Lemma 3. *An element $t \in L$ belongs to the ideal $\langle S \rangle$ generated in L by the elements of a stable set S, only if the word $\overline{t}$ contains one of the words of S^* as a subword.*

Proof. Suppose $t \in \langle S \rangle$. Then t can be written as a linear combination of elements d_i of the form

$$d_i = c_1 c_2 \cdots c_{k_i} s_{p_i} f_1 f_2 \cdots f_{\ell_i},$$

with some placement of parentheses, where $s_i \in S$ and c_j, f_j are regular words. Since for any regular associative words u and v, the greater of the words uv and vu is regular, we may assume without loss of generality that the following word is regular:

$$\overline{d}_i = \overline{c}_1 \overline{c}_2 \cdots \overline{c}_{k_i} \overline{s}_{p_i} \overline{f}_1 \overline{f}_2 \cdots \overline{f}_{\ell_i}.$$

The claim of the lemma is obvious if the word $\overline{d}_1$, which is the greatest of the words $\overline{d}_i$ of highest degree, does not occur among the other words[2] $\overline{d}_j$, $j \neq 1$, corresponding to the element t.

Now suppose that $\overline{d}_1 = \overline{d}_j$, $j \neq 1$. Consider the first and simplest case in which $\overline{s}_{p_j}$ is a subword of one of the words $\overline{c}_1 \overline{c}_2 \cdots \overline{c}_{k_1}$ or $\overline{f}_1 \overline{f}_2 \cdots \overline{f}_{\ell_1}$. Consider the former case (the latter is analogous). From the regularity of $\overline{d}_j$, $\overline{s}_{p_1}$, $\overline{s}_{p_j}$ it follows

[2]We have added a bar here, and twice in the first sentence of the next paragraph. [Translators]

(by Lemma 4 of [1]) that we can place parentheses in the word $\overline{d}_j$ in the following way[3]:

$$d' =$$

$$c_1c_2\cdots c_q[\cdots((\widetilde{\overline{s}}_{p_j}c'_{q+1})c'_{q+2})\cdots c'_r]\cdots c_{k_1}[\cdots((\widetilde{\overline{s}}_{p_1}f'_1)f'_2)\cdots f'_m]f_{m+1}\cdots f_{\ell_1},$$

where c'_ρ and f'_ν are regular words,

$$c'_{q+1}\le c'_{q+2}\le\cdots\le c'_r,\quad\text{and}\quad f'_1\le f'_2\le\cdots\le f'_m,$$

and the remaining parentheses are placed in the same way as in $\widetilde{\overline{d}}_j$, where the symbol $\widetilde{\ }$ means the regular nonassociative word corresponding to a given regular associative word. Furthermore, let d'_1 and d'_j denote the elements of L obtained from d' by replacing $\widetilde{\overline{s}}_{p_1}$ by s_{p_1} and $\widetilde{\overline{s}}_{p_j}$ by s_{p_j} respectively.

The differences $d_1-d'_1$ and $d_j-d'_j$ can obviously be written as linear combinations of elements similar to the elements d_i but having smaller leading terms than[4] d_1. As in the proof of Lemma 2 of [2], one can show that the difference $d'_j-d'_1$ can be written in an analogous way. From this, by virtue of the equation

$$d_j=d_1-(d_1-d'_1)+(d'_j-d'_1)+(d_j-d'_j),$$

it follows that the element d_j can be replaced by the sum of d_1 and some other similar elements with smaller leading terms. Combining like terms will either decrease the number of occurrences of the leading term or produce an expression with a smaller leading term. The induction is obvious.

One more case is possible: $\overline{s}_{p_1}=e_1e_2$, $\overline{s}_{p_j}=e_2e_3$. Then by Lemma 1, the subword $e_1e_2e_3$ of $\overline{d}_1$ is regular, and on $e=e_1e_2e_3$ parentheses can be placed in two ways as described in the definition of composition; we can then extend each of these placements of parentheses in a unique way to a complete placement of parentheses on $\overline{d}_1$. Let δ be the difference of the elements d''_1 and d''_j obtained from

[3]We have omitted the primes on $c_1,\ldots,c_q$. [Translators]

[4]Let us simplify and put $d'_1=d'_j=(c\,s_{p_j}c's_{p_1}f)$ where c,c',f are some associative words and $(\ldots)$ is the same placement of parentheses as in Shirshov's paper. (We shorten Shirshov's notation, and instead of two expressions d'_1,d'_j we use only one). Then, for example, $d_1-d'_1$ has the shorter form $(c\,\overline{s_{p_j}}c's_{p_1}f)-(c\,s_{p_j}c's_{p_1}f)$ where c,c',f are the same associative words, and the maximal associative words of each expression $\overline{d_1}$ and $\overline{d'_1}$ are equal to $\overline{d_1}$. Then we can rewrite d_1 as an associative expression $c\,\overline{s_{p_j}}c's_{p_1}f$ with maximal word $\overline{d_1}$ plus a linear combination of associative expressions $a_is_{p_1}b_i$ with maximal words less than $\overline{d_1}$. We can do the same with d'_1. The result is

$$D=d_1-d'_1=\sum_{1\le j\le k}\alpha_ja_js_{p_1}b_j,$$

with maximal words less than $\overline{d_1}$. Without loss of generality, we can assume $a_1\overline{s_{p_1}}b_1>a_2\overline{s_{p_1}}b_2>\ldots$, since the maximal word of s_{p_1} is a regular word, and any regular word has the property that its prefix cannot coincide with its suffix. Then $\overline{D}=a_1\overline{s_{p_1}}b_1$. By Lemma 4 of [1], one can place parentheses to obtain $(a_1s_{p_1}b_1)$ with the maximal word equal to $\overline{D}$. Then $D-\alpha_1(a_1s_{p_1}b_1)$ has the same form as D, but its maximal word is less than $\overline{D}$. The result now follows by induction on the maximal word. [Editors]

those described above by replacing the words $\widetilde{\overline{s}}_{p_1}, \widetilde{\overline{s}}_{p_j}$ by s_{p_1}, s_{p_j} respectively; then δ can be obtained from the word $\overline{d}_1$ by replacing the word e by the composition $(s_{p_1}, s_{p_j})_{e_2}$ and subsequently placing parentheses as on the words d_1'' and d_j''. As in the previous case, the proof is completed by considering the equation

$$d_j = d_1 - (d_1 - d_1'') + (d_j - d_j'') - \delta.$$

The lemma is proved. □

To prove Theorem 1 it suffices to verify that one can write down in a finite number of steps all the elements of the set S^* whose degrees do not exceed the degree of the element t. If the word $\overline{t}$ occurs in an element of S^* as a subword, then in the ideal $\langle S \rangle$ there can be found an element t_0 such that $\overline{t}_0 = \overline{t}$. Then instead of the element t, one should consider the difference $t - t_0$.

The theorem is proved.

Corollary 1. *There exists an algorithm that solves the word problem for Lie algebras with one defining relation.*

This follows from the obvious stability of a set that consists of one element.

Corollary 2. *There are no Lie algebras with one defining relation that have a finite dimension* ≥ 3.

This statement follows from the fact that in a Lie algebra with defining relation $s = 0$, all the distinct words v_i, such that $\overline{v}_i$ does not contain $\overline{s}$ as a subword, are linearly independent.

Theorem 2. *There exists an algorithm that solves the word problem for Lie algebras with a homogeneous set of defining relations.*

Proof. Suppose that in the algebra L some homogeneous set S has been selected. If S is not reduced, then it can be replaced by a reduced set S_1 such that $\langle S \rangle = \langle S_1 \rangle$. Indeed, if $\overline{s}_i$ ($s_i \in S$) is a subword of $\overline{s}_j$ ($s_j \in S$), then one constructs an element s_0 of the ideal $\langle s_i \rangle$ such that $\overline{s}_0 = \overline{s}_j$, and considers the element $s_j' = s_j - s_0$ instead of the element s_j.

The proof that this process of reduction will terminate in a finite number of steps coincides with the proof of Lemma 1 in [2]. Obviously, the resulting set S_1 will consist of homogeneous elements. Since the composition of homogeneous elements is homogeneous, the requirement on degrees in the definition of stability is satisfied. It is also obvious that after a finite number of steps one can write down all elements of S^* whose degrees do not exceed the degree of a given element $t \in L$; during this procedure it may be necessary to perform the reduction process on the sets obtained from S_1 by adjoining compositions of certain elements. The proof is completed as in Theorem 1. □

Theorem 3. (Freeness Theorem) *Let L_0 be a Lie algebra with a set R of generators and one defining relation $s = 0$ whose left side contains the generator a_α. Then the subalgebra L_0', generated in L_0 by the set $R \setminus \{a_\alpha\}$, is free.*

Proof. In addition to the natural ordering of the regular words that form a basis of the free Lie algebra L, we will consider the following ordering. A regular word u is considered to be greater than a regular word v if the generator a_α occurs in u more times than in v. If a_α occurs in u and v the same number of times, then these words are first compared by degree, and if the degrees are equal, then by the usual lexicographical comparison of the words $\overline{u}$ and $\overline{v}$. The associative word $\overline{\overline{s}}$ that corresponds to the leading term of an element s in the sense of the new ordering, may be different from the word $\overline{s}$. Repeating the arguments used in the proof of Lemma 3, and applying Lemma 2, we obtain the result that an element t belongs to the ideal $\langle s \rangle$ only if[5] the word $\overline{\overline{s}}$ is a subword of $\overline{\overline{t}}$. Since the generator a_α occurs in the expression of s, it follows that the subalgebra L_0' has zero intersection with the ideal $\langle s \rangle$. This is equivalent to the claim of the theorem. □

References

[1] A.I. Shirshov, *On free Lie rings*, Mat. Sbornik 45 (1958), no. 2, 113–122.

[2] A.I. Shirshov, *Some algorithmic problems on ε-algebras*, Sibirsk. Mat. Zh. 3, (1961), no. 1, 132–137.

[5] In the rest of this sentence, we have added double bars over s and t. [Translators]

On a Hypothesis in the Theory of Lie Algebras

A.I. Shirshov

1. Introduction

The concepts of a free group and the free product of groups, as well as the results related to these concepts, have their analogues in the theory of algebras. It is known, for example, that any subalgebra of a free Lie algebra is also free. This result is analogous to the well-known theorem of Nielsen-Schreier in group theory. The results of A.T. Gainov [1] on subalgebras of the free commutative and free anticommutative products of algebras, are analogous to the theorem of A.G. Kurosh [2] on subgroups of the free product of groups. Under the influence of this analogy, there existed a conjecture that subalgebras of the free Lie product of Lie algebras are described by a theorem analogous to the theorem of A.T. Gainov cited above. In the present note, we prove that this is not the case. Moreover, we give here a construction of interest in its own right, which it is natural to call the free Lie product of Lie algebras with an amalgamated subalgebra.

2. The free Lie product of Lie algebras with an amalgamated subalgebra

Let L_α $(\alpha \in I)$ be a family of Lie algebras over some fixed field P, each of which contains a subalgebra $L_{\alpha,0}$ which is isomorphic to a given algebra L_0. We construct a Lie algebra L with the following properties:

(1) L contains subalgebras L'_α which are isomorphic to the algebras L_α $(\alpha \in I)$ respectively;
(2) the intersection $L'_0 = \bigcap L'_\alpha$ of the algebras L'_α is a subalgebra isomorphic to L_0, and some fixed isomorphism of L_0 with L'_0 can be extended to isomorphisms of L_α with L'_α for all α;
(3) L is generated by the subalgebras L'_α $(\alpha \in I)$.

Sibirsk Mat. Zh. 3, (1962), no. 2, 297–301.

We choose an arbitrary basis of L_0, and for each $\alpha \in I$ we extend its isomorphic image in L_α to a basis of this latter algebra. As a result of this, we obtain a set S of elements of the algebras L_α, namely $S = \{e_{\alpha\gamma}\}$ ($\alpha \in I$, $\gamma \in J_\alpha$), where all the index sets J_α contain subsets J'_α of equal cardinality (which we will identify in what follows: $J'_\alpha = J'$) such that $\gamma \in J'_\alpha$ implies $e_{\alpha\gamma} \in L_{\alpha,0}$. Clearly, the symbols $e_{\alpha\gamma}$ and $e_{\beta\gamma}$ will not be distinguished if $\gamma \in J'$.

We take a set $R = \{f_{\alpha\gamma}\}$ ($\alpha \in I$, $\gamma \in J_\alpha$) in one-to-one correspondence with S, and make it into the set of free generators of the free Lie algebra $\overline{L}$. We choose a basis of $\overline{L}$ formed by regular words (see [3]), starting from some ordering of the sets I and J_α, where the ordering of J_α extends some ordering of J', and the conditions $\gamma \in J'$, $\delta \in J_\alpha$, $\delta \notin J'_\alpha$ imply that $\gamma < \delta$. That is, $f_{\alpha\gamma} < f_{\alpha'\gamma'}$ if either $\alpha < \alpha'$, or $\alpha = \alpha'$, $\gamma < \gamma'$. Consider the ideal Q of $\overline{L}$ generated by all elements of the form

$$q_{\alpha\gamma\delta} = f_{\alpha\gamma} f_{\alpha\delta} - \sum_\tau p^\tau_{\alpha\gamma\delta} f_{\alpha\tau} \quad (\gamma > \delta),$$

where the following equation holds in the algebra L_α:

$$e_{\alpha\gamma} e_{\alpha\delta} = \sum_\tau p^\tau_{\alpha\gamma\delta} e_{\alpha\tau} \quad (p^\tau_{\alpha\gamma\delta} \in P).$$

Definition. A basis word v of the algebra $\overline{L}$ will be called *special* if the corresponding regular associative word does not contain subwords of the form $f_{\alpha\beta} f_{\alpha\beta'}$, $\beta > \beta'$.

Clearly, a special word of length ≥ 2 can contain none of the symbols $f_{\alpha\beta}$ when $\beta \in J'$.

In what follows, by the *leading term* of an element $t \in \overline{L}$ we will mean the lexicographically maximal term among the terms of the highest degree.

Lemma 1. *An element $t \in \overline{L}$ belongs to the ideal Q only if its leading term is not special.*

Proof. Suppose that an element t of the algebra $\overline{L}$ belongs to the ideal Q, i.e., t can be represented as a linear combination of products of elements $q_{\alpha\gamma\delta}$ with elements of R. Obviously, the leading term of each of the elements $q_{\alpha\gamma\delta}$ corresponds to a regular associative word that contains a subword of the form $f_{\alpha\beta} f_{\alpha\beta'}$, $\beta > \beta'$.

If the greatest of these leading terms does not occur among the other leading terms, then the claim is proved. Otherwise, some of the leading terms are equal, and in view of the complete analogy with the proof of Lemma 3 of [4], it suffices to consider only the case in which the equal regular associative words, corresponding to the equal leading terms, have the form $c_1 c_2 \cdots c_s f_{\alpha\beta} f_{\alpha\gamma} f_{\alpha\delta} d_1 d_2 \cdots d_r$, and the products themselves have the form

$$v_1 = c_1 c_2 \cdots c_s \Big(f_{\alpha\beta} f_{\alpha\gamma} - \sum_\tau p^\tau_{\alpha\beta\gamma} f_{\alpha\tau} \Big) f_{\alpha\delta}\, d_1 d_2 \cdots d_r,$$

$$v_2 = c_1 c_2 \cdots c_s f_{\alpha\beta} \Big(f_{\alpha\gamma} f_{\alpha\delta} - \sum_\tau p^\tau_{\alpha\gamma\delta} f_{\alpha\tau} \Big) d_1 d_2 \cdots d_r,$$

where $\beta > \gamma > \delta$ and the parentheses on the products v_1 and v_2 are placed in the same way. By virtue of the known properties of the structure constants of a Lie algebra, the following equation holds:

$$v_1 = c_1 c_2 \cdots c_s \Big(f_{\alpha\beta} f_{\alpha\delta} - \sum_\tau p^\tau_{\alpha\beta\delta} f_{\alpha\tau} \Big) f_{\alpha\gamma} d_1 d_2 \cdots d_r$$
$$+ c_1 c_2 \cdots c_s f_{\alpha\beta} \Big(f_{\alpha\gamma} f_{\alpha\delta} - \sum_\tau p^\tau_{\alpha\gamma\delta} f_{\alpha\tau} \Big) d_1 d_2 \cdots d_r + w,$$

where the omitted parentheses are placed as on the element v_1, and the element w is a linear combination of the elements[1] of the form $q_{\alpha\gamma\delta}$, but of lower degree.

Having performed the corresponding substitution in the expression for the element t, and combined like terms (the second summand in the expression for v_1 coincides with v_2), we either decrease the number of the above-mentioned products with equal leading terms, or reduce the leading term itself. The proof is completed by induction on the leading term[2]. □

Now consider the quotient algebra $L = \overline{L}/Q$. Lemma 1 implies that the images of special words are linearly independent in L.

Theorem 1. *The images of the special words form a basis of the algebra L.*

Proof. By the remark preceding the statement of the theorem, it suffices to prove that the images of regular words can be represented as linear combinations of special words. A regular word is not special if it contains either

(1) a subword of the form $f_{\alpha\beta} f_{\alpha\gamma}$, $\beta > \gamma$, or
(2) a subword of the form $f_{\alpha\beta}(f_{\alpha\gamma} w)$, $\beta > \gamma$, where w is a regular word, or
(3) a subword of the form $f_{\alpha\beta}(uv)$ where the regular associative word that corresponds to u starts with $f_{\alpha\gamma}$, $\beta > \gamma$.

In the first case, since

$$f_{\alpha\beta} f_{\alpha\gamma} - \sum_\tau p^\tau_{\alpha\beta\gamma} f_{\alpha\tau} \equiv 0 \pmod{Q},$$

the word can be replaced by a linear combination of words of lower degree. In the second case, it follows from the equation

$$f_{\alpha\beta}(f_{\alpha\gamma} w) = (f_{\alpha\beta} f_{\alpha\gamma}) w + f_{\alpha\gamma}(f_{\alpha\beta} w),$$

that the given word can be replaced by a linear combination of words either of lower degree or smaller in the lexicographical sense. The argument in the third case is analogous. The rest is obvious. □

It is also obvious that the algebra L satisfies the required conditions stated at the beginning of this section. Furthermore, it is clear that L can be homomorphically mapped onto any Lie algebra satisfying the same list of conditions, and that the kernel of this homomorphism will have zero intersection with each of the

[1] Multiplied by the c_i and d_j. [Translators]
[2] And on the number of products with equal leading terms. [Translators]

algebras L'_α. From the latter remark it easily follows that L is uniquely determined up to isomorphism. Therefore, L does not depend on the choice of whichever ordering of the sets I and J_α is used in the construction of L. By analogy with the well-known definition in group theory, we will call L the *free Lie product of the Lie algebras L_α with an amalgamated subalgebra L_0*.

3. On subalgebras of free Lie products of Lie algebras

A special case of the construction considered above is the free Lie product of Lie algebras L_α, $\alpha \in I$, obtained with the assumption that $L_0 = 0$, i.e., J' is the empty set. As in the general case, the free Lie product is commutative, associative, and has many properties usually associated with free compositions. We point out only one of them.

Lemma 2. *Let L be the free Lie product of the Lie algebras L_α, $\alpha \in I$. Then the quotient $\overline{L}$ of L by the ideal S_β, generated in L by one of the factors L_β, is isomorphic to the free Lie product of the L_α, $\alpha \in \overline{I}$, $\overline{I} = I \setminus \{\beta\}$.*

The proof of this statement follows immediately from the fact that an element $c \in L$ belongs to the ideal S_β if and only if each basis element occurring in the expression of c contains at least one of the generators $f_{\beta\mu}$.

Theorem 2. *There exist Lie algebras such that their free Lie product has a subalgebra that is not free, is not isomorphic to any subalgebra of any of the factors, and cannot be decomposed as the free Lie product of any of its subalgebras.*

Proof. Let L_1 be a 1-dimensional Lie algebra with generator e_{11}, and let L_2 be the 2-dimensional Lie algebra with basis e_{21}, e_{22} such that $e_{22}e_{21} = e_{21}$. Let L be the free Lie product of L_1 and L_2. It follows from the above discussion that for a basis of L we can choose the collection of special words, i.e., regular nonassociative words whose corresponding associative words do not contain the subword $e_{22}e_{21}$. Note that here we assume the following ordering: $e_{22} > e_{21} > e_{11}$.

Consider the subalgebra L' of L generated by the elements e_{21}, e_{22}, $e_{21}e_{11}$, $e_{22}e_{11}$. First we show that L' is isomorphic to the Lie algebra L^* with four generators c_1, c_2, c_3, c_4 and two defining relations:

$$c_4c_1 + c_3c_2 - c_1 = 0, \qquad c_4c_2 - c_2 = 0.$$

We establish the following correspondence among the generators:

$$c_4 \to e_{22}, \qquad c_3 \to e_{22}e_{11}, \qquad c_2 \to e_{21}, \qquad c_1 \to e_{21}e_{11}.$$

Since the following relations hold in the algebra,

$$e_{22}(e_{21}e_{11}) + (e_{22}e_{11})e_{21} - e_{21}e_{11} = 0, \qquad e_{22}e_{21} - e_{21} = 0,$$

the correspondence above extends to a homomorphism of algebras from L^* onto L'. The algebra L^* is one of the algebras for which the word problem is decidable (see [4]).

As basis elements of L^* we can take the regular nonassociative words whose corresponding associative words do not contain the subwords c_4c_1 or c_4c_2. However, it is easy to see that every nonzero linear combination of such elements corresponds to a nonzero element of L'. Therefore, the above-mentioned homomorphism is an isomorphism.

In what follows, we will work with the algebra L^*. We will assume that L^* does not contain subalgebras of finite dimension, except for those of dimension 1 and the subalgebra generated by c_4 and c_2, since such a subalgebra would give the required example; for the same reason, we will assume that the free Lie product of Lie algebras which do not have finite-dimensional subalgebras except for those of dimension 1, does not contain such subalgebras either. From this it follows that, if L^* were decomposed as the free Lie product of algebras $\overline{L}_1$ and $\overline{L}_2$, then one of them, say $\overline{L}_1$, would contain the elements c_4 and c_2.

The ideal T generated by these elements contains the element c_1, and hence the quotient algebra L^*/T is 1-dimensional; however by Lemma 2 it is isomorphic to $\overline{L}_2$. The algebra L^* is not isomorphic to L, since it does not contain an element that together with c_4 and c_2 would generate L^*. Therefore, the algebra $\overline{L}_1$ is not generated by c_4 and c_2. It cannot be decomposed into the free Lie product of two Lie algebras, since otherwise it would follow from Lemma 2 that the quotient of L^* by the ideal T would not be 1-dimensional. Therefore, as the required example, we can take the subalgebra $\overline{L}_1$ of L. The theorem is proved. □

Remark. In fact, even the algebra L' cannot be decomposed as a free Lie product of its subalgebras. However, the proof of this fact is considerably more complicated than the proof given above.

The theorem just proved shows that subalgebras of the free Lie product of Lie algebras have a rather complicated structure, and the problem of their description is of great interest.

References

[1] A.T. Gainov, *Free commutative and free anti-commutative products of algebras*, Sibirsk. Mat. Zh. 3, (1962), no. 6, 805–833.

[2] A.G. Kurosh, *Die Untergruppen der freien Produkte von beliebigen Gruppen*, Math. Ann. 109, 1 (1934) 647–660.

[3] A.I. Shirshov, *On free Lie rings*, Mat. Sbornik 45, (1958), no. 2, 113–122.

[4] A.I. Shirshov, *Some algorithmic problems for Lie algebras*, Sibirsk Mat. Zh. 3, (1962), no. 2, 292–296.

On the Bases of a Free Lie Algebra

A.I. Shirshov

Introduction

In the work of M. Hall [1], a certain way of fixing a basis of a free Lie algebra is indicated. However, the concrete bases which one needs to construct, in order to solve certain problems, do not always fall into Hall's scheme. For instance, the basis of a free Lie algebra considered in the work [2] cannot be constructed using Hall's method. For this reason, in each such case it is necessary to reprove that a certain subset of a free Lie algebra is a basis. Below, we give a method that generalizes Hall's method for choosing a basis in a free Lie algebra.

A construction of a basis of a free Lie algebra

Let $R = \{a_\alpha\}$ be a set of symbols, where α ranges over a nonempty set of indices. The set of all nonassociative words that can be formed from the elements of R will be denoted by K.

Definition 1. Nonassociative words of length 1 in K will be called *regular* and ordered arbitrarily. Suppose regular words for all lengths less than n have already been defined and ordered by some relation $>$ such that for any regular words u, v and w the condition $w = uv$ implies $w > v$. Then a word t of length n, $n > 1$, will be called *regular* if

1) $t = rs$ where r and s are regular words with $r > s$, and
2) if $r = r_1 r_2$ then $r_2 \leq s$.

The regular words of length $\leq n$ defined in this way will be ordered arbitrarily, except that we preserve the existing ordering of the regular words of length less than n, and require as before that $w = uv$ implies $w > v$.

Algebra Logika 1, (1962), no. 1, 14–19.

The ordering described in this definition can be realized, for instance, by ordering words of the same length arbitrarily and declaring that words of smaller length precede words of greater length (see Hall [1]). This case, however, does not exhaust all the possibilities.

We indicate a method that assigns to every element w of K the unique formal expression,

$$w^* = \sum_{i=1}^{k(w)} n_i^{(w)} w_i,$$

where $k(w) \geq 0$, the $n_i^{(w)}$ are nonzero elements of the base field, and the w_i are distinct regular words. If the length of the word w equals 1, then we set $w^* = w$. Assume by induction that for words w whose length is less than n the following conditions hold:

i) the required method has been indicated,
ii) the words w_i obtained by this method have the same content relative to R as w (i.e., in each of these words every element of R occurs the same number of times as in w),
iii) if w is the product of two *distinct* regular words, $w = uv$, then all the w_i, $i = 1, 2, \ldots, k(w)$, are greater than the lesser of u and w (in the sense of the ordering of regular words), and
iv) if w is regular then $w^* = w$, i.e., $k(w) = 1$ and $n_1^{(w)} = 1$.

Suppose now that a word w has length $n > 1$. Then $w = uv$. By the inductive hypothesis it follows that the expressions,

$$u^* = \sum_{i=1}^{k(u)} n_i^{(u)} u_i, \qquad v^* = \sum_{j=1}^{k(v)} n_j^{(v)} v_j,$$

have already been defined. Let

$$w' = \sum_{i=1}^{k(u)} \sum_{j=1}^{k(v)} n_i^{(u)} n_j^{(v)} u_i v_j.$$

We delete in the expression w' the terms $n_j^{(v)} n_i^{(u)} u_i v_j$ in which $u_i = v_j$, and replace each term in which $u_i < v_j$ by the expression $-n_i^{(u)} n_j^{(v)} v_j u_i$.

After performing the formal combination of like terms, and removing the terms whose coefficients turn out to be zero, we denote the resulting expression by w''. In the expression w'', if it turns out that for some $mu_i v_j$ we have $u_i = u_i' u_i''$ with $u_i'' > v_j$, then we replace each such expression by $m(u_i' v_j) u_i'' + m u_i' (u_i'' v_j)$; we act analogously for the elements $m v_j u_i$ if it turns out that $v_j = v_j' v_j''$ with $v_j'' > u_i$. After this, we combine like terms and denote the resulting expression by w'''. For each monomial that occurs in w''' we perform all the transformations that have been done for w, each time replacing the monomial in w''' by the corresponding formal expression, multiplied by the original coefficient of the monomial; we then

combine like terms. Then for the resulting expression $w^{(4)}$ we perform the same transformations as were done for w''', and so forth. We will show that at some step this process must stabilize.

Indeed, by the inductive hypothesis for the element $u_i v_j$, with each passage to the sum of products of regular words, the lesser of the factors will be greater than the lesser of the words u_i and v_j. However, also by the inductive hypothesis, the content of the words will not change, but the number of words with the same content is finite. This stabilized expression obtained for w we will take as w^*.

Therefore, we have indicated a method which, to each word w of length n, assigns in a unique manner the formal expression w^*. Since at each step the content of the words is preserved, all the w_j will have the same content as w. If $w = uv$ is a product of two regular words, then all the w_i will be greater than the lesser of the words u and v, since at no step can a decrease of the lesser factor occur, and hence $w_i = u_i v_i$ where v_i is not less than the lesser of the words u and v, but $w_i > v_i$ by Definition 1. In the case that w is regular, it cannot undergo any changes, and hence $w^* = w$. Therefore, all the assumptions of the inductive hypothesis have been verified for words of length n.

Now consider the vector space $\mathfrak{A}$ over the base field with the basis of regular words. We make this space into an algebra $\mathfrak{S}$ by defining the product of basis elements as follows:

$$v_i \cdot v_j = (v_i v_j)^*.$$

Theorem. *The algebra $\mathfrak{S}$ is the free Lie algebra with the set of generators R.*

Proof. First we prove that $\mathfrak{S}$ is a Lie algebra. The construction for w^* explained above shows that

$$\Big(\sum_i \delta_i a_i + \sum_j \delta'_j u_j\Big) \cdot \Big(\sum_i \delta_i a_i + \sum_j \delta'_j u_j\Big) = 0,$$

which implies that the identical relation $x^2 = 0$ holds in $\mathfrak{S}$.

It is more difficult to prove that the Jacobi identity holds. By virtue of its multilinearity, it suffices to show that if u_i, u_j, u_k are regular words, then

$$[(u_i u_j)^* u_k]^* + [(u_j u_k)^* u_i]^* + [(u_k u_i)^* u_j]^* = 0. \tag{1}$$

If the sum of the lengths of u_i, u_j, u_k equals 3, then the validity of equation (1) follows from the definition of the operation w^*. Assume by induction that for any set R, and any way of defining regular R-words, i.e., words formed from the symbols of the set R, equation (1) holds if the sum of the lengths of u_i, u_j, u_k is less than n. Suppose now that u_i, u_j, u_k are such that the sum of their lengths equals n, $n > 3$. Let a_β be the lowest symbol (in terms of the ordering) of the set R, from among the symbols that occur in u_r $(r = i, j, k)$.

First, we assume that $u_r \neq a_\beta$ $(r = i, j, k)$. Consider the set of symbols $R' = \{a_\alpha^n\}$, $n = 0, 1, 2, \ldots$, where $a_\alpha \in R$ and $a_\alpha > a_\beta$. To each R'-word $\overline{w}$ we

assign an R-word w by replacing in $\overline{w}$ each symbol a_α^n by the monomial

$$[\cdots(a_\alpha \underbrace{a_\beta)a_\beta\cdots]a_\beta}_{n \text{ times}}.$$

We will say that the word $\overline{w}$ is *regular* if the corresponding word w is regular, and we will order regular R'-words using the already defined ordering of the corresponding regular R-words. Then R'-words of length 1 are regular, and R'-words of length n, $n > 1$, are regular if and only if they satisfy the conditions of Definition 1. Therefore, the definition of regular R'-words agrees with Definition 1. In our words u_r $(r = i, j, k)$ there occur symbols from R that are not less than a_β, and by Definition 1 the symbol a_β can occur only in words of the form $[\cdots(a_\alpha a_\beta)a_\beta\cdots]a_\beta$; hence we can find R'-words $\overline{u}_r$ $(r = i, j, k)$ which correspond, in the sense explained above, to the R-words u_r $(r = i, j, k)$. Since a_β occurs in at least one of the words u_r $(r = i, j, k)$, the sum of the lengths of the R'-words $\overline{u}_r$ $(r = i, j, k)$ is less than n. Hence by the inductive hypothesis it follows that

$$[(\overline{u}_i\overline{u}_j)^*\overline{u}_k]^* + [(\overline{u}_j\overline{u}_k)^*\overline{u}_i]^* + [(\overline{u}_k\overline{u}_i)^*\overline{u}_j]^* = 0.$$

But each transformation for $(\overline{u}_i\overline{u}_j)^*$ etc. corresponds to an analogous transformation for $(u_iu_j)^*$ etc., and as a result of performing these transformations, we obtain elements which correspond as explained above. Hence equation (1) holds in this case.

Now assume that a_β equals one of our words, for instance u_k. Then equation (1) takes the form

$$[(u_iu_j)^*a_\beta]^* + [(u_ja_\beta)^*u_i]^* + [(a_\beta u_i)^*u_j]^* = 0. \tag{2}$$

We also assume that $u_i \neq a_\beta$, $u_j \neq a_\beta$ and $u_i \neq a_j$, since otherwise equation (2) is obvious. Without loss of generality, we may assume that $u_i > u_j$, since otherwise, using the equation $(uv)^* = -(vu)^*$, we can reduce equation (2) to the equation

$$[(u_ju_i)^*a_\beta]^* + [(u_ia_\beta)^*u_j]^* + [(a_\beta u_j)^*u_i]^* = 0.$$

If it turns out that the following equation holds,

$$(u_iu_j)^* = u_iu_j, \tag{3}$$

then

$$\begin{aligned}&[(u_iu_j)^*a_\beta]^* + [(u_ja_\beta)^*u_i]^* + [(a_\beta u_i)^*u_j]^* = \\ &[(u_ia_\beta)^*u_j]^* + [u_i(u_ja_\beta)^*]^* + [(u_ja_\beta)^*u_i]^* + [(a_\beta u_i)^*u_j]^* = 0,\end{aligned}$$

by the definition of the operation w^*, and hence equation (2) holds. Equation (3) is valid if the length of u_i equals 1, or if u_i has the form $u_{i1}u_{i2}$ where $u_{i2} \leq u_j$. Hence we can exclude these cases and assume that $u_i = u_{i1}u_{i2}$ where $u_{i2} > u_j$. Consider the finite set of pairs u_i', u_j' of regular words which can be formed from the symbols that occur in u_i, u_j and for which $u_i' \geq u_j'$. Let u_j'' be the maximal

value taken on by u'_j. Then $(u''_i u''_j)^* = u''_i u''_j$ where u''_i is some value of the word u'_i that corresponds to the word u''_j. Indeed, if $u''_i = u''_{i1} u''_{i2}$ with $u''_{i2} > u''_j$, then

$$(w'')^* = (u''_i u''_j)^* = [(u''_{i1} u''_j)^* u''_{i2}]^* + [u''_{i1} (u''_{i2} u''_j)^*]^*.$$

During the application of the operation $*$, the content of the words does not change, and the lowest factor will not decrease, but each of the regular words in the expressions $(u''_{i1} u''_j)^*$, $(u''_{i2} u''_j)^*$, u''_{i2}, u''_{i1} is greater than u''_j. Hence, u''_j is not maximal. Therefore, equation (2) holds for the words u''_i, u''_j, a_β. We carry out induction on the finite number of values of the word u''_j in the pairs of words defined above.

Assume by induction that equation (2) holds for all possible values of the pairs u'_i, u'_j with $u'_j > u_j$. From the definition of the operation $*$ it follows that

$$\{[(u_{i1} u_{i2}) u_j]^* a_\beta\}^* = \{[(u_{i1} u_j)^* u_{i2}]^* a_\beta\}^* + \{[u_{i1} (u_{i2} u_j)^*]^* a_\beta\}^*. \tag{4}$$

Since each of the words u_{i1}, u_{i2}, u_j is distinct from a_β, from the case proved above the following equations hold:

$$[(u_j a_\beta)^* (u_{i1} u_{i2})]^* = \{[(u_j a_\beta)^* u_{i1}]^* u_{i2}\}^* + \{u_{i1} [(u_j a_\beta)^* u_{i2}]^*\}^*, \tag{5}$$

$$\{[(a_\beta u_{i1})^* u_{i2}]^* u_j\}^* = [(a_\beta u_{i1})^* (u_{i2} u_j)^*]^* + \{[(a_\beta u_{i1})^* u_j]^* u_{i2}\}^*, \tag{6}$$

$$\{[u_{i1} (a_\beta u_{i2})^*]^* u_j\}^* = [(u_{i1} u_j)^* (a_\beta u_{i2})^*]^* + \{u_{i1} [(a_\beta u_{i2})^* u_j]^*\}^*. \tag{7}$$

Finally, from the inductive hypothesis it follows that

$$\{[a_\beta (u_{i1} u_{i2})]^* u_j\}^* = \{[(a_\beta u_{i1})^* u_{i2}]^* u_j\}^* + \{[u_{i2} (a_\beta u_{i2})^*]^* u_j\}^*, \tag{8}$$

$$\{u_{i1} [(u_j a_\beta)^* u_{i2}]^*\}^* + \{u_{i1} [(u_{i2} u_j)^* a_\beta]^*\}^* + \{u_{i1} [(a_\beta u_{i2})^* u_j]^*\}^* = 0, \tag{9}$$

$$\{[(u_{i1} u_j)^* u_{i2}]^* a_\beta\}^* = \{[(u_{i1} u_j)^* a_\beta]^* u_{i2}\}^* + [(u_{i1} u_j)^* (u_{i2} a_\beta)^*]^*, \tag{10}$$

$$\{[u_{i1} (u_{i2} u_j)^*]^* a_\beta\}^* = [(u_{i1} a_\beta)^* (u_{i2} u_j)^*]^* + \{u_{i1} [(u_{i2} u_j)^* a_\beta]^*\}^*, \tag{11}$$

$$\{[(u_j a_\beta)^* u_{i1}]^* u_{i2}\}^* + \{[(a_\beta u_{i1})^* u_j]^* u_{i2}\}^* + \{[(u_{i1} u_j)^* a_\beta]^* u_{i2}\}^* = 0. \tag{12}$$

Adding separately the left and right sides of equations (4)–(12) with the corresponding sides of the obvious equations,

$$[(u_{i1} u_j)^* (u_{i2} a_\beta)^*]^* = -[(u_{i1} u_j)^* (a_\beta u_{i2})^*]^*, \tag{13}$$

$$[(u_{i1} a_\beta)^* (u_{i2} u_j)^*]^* = -[(a_\beta u_{i2})^* (u_{i2} u_j)^*]^*, \tag{14}$$

and comparing the results, we obtain

$$\{[(u_{i1} u_{i2}) u_j]^* a_\beta\}^* + [(u_j a_\beta)^* (u_{i1} u_{i2})]^* + \{[a_\beta (u_{i1} u_{i2})]^* u_j\}^* = 0,$$

which completes the proof that $\mathfrak{S}$ is a Lie algebra.

Now let S be any Lie algebra with R as the set of generators. To each element $h = \sum_i \delta_i a_i + \sum_j \delta'_j u_j$ of the algebra $\mathfrak{S}$ we assign the analogously written element $\overline{h}$ of S where δ_i, δ'_j are elements of the base field. Since the transformations that carry the word w to the element w^* can be performed in any Lie algebra, it follows that the above-mentioned correspondence is a homomorphism of $\mathfrak{S}$ onto S. □

Instead of coefficients from the base field one can consider integers. In this case, we will obtain a free Lie ring $\mathfrak{S}$. From what has been proved it follows that regular words form a basis of the free Lie ring, which is a generalization of the well-known theorem of Hall [1], since Definition 1 is broader than the corresponding definition given by Hall.

Obviously, this also implies a group-theoretic statement generalizing the corresponding result of Hall. To be specific, we introduce the notation $[x, y] = xyx^{-1}y^{-1}$ in the free group G with R as a set of free generators, and call a commutator product (i.e., an R-word with some placement of square brackets) *regular* if it is regular in the sense of Definition 1. Then from the well-known isomorphism of the group G^n/G^{n+1} with the subgroup generated by words of length n in the additive group of the free Lie ring with generating set R, it follows that *regular commutator products of length n form a basis of the Abelian group* G^n/G^{n+1}.

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.I. Shirshov, *On free Lie rings*, Mat. Sbornik 45 (1958), no. 2, 113–122.

On Some Groups which are Nearly Engel

A.I. Shirshov

1. Introduction

In the present work, we give a certain modification of one of the possible definitions of an Engel group. As a consequence of this, we define a class of groups which in the finite case turns out to be wider than the class of Engel groups. For the finite case, we obtain a complete description of groups of this wider class (Section 3). In Section 4 we define a subclass of Engel groups that contains in particular the 3-Engel groups.

In this work we formulate several problems that can, in the author's opinion, attract the attention of mathematicians.

The author expresses his gratitude to M.I. Kargapolov, who looked over the manuscript and made a number of important remarks.

2. The definition of ν-group

Let G be a group. We introduce the following notation:

$$[a,b,1] = [a,b] = aba^{-1}b^{-1}; \qquad [a,b,k] = [\,[a,b,k-1],b\,] \ \ (k = 2,3,\ldots).$$

A group G in which, for any two elements a and b and some fixed number k, the equality $[a,b,k] = e$ holds, where e is the identity element of G, is called k-*Engel* or simply *Engel*. Obviously, any nilpotent group is Engel. However, it is not known up to now if there exist Engel groups which are not locally nilpotent. Local nilpotence has been proved only for 3-Engel groups [2].

The definition of Engel groups can be formulated in a slightly different way. Suppose that a variety M_1 of groups is determined by the equation

$$f_1(x,y) = \varphi_1(x,y),$$

Algebra Logika 2, (1963), no. 5, 5–18.

where f_1 and φ_1 are words in the variables x and y. Then setting

$$f_2(x,y) = f_1(xyx^{-1}, y), \qquad \varphi_2(x,y) = \varphi_1(xyx^{-1}, y),$$

we define a new variety M_2 by the equation

$$f_2(x,y) = \varphi(x,y).$$

Clearly $M_1 \subseteq M_2$. Analogously, we define the varieties M_3, M_4, and so on. Applying the above process to the variety E_1 of Abelian groups, i.e., to the relation $xy = yx$, we obtain the variety E_2 determined by the relation $xyx^{-1}y = yxyx^{-1}$, or equivalently by the relation $[x,y,2] = e$. Since $[xyx^{-1}, y, k] = [x,y,k+1]$, the variety E_k coincides with the variety of k-Engel groups.

The passage from M_1 to M_2 consists in replacing arbitrary elements x and y by a pair of conjugates xyx^{-1} and y. Taking into account that a pair of conjugate elements can always be written in the form xy and yx, we can define in a similar way another process of passing from a variety $M^{(1)}$ to another variety $M^{(2)}$. Suppose that the variety $M^{(1)}$ is determined by the relation

$$f^{(1)}(x,y) = \varphi^{(1)}(x,y).$$

Setting

$$f^{(2)}(x,y) = f^{(1)}(xy, yx), \qquad \varphi^{(2)}(x,y) = \varphi^{(1)}(xy, yx),$$

we define the variety $M^{(2)}$ by the relation

$$f^{(2)}(x,y) = \varphi^{(2)}(x,y).$$

Analogously, we define the varieties $M_{(k)}$, $k = 3, 4, \ldots$. Applying this process to the variety $E_1 = N^{(1)}$ of Abelian groups, i.e., again to the relation $xy = yx$, we obtain the variety $N^{(2)}$ determined by the relation $xy^2x = yx^2y$, the variety $N^{(3)}$ determined by the relation $xy^2xyx^2y = yx^2yxy^2x$, and so on.

Definition 1. The groups that belong to the variety $N^{(k)}$ will be called *ν_k-groups* or simply *ν-groups*.

The first question that arises in connection with the study of ν-groups is the question of the relation of this class with the class of Engel groups. Obviously, the varieties E_2 and $N^{(2)}$ coincide, since each of them is determined by the commutativity of any two conjugate elements. As the following theorem shows, starting with $k = 3$, the varieties E_k and $N^{(k)}$ no longer coincide.

Theorem 1. *A group G is 3-Engel if and only if it satisfies the following identical relations:*

$$xy^2xyx^2y = yx^2yxy^2x, \tag{1}$$

$$xy^2xyxyx^2y = yx^2yyxxy^2x. \tag{2}$$

The relations (1) *and* (2) *are independent.*

Proof. Let G be a 3-Engel group. Then by virtue of the easily and immediately verifiable relation,

$$\begin{aligned} &xy^2xyx^2yx^{-1}y^{-2}x^{-1}y^{-1}x^{-2}y^{-1} \\ &= [x, yx, 3]yx^2yxy^2x[x^{-1}, y^{-1}x^{-1}, 3]x^{-1}y^{-2}x^{-1}y^{-1}x^{-2}y^{-1}, \end{aligned}$$

it is obvious that G satisfies relation (1). In addition, since in the group G we have

$$e = [x, yx, 3] = xy^2xy^{-1}x^{-1}yx^2yx^{-1}y^{-1} \cdot y^{-1}x^{-2}y^{-1},$$

it follows that

$$\begin{aligned} e &= y^{-1}x^{-2}y^{-1} \cdot xy^2xy^{-1}x^{-1}yx^2yx^{-1}y^{-1} \\ &= y^{-1}x^{-2}y^{-1}xy^2xy^{-1}x^{-2}y^{-1}yxyx^2yx^{-1}y^{-1}. \end{aligned}$$

Using the already established relation (1), we obtain

$$e = y^{-1}x^{-2}y^{-1} \cdot y^{-1}x^{-2}y^{-1}xy^2x \cdot yx^2y \cdot x^{-1}y^{-1},$$

or equivalently $xy^2x \cdot yx \cdot yx^2y = yx^2y \cdot yx \cdot xy^2x$, i.e., relation (2).

If we now assume that G satisfies relations (1) and (2), then doing the just performed transformations in the reverse order, we obtain $[x, yx, 3] = e$, or equivalently $[x, y, 3] = e$.

To prove the independence of relations (1) and (2), it suffices to give examples of groups in which one of the relations holds but not the other.

It is easy to verify that the symmetric group S_3 of degree 3 satisfies relation (1). It is well known that S_3 is not Engel, and hence does not satisfy relation (2). Another group with the same properties is, for example, the free product of two groups of order 2.

Denote by Z_3 the collection of all pairs of the form (ε_i, t) where t is an arbitrary complex number, and ε_i is one of the three cube roots of unity. We define multiplication of elements of Z_3 by the formula $(\varepsilon_i, t_1)(\varepsilon_j, t_2) = (\varepsilon_i\varepsilon_j, t_1\varepsilon_j + t_2)$. It is easy to verify that the set Z_3, with the above operation, is a group that is isomorphic to the group of all rotations of the complex plane, by angles that are multiples of $2\pi/3$ around various points, and all translations. A direct computation shows that the identity (2) holds in Z_3. On the other hand, setting $\alpha = (\varepsilon_i, 1)$, $\beta = (1, 1)$, $\varepsilon_i \neq 1$, we convince ourselves that $\alpha\beta^2\alpha\beta\alpha^2\beta \neq \beta\alpha^2\beta\alpha\beta^2\alpha$. We note that the group Z_3 is a solvable group with Abelian commutator subgroup. □

Remark 1. The theorem just proved indicates the possibility of defining 3-Engel groups by relations that make sense for semigroups. Relations (1) and (2) can therefore be taken as the definition of a 3-Engel semigroup. From the results of the works [2] and [4] it follows that a 3-Engel semigroup with cancelation is locally nilpotent.

It would be interesting to find semigroup relations (if they exist) that define k-Engel groups for any k. The following two questions are also of interest:

1) Do there exist Engel groups that are not ν-groups?
2) Do there exist ν-groups that are not locally solvable?

Negative answers to both of these questions would give an affirmative solution to the problem of local nilpotence of Engel groups.

3. Finite ν-groups

In this section, we consider finite ν-groups in a little more detail. The example of the group S_3 shows that there exist finite ν-groups that are not nilpotent. On the other hand, the example of the alternating group A_4 shows that there exist finite solvable groups which are not ν-groups.

In Section 1, the ν_k-groups were defined by the equation

$$f^{(k)}(x,y) = \varphi^{(k)}(x,y), \text{ where } f^{(1)}(x,y) = xy,\ \varphi^{(1)}(x,y) = yx.$$

By induction we show that

$$f^{(k)}(x,y) = f^{(k-1)}(x,y)\,\varphi^{(k-1)}(x,y); \quad \varphi^{(k)}(x,y) = \varphi^{(k-1)}(x,y)\,f^{(k-1)}(x,y).$$

Indeed,

$$\begin{aligned} f^{(k)}(x,y) &= f^{(k-1)}(xy,yx) = f^{(k-2)}(xy,yx)\,\varphi^{(k-2)}(xy,yx) \\ &= f^{(k-1)}(x,y)\,\varphi^{(k-1)}(x,y), \end{aligned}$$

and the second equation is proved similarly.

Consider the set S of pairs (a,b) of elements of a group G. On the set S we define the mapping φ that sends each pair (a,b) to the pair (ab,ba); we write $(a,b)^{\varphi} = (ab,ba)$. The pairs of the form (a,a) will be called *trivial*. Obviously, G is a ν-group if and only if some power of the mapping φ sends every pair to a trivial pair. The group A_4 mentioned above is not a ν-group because

$$((1,2,3),(1,3,4))^{\varphi^2} = ((1,2,3),(1,3,4)).$$

Obviously, no power of the mapping φ can send $((1,2,3),(1,3,4))$ to a trivial pair.

It follows from the work of A.I. Malcev [4] that any nilpotent group G is a ν-group. A wider class of ν-groups is described by the following theorem.

Theorem 2. *A group G which is an extension of a nilpotent group, by a nilpotent group with an identical relation of the form $x^{2^k} = e$, is a ν-group.*

Proof. By assumption, G has a nilpotent normal subgroup N, such that the quotient group $\overline{G} \simeq G/N$ is a nilpotent group with the identical relation $x^{2^k} = e$. Therefore, any pair (a,b) of elements of G is sent by a power of φ to a pair of the form (cn,cm), $n,m \in N$, $c^{2^k} \in N$. Since

$$(cn,cm)^{\varphi} = (c^2 \cdot c^{-1}ncm, c^2 \cdot c^{-1}mcn) = (c^2 n_1, c^2 m_1), \quad n_1, m \in N,$$

it follows that φ^k sends the pair (cn,cm) to a pair of the form $(\overline{n},\overline{m})$, $\overline{n},\overline{m} \in N$ which, by nilpotence of the group N, will be sent by some power of φ to a trivial pair. The theorem is proved. □

The description of finite ν-groups of odd order is achieved by the following theorem.

Theorem 3. *A finite ν-group of odd order is nilpotent.*

For the proof we will need some auxiliary results.

Lemma 1. *Let s and t be natural numbers with $(s,t)=1$. Then the matrix $A_{(s,t)}$ of the form*

$$A_{(s,t)} = \left\| \begin{array}{ccccccccccc} 1 & 0 & 0 & \cdots & 0 & -1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 & -1 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & -1 \\ -1 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 \\ 0 & -1 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & -1 & 0 & 0 & 0 & \cdots & 1 \\ \underbrace{\qquad\qquad\qquad}_{s} & & & & & \underbrace{\qquad\qquad\qquad}_{t} & & & & \end{array} \right\|$$

$$= E_{s+t} - \left\| \begin{array}{cc} 0_{t\times s} & E_t \\ E_s & 0_{s\times t} \end{array} \right\|,$$

has rank $s+t-1$. (Here E_q and $0_{r\times p}$ are the identity and zero matrices of the indicated sizes.)

Proof. Without loss of generality, we may assume that $s > t$ since otherwise we could transpose the matrix $A_{(s,t)}$. We now add the first row of $A_{(s,t)}$ to the $(t+1)$-st row, the second row to the $(t+2)$-nd row, and so on, finally adding row t to row $2t$. As a result of these operations we obtain the new matrix $A^{(1)}_{(s,t)}$ of the form

$$A^{(1)}_{(s,t)} = \left\| \begin{array}{c|c|c} E_t & 0_{t\times(s-t)} & -E_t \\ \hline 0_{s\times t} & \multicolumn{2}{c}{A_{(s-t,t)}} \end{array} \right\|.$$

Let $r(C)$ denote the rank of a matrix C. Clearly,

$$r(A_{(s,t)}) = t + r(A_{(s-t,t)}).$$

Since $(s-t,t)=1$, the proof is completed by induction:

$$r(A_{(s,t)}) = t + (s-t) + t - 1 = t + s - 1.$$

The lemma is proved. □

Lemma 2. *Let G be a ν-group, let p and q be distinct odd primes, and let $a \in G$ be an element such that a^q belongs to the centralizer of an element b of order p lying in an Abelian normal subgroup N of G. Then a belongs to the centralizer of b.*

Proof. Let $b_s = a^{-s}ba^s$. Obviously,

$$(ab,a)^\varphi = (a^2b_1, a^2b_0), \quad (a^2b_1, a^2b_0)^\varphi = (a^4b_3b_0, a^4b_2b_1),$$

and so on. The indices of the elements b are reduced modulo q, and the powers of the elements b_r are reduced modulo p. A pair

$$C = \big(a^{2^i} b_0^{k_0} b_1^{k_1} \cdots b_{q-1}^{k_{q-1}},\ a^{2^i} b_0^{\ell_0} b_1^{\ell_1} \cdots b_{q-1}^{\ell_{q-1}} \big),$$

is sent by φ to the pair

$$C^\varphi = \big(a^{2^{i+1}} b_{2^i}^{k_0} b_{2^i+1}^{k_1} \cdots b_{2^i+q-1}^{k_{q-1}} b_0^{\ell_0} b_1^{\ell_1} \cdots b_{q-1}^{\ell_{q-1}},\ a^{2^{i+1}} b_{2^i}^{\ell_0} b_{2^i+1}^{\ell_1} \cdots b_{2^i+q-1}^{\ell_{q-1}} b_0^{k_0} b_1^{k_1} \cdots b_{q-1}^{k_{q-1}} \big).$$

Consider the q-dimensional vector space Q over the field of congruence classes modulo p. If $a = (\alpha_0, \alpha_1, \ldots, \alpha_{q-1}) \in Q$ then we set $a_{(1)} = (\alpha_{q-1}, \alpha_0, \alpha_1, \ldots, \alpha_{q-2})$, and by induction $a_{(t)} = (a_{(t-1)})_{(1)}$. To the pair C we assign the number 2^i and the vector $c \in Q$ of the form

$$c = (k_0 - \ell_0, k_1 - \ell_1, \ldots, k_{q-1} - \ell_{q-1}), \qquad C \mapsto (2^i, c).$$

Obviously, in this way, to the pair C^φ will be assigned the pair $(2^{i+1}, C_{(2^i)} - C)$:

$$C^\varphi \mapsto (2^{i+1}, C_{(2^i)} - C).$$

If we start transforming consecutively (with φ) the pair $(a^2 b_1, a^2 b_0)$, then all the vectors in Q that correspond to the resulting pairs will belong to the subspace Q' which consists of vectors for which the sum of the coordinates equals zero. Since the number of vectors in Q' is finite, and the numbers 2^i can be reduced modulo q, it follows that there will be repetitions in the indicated sequence of vectors for which the corresponding numbers are congruent modulo q.

On the other hand, if we wish to recover C from the known vector $C^{(2^i)} - C$, then we obtain a system of q linear equations with q unknowns, such that the coefficient matrix has the form $A_{(s,t)}$, $(s,t) = 1$, which by Lemma 1 is a matrix of rank $q-1$. Its columns, as well as the column of constant terms, are vectors in the subspace Q'. Clearly, this system of equations will have a unique solution in Q'. The above-mentioned sequence of vectors will therefore be periodic, and the vector $(-1, 1, 0, \ldots, 0)$ which begins the sequence will reoccur as far from the beginning as we wish. However, at a sufficient distance from the beginning of the sequence, all occurring pairs will be trivial, and hence the pair $(a^s b_1, a^s b_0)$ corresponding to our vector will also be trivial. Therefore $b_1 = b_0$ and $ab = ba$. The lemma is proved. □

Proof. (of Theorem 3) Assume that the claim of the theorem is valid for groups that have order less than that of G. Then all subgroups of G are supersolvable, and therefore the group G is solvable [3]; hence one of the commutator subgroups $G^{(s)}$ is an Abelian normal subgroup.

Let N_p be the primary component of $G^{(s)}$ relative to a prime number p, and let d be one of the elements of order p in N_p. The element d lies in a normal subgroup $\widetilde{N}_p \subseteq G$ all of whose elements have order p. By the inductive hypothesis, the quotient group $G/\widetilde{N}_p$ is nilpotent, and hence is the direct product of its Sylow subgroups. The subgroup $Q_p \subseteq G$, that corresponds to the Sylow p-subgroup of

$G/\widetilde{N}_p$, is the unique Sylow p-subgroup, and thus is a normal subgroup of G. Its center Z_p is also a normal subgroup of G. Let b be an element of order p in Z_p, and let a be an element of order m with $(m,p)=1$. If q is one of the prime factors of m, then by Lemma 2 the element $a^{m/q}$ lies in the centralizer of b. Considering the prime factorization of m/q, and repeating the argument as many times as required, we arrive at the statement that a lies in the centralizer of b.

Therefore, the element b is in the center Z of the group G. The quotient group G/Z of G by the (non-trivial) center Z is nilpotent by the inductive hypothesis. Therefore G is also nilpotent. Theorem 3 is proved. □

Below we will give a complete description of finite ν-groups. To this end, we first prove two more lemmas.

Lemma 3. *If a ν-group G has an Abelian normal subgroup N which is a 2-group of odd index, then N is a direct factor of G.*

Proof. Assume that the statement of the lemma is valid for groups whose order is smaller than that of G.

Let $a \in N$, $a^2 = e$, $b \in G$. Since $(aba, b)^\varphi = (a \cdot baba \cdot a, baba)$, it is clear that the mapping φ replaces b by $baba$. We form the sequence

$$b_1 = b, \quad b_2 = b_1 a b_1 a, \quad \ldots, \quad b_i = b_{i-1} a b_{i-1} a, \quad \ldots.$$

Since G is a ν-group, for some n we have $ab_n a = b_n$, i.e., $(ab_{n-1})^2 = (b_{n-1}a)^2$. On the other hand, for some q we have $(ab_{n-1})^{2q+1} \in N$. Hence

$$(ab_{n-1})^{2q+1} a = a(ab_{n-1})^{2q+1}.$$

But $(ab_{n-1})^{2q+1}a = a(b_{n-1}a)^{2q+1}$. Therefore $(ab_{n-1})^{2q+1} = (b_{n-1}a)^{2q+1}$, and hence $ab_{n-1} = b_{n-1}a$. From this we see that the equation $ab_n a = b_n$ implies $ab_{n-1}a = b_{n-1}$. It immediately follows that $ab = ba$. Therefore, the elements of order 2 of the group N form a subgroup Z of the center of G.

By the inductive hypothesis, the quotient $\overline{G} \simeq G/Z$ decomposes as a direct product $\overline{G} = \overline{P} \times \overline{N}$ where $\overline{P}$ is a subgroup of odd order, and the intersection of the corresponding subgroup $P \subseteq G$ with N is Z. By the inductive hypothesis, $P = P_1 \times Z$. Since the group P_1 coincides with the set of all elements of odd order in P, it follows that P_1 is a normal subgroup of G, and the elements of P_1 commute with the elements of N. Therefore, $G = P_1 \times N$. The lemma is proved. □

Lemma 4. *If a Sylow 2-subgroup N of a finite ν-group G is normal, then it is a direct factor.*

Proof. The center Z of N is a normal subgroup of G. Performing induction on the index of nilpotence of N, we consider the quotient group $\overline{G} \simeq G/Z$. Now the argument is completely identical to that concluding the proof of Lemma 3. □

Theorem 4. *The extensions of nilpotent groups of odd order by 2-groups are the only ν-groups among finite groups.*

Proof. According to Theorem 2, it suffices to prove that any finite ν-group is an extension of a nilpotent group of odd order by a 2-group.

We choose a Sylow 2-subgroup Q in the ν-group G, an arbitrary subgroup $S \subseteq Q$, and an element a of odd order in the normalizer of S. Then in the group $T = \langle a, S\rangle$ generated by a and S, the group S will be a normal Sylow 2-subgroup, and hence a direct factor by Lemma 4. Therefore, the element a is in the centralizer of the group T. Now appealing to the well-known result on the existence of p-complements [1, Theorem 14.4.7] we conclude that G has a normal subgroup of odd order for which the corresponding quotient group is a 2-group. The theorem is proved. □

Theorem 4 gives a complete description of finite ν-groups.

4. One subclass of ν-groups

With each element c of a semigroup G, we can associate a mapping φ_c from the set S of pairs of elements of G to itself that sends the pair (a, b) to the pair (acb, bca):

$$(a, b)^{\varphi_c} = (acb, bca).$$

If the semigroup G has an identity element e, then it is clear that the map φ_e coincides with the mapping φ considered earlier. All possible mappings φ_c generate a semigroup $[G]$, of self-mappings of the set S, which we will call *adjoint* to G.

In the theory of semigroups, two completely different concepts of nilpotence are used, brought to the theory of semigroups on the one hand from ring theory and on the other hand from group theory. We need to distinguish them.

Definition 2. A semigroup G with zero is called *r-nilpotent* if there exists a natural number n such that $a_1 a_2 \cdots a_n = 0$ for all elements a_i of G.

A.I. Malcev [4] gave the following definition in a slightly different form.

Definition 3. A semigroup G is called *g-nilpotent* if the adjoint semigroup $[G]$ is r-nilpotent. (The role of zero in $[G]$ is played by the mapping which sends any pair in S to a trivial pair.)

A.I. Malcev showed in the same work that if G is a group, then the concept of g-nilpotence coincides with the usual concept of nilpotence for groups.

Definition 4. A pair (a, b) in S will be called *m-central* and written $(a, b)_m$ if every element of the semigroup $[G]^m$ sends it to a trivial pair.

Lemma 5. *In a group G with generators c_1, c_2, …, c_k, the condition $(a, b)_n$ is equivalent to the conjunction of the conditions $(ab, ba)_{n-1}$ and $(ac_i b, bc_i a)_{n-1}$ for $i = 1, 2, \ldots, k$.*

Proof. By definition, we declare that $(a, b)_0$ means $a = b$. Obviously, the condition $(a, b)_n$ implies the indicated $k + 1$ conditions.

For the proof of the converse, we first take $n = 1$. Then we have $ab = ba$ and $ac_ib = bc_ia$ for $i = 1, 2, \ldots, k$. The following equations are obvious: $c_iba^{-1} = a^{-1}bc_i$ and $ba^{-1} = a^{-1}b$. Clearly, the element $a^{-1}b$ lies in the center. Therefore, for any d we have $adb = bda$, i.e., $(a, b)_1$. Now suppose that the lemma has been proved for all natural numbers less than n, and that the following conditions hold:

$$(ab, ba)_{n-1}, \quad (ac_ib, bc_ia)_{n-1}, \quad i = 1, 2, \ldots, k.$$

Obviously, the center Z of G is non-trivial. Denoting by $\overline{d}$ the image of an element $d \in G$ in the quotient group $\overline{G} \simeq G/Z$, we have

$$(\overline{a}\overline{b}, \overline{b}\overline{a})_{n-2}, \quad (\overline{a}\,\overline{c}_i\,\overline{b}, \overline{b}\,\overline{c}_i\,\overline{a})_{n-2}, \quad i = 1, 2, \ldots, k.$$

From the inductive hypothesis it follows that $(\overline{a}, \overline{b})_{n-1}$, i.e., any element from $[\overline{G}]^{n-1}$ sends the pair $(\overline{a}, \overline{b})$ to a pair of the form $(\overline{d}, \overline{d})$. This means that any element of $[G]^{n-1}$ sends the pair (a, b) to a pair of the form (d, dz), $z \in Z$, and hence any element of $[G]^n$ sends the pair (a, b) to a trivial pair, i.e., we have $(a, b)_n$. The lemma is proved. □

The lemma easily implies the following interesting property of 3-Engel groups.

Theorem 5. *Any two conjugate elements of a* 3*-Engel group generate a* 2*-Engel group.*

Proof. In the 3-Engel group G we choose any two conjugate elements a and b, which can always be written in the form $a = cd$ and $b = dc$ with $c, d \in G$. From equations (1) and (2) it follows that

$$ab^2a = ba^2b, \quad ab^3a = babab, \quad ba^3b = ababa.$$

From Lemma 5 it follows that the condition $(ab, ba)_1$ holds in the group G_1 generated by a and b. Now we prove the condition $(a, b)_2$ for which it suffices to verify the conditions $(a^2b, ba^2)_1$ and $(ab^2, b^2a)_1$. By the obvious symmetry we will prove only the condition $(a^2b, ba^2)_1$, which is equivalent to the equations:

$$a^2b^2a^2 = ba^4b, \quad a^2baba^2 = ba^5b, \quad a^2b^3a^2 = ba^2ba^2b.$$

However,

$$a^2b^2a^2 = aba^2ba = ba^4b,\ a^2baba^2 = aba^3ba = ba^5b,\ a^2b^3a^2 = abababa = ba^2ba^2b,$$

where we have used in every case the condition $(ab, ba)_1$, i.e., $abqba = baqab$ for all $q \in G_1$. The theorem is proved. □

The result of Theorem 5 suggests the following definition.

Definition 5. Abelian groups will be called σ_1*-groups*. Any group in which any two conjugate elements generate a σ_{i-1}-group will be called a σ_i*-group*. Finally, σ_i-groups, as i ranges over all natural numbers, will be called σ*-groups*.

Remark 2. We can also speak of σ-semigroups if by conjugate elements we understand elements of the form xy and yx.

Remark 3. Obviously, σ-groups lie in the intersection of the classes of ν-groups and Engel groups. It is not known to the author whether there exist Engel groups that are not σ-groups. Local nilpotence of σ_k-groups for $k > 3$ is also unclear.

Definition 6. A group G will be called *weakly nilpotent of bounded index* if there exists a natural number k such that any subgroup of G generated by two elements is nilpotent with nilpotence index less than or equal to k.

Theorem 6. *Every weakly nilpotent group of bounded index is a σ-group.*

Proof. Let G be a weakly nilpotent group of weak nilpotence index not exceeding k. We show that any two conjugate elements in G generate a nilpotent subgroup of nilpotence index not exceeding $k-1$. In what follows, by the symbol $(c_1, c_2, \ldots, c_s)$ we will understand the simple commutator in the sense of M. Hall's book [1]. Suppose elements x_1 and $x_2 = y^{-1}x_1y$ generate a subgroup Q in G. In any simple commutator $t = (x_{i1}, x_{i2}, \ldots, x_{ik})$ where i_s takes values 1 or 2, we have either $x_{i1} = x_{i2}$ and hence $t = e$, or the commutator (x_{i1}, x_{i2}) can be written as a triple commutator. Indeed,

$$(x_1, x_2) = (x_1, y^{-1}x_1y) = (y^{-1}x_1y, y^{-1}, y^{-1}x_1y),$$
$$(x_2, x_1) = (y^{-1}x_1y, x_1) = (x_1, y_1, x_1).$$

Therefore any commutator t of the indicated form is equal to the identity in G. The proof that the nilpotence index of Q does not exceed $k-1$, and hence the proof of Theorem 6 (by an obvious induction), follow immediately from the next lemma. □

Lemma 6. *Let the group F be generated by a_1, a_2, …, a_m. Then any normal subgroup that contains all simple commutators of the form $\alpha_i = (a_{i1}, a_{i2}, \ldots, a_{it})$, $i_s = 1, 2, \ldots, m$, where t is an arbitrary natural number, contains F_t (term t in the lower central series).*

Proof. For $t = 1$ the statement is trivial. Suppose now that $\tau = (q_1, q_2, \ldots, q_{t-1}, q_t)$ is an arbitrary simple commutator, $q_i \in F$. By the inductive hypothesis, we conclude that the commutator $\tau' = (q_1, q_2, \ldots, q_{t-1})$ lies in the normal subgroup generated by the commutators of the form $A_i = (a_{i1}, a_{i2}, \ldots, a_{i_{t-1}})$, i.e., $\tau' = \prod_i \ell_i^{-1} A_i \ell_i$. Using the well-known formulas relating commutators,

$$(xy, z) = y^{-1}(x, z)y(y, z), \qquad (x, yz) = (x, z)z^{-1}(x, y)z,$$
$$(x^{-1}, y) = x(x, y)^{-1}x^{-1}, \qquad (x, y^{-1}) = y(x, y)^{-1}y^{-1},$$

we convince ourselves that the commutator τ lies in any normal subgroup containing all commutators of the form $(\ell_i^{-1}A_i\ell_i, a_i)$, and hence in the normal subgroup generated by the commutators $(A_i, \ell_i a_i \ell_i^{-1})$. Using the stated formulas one more time, we arrive at the conclusion that τ is contained in the normal subgroup generated by all commutators of the form α_i. If N is the normal subgroup generated in

F by all commutators of the form α_i, then the quotient group $\overline{F} \simeq F/N$ satisfies the following identical relation:

$$(x_1, x_2, \ldots, x_t) = e,$$

which is equivalent to the statement of the lemma. The lemma, and hence Theorem 6, are proved. □

It is very probable that the converse of Theorem 6 is also true.

References

[1] M. Hall, *The Theory of Groups*, Macmillan, New York, 1959.

[2] H. Heineken, *Engelsche Elemente der Länge drei*, Illinois J. Math. 5, 4 (1961) 681–707.

[3] B. Huppert, *Normalteiler und maximale Untergruppen endlicher Gruppen*, Math. Z. 60 (1954) 409–434.

[4] A.I. Malcev, *Nilpotent semigroups*, Ivanov. Gos. Ped. Inst. Uch. Zap. Fiz.-Mat. Nauki 4 (1953) 107–111.

On Some Identical Relations for Algebras

A.I. Shirshov

1. In the work of A.I. Malcev [2], results of a general nature are applied in particular to the classification of identical relations of degree 3 for associative algebras. It is shown there that, under natural assumptions on the characteristic, any such identical relation is a linear combination of the following relations:

$$\sum_{(i_1,i_2,i_3)} x_{i_1}x_{i_2}x_{i_3} = 0, \tag{1}$$

$$\sum_{(i_1,i_2,i_3)} (-1)^{\sigma_i} x_{i_1}x_{i_2}x_{i_3} = 0, \tag{2}$$

$$x_1x_2x_3 + x_2x_1x_3 - x_2x_3x_1 - x_3x_2x_1 = 0, \tag{3}$$

$$x_1x_2x_3 + x_1x_3x_2 - x_3x_1x_2 - x_3x_2x_1 = 0, \tag{4}$$

where the summations in relations (1) and (2) are performed over all substitutions, and σ_i is the number of inversions in the permutation (i_1, i_2, i_3) of 1, 2, 3.

In the present note, we study algebras that satisfy one of the relations (3) and (4) and show that such algebras, in a sense to be made precise later, are close to commutative. In conclusion, we give and study a generalization of this closeness to commutativity.

2. For brevity, throughout this note, algebras with relations (3) and (4) will be called μ-algebras and μ'-algebras respectively.

Theorem 1. *Let S be a μ-algebra over a field P of characteristic $\neq 2$. Then the ideal S^3 lies in the center Z of S, and the ideal S^2 is commutative.*

Proof. It is easy to see that when relation (3) holds identically, these relations follow:

$$x_2x_4x_3x_1 + x_4x_2x_3x_1 - x_4x_3x_1x_2 - x_3x_1x_4x_2 = 0, \tag{5}$$

$$-x_3x_4x_2x_1 - x_4x_3x_2x_1 + x_4x_2x_1x_3 + x_2x_1x_4x_3 = 0, \tag{6}$$

Sibirsk Mat. Zh. 7, (1966), no. 4, 963–966

$$-x_2x_1x_4x_3 - x_1x_2x_4x_3 + x_1x_4x_3x_2 + x_4x_3x_1x_2 = 0, \tag{7}$$

$$-x_3x_4x_1x_2 - x_4x_3x_1x_2 + x_4x_1x_2x_3 + x_1x_2x_4x_3 = 0, \tag{8}$$

$$x_3x_4x_1x_2 + x_4x_3x_1x_2 - x_4x_1x_3x_2 - x_1x_4x_3x_2 = 0, \tag{9}$$

$$-x_2x_4x_3x_1 - x_4x_2x_3x_1 + x_4x_3x_2x_1 + x_3x_4x_2x_1 = 0, \tag{10}$$

$$-x_4x_2x_1x_3 - x_4x_1x_2x_3 + x_4x_1x_3x_2 + x_4x_3x_1x_2 = 0. \tag{11}$$

Adding equations (5)–(11) we obtain

$$x_4x_3x_1x_2 - x_3x_1x_4x_2 = 0. \tag{12}$$

Furthermore, the relations

$$x_4x_2x_1x_3 - x_2x_1x_4x_3 = 0, \tag{13}$$

$$x_4x_1x_2x_3 - x_1x_2x_4x_3 = 0, \tag{14}$$

are corollaries of relation (12). If we subtract the left side of relation (7) from the sum of the left sides of relations (11), (13), (14) then we obtain

$$x_4x_1x_3x_2 - x_1x_4x_3x_2 = 0. \tag{15}$$

Relations (12) and (15) together are equivalent to a system of relations of the form

$$x_1x_2x_3x_4 - x_{i_1}x_{i_2}x_{i_3}x_4 = 0, \tag{16}$$

where (i_1, i_2, i_3) is an arbitrary permutation of 1, 2, 3. Using relation (16) we rewrite relation (11) in the form

$$2x_4x_1x_3x_2 - 2x_2x_4x_1x_3 = 0,$$

or equivalently,

$$x_2(x_4x_1x_3) = (x_4x_1x_3)x_2. \tag{17}$$

Finally, repeated application of the last relation gives

$$(x_2x_4)(x_1x_3) = (x_1x_3)(x_2x_4). \tag{18}$$

The last two relations constitute the statement of the theorem. □

Remark 1. It follows from the proof that the restriction on characteristic is only essential in the derivations of relations (17) and (18); relation (16) is valid without restriction.

Remark 2. From the fact that an algebra which is anti-isomorphic to a μ-algebra is a μ'-algebra, it follows that Theorem 1 holds also for μ'-algebras.

3. Consider the following properties of an algebra A:

α) some power A^k of A is a commutative algebra;
β) some power A^t of A lies in the center.

Lemma 1. *Properties α and β are equivalent.*

Proof. Obviously, β implies α. Now, if A satisfies property α, then it is obvious that

$$\begin{aligned}(x_1x_2\cdots x_k)(x_{k+1}\cdots x_{2k}x_{2k+1}) &= (x_{k+1}\cdots x_{2k})(x_{2k+1}x_1\cdots x_k)\\ &= x_{2k+1}x_1\cdots x_kx_{k+1}\cdots x_{2k}.\end{aligned}$$

In other words, A satisfies property β for $t = 2k$. □

Definition 1. An algebra A that satisfies α and β will be called a *KD-algebra.*

The statement of Theorem 1 can be strengthened using the following lemma.

Lemma 2. *If every algebra A satisfying a multilinear identical relation*

$$F(x_1, x_2, \ldots, x_k) = 0,$$

over a field of characteristic zero is a KD-algebra, then every algebra B over the same field satisfying an identical relation of the form

$$F(x_1^{t_1}, x_2^{t_2}, \ldots, x_k^{t_k}) = 0,$$

where the t_i are arbitrary natural numbers, is also a KD-algebra.

Proof. Let $t = \max(t_1, t_2, \ldots, t_k)$. Then it was shown by Higman [1] that there exists a natural number $f(t)$ such that any element of the ideal $B^{f(t)}$ can be written as a linear combination of the s-th powers of elements of B, where s is any natural number less than or equal to t. From this it follows that the algebra $B^{f(t)}$ satisfies the identical relation $F(x_1, x_2, \ldots, x_k) = 0$, and thus by assumption $B^{f(t)}$ is a KD-algebra. Hence for some number q the algebra $[B^{f(t)}]^q = B^{qf(t)}$ is commutative. □

Theorem 2. *Any algebra A with identical relation*

$$x_1^{t_1}x_2^{t_2}x_3^{t_3} + x_2^{t_2}x_1^{t_1}x_3^{t_3} - x_2^{t_2}x_3^{t_3}x_1^{t_1} - x_3^{t_3}x_2^{t_2}x_1^{t_1} = 0, \tag{19}$$

over a field of characteristic zero, is a KD-algebra.

Remark 3. The result of Higman used above allows us to point out that for algebras over a field of characteristic zero, any identity of the form

$$x^py^q - y^qx^p = 0, \tag{20}$$

is equivalent to the definition of a KD-algebra.

4. The study of KD-algebras is of interest, if only for the reason that they include commutative and nilpotent algebras. But there is yet another reason.

Definition 2. An associative algebra is called *locally Noetherian* if every increasing chain of right ideals of every finitely generated subalgebra stabilizes after a finite number of steps.

Theorem 3. *Every KD-algebra is locally Noetherian.*

Proof. Obviously, a finitely generated subalgebra S of a KD-algebra is itself a KD-algebra, and hence is an extension of the commutative finitely generated algebra S^m by the nilpotent finite-dimensional algebra S/S^m; in both of these algebras, every increasing chain of right ideals must terminate. Hence, for any increasing chain of right ideals $J_1 \subset J_2 \subset \cdots \subset J_n \subset \cdots$ there exists a number k such that $S^m \cap J_k = S^m \cap J_{k+r}$ and $\overline{J}_k = \overline{J}_{k+r}$, where $\overline{J}_p$ is the pre-image of the ideal J_p under the natural homomorphism of S onto S/S^m, and r is any natural number. This immediately implies that $J_k = J_{k+r}$. □

Corollary. *An algebra with identical relation* (19) *over a field of characteristic zero is locally Noetherian.*

5. It is well known that the sum of any finite number of nilpotent ideals is a nilpotent ideal. On the other hand, it is not difficult to construct an example of an algebra in which the sum of two commutative ideals is not a commutative ideal. For this reason, the following result is of interest.

Theorem 4. *The sum of any finite number of KD-ideals* (*i.e., ideals that are KD-algebras*) *of an algebra A is again a KD-ideal.*

Proof. It suffices to prove the claim for two ideals. Let J_1 and J_2 be KD-ideals of the algebra A, and let Z_1 and Z_2 be their respective centers. Then

$$J_1^{t_1} \subset Z_1, \qquad J_2^{t_2} \subset Z_2, \qquad (J_1 + J_2)^{t_1+t_2-1} \subset Z_1 + Z_2.$$

If z_1, z_1', $z_1'' \in Z_1$ and z_2, z_2', $z_2'' \in Z_2$ then

$$(z_1 + z_2)(z_1' + z_2')(z_1'' + z_2'') = (z_1'' + z_2'')(z_1 + z_2)(z_1' + z_2'),$$

which can be easily and immediately verified. The commutativity of the ideal

$$[(J_1 + J_2)^{t_1+t_2-1}]^2 = (J_1 + J_2)^{2t_1+2t_2-2},$$

follows from this. □

Remark 4. The theorem just proved could be used in an obvious way to construct KD-radicals analogous to radicals based on nilpotency.

References

[1] G. Higman, *On a conjecture of Nagata*, Proc. Cambridge Philos. Soc. 52, 1 (1956) 1–4.

[2] A.I. Malcev, *On algebras with identical defining relations*, Mat. Sbornik 26, (1950), no. 1, 19–33.

On Some Positively Definable Varieties of Groups

A.I. Shirshov

1. A variety $\mathfrak{N}$ of groups will be called *positively definable* if it can be defined by identical relations that do not include variables with negative powers.

For example, the variety of Abelian groups is obviously positively definable. A.I. Malcev [2] proved positive definability of the varieties of nilpotent groups (with a given index of nilpotence) and showed that the varieties of solvable groups are not positively definable. In the author's work [3], it is also shown that the varieties of Engel groups for $n = 2$ and $n = 3$ are positively definable, and are determined respectively by the identities (A) and (B):

$$xy^2x = yx^2y, \tag{A}$$

$$xy^2xyx^2y = yx^2yxy^2x, \quad xy^2xyxy^2y = yx^2y^2x^2y^2x. \tag{B}$$

In the present note, we prove positive definability for a sufficiently broad class of varieties, which generalizes the class of n-nilpotent groups introduced by Baer [1].

Let $[a, b]_s = (ab)^s b^{-s} a^{-s}$ where a, b are elements of a group G and s is an integer, and let $(k) = (k_1, k_2, \ldots, k_t)$ be a t-tuple of integers.

Definition 1. A group G is called *nilpotent relative to the t-tuple* (k) if for any elements a_i, $i = 0, 1, 2, \ldots, t$, the following equality holds:

$$(a_0, a_1, \ldots, a_t)_{(k)} \stackrel{\text{def}}{=} [[\ldots[a_0, a_1]_{k_1}, \ldots]_{k_{t-1}}, a_t]_{k_t} = e. \tag{1}$$

Obviously, the collection of all groups that are nilpotent relative to a fixed t-tuple (k) is a variety. This variety will be denoted by

$$\mathfrak{N}_{(k)} = \mathfrak{N}_{(k_1, k_2, \ldots, k_t)}.$$

Special cases of varieties of the form $\mathfrak{N}_{(k)}$ are the n-nilpotent groups introduced by Baer [1]. The following statement holds.

Sibirsk Mat. Zh. 8 (1967), no. 5, 1190–1192

Theorem. *Any variety of the form $\mathfrak{N}_{(k)}$ is positively definable.*

2. We consider the so-called n-center of the group G.

Definition 2. The collection of all elements z in G, such that $[z,a]_n = e$ for all $a \in G$, is called the *n-center* of G and is denoted by $Z_n(G)$.

Obviously, $Z_{-1}(G)$ coincides with the center of G.

Lemma 1. *For every element $a \in G$ and every $z \in Z_n(G)$ we have $[a,z]_n = e$.*

Proof. The claim follows from the easily verified equation

$$[a,z]_n = a^n [z, z^{-1}a^{-1}]_n a^{-n},$$

and the definition of $Z_n(G)$. □

It is well known, and can be easily verified, that the n-center is a characteristic subgroup. The following statement can also be immediately verified.

Lemma 2. *We have $Z_n(G) = Z_{1-n}(G)$.*

3. We fix a t-tuple $(k) = (k_1, k_2, \ldots, k_t)$ and associate to it two sequences of recursively defined elements of the free group with generators x, y, z_1, z_2, …, z_t:

$$\left.\begin{array}{l} u_0 = x, \quad v_0 = y, \\ u_s = u_{s-1}^{k_s - 1}(v_{s-1}z_s)^{k_s-1}v_{s-1}, \quad v_s = v_{s-1}^{k_s}(z_s u_{s-1})^{k_s-1} \quad \text{for } k_s \geq 1, \\ u_s = u_{s-1}^{-k_s}(v_{s-1}z_s)^{-k_s}v_{s-1}, \quad v_s = v_{s-1}^{1-k_s}(z_s u_{s-1})^{-k_s} \quad \text{for } k_s < 1, \end{array}\right\} \quad (2)$$

for $s = 1, 2, \ldots t$.

Definition 3. A group G is called a *$\overline{(k)}$-group* if it satisfies the identical relation $u_t = v_t$.

Lemma 3. *A group G is a $\overline{(k)}$-group if and only if it is nilpotent relative to the t-tuple (k).*

Proof. We carry out induction on the length of (k), remarking that the case of length 1 is included in the general argument. We write $(k') = (k_1, k_2, \ldots, k_{t-1})$.

Assume it has been proved that any group nilpotent relative to (k') is a $\overline{(k')}$-group, and suppose that a group G is nilpotent relative to (k). Then

$$(a_0, a_1, \ldots, a_{t-1})_{(k')} \in Z_{k_t}(G) = Z_{1-k_t}(G).$$

For this reason, the group $\overline{G} = G/Z_{k_t}(G)$ is nilpotent relative to (k'), and hence by the inductive hypothesis it is a $\overline{(k')}$-group. Therefore,

$$u_{t-1}v_{t-1}^{-1} \in Z_{k_t}(G) = Z_{1-k_t}(G),$$

for any corresponding values of the words u_{t-1} and v_{t-1} in the group G. Hence for any $q \in G$ it follows that

$$(u_{t-1}v_{t-1}^{-1}v_{t-1}q)^\alpha = (u_{t-1}v_{t-1}^{-1})^\alpha (v_{t-1}q)^\alpha, \text{ where } \alpha = \max(k_t, 1-k_t).$$

In other words,

$$(u_{t-1}q)^{\alpha}(v_{t-1}q)^{-\alpha} = (u_{t-1}v_{t-1}^{-1})^{\alpha}. \tag{3}$$

Since the right side does not depend on q, it follows from (3) that

$$(u_{t-1}q)^{\alpha}(v_{t-1}q)^{-\alpha} = (u_{t-1}z_t)^{\alpha}(v_{t-1}z_t)^{-\alpha}, \tag{4}$$

which is valid for all values of z_t. Setting $q = v_{t-1}^{-1}u_{t-1}^{-1}$ in (4), and performing the obvious transformations, we obtain

$$(u_{t-1}v_{t-1}^{-1}u_{t-1}^{-1})^{\alpha}u_{t-1}^{\alpha} = (u_{t-1}z_t)^{\alpha}(v_{t-1}z_t)^{-\alpha},$$

$$u_{t-1}v_{t-1}^{-\alpha}u_{t-1}^{\alpha-1} = (u_{t-1}z_t)^{\alpha}(v_{t-1}z_t)^{-\alpha}, \tag{5}$$

$$u_{t-1}^{\alpha-1}(v_{t-1}z_t)^{\alpha-1}v_{t-1} = v_{t-1}^{\alpha}(z_tu_{t-1})^{\alpha-1}. \tag{6}$$

Therefore, the group G satisfies the identical relation $u_t = v_t$; i.e., it is a $\overline{(k)}$-group.

Conversely, suppose that G is a $\overline{(k)}$-group; i.e., it satisfies relation (6), and hence also (5). Since the left side of relation (5) does not depend on z_t, obviously relation (4) holds. If, in the latter relation, we set $z_t = v_{t-1}^{-1}p$, then we obtain

$$(u_{t-1}q)^{\alpha}(v_{t-1}q)^{-\alpha} = (u_{t-1}v_{t-1}^{-1}p)^{\alpha}p^{-\alpha}. \tag{7}$$

If, in relation (7), we make the two substitutions, $q = e$ and $q = p = e$, then we obtain respectively

$$u_{t-1}^{\alpha}v_{t-1}^{-\alpha} = (u_{t-1}v_{t-1}^{-1}p)^{\alpha}p^{-\alpha}, \tag{8}$$

$$u_{t-1}^{\alpha}v_{t-1}^{-\alpha} = (u_{t-1}v_{t-1}^{-1})^{\alpha}. \tag{9}$$

From these last relations it follows that

$$(u_{t-1}v_{t-1}^{-1}p)^{\alpha} = (u_{t-1}v_{t-1}^{-1})^{\alpha}p^{\alpha}, \tag{10}$$

for all $p \in G$; i.e., $u_{t-1}v_{t-1}^{-1} \in Z_{k_t}(G) = Z_{1-k_t}(G)$. By assumption, the group $\overline{G}$ is nilpotent relative to (k'), and hence G is nilpotent relative to (k). The lemma is proved. □

The statement of the theorem follows trivially from the lemma.

References

[1] R. Baer, *Factorization of n-soluble and n-nilpotent groups*, Proc. Amer. Math. Soc. 4 (1953), no. 1, 15–26.

[2] A.I. Malcev, *Nilpotent semigroups*, Ivanov. Gos. Ped. Inst. Uch. Zap. Fiz.-Mat. Nauki 4 (1953) 107–111.

[3] A.I. Shirshov, *On some groups which are nearly Engel*, Algebra Logika 2 (1963), no. 5, 5–18.

On the Definition of the Binary-Lie Property

A.I. Shirshov

In the present note we construct an example of an algebra over a field of characteristic 2 that satisfies the identical relations

$$x^2 = 0 \quad \text{and} \quad [(xy)y]x + [(yx)x]y = 0,$$

but is not binary-Lie. This example has been announced earlier [2]. For the necessary definitions and the history of the problem, see for example the work [1].

Over an arbitrary field P of characteristic 2, a 16-dimensional algebra A with basis a_i, $i = 1, 2, \ldots, 16$, is determined by the following multiplication table:

$a_i a_j = a_j a_i$ for $i, j = 1, 2, \ldots, 16$,

$a_1 a_2 = a_3$,	$a_1 a_3 = a_5$,	$a_1 a_4 = a_7$,	$a_1 a_5 = a_8$,
$a_1 a_6 = a_{10}$,	$a_1 a_7 = a_{12}$,	$a_1 a_9 = a_{13}$,	$a_1 a_{10} = a_{15}$,
$a_2 a_3 = a_4$,	$a_2 a_4 = a_6$,	$a_2 a_5 = a_7$,	$a_2 a_7 = a_9 + a_{10}$,
$a_2 a_8 = a_{11} + a_{12}$,	$a_2 a_{11} = a_{13}$,	$a_2 a_{12} = a_{15} + a_{16}$,	$a_3 a_4 = a_9$,
$a_3 a_5 = a_{11}$,	$a_3 a_7 = a_{14}$,	$a_4 a_5 = a_{16}$;	

all remaining products equal zero. It is easy to verify directly that the algebra A is generated by the elements a_1 and a_2; it is also obvious that $c^2 = 0$ for all $c \in A$.

Theorem. *The algebra A satisfies the identity*

$$[(xy)y]x + [(yx)x]y = 0, \tag{1}$$

but it is not a Lie algebra; i.e., it is not binary-Lie, since it is generated by two elements.

We remark that identity (1) is equivalent to the identity

$$J(xy, x, y) = 0, \tag{2}$$

where $J(x, y, z) \stackrel{\text{def}}{=} (xy)z + (yz)x + zx)y$ is the Jacobian of the elements x, y, z.

Algebra Logika 10, (1971), no. 1, 100–102.

Lemma. *If, for all distinct basis elements a_i, a_j, a_k, a_ℓ of the algebra A, the following equations hold,*

$$\Phi_1(a_i, a_j) \stackrel{\text{def}}{=} J(a_i a_j, a_i, a_j) = 0,$$

$$\Phi_2(a_i, a_j, a_k) \stackrel{\text{def}}{=} J(a_i a_j, a_i, a_k) + J(a_i a_k, a_i, a_j) = 0,$$

$$\Phi_3(a_i, a_j, a_k, a_\ell) \stackrel{\text{def}}{=}$$
$$J(a_i, a_j, a_k, a_\ell) + J(a_i a_\ell, a_k, a_j) + J(a_k a_j, a_i, a_\ell) + J(a_k a_\ell, a_i, a_j) = 0,$$

then A satisfies the identity (1)*: $\Phi_1(x, y) = 0$.*

Proof. It is easy to see (computing by hand if this is not clear) that

$$\Phi_1(a+b, c+d) = \Phi_1(a,c) + \Phi_1(a,d) + \Phi_1(b,c) + \Phi_1(b,d) + \Phi_2(a,c,d) + \Phi_2(b,c,d) + \Phi_2(c,a,b) + \Phi_2(d,a,b) + \Phi_3(a,c,b,d),$$

$$\Phi_2(a+b, c, a) = \Phi_2(a,c,d) + \Phi_2(b,c,d) + \Phi_3(a,c,b,d).$$

From the above equations, as well as the multilinearity of Φ_3, it follows that for all $u, v \in A$ the element $\Phi_1(u, v)$ can be written as a linear combination of the elements indicated in the statement of the lemma. In general, the indices i, j, k, ℓ occurring in this expression may coincide. But in this case, either the index of the corresponding Φ_s changes or we obviously obtain zero. The lemma is proved. □

Proof. (of the theorem) For the proof of the theorem, we assign to each basis element a_i the weights $p_j(a_i)$, $j = 0, 1, 2$, $i = 1, 2, \ldots, 16$, according to the following table:

$p_j(a_i)$	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9	a_{10}	a_{11}	a_{12}	a_{13}	a_{14}	a_{15}	a_{16}
p_0	1	1	2	3	3	4	4	4	5	5	5	5	6	6	6	6
p_1	1	0	1	1	2	1	2	3	2	2	3	3	3	3	3	3
p_2	0	1	1	2	1	3	2	1	3	3	2	2	3	3	3	3

It easy to verify that $p_s(a_i a_j) = p_s(a_i) + p_s(a_j)$, $s = 0, 1, 2$, if $a_i a_j \neq 0$. As a result of this remark and the lemma, it suffices for the proof of equation (1) to verify the vanishing only of those Φ for which the sum of all weights p_s, $s = 0, 1, 2$, of the arguments of the corresponding Jacobians, does not exceed the limit value; namely, $\Phi_1(a_1, a_2)$, $\Phi_2(a_1, a_2, a_3)$, $\Phi_2(a_1, a_2, a_4)$, $\Phi_2(a_2, a_1, a_3)$, $\Phi_2(a_2, a_1, a_5)$, $\Phi_2(a_3, a_1, a_2)$. The verification is obvious. On the other hand,

$$J(a_1, a_2, a_7) = a_{13} + a_{14} + a_{16} \neq 0.$$

The theorem is proved. □

Remark. Some quotients of the algebra A have the same property. For instance, it is easy to see that the subspace J of A with basis $\{a_6, a_8, a_9, a_{10}, a_{11}, a_{12}, a_{13}, a_{15}, a_{16}\}$ is an ideal, and that in the quotient $B = A/J$ we have $J(b_1, b_2, b_7) = b_{14} \neq 0$ where b_i is the image of a_i under the natural homomorphism of A onto B. Finally, if $P = GF(2)$, then B is a finite ring (with 128 elements) which satisfies the property indicated above.

References

[1] A.T. Gainov, *Binary-Lie algebras of characteristic* 2, Algebra Logika 8 (1969), no. 5, 505–522.

[2] A.I. Shirshov, *On a variety of rings*, Ninth All-Union Algebra Colloquium (Abstracts), Gomel, Belarus, 1968, pages 213–214.

On the Theory of Projective Planes

A.I. Shirshov and A.A. Nikitin

In 1976, in the special course on Projective Planes given at Novosibirsk State University, and later in 1977, in the report on Projective Planes given at the Fourteenth All-Union Algebra Conference, A.I. Shirshov presented the concept of a projective plane as a partial algebraic system. This approach allowed the formulation of a number of new problems, together with a new viewpoint on known results and problems in the theory of projective planes. In the present work, we discuss part of the results contained in the special course and in the report, and also some further developments.

In the study of projective planes, different authors starting with M. Hall [2] implicitly used a partial binary operation. Projective planes as a partial algebraic system were considered for the first time by Magari [7]. The works of Giovagnoli [1] and Kim and Roush [5] also follow this approach.

In [7] and [1], free and completely free projective planes were constructed as partial algebraic systems, in which every element was regarded as an equivalence class defined on the set of nonassociative words in the generators of the plane. In §2 of the present article, we give constructions of free and completely free projective planes as partial algebraic systems, in which each element is uniquely represented as a nonassociative word in the generators of the plane.

In the above-mentioned special course and report, A.I. Shirshov gave a construction of an embedding of the completely free projective plane with a finite number of generators into the completely free projective plane with four generators, and formulated the problem of constructing an embedding of the completely free projective plane with a countable number of generators into the completely free projective plane with a finite number of generators.

In 1972, Johnson [4] showed that every free projective plane with a finite number of generators is a homomorphic image of a completely free projective plane with four generators. In §4 of the present work, we show that in the completely free projective plane $\mathfrak{CF}(C_1)$ with four generators, there exists a countable

Algebra Logika 20, 3 (1981) 330–356.

subconfiguration $\mathfrak{C}_0$ such that $\mathfrak{CF}(C_1)$ is freely generated by $\mathfrak{C}_0$. Based on this result, we further prove that any finite or countably infinite projective plane is a homomorphic image of the completely free projective plane with four generators.

Theorems 1 and 2 were obtained by A.I. Shirshov, and Theorems 3 and 4 by A.A. Nikitin.

1. Preliminary definitions and results

1. Let A be an arbitrary nonempty set, and let A^0 and ${}^0A$ be subsets of A such that $A = A^0 \cup {}^0A$ and $A^0 \cap {}^0A = \emptyset$. In this case we will say that $(A^0, {}^0A)$ is a partition of A. Here one of the subsets A^0 and ${}^0A$ may be empty.

We now fix a partition $(A^0, {}^0A)$ of A. Elements a and b in A will be called *unitypical* relative to the partition $(A^0, {}^0A)$ if a and b belong to the same subset of the partition $(A^0, {}^0A)$. Otherwise, the elements a and b in A will be called *non-unitypical* relative to this partition.

Suppose now that on the set A, with a fixed partition $(A^0, {}^0A)$, a partial binary commutative operation $\cdot$ is defined, such that the following conditions hold:

1.1. If a and b are distinct unitypical elements of A relative to $(A^0, {}^0A)$, then the product $a \cdot b$ is defined.

1.2. If the product $a \cdot b$ is defined for elements a and b in A, then a and b are distinct unitypical elements, but a and $a \cdot b$ are non-unitypical relative to $(A^0, {}^0A)$.

1.3. If the products $a \cdot b$, $a \cdot c$ and $(a \cdot b) \cdot (a \cdot c)$ are defined for elements a, b and c in A, then we have

$$(a \cdot b) \cdot (a \cdot c) = a. \tag{1}$$

1.4. The set A contains pairwise distinct elements a, b, c and d such that the products $a \cdot b$, $b \cdot c$, $c \cdot d$ and $d \cdot a$ are defined and pairwise distinct.

Such a partial algebraic system $\langle A, (A^0, {}^0A), \cdot \rangle$ will be called a *projective plane*.

Suppose that a partial binary commutative operation $*$ is defined on the set A with a fixed partition $(A^0, {}^0A)$ such that Conditions 1.2 and 1.3 hold, as well as the condition

1.5. If the products $a * b$ and $a * c$ are defined for elements a, b and c in A, and $a * b \neq a * c$, then the product $(a * b) * (a * c)$ is also defined.

Here for the operation $*$ one or both of the Conditions 1.1 and 1.4 may not necessarily hold. A partial algebraic system with a partial binary commutative operation $*$ satisfying Conditions 1.2, 1.3 and 1.5 will occasionally be denoted by $\langle A, (A^0, {}^0A), * \rangle$.

Example 1. Let B be an arbitrary nonempty subset of elements of a projective plane $\mathfrak{P} = \langle A, (A^0, {}^0A), \cdot \rangle$. Then the partition $(A^0, {}^0A)$ of the set A of elements of the projective plane $\mathfrak{P}$ determines a partition $(B^0, {}^0B)$ of the set B where $B^0 = B \cap A^0$ and ${}^0B = B \cap {}^0A$. For the elements of B the concepts of unitypical

and non-unitypical elements are defined in the natural way relative to the partition $(B^0, {}^0B)$. The operation $\cdot$ defined in $\mathfrak{P}$ induces a partial binary commutative operation $\circ$ on the set B. For this operation $\circ$ Conditions 1.2, 1.3 and 1.5 hold.

Let $\mathfrak{A} = \langle A, (A^0, {}^0A), * \rangle$ be a partial algebraic system with a partial binary commutative operation $*$ satisfying Conditions 1.2, 1.3 and 1.5. We will say that an element a in A is a *divisor* of an element b in A if there exists an element c in A such that $b = a * c$. The set of all divisors of an element b in A will be denoted by $T_b^{\mathfrak{A}}$.

In what follows, the symbol of the operation $*$ defined in a partial algebraic system satisfying Conditions 1.2, 1.3 and 1.5 will be occasionally omitted if this does not lead to misunderstanding.

Proposition 1. *Let $\mathfrak{A} = \langle A, (A^0, {}^0A), * \rangle$ be a partial algebraic system with a partial binary commutative operation $*$ satisfying Conditions* 1.2, 1.3 *and* 1.5. *Then*

(a) *If the equation $ab = cd$ holds for elements a, b, c in A, and the product ac is defined, then we have $ab = ac$;*

(b) *If a, b, c and d are pairwise distinct elements of A^0 such that the elements ab, bc, cd and da are defined and pairwise distinct, then in the set ${}^0A$ there exist pairwise distinct elements $\overline{a}$, $\overline{b}$, $\overline{c}$ and $\overline{d}$ such that the elements $\overline{a}\overline{b}$, $\overline{b}\overline{c}$, $\overline{c}\overline{d}$ and $\overline{d}\overline{a}$ are defined and pairwise distinct.*

Proof. Indeed, if the product ac is defined and $ab \neq ac$, then from Condition 1.5 it follows that the products $(ab)(ac)$ and $(cd)(ac)$ are defined. From Condition 1.3 and the assumption of the proposition we obtain $a = (ab)(ac) = (cd)(ac) = c$. But this contradicts Condition 1.2. Therefore, $ab = ac$ and part (a) is proved.

For the proof of part (b) it suffices to set $\overline{a} = ab$, $\overline{b} = bc$ and $\overline{c} = cd$, $\overline{d} = da$ and then use the assumptions of the proposition, Conditions 1.3 and 1.5, and the statement of part (a). □

The following result holds:

Proposition 2. [1] *Let $\mathfrak{P} = \langle A, (A^0, {}^0A), * \rangle$ be a projective plane. Then, if the products ab, $(ab)c$ and $[(ab)c]a$ are defined for elements a, b and c, then the following equation holds:* $[(ab)c]a = ab$.

2. Now consider a set A with a fixed partition $(A^0, {}^0A)$ in a different situation. Suppose that a symmetric relation α is defined on the set A, such that α includes only pairs of elements which are non-unitypical relative to the partition $(A^0, {}^0A)$. If, for any elements a, b, c and d in A, the conditions $(a, c), (b, c), (a, d), (b, d) \in \alpha$ imply that at least one of the equations $a = b$, $c = d$ holds, then the relation α is called an *incidence relation relative to the partition* $(A^0, {}^0A)$. The system $\langle A, (A^0, {}^0A), \alpha \rangle$ thus obtained is sometimes called a *partial plane*.

[1] In this regard, see also [5].

If it does not lead to misunderstanding, then an incidence relation α relative to the partition $(A^0, {}^0A)$ will be called an *incidence relation*, and if a pair (a, b) belongs to α then we will sometimes say that the elements a and b are *incident*.

Remark 1. If the elements of A^0 are called 'points', and the elements of ${}^0A$ are called 'lines', and we declare that a point a is incident to a line b if and only if b passes through a, then as a result we obtain an interpretation of a partial plane. If we interchange the names of the elements of A^0 and ${}^0A$, then we obtain another interpretation which is sometimes called the 'dual' of the first interpretation.

Suppose now that on the set A there is a partition $(A^0, {}^0A)$, an incidence relation α relative to $(A^0, {}^0A)$, and a partial binary commutative operation $\cdot$ satisfying Conditions 1.2, 1.3 and 1.5 relative to $(A^0, {}^0A)$. We will say that the operation $\cdot$ and the relation α are *compatible* on A if the following conditions hold:

1.6. If the equation $a \cdot b = c$ holds for elements a, b and c in A, then we have $(a, c) \in \alpha$ and $(b, c) \in \alpha$.

1.7. If $(a, c) \in \alpha$ and $(b, c) \in \alpha$ and also $a \neq b$, then $a \cdot b$ is defined and we have $a \cdot b = c$.

In what follows, a partial algebraic system $\mathfrak{A} = \langle A, (A^0, {}^0A), \cdot, \alpha\rangle$, where the partial binary commutative operation $\cdot$ (satisfying Conditions 1.2, 1.3, 1.5) and the incidence relation α are compatible on A, will be called a *configuration*.

Remark 2. Condition 1.7 implies that the partial operation $\cdot$ in a configuration is uniquely determined by the incidence relation α.

Remark 3. Condition 1.6 implies that if, for each element a in a configuration $\mathfrak{A} = \langle A, (A^0, {}^0A), \cdot, \alpha\rangle$ either $T_a^{\mathfrak{A}} \neq \emptyset$ or there exists an element b in A such that $a \in T_b^{\mathfrak{A}}$, then the relation α is uniquely determined by the partial operation $\cdot$. If we define a symmetric relation $\widetilde{\alpha}$ on the set A in such way that $(a, b) \in \widetilde{\alpha}$ if and only if either $a \in T_b^{\mathfrak{A}}$ or $b \in T_a^{\mathfrak{A}}$, then we obtain the equation $\alpha = \widetilde{\alpha}$. In particular, it follows from this that the definition of projective plane given above is equivalent to the traditional definition, and that any partial plane can be considered as a configuration.

In what follows, we will sometimes omit the set of elements in the symbol for a configuration, and indicate only the partition. Thus, for example, $\mathfrak{A} = \langle (A^0, {}^0A), \cdot, \alpha\rangle$. Here we assume that $A = A^0 \cup {}^0A$ and $A^0 \cap {}^0A = \emptyset$.

Example 2. Let $\mathfrak{B} = \langle B, (B^0, {}^0B), \circ\rangle$ be one of the partial algebraic systems from Example 1, and let $\mathfrak{P} = \langle A, (A^0, {}^0A), \cdot\rangle$ be the projective plane containing $\mathfrak{B}$. Denote by α the incidence relation on A that is compatible with the operation $\cdot$ in $\mathfrak{P}$, and let β be the relation induced by α on the set B, namely $\beta = (B \times B) \cap \alpha$. Then β is an incidence relation compatible on B with the partial operation $\circ$ defined on $\mathfrak{B}$, and the partial algebraic system $\langle (B^0, {}^0B), \circ, \beta\rangle$ is a configuration.

3. At the present time in the theory of projective planes, it is traditional to use a number of definitions going back to [2, 3, 8, 9]. Below in this subsection, we give

the corresponding definitions and concepts in the form that is convenient for the rest of this paper.

A configuration $\mathfrak{B} = \langle (B^0, {}^0B), \circ, \beta \rangle$ will be called an *extension* of a configuration $\mathfrak{A} = \langle (A^0, {}^0A), \cdot, \alpha \rangle$ if $B^0 \supseteq A^0$, ${}^0B \supseteq {}^0A$ and $\beta \supseteq \alpha$.

Remark 4. It immediately follows from this definition, and the compatibility of the corresponding operations and incidence relations in the configurations $\mathfrak{A}$ and $\mathfrak{B}$, that if the product $a \cdot b$ is defined for elements a and b in $\mathfrak{A}$, then the product $a \circ b$ is also defined in $\mathfrak{B}$ and we have $a \cdot b = a \circ b$.

If $\mathfrak{B}$ is an extension of a configuration $\mathfrak{A}$, then $\mathfrak{A}$ will sometimes be called a *subconfiguration* of $\mathfrak{B}$; this will be written in the form $\mathfrak{B} \supseteq \mathfrak{A}$ or $\mathfrak{A} \subseteq \mathfrak{B}$.

An extension $\mathfrak{B}$ of a configuration $\mathfrak{A}$ will be called a *one-step extension*, if for any element a in $\mathfrak{B}$ that is not contained in $\mathfrak{A}$, there exist elements b and c in $\mathfrak{A}$ such that $a = bc$.

A one-step extension $\mathfrak{B}$ of a configuration $\mathfrak{A}$ will be called a *complete* one-step extension if for any two distinct unitypical elements a and b in $\mathfrak{A}$, there exists an element c in $\mathfrak{B}$ such that $ab = c$.

A one-step extension $\mathfrak{B}$ of a configuration $\mathfrak{A}$ will be called a *free* one-step extension if for any element a in $\mathfrak{B}$ that is not contained in $\mathfrak{A}$, there exist two and only two elements b and c in $\mathfrak{A}$ such that $a = bc$.

An extension $\mathfrak{B}$ of a configuration $\mathfrak{A}$ will be called a *complete free* one-step extension if this extension is simultaneously a complete one-step extension and a free one-step extension.

We will say that a configuration $\mathfrak{A} = \langle A, (A^0, {}^0A), \cdot, \alpha \rangle$ is *closed* if the operation $\cdot$ satisfies Condition 1.1.

A subconfiguration $\mathfrak{A}$ of a configuration $\mathfrak{B}$ will be called a *closed* subconfiguration if $\mathfrak{A}$ is closed as a configuration.

A closed subconfiguration $\mathfrak{A}$ of a projective plane $\mathfrak{P}$ will be called a *projective subplane* in $\mathfrak{P}$ if $\mathfrak{A}$ is a projective plane.

Let $\mathfrak{B}$ be a closed configuration and let $\mathfrak{A}$ be a subconfiguration of $\mathfrak{B}$. We denote by $\langle \mathfrak{A} \rangle_{\mathfrak{B}}$ the intersection of all closed subconfigurations in $\mathfrak{B}$ that contain $\mathfrak{A}$ as a subconfiguration.

For a subconfiguration $\mathfrak{A}$ in a closed configuration $\mathfrak{B}$, we set by definition $\mathfrak{A}^{[0]} = \mathfrak{A}$. Now, if for a natural number i the configuration $\mathfrak{A}^{[i-1]}$ is defined, then by $\mathfrak{A}^{[i]}$ we denote the complete one-step extension of the configuration $\mathfrak{A}^{[i-1]}$ in $\mathfrak{B}$. Then we have the following result.

Proposition 3. [2] *The configuration* $\langle \mathfrak{A} \rangle_{\mathfrak{B}}$ *is closed and we have* $\langle \mathfrak{A} \rangle_{\mathfrak{B}} = \bigcup_{i=0}^{\infty} \mathfrak{A}^{[i]}$.

We will say that a closed configuration $\mathfrak{B}$ is *generated by* a configuration $\mathfrak{A}$ if we have $\langle \mathfrak{A} \rangle_{\mathfrak{B}} = \mathfrak{B}$.

In the case when a closed configuration $\mathfrak{B}$ is generated by a configuration $\mathfrak{A}$, and for any natural number i the one-step extension $\mathfrak{A}^{[i]} \supseteq \mathfrak{A}^{[i-1]}$ is a complete free one-step extension, then we will say that $\mathfrak{B}$ is *freely* generated by $\mathfrak{A}$.

[2] See also for example Theorem 11.3 in [3].

A projective plane $\mathfrak{P}$ is called *free* if $\mathfrak{P}$ is freely generated by a configuration $\mathfrak{A} = \langle (A^0, {}^0A), \cdot, \alpha \rangle$ such that the set ${}^0A$ has only one element a, the set A^0 has at least four elements, and only two elements in the set A^0 are not incident to the element a in ${}^0A$.

A configuration $\mathfrak{A} = \langle (A^0, {}^0A), \cdot, \alpha \rangle$ will be called *a configuration without incidence* if $\alpha = \emptyset$.

A projective plane $\mathfrak{P}$ will be called *completely free* if $\mathfrak{P}$ is freely generated by a configuration $\mathfrak{A} = \langle (A^0, {}^0A), \cdot, \emptyset \rangle$ without incidence. In this case, we will also say that $\mathfrak{P}$ is *freely generated by the set* $A = A^0 \cup {}^0A$.

We will say that configurations $\mathfrak{A}_1$ and $\mathfrak{A}_2$ are *freely equivalent* if there exists a natural number n and configurations $\mathfrak{B}_1$, $\mathfrak{B}_2$, ..., $\mathfrak{B}_n$ such that $\mathfrak{B}_1 = \mathfrak{A}_1$, $\mathfrak{B}_n = \mathfrak{A}_2$, and for any natural number i, $i = 1, 2, \ldots, n-1$, either $\mathfrak{B}_i$ is a free one-step extension of $\mathfrak{B}_{i+1}$ or, vice versa, $\mathfrak{B}_{i+1}$ is a free one-step extension of $\mathfrak{B}_i$.

In the case when a projective plane $\mathfrak{P}$ is freely generated by a configuration $\mathfrak{A} = \langle A, (A^0, {}^0A), \cdot, \alpha \rangle$ containing a finite number of elements, then following [2] we will call the number

$$r(\mathfrak{A}) = 2|A| - \frac{1}{2}|\alpha|,$$

the *rank of the configuration* $\mathfrak{A}$. The following result holds.

Remark 5. [2] If $\mathfrak{A}$ is a finite configuration and $\mathfrak{B}$ is a configuration that is freely equivalent to $\mathfrak{A}$, then their ranks are equal: $r(\mathfrak{A}) = r(\mathfrak{B})$.

By virtue of Remark 5, in the case when a projective plane $\mathfrak{P}$ is freely generated by a configuration $\mathfrak{A}$ of finite rank $r(\mathfrak{A})$, it is natural to call the number $r(\mathfrak{A})$ the *rank of the plane* $\mathfrak{P}$. In all other cases, the rank of a freely generated plane will be understood to be the cardinality of the set of its elements.

Remark 6. From the results of [6, §1] it follows that a projective plane $\mathfrak{P}$ is free if and only if either

(1) $\mathfrak{P}$ is a completely free plane of infinite rank, or
(2) $\mathfrak{P}$ is a completely free plane of finite rank, and in this case the rank $r(\mathfrak{P})$ of the plane $\mathfrak{P}$ is an even number, or
(3) $\mathfrak{P}$ is a free plane of finite rank which is an odd number, and in this case there exists a configuration $\mathfrak{A} = \langle (A^0, {}^0A), \cdot, \alpha \rangle$ such that the plane $\mathfrak{P}$ is freely generated by $\mathfrak{A}$, where
   (i) the set A^0 contains n elements, $n \geq 4$, i.e., $A^0 = \{t_1, t_2, \ldots, t_n\}$,
   (ii) the set ${}^0A$ contains one element p, i.e., ${}^0A = \{p\}$,
   (iii) the operation is nowhere defined in $\mathfrak{A}$, and
   (iv) $\alpha = \{(t_n, p), (p, t_n)\}$.

We will say that a plane $\mathfrak{P}$ is *freely generated by the set* A if $\mathfrak{P}$ is freely generated by a configuration of the form $\langle A, (A^0, {}^0A), \cdot, \emptyset \rangle$ where $A = A^0 \cup {}^0A$.

We have the following result:

Proposition 4. [3] *Let $\mathfrak{P}$ be a projective plane freely generated by a configuration $\mathfrak{B}$ without incidence. Then there exists a set A of unitypical elements in $\mathfrak{P}$ such that $\mathfrak{P}$ is freely generated by the configuration $\mathfrak{A} = \langle (A, \emptyset), \cdot, \emptyset \rangle$ and $\mathfrak{A}$ is freely equivalent to $\mathfrak{B}$.*

The following holds:

Proposition 5. [4] *Let a projective plane $\mathfrak{P}$ be freely generated by a configuration $\mathfrak{A}$, and let a configuration $\mathfrak{B}$ be freely equivalent to $\mathfrak{A}$. Then $\mathfrak{P}$ is also freely generated by $\mathfrak{B}$.*

2. Constructions of free and completely free projective planes

1. We give a construction for a completely free plane freely generated by a fixed set V of symbols where $|V| \geq 4$.

Construction 1. Fix a set of pairwise distinct symbols $V = \{v_i\}$ where i ranges over a well-ordered set I of indices and the cardinality of V is at least 4. We denote by $W(V)$ the set of all nonassociative words in the alphabet V. As usual, the number $d(w)$ of occurrences of elements of the set V in a word w in $W(V)$ will be called the *V-length* of w. If it does not lead to misunderstanding, the V-length will be called simply the length.

On the set $W(V)$ we define a lexicographical order as follows. For words u and w in $W(V)$ we set $u > w$ if either (i) the length of u is greater than the length of w, or (ii) the lengths of u and w equal 1 and the index of u is greater than the index of w, or (iii) the lengths of u and w are equal, $u = u_1u_2$, $w = w_1w_2$ and $u_1 > w_1$, or (iv) the lengths of u and w are equal, $u = u_1u_2$, $w = w_1w_2$, $u_1 = w_1$ and $u_2 > w_2$.

The words of length 1 in $W(V)$ will be called *regular words of the first type* (of length 1) relative to the set V. The words of length 2 in $W(V)$ of the form v_iv_j where $v_i > v_j$ will be called *regular words of the second type* (of length 2) relative to the set V.

A word w in $W(V)$ of length $3k + 1$ (respectively $3k + 2$) will be called a *regular word of the first type* (respectively *of the second type*) relative to the set V, if

(1) $w = w_1w_2$ where w_1 and w_2 are regular words of the second (respectively first) type, and w_1 is greater than w_2, and
(2) if $w = (w_1'w_1'')(w_2'w_2'')$ then the intersection of the sets $\{w_1', w_1''\}$ and $\{w_2', w_2''\}$ is empty, and
(3) if $w = ((w_1'w_1'')w_1''')w_2$ or $w = (w_1'''(w_1'w_1''))w_2$ then w_2 is not an element of the set $\{w_1', w_1''\}$.

[3] See for example Lemma 1 in [6].
[4] See for example Theorem 4.2 in [2].

If it does not lead to misunderstanding, then words which are regular relative to the set V will be called simply regular.

The set of all regular words of the first (respectively second) type contained in $W(V)$ will be denoted by W^0 (respectively ${}^0W$).

If, for elements w_1 and w_2 in $W(V)$, one of the words w_1w_2 and w_2w_1 is regular, then we will denote this regular word by $\overline{w_1w_2}$.

On the set $W^0 \cup {}^0W$ we define a partial binary commutative operation $\cdot$ in the following way. Given distinct unitypical regular words w_1 and w_2,

2.1. if one of the words w_1w_2 and w_2w_1 is regular, then $w_1 \cdot w_2 = \overline{w_1w_2}$,

2.2. if $w_1 = w_1'w_1''$, $w_2 = w_2'w_2''$ and the intersection $\{w_1', w_1''\} \cap \{w_2', w_2''\}$ contains an element w, then $w_1 \cdot w_2 = w$,

2.3. if $w_1 = \overline{\overline{(w_1'w_2)}w_1''}$ then $w_1 \cdot w_2 = \overline{w_1'w_2}$, and

2.4. in all other cases the operation $\cdot$ on the elements of $W^0 \cup {}^0W$ is undefined.

The partial algebraic system $\langle (W^0, {}^0W), \cdot \rangle$ obtained in this way will be regarded as *the result of Construction* 1 for the set V and denoted by $\mathfrak{CF}(V)$.

Lemma 1. *The partial algebraic system $\mathfrak{CF}(V)$ is a projective plane.*

Proof. We observe that for the operation $\cdot$ in $\mathfrak{CF}(V)$, Conditions 1.1, 1.2 and 1.4 follow immediately from the definition of this operation and the definition of regular words relative to the set V. To verify Condition 1.3 we need to prove that if w_1, w_2, w_3 are unitypical words such that $w_1 \neq w_2$, $w_1 \neq w_3$ and $w_1 \cdot w_2 \neq w_1 \cdot w_3$, then equation (1) holds. For this, it suffices to consider the following cases[5]:

(a) $w_1w_2 = \overline{w_1w_2}$, and either $w_1 \cdot w_3 = \overline{w_1w_3}$ or $w_3 = \overline{\overline{(w_1w_3')}w_3''}$ or $w_1 = \overline{\overline{(w_3w_1')}w_1''}$ or $w_1 = w_1'w_1''$, $w_3 = \overline{w_1w_3'}$;

(b) $w_1 = w_1'w_1''$, $w_2 = \overline{w_1'w_2'}$, and either $w_3 = \overline{w_1''w_3'}$ or $w_3 = \overline{\overline{(w_1w_3')}w_3''}$;

(c) $w_3 = \overline{\overline{(w_1w_3')}w_3''}$, and either $w_1 = \overline{\overline{(w_2w_1')}w_1''}$ or $w_2 = \overline{\overline{(w_1w_2')}w_2''}$;

(d) $w_1 = w_1'w_1''$, $w_2 = \overline{w_1'w_2'}$, and either $w_3 = \overline{w_1'w_3'}$ or $w_1 = \overline{\overline{(w_3w_1''')}w_1''''}$;

(e) $w_1 = \overline{\overline{(w_2w_1')}w_1''}$, $w_1 = \overline{\overline{(w_3w_1''')}w_1''''}$.

Cases (a)–(c) follow immediately from Conditions 2.1–2.3.

In case (d) the equation $w_3 = \overline{w_1'w_3'}$ and Condition 2.2 imply $w_1 \cdot w_2 = w_1 \cdot w_3$, which contradicts the assumption. Now let $w_1 = \overline{\overline{(w_3w_1''')}w_1''''}$. Then from $w_1 = \overline{w_1'w_1''}$ it follows that either $\overline{w_3w_1'''} = w_1'$, $w_1'''' = w_1''$ or $\overline{w_3w_1'''} = w_1''$, $w_1'''' = w_1'$. From Conditions 2.2 and 2.3, and from $w_1 \cdot w_2 \neq w_1 \cdot w_3$, we obtain $w_1'' = \overline{w_3w_1'''}$ and $w_1' = w_1''''$. Therefore $(w_1 \cdot w_2)(w_1 \cdot w_3) = w_1$.

In case (e), from Condition 2.3 we obtain $w_1 \cdot w_2 = \overline{w_2w_1'}$ and $w_1 \cdot w_3 = \overline{w_3w_1'''}$. From this, and from the equation $w_1 \cdot w_2 \neq w_1 \cdot w_3$ it follows that $\overline{w_2 \cdot w_1'} \neq \overline{w_3w_1'''}$. Hence $w_1'' = \overline{w_3w_1'''}$ and $w_1'''' = \overline{w_2w_1'}$. Therefore

$$(w_1 \cdot w_2) \cdot (w_1 \cdot w_3) = \overline{(w_2w_2')} \cdot \overline{(w_3w_1''')} = \overline{\overline{(w_2w_1')}\,\overline{(w_3w_1''')}} = w_1.$$

[5]In the rest of this proof, there are some typographical errors in the original text, especially regarding the superscripts. We have attempted to correct these errors. [Translators]

All the necessary cases have been considered. Thus the operation $\cdot$ in $\mathfrak{CF}(V)$ satisfies Conditions 1.1–1.4. Therefore the partial algebra system $\mathfrak{CF}(V)$ is a projective plane. □

Now we prove the following result:

Theorem 1. *Let V be a set containing at least four elements, and let $\mathfrak{CF}(V)$ be the partial algebraic system resulting from Construction 1 for the set V. Then $\mathfrak{CF}(V)$ is a completely free projective plane, freely generated by the set V of unitypical elements.*

Proof. From the construction of the plane $\mathfrak{CF}(V)$ it follows that we can choose in $\mathfrak{CF}(V)$ a subconfiguration of the form $\mathfrak{D} = \langle (V, \emptyset), \cdot, \emptyset \rangle$. Consider the sequence of configurations $\mathfrak{D}^{[0]} = \mathfrak{D}$, $\mathfrak{D}^{[1]}$, …, $\mathfrak{D}^{[i]}$.

From the definitions of the operation $\cdot$ in $\mathfrak{CF}(V)$ and the configuration $\mathfrak{D}^{[1]}$, it follows that for any $w \in \mathfrak{D}^{[1]}$, since $w = \overline{uv}$, we have $u, v \in \mathfrak{D}^{[0]}$, and if $w \notin \mathfrak{D}^{[0]}$ and $u_1, v_1 \in \mathfrak{D}^{[0]}$ are such that $w = u_1 v_1$, then $w = \overline{u_1 v_1}$. Thus $\mathfrak{D}^{[1]} \supset \mathfrak{D}^{[0]}$ is a free one-step extension. Therefore we have the basis of the induction.

Assume, for any natural number i not exceeding a natural number s, that $\mathfrak{D}^{[i]} \supset \mathfrak{D}^{[i-1]}$ is a free one-step extension.

Now choose arbitrarily an element $w \in \mathfrak{D}^{[s+1]}$. Then by definition of a complete one-step extension it follows that in $\mathfrak{D}^{[s]}$ there exist elements u and v such that $w = u \cdot v$. The definition of the operation $\cdot$ in $\mathfrak{CF}(V)$ implies that we have the following cases:

(a) $w = \overline{uv}$,
(b) $u = \overline{wu'}$, $v = \overline{wv'}$,
(c) $w = \overline{w_1 w_2}$ and either $u = \overline{wu'}$, $v = w_i$, $i \in \{1, 2\}$, or $v = \overline{wv'}$, $u = w_i$, $i \in \{1, 2\}$.

In cases (b) and (c) it follows from the inductive hypothesis that $w \in \mathfrak{D}^{[s]}$. This contradicts the choice of w in $\mathfrak{D}^{[s+1]}$. Therefore we have the equation $w = \overline{uv}$ and hence the inductive step from s to $s + 1$: that is, $\mathfrak{D}^{[s+1]} \subset \mathfrak{D}^{[s]}$ is a free one-step extension. Therefore, for any natural number i, $\mathfrak{D}^{[i]} \subset \mathfrak{D}^{[i-1]}$ is a free one-step extension, and

$$\mathfrak{CF}(V) = \bigcup_{i=1}^{\infty} \mathfrak{D}^{[i-1]} = \langle \mathfrak{D} \rangle_{\mathfrak{CF}(V)}.$$

From this and Lemma 1 we obtain that $\mathfrak{CF}(V)$ is a completely free projective plane, freely generated by the configuration $\mathfrak{D}$. □

2. Now we apply Construction 1 to build a free projective plane of odd rank.

Construction 2. Let $V_n = \{v_1, v_2, \ldots, v_n\}$ be a set consisting of n ($n \geq 5$) pairwise distinct symbols. We define the elements of V_n to be unitypical. Let $\mathfrak{CF}(V_n) = \langle (W_n^0, {}^0W_n), \cdot \rangle$ be the completely free projective plane freely generated by the set V_n, which is built according to Construction 1. Let W_n^0 and ${}^0W_n$ be the sets of all regular words relative to V_n of the first and second types respectively; let W_n' be

the subset of $W_n^0 \cup {}^0W_n$ consisting of the regular words that are formed from the elements of the set $V_{n-1} = V_n \setminus \{v_n\} = \{v_1, v_2, \ldots, v_{n-1}\}$; let W_n'' be the subset of $W_n^0 \cup {}^0W_n$ consisting of the regular words that have subwords of the form $v_n v_{n-1}$ but do not have subwords of the form $\overline{v_n v}$ where v is an arbitrary regular word of the first type distinct from v_{n-1}.

The operation $\cdot$ defined in the plane $\mathfrak{CF}(V_n)$ induces on the set $W_n' \cup W_n''$ a partial operation $\circ$. The partial algebraic system thus obtained,

$$\big\langle \big((W_n' \cup W_n'') \cap W_n^0, (W_n' \cup W_n'') \cap {}^0W_n\big), \circ \big\rangle,$$

will be denoted by $\mathfrak{F}(\widetilde{V}_n)$ where $\widetilde{V}_n = \{v_1, v_2, \ldots, v_{n-1}; v_n v_{n-1}\}$ and regarded as *the result of Construction* 2.

It immediately follows from the definition that $\mathfrak{F}(\widetilde{V}_n)$ is a closed subconfiguration in the projective plane $\mathfrak{CF}(V_n)$. From this, and from the construction of the configuration $\mathfrak{F}(\widetilde{V}_n)$, it follows that $\mathfrak{F}(\widetilde{V}_n)$ is a projective plane. From the definition of multiplication in the plane $\mathfrak{CF}(V_n)$ it follows that $\mathfrak{F}(\widetilde{V}_n)$ is generated by the configuration of the form

$$\mathfrak{D}_n = \big\langle \widetilde{V}_n, \big(\{v_1, v_2, \ldots, v_n\}, \{v_n v_{n-1}\}\big), *, \nu \big\rangle,$$

where $\nu = \{(v_{n-1}, v_n v_{n-1}), (v_n v_{n-1}, v_n)\}$, and for all elements in $\mathfrak{D}_n$ the operation $*$ is undefined.

If we apply, to the sequence of configurations $\mathfrak{D}_n^{[0]} = \mathfrak{D}_n$, $\mathfrak{D}_n^{[1]}$, …, $\mathfrak{D}_n^{[i]}$, …, arguments analogous to those done in the proof of Theorem 1 for the sequence $\mathfrak{D}$, $\mathfrak{D}^{[1]}$, …, $\mathfrak{D}^{[i]}$, …, then we obtain that for any natural number i, the complete one-step extension $\mathfrak{D}^{[i]} \supset \mathfrak{D}^{[i-1]}$ is a free one-step extension, and

$$\mathfrak{C}(\widetilde{V}_n) = \bigcup_{i=1}^{\infty} \mathfrak{D}_n^{[i-1]} = \langle \mathfrak{D} \rangle_{\mathfrak{C}(\widetilde{V}_n)}.$$

Thus we have the next result.

Proposition 6. *The partial algebraic system* $\mathfrak{F}(\widetilde{V}_n)$ *built in Construction* 2 *is a free projective plane of rank* $2n-1$ *where* $n \geq 5$.

From Propositions 4 and 6, Remark 6, Theorem 1, and Constructions 1 and 2, we obtain the following result.

Remark 7. Any free (including also completely free) projective plane can be regarded as a partial algebraic system in which every element has the form of a suitable regular word.

Remark 8. [6] In [1] and [7] are given constructions of free and completely free projective planes, but the elements of these planes are defined by the authors only up to a certain equivalence relation which is not always convenient for applications.

[6] With regard to completely free projective planes, see also [5].

3. On embeddings of projective planes

1. We have the following construction.

Construction 3. Let $C_1 = \{a_1, a_2, a_3, a_4\}$ be a fixed set of four elements. We define

$$\begin{aligned}
e_1 &= \big[\big((a_4a_2)(a_3a_1)\big)\big((a_4a_1)(a_3a_2)\big)\big](a_2a_1),\\
e_2 &= \big[\big((a_4a_2)(a_3a_1)\big)\big((a_4a_1)(a_3a_2)\big)\big](a_4a_3),\\
e_3 &= \big[\big((a_4a_3)(a_2a_1)\big)\big((a_4a_1)(a_3a_2)\big)\big](a_3a_1),\\
e_4 &= \big[\big((a_4a_3)(a_2a_1)\big)\big((a_4a_1)(a_3a_2)\big)\big](a_4a_2),\\
e_5 &= \big[\big((a_4a_3)(a_2a_1)\big)\big((a_4a_2)(a_3a_1)\big)\big](a_3a_2),\\
e_6 &= \big[\big((a_4a_3)(a_2a_1)\big)\big((a_4a_2)(a_3a_1)\big)\big](a_4a_2).
\end{aligned}$$

We further set

$$\begin{aligned}
&g_1 = (e_2a_2)(e_1a_4), \qquad g_2 = (e_3a_2)(e_2a_1), \qquad g_3 = (e_4a_1)(e_3a_4),\\
&g_4 = (e_5a_1)(e_4a_3), \qquad g_5 = (e_6a_2)(e_1a_3), \qquad g_6 = (e_6a_3)(e_5a_4).
\end{aligned}$$

We will regard the set $G = \{g_1, g_2, g_3, g_4, g_5, g_6\}$ as *the result of Construction* 3. It immediately follows from the definition of the elements of the set G that all of them are regular words relative to C_1. Hence, the set G is contained in the projective plane $\mathfrak{CF}(C_1)$ obtained from the set C_1 according to Construction 1. Now consider the subconfiguration $\langle (G, \emptyset), \cdot, \emptyset\rangle$ in $\mathfrak{CF}(C_1)$, where the operation $\cdot$ is undefined for all pairs of elements in the set G. This configuration will be denoted by $\mathfrak{G}$.

We have the following result.

Proposition 7. *In the projective plane $\mathfrak{CF}(C_1)$, the configuration $\widetilde{\mathfrak{G}} = \langle \mathfrak{G}\rangle_{\mathfrak{CF}(C_1)}$ is a completely free plane, freely generated by the set G which consists of six unitypical elements.*

Proof. For the proof of this statement, it suffices to observe that any word that is regular relative to the set G is also regular relative to the set C_1. Hence, for any natural number i, the complete one-step extension $\mathfrak{G}^{[i]} \supset \mathfrak{G}^{[i-1]}$ is also a free one-step extension within the plane $\mathfrak{CF}(C_1)$. The claim of the proposition follows from this and from the fact that $\widetilde{\mathfrak{G}} = \langle \mathfrak{G}\rangle_{\mathfrak{CF}(C_1)} = \langle \mathfrak{G}\rangle_{\widetilde{\mathfrak{G}}}$. □

Construction 4. Let $V_n = \{v_1, v_2, \ldots, v_n\}$ where $n \geq 6$, and let $\mathfrak{CF}(V_n)$ be the completely free projective plane obtained from the set V_n according to Construction 1. For any quadruple (i_1, i_2, i_3, i_4) of natural numbers such that $1 \leq i_1 < i_2 < i_3 < i_4 \leq n$, we will denote by $h(i_1, i_2, i_3, i_4)$ the word

$$\big((v_{i_4}v_{i_3})(v_{i_2}v_{i_1})\big)\big((v_{i_4}v_{i_2})(v_{i_3}v_{i_1})\big). \tag{2}$$

The set H of all words (2) formed from the elements of the set V_n will be regarded as *the result of Construction* 4. It is clear from the construction of the elements of H that all of them are regular words relative to the set V_n, and hence H is contained

in the projective plane $\mathfrak{CF}(V_n)$. Now consider the configuration $\langle (H, \emptyset), \cdot, \emptyset \rangle$ where the operation $\cdot$ is undefined for all pairs of elements in H. We will denote this configuration by $\mathfrak{H}$.

The proof of the next result is similar to that of Proposition 7.

Proposition 8. *In the projective plane $\mathfrak{CF}(V_n)$ the configuration $\widetilde{\mathfrak{H}} = \langle \mathfrak{H} \rangle_{\mathfrak{CF}(V_n)}$ is a completely free plane, freely generated by the set H of unitypical elements.*

Observe that since the cardinality $|V_n|$ of the set V_n equals n, the cardinality $|H|$ of the set H equals $\binom{n}{4}$. Hence if $n \geq 6$ then $|H| > |V_n|$. This, together with Propositions 7 and 8, implies the following result.

Theorem 2. *Let C_1 be a set which contains four symbols, and let $\mathfrak{CF}(C_1)$ be the completely free projective plane freely generated by the set C_1 of unitypical elements. Then for any natural number $n \geq 4$, there exists a projective subplane of $\mathfrak{CF}(C_1)$ which is a completely free projective plane freely generated by a set of n unitypical elements.*

It is easy to see that the rank of a free plane cannot be smaller than 8. Hence from Theorem 2 and Proposition 6 we obtain the following result.

Corollary 1. [2] *For any natural number $n \geq 8$, the completely free plane $\mathfrak{CF}(C_1)$ contains a projective subplane which is a free projective plane of rank n.*

2. In what follows we will need the next result.

Lemma 2. *Let $\mathfrak{CF}(V)$ be the completely free projective plane freely generated by the set V, and let U be a set of unitypical elements in $\mathfrak{CF}(V)$ such that*

(i) *for any two distinct words u_i and u_j in U, there exists*[7] *a word $\overline{u_i u_j}$ in $\mathfrak{CF}(V)$ which is regular relative to V, and*

(ii) *if, in the expression of an element u_k in U, there occurs a word u which is regular relative to V, then for any words of the form $\overline{uw_1}$ or $\overline{\overline{(uw_2)}w_3}$ which are regular relative to V, we have $u_k \neq \overline{uw_1}$ and $u_k \neq \overline{\overline{(uw_2)}w_3}$.*

Then any word which is regular relative to U is also regular relative to V.

Proof. For words of U-length 1 or 2 that are regular relative to U, the statement of the lemma follows immediately from the assumptions. Thus we have the basis of induction on the U-lengths of the words.

Assume that any word of U-length n which is regular relative to U is also regular relative to V, and consider an arbitrary word w that is regular relative to U and has U-length $n+1 \geq 2$. For the word w there exist words x_1 and x_2 that are regular relative to U such that $w = x_1 x_2$ and the U-lengths of both of these words are strictly less than $n+1$, and hence the inductive hypothesis applies to the words x_1 and x_2.

From the definition of regular words, it follows that if w fails to be regular relative to V, then we are in one of the following cases:

[7] That is, either $u_i u_j$ or $u_j u_i$ is regular relative to V, and hence $\overline{u_i u_j}$ is defined. [Translators]

(a) $x_1 = \overline{y'_1 y''_1}$, $x_2 = \overline{y'_2 y''_2}$, and the intersection $\{y'_1, y''_1\} \cap \{y'_2, y''_2\}$ is not empty;
(b) there exist elements z' and z'' such that for some index $i \in \{1, 2\}$ the elements x_i, x_{3-i}, z', z'' satisfy $x_{3-i} = \overline{\overline{(x_i z')} z''}$.

We consider the two cases separately.

(a) From the definition of regular words, it follows that the words y'_1, y''_1, y'_2, y''_2 cannot simultaneously be regular relative to the set U. Hence, without loss of generality, we can assume that y''_2 is not regular relative to U; but in this case $x_2 \in U$. If now at least one of the elements y'_1, y''_1 is not regular relative to U, then $x_1 \in U$ and hence by the conditions of the lemma there exists a word $\overline{x_1 x_2}$ that is regular relative to V, which contradicts the original assumption. Hence y'_1 and y''_1 are regular relative to U. From this, and from the fact that the intersection $\{y'_1, y''_1\} \cap \{y'_2, y''_2\}$ is not empty, we can assume without loss of generality that $y'_1 = y'_2$. Therefore the word w has the form $x_1 x_2 = \overline{(y'_1 y''_1)}\,\overline{(y'_1 y''_2)}$.

First consider x_1. This word has the form $\overline{y'_1 y''_1}$, where y'_1 and y''_1 are words that are regular relative to U, and hence the U-lengths of both of the words y'_1 and y''_1 are less than the U-length of x. From this, and the fact that $x_2 \in U$, it follows that y'_1 is a word of second type relative to U, and hence there exist words v' and v'', regular relative to U, such that the U-lengths of both of v' and v'' are strictly less than the U-length of y'_1 and we have $y'_1 = v'v''$. But then x_2 has the form $\overline{y'_1 y''_2} = \overline{\overline{(v'v'')} y''_2}$, which contradicts the assumptions of the lemma. For this reason, case (a) is impossible.

(b) From the definition of regular words, it follows that the elements z' and z'' cannot simultaneously be regular relative to U. If z'' is not regular relative to U, then the word $\overline{\overline{(x_i z')} z''}$ must be an element of U. But this contradicts the assumptions of the lemma. If z'' is regular relative to U, then z' is not regular relative to U, and in this case either $\overline{x_i z'} \in U$ or $\overline{\overline{(x_i z')} z''} \in U$, which also contradicts the assumptions of the lemma. Consequently case (b) is also impossible.

Therefore, the word w is regular relative to V, contrary to the assumption. Hence any word w which is regular relative to U and has U-length $n + 1$ is also regular relative to V. The induction is complete. □

Construction 5. Let $C_1 = \{a_1, a_2, a_3, a_4\}$ be a fixed set of symbols, and let $G = \{g_1, g_2, g_3, g_4, g_5, g_6\}$ be the set of words resulting from Construction 3. Take the elements g_1, g_2, g_3, g_4 from G and substitute them for the elements a_1, a_2, a_3, a_4 respectively into the words g_1, g_2, g_3, g_4, g_5, g_6. Denote the resulting words by $g_{1,1}$, $g_{1,2}$, $g_{1,3}$, $g_{1,4}$, $g_{1,5}$, $g_{1,6}$. Now suppose that for any natural number i the words $g_{i,1}$, $g_{i,2}$, $g_{i,3}$, $g_{i,4}$, $g_{i,5}$, $g_{i,6}$ have been constructed. Then we denote by $g_{i+1,1}$, $g_{i+1,2}$, $g_{i+1,3}$, $g_{i+1,4}$, $g_{i+1,5}$, $g_{i+1,6}$ the words resulting from substituting the elements $g_{i,1}$, $g_{i,2}$, $g_{i,3}$, $g_{i,4}$ for the symbols a_1, a_2, a_3, a_4 respectively into the words g_1, g_2, g_3, g_4, g_5, g_6. We denote the element g_6 by $g_{0,6}$. We define the set

$$\overline{G} = \{g_{0,6}, g_{1,6}, \ldots, g_{i,6}, \ldots\},$$

to be *the result of Construction* 5. It follows from the definition of the elements of $\overline{G}$, that for any natural number i, the element $g_{i-1,6}$ is a regular word relative to C_1. Hence the set $\overline{G}$ is contained in the projective plane $\mathfrak{CF}(C_1)$ obtained from the set C_1 according to Construction 1. Consider in $\mathfrak{CF}(C_1)$ the subconfiguration $\langle(\overline{G},\emptyset),\cdot,\emptyset\rangle$ where the operation $\cdot$ is undefined for all pairs of elements of $\overline{G}$. Denote this configuration by $\overline{\mathfrak{G}}$.

It follows from the construction of $\overline{G}$, that C_1 and $\overline{G}$ are sets of unitypical elements satisfying the conditions of Lemma 2. Thus any word that is regular relative to $\overline{G}$ is also regular relative to C_1. Hence for any natural number i, the complete one-step extension $\overline{\mathfrak{G}}^{[i]} \supset \overline{\mathfrak{G}}^{[i-1]}$ in the plane $\mathfrak{CF}(C_1)$ is a free one-step extension. For this reason the closed configuration $\langle\overline{\mathfrak{G}}\rangle_{\mathfrak{CF}(C_1)}$ is a completely free projective plane, freely generated by a countable set $\overline{G}$ of unitypical elements. Therefore we have the following result.

Theorem 3. *Let C_1 be a set of four elements, let $\mathfrak{CF}(C_1)$ be the completely free projective plane freely generated by the set C_1 of unitypical elements, and let $\overline{G}$ be the countable set of elements obtained according to Construction* 5. *Then $\mathfrak{CF}(C_1)$ contains a projective subplane which is a completely free projective plane freely generated by the set $\overline{G}$ of unitypical elements.*

4. On homomorphisms of projective planes

1. The following result holds.

Lemma 3. *Let $\mathfrak{CF}(V)$ be the completely free projective plane, freely generated by the set V of unitypical elements according to Construction* 1. *Let $\mathfrak{A}_1$, $\mathfrak{A}_2$, ..., $\mathfrak{A}_n$, ... be a sequence of subconfigurations in $\mathfrak{CF}(V)$ such that*

(i) $\mathfrak{A}_1 = \langle(V,\emptyset),\cdot,\emptyset\rangle$,

(ii) *for any natural number i the configuration $\mathfrak{A}_{i+1}$ is a free one-step extension of $\mathfrak{A}_i$, and*

(iii) $\mathfrak{A}_0 \stackrel{\text{def}}{=} \bigcup_{i=1}^{\infty} \mathfrak{A}_i \neq \mathfrak{CF}(V)$.

Then the following conditions hold:

(a) *for any natural number n, if $w \in \mathfrak{A}_{n+1}$ and $w \notin \mathfrak{A}_n$ then in $\mathfrak{A}_n$ there exist elements u and v such that $w = \overline{uv}$;*

(b) *the projective plane $\mathfrak{CF}(V)$ is freely generated by the configuration $\mathfrak{A}_0$.*

Proof. (a) In the case $n = 1$, the claim is obvious. Thus we have a basis for the induction. Suppose, for all natural numbers $k < n$, that from $w \in \mathfrak{A}_{k+1}$, $w \notin \mathfrak{A}_k$ it follows that there exist elements u and v in $\mathfrak{A}_k$ such that $w = \overline{uv}$. Now choose arbitrarily an element w in $\mathfrak{A}_{n+1}$ such that $w \notin \mathfrak{A}_n$, and let u and v be the elements in $\mathfrak{A}_n$ such that $w = u \cdot v$.

From the definition of the plane $\mathfrak{CF}(V)$, and Conditions 2.1–2.3 in the definition of the operation $\cdot$ in $\mathfrak{CF}(V)$, it follows that the equation $w = u \cdot v$ holds in $\mathfrak{CF}(V)$ in any of the following cases:

- $w = \overline{uv}$;
- $u = \overline{wu'}$, $v = \overline{wv'}$;
- $w = \overline{w_1 w_2}$ and either $u = \overline{wu'}$, $v = w_i$, $i \in \{1, 2\}$, or $v = \overline{wv'}$, $u = w_i$, $i \in \{1, 2\}$.

Assume that

$$u = \overline{wu'}. \tag{3}$$

Then $u \notin \mathfrak{A}_1$. From this, and from the assumptions of the lemma, it follows that there exists a smallest natural number s such that $1 < s \leq n$, $u \in \mathfrak{A}_s$, $u \notin \mathfrak{A}_{s-1}$. Hence from the inductive hypothesis, the definition of regular words in Construction 1, and equation (3), it follows that $w, u' \in \mathfrak{A}_{s-1}$. But this contradicts the choice of the element w. The case $v = \overline{wv'}$ is treated similarly. Therefore, $w = \overline{uv}$. The inductive step is complete. Part (a) of the lemma is proved.

(b) We show that for any natural number n, the complete one-step extension $\mathfrak{A}_0^{[n]} \supset \mathfrak{A}_0^{[n-1]}$ is a free one-step extension.

Let $n = 1$. We choose arbitrarily an element w in $\mathfrak{A}_0^{[1]}$ such that $w \notin \mathfrak{A}_0^{[0]} = \mathfrak{A}_0$. Then in $\mathfrak{A}_0$ there exist elements u and v such that $w = u \cdot v$. From the definition of the configuration $\mathfrak{A}_0$ it follows that there exists a smallest natural number s such that $u \in \mathfrak{A}_s$. Now, if $u > w$ then from the definition of the multiplication in the plane $\mathfrak{CF}(V)$ it follows that w occurs in the expression of the word u. Hence from part (a) of this lemma we obtain $w \in \mathfrak{A}_s \subset \mathfrak{A}_0$. This contradicts the choice of w. Consequently $u < v$. Similarly one shows that $v < w$. From this and the definition of multiplication in the plane $\mathfrak{CF}(V)$, it follows that $w = \overline{uv}$, i.e., for w there exist two and only two elements u and v in $\mathfrak{A}_0$ such that $w = u \cdot v$. For this reason the extension $\mathfrak{A}_0^{[1]} \supset \mathfrak{A}_0$ is a complete free one-step extension. Therefore we have the basis of induction.

Now suppose, for any natural number $k < n$, that the extension $\mathfrak{A}_0^{[k]} \supset \mathfrak{A}_0^{[k-1]}$ is a complete free one-step extension, and that for any element $w \in \mathfrak{A}_0^{[k]}$ with $w \notin \mathfrak{A}_0^{[k-1]}$ there exist elements u and v in $\mathfrak{A}_0^{[k-1]}$ for which $w = \overline{uv}$. Choose arbitrarily an element $w \in \mathfrak{A}_0^{[n]}$ such that $w \notin \mathfrak{A}_0^{[n-1]}$. Then for this element there exist elements u and v in $\mathfrak{A}_0^{[n-1]}$ such that $w = u \cdot v$. From this, the inductive hypothesis, and the definition of the operation $\cdot$ in the plane $\mathfrak{CF}(V)$, it follows that $w > u$ and $w > v$. Hence $w = \overline{uv}$, and the extension $\mathfrak{A}_0^{[n]} \supset \mathfrak{A}_0^{[n-1]}$ is a complete free one-step extension. The inductive step is complete. Therefore part (b) is also proved. □

2. We have the following construction.

Construction 6. Let $C_1 = \{a_1, a_2, a, a_4\}$ be a fixed set of four elements, and let $\mathfrak{CF}(C_1)$ be the completely free projective plane obtained from C_1 according to Construction 1. In the alphabet C_1, we introduce notation for words which will be needed in what follows: $b_{0,m}$, $c_{0,j}$, $d_{0,j}$, $e_{0,m}$, $f_{0,k}$, $g_{0,\ell}$ where $m = 1, 2, \ldots, 6$, $j = 1, 2, 3$, $k = 1, 2, \ldots, 12$, $\ell = 1, 2, 3, 4$, as displayed in Table 1; in each column, the definition of the element in the first row is given in the second row.

$b_{0,1}$	$b_{0,2}$	$b_{0,3}$	$b_{0,4}$	$b_{0,5}$	$b_{0,6}$	$c_{0,1}$	$c_{0,2}$
a_2a_1	a_3a_1	a_3a_2	a_4a_1	a_4a_2	a_4a_3	$b_{0,4}b_{0,3}$	$b_{0,5}b_{0,2}$

$c_{0,3}$	$d_{0,1}$	$d_{0,2}$	$d_{0,3}$	$e_{0,1}$	$e_{0,2}$	$e_{0,3}$	$e_{0,4}$
$b_{0,6}b_{0,1}$	$c_{0,2}c_{0,1}$	$c_{0,3}c_{0,1}$	$c_{0,3}c_{0,2}$	$d_{0,1}b_{0,1}$	$d_{0,1}b_{0,6}$	$d_{0,2}b_{0,2}$	$d_{0,2}b_{0,9}$

$e_{0,5}$	$e_{0,6}$	$f_{0,1}$	$f_{0,2}$	$f_{0,3}$	$f_{0,4}$	$f_{0,5}$	$f_{0,6}$
$d_{0,3}b_{0,3}$	$d_{0,3}b_{0,4}$	$e_{0,1}a_3$	$e_{0,1}a_4$	$e_{0,2}a_1$	$e_{0,2}a_2$	$e_{0,3}a_2$	$e_{0,3}a_4$

$f_{0,7}$	$f_{0,8}$	$f_{0,9}$	$f_{0,10}$	$f_{0,11}$	$f_{0,12}$	$g_{0,1}$	$g_{0,2}$
$e_{0,4}a_1$	$e_{0,4}a_3$	$e_{0,5}a_1$	$e_{0,5}a_4$	$e_{0,6}a_2$	$e_{0,6}a_3$	$f_{0,4}f_{0,2}$	$f_{0,5}f_{0,3}$

$g_{0,3}$	$g_{0,4}$
$f_{0,7}f_{0,6}$	$f_{0,9}f_{0,8}$

TABLE 1. Definition of the words $b_{0,m}$, $c_{0,j}$, $d_{0,j}$, $e_{0,m}$, $f_{0,k}$, $g_{0,\ell}$.

Now, if for a natural number i we have already defined the elements $b_{i-1,m}$, $c_{i-1,j}$, $d_{i-1,j}$, $e_{i-1,m}$, $f_{i-1,k}$, $g_{i-1,\ell}$ where $m = 1, 2, \ldots, 6$, $j = 1, 2, 3$, $k = 1, 2, \ldots, 12$, $\ell = 1, 2, 3, 4$, then we denote by $b_{i,m}$, $c_{i,j}$, $d_{i,j}$, $e_{i,m}$, $f_{i,k}$, $g_{i,\ell}$ respectively the words obtained by substituting the words $g_{i-1,1}$, $g_{i-1,2}$, $g_{i-1,3}$, $g_{i-1,4}$ for a_1, a_2, a_3, a_4 respectively in the expressions of the words $b_{0,m}$, $c_{0,j}$, $d_{0,j}$, $e_{0,m}$, $f_{0,k}$, $g_{0,\ell}$ where $m = 1, 2, \ldots, 6$, $j = 1, 2, 3$, $k = 1, 2, \ldots, 12$, $\ell = 1, 2, 3, 4$. We denote by C_0 the set of words

$$\{a_1, a_2, a_3, a_4\} \cup \{b_{i,m}, c_{i,j}, d_{i,j}, e_{i,m}, f_{i,k}, g_{i,\ell}\},$$

where $i = 0, 1, \ldots$ and $m = 1, 2, \ldots, 6$, $j = 1, 2, 3$, $k = 1, 2, \ldots, 12$, $\ell = 1, 2, 3, 4$.

Remark 9. Every element of the set C_0 is a regular word relative to C_1, and hence we have $C_0 \subset \mathfrak{CF}(C_1)$.

By definition $C_1 = \{a_1, a_2, a_3, a_4\}$. Now, if for some natural number i the set C_{6i-5} has been defined, then by $C_{6i-4}, C_{6i-3}, C_{6i-2}, C_{6i-1}, C_{6i}, C_{6i+1}$ respectively we denote the following sets:

$C_{6i-5} \cup \{b_{i-1,m}\}$, $m = 1, 2, \ldots, 6$; $\quad C_{6i-4} \cup \{c_{i-1,j}\}$, $j = 1, 2, 3$;

$C_{6i-3} \cup \{d_{i-1,j}\}$, $j = 1, 2, 3$; $\quad C_{6i-2} \cup \{e_{i-1,m}\}$, $m = 1, 2, \ldots, 6$;

$C_{6i-1} \cup \{f_{i-1,k}\}$, $k = 1, 2, \ldots, 12$; $\quad C_{6i} \cup \{g_{i-1,\ell}\}$, $\ell = 1, 2, 3, 4$.

On each of the sets C_i, $i = 0, 1, \ldots$ we define a partial binary commutative operation f_i (respectively) as follows:

4.1. If, for two distinct unitypical elements a and b in the set C_i, the product $a \cdot b$, using the operation $\cdot$ defined in the plane $\mathfrak{CF}(C_1)$, is also contained in C_i, then $f_i(a, b) = a \cdot b$, $i = 0, 1, \ldots$.

a_1	a_2	a_3	a_4	$b_{0,1}$	$b_{0,2}$	$b_{0,3}$	$b_{0,4}$
$b_{0,1}$	$b_{0,1}$	$b_{0,2}$	$b_{0,4}$	a_1	a_1	a_2	a_1
$b_{0,2}$	$b_{0,3}$	$b_{0,3}$	$b_{0,5}$	a_2	a_3	a_3	a_4
$b_{0,4}$	$b_{0,5}$	$b_{0,6}$	$b_{0,6}$	$c_{0,3}$	$c_{0,2}$	$c_{0,1}$	$c_{0,2}$
$f_{0,3}$	$f_{0,4}$	$f_{0,1}$	$f_{0,2}$	$e_{0,1}$	$e_{0,3}$	$e_{0,5}$	$e_{0,6}$
$f_{0,7}$	$f_{0,5}$	$f_{0,8}$	$f_{0,6}$				
$f_{0,9}$	$f_{0,11}$	$f_{0,12}$	$f_{0,10}$				

$b_{0,5}$	$b_{0,6}$	$c_{0,1}$	$c_{0,2}$	$c_{0,3}$	$d_{0,1}$	$d_{0,2}$	$d_{0,3}$
a_2	a_3	$b_{0,3}$	$b_{0,2}$	$b_{0,1}$	$c_{0,1}$	$c_{0,1}$	$c_{0,2}$
a_4	a_4	$b_{0,4}$	$b_{0,5}$	$b_{0,6}$	$c_{0,2}$	$c_{0,3}$	$c_{0,3}$
$c_{0,3}$	$c_{0,1}$	$d_{0,1}$	$d_{0,1}$	$d_{0,2}$	$e_{0,1}$	$e_{0,3}$	$e_{0,5}$
$e_{0,4}$	$e_{0,2}$	$d_{0,2}$	$d_{0,3}$	$d_{0,3}$	$e_{0,2}$	$e_{0,4}$	$e_{0,6}$

$e_{0,1}$	$e_{0,2}$	$e_{0,3}$	$e_{0,4}$	$e_{0,5}$	$e_{0,6}$	$f_{0,1}$	$f_{0,2}$
$b_{0,1}$	$b_{0,6}$	$b_{0,2}$	$b_{0,5}$	$b_{0,3}$	$b_{0,4}$	a_3	a_4
$d_{0,1}$	$d_{0,1}$	$d_{0,2}$	$d_{0,2}$	$d_{0,3}$	$d_{0,3}$	$e_{0,1}$	$e_{0,1}$
$f_{0,1}$	$f_{0,3}$	$f_{0,5}$	$f_{0,7}$	$f_{0,9}$	$f_{0,11}$		$g_{0,1}$
$f_{0,2}$	$f_{0,4}$	$f_{0,6}$	$f_{0,8}$	$f_{0,10}$	$f_{0,12}$		

$f_{0,3}$	$f_{0,4}$	$f_{0,5}$	$f_{0,6}$	$f_{0,7}$	$f_{0,8}$	$f_{0,9}$	$f_{0,10}$
a_1	a_2	a_2	a_4	a_1	a_3	a_1	a_4
$e_{0,2}$	$e_{0,2}$	$e_{0,3}$	$e_{0,3}$	$e_{0,4}$	$e_{0,4}$	$e_{0,5}$	$e_{0,5}$
$g_{0,2}$	$g_{0,1}$	$g_{0,2}$	$g_{0,3}$	$g_{0,3}$	$g_{0,4}$	$g_{0,4}$	

$f_{0,11}$	$f_{0,12}$	$g_{0,1}$	$g_{0,2}$	$g_{0,3}$	$g_{0,4}$
a_2	a_3	$f_{0,2}$	$f_{0,3}$	$f_{0,6}$	$f_{0,8}$
$e_{0,6}$	$e_{0,6}$	$f_{0,4}$	$f_{0,5}$	$f_{0,7}$	$f_{0,9}$
		$b_{1,1}$	$b_{1,1}$	$b_{1,2}$	$b_{1,4}$
		$b_{1,2}$	$b_{1,3}$	$b_{1,3}$	$b_{1,5}$
		$b_{1,4}$	$b_{1,5}$	$b_{1,6}$	$b_{1,6}$
		$f_{1,3}$	$f_{1,4}$	$f_{1,1}$	$f_{1,2}$
		$f_{1,7}$	$f_{1,5}$	$f_{1,8}$	$f_{1,6}$
		$f_{1,9}$	$f_{1,11}$	$f_{1,12}$	$f_{1,10}$

TABLE 2. The incidence relation α_0 (basis of induction).

4.2. In all other cases we declare that the operation f_i on C_i is undefined, $i = 0, 1, \ldots$.

Table 2 gives the incidence relation for elements of C_0: in each column, the first row gives an element $w \in C_0$, and the other rows give the elements of C_0

$b_{i,1}$	$b_{i,2}$	$b_{i,3}$	$b_{i,4}$
$g_{i-1,1}$	$g_{i-1,1}$	$g_{i-1,2}$	$g_{i-1,1}$
$g_{i-1,2}$	$g_{i-1,3}$	$g_{i-1,3}$	$g_{i-1,4}$
$c_{i,3}$	$c_{i,2}$	$c_{i,1}$	$c_{i,1}$
$e_{i,1}$	$e_{i,3}$	$e_{i,5}$	$e_{i,6}$

$b_{i,5}$	$b_{i,6}$	$c_{i,1}$	$c_{i,2}$	$c_{i,3}$	$d_{i,1}$	$d_{i,2}$	$d_{i,3}$
$g_{i-1,2}$	$g_{i-1,3}$	$b_{i,3}$	$b_{i,2}$	$b_{i,1}$	$c_{i,2}$	$c_{i,1}$	$c_{i,2}$
$g_{i-1,4}$	$g_{i-1,4}$	$b_{i,4}$	$b_{i,5}$	$b_{i,6}$	$c_{i,3}$	$c_{i,3}$	$c_{i,3}$
$c_{i,2}$	$c_{i,3}$	$d_{i,1}$	$d_{i,1}$	$d_{i,2}$	$e_{i,1}$	$e_{i,3}$	$e_{i,5}$
$e_{i,4}$	$e_{i,2}$	$d_{i,2}$	$d_{i,3}$	$d_{i,3}$	$e_{i,2}$	$e_{i,4}$	$e_{i,6}$

$e_{i,1}$	$e_{i,2}$	$e_{i,3}$	$e_{i,4}$	$e_{i,5}$	$e_{i,6}$	$f_{i,1}$	$f_{i,2}$
$b_{i,1}$	$b_{i,6}$	$b_{i,2}$	$b_{i,5}$	$b_{i,3}$	$b_{i,4}$	$g_{i-1,3}$	$g_{i-1,4}$
$d_{i,1}$	$d_{i,1}$	$d_{i,2}$	$d_{i,2}$	$d_{i,3}$	$d_{i,3}$	$e_{i,1}$	$e_{i,1}$
$f_{i,1}$	$f_{i,3}$	$f_{i,5}$	$f_{i,7}$	$f_{i,9}$	$f_{i,11}$		$g_{i,1}$
$f_{i,2}$	$f_{i,4}$	$f_{i,6}$	$f_{i,8}$	$f_{i,10}$	$f_{i,12}$		

$f_{i,3}$	$f_{i,4}$	$f_{i,5}$	$f_{i,6}$	$f_{i,7}$	$f_{i,8}$	$f_{i,9}$	$f_{i,10}$
$g_{i-1,1}$	$g_{i-1,2}$	$g_{i-1,2}$	$g_{i-1,4}$	$g_{i-1,1}$	$g_{i-1,3}$	$g_{i-1,1}$	$g_{i-1,4}$
$e_{i,2}$	$e_{i,2}$	$e_{i,3}$	$e_{i,3}$	$e_{i,4}$	$e_{i,4}$	$e_{i,5}$	$e_{i,6}$
$g_{i,2}$	$g_{i,1}$	$g_{i,2}$	$g_{i,3}$	$g_{i,3}$	$g_{i,4}$	$g_{i,4}$	

$f_{i,11}$	$f_{i,12}$	$g_{i,1}$	$g_{i,2}$	$g_{i,3}$	$g_{i,4}$
$g_{i-1,2}$	$g_{i-1,3}$	$f_{i,2}$	$f_{i,3}$	$f_{i,6}$	$f_{i,8}$
$e_{i,1}$	$e_{i,6}$	$f_{i,4}$	$f_{i,5}$	$f_{i,7}$	$f_{i,9}$
		$b_{i+1,1}$	$b_{i+1,1}$	$b_{i+1,2}$	$b_{i+1,4}$
		$b_{i+1,2}$	$b_{i+1,3}$	$b_{i+1,3}$	$b_{i+1,5}$
		$b_{i+1,4}$	$b_{i+1,5}$	$b_{i+1,6}$	$b_{i+1,6}$
		$f_{i+1,3}$	$f_{i+1,4}$	$f_{i+1,1}$	$f_{i+1,2}$
		$f_{i+1,7}$	$f_{i+1,5}$	$f_{i+1,8}$	$f_{i+1,6}$
		$f_{i+1,9}$	$f_{i+1,11}$	$f_{i+1,12}$	$f_{i+1,10}$

TABLE 3. The incidence relation α_0 (inductive step).

which are incident with w in $\mathfrak{CF}(C_1)$. This incidence relation[8] will be denoted by α_0. We construct a sequence of configurations using Tables 2 and 3.

Let C^0 and ${}^0C$ be the sets of regular words of first and second type respectively relative to the set C_1 in the plane $\mathfrak{CF}(C_1)$. Choose arbitrarily an element w in $\mathfrak{CF}(C_1)$ such that for some elements u and v in $\mathfrak{CF}(C_1)$ we have $w = \overline{uv}$.

[8]Table 2 gives the basis of the induction defining α_0, and Table 3 gives the inductive step. [Translators]

Then the pairs of the form (w,u), (u,w), (w,v) and (v,w) will be called the *basic incidences* of the element w, and the set $\{(w,u),\ (u,w),\ (w,v),\ (v,w)\}$ will be denoted by $\mathfrak{O}_w$ and called the *full set of basic incidences* of w in $\mathfrak{CF}(C_1)$.

We define the sequence of sets α_1, α_2, ..., α_i, ... as follows:

4.3. Set by definition $\alpha_1 = \emptyset$.

4.4. If, for some natural number i the set α_i has already been defined, then we define α_{i+1} in this way: for all elements in $C_{i+1} \setminus C_i$ we denote by β_{i+1} the union of all full sets of basic incidences,

$$\beta_{i+1} = \bigcup_{w \in C_{i+1} \setminus C_i} \mathfrak{O}_w,$$

and define $\alpha_{i+1} = \alpha_i \cup \beta_{i+1}$.

For each natural number i, we will denote by $\mathfrak{C}_i$ the partial algebraic system

$$\big\langle (C_i \cap C^0, C_i \cap {}^0C), f_i, \alpha_i \big\rangle, \qquad i = 1, 2, \ldots,$$

where f_i is the partial binary commutative operation defined on C_i and satisfying Conditions 4.1 and 4.2, and the relation α_i is defined for each i according to Conditions 4.3 and 4.4.

It follows immediately from the definitions of f_i and α_i, and the construction of the sets C_i, $i = 1, 2, \ldots$, that α_i is an incidence relation relative to the partition $(C_i \cap C^0, C_i \cap {}^0C)$ such that α_i and f_i are compatible on the set. Therefore we have the following result.

Lemma 4. *For every natural number i, the partial algebraic system*

$$\mathfrak{C}_i = \big\langle (C_i \cap C^0, C_i \cap {}^0C), f_i, \alpha_i \big\rangle,$$

is a configuration, and the extension $\mathfrak{C}_{i+1} \supset \mathfrak{C}_i$ is free.

Denote by $\mathfrak{C}_0$ the configuration equal to the union of the configurations $\mathfrak{C}_i$, $i = 1, 2, \ldots$:

$$\mathfrak{C}_0 = \bigcup_{i=1}^{\infty} \mathfrak{C}_i.$$

The configuration $\mathfrak{C}_0$ will be regarded as *the result of Construction* 6.

Remark 10. It follows from the construction of the sequence of configurations $\mathfrak{C}_1$, $\mathfrak{C}_2$, ..., $\mathfrak{C}_i$, ... that the configuration $\mathfrak{C}_0$ can also be defined as follows:

$$\mathfrak{C}_0 = \big\langle (C_0 \cap C^0, C_0 \cap {}^0C), \alpha_0, f_0 \big\rangle,$$

where α_0 is defined by Tables 2 and 3, and f_0 is the partial binary commutative operation satisfying Conditions 4.1 and 4.2.

For the sequence of configurations $\mathfrak{C}_i$, $i = 1, 2, \ldots$, and the configuration $\mathfrak{C}_0$, by virtue of their constructions and Lemma 4, all the conditions of Lemma 3 are satisfied. Hence the following holds.

Lemma 5. *Let $\mathfrak{CF}(C_1)$ be the completely free projective plane freely generated by the set C_1 of unitypical elements according to Construction* 1*, and let $\mathfrak{C}_0$ be the configuration resulting from Construction* 6*. Then $\mathfrak{CF}(C_1)$ is freely generated by $\mathfrak{C}_0$.*

3. Let $\mathfrak{B}_1$ and $\mathfrak{B}_2$ be configurations contained respectively in the projective planes $\mathfrak{A}_1$ and $\mathfrak{A}_2$. A mapping φ of $\mathfrak{B}_1$ onto $\mathfrak{B}_2$ will be called a *homomorphism of configurations* if the incidence of the elements x and y in $\mathfrak{B}_1$ implies the incidence of the elements $\varphi(x)$ and $\varphi(y)$ in $\mathfrak{B}_2$. In the case $\mathfrak{A}_i = \mathfrak{B}_i$, $i = 1, 2$, we will say that φ is a *homomorphism of projective planes* from $\mathfrak{A}_1$ onto $\mathfrak{A}_2$.

Construction 7. Let $U^0 = \{u_1, u_2, \ldots, u_i, \ldots\}$ be a fixed countable set of symbols ordered according to the indices, and let $\mathfrak{CF}(U^0)$ be the completely free plane freely generated by U^0 according to Construction 1. Denote by ${}^0U$ the set of all words of the form $u_{i+1}u_i$ where $i = 1, 2, \ldots$. Denote by $\mathfrak{U}$ the subconfiguration $\langle (U^0, {}^0U), *, \alpha\rangle$ in the projective plane $\mathfrak{CF}(U^0)$, where α is the union of the full sets of basic incidences for all elements of ${}^0U$,

$$\alpha = \bigcup_{w \in {}^0U} \mathfrak{O}_w,$$

the partial binary commutative operation $*$ is defined on the set $U^0 \cap {}^0U$ as follows,

$$u_{i+1} * u_i = u_{i+1}u_i, \qquad (u_{i+2}u_{i+1}) * (u_{i+1}u_i) = u_{i+1}, \qquad i = 1, 2, \ldots,$$

and all remaining products in $\mathfrak{U}$ are undefined. The configuration $\mathfrak{U}$ just obtained will be regarded as *the result of Construction* 7.

We have the following result.

Lemma 6. *Let U^0 be a countable set of symbols, and let $\mathfrak{CF}(U^0)$ be the completely free projective plane obtained from U^0 according to Construction* 1*. Let C_1 be a set consisting of four symbols, and let $\mathfrak{CF}(C_1)$ be the completely free projective plane obtained from C_1 according to Construction* 1*. Then there exists a homomorphism $\overline{\theta}$ of projective planes from $\mathfrak{CF}(C_1)$ onto $\mathfrak{CF}(U^0)$.*

Proof. First, we construct a mapping θ of the configuration $\mathfrak{C}_0$, obtained as the result of Construction 6, onto the configuration $\mathfrak{U}$, obtained as the result of Construction 7:

$$\begin{aligned}
&\theta(a_\ell) = \theta(c_{0,j}) = \theta(e_{0,m}) = u_1,\\
&\theta(b_{0,m}) = \theta(d_{0,j}) = \theta(f_{0,k}) = u_2u_1,\\
&\theta(g_{0,\ell}) = u_2,\ \ldots,\ \theta(g_{i-1,\ell}) = \theta(c_{i,j}) = \theta(e_{i,m}) = u_{i+1},\\
&\theta(b_{i,m}) = \theta(d_{i,j}) = \theta(f_{i,k}) = u_{i+2}u_{i+1},
\end{aligned}$$

where $m = 1, 2, \ldots, 6$, $j = 1, 2, 3$, $k = 1, 2, \ldots, 12$, $\ell = 1, 2, 3, 4$, $i = 1, 2, \ldots$.

It is clear from inspection of Tables 2 and 3, and the definition of the mapping θ, that if elements a and b are incident in the configuration $\mathfrak{C}_0$ then the elements $\theta(a)$ and $\theta(b)$ are incident in the configuration $\mathfrak{U}$. Hence the mapping θ is a homomorphism of configurations from $\mathfrak{C}_0$ onto $\mathfrak{U}$.

The configuration $\mathfrak{U}$ is freely equivalent to the configuration $\langle U^0, (U^0, \emptyset), \cdot, \emptyset\rangle$, and hence by Proposition 5 the projective plane $\mathfrak{CF}(U^0)$ is freely generated by the configuration $\mathfrak{U}$.

In [3] it is shown that if the plane $\mathfrak{P}_1$ is freely generated by a configuration $\mathfrak{A}_1$, the plane $\mathfrak{P}_2$ is generated by a configuration $\mathfrak{A}_2$, and there exists a homomorphism τ of configurations from $\mathfrak{A}_1$ onto $\mathfrak{A}_2$, then there exists a homomorphism $\overline{\tau}$ of projective planes from $\mathfrak{P}_1$ onto $\mathfrak{P}_1$ such that $\overline{\tau}$ is an extension of τ.

From this, together with Lemma 5, the definition of the configurations $\mathfrak{C}_0$ and $\mathfrak{U}$, and the construction of the homomorphism θ, it follows that there exists a homomorphism $\overline{\theta}$ of projective planes from $\mathfrak{CF}(C_1)$ onto $\mathfrak{CF}(U^0)$ such that $\overline{\theta}$ is an extension of θ. The lemma is proved. □

For what follows we will need the next result.

Proposition 9. [10] *Let $\mathfrak{P} = \langle (P^0, {}^0P), \cdot\rangle$ be a projective plane where P^0 and ${}^0P$ are the sets of elements of the first and second types in P. Then there exists a completely free projective plane $\mathfrak{CF}(\overline{V})$ such that $\mathfrak{CF}(\overline{V})$ is freely generated by a set $\overline{V}$ of unitypical elements, where the cardinalities of the sets P^0 and $\overline{V}$ are equal and there exists a homomorphism of planes from $\mathfrak{CF}(V)$ onto $\mathfrak{P}$.*

Now we will prove the following result.

Theorem 4. *Any finite or countably infinite projective plane is a homomorphic image of a completely free projective plane freely generated by a set of four elements.*

Proof. Let $\mathfrak{P} = \langle (P^0, {}^0P), \cdot\rangle$ be an arbitrary finite or countable infinite projective plane. Then from Proposition 9 it follows that there exists a completely free projective plane $\mathfrak{P}_1 = \mathfrak{CF}(\overline{V})$ such that $\mathfrak{P}_1$ is freely generated by the set $\overline{V}$ of unitypical elements, where the cardinalities of P^0 and $\overline{V}$ are equal, and there exists a homomorphism τ_1 of planes from $\mathfrak{P}_1$ onto $\mathfrak{P}$. Observe that any completely free projective plane, freely generated by a finite or countably infinite set, consists of a countably infinite set of elements.

If U^0 is a countably infinite set of symbols, and $\mathfrak{CF}(U^0)$ is the completely free projective plane freely generated by the set U^0 according to Construction 1, then it follows from Proposition 9 that there exists a homomorphism τ of planes from $\mathfrak{CF}(U^0)$ onto $\mathfrak{P}_1$.

By Proposition 4 it follows that if a plane is freely generated by a set of four elements, then this plane can also be freely generated by a set of four unitypical elements. For this reason let $C_1 = \{a_1, a_2, a_3, a_4\}$ be a set of four elements, let $\mathfrak{CF}(C_1)$ be the completely free plane obtained from C_1 according to Construction 1, and let $\overline{\theta}$ be the homomorphism of planes from $\mathfrak{CF}(C_1)$ onto $\mathfrak{CF}(U^0)$ constructed in Lemma 6. Then we obtain the following sequence of homomorphisms:

$$\mathfrak{CF}(C_1) \xrightarrow{\overline{\theta}} \mathfrak{CF}(U^0) \xrightarrow{\tau_1} \mathfrak{P}_1 \xrightarrow{\tau} \mathfrak{P}.$$

The composition of these homomorphisms gives the required homomorphism of planes from $\mathfrak{CF}(C_1)$ onto $\mathfrak{P}$. □

Corollary 2. [4] *Any projective plane with a finite number of generators is a homomorphic image of a completely free projective plane freely generated by a set of four elements.*

References

[1] A. Giovagnoli, *Sulla rappresentazione di un piano libero mediante una classe di simboli*, Rend. Mat. e Appl. 25, 3–4 (1966) 427–438.

[2] M. Hall, *Projective planes*, Trans. Amer. Math. Soc. 54 (1943) 229–277.

[3] D.R. Hughes and F.C. Piper, *Projective Planes*, Graduate Texts in Mathematics 6, Springer-Verlag, New York-Berlin, 1973.

[4] N.L. Johnson, *Homomorphisms of free planes*, Math. Z. 125 (1972) 255–263.

[5] K.H. Kim and F.W. Roush, *A universal algebra approach to free projective planes*, Aequationes Math. 19, 1 (1979) 48–52.

[6] L.I. Kopeikina, *Free decompositions of projective planes*, Izv. Akad. Nauk SSSR Ser. Mat. 9, 1 (1945) 495–526.

[7] R. Magari, *Su una classe di simboli atta a rappresentare gli elementi di un piano grafico e su un teorema di riduzione a forma normale*, Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. 33, 1 (1962) 37–44.

[8] G. Pickert, *Projektive Ebenen*, Die Grundlehren der Mathematischen Wissenschaften LXXX, Springer-Verlag, Berlin-Göttingen-Heidelberg, 1955.

[9] G. Pickert, *Projektive Ebenen*, Zweite Auflage, Die Grundlehren der Mathematischen Wissenschaften 80, Springer-Verlag, Berlin-New York, 1975.

[10] L.A. Skornyakov, *Projective planes*, Uspekhi Mat. Nauk 6, 6 (1951) 112–154.

Indication of Sources

[1] Подалгебры свободных алгебр Ли
(Subalgebras of free Lie algebras)
Mat. Sbornik N.S. 33 (75), (1953), no. 2, 441–452

[2] О представлении лиевых колец в ассоциативных кольцах
(On the representation of Lie rings in associative rings)
Uspekhi Mat. Nauk N.S. 8, (1953), no. 5 (57), 173–175

[3] Подалгебры свободных коммутативных и свободных антикоммутативных алгебр
(Subalgebras of free commutative and free anticommutative algebras)
Mat. Sbornik N.S. 34 (76), (1954), no. 1, 81–88

[4] О специальных J-кольцах
(On special J-rings)
Mat. Sbornik N.S. 38 (80), (1956), no. 2, 149–166

[5] Некоторые теоремы о вложении для колец
(Some theorems on embedding of rings)
Mat. Sbornik N.S. 40 (82), (1956), no. 1, 65–72

[6] О некоторых неассоциативных ниль-кольцах и алгебраических алгебрах
(On some nonassociative nil-rings and algebraic algebras)
Mat. Sbornik N.S. 41 (83), (1957), no. 3, 381–394

[7] О кольцах с тождественными соотношениями
(On rings with identical relations)
Mat. Sbornik N.S. 43 (85), (1957), no. 2, 277–283

[8] О свободных кольцах Ли
(On free Lie rings)
Mat. Sbornik N.S. 45 (87), (1958), no. 2, 113–122

[9] О проблеме Левицкого
(On a problem of Levitzki)
Doklady Akad. Nauk SSSR 120, (1958), no. 1, 41–42

[10] Некоторые вопросы теории колец, близких к ассоциативным
(Some problems in the theory of rings that are nearly associative)

Uspekhi Mat. Nauk 13, (1958), no. 6 (84), 3–20
Translated from the Russian original by Murray Bremner
and Natalia Fomenko.
Lect. Notes Pure Appl. Math., 246,
Non-associative algebra and its applications, 441–459,
Chapman & Hall/CRC, Boca Raton, FL, 2006

[11] Некоторые алгоритмические проблемы для ε-алгебр
(Some algorithmic problems for ε-algebras)
Sibirsk Mat. Zh. 3, (1962), no. 1, 132–137

[12] Некоторые алгоритмические проблемы для алгебр Ли
(Some algorithmic problems for Lie algebras)
Sibirsk Mat. Zh. 3, (1962), no. 2, 292–296

[13] Об одной гипотзе теории алгебр Ли
(On a hypothesis in the theory of Lie algebras)
Sibirsk Mat. Zh. 3, (1962), no. 2, 297–301

[14] О базах свободных алгебр Ли
(On the bases of a free Lie algebra)
Algebra Logika 1, (1962), no. 1, 14–19

[15] О некоторых группах, близких к энгелевым
(On some groups which are nearly Engel)
Algebra Logika 2, (1963), no. 5, 5–18

[16] О некоторых тождественних соотношениях в алгебрах
(On some identical relations for algebras)
Sibirsk Mat. Zh. 7, (1966), no. 4, 963–966

[17] О некоторых положительно определенных мнолообразиях групп
(On some positively definable varieties of groups)
Sibirsk Mat. Zh. 8, (1967) no. 5, 1190–1192

[18] К определению бинарной лиевости
(On the definition of the binary-Lie property)
Algebra Logika 10, (1971), no. 1, 100–102

[19] (с А.А. Никитиным) К теории проективных плоскостей
(with A.A. Nikitin. On the theory of projective planes)
Algebra Logika 20, (1981), no. 3, 330–356