Certain Algorithmic Problems for Lie Algebras*

A. I. Shirshov

Historical Background
by Michael Abramson

This short paper describes work similar to that appearing in Buchberger's 1965 thesis inventing Gröbner bases, but in the context of Lie Algebras. Preceding Buchberger by only three years, this paper, along with the two cited references, are the original papers defining what have become known as Gröbner-Shirshov bases.

1 Introduction

In the preceding work of the author [1], we examined certain algorithms and problems in the theory of ϵ-algebras. There we indicated some literature pertaining to the questions considered.

In the present work, similar questions are examined in the case of Lie algebras.

Unfortunately, obtaining solutions to the identity problem in this case has been unsuccessful. However, the identity problem is solved for Lie algebras with their defining relations and for Lie algebras with homogeneous sets of their defining relations. In addition, proving theorems for free Lie algebras is analogous to corresponding theorems in group theory.

2 Definition of Composition

Let L be a free Lie algebra over some field P with a set $R = \{a_\alpha\}$, $\alpha \in I$, of free generators. For brevity of exposition in what follows, definitions and results of the author's work [2] are utilized without special explanation.

Having fixed once and for all some ordering on the set R, we define regular associative and regular non-associative words, the generating elements of this set.

In [2], we proved that the regular non-associative words form a basis of the algebra L. In what follows, unless otherwise stipulated, no matter of which element of the algebra L we speak, we have in mind its representation in the form of a linear combination of elements of this basis.

The regular associative word corresponding to the leading term of an element $b \in L$ (without coefficient) is denoted by $\overline{b}$.

Thus we choose two arbitrary elements b and c in L, such that $\overline{b} = b_1 b_2$ and $\overline{c} = c_1 c_2$, where $b_2 = c_1$; b_1, b_2, c_2 are some (nonempty associative) words, and the leading term coefficients of the elements b and c are equal to one.

Lemma 1. *The associative word $u = b_1 b_2 c_2 = b_1 c_1 c_2$ is regular.*

Proof. Let $u = w_1 w_2$ and w_1 appear as a subword of the word b. Then $\overline{b} = w_1 v$, $\overline{b} > v$, and this means $w_1 w_2 > w_2 w_1$. In this same case, when w_2 appears as a subword of the word c_2, i.e. $c_2 = c_2' w_2$, the inequality $w_1 w_2 > w_2 w_1$ appears as a consequence of the obvious inequalities $w_2 < c_2 < \overline{c} < u$. □

In agreement with Lemma 4 of [2], we form non-associative words b_1 and b_2, having arranged the parentheses in the word u in two different ways: $u_1 = \{\ldots[(\overline{b}q_1)q_2]\ldots\}q_s$, where the q_i are regular (non-associative) words, $\overline{q}_1\overline{q}_2\cdots\overline{q}_s = c_2$ and $q_1 \leq q_2 \leq \ldots \leq q_s$; $u_2 = r_1\{r_2\ldots[r_{t-1}(r_t\overline{c})]\ldots\}$, where the r_j are regular non-associative words and $\overline{r}_1\overline{r}_2\cdots\overline{r}_t = b_1$. Let $u_1' = \{\ldots[(bq_1)q_2]\ldots\}q_s$ and $u_2' = r_1\{\ldots[r_{t-1}(r_t c)]\ldots\}$.

Definition 1. We will denote the composition $(b,c)_{c_1}$ of the elements b and c relative to the word c_1 by the element $t = \alpha(u_1' - u_2')$, where $\alpha \in P$ is a factor, the inverse of the leading term coefficient, of the element $u_1' - u_2'$.

Consequently, composition is clearly not defined for every pair b, c of elements of the algebra L and its existence depends on the word c_1.

Lemma 2. *For the pair b, b, composition is impossible to form.*

Proof. It is sufficient to show that two representations $\overline{b} = b_1 b_2 = b_2 b_3$ are impossible, where b_2 is a nonempty associative word.

* *Sibirskii Matematicheskii Zhurnal* [*Siberian Math. J.*] **3** (1962), 292-96. Translated by Michael and Rebecca Abramson.

Let $\overline{b} = b_1 b_2 = b_2 b_3$. From the definition of regular, it follows that $\overline{b} > b_3 b_2$, i.e. $b_1 > b_3$. On the other hand, $\overline{b} > b_2 b_1$, i.e. $b_3 > b_1$. The contradiction is obvious. We 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 is impossible to form, since the previous result on the existence of the composition $(b,c)_{c_1}$ induces the inequality $\overline{b} > \overline{c}$. □

3 Some Identity Problems

We examine the essentials for the definitions that follow.

Definition 2. The finite set $S = \{s_i\}$, $i = 1, \ldots, k$, of elements of the algebra L is called *reduced* if none of the associative words $\overline{s_i}$ appears as a subword of any other word $\overline{s_j}$ $(s_i, s_j \in S)$, and the leading term coefficients of its elements are equal to one.

Let S be some reduced set of elements of the algebra L, and S^* be the set of leading terms of elements of the set S and of elements obtained from elements of the set S with the help of all possible (for every term) compositions.

Definition 3. The reduced set S of elements of the algebra L is called *stable* if the degree of the composition $(s', s'')_c$ of any two elements s' and s'' belonging to S, is obtained either from elements of the set S with the aid of some number of compositions, each of greater degree than the elements s', s'', or if none of the elements of the set S^* contains any other element of this same set as a subword (in particular, all elements of the set S^* are distinct).

Theorem 1. *Let S be some stable set of elements of the algebra L. Then there exists an algorithm, allowing 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 the algebra L.*

Proof. We deduce Theorem 1 from the following lemma.

Lemma 3. *An element $t \in L$ belongs to the ideal $\langle S\rangle$, generated in L by elements of the stable set S, if and only if the word $\overline{t}$ contains one of the words of the set S^* as a subword.*

Proof. Let $t \in \langle S\rangle$. Then the element t is represented in the form of a linear combination of elements d_i of the form $d_i = c_1 c_2 \cdots c_{k_i} s_{p_i} f_1 f_2 \cdots f_{l_i}$, where parentheses are arranged in some way, $s_i \in S$, and c_j, f_j are regular words. Since the regular associative words u and v are greater than the regular words uv and vu, without loss of generality, it is possible to assume that $\overline{d}_i = \overline{c}_1 \overline{c}_2 \cdots \overline{c}_{k_i} \overline{s}_{p_i} \overline{f}_1 \overline{f}_2 \cdots \overline{f}_{l_i}$ is a regular word. The assertion of the lemma is obvious if the word $\overline{d}_1$ is greater than the word $\overline{d}_i$ of highest degree; it has no equal among the remaining words d_j, $j \neq 1$, dependent on the element t. Now let $d_1 = d_j$, $j \neq 1$. We consider first the simplest case, when $\overline{s}_{p_j}$ appears as a subword of one of the words $\overline{c}_1 \overline{c}_2 \cdots \overline{c}_{k_i}$ or $\overline{f}_1 \overline{f}_2 \cdots \overline{f}_{l_i}$.

We consider the first case (the second is entirely analogous to the first). From the regularity of the words $\overline{d}_j, \overline{s}_{p_1}, \overline{s}_{p_j}$, it follows ([2, Lemma 4]) that it is possible to arrange the parentheses in the word $\overline{d}_j$ in the following manner:

$$d' = c_1' c_2' \cdots c_q' [\cdots((\tilde{\overline{s}}_{p_j} c_{q+1}') c_{q+2}') \cdots] c_r' \\ \cdots c_{k_1} [\cdots ((\tilde{\overline{s}}_{p_1} f_1') f_2') \cdots f_m'] f_{m'} \cdots f_{l_1}$$

where c_ρ', f_ν' are regular words, $c_{q+1}' \leq c_{q+2}' \leq \ldots \leq c_r'$, $f_1' \leq f_2' \leq \ldots \leq f_m'$, parentheses stand in the remaining places just as in the word $\tilde{\overline{d}}_j$, and $\tilde{\overline{s}}_i$ denotes the regular non-associative word corresponding to $\overline{s}_i$. Let further d_1' and d_j' denote the elements of the algebra L obtained from d' as a result of substituting $\tilde{\overline{s}}_{p_1}$ for s_{p_1}, $\tilde{\overline{s}}_{p_j}$ for s_{p_j}, respectively.

In an obvious way, the differences $d_1 - d_1'$ and $d_j - d_j'$ admit expression in the form of a linear combination of elements, analogous to d_i, but having a leading term less than that of d_1. As in the proof of [1, Lemma 2], it was proved that the difference $d_j' - d_1'$ admits an analogous expression. Consequently, the equation

$$d_j = d_1 - (d_1 - d_1') + (d_j' - d_1') + (d_j - d_j')$$

follows, where it is possible to replace the element d_j by a sum of the element d_1 and of some other analogous elements with smaller leading terms. Reduction of such terms decreases the domain of leading terms, or obviously lowers the leading term induction.

Still possible is the case when $\overline{s}_{p_1} = e_1 e_2$, $\overline{s}_{p_j} = e_2 e_3$. Then by Lemma 1, the subword $e_1 e_2 e_3$ of the word $\overline{d}_1$ is regular; it is possible to order the parentheses in the word $e = e_1 e_2 e_3$ in the two ways described in the definition of composition, and to extend both this and other orderings of parentheses in a unique way to the complete ordering of parentheses in the word $\overline{d}_1$. The difference δ of elements d_1'' and d_j'', obtained as indicated with the help of the substitution of the words $\tilde{\overline{s}}_{p_1}$ and $\tilde{\overline{s}}_{p_j}$ corresponding to s_{p_1} and s_{p_j}, might be obtained from the word $\overline{d}_1$ with the help of the substitution of the word e in the composition

$(s_{p_1}, s_{p_j})_{e_2}$ and the consequent ordering of parentheses, as in the elements d_1'' and d_j''. As in the preceding case, the proof is complete by the considered equation

$$d_j = d_1 - (d_1 - d_1'') + (d_j - d_j'') - \delta. \qquad \square$$

To prove Theorem 1, it suffices to convince oneself that it is possible in a finite number of steps to write out the elements of the set S^* whose degree does not exceed the degree of the element t. If the word $\bar{t}$ is contained as a subword in some word from S^*, then an element t_0 can be found in the ideal $\langle S \rangle$ such that $\bar{t}_0 = \bar{t}$. Then instead of the element t above, we should consider the difference $t - t_0$. $\square$

Corollary 1. *There exists an algorithm solving the identity problem for Lie algebras with one defining relation.*

This follows from the obvious stability of the set consisting of one element.

Corollary 2. *No Lie algebra with one defining relation exists, having finite dimension ≥ 3.*

From this, the assertion follows, that in the Lie algebra with relation $s = 0$, distinct words v_i, for which $\overline{v}_i$ is not contained as a subword of the word $\overline{s}$, are nevertheless linearly independent.

Theorem 2. *There exists an algorithm solving the identity problem for Lie algebras with homogeneous sets of defining relations.*

Proof. Let us choose some homogeneous set S in the algebra L. If the set S is not reduced, then it is possible to replace it with an already reduced set S_1, such that $\langle S \rangle = \langle S_1 \rangle$. Indeed, if $\overline{s}_i$, $s_i \in S$, appears as a subword of some word $\overline{s}_j$, $s_j \in S$, then it is possible to construct an element s_0 of the ideal $\langle s_i \rangle$, such that $\overline{s}_0 = \overline{s}_j$, so instead of the element s_j, we consider the element $s_j' = s_j - s_0$.

The proof that the process of reduction finishes in a finite number of steps coincides with the proof of [1, Lemma 1]. It is obvious that, in addition, the resulting set S_1 will consist of homogeneous elements. Since the composition of homogeneous elements is homogeneous, it fulfills the requirement of the definition of stability for degrees. It is also obvious that in a finite number of steps, it is possible to write out all of the elements of the set S^* whose degree does not exceed the degree of some given element $t \in L$. In addition, it may be necessary to carry out the process of reduction on the sets obtained from the set S_1 by adjoining the composition of these or other elements. The proof is finished as in Theorem 1. $\square$

Theorem 3 (on freeness). *Let L_0 be a Lie algebra with a set R of generators and with one defining relation $s = 0$ on the left side which contains the generator a_α. Then the subalgebra L_0', generated by the set $R - a_\alpha$ in the algebra L_0, is free.*

Proof. Except for the natural ordering of regular words, we consider the following ordering on the component basis of the free Lie algebra L. The regular word u will be regarded as greater than the regular word v if the generators a_α contained in the word u are greater than the number one. If in fact the a_α contained in u and v are equal to the number one, then these words are first compared by degree, and in the case of equal degrees, by the usual lexicographic comparison of the words $\overline{u}$ and $\overline{v}$. The associative word $\overline{\overline{s}}$, corresponding to the leading term of the element s in the sense of this new ordering, may not coincide with the word $\overline{s}$. Repeating the argument using the proof of Lemma 3 and based on Lemma 2, we come to the assertion that the element t belongs to the ideal $\langle s \rangle$ if and only if the word s appears as a subword of the word t. Since the generators a_α are contained in a component of the word s, it follows that the subalgebra L_0 has empty intersection with the ideal $\langle s \rangle$. This is equivalent to the assertion of the theorem. $\square$

Received 29 June 1961

References

[1] A. I. Shirshov (1961). *Some Algorithmic Problems for ϵ-Algebras.* Siberian Math. J. **3**: 132-137.

[2] A. I. Shirshov (1958). *On Free Lie Rings.* Mat. Sb. **45**: 113-121.