Encyclopaedia of Mathematical Sciences
Volume 57

A. I. Kostrikin · I. R. Shafarevich (Eds.)

Algebra VI

Springer-Verlag

Encyclopaedia of Mathematical Sciences

Volume 57

Editor-in-Chief: R.V. Gamkrelidze

Springer
Berlin
Heidelberg
New York
Barcelona
Budapest
Hong Kong
London
Milan
Paris
Tokyo

A. I. Kostrikin I. R. Shafarevich (Eds.)

Algebra VI

Combinatorial and Asymptotic Methods of Algebra. Non-Associative Structures

Springer

Title of the Russian edition:
Itogi nauki i tekhniki, Sovremennye problemy matematiki,
Fundamental'nye napravleniya, Vol. 57, Algebra 6
Publisher VINITI, Moscow 1990

Library of Congress Cataloging-in-Publication Data

Algebra 6. English.
Algebra VI : combinatorial and asymptotic methods of algebra : nonassociative structures / A.I. Kostrikin, I.R. Shafarevich (eds.).
p. cm. -- (Encyclopaedia of mathematical sciences ; v. 57)
Includes bibliographical references and index.
ISBN 3-540-54699-5 (Berlin : alk. paper). -- ISBN 0-387-54699-5 (New York : alk. paper)
1. Nonassociative algebras. 2. Algebra, Homological. 3. Combinatorial analysis. I. Kostrikin, A. I. (Alekseĭ Ivanovich) II. Shafarevich, I. R. (Igor' Rostislavovich), 1923- III. Title. IV. Title: Algebra 6. V. Series.
QA252.A4413 1994
512--dc20 93-25596
CIP

Mathematics Subject Classification (1991):
16Pxx, 16Wxx, 17-XX, 17D10, 17D25, 18Gxx, 20F10,
20N05, 20N07, 55-XX, 68Q20, 68Rxx, 81R50

ISBN 3-540-54699-5 Springer-Verlag Berlin Heidelberg New York
ISBN 0-387-54699-5 Springer-Verlag New York Berlin Heidelberg

Printed in Germany
Typesetting: Springer TEX in-house system
SPIN 10020719 41/3142 - 5 4 3 2 1 0 - Printed on acid-free paper

List of Editors, Authors and Translators

Editor-in-Chief

R. V. Gamkrelidze, Russian Academy of Sciences, Steklov Mathematical Institute, ul. Vavilova 42, 117966 Moscow, Institute for Scientific Information (VINITI), ul. Usievicha 20a, 125219 Moscow, Russia, e-mail: gam@ips.ac.msk.su

Consulting Editors

A. I. Kostrikin, Moscow University, MEHMAT, 119899 Moscow, GSP-1, Russia
I. R. Shafarevich, Steklov Mathematical Institute, ul. Vavilova 42, 117966 Moscow, Russia

Authors

E. N. Kuz'min, Mathematical Institute of the Siberian Division of the Russian Academy of Sciences, 4 University Ave., 630090 Novosibirsk, Russia
V. A. Ufnarovskij, Mathematical Institute of the Academy of Sciences of Moldavia, 5 ul. Grosula, 277028 Kishinev, Moldavia and Department of Mathematics, University of Lund, Box 118, 22100 Lund, Sweden, e-mail: ufn@maths.lth.se
I. P. Shestakov, Mathematics Institute of the Russian Academy of Sciences, Universitetskij prospekt 4, 630090 Novosibirsk, Russia

Translator

R. M. Dimitrić, Department of Mathematics, University of California, Evans Hall, Berkeley, CA 94702, USA, e-mail: dimitric@ocf.Berkeley.edu

Contents

I. Combinatorial and Asymptotic Methods in Algebra

V. A. Ufnarovskij

Translated from the Russian
by R. M. Dimitrić

Contents

Preface to the English Edition

Almost five years have past since the original book had been written. At the time the English version became ready, it seemed natural to write an additional chapter in order to add some new results, and perhaps even more importantly, to express some new points of view on the subject of the book.

At this time distance, it is not surprising that some things look too naive now. For example, it would appear strange that quantum groups, that are so much in fashion today, would need additional "advertising", which was the purpose of the last chapter of the original book. That chapter could be harmlessly excluded from the English translation: its main aim was to attract more attention to some important subjects – something that has been already achieved today. We have nevertheless retained the chapter, for books have their own lives and, to change a book in this way would mean to create a new one. We also think that the chapter in question will provide an insight into the fast development of the subject of quantum groups over a relatively short period of time.

The last chapter contains more results, both new and old, unavailable to the author at the time of writing of the main body of the text. After selecting them in a limited period of time, the author was unable to paint the complete picture, but he still hopes that every bit of new information will be useful. At the end we have added a number of new references mentioned in this chapter.

I would like to thank Prof. R. Dimitrić for completing a hard work of translating this book from the Russian into English. In addition, he has rendered the author's rudimentary English version of the last chapter into a readable text. I am also grateful for his patience in clarifying mathematical concepts as well as finding the most suitable way of expressing them, even in the cases when the author himself was unsure of the intended meaning.

The author also expresses gratitude to his publisher "Springer-Verlag", for their attention and help.

Introduction

While admiring elegant proofs that lead us to the very tops of peaks of mathematical achievement, we often ask ourselves one and the same question: how was it possible to think of that? There are no surprises here: all that elegance is a result of tuning up of sufficiently coarse, technically complex and intricate reasoning, when the work was done in terms of perfectly elementary objects and formulas in the area called "calculations" that are rarely shown in a mathematical paper with its true weight. What are these elementary reasonings based upon? Certainly (and arguably) upon two components: on purely physical, for instance geometrical intuition, "the sense" for simple mathematical objects and the highly developed combinatorial thinking of a mathematician, enabling him to operate easily with elementary abstract objects: diagrams, words, formulas.

In this article we primarily discuss this combinatorial aspect of algebraic reasoning, the matter that could be called combinatorial algebra. In this wide context, however, combinatorial algebra contains homological algebra and vigorously developing computer algebra. On the other hand, by the term combinatorial algebra in its narrow meaning, we mean the study of algebraic objects defined by its generators and relations. We will find ourselves somewhere in between these two interpretations.

It is not possible to encompass the whole of combinatorial algebra. Part of the questions, connected with homological algebra, identities and combinatorial group theory has been left out consciously since that material is contained in sufficient detail in other volumes of the series: (Bakhturin, Ol'shanskij, 1988), (Gel'fand, Manin, 1989), (Bokut', L'vov, Kharchenko, 1988), (Ol'shanskij, Shmel'kin, 1989). Topics related to computer algebra and asymptotical methods in topology have been presented in a sketchy form, since there are fairly detailed surveys in those directions in Russian such as (Babenko, 1986), (Latyshev, 1988), (Buchberger, Collins, Loos, 1982) and new volumes are in preparation. On the other hand, some questions have been treated in more detail, primarily in order to show those elementary bricks that make up complicated combinatorial proofs. Consequently, the text contains quite a few completely simple claims, with short, almost obvious proofs and illustrating examples whose aim is to help in familiarizing with the technique of combinatorial reasoning. On the other hand, the article contains sufficiently many of the latest results in the area of combinatorial algebra, equipped with sketchy proofs and references to more rigorous reasoning. In that, the author did not strive to find the initial sources of this or that fact, but was rather led by considerations on availability of the sources to the Soviet reader. For example, the book by Krause and Lenagan: "Growth of algebras and Gelfand-Kirillov dimension", which would be natural to quote, was absent not only during preparation of the script by I.M. Gel'fand and

A.A. Kirillov, but also in USSR in general, thus the unique reference to this work is the acknowledgement of its existence.

The main object of our investigations will be infinite-dimensional algebras and their asymptotic behavior. In the whole, however, the class of the objects we will study will be considerably wider. For example, considerable attention will be paid to infinite groups and semigroups. Giving up certain finiteness conditions is usually telling in a most radical way through the character of problems solved and the obstacles arising in the process. Sometimes the difficulties arise already at the level of definitions, when this or that idea, based on some sorting out turns to be unsuitable. Here is the kingdom of unsolvability. In addition, problems of exact description of objects, so characteristic in the finite case, are replaced here by problems on description and calculation of some, fairly coarse characteristics of objects, such as their growth, which allow us to give a relatively clear picture of laws of asymptotic behavior of objects.

The main technique in the exposition is based on application of Gröbner basis (Sect. 2) as well as the method of generating functions (Sect. 3). Graded algebras of general position are studied in Sect. 4 and the algorithmic unsolvability of fundamental asymptotic questions is shown. Section 5 and part of Sect. 7 are devoted to problems on growth. The sixth section is devoted to word combinatorics as well as to nilpotency questions, while the seventh is devoted to identities in algebras. The eighth and partly the ninth sections concentrate around questions on relationships among different series: Hilbert, Poincaré, Poincaré-Betti. Basic properties of local rings are briefly considered in the ninth section. Hyperbolic and quantum groups are the subject of consideration in the last section. Lastly, the first section and sufficiently detailed index have an auxiliary character.

This work would not have appeared without help of other mathematicians. First of all, I would like to single out I.K. Babenko, whose paper (Babenko, 1986) was substantially explored by the author. It would have been impossible to have worked without material (manuscripts among them) that were kindly allowed to my disposal by L.A. Bokut', E.S. Golod, R.I. Grigorchuk, V.N. Gerasimov, A.A. Kirillov, V.T. Markov, A.A. Mikhalev, M.V. Sapir, V.I. Trofimov as well as by foreign colleagues D. Anick, J. Backelin, L. Avramov, T. Gateva-Ivanova (who also gave many valuable advices after reading the manuscript), J.E. Roos. Extremely useful and fruitful were discussions on the material in the article with A.Z. Anan'in, A.Ya. Belov, V.V. Borisenko, A.I. Bondal, E.I. Zel'manov (who also allowed me to get acquainted with proofs in his manuscripts), S.K. Kozhokar', I.V. L'vov, A.V. Mikhalev, Yu. M. Ryabukhin, A.D. Chanyshev, G.P. Chekanu. After reading the first variant of the manuscript I received valuable comments by V.N. Latyshev, A.I. Kostrikin, I.R. Shafarevich. I deeply acknowledge all of them and other of my colleagues for their help. All the deficiences are on the author's conscience. Note that the references cited with the results are not necessarily pointing to the first authors of those results.

§1. Basic Objects and Constructions

1.1. Introduction. This section has an introductory character. We have gathered here, for the convenience of the reader, the most important definitions and constructions that we will need in the sequel.

Let us introduce the basic notation in our investigations. First of all, we will fix the symbol K to denote the ground field, throughout the whole paper. Recall that an algebra A is a vector space with a multiplication law satisfying the conditions of linearity and distributivity. For example $(\alpha a+\beta b)c = \alpha ac+\beta bc$ for $\alpha, \beta \in K; a, b, c \in A$.

As a rule we will omit the multiplication symbol, but, in the case of Lie (super)algebras, we will, following tradition, denote the product of two elements by $[ab]$ (details follow).

The term *algebra* will usually denote an associative algebra with the unity **1**, i.e. multiplication will be assumed to be associative: $(ab)c = a(bc)$. The exceptions will be the nil algebras (1.2), where the unity is not required, and, naturally, Lie (super)algebras, where there is no associativity. In order to give uniform definitions of Lie algebras and superalgebras, we recall that a mapping $d : A \longrightarrow A$ is called *derivation* on a (not necessarily associative) algebra A if the following conditions are satisfied: $d(xy) = (dx)y + x(dy)$. A *Lie algebra* L is an anticommutative algebra, where multiplication by any element is a derivation. In other words, the following two identities are satisfied in L:

$$[xy] + [yx] = 0,$$

$$[x[yz]] = [[xy]z] + [y[xz]]$$

(the second identity is equivalent to the Jacoby identity – see 1.2).

Any algebra of derivations of an associative algebra with the following multiplication:

$$[d_1d_2] = d_1d_2 - d_2d_1$$

may be an example of a Lie algebra.

Remark. In the case of characteristic 2, the identity $[xx] = 0$ (automatically satisfied for other characteristics) ought to be added to the definition of a Lie algebra.

The use of superalgebras will be not for the sake of fashion but rather for acknowledging their most important role in the theory that follows. Recall that a *superalgebra* (or a $\mathbb{Z}_2$-graded algebra) is a (not necessarily associative) algebra A expressible in the form of the direct sum of two of its subspaces

$$A = A_{\bar{0}} \oplus A_{\bar{1}}$$

– the even and odd parts, such that $A_{\bar{i}}A_{\bar{j}} \subseteq A_{\overline{i+j}}$. Here, the sum $i + j$ is taken modulo 2, for instance $A_{\bar{1}}A_{\bar{1}} \subseteq A_{\bar{0}}$, thus the decomposition of this kind is called the $\mathbb{Z}_2$-graduation. If $x \in L_{\bar{i}}$, then x has *parity* $|x| = i$.

The main example of a superalgebra is a *graded* algebra A, i.e. an algebra A representable as the direct sum of its finite-dimensional subspaces $A = \bigoplus_{n=0}^{\infty} A_n$, such that $A_n A_m \subseteq A_{n+m}$. Naturally, the elements in even components A_n are even and the elements in the odd components are odd. We will study graded algebras, beginning with Section 3 and they will be the principal objects of investigations in the present paper.

Just as for algebras, we will assume without saying that the term "superalgebra" denotes an associative superalgebra with unity, making an exception from that rule only for the Lie (super)algebras. We will also assume without saying that all linear transformations, connected with superalgebras (e.g. homomorphisms, derivations etc.) preserve the $\mathbb{Z}_2$-graduation i.e. map the elements with parity into the elements with parity. Moreover, for homomorphisms, it will be assumed that even elements are mapped into even and odd into odd.

In order to memorize formulas in the super-case, it will be useful to be guided by the following mnemonic rule: compared with the ordinary formulas, they differ in that they have the sign $(-1)^{|x||y|}$ appearing every time when the symbols x and y have reversed their places in the formula. We attempt to define a Lie superalgebra, lead by this rule. First of all we define *derivation* of a (not necessarily associative) *superalgebra of parity* $|d|$ as a linear transformation into itself, satisfying the following condition

$$d(xy) = (dx)y + (-1)^{|d||x|}x(dy)$$

for elements x, y with parity.

A superalgebra with multiplication, defined via brackets [ ], is called a *Lie superalgebra* if the following identities are satisfied there:

$$[xy] + (-1)^{|x||y|}[yx] = 0$$

$$[x[yz]] = [[xy]z] + (-1)^{|x||y|}[y[xz]]$$

for the elements with parity. The last identity means that the multiplication by an element x with parity is derivation of the corresponding parity.

The algebra generated by the derivatives on any superalgebra can provide an example of a Lie superalgebra. Here, even derivations form the even part, odd form the odd part and the multiplication is defined by the graded commutator:

$$[d_1 d_2] = d_1 d_2 - (-1)^{|d_1||d_2|} d_2 d_1.$$

We see that superalgebras are natural generalizations of ordinary algebras (if all elements are even, then we get ordinary algebras and Lie algebras). In the main, the theories in the ordinary and the super-case are perfectly parallel. Super-theory however has not only the advantage that it is more general. It turns out that taking signs into account can be seen as the other side of the mirror of the ordinary mathematical world. For instance the "behind-the-mirror" analogue of the polynomial algebra of several variables is the exterior algebra (see 1.3). This is confirmed through a connection between the super-theory with modern physics (see Lejtes, 1984). On the other hand, the super-theory is a striking little bridge, enabling a special kind of induction for the proof of important theorems (see Kemer, 1984 and Zelmanov, 1988). The basic idea here consists of the fact that the role of the inductive transition enables the transition from the superalgebra to its even part, that is an ordinary algebra. The meaning of this idea is also in that the notion of a superalgebra unites into one whole the notions of an algebra and the module over it (see 1.5), since the odd part is a module over the even part.

Nevertheless, the reader may courageously count on the fact that the unfamiliarity with the super-theory will not cause even the least damage, especially if he is accustomed to view the bracket $[xy]$ as the *graded commutator* $xy - (-1)^{|x||y|}yx$, in the super-case.

Remark. In the case of characteristics 2 and 3 the following additions to the definition of a Lie superalgebra are necessary:

(1) $[xx] = 0$ for even elements.

(2) $[x[xx]] = 0$ for odd elements.

(3) the existence of the quadratic operator $q : L \longrightarrow L_{\bar{0}}$ satisfying the following conditions:

(a) $q(\alpha a) = \alpha^2 q(a); \alpha \in K, a$ even,

(b) $[ab] = q(a+b) - q(a) - q(b); a, b$ odd,

(c) $[a[ab]] = [q(a)b]; a, b$ odd.

Therefore, in order not to specify similar exceptions, we can restrict ourselves to the characteristics of the field different from two and three at least in the case when we discuss Lie superalgebras.

1.2. Ways of Defining Infinite-dimensional Algebras. The most comfortable way in working directly with an algebra is, after all, by giving a basis and a multiplication table on it. For instance this is the way to define the *polynomial algebra* and a *free associative algebra* (i.e. the algebra of polynomials over the non-commuting variables). The basis in both of these algebras is formed by the monomials (in the case of free algebras, they are indeed often called words), while the multiplication table is given in the natural way since the product of monomials is again a monomial. For instance, the product of the monomial xy by itself will be the monomial $xyxy$, but in the first algebra it could be written down also in the form x^2y^2.

With all its comfort, this method of representation is not used all that frequently, because it requires more or less the multiplication rules of the same type because of the infinity of the "multiplication table". In practice, a much more frequent situation is when it is not possible to describe even the basis uniformly, not to speak of the multiplication laws. In one case, however, this way is used regularly; we have in mind the group and semigroup algebras.

Sometimes (and in our paper frequently enough) it is more comfortable to consider, instead of a group G, its *group algebra* $K[G]$ over a field K, that may be defined in the following way: the elements of G are declared to form its basis and the multiplication law in G (Cayley's table) is nothing else but the multiplication table in $K[G]$. In order to avoid ambiguity (especially when the multiplication law is written additively) we will frequently enough use, instead of the elements g, for the basis the, symbols e_g indexed by the elements of the group.

For instance, for the group $\mathbb{Z}$ of integers, the group algebra will have the basis e_i and the multiplication law $e_i e_j = e_{i+j}$ $(i, j \in \mathbb{Z})$.

All the aforementioned carries over literally from a group to a semigroup with the use of the notion of a *semigroup algebra*. Let us point out that isomorphic group algebras may correspond to non-isomorphic groups (for example, the group algebras over the complex numbers for the dihedral and the quaternion groups (1.3) are isomorphic).

One usually tries to define algebras descriptively and directly through its defining properties. This is the characteristic "physical" definition. For example, we can describe the algebra whose elements are all linear operators acting on some spaces and preserving their structures. As an example, we mention the endomorphism algebra $\mathrm{End}(A)$ and the *algebra of Lie derivatives* $\mathrm{Der}(A)$ of a fixed algebra A.

In the majority of the cases such a description enables us to get a description of the basis and the multiplication table. However, in this process, "the physical intuition" is lost and an effort is made not to use this basis until the beginning of direct calculations.

One more approach is a reduction to the classical or almost classical objects. For instance many infinite groups arise as matrix groups. Infinite-dimensional algebras can also be viewed as matrix algebras, but of infinite dimension. For example, if we choose a basis in an infinite-dimensional algebra, then the endomorphism algebra $\mathrm{End}(A)$ is realized through infinite matrices in that basis.

Another way is to introduce new operations on classical objects. Here are examples of this kind (that themselves have become classical).

We can make a Lie algebra A_L from an associative algebra A, introducing a new multiplication: $[ab] = ab - ba$. It is easy to see that it will satisfy the defining identities for a Lie algebra:

$$[ab] = -[ba] \quad \text{(the anti-commutativity identity)}$$

$$[[ab]c] + [[bc]a] + [[ca]b] = 0 \quad \text{(the Jacoby identity).}$$

If A is a superalgebra, then a Lie superalgebra A_L can be made by introducing the graded commutator:

$$[xy] = xy - (-1)^{|x||y|} yx.$$

Jacoby's identity in the super-case assumes the following form:

$$(-1)^{|x||z|}[x[yz]] + (-1)^{|y||x|}[y[zx]] + (-1)^{|z||y|}[z[xy]] = 0.$$

1.3. Combinatorial Approach. The most important way of defining algebras for us consists of describing them in terms of generators and defining relations.

The method of generators and relations is similar to the axiomatic method in the miniature, where the role of axioms is played by the relations. Let us first consider an example and then give an exact definition.

Let us assume that we are studying an (associative) algebra A defined by three generators a, b, c and the three relations:

$$2ab - c = 0; \quad 2bc - a = 0; \quad 2ca - b = 0.$$

What is this algebra like? This is an algebra that automatically has the three given elements and also all the possible products generated by them (for example cba, a^3 etc.), usually called words. The products of words are defined in the natural way, say $ba \cdot ac = baac$ (or ba^2c in the abbreviated form). However, some of these words are linearly dependent or moreover equal. Which ones? Naturally those that are included in the defining relations, say $2ab = c$. However, the other relationships derivable from the defining relations are not excluded. For instance, if the equality $2ab = c$ is multiplied by c on the right, then we get the equality $2abc = c^2$. Substituting $2bc$ by a on the left-hand-side we obtain the equality $a^2 = c^2$. We may obtain the equality $a^2 = b^2$ analogously. Both of these equalities follow from the defining relations. Therefore, when we write $A = \langle a, b, c \,|\, 2ab = c,\ 2bc = a,\ 2ca = b \rangle$, then we keep in mind that, not only these defining relations are fulfilled in A, but also those that are their consequences. Thus this property allows the effective use of the given method for defining algebras. However the effectiveness in defining has its other side too. The fact is that in defining algebras this way, many perfectly natural questions turn out to be non-trivial and often unsolvable. For instance let us ask the reader to try to give an answer to the following question: what is the dimension of the algebra A defined above? It is difficult to say even whether A is infinite-dimensional or, on the other hand, non-zero.

It is even more difficult to answer questions about concrete elements. For example, are the elements representing the words ab and ba same or different in the algebra A? Nonetheless, in the majority of the important cases it is possible to obtain satisfactory answers to fundamental questions and we will discuss some standard methods for this later.

We return to the formal definition of an algebra A defined by the generators $x_1, x_2, \dots, x_g$ and the defining relations

$$f_1 = 0, f_2 = 0, \dots, f_r = 0.$$

(Both the generating set as well as the set of relations, generally speaking, may be infinite, but since there are no principal differences, we will use only finite variants for convenience.)

Thus, let us consider a *free algebra* $\mathfrak{A}$ with the set of generators $X = \{x_1, x_2, \dots, x_g\}$. We point out that its elements are polynomials of non-commuting variables x_i and the basis consists of the words (monomials).

In particular, all f_j are elements of this algebra. We can consider the ideal I in $\mathfrak{A}$ generated by these elements (i.e. the smallest ideal containing them). The factor algebra $\mathfrak{A}/I$ is the *algebra defined by the generators* x_i *and the relations* f_j.

Several variants are used for its notation – from the very short $A = \langle x_1, \dots, x_g \,|\, f_1, \dots, f_r \rangle$ to the most detailed $A = \langle x_1, \dots, x_g \,|\, f_1 = 0, \dots, f_r = 0 \rangle$. When the notation of the form $A = \langle x_1, \dots, x_g \,|\, u_1 = v_1, \dots, u_r = v_r \rangle$ is encountered then it should be formally understood as $A = \langle x_1, \dots, x_g \,|\, u_1 - v_1, \dots, u_r - v_r \rangle$, but in practice, the former is simply more comfortable to work with. Sometimes we will also write $A = \mathfrak{A}/(f_j, j \in J)$.

The defined algebra has the corresponding universal property: for every algebra B with the same set of generators for which the same relations are satisfied (and possibly some other ones too), there is a unique homomorphism from A to B fixing the generators.

If the set of generators is finite, then the algebra is called *finitely generated* and if, moreover, the set of the defining relations is finite, then the algebra is called *finitely presented.*

In order to define a superalgebra, it is necessary to assign parity $|x|$ to every generator x, extending it to words by setting $|fg| = |f| + |g|$ (the addition modulo 2). By the same token we define the $\mathbb{Z}_2$-graduation on the free algebra. It is then necessary to see that all words participating in one relation have the same parity. In this case parity is carried over correctly from a free algebra into the factor algebra.

Examples of defining associative algebras.

a) *Free algebra*

$$K\langle X \rangle = \mathfrak{A} = \langle x_1, \dots, x_g \rangle$$

with empty set of defining relations.

b) *Free commutative algebra (a polynomial algebra)*

$$K[X] = \langle x_1, \dots, x_g \,|\, x_i x_j = x_j x_i; i, j = 1, 2, \dots, g \rangle.$$

c) *Exterior (Grassman) algebra*

$$E = \Lambda K[X] = \langle x_1, \dots, x_g \,|\, x_i x_j = -x_j x_i; i, j = 1, 2, \dots, g \rangle.$$

d) *Free commutative superalgebra*

$$K[X] = \langle x_1, \dots, x_g \,|\, x_i x_j = (-1)^{|x_i||x_j|} x_j x_i; i, j = 1, 2, \dots, g \rangle.$$

It is assumed here that every generator x_i is assigned its parity $|x_i|$.

It is not difficult to see that this example generalizes both of the preceding ones: if all the generators are even, then we obtain the commutative algebra, if they are odd, then we get the exterior algebra.

All these examples have the property that all their defining relations are *quadratic* i.e. they are all combinations of words of length two. An algebra defined by quadratic relations will also be called *quadratic.*

Up to now, we have considered associative algebras only. The definition however carries over analogously to the other objects, for example to Lie groups and algebras. The only thing needed in the definition in this case is the notion of a free group and a free Lie algebra respectively. In addition, the role of an ideal in the group case has to be played naturally by a normal subgroup. Both free objects are constructed less trivially then a free associative algebra. We can give corresponding definitions starting from associative algebras in the following way.

Let X be the set of generators. Let us consider a free associative algebra $\mathfrak{A}$ defined by this set X. Let us consider its subset $\mathfrak{L}$, generated by the set X with respect to the commutator operation: $[xy] = xy - yx$. As pointed out above, $\mathfrak{L}$ will be a Lie algebra with respect to this operation. This is a *free Lie algebra* with the given generating set X (see also 2.8).

A *free Lie superalgebra* is defined in the same way: it is sufficient to introduce only parities of the generators and the graded commutator $[xy] = xy - (-1)^{|x||y|}yx$.

As for a free group we first give a construction of its group algebra. Let, as before, X be a generating set. Let us consider another set $Y = X \cup X^{-1}$, where together with every generator x, a new one, conveniently denoted by x^{-1} has been added. We can now consider the following algebra defined by its generators and defining relations:

$$\langle Y \mid xx^{-1} = 1, x^{-1}x = 1; x \in X\rangle.$$

This will be the group algebra of the given free group. Naturally, its basis of words is the *free group* itself. Its construction is sufficiently complex, but well studied (see Lyndon, Schupp, 1977).

Let us mention a few examples of defining Lie groups and algebras by their generators and relations.

Example. The Lie algebra L_1 is given by its generators e_i $(i = 1, 2, \ldots)$ and relations $[e_i e_j] = (i - j)e_{i+j}$. It is not difficult to check that in fact the e_i's form a basis of this algebra. Later in (8.3) we will find out about its more economical presentation.

Example. The quaternion group and the dihedral group of order 8:

$$\langle a, b \mid a^2 = b^2 = (ab)^2\rangle$$

$$\langle a, b \mid a^4 = b^2 = (ab)^2 = 1\rangle.$$

1.4. Connections Between Different Ways of Defining by Generators and Relations

1) Let $G = \langle x_1, \ldots, x_g \mid f_1 = 1, \ldots, f_r = 1\rangle$ be a group, and f_i words (made up of the letters x_j, x_j^{-1}). How to define $K[G]$? Almost in the same way:

$$K[G] = \langle x_1, \ldots, x_g, x_1^{-1}, \ldots, x_g^{-1} \mid f_1 = 1, f_2 = 1, \ldots, f_r = 1, \\ x_i x_i^{-1} = 1, x_i^{-1} x_i = 1; i = 1, \ldots, g \rangle.$$

Here, x_i^{-1} are simply new generators. Introducing them as well as introducing new relations is conditioned by the fact that in an algebra, in a difference from a group, there are no invertible elements. It is specially comfortable to define $K[G]$ when any generator x_j is the first letter of some f_k and the last letter of some f_l, where f_k and f_l do not contain x_j^{-1}. (For instance this is the case if there is a relation $x_j^n = 1$.) In this case there is no need for either a new generator or a new relation for x_j; for instance if $x_j^n = 1$, then the role of the inverse is played by x_j^{n-1}. If all the generators have this property, then the representations of G and $K[G]$ by generators and relations have visually indistinguishable representation. For instance this is the case for the dihedral group, but not for the quaternion group.

2) Let $L = \langle x_1, \ldots, x_g \mid f_1 = 0, \ldots, f_r = 0 \rangle$ be a Lie algebra. Here f_i are the elements of a free Lie algebra. Each of them is a linear combination of the *commutators* – the elements of the form $[x_{i_1} \ldots x_{i_k}]$ with an arbitrary distribution of parentheses inside. Let us assume now that A is an associative algebra with the identical set of generators and defining relations, where the commutators are thought of as in the ordinary associative sense: $[xy] = xy - yx$. Such an algebra is called the *universal enveloping algebra* of the Lie algebra L and is denoted by $U(L)$. As a rule we assume that A contains unity. For instance the universal enveloping algebra of a free Lie algebra will be a free associative algebra while the universal enveloping Lie algebra with the zero multiplication will be a free commutative algebra.

The *universal enveloping superalgebra* $U(L)$ of a Lie superalgebra L is introduced in exactly the same way; only the commutator should be taken in the graded sense as usual.

It is easy to understand that the Lie (super)algebra A_L contains L. The elements of L are called the *Lie elements*. They are commutators of the generators (of arbitrary length) and their linear combinations. They do not however exhaust A. Moreover, knowing a basis of L we can always find a basis of $A = U(L)$.

Poincaré-Birkhoff-Witt Theorem. *If $e_1, e_2, \ldots$ is a basis of L, then the basis for $U(L)$ is made up of the products of the form $e_{i_1} e_{i_2} \ldots e_{i_k}$, where $k \geqslant 0$ and $i_1 \leqslant i_2 \leqslant \ldots$, while in the super-case it is assumed in addition that all the basis elements have parity and the inequalities are strict for the indices of the odd elements.*

We will prove this theorem in 2.8.

In other words, the basis of $U(L)$ is the same as for the free commutative superalgebra (1.3) with the generators e_i.

The question of zero divisors is also resolved rather easily in $U(L)$. Following (Aubry, Lemaire, 1985), we will say that there is no torsion in L, if $[xx] \neq 0$, for every non-zero odd element and that L is absolutely torsion free if there is no torsion in the superalgebra $\overline{L}$ obtained from L by extending the ground field K to an algebraically closed one. The following theorem has been proved in (Aubry, Lemaire, 1985):

Theorem. *If L is absolutely torsion free, then $U(L)$ has no zero divisors.*

Corollary. *If L is a Lie algebra, then $U(L)$ has no zero divisors.*

Proof. There are no odd elements in L. □

We point out that, in the modern literature, the term "Lie superalgebra" is very often substituted by "graded Lie algebra" or simply by "Lie algebra".

1.5. Modules. Recall that a vector space V is called a *module* over an algebra A (or an A-module) if every element of the algebra acts as a linear operator, while the sum and the product of the elements are assigned the sum and the product of the corresponding operators. In other words, for every $a \in A$ and every $v \in V$, their product $v * a$ is defined (and called the *action* of a on v) and all the natural properties of linearity and distributivity as well as the characteristic associativity $(v * a) * b = v * (ab)$ for $a, b \in A$ are satisfied. If A is a superalgebra, then usually it is assumed that the module V is also graded: $V = V_{\overline{0}} + V_{\overline{1}}$ and $V_{\overline{i}} * A_{\overline{j}} \subseteq V_{\overline{i+j}}$ (the sum $i + j$ is modulo 2).

Defining a module over a Lie (super)algebra is done in the easiest if seen as a module over its universal enveloping algebra. This means in particular that a commutator of linear operators corresponds to a commutator: for instance, in the case of a Lie algebra, $v * [ab] = (v * a) * b - (v * b) * a$. Analogously, the G-module for a group G is a $K[G]$-module. In these cases it is customary to talk about group representations.

We emphasize that modules are assumed to be unitary, i.e. the unity acts as an identity.

The notion of a module is a natural generalization of the notion of a vector space: if we take A to be the field K, then a K-module is exactly a vector space.

The definition we stated above is the definition of a *right* A-module, since A was acting on the right. Defining a *left* module is done in exactly the same way. Sometimes, two actions are defined simultaneously on V: by an algebra A on the right and by an algebra B on the left. In this case we talk about a (B, A)-bimodule if these actions are compatible:

$$(b * v) * a = b * (v * a) \quad \text{for} \quad a \in A, b \in B, v \in V.$$

To avoid ambiguity, as a rule, we will talk in the sequel about the right modules only.

The simplest example of an A module is the algebra A itself, where the action is given simply by multiplication.

The notions of a submodule and a factor module are defined in a natural way – these are subspaces and factor spaces with the induced action: for instance if W is a submodule of V, then the action on the coset $v + W$ is defined by the following rule:

$$(v + W) * a = v * a + W.$$

The simplest example of a submodule is any right ideal. The direct sum $V_1 \oplus V_2$ (as vector spaces) of two A-modules can be furnished with a natural structure of an A-module with an action $(v_1 \oplus v_2) * a = (v_1 * a) \oplus (v_2 * a)$. This module is called the *direct sum of modules* V_1 and V_2. Understandably, the direct sums of greater number (not necessarily finite) of modules, are also defined.

The direct sum of several copies of modules isomorphic to A is called *A free A-module*. If the unity of the i-th copy is denoted by x_i, then every element of the free module is a linear combination of the elements of the form $\sum x_i a_i$ (the asterisks are omitted), where this representation is unique up to zero summands. Having the notion of a free module, we introduce naturally the notion of a *module presented by generators and their relations* $\{v_j = 0\}$, (where v_j are arbitrary elements of the free module), as the quotient over the smallest submodule containing them. The notation will be the same as in the case of algebras: $\langle \ldots, x_i, \ldots \mid \ldots, v_j = 0, \ldots \rangle$. It is easy to see that, since every module is a factor of a free module, it can be defined by generators and relations.

Example. The polynomial algebra $K[x, y]$ is a module over the free algebra $K\langle x, y\rangle$. Actions are defined by the following rules:

$$x^n y^m * x = x^{n+1} y^m$$

$$x^n y^m * y = x^n y^{m+1}$$

(we note that it is sufficient to determine the action on the generators of the algebra $K\langle x, y\rangle$, extending it to words by associativity). If we wanted to define that module via generators and relations, than one generator – call it u, would suffice (it corresponds to the unity $1 \in K[x, y]$), and the number of relations will be infinite:

$$ux^{a_1} y^{b_1} \ldots x^{a_n} y^{b_n} = ux^{a_1 + \cdots + a_n} y^{b_1 + \ldots b_n}.$$

Example. If V_1, V_2 are two modules with non-intersecting generating sets (and this can always be attained by changing notation), then, taking unions of its generating sets as well as sets of relations, we obtain a presentation of the direct sum of these modules.

If the algebra A itself is defined via generators and relations, then in order to make a vector space V into an A-module, it is necessary to introduce actions of the algebra generators, extend it with the aid of associativity and linearity to the free algebra and convince ourselves that every element corresponding to the relations acts as a zero.

Example. If $A = \langle x, y \,|\, xy = x \rangle$, then $V = \langle a, b \,|\, ay^n x = 0, by^n x^m y = by^n x^m; m > 0, n \geqslant 0 \rangle$ is an A-module, with a basis $\{ay^n, by^n x^m \,|\, n, m \geqslant 0\}$.

Singly generated module is also called *cyclic.* Obviously it is isomorphic to the factor module of the module A over a right ideal. A module with a finite number of generators is called *finitely generated.*

1.6. The Tensor Product. Recall that if V and W are two vector spaces with bases $e_1, e_2, \dots$ and $f_1, f_2, \dots$ respectively, then their tensor product $V \otimes W$ is a vector space with the basis denoted by $e_i \otimes f_j$. Here, if $v = \sum \alpha_i e_i \in V$ and $w = \sum \beta_j f_j \in W$, then the linear combination $\sum_{i,j} \alpha_i \beta_j e_i \otimes f_j$ is otherwise denoted by $v \otimes w$, thus the natural properties of linearity and distributivity of the following type are valid: $\alpha(v \otimes w) = \alpha v \otimes w = v \otimes \alpha w$; $(\alpha \in K)$; $(v_1 + v_2) \otimes w = v_1 \otimes w + v_2 \otimes w$ and the notation does not depend on the choice of a basis. Note that not every element in $V \otimes W$ is of the form $x \otimes y$.

The tensor product is often introduced differently – as a K-module with the generators $v \otimes w$ and the linearity and distributivity relations. Although this definition is more invariant, it is less obvious here that the dimension of the tensor product is equal to the product of the dimensions.

The tensor product is similar to the ordinary product with its properties, the difference is only in the fact that the result is not in the same space as the factors. We can correct this however considering, for every vector space V its *tensor algebra* $T(V) = K \oplus V \oplus (V \otimes V) \oplus (V \otimes V \otimes V) \oplus \dots$, where the product of an element of the form $v_1 \otimes v_2 \otimes \dots \otimes v_k$ by an element $u_1 \otimes u_2 \otimes \dots \otimes u_l$ is equal to $v_1 \otimes \dots \otimes v_k \otimes u_1 \otimes \dots \otimes u_l$.

It is not difficult to see that the tensor algebra is isomorphic to the free algebra where the generating set can be any basis of the space V.

If A and B are algebras, then their tensor product $A \otimes B$ may also be furnished with the structure of an algebra with the following multiplication:

$$(a \otimes b)(a' \otimes b') = aa' \otimes bb'.$$

Analogously, if A and B are superalgebras, then $A \otimes B$ is a superalgebra too: $(A \otimes B)_{\bar{0}} = A_{\bar{0}} \otimes B_{\bar{0}} \oplus A_{\bar{1}} \otimes B_{\bar{1}}$; $(A \otimes B)_{\bar{1}} = A_{\bar{0}} \otimes B_{\bar{1}} \oplus A_{\bar{1}} \otimes B_{\bar{0}}$;

$$(a \otimes b)(a' \otimes b') = (-1)^{|b||a'|}(aa' \otimes bb')$$

for the elements with parity.

The *tensor product of (super)algebras* may also be determined in a combinatorial way. If we assume that the generating sets of A and B are disjoint (which can always be attained by changing notation), then the generating set of $A \otimes B$ is the union of the generators of A and B and relations are obtained as the union of the relations of A and B with the commutativity relations $[xy] = 0$ for the generators $x \in A, y \in B$.

Example. Let $A = \langle x, y \mid xy = 0\rangle$. Then

$$A \otimes A = \langle x, y, x', y' \mid xy, x'y', [xx'], [xy'], [yx'], [yy']\rangle.$$

Dealing with modules is a little bit more tricky. In order for $V \otimes W$ to be a right A-module it is sufficient for W to be such; the action is then given by the rule $(v \otimes w) * a = v \otimes (w * a)$. In particular, $V \otimes A$ is a free A-module. Analogously, for a left module V, $V \otimes W$ will also be a left A-module. However a much more interesting situation is when V is, on the contrary, a right A-module and W – a left one. In that case the tensor product $V \otimes W$ can be considered as a K-module and factored out modulo additional relations $(v * a) \otimes w = v \otimes (a * w)$. The obtained K-module (or simply speaking – vector space) is denoted by $V \otimes_A W$ and is called the *tensor product of modules.* It is clear that $V \otimes_K W = V \otimes W$, but, in the general case, for instance $V \otimes_A W = 0$ is not ruled out, even when $V, W \neq 0$.

If we wanted $V \otimes_A W$ to be a module too, it would be necessary for either V or W to be a bimodule. For example this will always be the case when the algebra is commutative. The most important example is a *field extension.* When we want to consider an algebra A not over a ground field K, but rather over a bigger field $\overline{K}$, then the correct way consists in substituting A by $A \otimes \overline{K} = \overline{A}$. Here A is identified with the subset $a \otimes 1$ and $\dim_K A = \dim_{\overline{K}} \overline{A}$.

Somewhat later, we will need the notion of a *semitensor* product of two (super)algebras A and B. Let $x_1, \dots, x_n$ be some generators of the first algebra, $y_1, \dots, y_m$ be generators of the second and let h_{ij} $(i = 1, \dots n; j = 1, \dots m)$ be arbitrary elements of the first algebra. Then the semitensor product differs from the tensor product in that the commutators $[x_i y_j]$ are equal not to zero but to elements h_{ij} of the algebra A.

An additional requirement is that, as a vector space, the semitensor product is isomorphic to $A \otimes B$ as before, although the multiplication is defined differently. This imposes restrictions on h_{ij} that are most comfortably checked with the aid of the lemma on composition (2.5): The full system of relations should be equal to the union of the full systems of relations of A, B together with the relations $[x_i y_j] = h_{ij}$. For instance it is trivially the case if A and B are free. Another sufficient condition can be found in (Anick, 1982b).

1.7. Coalgebras. Hopf and Roos Algebras. Let us try to consider the notion of an algebra from the tensor viewpoint. It is not difficult to see that multiplication in an algebra A is nothing else but a linear transformation of two vector spaces $\nabla : A \otimes A \longrightarrow A$, defined by the rule $a \otimes b \longrightarrow ab$. How is then the associative law expressed? Precisely by commutativity of the following diagram:

$$\begin{array}{ccc} A \otimes A \otimes A & \xrightarrow{\nabla \otimes 1} & A \otimes A \\ {\scriptstyle 1 \otimes \nabla}\downarrow & & \downarrow{\scriptstyle \nabla} \\ A \otimes A & \xrightarrow{\nabla} & A \end{array}$$

i.e. by the equality $\nabla \circ (\nabla \otimes 1) = \nabla \circ (1 \otimes \nabla)$. We mention that the tensor product of two linear mappings $f_i : V_i \longrightarrow W_i$ is defined by the rule $f_1 \otimes f_2 : v_1 \otimes v_2 \longrightarrow f(v_1) \otimes f(v_2)$.

Reversing all the arrows leads us to the notion of a coalgebra. Thus, an associative *coalgebra* is a vector space A with a fixed linear mapping $\Delta : A \longrightarrow A \otimes A$, called *comultiplication* or diagonal multiplication, making the following diagram commutative:

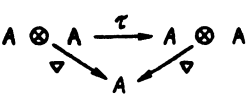
$$\begin{array}{ccc} A & \xrightarrow{\Delta} & A \otimes A \\ {\scriptstyle\Delta}\downarrow & & \downarrow{\scriptstyle\Delta\otimes 1} \\ A \otimes A & \xrightarrow{1\otimes\Delta} & A \otimes A \otimes A \end{array}$$

Since we agreed to consider only algebras with the unity, we need to deal here with a counity. How should it be introduced? One viewpoint in asserting the existence of the unity in an algebra is the existence of the inclusion $K \longrightarrow A$, compatible with multiplication (the reader will easily write down the compatibility diagrams). Analogously, counity is a map $\epsilon : A \longrightarrow K$, with the property that if $\Delta(x) = \sum x' \otimes x''$, then $\sum \epsilon(x')x'' = \sum \epsilon(x'')x' = x$. We will always consider coalgebras with counities. We point out that it is not very pleasant to use notation for comultiplication. For instance, it is not convenient to show exactly and explicitly the way the summation goes in $\sum x' \otimes x''$.

Example. Let A be a finite-dimensional algebra. Let us define a structure of a coalgebra on the *dual space* A^* (recall that it consists of all the linear transformations $A \longrightarrow K$). Let $f : A \longrightarrow K$. In order to define $\Delta(f)$, recall that $A^* \otimes A^* \cong (A \otimes A)^*$ and let $(\Delta f)(a \otimes b) = f(a)f(b)$. As for the counity, let $\epsilon(f) = f(\mathbf{1})$.

It is possible to realize an analogous construction in the case of graded algebras, using finite dimensionality of its homogeneous components (see 3.10). Conversely, if A is a coalgebra, then one introduces a structure of an algebra with multiplication on A^* defined by the following rule: if $\Delta(x) = \sum x' \otimes x''$, $f, g \in A^*$, then $(fg)(x) = \sum f(x')g(x'')$.

What corresponds to the commutativity of multiplication? If $\tau : A \otimes A \longrightarrow A \otimes A$ is a map defined by the rule $\tau(x \otimes y) = (-1)^{|x||y|} y \otimes x$, then supercommutativity denotes the commutativity of the following diagram:



i.e. $\nabla\tau = \nabla$. Reversing the arrows in the diagram, we get a definition of commutative comultiplication $\tau\Delta = \Delta$.

The most interesting case is, when both structures are present at the same time.

Definition. *Bialgebra* is a superalgebra equipped at the same time with the structure of a coalgebra, with the fulfilment of the following compatibility conditions of the two structures:

a) $\Delta(\mathbf{1}) = \mathbf{1} \otimes \mathbf{1}$ and $\epsilon(\mathbf{1}) = \mathbf{1}$.
b) The maps $\epsilon : A \longrightarrow K$ and $\Delta : A \longrightarrow A \otimes A$ are homomorphisms of superalgebras.

We emphasize that we are talking about superalgebras, in order to take into account the sign in the tensor product and in order to ensure that even elements go into even and odd into odd (specially $\epsilon(x) = 0$ for all the odd elements).

Example 1. The tensor algebra $T\langle V\rangle$ has the unique bialgebra structure, for which

$$\Delta(v) = v \otimes \mathbf{1} + \mathbf{1} \otimes v; \quad (v \in V).$$

We point out that, in a bialgebra, it is sufficient to define comultiplication on generators only, and further we know that $\Delta(ab) = \Delta(a)\Delta(b)$.

Example 2. The group algebra is a bialgebra with the comultiplication $\Delta(e_g) = e_g \otimes e_g$ (all elements are considered to be even).

Example 3. The universal enveloping algebra $U(L)$ of any Lie superalgebra L is a bialgebra with comultiplication, defined on the Lie elements $x \in L$ by the rule

$$\Delta(x) = x \otimes \mathbf{1} + \mathbf{1} \otimes x.$$

All these examples are in fact examples of Hopf algebras. The difference between *Hopf algebras* and bialgebras is in the existence, in the former, of so called antipodes (see definition in Manin, 1988). This difference is not essential for us since, in the graded case (which we will deal with) the antipodes are always present, thus we will consider the terms of bialgebra and Hopf algebra synonymous. Moreover, the latter notion will be fundamental for us since all Hopf algebras appearing in the sequel will in fact be universal enveloping algebras of some Lie superalgebra. The reader, who is prepared to take this for granted may consider these two terms synonymous and forget about comultiplication. The most important consequence of this approach for us is possibility of defining Hopf algebras by generators and relations. Specially important is the case of quadratic relations (1.3). Following Anick, quadratic Hopf algebra will be called *Roos algebra.* In other words, a Roos algebra is a free algebra, factored out by relations that are linear combinations of graded commutators $x_i x_j + x_j x_i$ of generators (and the squares x_i^2 in characteristic two).

The following two theorems will be helpful in understanding the origin of Lie superalgebras in Hopf algebras.

Theorem 1. *The set of primitive elements, i.e. elements x such that $\Delta(x) = x \otimes \mathbf{1} + \mathbf{1} \otimes x$, of a Hopf algebra is a Lie superalgebra with respect to the multiplication defined by the graded commutator.*

Proof. If x, y are primitive elements, then

$$\Delta(xy) = \Delta(x)\Delta(y) = (x \otimes \mathbf{1} + \mathbf{1} \otimes x)(y \otimes \mathbf{1} + \mathbf{1} \otimes y) = \\ = xy \otimes \mathbf{1} + \mathbf{1} \otimes xy + x \otimes y + (-1)^{|x||y|} y \otimes x,$$

which implies $\Delta([xy]) = \Delta(xy - (-1)^{|x||y|}yx) = [xy] \otimes \mathbf{1} + \mathbf{1} \otimes [xy]$. □

In the majority of applications, the cocommutative Hopf algebras arise, i.e. algebras where comultiplication (but not multiplication!) is commutative. Let us remark that if A is a graded Hopf algebra, then A^* will also be a Hopf algebra, where cocommutativity of A is equivalent to commutativity of multiplication on A^*. For the cocommutativity it is necessary and sufficient that the images of generators x be symmetric, i.e. invariant with respect to τ. From this, it follows easily that the examples considered above correspond to the cocommutative Hopf algebras. We point out that sometimes some authors speak of commutative Hopf algebras, instead of cocommutative.

Theorem 2 (Milnor, Moore, 1965). *Over a field of zero characteristic, a graded commutative Hopf algebra is the universal enveloping algebra of the Lie superalgebra of its primitive elements.*

It is assumed that the zero component of the graduation $A = \bigoplus_0^\infty A_n$ is one-dimensional, hence the group algebra does not satisfy conditions of the theorem. Over a field of characteristic greater than zero, the theorem is valid in the presence of additional restrictions (such as so called divided powers).The corresponding details and definitions may be found in (Andreé, 1971), (Avramov, 1984a), (Sjödin, 1980); we will take it for granted, that in all the situations arising in the sequel, those conditions will be fulfilled.

1.8. Elements of Homological Algebra. Throughout the following sections we will appeal to the notions and methods of homological algebra a number of times. We advise the reader to get familiar with the book (Gel'fand, Manin, 1989), written in this series, in order to get deeper understanding of contemporary homological algebra from one stand-point. In this subsection we gather necessary technical notions and theorems, that should facilitate the reader in understanding of the material and search for the corresponding references. We will allow ourselves to use the language of category theory in some cases. The reader can familiarize himself with fundamental notions of category theory also in (Gel'fand, Manin, 1989).

Let R be an arbitrary ring. Recall that a *free module* is a direct sum of a some copies of R itself, considered as a module. A free module may be represented in another way, namely as the sum of its submodules, and every such submodule is called *projective*. It is obvious that a free module is always projective, but the converse is not always true and when it is true, it is not always obvious.

A module M is called a *complex* if there is a homomorphism $d : M \longrightarrow M$, satisfying the condition $d^2 = 0$, while the module is representable in the form of the direct sum of its submodules $M = \bigoplus_{n \in \mathbf{Z}} M_n$, and the differential d satisfies the condition $d(M_n) \subseteq M_{n-1}$. Complexes are usually represented by the sequence

$$\ldots \longrightarrow M_{n+1} \xrightarrow{d_{n+1}} M_n \xrightarrow{d_n} M_{n-1} \ldots \quad (1)$$

The sequence (1) is called *exact* and the complex acyclic, if $\operatorname{Ker} d = \operatorname{Im} d$. The degree of the deviation from exactness is measured by the *homology* factor-module $H(M) = \operatorname{Ker} d / \operatorname{Im} d$, which can also be considered to be a complex, with $d = 0$. In any case, it is appropriate to single out the n-th component in this module too:

$$H_n = \operatorname{Ker} d_n / \operatorname{Im} d_{n+1}.$$

As a rule, we will be interested only in complexes for which all the components M_n are zero for negative values of n. Thus the homologies H_n will be usually considered starting with zero. We will also study the complexes, for which all the positive parts will be zero. Practically, however, it is more comfortable to do differently with those complexes, replacing every negative index $-n$ by the opposite n. In that case, in a difference from (1), all the arrows will be "reversed", and in order to distinguish these two cases, the index n will be written on top:

$$\ldots \longleftarrow M^{n+1} \xleftarrow{d_{n+1}} M^n \xleftarrow{d_n} M^{n-1} \ldots$$

(it is rather easy to remember: if the index is on top, then the differential "lifts" the number, if it is on the bottom, it lowers it). In this case we speak of *cohomologies*: $H^n(M) = \operatorname{Ker} d_n / \operatorname{Im} d_{n-1}$. In order to explicitly state the way a given complex M is going to be considered, we will write M^* and M_* respectively. Thus, H^* is the notation for cohomology.

Every module N defines a 0-complex $\tilde{N}$, for which $\tilde{N}_0 = N$, and the other components $\tilde{N}_n$ as well as the differential are zero. It is obvious that $H(\tilde{N}) = \tilde{N}$. A complex P will be called a *resolution* of the module N, if $H(P) = \tilde{N}$. Realistically this means that there is an exact sequence

$$\ldots \longrightarrow P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \longrightarrow N \longrightarrow 0. \quad (2)$$

A resolution is called *projective*, if all the P_i are projective and *free*, if they are all free.

Before giving further definitions, we make an important remark. The reader should clearly understand, that all the notions of this section have a general categorical sense, i.e. depend on what additional categorical structure the ring R has. For instance, if R is an algebra, then all the modules, after all, are vector spaces; if R is a superalgebra, then the super-structure (i.e. the existence of even and odd parts with the corresponding multiplication rules) exists in a module too. The existence of graduation on R implies graduation of all the considered modules. Even assuming the existence of differentiation on R automatically induces the assumption of the existence of differentiation on modules. In the same way, same characteristic (such as global dimension for instance) may get, generally speaking, different meanings, depending on the category the ring R belongs to. Let us describe right away all those cases which will have some meaning to us. First of all we will always deal with *augmentation* (or completed) rings R. This means that a fixed field K is given as well as the *augmentation homomorphism* of rings $\epsilon : R \longrightarrow K$, whose kernel is called the *augmentation ideal*. Such a homomorphism is required only in order to equip the field K with the structure of both left as well as right module with the natural action:

$$f * \mathbf{1} = \mathbf{1} * f = \epsilon(f).$$

Aside a perfectly trivial structure of this module, it plays an extremely valuable role in the sequel. In some sense, it carries the whole homological complexity of the algebra. The most important examples of rings are the following.

First of all, the case of a graded algebra, where the role of K is played by the ground field and the augmentation homomorphism is defined by singling out of the free term, another words, it carries every generator into zero, and the unity into unity. If $A = \bigoplus_0^\infty A_n$, then the augmentation ideal consists of the positive components: $I = \bigoplus_1^\infty A_n$, since we always assume connectivity of a graded algebra (i.e. $A_0 \cong K$ is satisfied). An important special case – a differential graded algebras, will appear starting with the eighth section, where we will talk about them in more detail.

We also remark that, if A is a Hopf algebra, then its counity defines augmentation.

The second important type of rings are local rings R, i.e. commutative rings having a unique maximal ideal $\mathfrak{M}$. The quotient $K = R/\mathfrak{M}$ is a field, and the natural homomorphism is the augmentation. The augmentation ideal will be of course $\mathfrak{M}$.

Finally, the third case we will be interested in is the case of a finite-dimensional nilpotent algebra N. In this case it is necessary to complete the algebra itself, considering $N' = K \oplus N$ instead, where the role of the augmentation homomorphism will be played by the natural projection. N itself will be the augmentation ideal.

Let now M be a right module over a ring R and P its projective resolution. If L is a left R-module, then we can form the tensor product $P \otimes_R L$, which after all looses an R-module structure, but still remains an abelian group (i.e. a $\mathbb{Z}$-module) and inherits from P a structure of a complex. The homology $\mathbb{Z}$-module $\mathrm{Tor}_*^R(M, L) = H_*(P \otimes_R L)$ is called the *torsion product* of modules M and L. This complex (abelian group) does not depend on the choice of a resolution. In case of algebras the structure of a K-module, i.e. of vector space, is preserved on Tor_*^A. We point out right away that $\mathrm{Tor}_0^R(M,L) = M \otimes L$. The meaning of Tor is as though it extends the tensor product, in rectifying the non-exactness carried by the tensor product. For us they will be valuable as purely technical means for calculating the inner invariants of the ring R as well.

First of all let us consider the augmentation $\epsilon : R \longrightarrow K$ and the torsion product $\mathrm{Tor}_*^R(K,K)$. Since K is a K-module, $\mathrm{Tor}_n^R(K,K)$ has the structure of a vector space. If these spaces are finite-dimensional, then their dimensions $b_n(R)$ are called the *Betti numbers* and the series

$$P_R(t) = \sum_0^\infty b_n(R)t^n = \sum_0^\infty \dim_K(\mathrm{Tor}_n^R(K,K))t^n$$

is called the *Poincaré series.* In the case of Noetherian local nilpotent rings, the Betti numbers and Poincaré series are determined. They carry a great amount of valuable information about R, which we will start studying beginning in section eight. Properties of the graded case will be considered in §3. Differential algebras are examined in §8. The Poincaré series may be determined for any module M in an analogous way: $P_R^M(t) = \sum_0^\infty \dim_K(\mathrm{Tor}_n^R(M,K))t^n$. Specially, $P_R = P_R^K$.

For modules, the following property is more important to us.

Definition. Call the number n the length of a resolution P of a module M, if n is maximal number satisfying $P_n \neq 0$. The minimum of lengths of all the projective resolutions of a module is called its projective dimension, denoted by $pd(M)$ and a maximum of all the projective dimensions of R-modules is called its *global dimension.*

We emphasize that, depending on the kind of modules (left or right) we are considering, the two defined values – the left and the right global dimensions $\mathrm{l.gl.dim}\, R$ and $\mathrm{r.gl.dim}\, R$ respectively, are different in general. Nevertheless, in our cases (commutative rings and graded augmentation algebras) these values will coincide. Moreover the following holds:

Theorem 1. *Let R be a graded algebra or a local ring. Then the following conditions are equivalent:*

a) $\mathrm{gl.dim}\, R \leqslant n$.
b) $\mathrm{Tor}_{n+1}^R(K,K) = 0$.

Rings with zero global dimension are exactly the classical semisimple rings (MacLane, 1963). Those are for instance the group algebras of a finite group.

$\mathrm{Tor}_*^R(M,L)$ may be computed in an analogous way using a projective resolution Q for L as well: $\mathrm{Tor}_n^R(M,L) = H_n(M \otimes_R Q)$, since a more general fact holds. Let R^{op} be the anti-isomorphic ring (i.e. the elements are the same, but the multiplication is inverted: $x \circ y = yx$). Then the following holds:

Theorem 2. $\mathrm{Tor}_*^R(M,L) \cong \mathrm{Tor}_*^{R^{op}}(L,M)$.

This theorem is especially useful for commutative rings, since, in this case $R = R^{op}$, by definition.

In parallel, it is possible to apply the same approach for the other functor too. Let M, N be right modules, P a projective resolution for M. Then the following complex of abelian groups is defined:

$$\operatorname{Hom}^*(P, N) : \ldots \longleftarrow \operatorname{Hom}_R(P_n, N) \longleftarrow \operatorname{Hom}_R(P_{n-1}, N) \longleftarrow \ldots$$

Its cohomologies $H^*(\operatorname{Hom}(P, N))$ are called *extensions* of the module M by N and are denoted by $\operatorname{Ext}_R^*(M, N)$. Of course, the result does not depend on the choice of the resolution. The meaning of the notion "extensions" is explained by their other interpretation: we may assume that the elements of $\operatorname{Ext}_R^n(M, N)$ are the exact sequences

$$0 \longrightarrow N \longrightarrow X_n \longrightarrow X_{n-1} \longrightarrow \ldots \longrightarrow X_1 \longrightarrow M \longrightarrow 0.$$

beginning with N and ending in M with suitably chosen equivalence relation of such sequences. The details and the meaning of addition of two extensions can be found in (MacLane, 1963).

We point out that in a difference from Tor, the Ext cannot be computed through the second argument, using a projective resolution for N. More precisely we need the so-called injective resolution Q (see MacLane, 1963) and

$$\operatorname{Ext}_R^*(M, N) = H^*(\operatorname{Hom}(M, Q)),$$

Important to us is also an operation of multiplication of extensions, so called the Yoneda product: If $0 \longrightarrow N \longrightarrow X_n \longrightarrow \ldots \longrightarrow X_1 \longrightarrow M \longrightarrow 0 \in \operatorname{Ext}_R^n(M, N)$; $0 \longrightarrow M \longrightarrow Y_m \longrightarrow \ldots \longrightarrow Y_1 \longrightarrow L \longrightarrow 0 \in \operatorname{Ext}_R^m(L, M)$, then $0 \longrightarrow N \longrightarrow X_n \longrightarrow \ldots \longrightarrow X_1 \longrightarrow Y_m \longrightarrow Y_{m-1} \longrightarrow \ldots \longrightarrow Y_1 \longrightarrow L \longrightarrow 0$ is an exact sequence which well defines an element of $\operatorname{Ext}_R^{m+n}(L, N)$.

In the case when $L = M = K$ we come to the conclusion that the set

$$\operatorname{Ext}_R^*(K, K)$$

is equipped with the structure of a graded algebra. In addition, if R has already been graded, then the algebra $\operatorname{Ext}_R^*(K, K)$ will have two graduations.

A purely technical methods of computing the Yoneda products may be found in (Gel'fand, Manin, 1989), (Löfwall, 1975), (MacLane, 1963).

For our main cases – local rings and graded algebras, the most essential property is the fact that in those cases, the spaces $\operatorname{Ext}_R^n(K, K)$ and $\operatorname{Tor}_n^R(K, K)$ are dual to each other, thus the Poincaré series will be the Hilbert series of the algebra $\operatorname{Ext}_R^*(K, K)$, or in other words

$$P_R(t) = \sum_0^\infty \dim(\operatorname{Ext}_R^n(K, K))t^n.$$

§2. Normal Words and a Gröbner Basis of an Ideal of a Free Algebra

2.1. Introduction. In the work with an algebra defined by generators and defining relations, we intuitively tend to work in the language of words, i.e. the elements of a free algebra. In this section we will discuss why and to what extent it is possible to do, introducing the notions of normal words and the decomposition of a free algebra into an ideal and its normal complement. Then we will introduce a rather important notion of a Gröbner basis (and its equivalent notion of complete system of relations) and we will show the way to construct a Gröbner basis for an arbitrary finitely presented algebra.

2.2. Basic Notation. Degree and Order. Let $\mathfrak{A} = K\langle X\rangle$ be a free associative algebra with the unity and S the set of all words in the alphabet X (including the empty word Λ, which will be identified with the unity $\mathbf{1}$). In order to abbreviate notation we feel comfortable with generalizing the ordinary notion of power. If $f, g \in S$, then we denote by $\deg_f g$ the number of different occurrences of the word f inside the word g. For instance, $\deg_{xx} xxx = 2$, $\deg_{xy} yx = 0$. If $F \subseteq S$ is some set of words, then we denote $\deg_F g = \sum_{f\in F} \deg_f g$. For instance $\deg_X g = |g|$ is the length of g. In order to generalize further these definitions, let us assume that the set of words S is well ordered (i.e. every two different words are comparable and we have a possibility of induction in the order $>$) and the order $>$ is preserved after multiplication:

$$f \geqslant g;\ h \geqslant k \ \Rightarrow\ fh \geqslant gk;\ hf \geqslant kg.$$

The smallest word should always be the unity.

In all the concrete examples, considered in this section, up to 2.8, the order will be as follows: the words are first ordered by their length, and, if the lengths are same, then lexicographically. We will call this order *homogeneous lexicographic*. Examples of uses of other orders can be found in the next section as well as in (Ufnarovskij, 1980). Now, with every non-zero element $u \in \mathfrak{A}$ we can associate its leading word (in the order $>$) $\hat{u}$ and we can extend $>$ to a (partial) order on $\mathfrak{A}$: $u > v \Leftrightarrow \hat{u} > \hat{v}$. Furthermore, if $U \subseteq \mathfrak{A}$, then $\hat{U} = \{\hat{u} : u \in U\}$ and if $v \in \mathfrak{A}$, then we set

$$\deg_U v = \deg_{\hat{U}} \hat{v}.$$

For example, $\deg_X v$ is the ordinary power and

$$\deg_{\{x^2-x,\,xy-yx\}} x^3y - x = 3.$$

In fact, the main example of the use of the introduced notion of power is the equality $\deg_U v = 0$, which is simply a short recording of the fact that neither of the leading words of the elements from U is a subword of the leading word of the element v.

2.3. Normal Words. Decomposition of a Free Algebra into an Ideal and Its Normal Complement. Let I be an ideal of the free algebra $\mathfrak{A}$, which will be considered fixed in this and in the next section.

Definition. A word $s \in S$ is called *normal* (modulo ideal I), if s is not the leading term of any element in I. The equivalent condition is $\deg_I s = 0$. Let us denote by N the linear hull of the set of normal words and call it the *normal complement of the ideal* I. The name is justified by the following:

Theorem. *The following direct sum decomposition of vector spaces holds:* $\mathfrak{A} = N \oplus I$.

Proof. It is obvious that $I \cap N = 0$. Consequently, it is sufficient to prove by induction on $>$ the representability of every word s in the form $\overline{s} + y$, where $\overline{s} \in N, y \in I$. If s is normal, then $\overline{s} = s$, otherwise, s is the leading word of the element $u \in I$. Let $u = \alpha s + v$. Then, by induction, v is representable in the form $\overline{v} + y$, hence $s = \alpha^{-1}(u - v) = -\alpha^{-1}\overline{v} + \alpha^{-1}(u - y)$, which is the desired representation. □

Definition. For every $u \in \mathfrak{A}$, its *normal form* $\overline{u}$ is defined to be its image by the natural projection $\mathfrak{A} \longrightarrow N$. Clearly, $\overline{u} = 0 \Leftrightarrow u \in I$.

Corollary. *We define a new operation on* N *by setting* $s * t = \overline{st}$. *Then,* N, *together with the introduced operation is isomorphic to the factor algebra* $A = \mathfrak{A}/I$.

Thus we see that, in order to work with A within the framework of the free algebra $\mathfrak{A}$, it is necessary to be able to find its normal words and know how to reduce an arbitrary word to its normal form. Unfortunately, this problem is generally speaking, algorithmically unsolvable, as even a simpler problem is unsolvable: to construct an algorithm determining whether two given words are equal in the factor algebra (or, equivalently, whether they have the same normal form). The last problem, called the *equality problem* for words is unsolvable already for the following quite concrete algebra $\langle a, b, c, d, e \,|\, ac = ca, ad = da, bc = cb, bd = db, eca = ce, edb = de, cca = ccae\rangle$ (see Tsejtin, 1958 and 7.4).

Nonetheless, we will be coming across solving such a problem, and in the majority of important cases it will be possible. One of the most effective approaches to this problem, discovered in various forms by the series of authors (see Bergman, 1978, Buchberger, 1983, Bokut', 1976, Ufnarovskij, 1980, Shirshov, 1962a) is exactly the next object of our attention.

2.4. Gröbner Basis. Complete System of Relations

Definition. A subset G of the ideal I is called a *Gröbner basis* if, for all $v \in I$, the following is satisfied:

$$\deg_G v > 0.$$

The value of Gröbner basis is shown through the following

Theorem. *A word s is normal if and only if*

$$\deg_G s = 0.$$

Proof. On one hand, $G \subseteq I$ implies $\deg_G s \leqslant \deg_I s$. On the other hand, if $\deg_v s > 0$, $v \in I$, $\deg_g v > 0$, $g \in G$, then obviously also $\deg_G s \geqslant \deg_g s > 0$. □

There are, generaly speaking, many Gröbner bases (for instance the ideal itself is one of them), however there is always a *minimal* one in the sense that no subset of it is a Gröbner basis. It is not difficult to see that the minimality condition is equivalent to the statement that, for every $v \in G$ $\deg_{G \setminus v} v = 0$ holds (i.e. none of the leading words is a subword of another). If, moreover, the stronger condition is fulfilled, namely that every element $v \in G$ has the form $f - \overline{f}$, where $f = \hat{v}$ is the leading word, then the basis is called *reduced.* The reduced basis is uniquely determined and it is easy to construct it starting with a minimal, by normalizing it (in order to make the coefficient with the leading term to be one) and reducing all the non-leading words with the aid of the basis itself into the normal form (compare the proof of the theorem from 2.3 and subsection 2.5). Thus, our immediate goal is to learn how to construct a minimal basis, and after solving that problem, we will usually always assume that all the Gröbner bases are reduced.

Working within the language of the factor algebra $A = \mathfrak{A}/I$, it is often more comfortable to speak of relations, thus we introduce one more synonym, calling a set of relations $f_i = v_i$ *complete system of relations* on A, if f_i are words, $f_i > v_i$ and $\{f_i - v_i\}$ is a Gröbner basis.

We point out that a Gröbner basis depends on the choice of generators X as well as the order relation $>$ and may cease to be such if one or the other is changed. We also point out that a Gröbner basis always generates an ideal.

2.5. Reduction. Composition. The Composition Lemma. Let us assume that the ideal I is generated by a set R. In order to get a Gröbner basis, starting with R (and consequently a complete system of relations of the factor algebra $\mathfrak{A}/I$), we need to transform R using three operations-stages.

I. *Normalization.* It is the substitution of every element by a proportional, of the form $f - w$, where f is the leading word, $f > w$. In other words, the coefficient with the leading word is made into 1. After all the elements have been normalized, we may go to the second stage.

II. *Reduction.* If u and v are normalized elements, such that $\deg_v u > 0$, then let $\hat{u} = g\hat{v}h$ be the occurrence of the leading word of v in the leading word of u. Then by reduction we mean the substitution of u by the element, obtained through normalization of the element $u - gvh$. Perhaps it looks more readable in the language of relations:

$$\left.\begin{array}{l} u = f - w \\ \\ v = k - l \end{array}\right\} \Longrightarrow \begin{array}{c} f = gkh \\ \| \quad\quad \| \\ \boxed{w \;=\; glh} \end{array}$$

We note that the reduced element is either zero (in which case we can painlessly remove it), or else, it is smaller than the element we started with. This guarantees that a series of reductions ends sooner or later. If all the reductions have been fulfilled (i.e. $\forall u \in U \deg_{U \setminus u} u = 0$), we can move on to the third stage.

A possible non-uniqueness of the results of this stage, depending on the order and the place of reductions, turns out to be unimportant, after all. An analogous remark applies to the third stage also.

III. *Compositions.* The composition of a pair u, v of normalized elements is a word f, such that $\hat{u}$ is its begining and $\hat{v}$ its ending, where the occurrences of the stated subwords intersect. In other words, $f = x \cdot y \cdot z$, where $xy = \hat{u}$, $yz = \hat{v}$, $y \neq \mathbf{1}$.

The element obtained by normalizing the element $xv - uz$ is called the *result of composition.* For clarity, a diagram in the language of relations: $u = xy - w$; $v = yz - l \Longrightarrow$

$$\begin{array}{c} xyz \\ // \backslash\backslash \\ \boxed{wz \;=\; xl} \end{array} .$$

At the third stage, the results of all compositions unaccounted for earlier should be adjoined to U (we note that even one pair can give several compositions) and return to the reduction stage.

The result of infinite number of repetitions of the second and the third stages is a minimal Gröbner basis since the following holds:

Lemma on Composition. *If the set U is such that $\forall u \in U \deg_{U \setminus u} u = 0$ (i.e. neither of the leading words of the elements $u \in U$ is a subword of another) and the result of any composition reduces to zero after a few steps, then U is a minimal Gröbner basis.*

Another name for this lemma is the diamond lemma; its proof in various forms may be found in any of the following: (Bokut', 1976), (Anick, 1986), (Bergman, 1978), (Ufnarovskij, 1980).

2.6. Examples

Example 1. $A = \langle x, y \mid x^2 + y^2 = 0 \rangle, x > y$. The unique starting element $u = x^2 + y^2$ allows for the composition with itself, defined by the word $x \cdot x \cdot x$.

The result of composition is the element $v = xu - ux = xy^2 - y^2x$ and it needs to be adjoined to u. The reduction is unnecessary, but a new composition has appeared, determined by the pair u, v and the word $x \cdot x \cdot y^2$, and it leads to the element $xv - uy^2 = -(xy^2x + y^4) = -w$. We need to apply reduction to w, with the aid of v. We need to apply reduction again to the obtained element $w - vx = y^2x^2 + y^4 = t$, but now by $u : t - y^2u = 0$. There are no more reductions and unaccounted compositions, thus our process is finished and we have obtained a Gröbner basis consisting of two elements: u and v. The basis of A is the set of normal words:

$$y^k(xy)^t; y^k(xy)^t x;\ (k, t = 0, 1, 2 \ldots).$$

In the sequel we will denote reduction by an arrow $\longrightarrow$ underlying, if necessary the occurance to which it applies. As a rule, we will perform reduction of non-leading terms as well, in order to obtain simultaneously a reduced Gröbner basis. A chain of obvious reductions will also be denoted by $\longrightarrow$. Finally, the composition f and its normalized result u will be denoted by $f : u$, braking up f by dots into three factors appearing in the definition.

Example 2. $A = \langle x\,, y \,|\, x^2 = yx \rangle$. Set $u_0 = x^2 - yx$ and compute a part of the composition:

$$x \cdot x \cdot x : xyx - yx^2 \longrightarrow xyx - y^2x = u_1.$$
$$x \cdot x \cdot yx : xy^2x - y\underline{xyx} \longrightarrow xy^2x - y^3x = u_2.$$
$$\cdots$$
$$x \cdot x \cdot y^n x : xy^{n+1}x - y\underline{xy^n x} \longrightarrow xy^{n+1}x - y^{n+2}x = u_{n+1}.$$

We prove that the set $U = \{u_n \,|\, n = 0, 1, \ldots\}$ is a Gröbner basis. Indeed, it is reduced and for every composition $xy^k \cdot x \cdot y^l x : \underline{xy^{k+l+1}x} - y^{k+1}\underline{xy^l x} \longrightarrow y^{k+l+2}x - y^{k+1}y^{l+1}x = 0$, which, according to the lemma on composition proves the desired claim. It is now easy to define normal words as well as a multiplication rule: $\{y^t, y^s xy^r\}; (y^s xy^r) * (y^t xy^l) = y^{s+r+t+1}xy^l$, and other multiplications are like ordinary words.

Example 3. The semigroup defined by the relations $\langle a, b, c \,|\, ab = c, bc = a, ca = b \rangle$ is a group isomorphic to the quaternion group.

In order to convince himself, the reader may find, by the algorithm, that there are not more than 8 normal non-empty words. Consequently, the natural homomorphism onto the quaternion group is an isomorphism.

Example 4. Let L be a Lie algebra with a basis e_i. Then its defining relations will be $[e_ie_j] = \sum_k c_{ij}^k e_k$. As we mentioned earlier (1.4), the defining relations for the universal enveloping algebra will be $e_ie_j - e_je_i = \sum_k c_{ij}^k e_k$, which we will write as $e_ie_j = e_je_i + [e_ie_j]$, regarding the last bracket as the notation for the corresponding element in L. We will prove that, for $i > j$

these elements form a complete system of relations of $U(L)$. Indeed, the compositions $e_ie_je_k$, with $i > j > k$ give:

$$e_j\underline{e_ie_k} + [e_ie_j]e_k - \underline{e_ie_k}e_j - e_i[e_je_k] \longrightarrow \underline{e_je_k}e_i + e_j[e_ie_k] + [e_ie_j]e_k - e_k\underline{e_ie_j} -$$

$$[e_ie_k]e_j - e_i[e_je_k] \longrightarrow e_ke_je_i + [e_je_k]e_i + [e_j[e_ie_k]] + [e_ie_j]e_k - e_k[e_ie_j] - e_ke_je_i -$$

$$e_i[e_je_k] = [[e_je_k]e_i] + [e_j[e_ie_k]] + [[e_ie_j]e_k] = [[e_je_k]e_i] + [[e_ke_i]e_j] + [[e_ie_j]e_k] = 0$$

According to the lemma on composition, therefore, a basis for $U(L)$ consists of the words of the form $e_1^{i_1}e_2^{i_2}\dots e_n^{i_n}$, and this is the contents of the *Poincaré-Birkhoff-Witt theorem.* An analogous proof goes also in the case of a Lie superalgebra (the definition of the latter is in 1.1). The difference in that case is in that, for the odd elements e_j, the coefficients i_j does not exceed 1 (since $[e_je_j] = 2e_j^2$), and, after all, it is assumed that all e_i have parity.

2.7. Gröbner Basis in the Commutative Case. A Gröbner basis of a commutative algebra, in the form as we have defined it above, may also be infinite (see 5.10). There is therefore sense in this case to examine all the notions considered and to introduce another basis, which we will also call a Gröbner basis. First of all, as the starting point, we will consider not a free algebra, but the algebra of polynomials $K[x_1, \dots, x_n]$. Its basis consists of the ordered set of words of the form $x_1^{a_1}\dots x_n^{a_n}$, which will be called monomials.

The set of monomials is equipped with a linear order $>$, but the conditions on it are not so rigid as in the noncommutative case: the requirements are only that the unity is the least element and that the order is preserved after multiplication: $f > g \Rightarrow fh > gh$. Well ordering is not necessary – instead the Hilbert basis theorem is used successfully (Bokut', L'vov, Kharchenko, 1988); the use of pure lexicographic order is allowed in the case when, say x is greater than every power of y.

The notion of the degree $\deg_f g$ is redundant here, and we can fully manage with the notion of divisibility. If $A = K[X]/I$, then a normal monomial is a monomial not equal to any of the leading monomials of the elements of I. Of course, $K[X] = N \oplus I$, where N is the linear hull of the set of normal monomials. A subset G of the ideal is called its Gröbner basis, if its set F of leading monomials has the property that the leading monomial of every element from the ideal is divisible at least by one word from F. In a difference from the noncommutative case, a minimal Gröbner basis is always finite. The algorithm of its construction goes along the same scheme, but with some simplifications. Normalizing, as earlier, denotes substitution of an element by a proportional one, in which the coefficient with the leading word equals one. If the leading word $\hat{u}$ of a normalized element u is divisible by the leading word $\hat{v}$ of a normalized element v: $\hat{u} = \hat{v}h$, then the reduction of u by v denotes the replacement of u by the element obtained after normalizing $u - vh$. The role of composition f of two normalized elements u and v is played by the least common multiple of the leading words. If $f = \hat{u}h$ and $f = \hat{v}g$, then the result of composition is obtained by normalizing the difference $uh - vg$. We point out that it is not necessary to consider compositions of elements with themselves as well as compositions that are products of leading words, their result, at any rate, reduces to zero.

We will not use either a Gröbner basis or the perfectly analogous lemma on composition outside of the present section. There are sufficiently many papers devoted to the commutative case – the first acquaintance is most comfortable to initiate with an article by Buchberger (Buchberger, 1983), which is the foundation of this direction. We discuss here however, one of the most important applications of Gröbner basis in commutative algebra. The fact is that nowadays, the process of Gröbner basis construction is one of the most universal ways of solving non-linear systems of polynomial equations, not only by hand, but by computers. We give concrete (and simple examples), not going too much into details.

Example. Let us consider the following system of three equations:

$$ab = c^2 + c;\ bc = a^2 + a;\ ac = b^2 + b.$$

How can we find out whether the number of its solutions over an algebraically closed field is finite or infinite? How to describe them? Let us consider the corresponding factor algebra A, defined by the given generators and relations. If a has only a finite number of possible values, then it is necessarily a root of a polynomial with the coefficients in the ground field. By the Hilbert root theorem, the corresponding degree of the polynomial is in the ideal, thus, a sufficiently large power of a is not a normal word. Analogously for b and c. In this way, the finiteness of of the number of solutions is equivalent to the finite-dimensionality of A, and this is exactly the question which we can clarify with the aid of Gröbner basis, in each of the orders. In problems of this kind, however, the pure lexicographic order is especially comfortable, because in the case of finite number of solutions an equation satisfied by the last unknown will necessarily appear. Thus, let us set $a > b > c$. Singling out the leading monomials, we get:

$$ab = c^2 + c;\ a^2 = -a + bc;\ ac = b^2 + b.$$

The first two relations determine the composition, given by the word a^2b. Its result $\underline{ac^2}+ac-(-ab+b^2c)$ reduces to $bc+\underline{ac}+\underline{ab}$, and then to $bc+b^2+b+c^2+c$, and we obtain a new relation:

$$b^2 = -bc - b - c^2 - c.$$

It is not difficult to check that all other compositions give trivial reduced results, thus the process of constructing a Gröbner basis (more precisely a complete system of relations) is finished. We see that the algebra is infinite dimensional. If we vary c as a parameter in an arbitrary fashion, we can find by it possible values of b and a.

Example. Let us change one sign in the system above:

$$ab = c^2 + c;\ a^2 = a + bc;\ ac = b^2 + b.$$

The relation obtained as the composition of the first two relations now assumes the form: $b^2 = -bc - b + c^2 + c$. The result of the composition of the second and the third element gives the following result:

$$a^2c : ac + bc^2 - \underline{ab^2} - ab \longrightarrow \underline{ac} - bc - \underline{ab} \longrightarrow \underline{b^2} + b - bc - c^2 - c \longrightarrow -2bc,$$

which, in the characteristic different from two, gives the relation $bc = 0$. Analogously, the composition of the first and the third gives: $abc : c^3 + c^2 - \underline{b^3} - b^2 \longrightarrow c^3 + c^2 + \underline{b^2c} - \underline{bc^2} - \underline{bc} \longrightarrow c^3 + c^2$, i.e. $c^3 = -c^2$. It is easy to see that the other compositions do not give non-trivial results. We have obtained the following four solutions: $(0,0,0)$; $(1,0,0)$; $(0,-1,0)$; $(0,0,-1)$. We also note that, over an algebraically closed field the absence of a solution is equivalent to the statement $A = 0$.

2.8. Regular Words. Basis of a Free Lie Algebra. In order to study the structure of Lie algebras, it is appropriate first to clarify the structure of free Lie algebras. We will be aided in this by the notions of regular associative and nonassociative words, introduced by A. I. Shirshov. Before that, it is convenient to introduce another order on the set S of associative words in an alphabet X. Let us assume that the lexicographic order $>$ is given. We note that this order, in a difference from the agreements at the begining of the section, is only a partial order: two words are incomparable, if one of them is the begining of the other. There are two possibilities for extending this order. We set $f \gg g$, if $f > g$ or if f and g are incomparable, but the length of f is less that the length of g (we emphasize, just less!). The other extension is as follows. Set $f \rhd g$, if $fg > gf$. If we also set $f \sim g$, when $fg = gf$, then it is not difficult to check that $\rhd$ is a linear order on the equivalence classes, that f and g are equivalent if and only if f and g are powers of the same word, that $f \rhd g$ if and only if $f^k > g^n$, for some $k, n > 0$ and, finally, that the order $\rhd$ is well defined (Ufnarovskij, 1985; see also 6.3).

Definition. A non-empty word is called *regular* (or special), if for every representation $f = gh$ in the form of the product of non-empty words, we have $g \rhd h$.

We note that, by definition, every generator is a regular word and that the regularity of f is equivalent to f being lexicographically greater than every word obtained from f by cyclic permutations of the letters. For example, the word $xyxz$ is regular, whereas xyx is not, since $x \rhd xy$, if $x > y > z$.

It turns out that the orders $\gg$ and $\rhd$ coincide on regular words:

Theorem 1. *If f and g are regular, then $f \gg g \Leftrightarrow f \rhd g$. In addition, the word fg is regular.*

Nevertheless, the order $\rhd$ is more suitable for the proof of the following facts.

Theorem 2. *The following conditions are equivalent:*
a) *The word f is regular.*
b) *For every proper ending h of the word f, $f > h$ holds.*
c) *For every proper ending h of the word f, $f \rhd h$ holds.*
d) *For every proper beginning g of the word f, $f \lhd g$ holds.*

Theorem 3. *Let h be maximal (with respect to length) regular word which is a proper ending of the word f; $f = gh$. Then:*
a) *For every proper ending k of the word f, either $h \sim k$, or $h \rhd k$. In particular $h \gg k$, for $k \neq h$.*
b) *The word f is regular $\Leftrightarrow g \rhd h$. In addition g is regular.*
c) *Every regular subword of f is either a subword of g, a subword of h or a beginning of f intersecting h.*
In the latter case, the word f is regular.

Theorem 4. *If the words ab and bc are regular, where b is non-empty, then abc is also a regular word.*

Proofs of these theorems may be found in 6.3.

Theorem 5. *Every word f decomposes uniquely into the product $f = f_1 f_2 \dots f_k$, where f_i are regular words and $f_1 \unlhd f_2 \unlhd f_3 \unlhd \dots \unlhd f_k$.*

Proof. If f is regular, then it is itself the desired decomposition and uniqueness follows from c) and d) of Theorem 2. Otherwise, consider g and h under the conditions of Theorem 3. By induction $g = g_1 g_2 \dots g_m$, where the condition $g_m \rhd h$ is impossible because of maximality of h and Theorem 1. This proves the existence of the decomposition. The uniqueness easily follows from c) of Theorem 3 and Theorem 2, by induction. □

We introduce now regular non-associative words by induction on the word length.

Definition. Let f be a regular associative word. Set $\tilde{f} = f$, if f is a letter (generator). Otherwise, let $f = gh$ in accordance with theorem 3. Set $\tilde{f} = [\tilde{g}\tilde{h}]$. The word $\tilde{f}$ will be called a *regular non-associative word* (corresponding to the regular associative word f).

Example. If $f = xxzxyzxy$, then

$$\tilde{f} = [[[x[xz]][x[yz]]][xy]].$$

We interpret here the brackets [ ] as the *commutators* in the free associative algebra: $[fg] = fg - gf$.

Theorem 6. *If $\tilde{f}$ is expressed through the associative words, then the leading term will be f (the word f is assumed to be regular).*

Proof. By induction. If f is a letter, then there is nothing to prove; otherwise $\tilde{f} = [\tilde{g}\tilde{h}]$. By induction, g and h are the leading terms of the elements $\tilde{g}$ and $\tilde{h}$ respectively. Consequently, the leading term of $\tilde{f}$ is either gh or hg. By the definition of a regular associative word, it will be exactly $f = gh$. □

Theorem 7 (Shirshov, 1962b). *The regular non-associative words form a basis of the free Lie algebra.*

Proof. By Theorem 6, these words are linearly independent and, by Theorem 5 and Poincaré-Birkhoff-Witt theorem, they generate (linearly) the whole of the Lie algebra. □

Remark. Using the Möbius inversion formula (Hall, 1967), it is easy to obtain a formula, from Theorem 5, expressing the number of regular words of length n in m letters (hence also the dimension of the corresponding homogeneous component of the Lie algebra $\mathfrak{L}_n$):

$$\dim \mathfrak{L}_n = \frac{1}{n} \sum_{d/n} \mu(d) m^{n/d}$$

(cf. also 5.5).

The way of practical decomposition of a concrete element is based on the following property:

Theorem 8. *Let $\tilde{g}$ and $\tilde{h}$ be regular non-associative words. Then their commutator $[\tilde{g}\tilde{h}]$ will be a regular word if and only if the following conditions are fulfilled:*

a) $g \rhd h$.

b) *If $\tilde{g} = [\tilde{a}\tilde{b}]$, then $b \unlhd h$.*

Let us assume now that either the condition a) or b) is not satisfied. How can we express the commutator $[\tilde{g}\tilde{h}]$ of two regular words through regular words? Suppose we already know how to solve this problem for the commutators of smaller lengths. Note that equivalent regular words must be equal, thus if $g \sim h$, then the commutator is simply equal to zero. In the opposite case, using anticommutativity, we can immediately assume that the condition a) is satisfied. Let us assume now that in addition, we already know how to solve the problem for all the words of this composition, with a greater (in the sense of $\rhd$) least factor of h. Then, if b) is not fulfilled, by the Jacobi identity,

$$[\widetilde{ab}, \tilde{h}] = [[\tilde{a}\tilde{h}]\tilde{b}] + [\tilde{a}[\tilde{b}\tilde{h}]],$$

and the least of the factors of each of the two summands will also be greater than h in the sense of the order $\rhd$.

Example. $[\tilde{y}\widetilde{zx^2y}] = -[[x[xy]][yz]] = -[[x[yz]][xy]] - [x[[xy][yz]]]$
$= [[xy]\widetilde{xyz}] - [x[[x[yz]]y]] - [x[x[y[yz]]]] = \widetilde{xyxyz} - \widetilde{x^2yzy} - \widetilde{x^2y^2z}.$

Understandably, this is not the unique way of choosing a basis in a free Lie algebra. Different analogues of Theorem 8 are possible. We can learn about it in more detail in (Shirshov, 1962b, Kukin, 1978). Variations on the notion of a regular words are also possible. Using some of them, A.I. Shirshov has established the following remarkable fact.

Theorem 9. *A subalgebra of a free Lie algebra is free.*

We point out that an analogous theorem is valid for groups, but not valid for associative algebras. A counter-example is already to be found in the subalgebra of $K[x]$ generated by the elements x^2 and x^3.

We will also need the following:

Theorem 10. *Let $f = ab$ be a regular word, where a is also regular. Let $b = b_1 b_2 \ldots b_k$ be a decomposition of the word b according to Theorem 5. Then, after eliminating the brackets in the commutator $[[\ldots[\tilde{a}\tilde{b}_1\tilde{b}_2]\ldots\tilde{b}_k]$, the leading associative word will be the word f.*

Proof. Note first of all that, according to Theorem 2 $a \triangleright f \triangleright b_k$, hence $a \triangleright b_i$, for every i. On the other hand, note that then the word ab_1 is also regular, by Theorem 1, thus, obviously, ab_1 is the leading term in the commutator $[\tilde{a}\tilde{b}_1]$. Then the matter is reduced to induction. □

We point out that the commutator in Theorem 10 is not necessarily a regular non-associative word, but Theorem 6 is a special case of this theorem, in case when the first letter is chosen in place of a.

2.9. A Composition Lemma for Lie Algebras. The question of construction of a complete system of relations for Lie algebras would be possible to solve in principle on the associative level, with the aid of universal enveloping algebras. It makes sense, however, to solve it, not outside the scope of the Lie algebras themselves.

Let u be an element of a free Lie algebra $\mathfrak{L}$. If we express it through a basis of regular words, we can consider among them the words of the greatest length, and among the latter consider the word $\tilde{f}$ with maximum possible word f in the lexicographic order. This associative word will be called the leading word of the element u and will be denoted by $\hat{u}$. Note that this notation, according to Theorem 6, is fully compatible with the notation introduced in 2.2, hence we may use all the other degree notation introduced there.

Definition. A set of relations $\{u = 0 \,|\, u \in U\}$ of a Lie algebra L is called its *complete system of relations*, if the regular non-associative words $\tilde{f}$ such that $\deg_U f = 0$ form a basis of the Lie algebra L.

In this case the term "Gröbner basis" is out of place as it should be more appropriate to speak of a Shirshov basis. The algorithm for computing a complete system of relations runs under the same scheme as in the associative case (2.5). The notion of normalizing is obvious – the coefficient with the leading term should be made to be one. In the sequel, an element will be considered normalized. As for the reduction and composition, we first make the following observation.

Let f be a regular associative word and a its regular subword. An easy induction with the use of Theorem 3 c) shows that in the arrangement of the brackets in $\tilde{f}$, one of them will have the following position: $\dots [ab] \dots$. Let us replace the regular word $[ab]$ in $\tilde{f}$ by the commutator, mentioned in Theorem 10 of 2.8 and let us denote the resulting element by $\langle f_a \rangle$. According to Theorem 10, from 2.8, the word f remains the leading word in the commutator $\langle f_a \rangle$, although the latter need not be regular any more. In addition, if u is a normalized element of the Lie algebra and $a = \hat{u}$ its leading word, set $\langle f_u \rangle$ to be equal to the element for which occurrence of $\tilde{a}$ in $\langle f_a \rangle$ is replaced by u.

Example. $f = x^2yz$, $u = [xy] - [yz]$, $\tilde{f} = [x[x[yz]]]$, $\langle f_{xy} \rangle = [x[[xy]z]]$, $\langle f_u \rangle = [x[[xy]z]] - [x[[yz]z]]$.

Let us now define reduction and composition.

Reduction. If $\deg_u v > 0$, i.e. the leading word $f = \hat{v}$ of the element v contains the leading word $a = \hat{u}$ as a subword, then the reduction consists in replacing v by $v - \langle f_u \rangle$ and normalizing.

Composition. If $\hat{u} = g$, $\hat{v} = f$, then the composition, as in the associative case is defined to be such an associative word $F = abc$ that $ab = g$, $bc = f$. By Theorem 4, this word is regular, thus the *result of composition* $\langle F_u \rangle - \langle F_v \rangle$, is well defined and and it is necessary only to normalize it.

Lemma on Composition *If the set of relations $\{u = 0 \mid u \in U\}$ is such that $\deg_{U \setminus u} = 0$, $\forall u \in U$ and the result of every composition of elements from U reduces to zero after a finite number of steps, then it is a complete system of relations (cf. 2.5).*

Remark. Possible non-uniqueness in the definition of $\langle f_u \rangle$ reflected in the presence of few occurrences does not play any role.

Example. $L = \langle x, y, z \mid [yz] = [[xz]y] = 0 \rangle$. Standard arrangement of brackets in the composition $xzyz$ is $[[xz][yz]]$. Consequently, the result of composition is $= [[[xz]y]z] - [[xz][yz]] = [[[xz]z]y] = \widetilde{xz^2y}$. Repeating this process, we arrive at the complete system of relations:

$$[yz] = 0; \ \widetilde{xz^ky} = 0 \quad (k \geqslant 1).$$

The difference in the supercase consists, first of all in the presence of additional regular words of the form f^2, where f is a regular word in the old sense, but is an odd element. The details as well as analysis of so called colored Lie superalgebras may be found in (Mikhalev, 1989).

2.10. The Triangle Lemma. It would be possible to continue variations on the theme of complete systems of relations further, starting with modules. A more detailed exposition of the questions arising there may be found in (Latyshev, 1988). We point out that the main problem in all the cases is the problem of shortening the sorting, since, we have seen from already considered examples that some compositions were dealt with in vain: their result reduced to zero anyway. One of the ways of computing optimization is based on the so called triangle lemma. We refer the reader to (Latyshev, 1988), for the general formulation and demonstrate here its application to the commutative and associative cases.

In the commutative case, the formulation is as follows: The composition f of two elements u and v should not be computed if it is divisible by the leading word of some third element w: its result would anyhow be reduced to the results of compositions of the pairs (u, w) and (v, w). For example, in the last example of 2.7 it would have been possible not to compute the composition of the first and the third element, since it is divisible by bc. Its result would all the same be obtained (and considerably faster) as the result of composition of the first relation with $bc = 0$.

In the associative case, the triangle lemma means that it is sufficient to calculate results of compositions for 2-chains only (see 3.6), i.e. for those compositions f for which $\deg_U f = 2$. For example, if one of the leading words is x^3, then it is not necessary to compute composition of x^5, since $\deg_{x^3} x^5 = 3 > 2$. One more optimization will be considered in 3.8.

2.11. Applications and Examples of Complete Systems of Relations

Theorem 1. *For the algebras with a finite complete system of relations the equality problem is solvable.*

Proof. Since we have an algorithm of reduction to the normal form, the question of equality of two elements reduces to the question of identity of their normal forms. □

Corollary. *For the Lie algebras with one defining relation, the problem of equality is solvable.*

Proof. A complete system of relations in this case consists of that very element, since a regular word, according to Theorem 2 in 2.8, cannot form the composition with itself. □

The analogue of this result by A.I. Shirshov for the case of Lie superalgebras as well as for the associative case remains an open problem.

Theorem 2. *Every associative algebra is embeddable into a simple one.*

Proof. In order for an algebra A to be simple, it is sufficient that every equation $xay = b$ with x, y as unknowns has a solution for every $a, b \in A$. If this is not the case for some a and b, then let X be the generating set of A and R a complete system of relations. Then, according to the lemma on composition, for the algebra $B = \langle X \cup \{x, y\} \mid R; xay = b\rangle$, the indicated set of relations is complete thus A is contained in B. We get the desired result by continuing this process of extensions, by transfinite induction. □

Developing this result further, its author, L.A. Bokut' (Bokut', 1976), has proved that a countable associative algebra may be embedded in a simple one, with two generators and has also proved the following remarkable fact:

Theorem 3 (Bokut', 1976). *Every associative algebra over a countable field may be embedded into a simple algebra which is the sum of three nilpotent subalgebras.*

Note that an algebra that is the sum of two nilpotent algebras is likewise nilpotent, as has been proved by Kegel (Kegel, 1963).

Analogous results may be obtained for Lie algebras too, with the aid of the lemma on composition. As an example, we state two theorems by L.A. Bokut'.

Theorem 4. *Let L, K_1 and K_2 be at most countable Lie algebras over a countable field K. Then L is embeddable into a simple Lie algebra, which is generated by its subalgebras K_1 and K_2.*

Corollary. *Every countable Lie algebra is embeddable into its simple Lie algebra with two generators.*

Theorem 5. *There are finitely presented Lie algebras with unsolvable equality problem.*

Proof. We give here the proof suggested by G.P. Kukin. Let $\Gamma = \langle x_1, \dots, x_n \mid A_k = B_k, k = 1, \dots, m\rangle$ be a finitely defined semigroup with unsolvable equality problem and non-empty words A_k, B_k (see e.g. 2.3). Let us consider the following Lie algebra: $L(\Gamma) = \langle a, x_1, \dots, x_n, y_1, \dots, y_n \mid [x_i y_j] = 0, [a x_i] = [a y_i], [a A_k] = [a B_k]; i, j = 1, \dots, n, k = 1, \dots, m\rangle$, where the distribution of brackets on $[aA_k]$ and $[aB_k]$ is left normalized: if $A_k = x_{i_1} \dots x_{i_t}$, then $[aA_k] = [\dots[a x_{i_1}] x_{i_2}] \dots x_{i_t}]$. Then it is possible to check (see Kukin, 1977) that for all words A and B in the alphabet $\{x_i\}$, we have $[aA] = [aB]$ in $L(\Gamma) \Leftrightarrow A = B$ in Γ. □

We state one more theorem on embedding, proved by G.P. Kukin (Kukin, 1980):

Theorem 6. *Every recursively defined Lie algebra L is embeddable into a finitely presented algebra (the field K is considered to be finitely generated over a simple subfield).*

An analogue of this theorem for groups has been proved by Higman (Higman, 1961) and for associative algebras, by V.Ya. Belyaev (Belyaev, 1978).

We finish this section by giving a few examples of complete systems of relations (the process of its computation is sufficiently elaborate).

1) *The general Clifford algebra* $C(n,m,f)$. Let $f(t_1,\dots,t_m)$ be a homogeneous polynomial of degree n in m commuting variables. The algebra $C(n,m,f)$ will be defined by m generators $e_1,e_2,\dots,e_m$ and some relations given by one formula

$$(e_1t_1+e_2t_2+\cdots+e_mt_m)^n=f(t_1,\dots,t_m),$$

which should be interpreted as follows: we eliminate parentheses on the left-hand-side, considering e_i non-commuting, but commuting with t_j. Equating the coefficients with equal monomials $t_1^{i_1}\dots t_m^{i_m}$ on both sides, we obtain the necessary relations.

Example. $f=t_1t_2$ $(e_1t_1+e_2t_2)^2=e_1^2t_1^2+(e_1e_2+e_2e_1)t_1t_2+e_2^2t_2^2=t_1t_2\Rightarrow C(2,2,f)=\langle e_1,e_2\,|\,e_1^2=0,e_1e_2+e_2e_1=1,e_2^2=0\rangle$.

It turns out (Nesterenko, 1983) that these relations form a complete system for $C(n,m,f)$.

2) *The Weyl algebra.* The complete system of relations is:

$$\begin{aligned}
[x_iy_j]&=\delta_{ij}; && 1\leqslant i,j\leqslant n;\\
[y_iy_j]&=0; && 1\leqslant i<j\leqslant n;\\
[x_ix_j]&=0; && 1\leqslant i<j\leqslant n.
\end{aligned}$$

3) *The Steenrod algebra* mod p (Anick, 1986). There are infinitely many generators and they are all of different degrees $\deg x_i=2(p-1)i$.

For $p>2$, the relations are: $y^2=0$;

$$x_mx_n=\sum_{i=0}^{[\frac{m}{p}]}(-1)^{m+i}\binom{(p-1)(n-i)-1}{m-pi}x_{m+n-i}x_i \text{ for } m<pn;$$

$$x_myx_n=\sum_{i=0}^{[\frac{m}{p}]}(-1)^{m+i}\binom{(p-1)(n-i)-1}{m-pi}yx_{m+n-i}x_i+$$

$$\sum_{i=0}^{[\frac{m-1}{p}]}(-1)^{m+i}\binom{(p-1)(n-i)-1}{m-pi-1}x_{m+n-i}yx_i \text{ for } m\leqslant pn.$$

The relations for $p=2$ are: $y^2=0$;

$$x_mx_n=y\sum_{i=0}^{[\frac{m-1}{2}]}\binom{2(n-i-1)}{2m-4i-2}x_{m+n-i-1}yx_i+\sum_{i=0}^{[\frac{m}{2}]}\binom{2(n-i)-1}{2m-4i}x_{m+n-i}x_i,$$

for $m<2n$;

$$x_m y x_n = \sum_{i=0}^{[\frac{m-1}{2}]} \binom{2(n-i)-1}{2m-4i-2} x_{m+n-i} y x_i + y \sum_{i=0}^{[\frac{m}{2}]} \binom{2(n-i)}{2m-4i} x_{m+n-i} x_i,$$

for $m \leqslant 2n$.

2.12. Comments. The term "Gröbner basis" has been introduced by Buchberger. The foundational paper connected to the commutative case is his however (Buchberger, 1983). For the associative case, the source is a paper by L.A. Bokut' (Bokut', 1976). The lemma on composition has begun to be used more frequently after Bergman has called it "the diamond lemma" in (Bergman, 1978) (proving it in a somewhat more generality). As strange as it seems, the first lemma on composition appeared in a very hard context – Lie algebras – in papers of A.I. Shirshov (Shirshov, 1962a). The earliest ideas in this direction though can apparently be considered to be the Gaussian methods of solving systems of linear equations. Terminology related to this branch is rather expressly colorful: we can come across here the notions such as "s-polynomial", "the fusion lemma", and many others. The terminology used here, after all, pursues the goal of expressing the meaning of the term through the name, and on the other hand, it corresponds to the terminology adopted in the original papers of Soviet authors.

Great attention is paid nowadays to the algorithmic questions, from the point of view of purely machine approach. The use of a Gröbner basis in symbolic algebraic computations has proven to be sufficiently effective. Many valuable references along these lines may be found in the book (Comp alg, 1982) and the papers (Kandri-Rody, Weispfenning, 1987, Mora, 1985).

The approach of A.I. Shirshov to regular words in Lie algebras was constructed based on other ideas: the brackets there were eliminated in the reverse order, begining from the inner ones. Just as other of his ideas, these deserve a separate study (cf. Shirshov, 1984).

A systematic exposition of ideas connected with the Gröbner basis may be found in (Latyshev, 1988).

§3. Graded Algebras. The Golod-Shafarevich Theorem. Anick's Resolution

3.1. Introduction. Let us assume that an algebra A is defined by *homogeneous* defining relations, in other words, let all the words included in the relations $u_i = 0$ have the same length $\deg u_i$. It is not difficult to see that in this case the elements of a reduced Gröbner basis will also be homogeneous, and that the algebra A breaks up into the direct sum of homogeneous components $A = \bigoplus_0^\infty A_n$, corresponding to the normal words of the same length, where, because of homogeneity,

$$A_i A_j \subseteq A_{i+j}. \tag{1}$$

An algebra A (not necessarily associative), decomposable into the direct sum of subspaces, satisfying condition (1) is called *graded*. If all the components of the decomposition $A = \bigoplus_0^\infty A_n$ are finite-dimensional (and we will always assume this), then we can consider the formal series $H_A = H_A(t) = \sum_0^\infty (\dim A_n)t^n$, which is called the *Hilbert series* of the algebra. This series carries a meaningful information on the character of asymptotic behaviour of the algebra A. On the other hand, it allows us to use a sufficiently effective method of the generating functions, with the aid of which we will prove an important theorem of Golod-Shafarevich on the number of relations required for attaining finite-dimensionality as well as obtain formulas for calculations of the Hilbert series. For a deeper study of the structure of graded algebras we will need a resolution constructed by Anick. With its aid we will learn how to calculate the Poincaré series, to determine the global dimension as well as increase the effectiveness of the algorithm for constructing a Gröbner basis, considered in the previous section.

Throughout this section we will be working only with the graded associative algebras with unity, assuming that the zero component is one-dimensional and is generated by the unity (this condition is usually called the *connectedness* of A). The connectedness of the graded associative algebra will be assumed in the sequel. Nevertheless, many results carry over to the case of algebras without unity, after formally adjoining it.

3.2. Graded Algebras. Let us show that, if we generalize the notion of homogeneity, then we can obtain any graded algebra with the aid of homogeneous relations. Indeed, if $A = \bigoplus_0^\infty A_n$ is a graded algebra, then after enlarging the number of generators, if necessary, we may assume that each one of them belongs to some component A_n. Define the degree $|x|$ of the corresponding *generator* as the index of the corresponding component ($|x| = n$) and the degree of a word f as the sum of degrees of its letters: $|f| = \sum_{x\in X} |x| \deg_x f$. We call an element u of a free algebra (generalized) *homogeneous* if all the words participating in its decomposition have the same degree $|u|$. We remark that the condition (1) implies that the image of a homogeneous element is fully contained in one of the components A_n, where $n = |u|$.

In light of uniqueness of decomposition into the corresponding summands in A, this means that if $u = 0$ is a relation in A, then every homogeneous summand u_n of the element u will also be a relation: $u_n = 0$. Therefore, all the defining relations may be considered homogeneous, which was the claim.

We see that the notion of homogeneity of an element depends on the definition of the degrees of the generators $|x|$. We will assume that the number of generators of the algebra A of the given degree n is finite and fixed throughout this section. Thus the notion of homogeneity is determined and the Hilbert series H_A is defined. The series $H_X = \sum_{x\in X} t^{|x|} = \sum_n d_n t^n$, where d_n is the number of generators of degree n is also determined.

The case of *natural graduation*, where the degree coincides with the length of a word and signifies the fineteness d of the number of generators ($|x| = 1, H_X = dt$), is the fundamental one and the reader may fully assume that we are discussing only that case. In any case, we will assume in all examples, unless otherwise specified, that we have a natural graduation. However in the sequel, not only the natural graduation will play fundamental role.

We point out that in the graded case it is natural to consider a different order than that in 2.2: the words are first ordered according to their degree and in the case of equality, lexicographically. In this section we adopt exactly this ordering (which, nonetheless, coincides with the former in case of natural graduation).

3.3. The Method of Generating Functions. Let V be a vector space, representable as the direct sum of finite-dimensional subspaces: $V = \bigoplus_0^\infty V_n$ (we call such a decomposition a *graduation*). The formal series

$$H_V = H_V(t) = \sum_0^\infty (\dim V_n) t^n.$$

is called the *generating function* for V.

The use of the generating functions is one of the most effective ways to fight infinity. They are a substitute for ordinary characteristics (the cardinality of a set, the dimension of a space) and behave in a nice way in many cases. The reason for this is that the homogeneity condition provides for work with separate homogeneous components independently, and therefore for application of finite-dimensional techniques. Following the principle "a generating function is a generalized dimension", it is important to ensure the *homogeneity* of the participating *mappings*, i.e. if $f : V \longrightarrow W$ is a linear transformation of spaces with graduation, then it is required that the image $f(V_n)$ is contained in W_n. Then, naturally, the spaces $\operatorname{Ker} f$ and $\operatorname{Im} f$ will be graded and, for instance, the following equality will hold:

$$H_V = H_{\operatorname{Ker} f} + H_{\operatorname{Im} f}. \tag{2}$$

Unless otherwise specified, all the mappings of the graded spaces will be assumed to be homogeneous.

The method of the generating functions assumes that in order to establish some relationship between the dimensions of the graded components, it is necessary to consider the set-theoretic operations with infinite sets as a whole and translate the derived properties into the language of the generating functions. The effect is achieved at the expense of direct computations, instead of which we obtain some equations between series, and the necessary relationships are found after solving these equations.

The second effect is based on the fact that in some neighbourhood of zero, a formal series may be convergent and equal to a quite concrete analytic function, so that studying properties of the latter (for instance its zeros and poles), we can also acquire additional information, for example by making use of differentiability and integrability. Before we go on to simple properties of the generating functions, we will agree that *comparison of series* will be *coefficient-wise* ($\sum a_n t^n \leqslant \sum b_n t^n \Leftrightarrow \forall n\; a_n \leqslant b_n$), so that it is a partial order, preserved under multiplication by a positive series (i.e. the one with non-negative coefficients) as well as that the infinite sum of formal series *makes sense* if, with every power t^n, only finitely many summands are different from zero.

If $U = \bigoplus U_n$ and $V = \bigoplus V_n$, then we introduce natural graduations on the spaces $U \oplus V$ and $U \otimes V$:

$$(U \oplus V)_n = U_n \oplus V_n; \quad (U \otimes V)_n = \sum_{i=0}^{n} (U_i \otimes V_{n-i}),$$

so that the following obviously holds:

Theorem 1. $H_{U\oplus V} = H_U + H_V; \quad H_{U\otimes V} = H_U H_V$.

A subspace V of a graded algebra A is called *homogeneous*, if $V_n = V \cap A_n$ is a graduation in V. Using the mappings $u \oplus v \to u + v$ and $u \otimes v \to uv$, we quickly obtain the following

Corollary. *If U and V are homogeneous spaces, then $H_{U+V} \leqslant H_U + H_V$; $H_{UV} \leqslant H_U H_V$.*

The inequalities become equalities if the representations (either as the sum or a linear combination of the products respectively) is unique.

Let us give two concrete examples of calculating the Hilbert series of algebras.

Theorem 2. *The Hilbert series of the polynomial algebra $K[X]$ is computed by the formula*

$$H_{K[X]} = \prod_{x \in X} (1 - t^{|x|})^{-1}.$$

The Hilbert series of the exterior algebra $\Lambda K[X]$ is calculated by the formula

$$H_{\Lambda K[X]} = \prod_{x \in X} (1 + t^{|x|}).$$

In particular, in case of natural graduation and a finite set of generators d, we have:

$$H^{-1}_{K[X]} = (1-t)^d; \quad H_{\Lambda K[X]} = (1+t)^d.$$

Proof. In the case of one generator, the Hilbert series in the power of $m = |x|$ is computed straightforwardly: it is equal to $1 + t^m + t^{2m} + \cdots = (1 - t^m)^{-1}$ in the case of the polynomial ring and $1 + t^m$ in the case of the exterior algebra. The case of finite number of generators reduces to this one, with the aid of Theorem 1 (see 1.6). Finally, in the case of infinite number of generators, the degrees of generators must increase, for if not, we do not get finite-dimensionality. Consequently, for every n, the segment of the Hilbert series up to the exponent n depends only on finite number of generators with the degree not exceeding n, thus everything reduces to the finite case. □

If M is a set of homogeneous elements, then the formal series $H_M = \sum d_n t^n$, where d_n is the number of elements in M of degree n, is called the *generating function of the set M*. We emphasize that if KM is the linear hull of the set M, then $H_{KM} \leqslant H_M$, and the equality holds if the elements are linearly independent (for instance when M consists of words). Consequently we will often use H_M instead of H_{KM}, supported by the fact that, as a rule, the previous corollary remains valid.

The series H_X introduced above is one example of a generating function of a set. Let us exhibit how to calculate the Hilbert series of an associative algebra with the aid of the method of the generating functions.

If the graduation is natural and d is the number of generators, then the series is computed straightforwardly: $H_{\mathfrak{A}} = 1 + dt + d^2t^2 + \cdots = (1 - dt)^{-1}$. In the case of an arbitrary graduation, where the degrees $|x|$ of the generators may differ from 1, the direct computation is more complicated, but the method of the generating functions allows for a quick arrival at the result. Indeed, $X\mathfrak{A} \oplus K = \mathfrak{A}$, hence, according to the Corollary,

$$H_X H_{\mathfrak{A}} + 1 = H_{\mathfrak{A}} \tag{3}$$

and consequently $H_{\mathfrak{A}} = (1 - H_X)^{-1}$.

Homogeneity of an ideal I in a free algebra is equivalent to the statement that it is generated by homogeneous elements (as an ideal) and thus the factor algebra $A = \mathfrak{A}/I$ is graded. The normal complement of the ideal (2.3) is always a homogeneous subspace, since it is generated by words and the decomposition $\mathfrak{A} = N \oplus I$ quickly implies the following equalities:

$$H_{\mathfrak{A}} = H_N + H_I, \tag{4}$$

$$H_A = H_N. \tag{5}$$

We point out that the formula (5) may be adopted as a definition of the Hilbert series of an arbitrary, not necessarily graded algebra, however such a definition would depend on the choice of the generators.

3.4. The Free Product. Exact Sequences. Let A and B be two algebras. We can always assume, even if the algebras are isomorphic, that they have non-intersecting sets of generators (after reindexing, if necessary). Under this assumption, we define their *free product* $A*B$ as the algebra whose generating set is the union of the generators of A and B, and the defining relations are the union of the defining relations of the components. An analogous definition is applicable in the case of groups too. For example, the free product of the algebra $A = \langle x \mid x^3 + 2x^2 \rangle$ by the algebra $B = \langle x, y \mid 2x^2 = y^2 \rangle$ is the algebra $A * B = \langle x, y, z \mid x^3 + 2x^2 = 0;\ 2y^2 = z^2 \rangle$. By the Lemma on composition, Gröbner basis is also the union of Gröbner bases of the components.

By the use of the method of the generating functions, we can easily prove the following

Theorem 1. *If A and B are graded algebras, then*

$$(H_{A*B})^{-1} = H_A^{-1} + H_B^{-1} - 1$$

(in the non-graded case, with the presence of the unity, this equality is still valid in the sense of formula (5)).

The notation A_n for graduation may sometimes be confused with indexing. For instance, when we want to consider a family $\{A_i\}$ of graded spaces, then i will be considered to be an index, rather than the indicator of the i-th homogeneous component. In this case, the n-th component of the corresponding space will be denoted by A_{in}. We mention also another way of combating this inconvenience, namely the indicator of the graduation is written as a superscript, enclosed in parentheses, not to confuse it with a power: $A = \bigoplus_0^\infty A^{(n)}$. In this section however, we will use only lower indices, counting on their meaning being always clear from the context.

On the other hand, in the supercase, the indices are fully in agreement: $A_{\bar{0}}$ is the sum of all even components A_n and $A_{\bar{1}}$ is the sum of the odd ones. Thus we can always (and often will) consider a graded algebra to be a superalgebra. The two different notations for $|x|$ do not cause ambiguity either: they are on equal footing in the expression $(-1)^{|x|}$.

We state one more example of manipulation with series.

Theorem 2. *Let* $\ldots A_n \xrightarrow{d_n} A_{n-1} \xrightarrow{d_{n-1}} \ldots \longrightarrow A_k \xrightarrow{d_k} K \longrightarrow 0$ *be an exact sequence of graded spaces (i.e.* $\operatorname{Ker} d_i = \operatorname{Im} d_{i+1}$*). Then* $\sum_{i=k}^\infty (-1)^i H_{A_i} = (-1)^k$*, if the sum makes sense.*

Proof. By (2),

$$H_{A_i} = H_{\operatorname{Ker} d_i} + H_{\operatorname{Im} d_i} = H_{\operatorname{Im} d_{i+1}} + H_{\operatorname{Im} d_i}.$$

Taking the alternating sum of these equalities, we see that all the summands on the right-hand-side, except $H_{\operatorname{Im} d_k} = H_K = 1$, cancel out. □

3.5. The Golod-Shafarevich Theorem. We would like to give an answer now to the following question: to what extent can we superimpose homogeneous relations of a given degree, so that the algebra remains infinite-dimensional, regardless the form of the relations. Let R be the set of non-linear defining relations, and let r_n be the number of relations of degree n. Then

$$H_R = \sum_{n=2}^{\infty} r_n t^n.$$

Let I be the (homogeneous) ideal generated by the set R and let $\mathfrak{A} = K\langle X\rangle = N \oplus I$ be the corresponding decomposition of the free algebra (2.3). Then $I = \mathfrak{A}R\mathfrak{A} = \mathfrak{A}R\mathfrak{A}X + \mathfrak{A}R$, hence

$$I \subseteq IX + NR \Longrightarrow H_I \leqslant H_I H_X + H_N H_R.$$

In view of (3–5), we get

$$H_{\mathfrak{A}} - H_A \leqslant H_{\mathfrak{A}} - 1 - H_A H_X + H_A H_R,$$

hence

$$H_A(1 - H_X + H_R) \geqslant 1. \tag{6}$$

Theorem. *If* $P(t) = (1 - H_X + H_R)^{-1} > 1$ *(i.e., all the terms of the series are non-negative), then the algebra A is infinite-dimensional.*

Proof. Using the equality $P(1 + H_R) = 1 + PH_X$, it is relatively easy to show that P cannot be a polynomial. On the other hand, (6) implies that $H_A(t) \geqslant P(t)$, thus $H_A(t)$ is not a polynomial and the algebra is infinite-dimensional. □

It is useful to write down the inequality (6) for the case of natural graduation: if d is the number of generators, then the inequality is of the form

$$H_A(t)\left(1 - dt + \sum_{2}^{\infty} r_n t^n\right) \geqslant 1.$$

In fact, this was the form the inequality was obtained in the original paper by E.S. Golod and I.R. Shafarevich (Golod, Shafarevich, 1964). In case the inequality $r_n \leqslant (d-1)^2/4$ holds for every n, it is not difficult to show that the series $P(t)$ has positive coefficients. In particular, for $d = 3$, this means that choosing not more than one relation of every degree, we ultimately obtain an infinite-dimensional algebra. Using this it is easy to construct a non-nilpotent finitely generated nil algebra (*nil algebra* is an algebra whose every element is *nilpotent*, i.e. its some power equals zero).

Let us assume that the ground field K is at most countable. Then all the elements of $\mathfrak{A}$ without the free term can be enumerated. We start raising each of these elements to a sufficiently large degree, so large that the words occurring in its decomposition would be longer than all the words occurring in the corresponding power of the preceeding elements. Then, on one hand, taking all the homogeneous components of all the constructed powers as the defining relations, we ensure the nil-conditions (in the factor algebra, every element without the free term, raised to the corresponding power will be equal to zero), and on the other hand, according to the remark made above, the algebra will be infinite-dimensional. Discarding the unity, we arrive at an infinite-dimensional and therefore not a nilpotent nil algebra. Moreover, if the characteristic of the ground field is equal to p, then the semigroup generated by the elements $(1 + x_i)$, where x_i are generators $(i = 1, 2, 3)$, turns out to be an infinite group, whose every element is of finite order, namely a power of the prime p. Indeed, every element of this semigroup is of the form $1 + u$ and since u is a nil-element, $(1 + u)^{p^k} = 1 + u^{p^k} = 1$, for a sufficiently large k. Infinity follows from the fact that the group algebra $K[G]$ contains 1 as well as all the generators $x_i = (1 + x_i) - 1$.

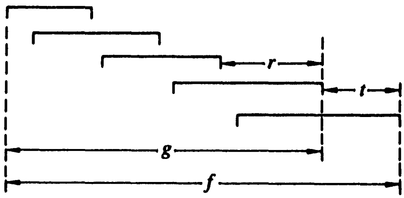
A series of more refined discussions on this theme may be found in the original paper (Golod, 1964) as well as the books (Andrunakievich, Ryabukhin, 1979) and (Herstein, 1968), but it is interesting that the other examples of infinite-dimensional finitely generated nil algebras have not been constructed, without use of the Golod-Shafarevich theorem; this apparently holds down solutions of the classical problems connected with nil rings (Köthe's problem whose one of the most tempting formulations is the following: will a nil ring of matrices over a nil ring be again a nil ring? The existence problem for a simple nil ring; the problem of existence of a finitely presented infinite-dimensional nil algebra). On the other hand, stronger results have been obtained for groups, on the existence of finitely generated groups where all their elements have order p, (Adyan, 1975), (Ol'shanskij, 1982).

3.6. Obstructions. The n-chains. The Graph of Chains. Let F be the set of the leading words of a reduced Gröbner basis and let N be the set of normal words (i.e. words s such that $\deg_F s = 0$. We point out that F determines uniquely not only N, but conversely, knowing N we can establish F as the set of all the words that themselves are not contained in N, but whose every subword is normal. We also remark that F is an *antichain* with respect to inclusion, i.e. $\deg_{F \setminus f} f = 0$, for every $f \in F$. We will call the elements of F *obstructions* and the algebra $B = \langle X \mid F \rangle$ the *associated algebra* for the source algebra A (these notions are determined in the ungraduated case too). The value of the associated algebra is in that it obviously has the same set of normal words as the source algebra, thus its Hilbert series will be the same: $H_B = H_A$. On the other hand, the algebra B is monomial, i.e. its defining relations are given by monomials ($f = 0$, where $f \in F$), which considerably facilitate its study. For example, it is obvious that the set F itself is its Gröbner basis.

Let us define the notion of an *n-chain* and its *tail*, by induction.

Naturally, (-1)-chain is the empty word $\Lambda = \mathbf{1}$, which is its own tail. Every generator $x \in X$ is declared as a 0-chain. It also coincides with its tail.

Furthermore, an n-chain is a word f of the form gt, where g is an $(n-1)$-chain and $t \in N$ is the tail of f, where, if r is the tail of g, then $\deg_F rt = 1$ and the unique occurrence of the obstruction is as the ending of the word rt. For example, 1-chains are exactly obstructions, and 2-chains are compositions (see 2.5), not all, but only those that do not contain another composition as a subword. It is convenient to represent n-chains as in the following diagram:

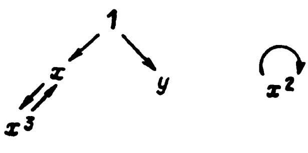


In other words, an n-chain is a word formed by linking one after another n obstructions, where only neighbouring obstructions are linked, the first $(n-1)$ form an $(n-1)$-chain and no proper begining is an n-chain. All the indicated obstructions are uniquely determined, however we point out that it is not ruled out that $\deg_F f > n$.

Example. Let $F = \{x^3\}$. The unique 1-chain is $x^3 = x \cdot x^2$ and its tail is x^2. Then the unique 2-chain is $\overline{xxxx} = x^3 \cdot x$. The word $x^3 \cdot x^2$ is not a 2-chain, since $\deg_F x^2 x^2 = 2$. The unique 3-chain is the word $x^6 = x^4 x^2$. The word $x^5 = x^4 x$ is not a 3-chain (because $\deg_F x \cdot x = 0$), regardless of the fact that it can be represented as a link of three obstructions: $\underline{\overline{xxxxx}}$ (the matter is that the first one intersects with the last). Thus, for every n there exists only one n-chain.

For a visual perception of n-chains, it is suitable to use the following *graph of chains* $C(F)$. Let us construct first a somewhat bigger oriented graph $\widetilde{C}(F)$, whose vertices are all proper endings of obstructions (including the empty word $\Lambda = \mathbf{1}$), together with the set of generators X. The edges are defined as follows: there is one edge from the empty word, to every generator $\mathbf{1} \to x$. Furthermore $f \to g$ if and only if $\deg_F fg = 1$ and the unique occurrence of the obstruction in the word fg is one of its ends. The graph $\widetilde{C}(F)$ consists of those vertices to which it is possible to arrive, starting with $\mathbf{1}$.

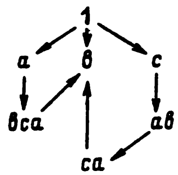
Example. Let $F = \{x^4\}$, $X = \{x, y\}$. Then the graph $\widetilde{C}(F)$ is of the following form



$C(F)$ is the component containing $\mathbf{1}$.

From the algorithmic point of view, it is most comfortable to do the construction "in stages", starting with **1** and the generators and adding the required new endings of the generators to the next stage.

Example. Let $F = \{abca, cab\}$. Then "the stages" of the graph $C(F)$ look as follows:



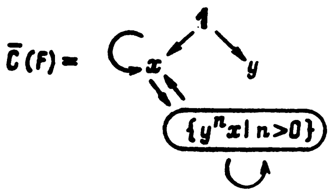
It is interesting that there are no 4-chains, although it is possible to link the 4 obstructions.

Just as well it is suitable to glue together the constructed vertices of the graph, denoting the pasted vortex as the union of the corresponding set of words. More exactly: two vertices f and g are pasted into one, if and only if for every vortex h the following hold:

$$h \to f \Longleftrightarrow h \to g; \quad f \to h \Longleftrightarrow g \to h.$$

The graph $\overline{C}(F)$ obtained after pasting is usually more compact and carries all the necessary information.

Example. Let $F = \{xy^n x \mid n = 0, 1, \dots\}$. The graph $C(F)$ is infinite. However, all the vertices $y^i x$, for $i > 0$ may be pasted into one



As a rule, we will work just with the graph $\overline{C}(F)$, while at the same time the graph $C(F)$ is valued by the fact that there is a bijective correspondence between the n-chains and the routes of length $n + 1$, starting with **1**, in the graph $C(F)$.

3.7. Calculating the Hilbert Series. Let us denote by C_n the linear hull of the set of n-chains. We point out that

$$H_{C_{-1}} = H_K = 1; \quad H_{C_0} = H_X; \quad H_{C_1} = H_F. \tag{7}$$

If t is the tail of an n-chain f and s is a normal word, then either ts is normal and $fs \in C_{n-1}N$, or ts contains an obstruction and it follows easily that

$fs \in C_{n+1}N$. Let us define a map $\delta_n : C_nN \longrightarrow C_{n-1}N$, setting $\delta_n(fs) = fs$ in the first case and $\delta_n(fs) = 0$ in the second. From the aforementioned, it is straightforward that the following sequence of vector spaces

$$\dots C_nN \xrightarrow{\delta_n} C_{n-1}N \xrightarrow{\delta_{n-1}} \dots C_{-1}N \xrightarrow{\epsilon} K \longrightarrow 0,$$

is exact (here $\epsilon(\mathbf{1}) = \mathbf{1}$, $\epsilon(f) = 0$). Consequently, by Theorem 2 of 3.3, we get the following equality:

$$\sum_{-1}^{\infty}(-1)^i H_{C_iN} = (-1).$$

Since no n-chain is a beginning of another n-chain, we may use the corollary from 3.3 to get $H_{C_iN} = H_{C_i}H_N$, thus, because of (5), we derive the following formula:

$$H_A(H_{C_{-1}} - H_{C_0} + H_{C_1} - \dots) = 1,$$

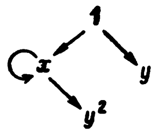
which, according to (7) may be rewritten in the form

$$H_A = (1 - H_X + H_F - H_{C_2} + H_{C_3} - \dots)^{-1}, \tag{8}$$

and it is useful to compare it with formula (6).

Example. Let $A = \langle x, y \mid x^2 + y^2 \rangle$. The obstructions for A are x^2 and xy^2, according to computations in 2.6. The graph of chains is:

$C(F) =$



therefore the n-chains are x^ny^2 and x^{n+1}, for $n > 0$. Consequently,

$$H_A^{-1} = (1 - 2t + (t^2 + t^3) - (t^3 + t^4) + \dots) = 1 - 2t + t^2.$$

Definition. We will call a set R of elements of a free algebra, *combinatorially free* or *inert* if it does not allow reduction and composition (2.5). In other words, all the leading words of the elements of R are different, they form an antichain F with respect to inclusion and no proper beginning of a word in F is an ending of a word in F. Understandably, this definition depends on the choice of the order relation $>$.

For instance, the element $xy + y^2$ forms an inert set by itself, if $x > y$ and does not in the opposite case.

Theorem 1. *Let $A = \langle X \mid R \rangle$, where R is a combinatorially free set. Then* $H_A^{-1} = 1 - H_X + H_R$.

Proof. By lemma on composition, the set R is a Gröbner basis, hence F is the set of obstructions. Since there are no 2-chains, everything reduces to (8). □

Nonetheless, the formula (8) is insufficiently convenient because of the necessity for computations of infinite set of the generating functions. Sometimes this work can be simplified. Let $\overline{C}(F)$ be the pasted graph of n-chains (3.6). We can associate to it a matrix $M = M(F)$ columns and rows of which are in the bijective correspondence with the set of vertices of the graph. If G_1 and G_2 are two vertices (recall that vertices are the unions of sets of words), we set

$$m_{G_1G_2} = \begin{cases} H_{G_2}, & \text{if } G_1 \longrightarrow G_2, \\ 0, & \text{otherwise.} \end{cases}$$

Examples. For the two graphs considered in (3.6) we have:

	$\mathbf{1}$	x	y	x^3
$\mathbf{1}$	0	t	t	0
x	0	0	0	t^3
y	0	0	0	0
x^3	0	t	0	0

	$\mathbf{1}$	x	y	$\{y^n x\}$
$\mathbf{1}$	0	t	t	0
x	0	t	0	s
y	0	0	0	0
$\{y^n x\}$	0	t	0	s

where $s = H_{\{y^n x \mid n>0\}} = t^2 + t^3 + \cdots = t^2/(1-t)$.

It turns out that it is easy to compute the Hilbert series in the case when the matrix M is algebraic over the field $K(t)$. It is not difficult to derive from (8) the following:

Theorem 2. *If $\sum_{i=0}^{k} a_i M^i = 0$, we set*

$$\begin{aligned} b_0 &= a_0 - a_1 + a_2 - \ldots \pm a_k, \\ b_1 &= \quad\; - a_1 + a_2 - \ldots \pm a_k, \\ b_2 &= \qquad\quad a_2 - \ldots \pm a_k, \\ &\;\;\ldots \\ b_k &= \qquad\qquad\quad \pm a_k. \end{aligned}$$

Then

$$b_0 H_A^{-1} = b_1 - b_2 H_X + b_3 H_F - b_4 H_{C_2} + b_5 H_{C_3} \cdots \pm b_k H_{C_{k-2}}.$$

Example. $A = \langle x, y \mid x^4 = 0\rangle$; $|x| = 1$; $|y| = 2$. Compared to calculations in the previous example, the matrix M changes only in one place. Its characteristic polynomial equals

$$\begin{vmatrix} -\lambda & t & t^2 & 0 \\ 0 & -\lambda & 0 & t^3 \\ 0 & 0 & -\lambda & 0 \\ 0 & t & 0 & -\lambda \end{vmatrix} = \lambda^4 - t^4\lambda^2.$$

Since every matrix is a root of its characteristic polynomial, we have $M^4 - t^4M^2 = 0$, hence $b_0 = b_1 = b_2 = 1 - t^4$; $b_3 = b_4 = 1$. Moreover $H_X = t + t^2$, $H_F = t^4$, $H_{C_2} = t^5$ (see the graph) and consequently,

$$(1 - t^4)H_A^{-1} = (1 - t^4) - (1 - t^4)(t + t^2) + t^4 - t^5 \Longrightarrow$$
$$H_A = \frac{1 - t^4}{1 - t - t^2 + t^6} = \frac{1 + t + t^2 + t^3}{1 - t^2 - t^3 - t^4 - t^5}.$$

We remark that it would have been easier to calculate the series by the use of Theorem 1 in 3.4.

We refer to 5.8 for other ways of calculating the Hilbert series.

3.8. Anick's Resolution. The exact sequence constructed in 3.7 has a drawback in that it does not reflect in any way the structure of the starting algebra A. Along with this fact, that sequence and the isomorphism of spaces with graduations C_nN and $C_n \otimes A$ leads us to think about the existence of a corresponding free resolution of the following form:

$$\dots C_n \otimes A \xrightarrow{d_n} C_{n-1} \otimes A \longrightarrow \dots C_{-1} \otimes A \xrightarrow{\epsilon} K \longrightarrow 0. \tag{9}$$

A resolution of this kind was constructed by Anick in (Anick, 1986), for any augmentation algebra A (1.8). We restrict ourselves here only to the graded case. We will construct the differentials d_n by induction, together with the splitting inverse mappings $i_n : \ker d_{n-1} \longrightarrow C_n \otimes A$, which, unlike d_n will not be homomorphisms of modules. Thus let us set $d_0(x \otimes \mathbf{1}) = \mathbf{1} \otimes x$; $i_{-1}(\mathbf{1}) = \mathbf{1} \otimes \mathbf{1}$; $i_0(\mathbf{1} \otimes x_{i_1} \dots x_{i_k}) = x_{i_1} \otimes x_{i_2} \dots x_{i_k}$. Exactness of the sequence (9) will follow from the following equalities:

$$d_{n+1}d_n = 0; \quad d_n i_n = \mathrm{id}\ |_{\ker d_{n-1}},$$

which are also proved by induction. We will construct the pair (d_{n+1}, i_n) in the following way: It is enough to define the differential d_{n+1} on the free generators $f \otimes \mathbf{1}$. Let $f = gt$ be an $(n+1)$-chain with the tail t. Set

$$d_{n+1}(gt \otimes \mathbf{1}) = g \otimes t - i_n d_n(g \otimes t),$$

and it remains only to define i_n for $n > 0$. To this end, let us note first that, thanks to the isomorphism from C_nN to $C_n \otimes N$, the following partial order is defined: $f \otimes t < g \otimes s \iff ft < gs$. In particular, in the definition of d_{n+1}, the first term in $g \otimes t$ will be the leading one and this can also be assumed to be satisfied by induction.

Thus, let $u \in \ker d_{n-1}$ and $f \otimes s$ be the leading term in u, participating in u together with a coefficient $\alpha \neq 0$. How does d_{n-1} act on $f \otimes s$? Let r be the tail of the $(n-1)$-chain $f = hr$. We know by induction that $d_{n-1}(f \otimes \mathbf{1}) = h \otimes r + \dots$ and that $h \otimes r$ is the leading term. $d_{n-1}(f \otimes s) = h \otimes \overline{rs} + \dots$, since d_{n-1} is a homomorphism of A-modules. The bar over rs is not placed accidentally: it denotes reduction to the normal form (cf. 2.3–2.4). If the word rs were normal, then $h \otimes rs$ would remain the leading word and the element u could not possibly belong to the kernel. Thus, rs contains an obstruction. Choosing its leftmost possible occurrence of the form $rs = abc$, where b is an obstruction, we easily see that $g = hab$ is an n-chain. Consequently $g \otimes c \in C_n \otimes A$. Let us now set $i_n(u) = \alpha g \otimes c + i_n(u - \alpha d_n(g \otimes c))$, and the matter will be done by one more induction, this time on the order $>$, since the parentheses already contain a smaller element.

Before starting analysing an example, the reader should observe that in practice, it is not necessary to construct all the mappings i_n, but rather only that needed for computing the differential d_{n+1}.

Example. $A = \langle x, y \mid x^2 = yx \rangle$. A Gröbner basis is known from (2.6); it is $\{x^n yx - y^{n+1}x \mid n \geqslant 0\}$. We have

$$\begin{gathered} d_0 : x \otimes s \longrightarrow \mathbf{1} \otimes \overline{xs}; \quad d_{-1} : \mathbf{1} \otimes s \longrightarrow \epsilon(s); \\ i_0 : \mathbf{1} \otimes x_{i_1} \dots x_{i_k} \longrightarrow x_{i_1} \otimes x_{i_2} \dots x_{i_k}; \\ d_1 : xy^n x \otimes \mathbf{1} \longrightarrow x \otimes y^n x - i_0 d_0(x \otimes y^n x) = x \otimes y^n x - i_0(\mathbf{1} \otimes \overline{xy^n x}) = \\ x \otimes y^n x - i_0(\mathbf{1} \otimes y^{n+1}x) = x \otimes y^n x - y \otimes y^n x; \\ d_2 : xy^n xy^m x \otimes \mathbf{1} \longrightarrow xy^n x \otimes y^m x - i_1 d_1(xy^n x \otimes y^m x). \end{gathered} \tag{10}$$

On the other hand

$$\begin{gathered} i_1 d_1(xy^n x \otimes y^m x) = i_1(x \otimes \overline{y^n xy^m x} - y \otimes \overline{y^n xy^m x}) = \\ xy^{n+m+1}x \otimes \mathbf{1} + i_1(x \otimes y^{n+m+1}x - y \otimes y^{n+m+1}x - d_1(xy^{n+m+1}x \otimes \mathbf{1})) = \\ xy^{n+m+1}x \otimes \mathbf{1} \\ \Rightarrow d_2 : xy^n xy^m x \otimes s \longrightarrow xy^n x \otimes \overline{y^m xs} - xy^{n+m+1}x \otimes s; \\ d_3 : xy^n xy^m xy^k x \otimes \mathbf{1} \longrightarrow xy^n xy^m x \otimes y^k x - i_2(xy^n x \otimes \overline{y^m xy^k x} - \\ xy^{n+m+1}x \otimes y^k x) = xy^n xy^m x \otimes y^k x - i_2(xy^n x \otimes y^{m+k+1}x - \\ xy^{n+m+1}x \otimes y^k x) = xy^n xy^m x \otimes y^k x - xy^n xy^{m+k+1}x \otimes \mathbf{1} - \\ i_2(xy^n x \otimes y^{m+k+1}x - xy^{n+m+1}x \otimes y^k x - d_2(xy^n xy^{m+k+1}x \otimes \mathbf{1})) = \\ xy^n xy^m x \otimes y^k x - xy^n xy^{m+k+1}x \otimes \mathbf{1} - i_2(-xy^{n+m+1}x \otimes y^k x + \\ xy^{n+m+k+1}x \otimes \mathbf{1}) = xy^n xy^m x \otimes y^k x - xy^n xy^{m+k+1}x \otimes \mathbf{1} + xy^{n+m+1}xy^k x \otimes \mathbf{1}. \end{gathered}$$

It makes sense to identify $C_n \otimes N$ with $C_n N$ and to look what the differentials look like in that language. For instance, the mapping d_{n+1}, for $f \in C_{n+1}$ looks rather simple:

$$d_{n+1}(f) = f - i_n d_n(f).$$

Furthermore, if $u \in \ker d_{n-1}$, then i_n is defined recursively:

$$i_n(u) = \alpha \hat{u} + i_n(u - \alpha d_n \hat{u}),$$

where $\hat{u}$ is the leading term and α is the coefficient with it. The resolution itself looks as follows:

$$\ldots C_nN \underset{i_n}{\overset{d_n}{\rightleftarrows}} C_{n-1}N \underset{i_{n-1}}{\overset{d_{n-1}}{\rightleftarrows}} \ldots C_0N \underset{i_0}{\overset{d_0}{\rightleftarrows}} KN \underset{i_{-1}}{\overset{\epsilon}{\rightleftarrows}} K \longrightarrow 0. \tag{11}$$

In order to construct d_{n+1} correctly in this language, it is necessary to introduce an additional mapping $R_n : C_{n+1}N \longrightarrow C_nN$, defined in the following way: if $f = gt \in C_{n+1}$, t is the tail of f, $s \in N$, then we set $R_n(fs) = g\overline{ts}$. In other words, the mapping R_n leaves fixed the n-chain placed at the beginning and reduces all others to the normal form. Consequently

$$d_{n+1}(fs) = R_n(fs - (i_nd_n(f))s).$$

In particular,

$$\begin{gathered} d_0 : f \longrightarrow \overline{f}; \quad (f \in XN); \\ i_0 : f \longrightarrow f; \quad (f \in N); \\ d_1 : f \longrightarrow f - \overline{f}; \quad (f \in C_1); \\ d_1 : fs \longrightarrow R_0(fs - \overline{f}s); \quad (f \in C_1, s \in N). \end{gathered}$$

We see that the differential d_1 calculates, by the obstruction, the whole element of Gröbner basis, whose leading term is that obstruction. On the other hand, we can observe, in the example considered above, some similarity in computing d_2 and computations of results of compositions in the Gröbner basis construction. This similarity is not accidental. In reality, computation of the differentials can substitute computation of compositions. However, let us first describe a more practical way to compute d_2. Let f be any composition (more precisely a 2-chain). Let us consider the following algorithm:

1) Let us single out all the words in $f - R_0f$ beginning with an obstruction and remember all the coefficients with these words.

2) Let us replace each of the noted obstructions by its normal form.

3) Apply R_0 to the obtained result (i.e. reduce in every word, to the normal form everything, starting with the second letter).

4) In the so obtained element we again single out all the words starting with an obstruction and again remember coefficients with all the singled out words.

5) We go back to the stage 2). Since the leading words decrease all the time, the process will sooner or later stabilize, but since we are inside the base ideal all the time, it will stabilize at zero.

It turns out (Anick, 1986) that all the words singled out during the process, together with its coefficients in fact make up the image of d_2!

This is what the process looks like in the previous example (the singled out words are underlined):

$$\begin{aligned}
&1)\quad \underline{xy^nxy^mx} - \underline{xy^{n+m+1}x};\\
&2)\quad y^{n+1}xy^mx - y^{n+m+2}x;\\
&3)\quad 0.
\end{aligned}$$

Consequently, $d_2 : xy^nxy^mx \longrightarrow xy^nxy^mx - xy^{n+m+1}x$, as was already calculated.

Let us return now to the process of constructing a reduced Gröbner basis in the graded case. Let us assume that we have already calculated all the elements of a Gröbner basis of degree n and that we want to find the elements of the $(n+1)$-st degree. Let us look at an arbitrary composition which is a 2-chain of degree $n+1$. We can apply to it the above algorithm too and it will sooner or later stabilize, not necessarily at zero though. The matter is that at the second step, if the obstruction was of length $n+1$, we would not be able to know that yet, since those obstructions would not have been constructed yet. Consequently, we would not be able to reduce it to the normal form. But in this case it means then that the given stabilized element should be added to the Gröbner basis ! In this way, calculating the differential, we obtain all the necessary elements of a Gröbner basis (although not yet in the reduced form). Reducing them to the reduced form, we get finally the possibility of calculating the differential.

Example.

$$A = \langle x, y \mid x^2 + 2y^2 \rangle.$$

The (unique) element of Gröbner basis of degree 2 is given. Let us find the elements of degree 3. The composition is unique: x^3.

$$\begin{aligned}
&1)\quad \underline{xx}x + 2xy^2;\\
&2)\quad -2y^2x + 2xy^2;\\
&3)\quad -2y^2x + 2xy^2.
\end{aligned}$$

Stabilization. Thus we add the given element, normalizing to a Gröbner basis: $xy^2 - y^2x$, the unique element of degree 3, and, incidentally $d_2 : x^3 \longrightarrow x^3 + 2xy^2$. Let us find the elements of degree 4. There is only one composition:

$$\begin{aligned}
&1)\quad \underline{x^2}y^2 - \underline{xy^2}x;\\
&2)\quad -2y^4 - y^2x^2;\\
&3)\quad -2y^4 + 2y^4 = 0.
\end{aligned}$$

Stabilizing at zero. Consequently, there are no more elements in Gröbner basis, as there are no unaccounted compositions. Moreover,

$$d^2 : x^2y^2 \longrightarrow x^2y^2 - xy^2x$$
$$(x^2y^2 \otimes \mathbf{1} \longrightarrow x^2 \otimes y^2 - xy^2 \otimes x).$$

We point out one more useful property. We can see that if we single out only obstructions in the image of $d_2(f)$, discarding the terms of the form $gs; g \in F, s \neq \mathbf{1}$, then we either obtain zero or a linear combination of obstructions one of which is the leading word of the reduced result of the compositions. The separation of this kind may be done in a more invariant way, returning to the language of tensors. Indeed, let us multiply the resolution (9), by the module K. Note that $A \otimes_A K \cong K$ (indeed if $f \notin N, f \neq 1$, then $f \otimes_A \mathbf{1} = \mathbf{1} \otimes \epsilon(f) = 0$, cf. (1.8)). Consequently $C_n \otimes A \otimes_A K \cong C_n \otimes K \cong C_n$. Thus, after multiplying, the resolution (9) gives the following sequence:

$$\dots C_n \xrightarrow{\overline{d}_n} C_{n-1} \xrightarrow{\overline{d}_{n-1}} \dots C_1 \xrightarrow{\overline{d}_1} C_0 \xrightarrow{\overline{d}_0} K \longrightarrow 0. \tag{12}$$

The mappings $\overline{d}_n$ are already ordinary linear mappings. We will establish the value of this sequence from the homological viewpoint somewhat later. Let us now establish its value from the point of view of computing a Gröbner basis. We conclude from the aforementioned that the image $\overline{d}_2(f)$ of the composition f contains the leading word of a reduced element of a Gröbner basis. Moreover, all the obstructions occuring in this image, correspond to the reductions, carried out with the aid of the obstructions of maximal degree, arising in computations of results of the composition f. Thus, it is not difficult to check that the following is true: If $\overline{d}_2(u) = 0$ and $u \in C_2$, then one of compositions occuring in the decomposition of u may not be calculated: its result would anyway reduce to zero through the results of compositions of the remaining obstructions as well as obstructions of smaller degrees.

From this viewpoint, the differential $\overline{d}_3$ is also valuable:

Theorem. *For every $c \in C_3$, one of the compositions, lying in the image $\overline{d}_3(c)$, may not be processed in the course of calculating a Gröbner basis: its result will reduce to a result of other compositions occuring in $\overline{d}_3(c)$ as well as compositions of smaller length.*

Proof. Since the condition $d^2 = 0$ translates into the condition $\overline{d}^2 = 0$, we have $u = \overline{d}_3(c) \in \ker \overline{d}_2$. □

For instance, we may not compute the result of the leading composition in $\overline{d}_3(c)$. Having some linearly independent results of $\overline{d}_3(c_i)$, the number of compositions carried out may be reduced still further.

Example. For the algebra $A = \langle x, y \mid x^2 = yx \rangle$, considered above, we know that

$$\overline{d}_3(xy^n xy^m xy^k x) = -xy^n xy^{m+k+1} x + xy^{n+m+1} xy^k x.$$

Thus the process of calculating the composition $xy^n xy^l x$, for $n > 0$, done in 2.6, turns out to be unnecessary: knowing $\overline{d}_3$, we would have been able to guarantee sooner that they would reduce to zero. This example is however not sufficiently instructive, since, in constructing d_3, we have already used the knowledge about all the obstructions, obtained exactly from the Gröbner basis.

In order to attain real economy in calculating a Gröbner basis, we need to try to replace calculations of the part of results of compositions by calculating d_3. Since the process of calculating d_2 runs parallel to calculating results of the compositions, it is possible to calculate the leading words in the image of d_3 relatively easily.

Example. Let us assume that we have only one relation of the form

$$\underline{x^2} = yz + \dots,$$

where in place of dots there are smaller words, but it is unknown exactly what. It turns out that it is sufficient to calculate all the obstructions. Indeed, we know the obstructions of degree 2 and the value of the differential d_1 for the unique such obstruction: $d_1(x^2) = x^2 - (yz + \dots)$.

Furthermore, calculating the result of applying d_2 to the unique composition xxx known now, by the process described above, we get:

$$\begin{aligned} &1) \quad \underline{x}^3 - xyz - \dots; \\ &2) \quad yzx + \dots - xyz - \dots \end{aligned}$$

The leading term xyz already does not reduce, hence it will be the leading word of the new element in the Gröbner basis, i.e. in the new obstruction and consequently, also the leading word in $d_2(x^3)$ (in fact, unique, but we will not utilize this). This means that $d_2(x^3) = x^3 - xyz + \dots$ and xyz is the unique obstruction of length 3. Before calculating obstructions with the aid of new compositions (it is unique: x^2yz), let us calculate $\overline{d}_3$ for the unique 3-chain of degree 4: $d_3(xxxx) = x^4 - i_2d_2(x^3x) = x^4 - i_2(x^2\overline{xx} - xyzx + \dots) = x^4 - x^2yz - i_2(\dots)$. We see that the leading word of $\overline{d}_3(x^4)$ will be x^2yz and consequently, by the theorem above, it is not necessary to deal with the composition, thus there are no other obstructions.

3.9. Calculating the Poincaré Series. The sequence (12) is exceptionally important from the homological viewpoint. Noting that the indexing of the n-chains in (9) differs for one from the standard indexing in the resolution (cf. formula (2) in 1.8), we see that the complex of the vector spaces in (12) is, up to the shift in indexing, exactly intended for calculating the following homology:

$$H_i(A, K) = \operatorname{Tor}_i^A(K, K) = \ker \overline{d}_{i-1} / \operatorname{Im} \overline{d}_i.$$

This way, by the use of Anick's resolution (just like with any other resolution) we can calculate homologies and the Poincaré series (see 1.8, where the necessary definitions have been collected).

For instance, we can easily clarify the meaning of the first terms in the Poincaré series. Let us consider the beginning of the sequence (12):

$$\dots C_2 \xrightarrow{\overline{d}_2} KF \xrightarrow{\overline{d}_1} KX \xrightarrow{\overline{d}_0} K \longrightarrow 0.$$

As all the differentials preserve degree, it is obvious that $\overline{d}_0 = 0$. If $x \in \operatorname{Im} \overline{d}_1$, then it means that the algebra has a homogeneous relation of the form $x = u$, i.e. x is a redundant generator. In particular $\overline{d}_1 = 0 \iff$ the number of generators is minimal. Thus $\dim H_0(A, K) = 1$ and $\dim H_1(A, K)$ is exactly the minimal number of generators. The image of $\overline{d}_2$ contains, as we saw above, all the leading words of the results of compositions, non-reducible to zero. Consequently, the dimension $\dim H_2(A, K)$ is the minimal required number of the defining relations. By use of the method of generating functions we can say more precisely that $H_{\operatorname{Tor}_2^A(K,K)}$ is the generating function of the minimal required collection of the defining relations of every degree.

Example. Let us calculate the Poincaré series of the algebra $A = \langle x, y \mid x^2 \rangle$. Its unique n-chain is the unique word x^{n+1}, for $n > 0$ and the generators are x, y, for $n = 0$. Because of $d_n : x^{n+1} \otimes \mathbf{1} \longrightarrow x^n \otimes x + i_n(x^{n-1} \otimes x^2 = 0)$, all the mappings $\overline{d}_n$ are zero and consequently,

$$\operatorname{Tor}_n^A(K, K) \cong C_{n-1} \Rightarrow P_A(t) = 1 + 2t + t^2 + t^3 + \dots$$

This situation may be naturally generalized. Recall that a *monomial* algebra is an algebra, with all the defining relations of the form $f = 0$, where f is a word. If F is the defining set of words, we may assume it to be an *antichain*, i.e. that none of them is a subword of another word. In this case, by Lemma on composition, F is the set of obstructions. Since all reductions in a monomial algebra mean the replacement of words containing obstructions by zero, it is easy to see that $\overline{d}_n = 0; (n \geqslant 0)$, hence there is the following isomorphism of vector spaces:

$$\operatorname{Tor}_n^A(K, K) \cong C_{n-1}.$$

In particular, for the Poincaré series of a monomial algebra to exist it is necessary and sufficient that both sets of generators and obstructions are finite.

We can see that here too we will turn to the method of generating functions and derive the following:

Definition. *The double Poincaré series* of a graded algebra $A = \bigoplus A_n$ is the following series in two variables:

$$P_A(s, t) = \sum_{i,n=0}^{\infty} \dim(\operatorname{Tor}_{in}^A(K, K)) s^i t^n.$$

Here n denotes the index of the graduation and the series could be written down otherwise in the form $P_A(s,t) = \sum_0^\infty H_{\operatorname{Tor}_i^A}(t) s^i$ in full compliance with the method of generating functions.

Returning to the monomial algebras, we derive the following:

Theorem 1. *If $A = \langle X \mid F \rangle$ is a monomial algebra, then*

$$P_A(s,t) = 1 + H_{C_0}(t)s + H_{C_1}(t)s^2 + H_{C_2}(t)s^3 + \dots,$$
$$\text{gl.dim}\, A \leqslant n \Longleftrightarrow C_n = 0.$$

If A is an arbitrary graded algebra, then knowing its set of obstructions F, we can construct its *associated monomial* algebra $\tilde{A}\langle X \mid F\rangle$, which inherits the same graduation on the generators. The Anick's resolution allows here to estimate from above the Poincaré series of the graded algebra (comparison of the series is coefficient-wise, as usual).

Theorem 2. $P_A(s,t) \leqslant P_{\tilde{A}}(s,t)$. *In particular, if there are finitely many obstructions as well as generators, then there exists the Poincaré series, and if the n-chains do not exist, then*

$$\text{gl.dim}\, A \leqslant n.$$

Proof. Because of $\ker \overline{d}_{i-1} \subset C_{i-1}$, we have $H_{\text{Tor}_i^A(K,K)} \leqslant H_{C_{i-1}}$ and it remains to reffer to the previous theorem and Theorem 1 from 1.8. □

Examples of another sort come from *combinatorially free sets R* of the defining relations. Recall (3.7) that combinatorial freeness of R denotes, that the set of leading words F is an antichain and that there are no linkages among the words in F. Then $C_2 = 0$ and we obtain the following result.

Theorem 3. *If the set R is combinatorially free, then*

$$\text{Tor}_3(K,K) = 0; \quad P_A(s,t) = 1 + H_X s + H_R s^2.$$

Example. $A = \langle x, y \mid xy = y^2\rangle$, $F = \{xy\}$, $P_A(s,t) = 1 + 2ts + t^2s^2$; $P_A(t) = 1 + 2t + t^2$.

Besides Anick's resolution, there are other resolutions suitable for work. A rather important is the so called *minimal resolution*. The construction is as follows: Let M be an arbitrary right A-module. Understandably, M as well as A are assumed to be graded. Thus we can choose a minimal set Y_0 of homogeneous generators in M. Let V_0 be the graded space whose basis $\{e_i\}$ is in a bijective correspondence with the set Y_0, hence $H_{V_0} = H_{Y_0}$. Let us consider the free module $P_0 = V_0 \otimes A$ and the mapping $d_0 : P_0 \longrightarrow M$ defined on the free generators $e_i \otimes \mathbf{1}$ by $d_0 : e_i \otimes \mathbf{1} \longrightarrow x_i$ and extended to a homomorphism of A-modules. Let M_1 be the kernel of the homomorphism d_0. It is also a graded module and it is possible to choose there a minimal set Y_1 of generators and to construct the corresponding free module $P_1 = V_1 \otimes A$ as well as the mapping $d_1 : P_1 \longrightarrow M_1 \subset P_0$. The mapping $d_n : P_n \longrightarrow P_{n-1}$ may be constructed in exactly the same way and consequently, the following sequence:

$$\dots V_n \otimes A \xrightarrow{d_n} V_{n-1} \otimes A \longrightarrow \dots \longrightarrow V_0 \otimes A \xrightarrow{d_0} M \longrightarrow 0 \qquad (13)$$

will be exact, by the construction. That is exactly called a minimal resolution (more exactly its terms $P_n = V_n \otimes A$). It turns out that it has an important property:

$$V_n \cong \operatorname{Tor}_n^A(M, K) \qquad (14)$$

is an isomorphism of graded spaces. Indeed, if $\sum e_i \otimes a_i \in \ker d_0$ is a homogeneous element, then, by the construction, $\sum x_i a_i = 0$ thus, by minimality of Y_0, all the coefficients of a_i are not in $A_0 = K$. Consequently, for every $u \in \operatorname{Im} d_1 = \ker d_0$, we have $u \otimes_A K = 0$, thus the mapping $\overline{d}_1 : P_1 \otimes_A K \longrightarrow P_0 \otimes_A K$ is zero. For exactly the same reason all of $\overline{d}_n : P_n \otimes_A K \longrightarrow P_{n-1} \otimes_A K$ will be zero. Then, by definition, $\operatorname{Tor}_n^A(K, K) = \ker \overline{d}_n / \operatorname{Im} \overline{d}_{n+1} = V_n \otimes K \cong V_n$.

We will use this fact for a deduction of the following remarkable formula (15):

Theorem 4. *If A is a graded algebra, then*

$$H_A^{-1}(t) = P_A(-1, t). \qquad (15)$$

Proof. Using Theorem 2 from 3.4, we get the following (in view of (13)):

$$\sum_{i=0}^{\infty} (-1)^i H_{V_i \otimes A} = 1. \quad (M = K).$$

By (14), with the aid of Theorem 1 from 3.3, we find that

$$H_A \left(\sum_{i=0}^{\infty} H_{\operatorname{Tor}_i^A(K,K)} (-1)^i \right) = 1,$$

and the desired equality follows. □

A simple application of Theorem 4 is a deduction of formula (8) from Theorem 1 and Theorem 1 (from 3.7) from Theorem 3.

We also point out the following formula, found by V.E. Govorov (Govorov, 1972, 1973a) aimed at calculating terms of the Poincaré series . Let $A = \mathfrak{A}/I$, where, as usual $\mathfrak{A}$ is the free algebra and I is a homogeneous ideal. Let us denote by T the augmentation ideal of the free algebra itself: $T = \bigoplus_1^\infty \mathfrak{A}_n$.

Theorem 5. *The following are isomorphisms of graded spaces*

$$\operatorname{Tor}_{2n-1}^A(K, K) \cong (TI^{n-1} \cap I^{n-1}T)/(TI^{n-1}T + I^n);$$
$$\operatorname{Tor}_{2n}^A(K, K) \cong (TI^{n-1}T \cap I^n)/(TI^n + I^nT),$$

where I^n are the powers of the ideal I, in particular $I^0 = \mathfrak{A}$, $I^1 = I$, $I^2 = \{\sum x_i y_j \mid x_i, y_j \in I\}$ etc.

3.10. Associated Lattices of Subspaces and Algebras with One Relation. Algebras with Quadratic Relations. We will not be interested in general questions in the lattice theory; we can familiarize ourselves with those in (Birkhoff, 1967), for example. Thus we will restrict ourselves to the following working definition, determining the class of lattices we are interested in.

Definition. Let V be an arbitrary vector space. A family L of its subspaces is called a *lattice*, if it is closed with respect to intersections and sums of finite number of its elements.

For example, if $A = V$ is an algebra, we may speak of the lattice of ideals, of the lattice of submodules etc.

Definition. A lattice is called *distributive*, if for every $X, Y, Z \in L$, $(X + Y) \cap Z = X \cap Z + Y \cap Z$ holds.

Any family of subspaces generates a lattice in an obvious way – the minimal lattice containing it. Thus, it makes sense to talk about *finitely generated* lattices.

Theorem 1. *A finitely generated lattice L is distributive if and only if we can choose a "general" basis B in the space V, i.e. such that $B \cap X$ is a basis in X, for every $X \in L$. Moreover L is finite.*

In applications to graded algebras A we will be primarily interested in the following lattice. Let, as above,

$$A = \mathfrak{A}/I, \quad \mathfrak{A} = \bigoplus_{0}^{\infty} \mathfrak{A}_n, \quad T = \bigoplus_{1}^{\infty} \mathfrak{A}_n.$$

Definition. The lattice *associated* with A is the lattice $L(A)$ generated in $\mathfrak{A}$ by the subspaces

$$T^n I^m T^k; (n, m, k \geqslant 0; T^0 = I^0 = \mathfrak{A})$$

(see the end of the previous section).

Example. Let $A\langle X \mid F\rangle$ be the monomial algebra. Then choosing in A the basis of words, we see that it will be a general basis for $L(A)$ and consequently $L(A)$ is distributive (the reverse implication to Theorem 1 is valid even without the assumption of finite generation).

The following important result has been proved by V.N. Gerasimov (Gerasimov, 1976):

Theorem 2. *Let A be defined by one homogeneous defining relation. Then $L(A)$ is distributive.*

This theorem was used by Backelin (Backelin, 1975, 1981) in obtaining a formula for explicit calculation of the Poincaré series of such an algebra and the following was proved in particular:

Corollary. *The Poincaré series $P_A(s,t)$ of an algebra with one defining relation is a rational function in s,t. In view of (15) we also obtain rationality of the Hilbert series.*

Let us show, following Dicks (Dicks, 1985), an explicit way to calculate the Hilbert and the Poincaré series. Let b be an element of the free algebra $\mathfrak{A} = K\langle X\rangle$ (at the start, not necessarily homogeneous), and let $A = \langle X \mid b\rangle$ be an algebra with the single defining relation. Let $S = \{f \in \mathfrak{A} \mid fb \in b\mathfrak{A}\}$. By definition, $b\mathfrak{A}$ is an ideal in S and we can consider the factor algebra $E = S/b\mathfrak{A}$, which will play the main role in the sequel.

Example. For every non-zero polynomial $f(x)$, if $b = f(xy)x$, then $S = K[xy] + b\mathfrak{A}$; $E \cong K[xy]/(by) \Rightarrow E \cong K[x]/(xf); (\mathfrak{A} = K\langle x,y\rangle)$.
In particular, for $b = xyx - x : E \cong K[x]/(x^2 - x) \cong K \oplus K$.

By a result of Bergman and Cohn, E is commutative, finite-dimensional algebra. Moreover, if b is homogeneous, there exists an m, such that $E \cong K[y_1, \ldots, y_m]/(y_1^n, y_iy_j; (i,j) \neq (1,1))$, for some $n \geqslant 2$ ($E = K$, if $n = 0$). We also note that in the homogeneous case, the natural mapping $E \longrightarrow A$ is an embedding. Now we can write down the necessary formulas. The Hilbert series of the algebra A is calculated by the following formula:

$$H_A^{-1} = H_{\mathfrak{A}}^{-1} + t^{|b|}H_E^{-1}.$$

Since E is commutative, its Hilbert series calculates even simpler – it is a polynomial. Moreover, if b is not necessarily homogeneous and lin (b) is the linear part of b, then it is possible to calculate the Poincaré series by the following formula:

$$P_A(t) = \begin{cases} 1 + t|X| + t^2P_E - t - t^2, & \text{if } \operatorname{lin}(b) \neq 0 \\ 1 + t|X| + t^2P_E, & \text{if } \operatorname{lin}(b) = 0. \end{cases}$$

Since, in the homogeneous case $P_E = (1 - mt)^{-1}$, we can also get explicit formulas ($d = |X| =$ the cardinality of X):

$$P_A(t) = \begin{cases} 1 - t + dt, \quad \text{here } m = 0) & \text{if } \operatorname{lin}(b) \neq 0; \\ (1 + dt - mt + t^2 - mdt^2)(1 - mt)^{-1}, & \text{if } \operatorname{lin}(b) = 0. \end{cases}$$

Finally, for the double series,

$$P_A(s,t) = \begin{cases} 1 + sH_X - st^{|b|}, & \text{if } \operatorname{lin}(b) \neq 0; \\ 1 + sH_X + s^2t^{|b|}P_E(s,t), & \text{if } \operatorname{lin}(b) = 0. \end{cases}$$

Example. $B = f(xy)x, m = 1, \mathfrak{A} = K\langle x,y\rangle, d = 2.$

$$P_A = \begin{cases} 1 + t, & \text{if } f(0) \neq 0; \\ (1 + t - t^2)(1 - t)^{-1}, & \text{if } f(0) = 0. \end{cases}$$

We state now a series of important homological properties of *quadratic algebras* (i.e. those given by the relations of second degree in the natural graduation). We will describe explicitly in this case a construction of the *dual* algebra $A^!$. Let $A = \mathfrak{A}/I$. Then $\mathfrak{A}^*$ is a graded space with $\mathfrak{A}_n^* = \mathrm{Hom}\,(\mathfrak{A}_n, K)$ and multiplication $(fg)(uv) = f(u)g(v)$, for $f \in \mathfrak{A}_n^*, g \in \mathfrak{A}_m^*, u \in \mathfrak{A}_n, v \in \mathfrak{A}_m$. It is understood that $\mathfrak{A}^*$ is a free algebra with the set of generators $x_1^*, \ldots, x_n^*$ dual to the starting generators: $x_i^*(x_j) = \delta_{ij}$. Let $I = \mathfrak{A}R\mathfrak{A}$, $R \subset \mathfrak{A}_2$, $R^* = \{f \in \mathfrak{A}_2^* \mid f(R) = 0\}$, $I^* = \mathfrak{A}^*R^*\mathfrak{A}^*$. Then $A^! = \mathfrak{A}^*/I^*$ is the *dual algebra.*

Theorem 3 (Löfwall, 1986). *If an algebra A is defined by quadratic relations, then*

A) *The algebra $A^!$ is also quadratic.*

B) $A^{!!} \cong A$.

C) *$A^!$ is isomorphic to the subalgebra* $[\mathrm{Ext}\,_A^1(K,K)]$, *generated by the subset* $\mathrm{Ext}\,_A^1(K,K)$ *of the algebra* $\mathrm{Ext}\,_A^*(K,K)$ *(cf. 1.8).*

Theorem 4 (Backelin, 1981). *Let A be a quadratic algebra. Then the following conditions are equivalent:*

A) *The lattice $L(A)$ is distributive.*

B) *For all $i, j \geqslant 0$ the following implication holds:*

$$\mathrm{Tor}\,_{ij}^A(K,K) \neq 0 \Rightarrow i = j.$$

C) *The Fröberg formula holds:*

$$P_A(s,t)H_A(-st) = 1.$$

A^*), B^*), C^*) are analogous formulations for the algebra $A^!$.

D) $\mathrm{Ext}\,_A(K,K) = [\mathrm{Ext}\,_A^1(K,K)]$. *This property allows for A to be called a homogeneous Koszul algebra.*

As a corollary, we obtain the following formula: if A is a quadratic and $L(R)$ is distributive, then

$$H_A(t)H_{A^!}(-t) = 1.$$

Indeed, in view of the latter parts of Theorems 3 and 4, we have $H_{A^!} = H_{\mathrm{Ext}\,_A^*}(K,K)$. On the other hand, by definition, $P_A = H_{\mathrm{Ext}\,_A^*}(K,K)$. It remains to establish a passage from the double Poincaré series to the ordinary $P_A(t) = P_A(t,1)$ and put $t = 1, s = -t$ in Fröberg's formula.

We finalize this section by a full classification of all algebras, given by two quadratic relations. We may assume the field K to be algebraically closed. Let us fix the following notation (not coinciding with that introduced at the beginning of the section). Let n be the number of generators, and let m be a minimal amount of generators (may be different) required for describing the relations. More formally, if R is the set of relations (consisting of two elements), then let E be a minimal subspace such that $R \subset E^2$. Then m

is the dimension of the space E. Furthermore $K_i = \mathfrak{A}_i$ for $i = 0, 1$ and $K_i = \mathfrak{A}_1 K_{i-1} \cap I_2 \mathfrak{A}_{i-2}$, for $i \geqslant 2$ are subspaces in the free algebra $\mathfrak{A}$, $A = \mathfrak{A}/I$, $K_i \subseteq \mathfrak{A}_i$. Finally, set $r = \dim K_3, d = \dim K_4$. The case of one relation (i.e. two linearly dependent relations) is sufficiently simple.

Theorem 5. *If an algebra A is defined by one quadratic relation, then $L(A)$ is distributive, $1 \geqslant r = d = \dim K_j \geqslant 0$, for $j \geqslant 4$ and*

$$P_A(s,t) = 1 + nst + s^2t^2 + \frac{rs^3t^3}{1 - st}.$$

Moreover, $r = 1$ if and only if $m = 1$.

For two relations, the situation is more complex:

Theorem 6. *If A is defined by two quadratic relations, then the ordered pair (r, d) may assume only the following four values: $(0,0), (1,0), (1,1), (2,2)$ and $d = \dim K_j$, for $j \geqslant 4$. If $L(A)$ is distributive, then*

$$P_A(s,t) = 1 + nst + 2s^2t^2 + rs^3t^3 + d\frac{s^4t^4}{1 - st},$$

and one of the following four alternatives holds: $(r, d) =$

a) $(0,0) \iff$ gl.dim $A = 2$ *and* $m \geqslant 3$;

b) $(1,0) \iff A \cong K\langle x_1, \ldots, x_n \mid x_1x_2, x_2x_3\rangle$ *(and this implies $m = 3$);*

c) $(1,1) \iff m \geqslant 3$ *and* $\exists y \in \mathfrak{A}_1$, *thus* $0 \neq y^2 \in I_2$, *but A is not isomorphic to the algebra $K\langle x_1, \ldots, x_n \mid x_1^2, x_1x_2 + x_3x_1\rangle$.*

d) $(2,2) \iff m = r = d = 2$.

If $L(A)$ is not distributive, then A is isomorphic to one of the following 10 algebras sorted out in the following table:

№	Relations	r	d	$P(s,t)$
a	$xy,\ yx + z^2$	0	0	$1 + nst + \dfrac{2s^2t^2 + 2s^3t^5 + 3s^4t^6}{1 - s^3t^5}$
b c d	$xy,\ x^2 + yz + zx$ $xy,\ yz + zy$ $xy,\ yz + tx$	0	0	$1 + nst + \dfrac{2s^2t^2 - s^3t^4}{1 - st^2}$
e f	$xy,\ x^2 + yz$ $xy,\ y^2 + zx$	0	0	$1 + nst + \dfrac{2s^2t^2 + 2s^3t^4}{1 - s^2t^3}$
g	$xy,\ x^2 + \alpha yx + y^2$; $(\alpha^2 \neq 1)$	0	0	$1 + nst + \dfrac{2s^2t^2 + 4s^3t^4 + 8s^4t^5}{1 - 4s^3t^4}$
h	$x^2,\ y(x + y)$	1	1	$1 + nst + \dfrac{2s^2t^2 - s^3t^3 + s^3t^4 - 2s^4t^5}{1 - st - s^2t^3 + s^3t^4}$
i	$x^2,\ xy + zx$	1	1	$1 + nst + \dfrac{2s^2t^2 - 2s^2t^3 - s^3t^3}{1 - st - t}$
j	$xy,\ y(x + y)$	1	0	$1 + nst + \dfrac{2s^2t^2 + s^3t^3 + s^3t^4 + 3s^4t^5 + 2s^5t^6}{1 - s^3t^4 - s^4t^5}$

All the algebras are automatons (5.10).

Setting $s = -1$, we can find the corresponding Hilbert series.

3.11. Comments. The term "Hilbert series" draws its source from classical results of Hilbert, related to the commutative case. Sometimes it was also called the Poincaré series, but nowadays it has been agreed to use exactly that term, connecting the name of Poincaré only with homological series. Besides, as was noted above, the Poincaré series is the Hilbert series of the algebra $\mathrm{Ext}_A^*(K, K)$ with the Yoneda multiplication.

The notions of obstruction and an n-chain have been introduced by Anick, although his definitions differ somewhat from those stated here; in (Anick, 1986) they have been introduced through so called prechains. A graphical interpretation of chains was introduced in (Ufnarovskij, 1989a). The remark, representing the content of the theorem in 3.8, has been made by the author as well as the translation of the resolution into the language of normal words. All the points with contents in this section belong to Anick. Construction of the Anick resolutions for path algebras may be found in (Anick, Green, 1987).

The content of section 3.10 has been basically taken from Backelin's paper (Backelin, 1981). The classification of algebras defined by two quadratic relations was done in (Ufnarovskij, 1984), however only the Hilbert series were discussed there, hence Theorem 6 contains considerably more valuable information.

The reader is also recommended to use a paper by E.S. Golod (Golod, 1988), where he will familiarize himself with a homological interpretation of the lemma on composition as well as with the so called Shafarevich complex.

Let us point out a sharp notation: if A is an algebra, then $A(t)$ is its Hilbert series.

§4. Generic Algebras. Diophantine Equations

4.1. Introduction. In order to introduce the objects we will be interested in, in this section, we will give, as an example, a classification of all the algebras of Hilbert series, defined by one relation of the third degree (Ufnarovskij, 1980). It turns out that either

$$H_A = (1 - H_X + t^3)^{-1},$$

or A is isomorphic to one of the following monomial algebras:

$$\langle x_1, \ldots, x_m \mid x_1^3 = 0 \rangle, \quad \langle x_1, \ldots, x_m \mid x_1 x_2 x_1 = 0 \rangle.$$

We can see that if we discard algebras exceptional in some sense, then the rest will have the same Hilbert series (cf. also Theorem 5 from 3.10).

Let us try to give this statement a more precise meaning. Let us assume that the set of generators is fixed as well as the number of (homogeneous) defining relations together with their degrees. Following Anick, we fix this data in the *vector of degrees* $d = (g; |x_1|, \dots, |x_g|/r; m_1, \dots, m_r)$, where g is the number of generators, $|x_1|, \dots, |x_g|$ are their degrees and r is the number of relations with their degrees $m_1, \dots, m_r$. We would like to understand the way the whole set G_d of the algebras with such generators and relations is built up. It turns out that the set of Hilbert series is well ordered with respect to the lexicographic ordering of the series. The infimum of those series is called the *generic* Hilbert series (for a given vector d). Correspondingly, an algebra with the generic Hilbert series is called *generic*. This section is devoted exactly to the study of generic series and algebras. For the majority of the cases it is possible to describe them quite satisfactorily. A great part of the section is devoted to investigating their properties. The remaining part is dedicated to describing properties of the set of Hilbert series and sufficiently unexpected connection between graded algebras and diophantine equations. A consequence of this connection is establishing the algorithmic insolubility of the problems of determining whether an algebra is standard as well as that of calculating its global dimension.

4.2. Order Properties for Series. Let us introduce the lexicographic ordering on the set of formal power series, besides the ordinary ordering: $\sum a_n t^n <_\wedge \sum b_n t^n$ if and only if the first non-zero coefficient of the difference $\sum (b_n - a_n) t^n$ is positive. For instance, $1 + t >_\wedge (1+t)^{-1}$. It is obvious that $\sum a_n t^n > \sum b_n t^n \Rightarrow \sum a_n t^n >_\wedge \sum b_n t^n$, but the reverse implication is not valid.

For every natural number n we index, in some way, all the words of degree n: $S_n = \{s_{1n}, s_{2n}, \dots, s_{l_n n}\}$. That is a basis for $\mathfrak{A}_n$ for an appropriate gradation of the free algebra $\mathfrak{A}$. For a fixed vector of degrees d, every of r relations is of the form $\beta_j = \sum_i c_{ij} s_{im_j} = 0$, $(|\beta_j| = m_j)$, where c_{ij} are some elements in the field K. Every such collection of scalars $c = \{c_{ij}\}$ determines uniquely the algebra $A^c = \langle X \mid \beta_1, \dots, \beta_r \rangle$ (although it is not ruled out that isomorphic algebras correspond to different collections). We have established a special parametrization of the algebras in G_d by the points in K^{N_0}, where

$$N_0 = \sum_{j=1}^{r} l_{m_j}.$$

Theorem 1. *For an arbitrary formal series $H = \sum a_n t^n$, the sets $\{c \mid H_{A^c} \geqslant H\}$, $\{c \mid H_{A^c} \geq_\wedge H\}$, $\{c \mid \dim(A^c)_n \geqslant a_n\}$ are affine varieties in K^{N_0} (i.e. they can be defined by systems of polynomial equations).*

Proof. It is sufficient to see that the sets $\{c \mid \dim(A^c)_n \geqslant a_n\}$ are affine, and the remaining would follow from the Hilbert basis theorem. In order to prove the affine property, let us consider an ideal I and its n-th homogeneous component I_n. Using the coefficients c_{ij}, the elements of I_n may be expressed through the words in S_n. But the condition $\dim(A^c)_n \geqslant a_n$ is equivalent to the condition $\dim I_n < B_n = \dim \mathfrak{A}_n - a_n + 1$, and the latter means that all the minors of the corresponding order are equal to zero. This is what gives the necessary polynomial equations. □

Corollary 1. *The set of all Hilbert series of the algebras from G_d is well ordered (in the increasing order), in other words, the following infinite increasing chain cannot exist:*

$$H_{A_1} <_\wedge H_{A_2} <_\wedge H_{A_3} <_\wedge \dots; \quad A_i \in G_d.$$

Corollary 2. *For every d there exist numbers $n_0 = n_0(d)$ and $n_1 = n_1(d)$, such that $A \in G_d$ is finite-dimensional if and only if all the homogeneous components A_n are equal to zero, for $n_0 \leqslant n \leqslant n_1$. If the graduation is natural ($|x_i| = 1$), then we may assume that $n_0 = n_1$.*

Proof. For the sake of simplicity, we consider only the case of natural graduation. In that case the affine varieties $V_n = \{c \mid \dim(A^c)_n \geqslant 1\}$ are embedded in each other: $V_0 \supseteq V_1 \supseteq \dots$, and, by the Hilbert basis theorem, they start stabilizing from some index on. This index is obviously the desired one. □

We point out that the proofs of both corollaries as well as of the theorem apply not only to the associative algebras (also, for instance, to Lie (super)algebras).

Let us temporarily consider the coefficients c_{ij} introduced above, not as elements of the field K, but rather as some generators of the polynomial ring $K[\dots c_{ij} \dots]$ of N_0 variables. Then we have right to consider the field $K(\dots c_{ij} \dots)$ of rational functions and consider c_{ij} to be elements of that field. We can also consider the algebra $\mathcal{A} = \mathcal{A}(d) = \langle X \mid \sum_i c_{ij} s_{im_j} = 0; j = 1, \dots r \rangle$ over that field and its Hilbert series $H_{\mathcal{A}}$.

Theorem 2. *For every algebra A in G_d we have $H_A \geqslant H_{\mathcal{A}}$. In particular, if $\mathcal{A}$ is infinite-dimensional, then all the algebras in G_d are infinite-dimensional.*

Proof. Repeating the reasoning carried out in the proof of Theorem 1, we see that the equality $\dim \mathcal{A}_n = a_n$ is guaranteed by the condition that all the minors of order b_n are equal to zero (as well as that one of the minors of order $b_n - 1$ does not equal to zero). Every algebra in G_d is obtainable from $\mathcal{A}$ by *specializing* i.e. by substituting c_{ij} by a concrete values from the field K. In specializing, all the minors equal to zero remain equal to zero, while non-zero ones may become zero. Consequently, the equality $\dim \mathcal{A}_n = a_n$ translates into the inequality $\dim A_n \geqslant a_n$, which was required to prove. □

Definition. The Hilbert series of the algebra $\mathcal{A} \in G_d$ will be called *standard* and an algebra A for which $H_A = H_{\mathcal{A}}$ will be called *a standard algebra* $A \in G_d$.

By Theorem 2, the standard series is a lower bound of all the Hilbert series $\mathcal{H}(d)$, however it is an open question whether this bound is exact. This is why, following Anick, we introduce one more definition.

Definition. The infimum of all the series from $\mathcal{H}(d)$, i.e. the series $\sum_0^\infty c_n t^n$, where $c_n = \min\{a_n \mid \sum a_n t^n \in \mathcal{H}(d)\}$ is called the *generic* series and the algebra $A \in G_d$, for which $H_A = \sum_0^\infty c_n t^n$ is called the *generic* algebra (for a given vector of degrees d).

It is obvious that if there exists a standard algebra that it will be generic too in which case the standard series coincides with the generic. However it is not obvious whether generic algebras exist. On the other hand, if there are sufficiently many elements of the field K, algebraically independent over a simple subfield, then we can substitute them in place of c_{ij} and obtain a standard algebra. The meaning of the notion "generic" is sufficiently clear: by Theorem 1, the condition $a_n > c_n$ defines an affine subvariety. This means that the condition of not being generic for an algebra $A^c \in G_d$ means membership in one of the varieties of smaller dimension. Unfortunately, the union of all these varieties may not be a variety in general and it is an open question whether it is contained in some variety smaller than K^{N_0}.

Nevertheless, we will see in the sequel that, for a sufficiently large spectrum of degree vectors, it will be possible to get generic algebras even with the additional structure of either a Hopf algebra or a monomial algebra.

If the degrees vector d is fixed and $A = \langle X \mid R\rangle$ is an arbitrary algebra in G_d, then the series $(1 - H_X + H_R)^{-1}$ depends only on d and does not depend on the choice of the set R. We will denote it by $P_d = P_d(t)$.

Theorem 3. *If there exists an algebra $A \in G_d$ such that $H_A = P_d$, then that algebra as well as the series P_d are standard.*

Proof. It is not difficult to derive the inequality $H_A \geq_\wedge P_d$ from formula (6) of 3.5 (we point out that it is valid only for the lexicographic ordering of series, but not for the ordinary ordering $\geqslant$). This inequality, together with the inequality of Theorem 2, ensures A to be standard. □

4.3. Algebras of Global Dimension Two. We call a set R *strongly free*, if for the algebra $A = \langle X \mid R\rangle$ the equality $H_A = (1 - H_X + H_R)^{-1}$ occuring in the previous theorem holds. The following has been proved in (Anick, 1982c):

Theorem 1. *If R is strongly free, then the algebra A is of global dimension two. Conversely, if the algebra A has global dimension two and the elements of R define a minimal set of defining relations, then they form a strongly free set* (see the definition of dimension in 1.8).

We also point out that, for an algebra of global dimension two, it is possible to calculate the Poincaré series at the same time (see 3.9):

$$P_A(s,t) = 1 + H_X(t)s + H_R(t)s^2.$$

Thus, if for a given degrees vector d there exist algebras of global dimension two, with r independent relations, then the standard algebras will be just like that. If the number r is sufficiently small, then such algebras indeed exist and the following holds:

Theorem 2. *If R is a combinatorially free set, then it is strongly free.*

The proof and the definition are contained in 3.7.

Example. Let $d = \langle 2m; 1, \dots, 1/r; 2, \dots, 2\rangle$ be the case of a quadratic algebra, where $r \leqslant m^2$. Let us denote the generators by $x_1, \dots, x_m, y_1, \dots, y_m$ and choose R to be the set of of the elements of the form $x_i y_j$. This set will obviously be combinatorially free and consequently the algebra will be standard and the standard Hilbert series will be equal to $(1 - 2mt + rt^2)^{-1}$. All the standard algebras for this vector have global dimension two.

Theorem 3. *Let us consider the following six statements, formulated for a given degrees vector d:*
(A) *There exist two polynomials $F(t)$ and $G(t)$ with non-negative integer coefficients, such that*

$$(1 - F)(1 - G) \geqslant 1 - H_X + H_R = P_d^{-1}.$$

(B) *There exists a monomial algebra $A \in G_d$ such that $H_A = P_d$.*
(C) *There exist a Hopf algebra $A = \langle x_1, \dots, x_g \mid y_1, \dots, y_r\rangle \in G_d$ (y_i are the Lie elements), such that $H_A = P_d$.*
(D) *There exist algebras $A \in G_d$ for which $H_A = P_d$ (in other words, there exists a strongly free set).*
(E) $P_d > 0$.
(F) $(P_d)^{-1}$ *has a real root in the interval* $[0, 1]$.
Then the following implications hold:

$$(A) \iff (B) \implies (C) \implies (D) \implies (E) \implies (F),$$

and there exist counterexamples showing that

$$(F) \not\Longrightarrow (E) \not\Longrightarrow (D) \not\Longrightarrow (C).$$

A proof of the theorem has been carried out in (Anick, Löfwall, 1986) and (Anick, 1988a). We will quote from them only the corresponding counterexamples.

(F) $\not\Longrightarrow$ (E). Let $d = (4; 1, 1, 1, 4/3; 2, 2, 2)$. Then $P_d^{-1}(1) = 0$, but $P_d = (1 - 3t - t^4 + 3t^2)^{-1} = 1 + 3t + 6t^2 + 9t^3 + 10t^4 + 6t^5 - 6t^6 \dots$

We point out that if we restrict to the natural graduation, the condition (E) is equivalent to the condition (F).

(E) $\not\Longrightarrow$ (D). Let $d = (3; 2, 3, 3/1; 4)$. Then $P_d = (1 - t^2 - 2t^3 + t^4)^{-1} > 0$, but the unique possible relation $x_1^2 = 0$ leads to the algebra of infinite global dimension (cf. 3.9). For the natural graduation, the implication remains an open question.

(D) $\not\Longleftarrow$ (C). A counterexample to the implication is given by the vector $(2;1,1/2;3,8)$. The details are in (Anick, 1988a).

We indicate only that the standard algebra is the algebra

$$\langle x,y,z \mid xy-y^2=z, xz=zx, z^2yzy=0\rangle,$$

which can obviously also be considered as an algebra from G_d and that the set of its obstructions is the set

$$\{xz,xy\}\cup\{z^2y^nzy \mid n=1,2,\dots\}.$$

The implication (C) $\Longrightarrow$ (B) remains open even for the case of the natural graduation.

Example. Because of the inequality $(1-t)(1-t-t^2)\geqslant 1-2t+t^3$, the standard Hilbert series for the vector $(2;1,1/1;3)$ is of the form $(1-2t+t^3)^{-1}$ and the standard algebras have the global dimension two. On the other hand, since $1-2t+2t^3=0$ does not have roots in the interval $[0,1]$, G_d does not contain algebras of global dimension two with linearly independent set of relations, if $d=(2;1,1/2;3,3)$.

Let us give now several numeric estimates, guaranteeing the conditions (A) and (F), for the case of the natural graduation.

Theorem 4. *Let $d=(2;1,1/r;n,n,\dots n)$. If $r<1+(2^n/4\sqrt{en})$, where $e=2.7182\dots$, then the condition (A) holds. If $r<2^n/e(n-1)$, then the condition (F) holds. For $r=4$, $n=6$, the implication (D) $\Longrightarrow$ (A) does not hold.*

A proof is in the same papers. A counterexample to the implication is the algebra $\langle x,y \mid x^2yxy^2, x^2y^2xy, x^3y^3, x^2y^4-xyxyxy\rangle$. According to the composition lemma, only the element x^2yxyxy is missing for a Gröbner basis. The Hilbert series is calculated by the formula (8) of 3.7:

$$(1-2t+(4t^6+t^7)-t^7)^{-1}=P_d(t).$$

Theorem 5. *Let $d=(g;1,1,\dots,1/r;2,\dots,2)$ (i.e. the algebras $A\in G_d$ are quadratic – cf. 1.7). Conditions (A)–(F) of Theorem 3 are mutually equivalent and are equivalent to the condition*

$$4r\leqslant g^2.$$

Proof. The condition (F) implies non-negativity of the discriminant of the quadratic equation, i.e. $4r\leqslant g^2$. On the other hand, the last condition implies the condition (B), according to the example considered after Theorem 2 (in the case of even g). For the case of odd g we have

$$\left(1-\frac{g-1}{2}t\right)\left(1-\frac{g+1}{2}t\right) \geqslant 1-gt+rt^2,$$

which is the condition (A). □

4.4. Conditions of Finite-dimensionality. In the case when the series $P_d(t)$ has negative coefficients, it after all, cannot be a standard series. On the other hand, another lower bound may be taken to be the polynomial $|P_d(t)|$ obtained from $P_d(t)$ by discarding all the summands beginning with the first negative one. For instance

$$|(1-3t+3t^2)^{-1}| = 1+3t+6t^2+9t^3+9t^4.$$

Theorem 1. *If d is the degrees vector, then, for every algebra in G_d, the inequality $H_A \geqslant |P_d|$ holds.*

Proof. It is sufficient to multiply formula (6) from 3.5 by the polynomial $|P_d|$ with non-negative coefficients. □

Thus, if there is an algebra in G_d, for which $H_A = |P_d|$, then that series will be standard. If there are sufficiently many relations, this is exactly the case.

Theorem 2. *Let $d = (g; 1, 1, \ldots, 1/r; 2, 2, \ldots, 2)$. If $r \geqslant g^2/2$, then the standard algebras exist and the standard series (which is also generic) is equal to*

$$|P_d| = 1+gt+rt^2.$$

Proof. It is sufficient to give explicitly an algebra with such a series. We confine ourselves to a more simple case of even $g = 2m$, for which the algebra is of the form

$$\langle x_1, \ldots, x_m, y_1, \ldots, y_m \mid x_i y_j; x_i x_j - y_i y_j \mid 1 \leqslant i, j \leqslant m\rangle.$$

It is not difficult to check, by constructing a Gröbner basis that all the words of length 3 are equal to zero. The odd variant can be found in (Anick, 1988a). □

We can find, at the same place, a proof of the fact that for the vector $(2; 1, 1/2; 2, n)$, the inequality of Theorem 1 does not became equality for any $n \geqslant 7$, although it is not difficult to check that the standard algebras exist and that they are finite-dimensional.

The interval $g^2/4 < r < g^2/2$ for the algebras defined by quadratic relations remains still uninvestigated, and at least the following two questions remain open:

Is it true that a standard (generic) algebra is either finite-dimensional or is of global dimension two? In other words, is it true that for $r > g^2/4$, there always exists a quadratic finite-dimensional algebra with g generators and r relations? It is true in case $g \leqslant 4$.

If not, then starting with what $r = r(g)$ does such an algebra exist? An analogous question may be made for the Lie algebras. Here an asymptotic estimate is known (Wisliceny, 1979):

$$\lim_{g \to \infty} \frac{r(g)}{g^2} = \frac{1}{4}.$$

4.5. Properties of the Set of Hilbert Series. We would like to investigate in this section the way the set of Hilbert series of finitely presented algebras is set up. First of all, it is obvious that after field extension, nether the Hilbert series nor the degrees vector defining a given algebra change. Thus, in many questions we may consider the base field K sufficiently large. It is useful not only because, according to 4.2 we get the standard algebras, but also because of the following fact:

Theorem 1. *If K is an algebraically closed uncountable field, then the set $\mathcal{H}(d)$ of the Hilbert series is closed with respect to the corresponding topology.*

Proof. Let H be the limit of the Hilbert series H_i of algebras $A^{c_i} \in G(d)$ (i.e. for every coefficient of the series H, all, except possibly finitely many, the series H_i have the same coefficient). It is necessary to prove that $H \in \mathcal{H}(d)$. By Corollary 1 from 4.2, after discarding a finite number of series, we may assume that all the series in our sequence are lexicographically not less than H. Thus, for every n there is an index i such that $H \leq_{\wedge} H_i <_{\wedge} H + t^n$. Let $W = \{c \mid H_{A^c} \geq_{\wedge} H\}$ and $V_n = \{c \mid H_{A^c} \geq_{\wedge} H + t^n\}$, $n = 0, 1, \ldots \Longrightarrow V_n \subset V_{n+1}$. Then, according to Theorem 1 of 4.2, $V = \{c \mid H_{A^c} >_{\wedge} H\}$ is a countable union of embedded affine varieties V_n, non of which equals W, thus $c_i \in W \setminus V_n$. Over an uncountable field this is sufficient for W not to be contained in V. For $c \in W \setminus V$, we have $H_{A^c} = H$. □

Theorem 2. *The set $\mathcal{H}$ of all Hilbert series of finitely presented algebras is countable.*

The set $\mathcal{H}$ and its subset $\mathcal{H}_1$ corresponding to the Hilbert series of finitely presented algebras with natural graduation are closed with respect to some natural operations. Recall that the *Hadamard product* of two series $H = \sum a_n t^n$ and $G = \sum b_n t^n$ is the series $H \circ G = \sum (a_n b_n) t^n$.

Theorem 3. *The sets $\mathcal{H}$ and $\mathcal{H}_1$ are closed with respect to the operations of addition, multiplication and the operation $H * G = (H^{-1} + G^{-1} - 1)^{-1}$. Moreover, the set $\mathcal{H}_1$ is closed with respect to Hadamard multiplication as well as taking derivatives with a shift: $H(t) \longrightarrow (tH(t))'$.*

Proof. The first claim may be easily derived from claims in 3.3, 3.4 and 1.6. The Hadamard multiplication is realized through the so called *Segre product* of two graded algebras $A = \bigoplus A_n$, $B = \bigoplus B_n$, defined as a subset of their tensor product, with graduation $A_n \otimes B_n$. Finally, the derivative with a shift is the Hadamard product of a Hilbert series and the polynomial ring

$$H_{K[x,y]} = 1 + 2t + 3t^2 + \dots \qquad \square$$

Considerably more complex is the following theorem (Anick, Löfwall, 1986):

Theorem 4. *Let $H = \sum a_n t^n \in \mathcal{H}$. Then the following series are also in $\mathcal{H}$:*

$$\text{(A)} \quad (1-t^2)^{-1}(1-t)^{-1}H^2 \prod_1^\infty (1+t^n H).$$

$$\text{(B)} \quad (1-t^2)^{-1}(1-t)^{-1}H^2 \prod_1^\infty (1-t^n H)^{-1}.$$

If H_X is a generating function of the set of generators X, then set $F = (1 - H_X - t^{-1}H_X^2)^{-1}(1 - t - H_X)^{-1}$. Then the following series also belong to $\mathcal{H}$:

$$\text{(C)} \quad F \cdot \prod_1^\infty (1-t^n)^{-a_n}, \ \textit{if char } K = 2;$$

$$F \cdot \prod_1^\infty (1+t^{2n-1})^{a_{2n-1}}/(1-t^{2n})^{a_{2n}}, \ \textit{char } K \neq 2.$$

Finally, if $H \in \mathcal{H}_1$, then the following series are also in $\mathcal{H}_1$

$$\text{(D)} \quad (H \circ H)(t^2)H(t) \prod_0^\infty (1 + a_n t^{n+1}).$$

$$\text{(E)} \quad (H \circ H)(t^2)H(t) \prod_0^\infty (1 - a_n t^{n+1})^{-1}.$$

The following theorem, showing how close the classes $\mathcal{H}$ and $\mathcal{H}_1$ are has been also proved in the same paper.

Theorem 5. *For every finitely defined algebra A, there exists a finitely defined algebra B with natural graduation and there exist polynomials P_1, P_2 with non-negative integer coefficients such that $H_B = P_1 H_A + P_2$. In addition, for every finitely defined algebra B with natural graduation, there exists an algebra C defined by quadratic relations such that $H_B \leqslant H_C \leqslant PH_B$, for some polynomial P with non-negative integer coefficients.*

We will now hold on to the set of radii of convergence of the series in $\mathcal{H}$. It is natural to restrict only to infinite-dimensional algebras since the generating function of a finite-dimensional algebra is a polynomial. Let $\mathcal{R}$ be the set of all the radii of convergence of infinite series in $\mathcal{H}$. By Theorem 5, we may in fact restrict to the set $\mathcal{H}_1$ and even only to the Hilbert series of algebras defined by quadratic relations.

Theorem 6. *The set $\mathcal{R}$ is a divisible semigroup with respect to multiplication and is a dense subset of the segment $[0,1]$ in the usual topology.*

Proof. Closeness with respect to products follows from the fact that the radius of convergence of the Hadamard product of two series equals the product of their radii of convergence. Furthermore, for every $r \in \mathcal{R}$ and a natural number m, it is necessary to prove that $r^{1/m} \in \mathcal{R}$. Let r be the radius of convergence of the series $H = \sum a_n t^n \quad (r^{-1} = \overline{\lim}\ \sqrt[n]{a_n})$. If A is the corresponding algebra for which $H_A = H$, then we can consider its graduation to be natural. Let us consider now the algebra B with the same relations and generators, but where the degree of every generator equals m. Then, as is easily seen, $H_B(t) = H_A(t^m)$, and the radius of convergence of this series is $r^{1/m}$. Since all the coefficients are integers, we have $0 \leqslant (a_n)^{-1/n} \leqslant 1$ and consequently, $\mathcal{R}$ is a subset of the segment $[0,1]$. We know from the example of the series $1 + t + t^2 + \cdots = H_{K[x]}$ that $1 \in \mathcal{R}$. On the other hand, the radius of convergence of a free n-generated algebra in the natural graduation equals $1/n$. Since it is sufficient to restrict to natural graduation and since the Hilbert series of any algebra does not exceed the Hilbert series of the corresponding free algebra, the radius of convergence is not smaller than $1/n > 0$. It remains to prove denseness. For any natural m, n, we can choose a graduation on some set X so that $H_X = 2^m t^n$. Then, according to formula (3) in 3.3, for the free algebra $K\langle X\rangle$, the Hilbert series is equal to $(1 - H_X)^{-1}$ and the radius of convergence equals $2^{-m/n}$. □

We point out that for every $r \in \mathcal{R}$, there exists an algebra defined by quadratic relations, such that r is an irremovable singularity of its Hilbert series (Anick, 1985a).

We finish this section by describing bounds for the radius of convergence when the number g of generators in the natural graduation is fixed (Anick, 1988a).

Theorem 7. *Assume that the vector $d = (g; 1, 1, \ldots, 1/r; m_1, \ldots, m_r)$ satisfies condition (F) in Theorem 3, 4.3. Then, for every series $H \in \mathcal{H}(d)$, its radius of convergence ρ satisfyes the inequality $\frac{1}{g} \leqslant \rho \leqslant \frac{2}{g}$. Moreover, for $r = 2$, either $H^{-1} = (1-t)^2$ or $\frac{1}{g} \leqslant \rho \leqslant 0.7$.*

4.6. Action of a Free Algebra. Diophantine Equations. In this section we assume that K has characteristic zero.

Let us assume that we are given action of a free algebra in a finite-dimensional vector space. Let us describe the situation in more detail. Assume that a natural numbers m and n are fixed. Let $\mathfrak{A} = K\langle x_1, \ldots, x_m\rangle$ be the free algebra in the corresponding graduation and let V be a finite-dimensional vector space with a basis $u_1, u_2, \dots u_n$, which is a $\mathfrak{A}$-module.

Let us fix a vector $u_0 \in V$ and let J be the set of all words among the generators annihilating u_0, in other words,

$$J = \{x_{i_1} x_{i_2} \dots x_{i_k} \mid u_0 * x_{i_1} \dots x_{i_k} = 0\}.$$

Theorem 1. *There exists a Roos algebra A defined by $g = 2m + n + 1$ generators and $r = m(m+n+1)+1$ relations for which*

$$H_A^{-1} = 1 - gt + rt^2 - t^2 H_J(t)(1 - mt).$$

In addition, the global dimension of A equals 3, except in the unique case when J is empty, and then it equals two.

Proof. Recall (1.7) that a *Roos algebra* is an algebra defined by quadratic relations of a special form, namely by linear combinations of graded commutators $[x_i x_j] = x_i x_j + x_j x_i$. In our case it will be defined as follows: Its generators will be the set $x_1, \dots x_m; u_1, \dots, u_n; v_1, \dots, v_m; w (\Rightarrow u_0 = \sum \alpha_i u_i \in A)$, and the relations will be the following commutators:

$$\begin{gathered}[wx_j] = 0; \\ [v_i x_j] = 0; \quad (1 \leqslant i, j \leqslant m); \\ [u_i x_j] = [u_i * x_j, v_j]; \\ [u_0 w] = 0; \quad (j = 1, \dots, m; i = 1, \dots, n).\end{gathered}$$

If we do not consider the last relation, then we obtain the semitensor product of the algebra $\mathfrak{A}$ and the algebra E – the free algebra $K\langle u_1, \dots, u_n, v_1, \dots, v_m, w\rangle$ (cf 1.6). The given algebra is also a semitensor product of the algebra $\mathfrak{A}$ and the algebra E/I, where I is the ideal generated by the graded commutators of the form $[[[\dots [u_0 * x_{i_1} \dots x_{i_q}, v_{j_q}] v_{j_{q-1}}] \dots v_{j_1}] w]$. In order to see this, it is enough to use the composition lemma to convince oneself that the given commutators are the necessary complement to a Gröbner basis (although in a non-trivial ordering). It is not difficult to check that the set of non-zero commutators is combinatorially free, therefore the algebra E/I has global dimension not greater than two (cf. 4.3) and the Hilbert series

$$(1 - (m+n+1)t + t^2(H_F - H_J))^{-1} \quad \text{(cf 3.7)}.$$

The rest follows from the fact that the Hilbert series of a semitensor product (just like the ordinary tensor product) is equal to the product of series and that the global dimension is equal to the sum of the global dimensions (Anick, 1985a). □

We will need a more convenient analogue of this theorem. Let us assume that the action and u_0 have been chosen in a way that J is empty, i.e. $u_0 * f \neq$

0, for every word $f \in \mathfrak{A}$. Let us assume that some linear mapping $\phi : V \longrightarrow W$ into some h-dimensional vector space is given. Let

$$M = \{x_{i_1} \dots x_{i_q} \mid \phi(u_0 * x_{i_1} \dots x_{i_q}) = 0\}.$$

Theorem 2. *There exists a Roos algebra A with $g = 2m+n+h+3$ generators and $r = (m+1)(m+n+h+2)+1$ relations, such that*

$$H_{\bar{A}} = 1 - gt + rt^2 - H_M t^3. \tag{1}$$

In addition,

$$H_M = \sum_{j=0}^{\infty} \dim(\mathrm{Tor}\,^A_{3,3+j}(K,K))t^j,$$

thus the global dimension of A does not exceed three and equals two if and only if M is empty.

Let us now go to the diophantine equations. In reality we will be considering even more general systems of *exponential-polynomial diophantine equations*

$$B(z_1, z_2, \dots z_m) = 0,$$

where B is a finite sum of expressions of the form

$$c_1^{z_1} c_2^{z_2} \dots c_m^{z_m} P(z_1, \dots, z_m),$$

where $c_1, c_2, \dots, c_m$ are non-zero complex numbers and P is a polynomial with complex coefficients.

If S is such a system of equations, then we will be interested in the solutions given by the collections $z = (z_1, \dots, z_m)$ of non-negative integers. If d_n is the number of solutions for which $|z| = z_1 + \dots + z_m = n$, then the series $H_S = \sum_0^\infty d_n t^n$ will be called the *generating function of the system of equations.*

Example. $2^x(2x+1) + (i)^y = 0$ is the system of one equation. Its solutions are $x = 0, y = 4k+2$, therefore,

$$H_S = t^2 + t^6 + t^{10} + \dots = t^2/(1-t^4).$$

Every system of this kind has a numeric characteristic, called the complexity and it will be defined somewhat later.

Theorem 3. *Let $S(z) = 0$ be the system of h exponential-polynomial equations of m variables with complexity d. Then there exists a Roos algebra A over a field of zero characteristic, with $g = 3m + d + h + 6$ generators and $r = (m+1)(2m+d+h+5)+1$ relations, such that*

$$H_A^{-1} = 1 - gt + rt^2 - H_S \cdot t^3,$$

where H_S is the generating function of the system of equations. The global dimension of the algebra A does not exceed three and equals two if and only if the system does not have solutions.

We will not prove the theorem here in its full generality, but rather in its rather special case $m = h = 1$ along with the comments which will clarify more the "ticking coils" behind the proof.

Thus, let us consider the case of one esponential-polynomial equation of one variable. For the start, we consider a rather simple concrete example. Let us assume that we are studying the quadratic equation $z^2 - 5z + 6 = 0$. Its Hilbert series is obviously equal to $t^2 + t^3$. For V we take a three-dimensional vector space with a basis denoted by $[1], [z], [z^2]$. We use the vector $[1]$ as $[u_0]$. The role of the free algebra will be played by the algebra $K[x]$ of polynomials of one variable. The first idea consists of making x act in a way that, for every z, $u_0 * x^z = 1[1] + z[z] + z^2[z^2]$. It is not difficult to achieve after choosing the action matrix for x to be

$$M = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 2 & 1 \end{pmatrix}. \quad \text{Then } M^n = \begin{pmatrix} 1 & 0 & 0 \\ n & 1 & 0 \\ n^2 & 2n & 1 \end{pmatrix}$$

and $u_0 * x^n = 1[1] + n[z] + n^2[z^2]$. Now choose an one-dimensional space for W and define a homomorphism ϕ in the following way: $\phi([1]) = 6, \phi([z]) = -5, \phi([z^2]) = 1$.

In this way, $\phi(u_0 * x^z) = z^2 - 5z + 6$ and the set M from Theorem 2 exactly corresponds to the roots of the quadratic equation.

If we now return to an arbitrary exponential-polynomial expression B of one variable, then we first write down B in the form $\sum_1^r (c_i)^z P_i(z)$, where P_i is a polynomial of degree m_i. We set $n = \sum(m_i + 1)$ and call n the *complexity* of the given expression. Let us consider a vector space V of dimension n and let us choose its basis which we will symbolically denote by $[c_i^z z^k]$ ($i = 1, \ldots, r$, $k = 0, \ldots, m_i$). Note that $c_i^{z+1}(z+1)^k$ may be expressed as a linear combination

$$c_i^{z+1}(z+1)^k = \sum_{j=0}^{k} \lambda_{jk} c_i^z z^j.$$

We define an action of a free generator x on V as follows:

$$[c_i^z z^k] * x = \sum_{j=k}^{m_i} \lambda_{kj} [c_i^z z^j].$$

(We emphasize that the matrix (λ_{kj}) is transposed.)

Now, a not-so-complicated induction shows that

$$\left(\sum [c_i^z]\right) * x^z = \sum_{i,k} c_i^z z^k [c_i^z z^k].$$

(if the ambiguity of z interferes, we can write down x^n, the same way as above). It remains to define the mapping $\phi : V \longrightarrow K$, setting

$$P_i(z) = \sum_{k=0}^{m_i} b_{ik} z^k; \quad \phi([c_i^z z^k]) = b_{ik}.$$

Then $\phi\left((\sum_i [c_i^z]) * x^z = \sum_i c_i^z P_i(z)\right)$ and we can successfully use Theorem 2 by setting $u_0 = \sum [c_i^z]$.

Let us comment on the general case. In that case the basis will be the set of elements of the form $[c^z z^k]$, where c, z, k are multi-indices (for instance, $z^k = z_1^{k_1}, z_2^{k_2}, \ldots, z_m^{k_m}$). Let us say that $c_1^z z^{k_1}$ divides $c_2^z z^{k_2}$, if $c_1 = c_2$, whereas the monomial z^{k_2}, as a polynomial in commuting variables, is fully divisible by z^{k_1}. *The complexity* of a system will be called the number of different expressions of the form $c^z z^k$ which divide at least one of the summands occuring in the system with non-zero coefficients. The corresponding element $[c^z z^k]$ will be in the basis of V. For instance, a basis for the system

$$\begin{cases} 2^a(a^2 - b^2 - 1) + 6^{ab}(5ab^2 - b^3 - 3a) = 0 \\ 3 \cdot 2^a(ab) + (7a - 8b^3) = 0 \end{cases}$$

will be the set $[2^a a^2], [2^a a], [2^a], [2^a b^2], [2^a b], [6^{ab} ab^2], [6^{ab} b^3], [6^{ab} b^2], [6^{ab} ab], [6^{ab} a], [6^{ab} b], [6^{ab}], [2^a ab], [a], [b^3], [b^2], [b], [1]$ and its complexity is 18. Since, in every expression $c^z z^k$, we can increase by 1, one of m variables z_i, we can introduce m actions x_i for which $u * x_i x_j = u * x_j x_i$, where $u \in V$ and, in particular $u_0 * x^z = \sum c_i^z z^k [c_i^z z^k]$. Since we have h equations, we need to consider an h-dimensional vector space W, where the coefficients of every equation determine the corresponding coordinate of the mapping ϕ. This is not all since, because of the noted commutativity, we have obtained not the wanted series but one with multiplicities. In order to correct this drawback we need to generalize the mapping more, making sure that the non-zero value is obtained only on the words of the form $x_1^{z_1} x_2^{z_2} \ldots x_m^{z_m}$ (cf. Anick, 1985a). (On the other hand, at the level of the existence of solutions (for instance for the last Fermat's problem) we may restrict to the variant of a series with multiplicities.)

Theorem 4. *Let B be an exponential-polynomial expression such that $B(z) \geqslant |z|$, for every $z = (z_1, \ldots, z_m)$. Then there exists a Roos algebra whose Hilbert series is rationaly expressed through the series $H = \sum_z t^{B(z)}$.*

Proof. Let us consider the expression $B'(z_0, z) = B(z) - |z| - z_0$. Then $(z_0, z_1, \ldots, z_m)$ is a solution of $B' = 0 \iff z_0 = B(z) - |z|$, consequently the series in the statement of the theorem is exactly the Hilbert series of the equation $B' = 0$:

$$\sum_{B(z_0,z)=0} t^{z_0+z_1+\cdots+z_m} = \sum_z t^{B(z)-|z|+z_1+\ldots z_m} = H. \qquad \square$$

Example. $m = 1, B(Z) = 2^z \geqslant z$.

$$H = t + t^2 + t^4 + t^8 + t^{16} + \dots$$

This series is remarkable in that it is transcendental and does not satisfy any algebraic differential equation (Anick, 1985a), (Mahler, 1930). Therefore, the same is valid for some Hilbert series.

Theorem 5. *Let $d = (g; 1, \dots, 1/r; 2, \dots, 2)$. Then there are g and r with the property that there is no algorithm allowing, for every algebra A in G_d (over a field of characteristic zero), an answer in terms of its generators and relations and in finite number of steps, to any of the following questions:*

1) *Is it true that the algebra A is standard?*
2) *Is it true that global dimension of the algebra equals two?*
3) *Same questions, with the additional assumptions that A is a Roos algebra and its global dimension does not exceed three.*

In other words, all the mentioned questions are algorithmically insoluble.

Proof. If the question number two were algorithmically solvable, then, according to Theorem 3, where a Roos algebra is built up constructively, there would be an algorithm determining, whether any system of diophantine equations has a solution. However it has been proved by Yu.V. Matiyasevich that such an algorithm does not exist even for one diophantine equation. The equality of the first question to the second has been discussed in 4.2 and 4.3. □

A simple consequence of this theorem is infinity of the set of Hilbert series for a given vector d. We may also state concrete values $g = 7$, $r = 11$, for which infinity is easily derived from Theorem 1 (Anick, 1988a). We may, after all also use Theorem 4. Theorem 5 means for instance that, over $\mathbb{Q}$, the set of all c for which A^c is standard is not recursive (although it is recursively enumerable).

We end this section by giving applications to the theory of diophantine equations.

Theorem 6. *Let S_n be a sequence of exponential-polynomial systems of equations in m variables, of limited complexity and of limited number of equations in every system. If $\Omega_1 \subseteq \Omega_2 \subseteq \dots$ is an increasing sequence of sets of solutions of those systems, then it stabilizes.*

Proof. In the opposite case, by Theorem 3, we would get an infinite increasing sequence of Hilbert series, corresponding to the same vector of degrees and this would contradict Corollary 1 of 4.2. □

4.7. Comments. In stating the results of the present section, we basically followed two papers by Anick (Anick, 1985a), (Anick, 1988a) and the paper (Anick, Löfwall, 1986) by Anick and Löfwall.

The paper (Anick, 1982c), mentioned in the course of presentation, also deserves separate attention since it offers a sufficiently reasonable analogue of a regular sequence in the non-commutative case as well as more general facts than the ones we have used here.

The study of actions of a free algebra was conducted simultaneously on the both sides of the Atlantic. Other constructions, connecting finitely presented algebras with diophantine equations have been obtained through the efforts of Swedish mathematicians – cf. (Anick, 1988b), (Fröberg, Gulliksen, Löfwall, 1986). The series of the type H_M in 4.6 (we will call them the M-series) have found one more application. It turned out the problem of calculating the coefficients of an M-series was $\#P$-complete (the specialists in the theory of complexity of computation will understand what this means). In particular, this says that a computer calculation of an arbitrary Hilbert series is a problem that takes the maximum of computational resources. On the other hand, a connection with complexity theory allowed for establishment of a series of positive results. For instance, if $f(n)$ can be computed in $O(n^\delta)$ time and with $O(n^\epsilon)$ memory, where $\epsilon + \delta < 1$, then there exists either a local ring R or a Roos algebra A such that $H_A \sim P_R \sim \sum_0^\infty f(n)t^n$ (cf. 8.3). For example a series in prime powers may be obtained:

$$P_R \sim t^2 + t^3 + t^5 + t^7 + t^{11} + \dots$$

More details about this may be found in (Anick, 1989) and (Anick, 1988b).

§5. Growth of Algebras and Graphs

5.1. Introduction. We have already indicated (3.3), that if we attempt to introduce the notion of a Hilbert series in the non-graded case, then we will be faced with non-invariance, namely the dependence of the series on the choice of a generating set. Nonetheless, there is something all these series, obtained for different choices of the generators have in common, and this commonality is reflected through the notion of growth.

The notion of growth is defined for every monotonous function and is an invariant notion for algebras and groups. In this section, we will introduce its simple properties, introduce types of growth such as polynomial, exponential, alternative (one of the two preceeding ones), as well as introduce notions of the Gel'fand-Kirillov dimension and superdimension.

It is useful to define the notion of growth for a graph too, defining it as the growth of the number of pathes. It turns out that the growth of a finite graph is alternative and there is a suitable criterion of determining the growth. Several ways of matching an algebra with a graph of the same growth are considered at the end of the section.

5.2. The Growth. Gel'fand-Kirillov Dimension. Superdimension. Let us start with the definition of the growth of a function. First of all, note that, instead of considering the function $g(n) = \dim V^n$, it is more suitable to consider the function $f(n) = \dim(V + V^2 + \cdots + V^n)$, which turns out to be monotonous. Hence, we will be considering only monotonous functions $f : \mathbb{N} \longrightarrow \mathbb{R}^+$. Let us define relations of (pre)order and equivalence on a set of such functions: $f \leqslant g$ if and only if there exist natural numbers m and $c > 0$ such that $f(n) \leqslant cg(mn)$, for all $n \in N$;

$$f \sim g \Leftrightarrow f \leqslant g \text{ and } g \leqslant f.$$

The equivalence class of f will be called the *growth* of f and will be denoted by $[f]$.

Natural operations of addition and multiplication and an order relation are introduced among the equivalence classes:

$$[f] + [g] = [f + g]; \quad [f] \cdot [g] = [fg];$$
$$[f] \leqslant [g] \Leftrightarrow f \leqslant g.$$

For example, $[a^n] = [b^n] > [n^\alpha] > [n^\beta]$, for all $a, b > 1$, $\alpha > \beta \geqslant 0$. All the polynomials of the same degree d obviously have equal growth $[n^d]$, which we call *polynomial of degree d.* If $[f] \leqslant [n^d]$, for some d, then the growth of f is considered to be *polynomial.* The growth $[2^n]$ is called *exponential.* The growth which is either polynomial or exponential is called *alternative.* Non-alternative growth is also called *intermediate.*

Example. The growth $[\sqrt{n+3}]$ is polynomial and the growth $[e^{\sqrt{n}}]$ is intermediate.

In order to simplify manipulations with growth functions, the following simple claim will be used:

Lemma. *Let* $g(n) = hf(an + b) + c$, *for* $n \geqslant N_0$, *where* $a, h > 0$. *Then* $[f] = [g]$.

In order to introduce a uniform notion of growth for different algebraic objects, it is suitable to define it through an abstract formulation.

Let A be a vector space and let $\mathcal{K}(A)$ be a family of its finite-dimensional subspaces. We will say that a *calibration* is given on A, if for every $V \in \mathcal{K}(A)$ there is an inclusion sequence of finite-dimensional subspaces

$$V^{(1)} \subseteq V^{(2)} \subseteq V^{(3)} \subseteq \ldots, \quad V^{(n)} \in \mathcal{K}(A),$$

satisfying the following condition: $V^{(k)} \subseteq W^{(m)} \Rightarrow \forall n \in \mathbb{N}\ V^{(kn)} \subseteq W^{(mn)}$. A calibrated space is called *finitely generated* if there exists a $V \in \mathcal{K}(A)$ such that $A = \bigcup_1^\infty V^{(n)}$. In this case, the set V will be called a generating set and its basis – the generators. We may associate *the growth function* $d_V(n) = \dim V^{(n)}$ with every $V \in \mathcal{K}(A)$.

Theorem 1. *The equivalence class $[d_V(n)]$ does not depend on the choice of the generating set; it is called the* growth *of the finitely generated calibrated space A and is denoted by $r(A)$.*

Proof. If V, W are two generating sets, then, for some m, $V^{(1)} \subset W^{(m)}$ holds, consequently

$$V^{(n)} \subset W^{(mn)} \Rightarrow d_V(n) \leqslant d_W(mn) \Rightarrow [d_V(n)] \leqslant [d_W(n)].$$

Analogously, $[d_W] \leqslant [d_V] \Rightarrow [d_V] = [d_W]$. □

Example 1. Let A be a finitely generated associative algebra. Set $V^{(n)} = V+V^2+\cdots+V^n$, for every finite-dimensional space V (if A is an algebra with the unity, then set $V^{(n)} = K+V+V^2+\cdots+V^n$). Such a calibration defines the *growth of the algebra.* The notion of finite generation in a calibrated space has the natural meaning, i.e. coincides with the natural one, in this as well as in the following three examples.

Example 2. Let L be a finitely generated Lie (super)algebra. The calibration $V^{(1)} = V$, $V^{(n+1)} = V^{(n)} + [V^{(n)}, V]$ defines the *growth of the Lie (super)algebra L.*

Example 3. Let M be a finitely generated right module, over a finitely generated algebra A. The calibration $V^{(n)} = V * (KX)^{(n)}$ (where X is the set of generators of A) defines the *growth of the module.* Obviously, the growth of a module does not depend on the choice of a generating set of the algebra X.

Example 4. The *growth* of a finitely generated (semi)group is defined as the growth of its (semi)group algebra.

Example 5. Let A be a space with graduation, for instance a graded algebra. Defining a calibration by the graduation $V^{(n)} = \sum_1^\infty A_k$, independently of V, we define the *growth of a graded space.* If A is a finitely generated graded algebra, then it is not difficult to check that it coincides with the ordinary growth and, in particular, does not depend on the choice of a graduation.

Growth is a cruder construction than the Hilbert series, but it is defined in a wider spectrum and, in many cases, exactly the growth influences the structure of an object. For instance, a particularly essential requirement is that of polynomial growth and we will find confirmation of this in the sequel. Nevertheless, restricting to finitely generated objects turns out to be fairly unsuitable in some cases and in that case numerical characteristics, that turn out to be even cruder are introduced: The Gel'fand-Kirillov dimension and superdimension. Let us define them first on the growth functions. Roughly speaking, the Gel'fand-Kirillov dimension is the degree of the polynomial growth whereas the superdimension is the degree of exponentiality (the superdimension of $[e^{n^\alpha}]$ is α).

Definition. The *Gel'fand-Kirillov dimension* of the equivalence class $[f]$ is defined to be

$$\mathrm{Dim}\,[f] = \varlimsup_{n\to\infty} \frac{\ln f(n)}{\ln n} = \inf\{d \mid [f] \leqslant [n^d]\}.$$

The *superdimension* of $[f]$ is defined as

$$\mathrm{DIM}\,[f] = \varlimsup_{n\to\infty} \frac{\ln\ln f(n)}{\ln n} = \inf\{\alpha \mid [f] \leqslant [2^{n^\alpha}]\}.$$

It is not difficult to see that these definitions do not depend on the choice of f.

The *Gel'fand-Kirillov dimension* of a calibrated space A is defined as

$$\mathrm{Dim}\,A = \sup_{V\in\mathcal{K}(A)} \mathrm{Dim}\,[d_V].$$

(Another notation is GK-dim A.)

Its *superdimension* is defined analogously:

$$\mathrm{DIM}\,A = \sup_{V\in\mathcal{K}(A)} \mathrm{DIM}\,[d_V].$$

Taking infimums instead of supremums, the quantities $\underline{\mathrm{Dim}}\,A, \underline{\mathrm{DIM}}\,A$ can be introduced. For instance,

$$\underline{\mathrm{DIM}}\,A = \sup_{\alpha, V\in\mathcal{K}(A)} \{\alpha \mid [d_V] \geqslant [2^{n^\alpha}]\}.$$

If A is a finitely generated calibrated space, then it is not difficult to see that $\mathrm{Dim}\,A = \mathrm{Dim}\,r(A)$ and $\mathrm{DIM}\,A = \mathrm{DIM}\,r(A)$.

Example 1. The growth of a polynomial algebra in d generators is polynomial of degree d, hence

$$\mathrm{Dim}\,K[X] = d, \quad \mathrm{DIM}\,K[X] = 0.$$

Example 2. The growth of a free algebra with $d > 1$ generators is exponential,

$$r(K\langle X\rangle) = [1 + \cdots + d^n] = \left[\frac{d^{n+1}-1}{d-1}\right] = [2^n] \Rightarrow$$
$$\mathrm{Dim}\,K\langle X\rangle = \infty, \quad \mathrm{DIM}\,K\langle X\rangle = 1.$$

Theorem 2. *Let A be either a finitely-generated associative or a Lie algebra, I its ideal and B its subalgebra. Then*

A) *$r(A/I) \leqslant r(A)$ and the equality holds for $I \neq A$ and finite-dimensional I.*

B) *If B is finitely-generated, then $r(A) \geqslant r(B)$ and the equality holds, if A is a finitely generated B-module.*

C) *Previous inequalities and equalities are preserved for the superdimension and the Gel'fand-Kirillov dimension even if we relinquish the condition of finite generation of A and B. For instance Dim $B \leqslant$ Dim A and Dim $A =$ Dim B, if A is finitely generated as a B-module.*

Proof. The equalities are the only non-obvious part. If I is finite-dimensional, $V \in \mathcal{K}(A)$, and $\overline{V}$ is the image under the natural homomorphism, then $\dim V^{(n)} \leqslant \dim \overline{V}^{(n)} + \dim I$ and we can use the lemma.

Assume now that $A = x_1 B + \cdots + x_p B$, $V \in \mathcal{K}(A)$. We can choose a $U \in \mathcal{K}(B)$ such that $V \subseteq \sum x_i U, B = \langle U \rangle$. For some k, we have $V x_j \subseteq \sum x_j U^{(k)}$, $\forall j = 1, 2, \ldots, p$. Consequently, we can easily prove by induction that

$$V^{(n)} x_j \subseteq \sum x_i U^{(kn)} \Rightarrow V^{(n)} \subseteq \sum V^{(n-1)} x_i U \subseteq \sum x_i U^{(kn-k+1)}$$

and consequently,

$$d_V(n) \leqslant p d_U(kn + (1-k)).$$

It remains only to refer to the lemma. □

Corollary. 1) *If an algebra contains a free two-generated subalgebra, then the growth of the algebra is exponential.*

2) *The growth of an algebra equals to the growth of any of its subalgebras of finite index.*

3) *The growth of a group equals to the growth of any of its subgroups of finite index.*

4) *The growth of a free group with more than two generators is exponential (since the subalgebra generated by those generators is free). Thus an analogue of claim 1) holds for groups.*

For other properties of growth and dimensions Dim, DIM, see section 7.

5.3. The Exponential Growth. Note that the exponential growth does not imply the existence of a free subalgebra or a subgroup. For groups, a counterexample is the Burnside group $B(2,p)$, defined by two generators and the identity $x^p \equiv 1$. For sufficiently large p its growth will be exponential (cf. Adyan, 1975), however, it is obvious that none of its subgroups is free.

For algebras such an example may be found in

Theorem. *There exist nilalgebras of exponential growth.*

Proof. Let us prove, first of all, that every graded algebra with three generators and one relation of every degree $d \geqslant 2$ has exponential growth. Indeed, by Golod-Shafarevich theorem (3.5), its Hilbert series is not less than $(1 - H_X + H_R)^{-1}$, where $H_R = t^2 + t^3 + t^4 + \ldots$ is the generating function of the set of generators. One of examples of such algebras is the algebra $A = \langle x, y, z \mid xy^n z = 0; (n = 0, 1, \ldots) \rangle$. However, its set of defining relations is given by a combinatorially free set, thus, by Theorem 1 in 3.7, $H_A = (1 - H_X + H_R)^{-1}$. Hence, in order to prove that all the algebras of that class have the exponential growth, it suffices to convince ourselves that the algebra A has exponential growth. On the other hand, the algebra A contains a free subalgebra, generated by the elements y, z, since the algebra $A/(x)$ is free (its Gröbner basis consists of one element x).

It remains now to use the example of a nilalgebra, constructed in 3.6. □

It would be interesting to construct examples of infinite-dimensional nilalgebras of the polynomial growth (if such exist).

5.4. The Growth of a Series. Since the Hilbert series carries all the information on asymptotic behaviour of an algebra, it would be useful to know how are the properties of growth exactly reflected in the nature of properties of the sum $H(t)$ of the series. It is useful not only for Hilbert and Poincaré series, but also for the non-invariant *Hilbert series* of an arbitrary finitely presented algebra (recall that it can be defined as the generating function of the set of normal words) and for a given function of growth d_V it is calculated as

$$\sum_0^{\infty}(d_V(n) - d_V(n-1))t^n.$$

Thus, let $H = \sum a_n t^n$ be an arbitrary series with non-negative integer coefficients and let $R = R(H)$ be its radius of convergence:

$$R^{-1} = \overline{\lim_{n\to\infty}} \sqrt[n]{a_n}.$$

The growth of the series will be called the equivalence class $r(H) = [d_H]$, where $d_H(n) = a_0 + \cdots + a_n$.

As we already pointed out, the growth of a finitely generated algebra is equal to the growth of its Hilbert series. We can analogously define the *growth of a local ring* and the *growth of a finite-dimensional algebra* as the growth of their Poincaré series (cf. 1.8). In the latter case though, it would be more correct to speak of the growth of homology, in order not to confuse that growth with its growth as an algebra (which is obviously the identity), but since in this case we will be interested in the growth of the homology, we will allow ourselves this inaccuracy. It is not difficult to obtain the following simple criterion.

Theorem 1. *The growth H is exponential* $\iff$ $0 < R(H) < 1$. *The growth H is polynomial* $\iff$ *either $R > 1$ and $H(t)$ is a polynomial or $R = 1$ and the point $t = 1$ is a pole of finite order of the function $H(t)$.*

Corollary. *If $H(t)$ is a rational function, then the growth $r(H)$ is alternative.*

Remark. If H is a rational function and has a pole of the k-th order for $t = 1$, then $\operatorname{Dim}[r(H)] = k$. In the general case this is not so, since the Gel'fand-Kirillov dimension is not necessarily always an integer (cf. 7.4).

Let us state now an important example of an intermediate growth.

Theorem 2. *Let $\mathcal{P}(n)$ be a partition function, defined as the number of different representations of the number n in the form of natural summands. Its generating function $H_{\mathcal{P}} = 1+\sum_1^\infty \mathcal{P}(n)t^n$ is equal to $\prod_1^\infty (1-t^i)^{-1}$ and its superdimension equals 1/2, thus the growth $r(H_{\mathcal{P}})$ is intermediate (cf. 7.8).*

Proof. Both the formula and the asymptotics

$$\mathcal{P}(n) \sim \frac{1}{4\sqrt{3}n} \exp\left(\pi\sqrt{\frac{2n}{3}}\right)$$

may be found in (Hall, 1967). □

5.5. The Growth of the Universal Enveloping Algebra. Let us assume first of all that a Lie superalgebra L is graded and that $H_L = \sum a_n t^n$ is its Hilbert series (recall that if $L = \bigoplus_1^\infty L_n$, then $a_n = \dim L_n$).

Theorem 1. *The Hilbert series of of the universal enveloping superalgebra $A = U(L)$ is calculated by the formula*

$$H_A(t) = \prod_1^\infty \frac{(1+t^{2i-1})^{a_{2i-1}}}{(1-t^{2i})^{a_{2i}}}.$$

Proof. Let $\{e_j\}$ be a basis of the even part and $\{f_k\}$ a basis of the odd part. By the Poincaré-Birkhoff-Witt theorem, $U(L)$ is isomorphic to a free commutative superalgebra, as a graded space (cf. 1.4, 1.3). The latter in turn is isomorphic to the tensor product of the polynomial algebra $K[\dots e_j \dots]$ and the exterior algebra $\Lambda K[\dots f_k \dots]$ with the corresponding gradation. It remains to refer to both theorems in 3.3. □

Remark. If L is an ordinary Lie algebra (without superstructure), then the Hilbert series for $U(L)$ is found by the following formula:

$$H_A(t) = \prod_1^\infty (1-t^i)^{-a_i}.$$

It is easy to derive this formula from the previous, by simply doubling all the powers of the generators.

We note also that the formulas are valid also in the non-graded case, for a non-invariantly defined Hilbert series.

Theorem 2. *If L is finite-dimensional, then $r(A) = [n^d]$, where the degree of polynomiality d of the growth equals the dimension of the even part. If the even part $L_{\bar{0}}$ is infinite-dimensional, then DIM $A \geqslant \frac{1}{2}$. The algebra L has the exponential growth if and only if $A = U(L)$ has the exponential growth.*

Proof. The finite-dimensional case immediately follows from the previous theorem and the remark in 5.4. By Theorem 2 in 5.4 and the formula for a Lie algebra, we have DIM $U(M) \geqslant 1/2$, if $L = L_{\bar{0}}$ is an infinite-dimensional Lie algebra in the natural graduation. In the general case, not so complicated arguments connected with the use of the lemma in 5.2 are needed. Somewhat more complex is the claim on the exponentiality of the growth and the corresponding calculations may be found in (Ufnarovskij, 1978) and (Babenko, 1980). □

Remark. It is possible to establish a stronger inequality for infinite-dimensional Lie algebras: $\underline{\mathrm{DIM}}\, L \geqslant \alpha \Rightarrow \underline{\mathrm{DIM}}\, A \geqslant \frac{1+\alpha}{2}$ (Ufnarovskij, 1978). An interesting question is whether the equality always holds. In any case, this is so in the following example.

Example. Let L_1 be a Lie algebra with a basis e_i ($i = 1, 2, \dots$) and multiplication $[e_i e_j] = (i - j)e_{i+j}$. Then $H_{U(L_1)}$ is the generating function of the partition number (5.4), therefore

$$\mathrm{DIM}\ U(L_1) = 1/2.$$

Theorem 3. *Let A be an (associative) superalgebra, generated by a finite set $X \cup Y$ and let B and C be its subalgebras generated by the sets X and Y respectively. If $[X, Y] \subseteq B$, then $r(A) \leqslant r(B)r(C)$ (Ufnarovskij, 1978).*

Corollary. *Let L be a finitely generated solvable Lie superalgebra. If for every commutator z of a sufficiently large length the derivation $\mathrm{ad}\, z : x \longrightarrow [zx]$ is algebraic, then L is finite-dimensional.*

Proof. Recall that commutative superalgebras are *solvable* of degree 1 and that L is *solvable* of degree $m+1 \iff [L, L]$ is *solvable* of degree m. Let A be the universal enveloping algebra for L. If x is any generator, and Y the rest of the generators, then let B be the subalgebra generated by the set $\bigcup_0^r (\mathrm{ad}\ z)^i(Y)$. Then, for a sufficiently large r, we have $[B, x] \subseteq B$. Doing exactly the same with other generators we fall into the commutator $[L, L]$ and we can prove that A has the polynomial growth by induction on the degree of solvability. L is finite-dimensional, by Theorem 2. □

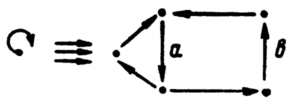
5.6. The Growth of Graphs. By a *graph* we will mean an oriented graph where the loops are allowed (a vertex can be joined with itself by an edge) as well as multiple edges (several edges may go from one vertex to another). A *path* of length n in a graph is a sequence of vertices v_i and the edges e_j: $v_0, e_1, v_1, e_2, \dots, v_n$ such that, for every edge e_j, its ending is the vertex v_j and its beginning is the vertex v_{j-1}. A path is called *cyclic* if its last vertex v_n coincides with the first. If, in addition, all the edges, except the first and the last, are mutually different, then we can consider a subgraph made up of the vertices v_i and the edges e_j, called a *cycle*. A path is called a *chain*, if all the vertices v_i are different.

If G is a finite graph, then the *growth of the graph* G is the equivalence class $r(G) = [d_G]$, where $d_G(n)$ is equal to the number of different paths in the graph, of lengths not greater that n.

Theorem 1. *The growth of every finite graph is alternative. It is exponential if and only if there are two different cycles in the graph with a common vertex. Otherwise it is polynomial of degree d, where d is the maximal possible number of cycles, through which one path can pass (in other words it is the maximal possible number of cycles embedded in a subgraph of the form* $\bigcirc \longrightarrow \bigcirc \longrightarrow \ldots \longrightarrow \bigcirc \longrightarrow \bigcirc$, *where the circles denote cycles and arrows denote chains).*

Proof. If there are two intersecting cycles, then, to every of 2^m collections $a_1a_2\ldots a_m$ of zeros and ones, we can associate a path obtained as the union of the paths C_{a_i}, where C_0 is a cyclical path along the first cycle and C_1 – along the second. Thus the total number of paths grows exponentially. If there are no such intersecting cycles, then the matter reduces to induction on the number of edges for the following reason: if there exist two edges e_1 and e_2 such that none of the paths pass through both of them, then $r(G) = r(G\setminus e_1) + r(G \setminus e_2)$. For more details cf. (Ufnarovskij, 1982). Rationality of the generating function of the number of paths has been also proved there. □

Example.



The growth of the graph is exponential. If the edge b is removed, then the growth will become polynomial of degree 2, and if a is removed, then the degree will be 1.

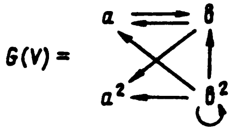
Calculating the growth of a finite graph is easy to be made algorithmic (5.9). We note that exactly the same term of the growth of a graph is used in a perfectly different situation, which will be considered later, in connection with the growth of groups (6.7).

5.7. Graphs for Normal Words. Let F be the set of obstructions of an algebra A, generated by a finite set X (3.6); for instance we may assume that $A = \langle X \mid F\rangle$ is a monomial algebra. Recall that a basis of A is the set N of normal words (in a difference from section 2, it will be suitable now to denote in this way the set of words itself, rather than its linear hull), i.e. words with the property that they do not contain elements from F as a subword. Let us also introduce the following notation: If f and g are words, then $f \blacktriangleleft g$ denotes that f is a proper beginning of g and

$$f \trianglelefteq g \iff (f \blacktriangleleft g) \vee (f = g).$$

Let V be an arbitrary set of non-empty normal words. Let us construct a graph $G(V)$ whose vertices are words from V and the edge $f \longrightarrow g$ is placed if and only if $fg \in N$ and there is no $v \in V$ such that $f \blacktriangleleft v \trianglelefteq fg$.

Example. $F = \{a^3, ab^2, a^2b\}$, $V = \{a, b, a^2, b^2\}$.



Theorem 1. *Let the set V contains X and satisfies the property that for every path $v_0 \to v_1 \to \cdots \to v_n$ the word $f = v_0v_1 \ldots v_n$ is normal and if $v \trianglelefteq f$, $v \in V$, then $v \trianglelefteq v_0$. Then there exists a bijective correspondence between the paths in the graph (counting every vertex as a path of length 0) and the set of normal words. In particular, if V is finite, then $r(A) = r(G(V))$.*

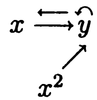
The main example is given by

Theorem 2. *Let V be the set of all proper endings of obstructions, united with the set of generators X. Then V satisfies the conditions of Theorem 1.*

Proof. Assume that the word $f = v_0v_1 \ldots v_n$ is not normal. Then it contains an obstruction. Taking k to be the minimal index such that $v_0v_1 \ldots v_k$ contains an obstruction and using the fact that every ending of the obstruction lies in V, we obtain that $v_{k-1} \to v_k$ is impossible. The second condition of Theorem 1 is proved analogously. □

Example. $F = \{x^3, yx^2\}$, $X = \{x, y\} \Rightarrow$

$V = \{x, y, x^2\}, \qquad g(V) =$



.

The growth is exponential. The example considered above shows applicability of Theorem 1 to other cases too. The growth there is polynomial of degree 2. The graph from Theorem 2 would, in this case, have 5 vertices.

In the case of finite set of words we can also construct another graph. Let $m + 1$ be the maximum of lengths of words in F and let W be the set of normal words of length m. Let us construct a graph $\hat{G}$ whose vertices are the elements of W and the edge $f \to g$ is placed if and only if there exist words $x, y \in X$, such that

$$fx = yg \in N.$$

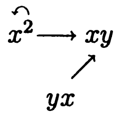
Theorem 3. *There is a bijective correspondence between the set of normal words of length $\geqslant m$ and the paths in the graph. In particular, $r(A) = r(\hat{G})$.*

Proof. To the normal word $f = x_{i_1} \ldots x_{i_t}$, $t \geqslant m$, we assign the path corresponding to the vertices $x_{i_1}x_{i_2} \ldots x_{i_m}$, $x_{i_2}x_{i_3} \ldots x_{i_{m+1}}$, $x_{i_3}x_{i_4} \ldots x_{i_{m+2}}, \ldots$, $x_{i_{t-m+1}} \ldots x_{i_t}$. □

Example.

$$A = \langle x, y \mid xyx, y^2, yx^2 \rangle.$$

$\hat{G}(A) =$



Corollary. *Growth of an algebra with a finite Gröbner basis is alternative.*

We will generalize this corollary somewhat later, introducing one more type of graph (5.10).

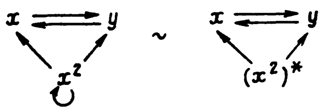
5.8. Transformations of Graphs. Formulas for Normal Words. Calculation of the Hilbert Series. Let G be one of the graphs considered above. We have already seen in 3.6 that for graphs, an operation of *pasting of vertices* is suitable. We will call two vertices to be *similar*, if for every vertex v, the following holds: the number of edges going out from the first vertex to v equals to the number of edges going out from the second vertex to v and the same holds for the incoming edges. All the similar vertices may be pasted into one. The newly formed vertex will have the same connections with other vertices as each of the similar ones and it will be joined with itself by the number of edges equal to the number of edges each of the similar vertices is connected with itself (or equivalently, with another vertex similar to it). It makes sense to mark the new vertex by the union of the sets of markings placed at the pasted vertices, so that in the new graph – the pasted graph $\overline{G}$, not only words are placed by the vertices, but possibly also a set of words. We have seen an example of pasting in 3.6. Let us call a vertex of a graph *last*, if there is no edge coming out of it and *the-last-but-one vertex* if all the edges coming out of it terminate in last vertices. A rather useful operation of *eliminating the-last-but-one* vertices is as follows: if H is such a vertex and $H \longrightarrow H_i$ are all the edges beginning with it, then the operation consists of elimination of all these edges and replacement of the mark for that vertex by $H \cup (\bigcup_i HH_i)$. After this, the vertex will itself become last. In reality this operation may be reduced to pasting and the operation of *removal of an edge*. For the latter, we need a new operation $*$, defined on the set of words. If H is a set of words, set $H^* = \bigcup_1^\infty H^n$. For instance, f^* consists of all the powers of f and X^* is the whole set of non-empty words. First, let us define an operation of *removing a loop* in a vertex denoted by H. It simply consists of erasing that loop and replacing the mark of the vertex by H^*. In order to remove the edge $H_1 \longrightarrow H_2$ we need to erase that edge and, at the same time add a new vertex. This vertex is marked by $(H_1H_2)^*$, if $H_2 \longrightarrow H_1$ and H_1H_2, in the opposite case. Edges from any vertex H come into the new vertex if and only if they come into H_1. Analogously, an edge comes into H from the new vertex, if and only if $H_2 \longrightarrow H$.

If after several transformations we arrive at a finite graph, we then may use the following theorem.

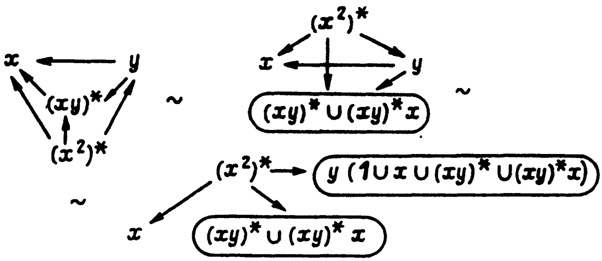
Theorem 1. *Let G be a finite graph obtained from $G(V)$ by the aforementioned transformations. Then there exists a formula expressing the whole set of normal words N through the sets marking the vertices of the graph by the operations of union, multiplication and $*$.*

Proof. First we get rid of the loops, then we get rid of the cycles by removing the edges from the longest cycles. Removing the-last-but-one vertices we leave only the isolated vertices. Pasting them into one we get the desired formula. □

Example. Let $X = \{x, y\}$; $F = \{y^2, yx^2\}$. The original graph constructed according to Theorem 2 from 5.7 is as follows:



After transforming it we obtain



Consequently, the formula for normal words turns into the following formula after several transformations (taking into account **1**)

$$(\mathbf{1} \cup y \cup (x^2)^* \cup (x^2)^* y)(\mathbf{1} \cup x \cup (xy)^* \cup (xy)^* x).$$

The graph obtained after several transformations, does not necessarily have the same growth as the algebra. Nevertheless, it carries all the information both about the growth as well as the Hilbert series.

Let us introduce, just like in 3.7, a matrix M, enumerated by the vertices of the graph. If p is the number of edges from the vertex G_i, into the vertex G_j, then we set $m_{G_i G_j} = pH_{G_j}$, where H_{G_j} is the generating function of the set placed at the vertex G_j.

Let v_0 be the row-vector of generating functions, corresponding to the sets at the vertices of the graph and placed in the same order as in the matrix M. Let $v_n = v_0 M^n$ and let H_n be the sum of all the coordinates of the vector v_n. An easy induction shows that H_n is the generating function of the set of normal words, corresponding to the paths of length n in the original graph (constructed according to Theorem 1). Therefore

$$H_A = 1 + H_0 + H_1 + H_2 + \dots$$

(comp. with formula (8) from 3.7). An analogue of Theorem 2 of the same section holds too:

Theorem 2. *Let the matrix M be algebraic over $K(t)$ (it is always the case if the graph is finite): $\sum_0^k a_i M^i = 0$. Set*

$$\begin{aligned} b_0 &= a_0 + a_1 + a_2 + \ldots + a_k, \\ b_1 &= \quad\;\; a_1 + a_2 + \ldots + a_k, \\ &\ldots\ldots\ldots\ldots\ldots\ldots \\ b_k &= \qquad\qquad\qquad\quad a_k. \end{aligned}$$

Then

$$b_0 H_A = b_0 + b_1 H_0 + b_2 H_1 + \cdots + b_k H_{k-1}.$$

Example. $X = \{x, y\}, |x| = 2, |y| = 1, F = \{xy^n x \mid n \geqslant 0\}$.

$$\overline{G} = \overset{\frown}{y} \longleftarrow \{y^n x \mid n \geqslant 0\}.$$

$$M = \begin{array}{c|cc} & y & \{y^n x\} \\ \hline y & t & 0 \\ \{y^n x\} & t & 0 \end{array}$$

$$v_0 = \left(t, \frac{t^2}{1-t}\right), \text{ since}$$

$$H_{\{y^n x\}} = t^2 + t^3 + \cdots = \frac{t^2}{1-t}.$$

$$M^2 - tM = 0 \Rightarrow a_0 = 0, \quad a_1 = -t, \quad a_2 = 1.$$

$$b_0 = b_1 = 1 - t, \quad b_2 = 1; \quad H_0 = t + \frac{t^2}{1-t} = \frac{t}{1-t}.$$

$$v_1 = v_0 M = \left(t^2 + \frac{t^3}{1-t}, 0\right) \Rightarrow H_1 = t^2 + \frac{t^3}{1-t} = \frac{t^2}{1-t}.$$

$$(1-t)H_A = (1-t) + (1-t)\frac{t}{1-t} + 1 \cdot \frac{t^2}{1-t} \Rightarrow H_A = \frac{1 - t + t^2}{(1-t)^2}.$$

There is a much easier way: H_A is the sum of 1 and all the coordinates of $v_0(E - M)^{-1}$.

5.9. An Algorithm for Calculating the Growth of an Algebra. In this section we give a machine realizable algorithm for computation of the growth of an algebra by any of its graphs (taking into account possible pastings of the vertices); it resembles the process of graph transformation. We will assume that only the incidence matrix T is given, where $T(i, j) = k \iff$ there are exactly k edges going from vertex i into the vertex j. In addition, we will assume that, to every vertex, its growth $r(i)$ has been assigned. For technical reasons, it will be suitable to single out the identity growth [1], in the case when there is only one word at the vertex, as well as a constant growth $[c]$, when the vertex has finitely many words, greater than 1. The operations of multiplication and addition are obvious, we note only that $[1] + [1] = [c]$.

It is not difficult now to construct an algorithm for computation of the growth, by complying with the following rules:

1) If $T = 0$, then the growth of the algebra equals $\sum r(i)$.

2) If $T(i,i) > 1$ or $T(i,i) = 1$ and $r(i) > [1]$, then the growth of the algebra is exponential.

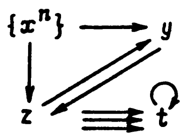
3) If $T(i,i) = 1$ and $r(i) = [1]$, then let $T(i,i) = 0$ and $r(i) = [n]$ (polynomial, of the first degree).

4) If the vertex i is the-last-but-one ($\Longleftrightarrow$ the i-th row is non-zero, but the i-th row in the matrix T^2 is zero), then the i-th row is replaced by the zero row and the growth $r(i)$ is replaced by $r(i) \sum_j T(i,j) r(j)$.

5) If there are no the-last-but-one vertices, but $T \neq 0$, then there must exist a cycle $i_1 \to i_2 \to \cdots \to i_k \to i_1$ and we may replace the row i_1 by the sum of all k, setting all other $(k-1)$ rows to be equal to zero. Then an analogous process should be applied to the columns and taking away $(k-1)$ from $T(i_1, i_1)$, immediately go to 2) with $i_1 = i$, setting $r(i) = \prod_j r(i_j)$. As a matter of fact, this is contraction of a cycle into a point with the replacement of the growth of the latter.

It is clear that it is more effective to look at once for a cycle, transforming along the way the-last-but-one vertices coming across into the last vertices.

Example.



$T =$

	$[n]$	$[1]$	$[1]$	$[1]$
$\{x^n\}$	0	1	1	0
y	0	0	1	0
z	0	1	0	3
t	0	0	0	1

$\Rightarrow$

$[n]$	$[1]$	$[1]$	$[n]$
0	1	1	0
0	0	1	0
0	1	0	3
0	0	0	0

$\Rightarrow$

$[n]$	$[1]$	$[1]$	$[n]$
0	2	0	0
0	1	0	3
0	0	0	0
0	0	0	0

$\Rightarrow$

$[n]$	$[n]$	$[1]$	$[n]$
0	2	0	0
0	0	0	3
0	0	0	0
0	0	0	0

$\Rightarrow$

$[n]$	$[n^2]$	$[1]$	$[n]$
0	2	0	0
0	0	0	0
0	0	0	0
0	0	0	0

$\Rightarrow$

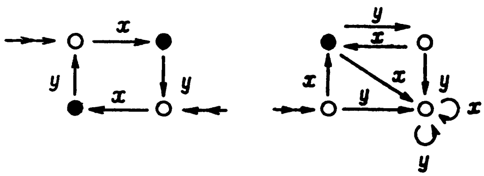
$[n^3]$	$[n^2]$	$[1]$	$[n]$
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0

$\Rightarrow \quad r(A) = [n^3]\,.$

5.10. Regular Languages. Automaton Algebras. Let us call a set of words in a finite alphabet X a *regular set* (or a *language*) if it has been obtained with the aid of finite number of operations of union, multiplication and $*$ (recall that $G^* = \bigcup_1^\infty G^n$, for every set of words G), from a finite collection of words. According to Theorem 1 from 5.8, if there are regular sets at the vertices of a finite graph obtained by pastings in a graph of normal words, then the set of normal words will be regular too. For instance, it is trivially going to be the case when the set of obstructions F is finite. We would like to generalize this fact. To this end, we turn to the theory of automata.

Definition. A *finite automaton* is an oriented graph (see 5.6) where two sets of vertices (possibly intersecting), called *beginning* and *ending*, have been singled out, and every edge has been marked by a letter from a finite alphabet X. An automaton is called a *determined* automaton, if there is only one beginning vertex and, at every vertex, for every letter, there exists a unique edge beginning with that vertex and marked by that letter. The *language* defined by an automaton consists of the set of all the words formed by reading through a path from any beginning vertex to any final vertex.

Example. Both of the represented automatons



define the same language: $x \cup x(yx)^*$, and in addition, the second automaton is determined, but the first is not. The initial vertices are denoted by the symbol $\rightarrowtail$ and in the ending vertices, the circles have been shaded.

In the automata theory the following is a well known

Theorem 1. *The language defined by an automaton is regular. Every regular language may be defined by a determined automaton* (Salomaa, 1981).

This theorem (also called Kleene's theorem) is a powerful instrument in proving regularity. Let us introduce the following notation before we start giving examples of its applications. For every set of words F, we define its subset $L(F)$ consisting of exactly those words of F having no proper beginning as a word in F. It is not difficult to see that, for every word in F, there exists a unique word in $L(F)$ which is its beginning. If we analogously consider the endings of F, then we can consider the set $R(F)$.

Lemma. *If the set F is regular, then the following sets will be regular too:*
a) $L(F), R(F)$,
b) *the complement $S \setminus F$ to the whole set of words S,*
c) *the intersection $F \cap G$ with every regular set G.*

Proof. Let Γ be a determined automaton, defining F. If we declare all its final vertices non-final, and conversely, non-final to be final, then the resulting automaton will define the complement of F. If, on the other hand, we remove all the edges coming out of the final vertices, then the resulting automaton will obviously define $L(F)$. The claim about $R(F)$ follows from the fact that the language obtained from a regular language by inverting all the words in the opposite order will obviously likewise be regular. Finally, the intersection is not difficult to get using complements and unions. □

Definition. An algebra A with the regular set of normal words will be called an *automaton algebra.* The main source of such algebras is

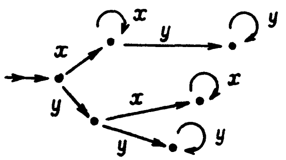
Theorem 2. *An algebra is automaton if and only if the set of its obstructions is regular.*

Proof. If F is the set of obstructions, then the set of normal words is determined by the formula $N = S \setminus SFS$. Conversely, knowing the set of normal words, it is not difficult to find the set of obstructions F by the formula $F = R(L(S \setminus N))$ (cf. 3.6). It remains to use the lemma and the obvious fact that the set of all words is regular. □

Theorem 3. *To every automaton algebra A there corresponds a graph – automaton $G(A)$ with a unique initial vertex and all the others – final vertices, such that there is a bijective correspondence between the set of normal words and the paths in the graph, starting from the initial vertex. In particular, $r(A) = r(G(A))$ and the Hilbert series of the algebra A is rational.*

Proof. Let us consider the determined automaton defining the set of normal words. The desired graph is obtained after discarding all the non-final vertices (excluding the initial). □

Example. $N = \{x^*y^* \cup yx^* \cup x^* \cup y^*\}$. The automaton defining the set of normal words is obtained from the determined automaton:



Corollary. *An automaton algebra has exponential growth if and only if it contains a free subalgebra with two generators.*

Proof. A free subalgebra is generated by normal words, formed by the intersecting cycles. □

We point out that not every algebra of polynomial growth of the first degree is an automaton. The following algebra is a simple example:

$$\langle x, y \mid x^2, yxy, xy^{2^n}x; (n = 0, 1, \dots)\rangle.$$

It is much more plausible that it is the case for a finitely presented algebra of the polynomial growth of the first degree. However, it is an open question.

Examples of automaton algebras are given by the following

Theorem 4. *The following finitely generated algebras are automatons* (Ufnarovskij, 1989a)

A) *commutative algebras;*

B) *algebras defined by not more than two quadratic relations;*

C) *algebras for which all the defining relations have the form* $[x_i x_j] = 0$ *for some pairs of generators.*

Corollary. *The Gel'fand-Kirillov dimension of a commutative finitely generated algebra is an integer (coinciding with its Krull dimension), and the Hilbert series is a rational function.*

5.11. Comments. The notion of growth was introduced by Milnor (Milnor, 1968b), who assumed that the growth of a group was always alternative. Although it turned out not to be the case (6.6), the question nevertheless remains open for finitely presented groups. We note that often enough the growth is defined somewhat differently, by $f \leqslant g \iff f(n) \leqslant g(mn)$, for some m and every n. In essence the difference is only that in this case all the finite-dimensional algebras have a different growth. The Gel'fand-Kirillov dimension was introduced in (Gelfand, Kirillov, 1966) and superdimension appeared in (Borho, Kraft, 1976) and we will present its principal moments in 7.7. In questions connected with graphs, we have followed (Ufnarovskij, 1989a). The theory of formal languages, apart from its specific methods is at present very actively using purely algebraic constructions. A specially interesting way of defining languages is as the solutions of equations in formal series in non-commuting variables. The details of this approach may be found in (Arbib, 1968) and for the initial familiarity with the theory of formal languages it would be best to consult the already cited book by Salomaa (Salomaa, 1981). A book by I. Cannon, D. Epstein, D. Holt, M. Pterson, W. Thurston: Word Processing and Group Theory. Math. Inst. Univ. Warwick, Coventry, England 1991, provides a deep study in the direction of automatic groups. The concept of a path algebra should also be mentioned (Green, 1983); it appears that it plays an important role in representation theory.

§6. Combinatorial Lemmas and Their Applications to Questions of Nilpotency. The Growth of Groups

6.1. Introduction. Studying the combinatorics of words is a problem that arises in various branches of mathematics: these are algebra, as well as dynamical systems, the coding theory as well as the theory of formal languages, we hardly touched upon in the previous section. Not having a possibility of dwelling upon a sufficiently detailed spectrum of various methods and devices in this section, we will put before us a rather more modest goal: to gather in one place a number of sufficiently subtle combinatorial facts on properties of words, that were successfully applied to the algebraic problems (the corresponding results on nilpotency will also be stated in this or in one of the sections that follow).

Thus, the main object of our attention will be a set of all nonempty words S in a finite alphabet X. We may view S as a free semigroup (together with the unity $\mathbf{1}$) as well as a basis of the free algebra $K\langle X\rangle$.

It will be also convenient for us to deal with infinite words. In addition, we may consider words infinite on both sides, as well as the one-sided ones, expanding only to the right. In order to differentiate between these two cases, the former will be exactly called infinite words, and latter will be called sequences. A formal definition is as follows: *infinite words* are the mappings $f : \mathbb{Z} \longrightarrow X$ and the *sequences of letters* are the mappings $f : \mathbb{N} \longrightarrow X$. For instance, $\ldots xyzxyzxyzx \ldots$ is an infinite word. If we cut it at any place, then the right half will be a sequence. A tipical example of an infinite word is the word f^∞, where f is an ordinary word. For instance, the infinite word above may be written down as $(xyz)^\infty$. In the majority of the cases, the infinite words will be used for replacing a formulation of the type " ... there exists an N such that, for every word of length greater than N ... " by an equivalent, shorter one: " ... for every infinite word ... ". In all the concrete cases, the reader will be able to translate by himself a corresponding formulation from one form to another and vice versa. Let us point out again that even the infinite words depend only on a finite number of letters. We will also tacitly assume that the term "subword" means a non-empty finite subword, even when we talk about infinite words. The length of the word f will always be denoted by $|f|$.

We will also discuss problems on the growth of groups, at the end of the section.

6.2. The Avoidable Words. We will show in the first place that many questions about the subwords of finite words may be translated into the language of infinite words. The following is obvious:

Theorem 1. *For every infinite set F of words, there exists an infinite word, such that its every subword is a subword of one of the words in F.*

This theorem can be considerably strengthened. Following (Furstenberg, 1981), we will call an infinite word ω *uniformly recurrent*, if, for every of its subwords u, there exists a number $l = l(u)$, such that u is contained in every subword of ω of length l. The following is an easy consequence derived from (Furstenberg, 1981):

Theorem 2. *For every infinite word f, there exists a uniformly recurrent (infinite) word ω, all of whose subwords are subwords of f.*

Such a uniform improvement of words allows for simplifications of some of the combinatorial arguments.

Definition. *The value* of a word f is any word obtained from f by substitution of its letters by arbitrary words (we emphasize: non-empty). In other words, the value of f is the image of f under a homomorphism of a free semigroup S into another arbitrary semigroup. The word f is called *avoidable* if there exists an infinite word none of whose subwords is a value of f.

An example of an avoidable word is the word x^3. The corresponding infinite word has been constructed independently by several authors: Thue, Arshon, Morse. Its simplest definition is as follows: Let $f_1 = x$ and $f_{n+1} = f_n\overline{f}_n$, where $\overline{f}_n$ is obtained from f_n by substituting x by y and y by x. For example, $f_2 = xy$, $f_3 = xyyx$, $f_4 = xyyxyxxy$ etc. The corresponding infinite word from Theorem 1 will be exactly the desired one. The limiting sequence

$$f_\infty = xyyx\,yx\,xy\,yxxy\,xyyxy\dots$$

is called the *Thue sequence* (it is sometimes called the Arshon sequence and sometimes the Morse sequence). It has even a stronger property: it does not contain subwords of the form g^2z, where z is the first letter of g.

An example of a non-avoidable word is xyx, since, in every infinite word, there are recurring subwords (for instance letters). Actually, even a stronger statement holds:

Theorem 3 (Dejean, 1972). *Every word of length $\geqslant 39$ of three letters contains a subword of the form fgf, such that $|g| \leqslant \frac{1}{3}|f|$. On the other hand, there exists an infinite word in three letters, such that for every of its subwords of the form fgf the inequality $|g| \geqslant \frac{1}{3}|f|$ holds.*

The criterion of avoidability of a word is sufficiently simple. We define by induction the following word in n letters: $Z_1 = x_1$, $Z_{n+1} = Z_n x_n Z_n$.

Theorem 4. *The word f of n letters is avoidable if and only if none of its values is a subword of the word Z_n.*

This theorem has been borrowed from the paper of A.I. Zimin (Zimin, 1982), where another criterion of avoidability can be found too.

Example. The word $yxzyx$ is non-avoidable. The corresponding value in $Z_3 = x_1x_2x_1x_3x_1x_2x_1$ is $x_1x_2(x_1x_3)x_1x_2$. On the contrary, the word x^2 is avoidable.

It is easy to obtain the corresponding sequence from the Thue sequence (Salomaa, 1981).

The essence of the following famous van-der-Waerden theorem is in unavoidability of a finite arithmetic sequence of same letters.

Theorem 5. *For every natural n, in every infinite word, there exist n equal letters spaced equally apart from each other.*

6.3. Comparison and Equivalency of Words. Periodic and Regular Words. This section is closely connected with 2.8, where the reader should find all the necessary definitions. First of all, we discuss the commutativity questions.

Theorem 1. *Let f and g be non-empty words. The following conditions are equivalent:*

(i) *f and g are equivalent (recall $f \sim g \iff fg = gf$).*
(ii) *$f^k = g^n$ for some powers k, $n > 0$.*
(iii) *f and g are powers of the same element.*
(iv) *The subalgebra generated by f and g in the free algebra $K\langle X\rangle$ is not isomorphic to the free algebra of two variables $K\langle x, y\rangle$ (an analogous statement is clearly valid for semigroups too).*

The proof goes by induction on the sum of the lengths $|f| + |g|$, without special complications. The item (iv) is somewhat more difficult, but all the details may be found in (Cohn, 1971), applicable also to a more general situation.

Recall that, in 2.8 we have considered an extension of the partial lexicographic order $>$ to the order $\triangleright$: $f \triangleright g \iff f^k > g^n$, for some $k, n > 0$. Let us define the symbol (f, g) by setting

$$(f,g) = \begin{cases} 0, & \text{if } f \sim g, \\ 1, & \text{if } f \triangleright g, \\ -1, & \text{if } f \triangleleft g. \end{cases}$$

Let a and b be two non-equivalent words. By Theorem 1, they generate a free subsemigroup in S. Assume that a new lexicographic order $>'$ has been defined on this semigroup, such that $a >' b$. This order may be extended in exactly the same way to the order $\triangleright'$. How are the orders $\triangleright$ and $\triangleright'$ related? We introduce the corresponding symbol:

$$\left(\frac{f,g}{a,b}\right) = \begin{cases} 0, & \text{if } f \sim g \text{ or } a \sim b, \\ 1, & \text{if } f \triangleright' g, \\ -1, & \text{if } f \triangleleft' g. \end{cases}$$

It turns out that the following theorem of invariance holds.

Theorem 2. *Let f and g be the elements of the semigroup generated by a and b. Then*

$$(f,g) = \left(\frac{f,g}{a,b}\right)(a,b).$$

Example. Since $ab >' ba$, then $(ab, ba) = \left(\frac{ab,ba}{a,b}\right) \cdot (a,b) = (a,b)$, which permitted another definition of $\triangleright$ in 2.8.

As another example we state the following

Corollary. *The word fg is always between the words f and g in the sense of the order $\rhd$.*

Proof. We may assume that f and g are not equivalent. Then

$$(fg,f)(fg,g) = \left(\frac{fg,f}{f,g}\right)\left(\frac{fg,g}{f,g}\right) \cdot (f,g)^2 = (-1)(1)(1) = -1,$$

and this implies the desired claim. □

Theorems 1 – 4 in 2.8 have been proved exactly on the basis of the Invariance theorem. Its another application may be found in (Ufnarovskij, 1985), where the following Independence theorem has been proved:

Theorem 3. *Let V be a module over a free algebra $\mathfrak{A}$. Let $v \in V$ be a non-zero vector and let $f = x_{i_1}x_{i_2}\ldots x_{i_n}$ be a word such that $v * f \neq 0$, but $v * h = 0$, for every $h > f$. If all the subwords of f act as nilpotent operators in V, then the vectors v, $v * x_{i_1}$, $v * x_{i_1}x_{i_2}, \ldots, v * f$ are linearly independent. (The non-trivial moment consists in the fact that if we do not choose the very last word, then the linear independence may be lost.) In case $V = A = \mathfrak{A}/I$, $v = \mathbf{1}$, we can say more: all subwords of f are independent (as elements of A).*

We now go on to the properties of periodicity. The following is easily proven by induction:

Theorem 4. *Let $f = gh$ be a word such that the word h is at the same time its beginning. If $|g| \leqslant \frac{|f|}{n}$, then $f = g^n s$.*

Theorem 5. *If f is a non-periodic word, then there is a uniquely defined representation $f = ab$, where b is non-empty and ba is a regular word.*

Proof. If f is regular, then $f = b$ and the uniqueness follows from Theorem 2 in 2.8. Otherwise $f = gh$, according to Theorem 3 from 2.8, where either $g \lhd h$ or $g \sim h$. The latter case is impossible because of non-periodicity of f. Thus, by definition, $f < hg$ and the case is closed after induction on the order $<$ from above. □

Corollary. *If f is a periodic word of period n (i.e. $f = g^n$, for some word g), then f contains a subword of the form u^{n-1}, where u is a regular word.*

Theorem 6. *For all natural N and n, every infinite word contains either a regular subword of length greater than N, or contains the n-th power of a regular word.*

Proof. Let us assume that all the subwords of length greater than N are not regular. Then there are only finitely many different regular subwords, say L in number. Let f be any subword of length greater than nLN. According to Theorem 5 in 2.8, $f = f_1 f_2 \ldots f_k$, where $f_1 \unlhd f_2 \unlhd \ldots \unlhd f_k$ and f_i are regular. Consequently, $k > nL$ and there are n equal f_i's, thus there is a subword of the form f_i^n. □

A further development of that theorem is the following

Theorem 7. *For every natural n and k, every infinite word contains either an n-th power of a regular word or a subword of the form* $u_1v_1u_2v_2\dots u_kv_k$, *where* u_i *are regular words and* $u_1 > u_2 > \dots > u_k$ *(some of the words* v_i *may be empty).*

Recall that a word f is called *n-decomposable* if f can be represented in the form $f = f_1f_2\dots f_n$, where, for every non-identity permutation π we have $f > f_{\pi(1)}f_{\pi(2)}\dots f_{\pi(n)}$. It is not difficult to check that in order to have that, it is necessary and sufficient that the condition $f_1 \rhd f_2 \rhd \dots \rhd f_n$ is satisfied.

Corollary. *Every infinite word contains either an n-th degree of a regular word or a k-decomposable subword.*

A proof of Theorem 7 may be found in the original paper by E.I. Zel'manov, who generalized the corresponding proof of the Corollary by A.I. Shirshov (cf. (Shirshov, 1957) and (Zel'manov, 1989) respectively). The following result of Higman (Higman, 1957) can be proved by a variation of this technique.

Theorem 8. *Let* f *be a sequence, composed of the letters* $x_1, x_2, \dots, x_{p-1}$ *(where p is a prime number). Then there exists either a beginning or a regular subword of the form* $x_{i_1}x_{i_2}\dots x_{i_k}$, *with the sum of the indices* $\sum_j i_j$ *divisible by p.*

Definition. Let us call a word *a semiregular*, if any of its ends is either lexicographically less than a or is the beginning of a.

It is easy to see that the beginning of a semiregular word is also semiregular. It is possible to verify the following fact too: a semiregular word, different from a power of the least letter, is the beginning of some regular word.

Lemma. *Every infinite word contains either the square of a semiregular word, or a subword of the form* fgf, *where* g *is regular and* f *is a semiregular word.*

Proof. Let us assume the opposite and let F be the corresponding counterexample. By Theorem 2 from 6.2, the word F may be assumed to be uniformly recurrent. We will be led to a contradiction by the following elegant reasoning of Backelin.

Since every subword in F appears infinitely many times, we can construct, by induction on n, an infinite sequence $\tilde{F}$ such that its first n letters form a word a_n which is lexicographically greatest among all the subwords of F of length n. Note that, since all the subwords of $\tilde{F}$ are also subwords of F, $\tilde{F}$ is also uniformly recurrent and also does not contain subwords of the form f^2 and fgf, where g is regular and f is semiregular. In addition, by the construction, every beginning – the word a_n, is a semiregular word, thus, in particular, $\tilde{F}$ does not start with a square. This, by Theorem 4, means that no proper ending of $\tilde{F}$ coincides with $\tilde{F}$ and we can correctly assign to every letter t_i of the word $\tilde{F}$ a number $n = n(i)$ such that $\tilde{F}$ is of the form $\tilde{F} = a_{i-1}t_ia_n\ldots$ and such that n is maximal with this property (for the sake of definiteness, we assume that a_0 is an empty word). For example

$$\begin{array}{ccccccccccccccccc} \tilde{F} & = & a & b & e & c & d & b & c & a & b & e & d & b & a & c & \ldots \\ n & = & 0 & 0 & 0 & 0 & 0 & 0 & 3 & 0 & 0 & 0 & 0 & 1 & 0 & . & \ldots \end{array}.$$

The numbers $n(i)$ are unbounded because of uniform recurrence, therefore, if we underline all the letters t_i, such that $n(j) < n(i)$, for all $j < i$, then infinitely many letters t_i will be underlined, with arbitrarily large values $n(i)$. Since there are finitely many letters in the alphabet, one of the letters, say t, would be underlined infinitely many times, thus there would exist subwords ta_n, with arbitrarily large number n. This means that all the subwords of the sequence $G = t\tilde{F}$ are also subwords of F and, in particular, there are no subwords of the form fgf among them, where g is regular and f semiregular. Let $t = t_i$ be any underlined occurrence of t in $\tilde{F}$. Then $G = ta_{i-1}ta_{n(i)}\ldots$. Since the letter t is regular, thus also a semiregular word, the word a_{i-1} cannot be regular. But we noted above that a_{i-1} was a semiregular word and therefore some of its proper endings b is also its beginning, i.e. $b = a_j$, for some $j < i$. Since t_i is underlined, j is smaller than $n(i)$, thus $a_{n(i)}$ begins with $a_j = b$. We have arrived at the subword btb and it remains to recall that $b = a_j$ is a semiregular word. This contradiction finishes the proof. □

Theorem 9. *Every infinite word contains either the square of a regular word or a word of the form fgf, where f and g are regular words, as a subword.*

Proof. According to the lemma, there is a subword either of the form f^2 or of the form fgf, where f is semiregular and g is regular. If f is not regular, then some of its endings f' coincides with its beginning, thus is semiregular too. But then $(f')^2$ (respectively $f'gf'$) is a subword and induction on the length of f finishes the proof.

6.4. Theorem on Height. Let V be a set of words in a finite alphabet X. We will say that the letter f has *height* k relative to V, if $f = v_1^{i_1}v_2^{i_2}\ldots v_k^{i_k}$, for some $v_i \in V$ and k is the minimal number with that property. For instance, the word *aabaabaab* is of height 6 relative to the set $\{a, b\}$ and of height 1 with respect to the set $\{a^2b\}$ and does not have height relative to $\{a\}$. □

Definition. The algebra A generated by the set X has a limited height over V, if every word f in A may be represented as a linear combination of words f_i of the same composition with respect to the generators (i.e. $\forall x \in X \quad \deg_x f = \deg_x f_i$), where the heights of all the words f_i, with respect to V, are bound by a constant h, which does not depend either on f_i or on f.

For instance, a finitely generated commutative algebra obviously has a bounded height over its generating set. A far reaching generalization of this fact is the following theorem of Shirshov on height (see the necessary definitions in 7.2).

Theorem 1. *If an algebra A satisfies an identity of degree n, then it has a bounded height over the set of all the words of length less than n.*

The proof decomposes into several simple ideas. First of all, the identity may be considered *multilinear*, i.e. of the form

$$x_1x_2\dots x_n = \sum_{\pi\in S_n\setminus e} \alpha_\pi x_{\pi(1)}x_{\pi(2)}\dots x_{\pi(n)},$$

where the sumation goes over all the non-identity permutations π (cf. 7.2). Thus every word containing an n-decomposable subword (see the previous section), may be expressed through lexicographically smaller ones. Therefore the problem reduces to showing that every word of sufficiently large height contains an n-decomposable subword. There are two ideas here. First of all, if u is a regular word of length greater than n, then u^{2^n} contains an n-decomposable subword $(a_1b_1)\dots(a_nb_n)$, where every a_i is obtained from u by a cyclic permutation of the letters. Secondly, if u and v are words of length smaller than n, where $|v| \leqslant |u|$, but v is not a beginning of u, then one of the following two words

$$(u^nva_1u)(u^{n-1}va_2u^2)\dots(uva_n),$$
$$(va_1u^{n-1})(uva_2u^{n-2})(u^2va_3u^{n-3})\dots(u^{n-1}va_n)$$

is n-decomposable (depending on what is greater: u or v).

It remains now to gather all these ideas into one with the aid of the corollary to Theorem 7 in 6.3, setting there $k \to n$, $n \to 2^n$. For more details see the original paper by A.I. Shirshov (Shirshov, 1957), where the variants for the nonassociative algebras may be found.

Corollary 1. *A* finitely generated PI-algebra *(i.e. an algebra with a non-trivial identity) has a polynomial growth.*

Corollary 2. *An* algebraic PI-*algebra with a finite number of generators is finite-dimensional (recall that "algebraic" means that every element is* algebraic, *i.e. a root of an equation of one variable).*

We point out that without the identity, this is already not valid (3.5). A semigroup with the identity $x^2 \equiv 0$ (6.2) will not be finite either. Nevertheless, in the presence of the identity, the algebraic condition is necessary only for the words of the length less than n. Is it possible to replace n by a better estimate? I.P. Shestakov raised a hypothesis that, instead of the degree n of the identity in the conditions of Theorem 1, we may use the complexity of the algebra A (cf. 7.2). Since the latter does not exceed $\left[\frac{n}{2}\right]$, this estimate is more effective and the best one. The hypothesis turned out to be correct, and the reader may familiarize himself with three independent approaches to the proof through the papers (Belov, 1988), (Ufnarovskij, 1985) and (Chekanu, 1988). For example, for nilalgebras, we may use the Independence theorem from (6.3). As far as the theorem on height, we note one more result from (Belov, 1988):

Theorem 2. *Let A be a finitely-generated, graded associative algebra of complexity n and let M be its finite subset of elements homogeneous in every variable. If M generates A and if the factor-algebra A/I, mod an ideal I generated by the n-th degrees of elements of M, is nilpotent, then A is of bounded height over M (the definition of height is analogous to the one given earlier).*

It has been also shown there, that an alternative or a Jordan PI-algebra, with an identity of degree n has a bounded height over the set of all the words of length not greater than n^2.

6.5. Nilpotency. Sandwiches. Recall that a (not necessarily associative super)algebra is called *nilpotent of index* n, if every product of any n of its elements equals to zero. In the case of a Lie (super)algebra, it is sufficient that the *left normalized commutators* $[[\dots[x_{i_1}x_{i_2}]x_{i_3}]\dots x_{i_n}]$, which we will shortly denote by $[x_{i_1}, x_{i_2}, \dots x_{i_n}]$, equal to zero. We note that the regular non-associative words (2.8) are not left normalized.

Since we will be often interested in questions on nilpotency of ideals, which rarely turn out to be finitely generated as algebras, it will be suitable to introduce the following

Definition. A (super)algebra A (not necessarily associative) is called *locally nilpotent*, if its every finitely generated subalgebra is nilpotent. In order to graduate this notion, we will call a nilpotent algebra *globally nilpotent.*

If A is an associative nilalgebra (1.2), then we have seen in 3.5, that it does not have to be locally nilpotent, although local nilpotence holds from the theorem on height (6.4), in the presence of the identity. Global nilpotency may not hold as the example of an exterior algebra with countable number of variables shows. Nilpotency may be ensured by a very unexpected conditions (cf. for instance Theorem 3 in 7.4 and the following result of Higman (Higman, 1957), based on a combinatorial Theorem 8 from 6.3):

Theorem 1. *Let A be an associative or a Lie algebra, with an automorphism ϕ, such that it does not leave fixed any non-zero elements (automorphisms of this kind are called* regular*). If the order of ϕ is a prime number p, then A is nilpotent (with the index $\leqslant p-1$, in the associative case).*

The question of estimating above the nilpotency index of a Lie algebra is interesting. The exponential estimate above has been proved in a paper by V.A. Kreknin and A.I. Kostrikin (Kreknin, Kostrikin, 1963). The hypothesis, that has been checked for $p \leqslant 7$, consists in the claim that the estimate equals to the lower estimate $\frac{p^2-1}{4}$, proved by Higman. They also proved in the same paper (Kreknin, Kostrikin, 1963) that, if a finite-dimensional Lie algebra L

over a field of characteristic p, has a regular automorphism ϕ, with the period $q^s < p$ (q is prime), then L is solvable.

In a Lie (super)algebra the ordinary nil conditions are meaningless, therefore, to every $x \in L$, we associate a mapping ad $x : L \longrightarrow L$, defined by the rule $y \longrightarrow [yx]$.

Definition. An element $x \in L$ is called ad*-nilpotent*, if $(\text{ad } x)^n = 0$, for some n. A Lie algebra L where, for every $x \in L$, $(\text{ad } x)^n = 0$ holds is called an *Engel algebra* (or an n-Engel algebra, if we want to specify the index n).

One of the most important results, obtained in the recent time, is the following theorem proved by E.I. Zel'manov.

Theorem 2. *An Engel Lie algebra is locally nilpotent.*

Local nilpotency for the n-Engel Lie algebras of characteristic either greater than n or zero was first proved by Kostrikin, who developed the method of sandwiches (cf. Kostrikin, 1986).

We note that, for a characteristic not equal to two, the condition $(\text{ad } x)^2 = 0$ implies the condition $(\text{ad } x)(\text{ad } y)(\text{ad } x) = 0$, for all $y \in L$.

Definition. An element x in a Lie (super)algebra L is called a *sandwich*, if the following conditions are satisfied: $(\text{ad}\, x)^2 = 0$ and $(\text{ad}\, x)(\text{ad}\, y)(\text{ad}\, x) = 0$, for all $y \in L$.

It is easy to see that the commutator of two sandwiches is again a sandwich. A considerably less trivial is the following fact, proved at first by A.I. Kostrikin for Engel Lie algebras and generalized by E.I. Zel'manov (cf. Zel'manov, Kostrikin, 1990):

Theorem 3. *A Lie (super)algebra generated by sandwiches is locally nilpotent.*

Proof. Let $y_1, \ldots, y_n$ be a finite set of sandwiches. It is necessary to prove that the associative algebra generated by the mapings $x_i = \text{ad } y_i$ is nilpotent. By Theorem 9 in 6.3, there exists an N, such that every associative word of length N in the alphabet of n letters contains either a square of a regular word or a subword of the form fgf, where f and g are regular words. Let us prove that our associative algebra has the nilpotency index not greater than N. Indeed, in the opposite case there would exist a minimal word (in the lexicographic sense) F of length N, which is not equal to zero. Let fgf be a corresponding subword, where f is regular and g is either empty or regular. Then let us consider the regular nonassociative words $\tilde{f}$ and $\tilde{g}$. By Theorem 6 in 2.8, because of minimality,

$$F = \ldots fgf \cdots = \ldots \tilde{f}\tilde{g}\tilde{f} \ldots.$$

On the other hand, since the commutators of sandwiches are also sandwiches, $\tilde{f}$ is a sandwich and $\tilde{f}\tilde{g}\tilde{f} = 0$, thus $F = 0$. □

An attempt to prove local nilpotency of an Engel algebra by the same means would require a hypothesis that, in Theorem 7 from 6.2, all the v_i may be considered to be empty. This hypothesis is refuted however by following example of A.D. Chanyshev. Let f_n be an infinite set of words, where $f_1 = a$ and f_{n+1} is obtained from f_n by substituting a by a^2b and b by ab. For instance $f_2 = a^2b$, $f_3 = a^2ba^2bab$. Then the infinite word, constructed according to Theorem 1 from 6.2 has the property that it does not contain cubes and subwords of the form $u_1u_2u_3$, where $u_1 \rhd u_2 \rhd u_3$ are regular words. It also does not contain the subwords of the form $v_1v_2v_3v_4$, where $v_1 \trianglerighteq v_2 \trianglerighteq v_3 \trianglerighteq v_4$ are regular. It is interesting however, that every infinite word contains a subword of the form $v_1v_2v_3$, where $v_1 \trianglerighteq v_2 \trianglerighteq v_3$ are regular.

Nevertheless, the proof of Theorem 2 is based on combinatorial lemmas, although more virtuous. Roughly speaking, the main ideas of the proof of local nilpotency are the following. First of all, after factoring out mod maximal locally nilpotent ideal, we may assume that there are no locally nilpotent ideals. In particular, there is no center and we may go to the associative algebra of multiplications, generated by all the ad x and considering L to be embedded in it. For example, the fact that $x \in L$ is a sandwich is written down as $x^2 = 0$ and $xyx = 0$ for $x \in L$. This already simplifies the technical work and allows for the use of combinatorial reasoning.

Secondly, if it is possible to find a homogeneous Lie polynomial, for instance a commutator, such that it is not identically equal to zero on L and such that each of its values is a sandwich, then in an algebraically closed field, everything reduces to Theorem 3, for the following holds:

Theorem 4. *Let $f(x_1, \ldots, x_k)$ be a homogeneous Lie polynomial. If the ground field K is infinite, then the linear hull of the set of its values is an ideal in L.*

Proof. Let us consider, for the simplicity's sake, the case of the (left normalized) commutator $f = [x_{i_1}, x_{i_2}, \ldots, x_{i_t}]$. On one hand, since multiplication by an element is a differentiation, we have

$$[f(a_1, \ldots, a_k), b] = f([a_1b], a_2, \ldots, a_k) + \cdots + f(a_1, a_2, \ldots, [a_kb]).$$

On the other hand, for every $\lambda \in K$, the image of f contains the element $f(a_1 + \lambda a_1b, a_2 + \lambda a_2b, \ldots, a_k + \lambda a_kb) = f(a_1, \ldots, a_k) + \lambda(f([a_1b], a_2, \ldots, a_k) + \cdots + \lambda f(a_1, a_2, \ldots, [a_kb])) + \lambda^2 \ldots$ The arguments connected with the Van der Monde's determinant show that the hull of the image also contains the required linear part equal to $[f(a_1, \ldots, a_k), b]$. □

This scheme works indeed for the Engel index smaller than the characteristic of the field as well as for the zero characteristic; the construction of the corresponding polynomial may be found in (Kostrikin, 1986). In the general case, when the characteristic is greater than three, it is possible to construct a superpolynomial for which the entire associative algebra of multiplications is embeddable into the superalgebra by tensoring by an exterior algebra.

This super-trick, however, does not work for small characteristics, thus E.I. Zel'manov, the author of this approach, had considered another extension of the signature, at the expense of so called divided powers.

The *Engel identity* $(\text{ad}\, x)^n = 0$ implies the *linearized Engel identity* $\sum_{\pi \in S_n} [y, x_{\pi(1)}, \dots x_{\pi(n)}] = 0$. The reverse implication does not hold for the characteristics less than n. Nevertheless, the following holds:

Theorem 5. *Assume that, in a Lie algebra L, the linearized Engel identity of degree n holds as well as that, for every commutator x of the generators, $(ad\, x)^m = 0$, for a fixed number m. Then L is locally nilpotent.*

The proof is based on reduction to Theorem 2. The basic idea is again in tensoring the associative envelope A, this time by the algebra $E = \langle t_i \mid t_i^2, t_i t_j - t_j t_i \rangle$ with an even number of variables. This tensoring also "improves the quality" of the algebra since the already present non-linearized Engel identity appears. An essential role is played here by Theorem 7 from 6.2. If f is a minimal word in the lexicographic sense, and

$$\dots u_1 v_1 u_2 v_2 \dots u_k \dots$$

its subword fitting the conditions of that theorem, then let us consider the element $a = \sum \tilde{u}_i \otimes t_i$, where $\tilde{u}_i$ are regular nonassociative words. Then a is not equal to zero and $\dots a v_1 a v_2 a \dots a \dots \neq 0$. On the other hand, it is possible to show that $(aA)^k = 0$, for a sufficiently large k. This sketch is deciphered in more detail in (Zel'manov, 1989).

Let us now discuss the problem of global nilpotency, in somewhat more detail. The situation is clear in the associative case. The example of truncated polynomials over $\mathbb{Z}_p$: $\langle x_i \mid x_i^p = 0, x_i x_j = x_j x_i \rangle$ shows that global nilpotency may not exist even in the presence of the identity $x^n \equiv 0$. It turned out, however, that the question depends intrinsically on characteristics.

Theorem 6. *An associative algebra over a field of characteristic greater than n (or zero), satisfying the identity $x^n \equiv 0$, is nilpotent.*

This theorem has been proved first by Ya.S. Dubnov and V.K. Ivanov (Dubnov, Ivanov, 1943) and then independently reproved by Nagata and Higman. As for the nilpotency index, Yu.P. Razmyslov has shown that it does not exceed n^2. On the other hand, E.N. Kuz'min has shown that, for a relatively-free algebra with the identity $x^n \equiv 0$ over the field of characteristic zero, the nilpotency index is not smaller than $\frac{n(n+1)}{2}$ (Razmyslov, 1978), (Kuz'min, 1975).

The picture for Lie algebras is similar, but more complicated. Over the field $\mathbb{Z}_p$, Yu.P. Razmyslov has constructed a non-nilpotent Lie algebra with the identity $(\text{ad}\, x)^{p-2} = 0$, $p \geqslant 5$ (cf. Razmyslov, 1971). On the other hand, for a field of characteristic zero, therefore also for characteristics much greater than n, the following non-trivial result of E.I. Zel'manov (Zel'manov, 1988) holds:

Theorem 7. *An n-Engel Lie algebra over a field of zero characteristic is globally nilpotent.*

Here too, the main moment turned out to be the use of the language of superalgebras. The reader is recommended to consult the paper (Zel'manov, 1988), where he will also find results related to nonassociative algebras.

At the end, we state one more result of A.D. Chanyshev, related to associative algebras. Let Γ be an arbitrary semigroup and let an algebra A be representable in the form of the sum (not necessarily direct) of its subspaces $A = \sum_{g\in\Gamma} A_g$, where $A_g A_h \subseteq A_{gh}$. In this situation we speak of graduation of A by the semigroup Γ. We have already used such graduations when the role of Γ was played by $\mathbb{Z}_2, \mathbb{Z}, \mathbb{Z}^+$. Let us call the elements A_g *homogeneous.*

Theorem 8. *Let a Γ-graded associative algebra A satisfy the following conditions:*

a) *a non-trivial identity of degree n holds in A,*
b) *for every homogeneous element a, $a^m = 0$ holds,*
c) *the algebra A is generated by a finite number l of its components A_g,*
d) *the characteristic of the ground field is zero.*

Then A is globally nilpotent, where the nilpotency index is bounded above by a function depending on n, m and l, but is not dependent on the form of the algebra A.

6.6. Nilpotency and Growth in Groups. Recall that the *commutator* $[g, h]$ of the elements g and h is defined by the equality $[g, h] = g^{-1}h^{-1}gh$. If H and K are subgroups of G, then their mutual commutator $[H, K]$ is defined as the smallest subgroup in G that contains all of the commutators $[h, k]$, where $h \in H$, $k \in K$. If we denote $y^{-1}xy$ by x^y, then the following identities are satisfied: $[x, y] = x^{-1}x^y$, $[x, y]^{-1} = [y, x]$, $[xy, z] = [x, z]^y[y, z]$, $[x, z]^y = [x^y, z^y]$, $[[x, y^{-1}], z]^y[[y, z^{-1}], x]^z[[z, x^{-1}]y]^x = 1$.

In particular, the mutual commutator of normal subgroups is itself normal. To every group G we associate two series of normal subgroups:

$$G = G^{(1)}; \quad G^{(2)} = [G, G^{(1)}]; \quad G^{(3)} = [G, G^{(2)}], \ldots;$$
$$G' = [G, G]; \quad G'' = [G', G']; \quad G''' = [G'', G''], \ldots$$

The first of them is called the *lower central series.* If it terminates, i.e. if $G^{(n)} = e$, for some n, then the group is called *nilpotent* and the minimal such n is called the *nilpotency index* (or *degree*). In case when the second series terminates, we speak of a *solvable group* and of *level* (degree) of *solvability.*

Let $K_1 = G \supseteq K_2 \supseteq K_3 \ldots$ be an arbitrary series of normal subgroups in G, satisfying the condition $[K_i, K_j] \subseteq K_{i+j}$. Let us assume that either all the factors K_i/K_{i+1} are torsion free, or to the contrary, all of them have the same period n. Since all of them are abelian groups by the assumption, we may consider their direct sum $L(G) = \bigoplus K_i/K_{i+1}$, introducing the additive notation for multiplication in every summand: $aK_{i+1} + bK_{i+1} = abK_{i+1}$. It turns out that we can introduce multiplication too, by setting $[aK_{i+1}, bK_{i+1}] = [a,b]K_{i+j+1}$ and extending it by additivity. As a result we obtain a Lie algebra (admittedly, over the ring $\mathbb{Z}$ or $\mathbb{Z}_n$, depending on the torsion), as follows from the identities written out earlier.

Let us assume that G is a group with the identity $x^n \equiv 1$.

We have said earlier (3.5) that this group in general need not be finite. The groups defined by m generators and by this identity are denoted by $B(m,n)$. A proof of the infinity of the group $B(m,n)$, for sufficiently large prime n, given by S.I. Adyan and P.S. Novikov (cf. Novikov, Adyan, 1968), gave a negative solution to the so called *Burnside problem*. We point out however, that the questions of finiteness of the groups $B(2,5)$ and $B(2,8)$ are still open. On the other hand, we pose the following question. Let us assume that G is finite and satisfies the identity $x^n \equiv 1$. Is it true that the order is bounded above by a function $f(m,n)$ which does not depend on the groups?

This is the so called *restricted Burnside problem*. It has a positive solution.

Theorem 1. *For all m, n, there is a "universal" finite group $B_0(m,n)$, such that every other finite group with m generators, satisfying the identity $x^n \equiv 1$ is its homomorphic image (for even n, the theorem utilizes the classification of finite simple groups).*

Proof. Let us first consider the case when $n = p$ is a prime number. Let G is a finite group of period p. Than it is nilpotent and the Lie algebra $L(G)$ constructed by its lower central series is nilpotent of the same index. Magnus has shown (Magnus, 1950) that the *Engel identity* $(\text{ad } x)^{p-1} \equiv 0$ holds in $L(G)$. Consequently, by Theorem 2 of 6.5, its nilpotency index is bounded by some function, depending only on the number of generators, i.e. by the nilpotency index of a free Engel algebra. Then it is obvious that the order of G is bounded too, since the order of every factor $G^{(i)}/G^{(i+1)}$ is bounded. The case of arbitrary n is somewhat more complicated. First of all a Hall-Higman Theorem (Hall, Higman, 1956) reduces the matter to a prime power p^k, under the condition that there is only a finite number of simple groups of period n (the classification of simple groups is used exactly in this place). Secondly, already taking into account that $n = p^k$, in passing to $L(G)$, we obtain an algebra over the ring $\mathbb{Z}_{p^k}$, not over a field. In addition, it already does not have an Engel identity, thus we cannot use Theorem 2 from 6.5. Everything works out however, since E.I. Zel'manov has shown (Zel'manov, 1989) that, by the use of results of I.N. Sanov and Higman (Sanov, 1951), (Higman, 1960), it is possible to pass to Theorem 5 in 6.5. □

We point out that the nilpotency index of $B_0(m,n)$ is bounded below exponentially (Adyan, 1975), (Adyan, Razborov, 1987), (Adyan, Razborov, 1986). Using the construction of $L(G)$, Higman proved the following theorem, by the use of Theorem 1 of 6.5:

Theorem 2. *Let G be a locally nilpotent or a finite solvable group having an automorphism of prime order p such that it does not leave fixed any non-unity* *element. Then the group G is nilpotent and the nilpotency index is bounded by a constant dependent only on p.*

Let us now go to discussion of the problem of growth in groups. We say that a group is *almost nilpotent* if it contains a nilpotent subgroup of finite index.

Theorem 3. *A finitely generated group has a polynomial growth if and only if it is almost nilpotent.*

The growth of a nilpotent group equals $[n^d]$, where

$$d = \sum_k \dim_{\mathbf{Z}}(G^{(k)}/G^{(k+1)})$$

(Bass, 1972). Since the growth does not change after passing to a subgroup of finite index, the nontrivial part is the reverse implication, proved by Gromov (Gromov, 1981). It is sufficient to derive solvability from the polynomial growth, since the following holds:

Theorem 4. *The growth of a solvable group is alternative. If it is not exponential, then G is almost nilpotent.*

The proof is contained in the papers of Milnor (Milnor, 1968a) and Wolf (Wolf, 1968). An analogous result has been proved by Tits (Tits, 1972), for linear groups.

Theorem 5. *The growth of a finitely generated subgroup of a connected Lie group is alternative.*

We note also the following important result of S.I. Adyan (Adyan, 1975):

Theorem 6. *The growth of the burnside group $B(m,p)$, for $p \geqslant 661$ is exponential.*

This makes examples of groups of nonalternative intermediate growth, thought out by R.I. Grigorchuk (Grigorchuk, 1980, 1983, 1984a, 1984b, 1985) even more astonishing.

Theorem 7. *Let $\mathcal{R}$ be the set of all the forms of the growths $r(G)$ of all finitely generated groups G. Then*

a) *$\mathcal{R}$ contains a chain of continuum cardinality as well as an antichain (i.e. mutually incomparable forms of growth) of the same cardinality.*
b) *For every $r \in \mathcal{R}$ such that $r < [2^n]$, there exists an $r' \in \mathcal{R}$, such that $r < r' < [2^n]$.*

A continuum of groups of intermediate growth may be chosen in one of the following classes of groups:

1) Torsion free groups.
2) Groups without infinite factor groups.

3) With a continuum of non-isomorphic factor groups.
4) Finitely-approximable p-groups.
5) Groups with the unsolvable equality problem.
6) Amenable p-groups.

Immediate unions of several properties are possible also. On the other hand, Grigorchuk proved the following result:

Theorem 8 (Grigorchuk, 1989). *Let G be a finitely generated group approximable by finite p-groups. If the growth $r(G)$ is smaller than $[2^{\sqrt{n}}]$, then G is almost nilpotent.*

(We recall the definition of *approximation*. Let $\mathcal{K}$ be an arbitrary class of groups. It is said that a group G is approximable by the groups in $\mathcal{K}$, if G contains a family G_i of normal subgroups such that $G/G_i \in \mathcal{K}$ and $\cap G_i = e$. For instance, the *finitely approximable groups* are those that are approximated by finite groups.)

For the specified class of groups, this theorem is an extension of Gromov's theorem (Theorem 3).

Another interesting theorem has been proved in the same paper and we will need the following definitions in order to be able to discuss it.

Let G be a group, p – a prime number, let $\mathbb{Z}_p[G]$ be the group algebra and let Δ be its *fundamental ideal*, generated by the elements of the form $g-1$, where $g \in G$. The *Zassenhaus filtration* is the sequence of groups

$$G_n = \{g \in G \mid g - 1 \in \Delta^n\}.$$

The series $\{G_n\}$ is also called a *lower p-central series* and it has the following properties:

$$[G_n, G_m] \subseteq G_{n+m}; \quad G_n^p \subseteq G_{np};$$
$$G_n = \prod_{jp^i \geqslant n} (G^{(j)})^{p^i}.$$

If we construct the Lie algebra $L(G)$ by this series in the above-described fashion, then we will get the so-called Lie p-algebra (Kostrikin, 1986). We will be interested in its p-enveloping algebra A (definitions cf. in (Passi, 1979)). By Quillen's theorem (cf. (Passi, 1979)), this algebra may be written down explicitly as:

$$A = \bigoplus_0^\infty A_n = \bigoplus_0^\infty (\Delta^n/\Delta^{n+1})$$

with multiplication defined in a natural way through the representatives of conjugacy classes. The Hilbert series of the algebra A is equal to

$$\prod_1^\infty \left(\frac{1-t^{pn}}{1-t^n}\right)^{a_n},$$

where $a_n = \dim L_n$ (compare with the formula in 5.5, for the ordinary universal enveloping algebra $U(L)$).

Since the intersection $\cap G_n$ does not have any influence on the construction of the algebra A, we may assume that $\cap_1^\infty G_n = e$. This condition, together with the natural requirement $\dim A_1 < \infty$ is equivalent to the condition

$$|G/G_n| = |G/[G, G_{n-1}]G^p| < \infty$$

and implies approximability of G by finite p-groups (Passi, 1979). Under these assumptions, the following holds:

Theorem 9. *The following conditions are equivalent:*

a) *The growth of algebra A is polynomial.*
b) *G is an almost solvable group, representable by matrices over the ring of integer p-adic numbers.*
c) *The Lie algebra L, constructed by the series G_n is finite-dimensional.*
d) *The Hilbert series of the algebra A is a rational function of the form*

$$\prod_{i=1}^{l}(1-t^{n_i})^{-r_i}\prod_{j=1}^{s}\frac{1-t^{pc_j}}{1-t^{c_j}}$$

for some natural l, s, r_i, c_j.

e) *The growth of the indexes $(G : G_n)$ is polynomial.*

We point out that, when the conditions of the theorem are not fulfilled, the growth of A is not smaller than $[2^{\sqrt{n}}]$, by Theorem 1, however the superdimension 1/2 is attainable even in the class of finitely generated p-groups. We also point out that the commutator of a group which satisfies the conditions of Theorem 9, may not satisfy these same conditions (for all these details cf. also (Grigorchuk, 1989)).

6.7. Comments. We have seen that it is simply impossible to gather a complete list of all the combinatorial lemmas, thus we have restricted ourselves here to a portion related to questions of nilpotency. The Height theorem has analogues in other classes of algebras, near the associative ones (Bakhturin, Slin'ko, Shestakov, 1981), (Belov, 1988). A passage to superalgebras is rather interesting from a purely philosophical point of view. Apparently A.R. Kemer was the first to find out that tensoring by an exterior algebra not only transforms the starting algebra into a superalgebra, but also considerably improves its properties. Evidently, the same effect is produced here as in extending a field to an algebraically closed one, incidentally also with the aid of the tensor product (1.6).

The growth of groups is important also from the point of view of applications. For instance in geometry, the growth of the fundamental group is connected with the curvature (Milnor, 1968c), and, in probability theory, it is important that the probability of a turn of a random walk in a group is also connected to the growth of the latter (Grigorchuk, 1978). Gromov's paper

(Gromov, 1981) is a source of many deep ideas and deserves a special attention. We also point out a series of papers by V.I. Trofimov (Trofimov, 1983, 1984a, 1984b, 1985, 1986). They also discuss the growth of graphs, but the meaning of that definition is different: it is more of the growth of the group G of automorphisms acting transitively on the set of vertices of a connected, non-oriented graph Γ. More precisely, if $d(x, y)$ is a metric on Γ, defined by the minimal number of edges between x and y and if x_0 is a fixed vortex, then we can introduce the growth function ξ_d, for every automorphism $g \in G$. Set $\xi_g(n) = \max\{d(y, g(y)) \mid d(x_0, y) \leqslant n\}$. For an arbitrary function f, the set of those $g \in G$ for which ξ_d is $O(f)$, forms a normal subgroup of the group G. The series of papers (Trofimov, 1983, 1984a, 1984b, 1985, 1986) is exactly devoted to the construction of these groups, description of possible growth functions ξ_d, relations of the make-up of the graph with the behaviour of the group G, study of the growth of the number of vertices in the sphere of radius n and other questions.

§7. The Algebras of Polynomial Growth. The Monomial Algebras

7.1. Introduction. We have already seen in 6.6 that the polynomial growth imposes essential restrictions on the structure of a group. We will discuss in this section the role of the polynomial growth for algebras. We have shown in 6.4 that the polynomial growth is implied by the presence of an identity. Thus it is appropriate to study the structure of PI-algebras exactly in this section. Without taking on a task of duplicating a wonderful survey (Bakhturin, Ol'shanskij, 1988), we will refer to this paper in everything concerning the notions and methods, giving only a short list of necessary definitions, notation and facts. Moreover, we will restrict ourselves only to characteristics zero and we will leave in force the ordinary convention about the presence of unity in an algebra, although, for the PI-algebras, this is a sufficiently fundamental question. Besides the questions of asymptotic behavior we are interested in, we will state several new results, not included in (Bakhturin, Ol'shanskij, 1988), in the first place the results of A.R. Kemer.

We will also pay some attention to identities in semigroups, although the polynomial growth may not exist here. Finally, a considerable part of the section will be occupied by monomial algebras. We will demonstrate the full wealth in possibilities for the growth allowed in associative algebras, on their example. Study of the monomial algebras is also appropriate because the questions on Hilbert series of associative algebras reduce exactly to them (3.6).

The remaining part of the section will be devoted to the algebras with finite Gröbner basis as well as to classification of simple Lie algebras of polynomial growth.

7.2. PI-algebras. Basic Definitions and Facts. Thus, let the field have characteristic 0. Let $\mathcal{F} = K\langle X\rangle$ be a free associative algebra with countable number of variables. The element $f(x_1,\dots,x_m) \in \mathcal{F}$ is called an *identity* in an algebra A, if it turns into zero after substituting arbitrary m elements of A: $f(a_1,\dots,a_m) = 0, \quad \forall a_i \in A$. An algebra A with a non-trivial identity is called a PI-*algebra.* A class of algebras $\mathfrak{M}$ satisfying a given system of identities $\{f_i(x_1,\dots,x_{m_i}) \equiv 0,\ i \in I\}$ is called a *variety of algebras* defined by that system of identities. The set $T(\mathfrak{M})$ of all the identities of a given variety forms an ideal in $\mathcal{F}$, invariant with respect to all the endomorphisms of $\mathcal{F}$. Such ideals are called T-*ideals.* The set of all the identities of an algebra A is denoted by $T(A)$. The variety defined by the set $T(A)$ is denoted by Var A and is called the variety generated by the algebra A. Standard examples of varieties and their notations are as follows:

1) The variety $\mathfrak{A}$ of commutative algebras is defined by the identity $[x_1,x_2] \equiv 0$ and is generated by the ground field K.
2) The variety of nilpotent algebras with the nilpotency index not higher than c (see 6.5) is denoted by $\mathfrak{N}_c$ and is defined by the identity $x_1x_2\dots x_c \equiv 0$.
3) The variety $\mathfrak{L}_d$ corresponding to the left Lie nilpotency and defined by the identity $[x_1,x_2,\dots,x_{d+1}] \equiv 0$ (a left-normalized commutator).

Note that $\mathfrak{A} = \mathfrak{L}_1$ and that $\mathfrak{L}_2$ contains the exterior Grassmann algebra E of countable number of generators, which plays a distinguished role in the theory of PI-algebras.

4) The variety $\mathfrak{U}_c$ generated by the algebra of upper triangular matrices of order c, is defined by the identity

$$[x_1x_2][x_3x_4]\dots[x_{2c-1}x_{2c}] = 0.$$

If $\mathfrak{M}$ is a variety, then the quotient algebra $\mathcal{F}(\mathfrak{M}) = \mathcal{F}/T(\mathfrak{M})$ is called a (relatively) *free algebra of the variety* $\mathfrak{M}$. We may view it as an algebra defined by an infinite number of relations. A necessity arises, sometimes, to work with finitely generated free algebras $\mathcal{F}_m(\mathfrak{M}) \subset \mathcal{F}(\mathfrak{M})$, which are obtained from $\mathcal{F}(\mathfrak{M})$ with the aid of additional relations $x_i = 0$, for $i > m$. This notation may cause confusion with graduation. Thus, in a difference from previous sections, we will write the indices of the graduation on top as well as in parentheses. For instance $\mathcal{F}_m(\mathfrak{M}) = \bigoplus_{n=0}^{\infty} \mathcal{F}_m^{(n)}(\mathfrak{M})$. A more detailed graduation $\mathcal{F}_m(\mathfrak{M}) = \sum_{n_1,\dots,n_m} \mathcal{F}_m^{(n_1,\dots,n_m)}(\mathfrak{M})$, where the polyhomogeneous component $\mathcal{F}^{(n_1,\dots,n_m)}$ is the linear hull of all the words f such that $\deg_{x_i} f = n_i$, has been considered in the theory of PI-algebras. Clearly, some of those words may turn out to be linearly dependent in $\mathcal{F}_m(\mathfrak{M})$, however the definition remains correct since, in characteristic zero, every variety, and consequently any T-ideal, is defined by its *multilinear identities* i.e. by the identities of the form $\sum_{\sigma \in S_n} \alpha_\sigma x_{\sigma(1)} \dots x_{\sigma(n)} = 0$. If we denote by P_n the set of all the multilinear elements of degree n in $\mathcal{F}$, then it is well known that every variety is defined by its vector spaces $T(\mathfrak{M}) \cap P_n$, $n = 1, 2, \dots$. However, it is more suitable to study the quotient spaces $P_n(\mathfrak{M}) = P_n / T(\mathfrak{M}) \cap P_n$. The generating function of their dimensions $c(\mathfrak{M}, t) = \sum_n c_n(\mathfrak{M}) t^n$, $c_n = \dim P_n(\mathfrak{M})$ is called the *series of codimension* $\mathfrak{M}$. This series, together with the *generalized Hilbert series*

$$H(\mathfrak{M}, t_1, \dots, t_n) = \sum_{n_1, \dots, n_m} \dim \mathcal{F}_m^{(n_1, \dots, n_m)}(\mathfrak{M}) t_1^{n_1} \dots t_m^{n_m}$$

carries a valuable information about the free algebra of a variety, therefore about the variety itself too. We point out that the ordinary Hilbert series is obtained from the generalized one in an obvious way:

$$H_{\mathcal{F}_m}(t) = H(\mathfrak{M}, t, \dots, t),$$

thus we will call both of these series simply Hilbert series (sometimes they are also called Hilbert-Poincaré series).

Dependence of the series $H(\mathfrak{M}, t_1, \dots, t_{m+1})$ on the series $H(\mathfrak{M}, t_1, \dots, t_m)$, for sufficiently large m turns out to be fairly simple, since the following fundamental theorem is satisfied:

Theorem 1. *Every variety may be defined by a finite number of identities.*

This result by Kemer represents a solution of a famous problem of Specht (Kemer, 1987). An essential role in it was played by another theorem of Kemer (Kemer, 1984):

Theorem 2. *For every variety $\mathfrak{M}$, there exists a finitely generated superalgebra $A = A_0 + A_1$ such that*

$$\mathfrak{M} = Var\,(A_0 \otimes E_0 + A_1 \otimes E_1).$$

(We point out that the notion of superalgebra is somewhat wider here, since the possibility of a non-trivial intersection of the even and odd parts is allowed.)

It is not difficult to derive from it the following

Corollary. *For every variety $\mathfrak{M}$, there exists a positive integer n such that $\mathfrak{M} \subset Var\,(M_n(E))$. Here $M_n(E) = M_n(K) \otimes E$ is the matrix algebra.*

Definition. *Complexity* or the PI-*degree* of a variety $\mathfrak{M}$ is a maximal integer m such that $T(\mathfrak{M}) \subset T(M_m(K))$. In other words, m is the maximal dimension of the matrix algebra $M_m(K)$, lying in $\mathfrak{M}$. The *complexity of the algebra A* is the complexity of the variety it generates:

$$\text{PIDEG}(A) = \text{PIDEG}(\text{Var } A).$$

For instance PIDEG$M_n(E)) = n$.

Complexity is defined for all varieties. The varieties of complexity 1, i.e. those that have an identity not satisfied in $M_2(K)$, are called *non-matrix*. An example of such a variety is $\mathfrak{L}_2 = \text{Var } E$.

We can check (it is not trivial!) that the tensor product of PI-algebras is also a PI-algebra, and this defines the notion of the tensor product of varieties

$$\mathfrak{M} \otimes \mathfrak{N} = \text{Var } \{A \otimes B \mid A \in \mathfrak{M}, B \in \mathfrak{N}\}.$$

It turns out that the following estimate holds (Gateva-Ivanova, 1983):

Theorem 3. *For every two varieties $\mathfrak{M}$ and $\mathfrak{N}$, the following inequalities hold:*

$$1 \leqslant \frac{PIDEG\, \mathfrak{M} \otimes \mathfrak{N}}{(PIDEG\, \mathfrak{M})(PIDEG\, \mathfrak{N})} \leqslant 2.$$

On the other hand, since no identity of degree smaller than $2n$ holds in the matrix algebra $M_n(K)$, the complexity of every variety with an identity of degree d, does not exceed $\left[\frac{d}{2}\right]$.

We will note one more result by A.R. Kemer. Recall that a *standard identity* of degree n is

$$\sum_{\sigma \in S_n} (-1)^{sgn\, \sigma} x_{\sigma(1)} \ldots x_{\sigma(n)}.$$

Theorem 4. *A standard identity holds in a variety $\mathfrak{M}$ if and only if $\mathfrak{M} =$ Var(A), for some finite-dimensional algebra A* (Kemer, 1988).

We finish by giving a definition of the *product of varieties* $\mathfrak{M}$ and $\mathfrak{N}$ as the class of all the algebras A such that they have an ideal I satisfying all the identities in $\mathfrak{M}$ and such that the quotient mod I is in $\mathfrak{N}$ (we cannot say that $I \in \mathfrak{M}$, since we assumed the presence of the unity). For example, $\mathfrak{U}_c = \mathfrak{N}_c\mathfrak{A}$, since the T-ideal $T(\mathfrak{M}\mathfrak{N})$ is generated by all the elements of the form $f(h_1, \ldots, h_m)$, where $f \in T(\mathfrak{M})$, $h_i \in T(\mathfrak{N})$.

Corresponding definitions may also be introduced for Lie algebras, groups, Jordan algebras etc. (Bakhturin, Ol'shanskij, 1988).

7.3. Calculation of Hilbert Series and Series of Codimensions in Varieties of Algebras. The problem stated in this title is fairly non-trivial since it is difficult to explicitly give a basis in a free algebra of varieties. Here, one of the principal ideas is the use of representation theory of the symmetric group S_n. Recall that, to every partition $\lambda = (\lambda_1, \ldots, \lambda_n)$ of the number n, with the property that $\lambda_1 \geqslant \lambda_2 \geqslant \ldots \geqslant \lambda_k \geqslant 0$, $\sum \lambda_i = n$, $\lambda_i \in \mathbb{Z}$, there corresponds a uniquely defined S_n-module $M(\lambda)$, defined by the Young diagram $[\lambda]$, and that all the irreducible S_n-modules are exhausted by these. The group S_n acts on P_n by the rule $(\sigma f)(x_1, \ldots, x_n) = f(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$, where $f \in P_n$,

$\sigma \in S_n$. The module P_n is isomorphic to the group algebra $K[S_n]$ and, for every T-ideal $T(\mathfrak{M})$, the subspace $P_n \cap T(\mathfrak{M})$ is invariant with respect to this action, therefore the quotient space $P_n(\mathfrak{M}) = P_n/P_n \cap T(\mathfrak{M})$ inherits a structure of an S_n-module and can be decomposed into the sum of the irreducible ones:

$$P_n(\mathfrak{M}) = \sum_{\lambda} k(\lambda) M(\lambda), \quad k(\lambda) \in \mathbb{Z}.$$

It is obvious then that $c_n(\mathfrak{M}) = \sum k(\lambda) \dim M(\lambda)$ and we have a possibility of calculating codimensions with the aid of representation theory. Instead of considering representations of the symmetric group, we may consider representations of the general linear group GL_m too. Since the free algebra $\mathcal{F}_m$ with m generators is isomorphic to a tensor algebra (1.6), an action of GL_m is defined on it via the rule $g(f(x_1, \ldots, x_m)) = f(g(x_1), \ldots, g(x_m))$, $(f \in \mathcal{F}_m)$. This action in turn, carries over to the relatively free algebra $\mathcal{F}_m(\mathfrak{M}) = \mathcal{F}_m/\mathcal{F}_m \cap T(\mathfrak{M})$. Irreducible polynomial representations of GL_m are also connected with partitions. We will denote by $N_m(\lambda)$ the irreducible GL_m-module corresponding to the partition λ and we will denote by $S_\lambda(t_1, \ldots, t_m)$ the Schur function.

Theorem 1. *If $P_n(\mathfrak{M}) = \sum k(\lambda) M(\lambda)$, then $\mathcal{F}_m^{(n)}(\mathfrak{M}) = \sum k(\lambda) N_m(\lambda)$ and the Hilbert series is calculated by the formula*

$$H(\mathfrak{M}, t_1, \ldots, t_m) = \sum_{n,k} k(\lambda) S_\lambda(t_1, \ldots, t_m).$$

In reality, it is more suitable to work with the set of characteristic or commutator identities. Let

$$B_m = \left\{ f \in \mathcal{F}_m(\mathfrak{M}) \mid \frac{\partial f}{\partial x_i} = 0, \ i = 1, 2, \ldots, m \right\};$$
$$B_m(\mathfrak{M}) = B_m/B_m \cap T(\mathfrak{M})$$

and $\Gamma_m(\mathfrak{M}) = B_m(\mathfrak{M}) \cap P_m(\mathfrak{M})$; $\Gamma_m(\mathfrak{M}) = \Gamma_m/\Gamma_m \cap T(\mathfrak{M})$. Note that B_m is generated by the products of the commutators $[x_{i_1} \ldots] \ldots [\ldots x_{i_m} \ldots]$, which explains the name "commutator identities". If $\gamma_n(\mathfrak{M}) = \dim \Gamma_n(\mathfrak{M})$, then the generating function $\gamma(\mathfrak{M}, t) = \sum \gamma_n(\mathfrak{M}) t^n$ is called the *series of characteristic codimensions*. Let us also denote

$$H(B_m(\mathfrak{M}), t_1, \ldots, t_m) = \sum \dim B_m^{(n_1, \ldots, n_m)} t_1^{n_1} \ldots t_m^{n_m}.$$

Theorem 2. *The GL_m-modules $\mathcal{F}_m(\mathfrak{M})$ and $B_m(\mathfrak{M}) \otimes K[x_1, \ldots, x_m]$ are isomorphic. In particular, the following formulas hold:*

$$c_n(\mathfrak{M}) = \sum_{s=1}^{n} \binom{n}{k} \gamma_s(\mathfrak{M});$$

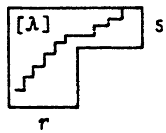
$$c(\mathfrak{M}, t) = \frac{1}{1-t} \gamma\left(\mathfrak{M}, \frac{t}{1-t}\right);$$

$$H(\mathfrak{M}, t_1, \ldots, t_m) = \prod_{i=1}^{m} \frac{1}{1-t_i} H(B_m(\mathfrak{M}), t_1, \ldots, t_m).$$

If $P_n(\mathfrak{M}) = \sum k(\lambda) M(\lambda)$ *and* $\Gamma_s(\mathfrak{M}) = \sum l(\mu) M(\mu)$*, then* $k(\lambda_1, \ldots, \lambda_m) = \sum l(\mu_1, \ldots, \mu_m)$*, where the summation goes over all the partitions* μ *such that*

$$\lambda_1 \geqslant \mu_1 \geqslant \lambda_2 \geqslant \mu_2 \geqslant \ldots \geqslant \lambda_m \geqslant \mu_m \text{ (Dicks, 1985).}$$

These technical theorems allow for calculations of necessary characteristics in smaller dimensions. We point out that, for every variety $\mathfrak{M}$, there exist numbers r and s such that all the Young diagrams participating in the decomposition of $P_n(\mathfrak{M})$ turn out to be enclosed in the following block:



A sufficiently large number of concrete results has been obtained through the use of the technique for calculation of possible sets with the aid of Young diagrams as well as through the use of special graphs (Drenski, 1974, 1981a, 1981b), (Drensky, 1984a, 1984b, 1985), (Drensky, Popov, 1987); we state a portion of them:

(i) Let us start with a simple case of the variety $\mathfrak{A}$ of commutative algebras. In this case, the decomposition of $P_n(\mathfrak{A})$ is trivial: $P_n(\mathfrak{A}) = M(n)$, therefore $c_n(\mathfrak{A}) = 1$ and $B_m(\mathfrak{A}) = K \Rightarrow$

$$H(\mathfrak{A}, t_1, \ldots, t_m) = \prod_{i=1}^{m} \frac{1}{1-t_i}.$$

(ii) The variety $\mathfrak{L}_2 =$ Var E. In this case, $\Gamma_{2n+1}(\mathfrak{L}_2) = 0$ and $\Gamma_{2n}(\mathfrak{L}_2) = M(1^{2n})$ (we will denote repeating numbers in a decomposition of λ by powers, thus $(1^{2n}) = (1, 1, \ldots, 1)$). Furthermore, $P_n(\mathfrak{L}_2) = \sum_{k=1}^{n} M(k, 1^{n-k})$, $c_n(\mathfrak{L}_2) = 2^{n-1}$. It is interesting that the growth of codimensions in every subvariety of $\mathfrak{L}_2$ is polynomial and that the relatively free algebra $\mathcal{F}(\mathfrak{L}_2)$ is embeddable in a free commutative superalgebra – a result of I.B. Volichenko.

(iii) The matrix variety $\mathfrak{M}_2 =$ Var $(M_2(K))$ is defined by two identities (this is fairly non-trivial – cf. (Drenski, 1981b), (Razmyslov, 1973a)): the standard one $S_4(x_1, x_2, x_3, x_4) \equiv 0$ and the identity $[[x_1 x_2]^2 x_1] \equiv 0$.

In this case, $\Gamma_n(\mathfrak{M}_2) = \sum M(\lambda_1, \lambda_2, \lambda_3)$, where $\lambda_1+\lambda_2+\lambda_3 = n$, $\lambda_2 \neq 0$ and $(\lambda_1, \lambda_2, \lambda_3) \neq (1,1,1)$.
Furthermore, $P_n(\mathfrak{M}_2) = \sum k(\lambda)M(\lambda)$, where

$$k(n) = 1;$$
$$k(\lambda_1, \lambda_2) = (\lambda_1 - \lambda_2 + 1)\lambda_2, \text{ for } \lambda_2 > 0;$$
$$k(\lambda_1, 1, 1, \lambda_4) = (\lambda_1 + 1)(2 - \lambda_4) - 1$$

and, for the other cases:

$$k(\lambda_1, \lambda_2, \lambda_3, \lambda_4) = (\lambda_1 - \lambda_2 + 1)(\lambda_2 - \lambda_3 + 1)(\lambda_3 - \lambda_4 + 1).$$

Finally

$$c(\mathfrak{M}_2, t) = \frac{1}{2t^2}(1 - 2t - \sqrt{1-4t}) - \frac{t^2}{(1-t)^4} + \frac{1}{1-t} - \frac{1}{1-2t};$$
$$H(\mathfrak{M}_2, t_1, t_2, t_3, t_4) = \frac{1 - t_1t_2t_3t_4}{\prod_{i=1}^{4}(1-t_i)^2 \prod_{i<j}(1-t_it_j)} -$$
$$\prod_{i=1}^{4} \frac{1}{(1-t_i)^2} + \left(1 - \sum_{i<j<k} t_it_jt_k\right) \prod_{i=1}^{4} \frac{1}{1-t_i}.$$

All the diagrams for $P_n(\mathfrak{M}_2)$ contain not more than four rows, which fully determines the Hilbert series in all cases. The exact formula is in (Le Bruyn, 1985).

(iv) If $\mathfrak{M}$ is defined by the standard identity $S_4(x_1, x_2, x_3, x_4) \equiv 0$, then $c_n(\mathfrak{M}) = c_n(\mathfrak{M}_2) + 5\binom{n}{5} + 5\binom{n}{6}$.

(v) If $\mathfrak{M}$ is defined by the Hall identity $[[x_1x_2]^2x_3] \equiv 0$, then $c_n(\mathfrak{M}) = 2^{n-1} + c_n(\mathfrak{M}_2) - 1 - \binom{n}{2} + 14\binom{n}{5} + 33\binom{n}{6} + 14\binom{n}{7}$, therefore, these varieties are sufficiently close to $\mathfrak{M}_2$.

(vi) Let $\mathfrak{G} = \text{Var}(E \otimes E)$. Then $\mathfrak{G}$ is defined by the following two identities: $[[x_1, x_2], [x_3, x_4], x_5] \equiv 0$, $[[x_1, x_2]^2, x_1] \equiv 0$. Furthermore $\Gamma_n(\mathfrak{G}) = \sum M(p, 2^q, 1^l)$, where the summation goes over all the decompositions of the form indicated, except (n) and (1^{2k+1}). Finally

$$c_n(\mathfrak{G}) = \frac{1}{2}\binom{2n}{n} + n + 1 - 2^n,$$

so that

$$c(\mathfrak{G}, t) = \frac{1}{2} + \frac{1}{2\sqrt{1-4t}} + \frac{t}{(1-t)^2} + \frac{1}{1-t} - \frac{1}{1-2t}.$$

If $\mathfrak{M}$ is defined only by the first of the two identities, then

$$c_n(\mathfrak{M}) = c_n(\mathfrak{G}) + 5\binom{n}{5} + 5\binom{n}{6}.$$

(vii) Let us describe a non-matrix variety with an identity of the fourth degree. Since $\Gamma_4 = M(3,1) + M(2^2) + M(2,1^2) + M(1^4)$, every characteristic identity of four variables is equivalent to one of the following:
a) $[x_2, x_1, x_1, x_1] \equiv 0$;
b) $[x_1 x_2]^2 \equiv 0$;
c) $[[x_1 x_2][x_3 x_4]] \equiv 0$;
d) $S_4(x_1, x_2, x_3, x_4) \equiv 0$.
The first three of them are non-matrix. The corresponding codimensions in every of the three cases are:

$$\text{a)} \quad c_n(\mathfrak{m}) = 2^{n-1} + 2\binom{n}{3} + 5\binom{n}{4} + 4\binom{n}{5};$$

$$\text{b)} \quad c_n(\mathfrak{M}) = 2^{n-1}(n-1) + 1 - \binom{n}{2} + 3\binom{n}{4} + 4\binom{n}{5};$$

$$\text{c)} \quad c_n(\mathfrak{M}) = 2^{n-1}(n-1) + 1 - \binom{n}{2} + 2\binom{n}{4}.$$

We formulate now a few general results.

Theorem 3. *The growth of codimensions is not greater than the exponential growth* (Regev, 1971) *(which, generaly speaking is not obvious, and for Lie algebras is not correct). It is interesting that for Lie algebras, the growth is smaller than exponential – it is polynomial* (S.P. Mishchenko).

Theorem 4. *Let $\mathfrak{M}$ be a subvariety in $\mathfrak{U}_c$. Then the Hilbert series $H(\mathfrak{M}, t_1, \ldots, t_m)$ is a rational function.*

Corollary. *Rationality of the Hilbert series is guaranteed by one of the following conditions:*
a) *The variety $\mathfrak{M}$ is non-matrix;*
b) *The codimensions $c_n(\mathfrak{M})$ have the polynomial growth.*

We point out that an analogue of this theorem as well as of its corollary are valid for Lie algebras. Much of it carries over to Jordan algebras too (cf. Drensky, 1984b).

For the variety $\mathfrak{L}_d$, the theorem may be refined by showing that its Hilbert series is of the form $H_m(\mathfrak{L}_d, t) = \frac{f(t)}{(1-t)^m}$, where $f(t)$ is a polynomial.

Many open and interesting questions remain in this subject and we may familiarize ourselves through (Drensky, Popov, 1987); we have followed the presentation in this paper which contains numerous references to the results mentioned here.

7.4. PI-algebras. Representability. T-primary and Non-matrix Varieties. The Equality Problem. A structure theory of T-ideals in the classical spirit has been constructed in (Kemer, 1984).

Definition. A T-ideal I is called *T-primary* if, for every two T-ideals not contained in I, their product is not contained in I either. A T-ideal is called *T-semiprimary* if, for every T-ideal J, the inclusion $J^n \subset I$ implies the inclusion $J \subset I$. A variety $\mathfrak{M}$ is called T-primary if its T-ideal $T(\mathfrak{M})$ is T-primary. A T-semiprimary variety is defined similarly.

Theorem 1. (i) *Every variety $\mathfrak{M}$ may be represented in the form $\mathfrak{M} = \mathfrak{N}_c\mathfrak{U} \cap \mathfrak{M}$, where $\mathfrak{U}$ is the greatest T-semiprimary subvariety of $\mathfrak{M}$. Equivalently, the free algebra $\mathcal{F}(\mathfrak{M})$ has a maximal nilpotent T-ideal.*

(ii) *The complexity of a variety is determined by its T-semiprimary part:* PIDEG ($\mathfrak{M}$) =PIDEG ($\mathfrak{U}$). *In addition, if $\mathfrak{M}' = \mathfrak{N}_{c'} \cap \mathfrak{M}'$ is a decomposition of another variety, then*

$$PIDEG\ (\mathfrak{M} \otimes \mathfrak{M}') = PIDEG\ (\mathfrak{U} \otimes \mathfrak{U}').$$

The structure of T-semiprimary varieties may be described explicitly. We mention that the union of varieties is the smallest variety containing both of them.

Let us define an algebra $M_{p,q}$ as a subalgebra of the matrix algebra over the exterior algebra $M_{p+q}(E)$ of the special form

$$\begin{matrix} & \overbrace{\phantom{a_{11}}}^{p} & \overbrace{\phantom{a_{12}}}^{q} \\ p\{ & a_{11} & a_{12} \\ q\{ & a_{21} & a_{22} \end{matrix} ,$$

where the elements of the blocks a_{11}, a_{22} are in $E_{\overline{0}}$ and the elements of the blocks a_{12}, a_{21} are in $E_{\overline{1}}$.

Theorem 2. *A variety $\mathfrak{U}$ is T-semiprimary if and only if it is the union of a finite number of T-primary varieties:*

A non-trivial variety is T-primary if and only if it is generated by one of the following algebras:

a) $M_n(K)$, $n \geqslant 1$;
b) $M_n(E)$, $n \geqslant 1$;
c) $M_{p,q}$, $p \geqslant q \geqslant 1$.

We point out that $T(E \otimes E) = T(M_{1,1})$; $T(M_{p,q} \otimes E) = T(M_{p+q}(E))$; $T(M_{k,l} \otimes M_{p,q}) = T(M_{kq+lp,kp+lq})$.

We see that, according to Theorem 1, every algebra of the variety $\mathfrak{M}$ has a nilpotent ideal such that the quotient mod that ideal lies in the T-semiprimary part of $\mathfrak{M}$. From this point of view, we cannot fail to mention a fundamental Kemer-Razmyslov theorem (Kemer, 1980b), (Razmyslov, 1974).

Theorem 3. *A finitely generated PI-algebra has nilpotent Jacobson radical $J(R)$ (a definition of the latter is in* (Bokut', L'vov, Kharchenko, 1988)).

Note that Braun generalized this theorem to the case of an arbitrary commutative Noetherian ring (Braun, 1982).

For finitely generated algebras, the question of their representability is also important.

Definition. An algebra A is called *representable* if it embeds isomorphically into the matrix algebra $M_n(C)$, over a commutative algebra C. If $J(A) = 0$ and if A is finitely generated or if it satisfies a standard identity, then A is representable (Bejdar, Latyshev, Markov, Mikhalev, Skornyakov, Tuganbaev, 1984).

Finitely generated right Noetherian PI-algebras (Anan'in, 1987) and relatively free algebras (Kemer, 1988) are representable. The following result has been proved by V.T. Markov (Markov, 1988).

Theorem 4. *A finitely generated representable algebra has integer Gel'fand-Kirillov dimension.*

If $\mathfrak{M}$ is a non-matrix variety, then we can define the non-matrix complexity to be the maximal n with the property that the algebra of upper triangular matrices $T_n(K)$ lies in $\mathfrak{M}$.

From this point of view, the following result, from the same paper, is important. $\overline{A} = A/J(A)$ will be the quotient mod the radical.

Theorem 5. *Let $\mathfrak{M}$ be a non-matrix variety. Then the following conditions are equivalent, for every n:*

a) $T_{n+1}(K) \in \mathfrak{M}$.
b) *For every finitely generated algebra $A \in \mathfrak{M}$ the following inequality holds:* $\operatorname{Dim} A \leqslant n \operatorname{Dim} \overline{A}$.

Corollary 1. $\operatorname{Dim} \mathcal{F}_m(\mathfrak{M}) = m \cdot \max\{n \mid T_n(K) \in \mathfrak{M}\} \quad (m \geqslant 2)$.

Corollary 2. *The following conditions are equivalent:*

a) $T_2(K) \notin M$.
b) *If A is a finitely generated algebra in $\mathfrak{M}$, then*

$$Dim\ A = Dim\ \overline{A}.$$

Corollary 3. *The following conditions are equivalent for a non-matrix variety $\mathfrak{M}$:*

a) $T_3(K) \in M$.
b) *Every finitely generated algebra in $\mathfrak{M}$ has integer Gel'fand-Kirillov dimension.*

We also note that for a right Noetherian PI-algebra A, $\operatorname{Dim} A = \operatorname{Dim} \overline{A}$.

We part with the PI-algebras, after formulating one more fresh result of M.V. Sapir (Sapir, 1989), related to the equality problem.

Since the equality problem is solvable in every finitely presented finitely approximable algebra, it follows from the results of A.Z. Anan'in (Anan'in, 1977), that the equality problem is solvable in the varieties satisfying the identities of the form

$$[x_1, \ldots, x_n][y_1, \ldots, y_m] = 0.$$

Examples of finitely presented algebras with unsolvable equality problem already exist in the varieties with the identity $[x_1x_2][x_3x_4][x_5x_6][x_7x_8] = 0$ (Kukin, 1983). Let $S = \langle a, b, c, d \mid bx = xa = c^2 = cdc = [c, d, d] = 0$, where x is any generator.

Theorem 6. *The equality problem is unsolvable in every variety containing the variety Var S and is solvable in any proper subvariety of this variety.*

Thus, we have the following scheme:

$$\begin{array}{ccc} \diagdown & \textit{Unsolvability} & / \\ & \textit{Var}S & \\ / & \textit{Solvability} & \diagdown \end{array}$$

A basis of identities of the variety Var S has been explicitly given in (Sapir, 1989). The following result has been obtained as a consequence: the equality problem is solvable in every variety satisfying the equality

$$[x_1, \ldots, x_n][y_1y_2][z_1, \ldots, z_m] \equiv 0,$$

but is not solvable if the middle commutator is replaced by a commutator of length 3: for all m and n the variety falls in the cone of "unsolvability".

The picture for Lie algebras is far more complicated (cf. the paper by Kharlampovich, 1989).

7.5. Varieties of Semigroups. We will state here the results of one of papers of M.V. Sapir (Sapir, 1987) who substantially used the series of combinatorial lemmas from 6.2. These results are related to varieties of semigroups. The majority of definitions here carry over from the theory of PI-algebras, hence we will formulate only the characteristic ones.

A semigroup is called *torsion* if its every singly generated subsemigroup is finite. A semigroup is called *locally finite* if its every finite subset generates a finite subsemigroup. A variety of semigroups is called torsion, if it consists of torsion semigroups and, locally finite, if it consists of locally finite semigroups. The main difficulty is in studying finitely generated infinite groups satisfying the identity $x^n \equiv 1$, for instance the groups $B(m, n)$ (6.6). We will call such groups the *groups of Novikov-Adyan type*.

We will also need the following definition. Let f be a word in the alphabet X and let ϕ be any homomorphism of free semigroups (without the unity). The value $\phi(f)$ is obtained simply by substitution of every letter $x \in X$ in f by the word $\phi(x)$ (cf. 6.2). A word w is called an *isoterm* for the identity $f = g$ if, for every ϕ, if $\phi(f)$ is a subword in w then $\phi(f) = \phi(g)$. For instance, the word $x_1^6x_2$ is an isoterm for $xyxy = yxyx$, since, every homomorphism ϕ such that $\phi(xy)^2$ is a subword of $x_1^6x_2$, must satisfy the condition $\phi(xy) = x_1^k$, so that $\phi(xyxy) = \phi(yxyx) = x_1^{2k}$. To the contrary, the word $\omega = x_1x_2x_1x_2x_3$ is not an isoterm, since we can use for ϕ the mapping sending x to x_1 and y to x_2. Then $\phi(xyxy) = x_1x_2x_1x_2$ is a subword in ω, but $\phi(yxyx) = x_2x_1x_2x_1 \neq \phi(xyxy)$.

We will call a word ω an *isoterm for the system of identities* Σ if, for every identity $f = g$ in Σ, the word ω is an isoterm both for $f = g$ as well as for $g = f$.

Finally, recall that $Z_{n+1} = Z_n x_n Z_n, Z_1 = x_1$.

Theorem 1. *Let $\mathfrak{M}$ be a variety of semigroups defined by a set of identities Σ in n variables, where $\mathfrak{M}$ is either not a torsion variety or it does not contain groups of Novikov-Adyan type. Then the following conditions are equivalent:*

a) *All torsion semigroups in $\mathfrak{M}$ are locally finite.*
b) *All the nilsemigroups in $\mathfrak{M}$ are locally finite.*
c) *For every m and k, all the semigroups with the identity $x^m = x^{m+k}$ $(k > 0)$ are locally finite.*
d) *The word Z_n is not an isoterm for Σ.*

Theorem 2. *Let $\mathfrak{M}$ be a variety of semigroups defined by a set of identities Σ of n variables. Then the following conditions are equivalent:*

a) *All the nilsemigroups from $\mathfrak{M}$ are locally finite.*
b) *All the semigroups from $\mathfrak{M}$ with the identity $x^2 = 0$ are locally finite.*
c) *The word Z_n is not an isoterm for Σ.*

Since the last condition in both theorems is algorithmic, we have effective algorithms for solutions of other questions. For instance, in the variety defined by identities $x^3 = y^3$ and $xyxz = xzxy$, every nilsemigroup is locally finite since, although no image $\phi(x)^3$ is a subword in $Z_3 = x_1x_2x_1x_3x_1x_2x_1$ and consequently it is an isoterm for the first identity, for the second identity, there exists the corresponding homomorphism $x \xrightarrow{\phi} x_1x_2$; $y \xrightarrow{\phi} x_1x_3$; $z \xrightarrow{\phi} x_1$, where $\phi(xyxz)$ is a subword in Z_3, but the image $\phi(xzxy)$ is not equal to it. At the same time, non-nilpotent finitely generated semigroups exist in the variety defined only by the first identity. (cf. also 6.2).

We state a series of corollaries. A paper of A.I. Zimin has been used in the first one (Zimin, 1980).

Corollary 1. *There exists an algorithm that determines, by an arbitrary finite collection of identities defining a non-torsion variety of semigroups $\mathfrak{M}$, whether every finitely generated semigroup in $\mathfrak{M}$ is finitely presented.*

Corollary 2. *Assume that in a variety of semigroups $\mathfrak{M}$, all the semigroups with the identity $x^2 \equiv 0$ are locally finite and that, for every n, the word Z_n is an isoterm for the identities of the variety $\mathfrak{M}$. Then $\mathfrak{M}$ does not have a finite basis of identities.*

This corollary shows that there is no analogue of Theorem 1 in 7.2.

Corollary 3. *Let all the subvarieties of the variety $\mathfrak{M}$ be with finite bases. Then all the nilsemigroups in $\mathfrak{M}$ are locally finite. If $\mathfrak{M}$ is not torsion or if it does not contain groups of Novikov-Adyan type, then all the torsion semigroups are also locally finite.*

Corollary 4. *A nilpotent group has a finite basis for semigroup identities if and only if it is either abelian or if it has a finite period.*

Corollary 5. *The word Z_n is an isoterm for the identities of a finite semigroup S, for all n, if and only if, every locally finite variety containing S has an infinite basis.*

7.6. The Automaton Monomial Algebras. We are beginning a study of *monomial algebras*. Let F be a set of words in a finite alphabet X, such that none of the words is a subword of another. The main object of our attention in 7.6 and 7.7 will be the algebra $A = \langle X \mid F \rangle$. Its defining relations are given by the conditions of the monomials (words) in F being equal to zero, which explains the term "monomial". It is most natural to start from the case when the set F is finite. It is however useful to consider questions, studied further in a wider context of automaton algebras (5.10), and we will constantly keep this in mind.

Thus, let F be a finite set and let $\hat{G}(A)$ be a graph constructed in accordance with Theorem 3, 5.7.

Theorem 1. *The following conditions are equivalent:*

a) *The algebra A has the polynomial growth.*
b) *The algebra A is a PI-algebra.*
c) *The algebra A is representable.*
d) *The graph $\hat{G}(A)$ does not have intersecting cycles* (Borisenko, 1985), (Ufnarovskij, 1982).

As a corollary we infer that the theorem is valid for other graphs of normal words too (5.7), (5.10). An analogue for the automaton monomial algebras also holds. We single out one special case. Let f be a non-periodic word of length n. Let us consider the infinite word f^∞ (6.1) as well as the algebra A_f where all the normal words are all the subwords of f^∞ and only those, whereas all the other words are equal to zero. It is easy to see that this algebra is defined by relations of degree not greater than n as well as that the graph $\hat{G}(A_f)$ consists of a unique cycle of length n. A less obvious is the following result of A.Ya. Belov (Belov, 1988).

Theorem 2. *The identities of the algebra A_f are exactly the identities of the matrix algebra:* $\mathrm{Var}\,(A_f) = \mathrm{Var}\,(M_n(K))$ *(this is true not only in characteristic 0, but for every infinite field).*

Thanks to this property, the algebras A_f may serve as main building blocks of "combinatorial" structure theory of algebras, fulfilling the role the matrix algebras have in the ordinary structure theory. Radical properties of the algebra A have been also described in the language of the graph $\hat{G}(A)$ in the papers of T. Gateva-Ivanova and V.N. Latyshev (Gateva-Ivanova, 1987), (Gateva-Ivanova, Latyshev, 1988). Let us call a word *cyclic*, if either its corresponding path is a part of some cycle of the graph, or when the length of the word is smaller than m ($m+1$ is the maximum of the lengths of words in F), then it is an end of some cyclic word of greater length.

Theorem 3. (i) *The Jacobson radical $J(A)$ of the algebra A is nilpotent and it is the linear hull of all the non-cyclic words. As an ideal, it is generated by non-cyclic words of length, not greater than m.*

(ii) *The algebra A is semiprimary if and only if it is semisimple (and this is, because of (i), equivalent to the condition that every edge of the graph is a part of some cycle).*

(iii) *The algebra A is primary if and only if we may get from any vertex of the graph to any other and every normal word of length smaller than m is the ending of a normal word of greater length.*

The reader will find in (Gateva-Ivanova, 1987), (Gateva-Ivanova, Latyshev, 1988), not only all the definitions and proofs but also the algorithms.

Example. The graph of the algebra $A = \langle x, y, z \mid xy, xz, yx, zx \rangle$ is

$$\hat{G}(A) = \overset{\curvearrowleft}{y} \rightleftarrows \overset{\curvearrowleft}{z}\ \overset{\curvearrowleft}{x}\ .$$

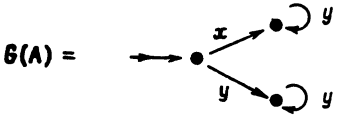
It is semisimple, but not primary, it has the exponential growth and is not a PI-algebra.

It is not difficult to formulate some analogues of the above theorem for the case of an arbitrary graph of normal words as well as for the automaton algebras, but in the general case, it is not possible to achieve such clarity.

The questions on Noetherian property are also easily solvable in monomial algebras.

Theorem 4. *A right Noetherian monomial algebra is an automaton. Its growth is polynomial, of degree not greater than one. If $G(A)$ is the graph constructed according to Theorem 3 in 5.10, then no edges come out of any cycle of its graph $G(A)$. Conversely, every automaton algebra with such a graph is Noetherian. (The left Noetherian property gives a symmetrical condition: there are no edges coming into a cycle* (Okniński, 1987), (Ufnarovskij, 1989a).

Example. The algebra $A = \langle x, y \mid x^2, yx \rangle$ is Noetherian from the right, but not from the left.



7.7. Finite Global Dimension. Radical and PI-properties of the Monomial Algebras. The following theorem is attributed to Anick (Anick, 1985b).

Theorem 1. *Let $A = \langle X \mid F \rangle$ be a monomial algebra of finite global dimension n. If A does not contain a free subalgebra of two generators, then A is finitely presented and has the polynomial growth of degree n and its Hilbert series is of the form $H_A(t) = \prod_{i=1}^{n}(1-t^{m_i})^{-1}$, for some $m_i \in \mathbb{N}$.*

Example. $A = \langle x, y \mid x^2y, xy^2 \rangle$. The Hilbert series is $H_A^{-1} = (1-t)^2(1-t^2)$.

By the use of this theorem, T. Gateva-Ivanova proved (Gateva-Ivanova, 1989b) the following:

Corollary. *Let A be an arbitrary graded algebra such that its associated monomial algebra $\tilde{A}$ (3.6) has finite global dimension n and the polynomial growth. Then*

a) $\mathrm{gl.dim}\, A = n =$ *the degree of the polynomial growth of A.*
b) *The Gröbner basis of the algebra A is finite.*
c) *The Hilbert series of H_A equals to $\prod_1^n(1-t^{m_i})^{-1}$, for some $m_i \in \mathbb{N}$.*

We note that all of the conditions of the corollary can be easily checked, by the use of the corresponding graphs (3.6), (5.7). Note also that there exist algebras of polynomial growth and finite global dimension whose associated algebras have infinite global dimension. An example of such an algebra is at the beginning of (2.6). It has a finite Gröbner basis and x^{n+1} is an n-chain for every n, thus gl. dim $\tilde{A} = \infty$. On the other hand, by a linear transformation of the basis, the relation may be reduced to the form $x'y' + \ldots$, thus, gl. dim$A = 2$, by the corollary.

We go on to the properties of monomial algebras connected with its various radicals (corresponding definitions are in (Andrunakievich, Ryabukhin, 1979)).We start with the following simple fact:

Theorem 2. *Let $u \in A$ be a homogeneous element of a monomial algebra. If $u^n = 0$, then the subalgebra of A generated by the words occuring in the decomposition of u with non-zero coefficients is nilpotent of index n.*

Proof. The subalgebra of the free algebra $K\langle X \rangle$ generated by those words is also free, because of homogeneity. This means that no products of n words in u cancel out and they are all equal to zero in A. □

Corollary. *A monomial nilalgebra is nilpotent.*

Proof. Take u to be the sum of all the generators. □

We point out that the theorem does not hold, without the homogeneity condition, which is shown by the example of the element $(a + bc - ab + c)$, whose cube equals zero in the algebra A_{abc} (7.6).

Let now S be a basis of normal words in A, which we will also consider as a semigroup (cf. 2.3). Our goal is to study how the radical properties of S and

A are connected. Let us denote by $\mathcal{N}(S)$ the greatest nilideal of S. Let $\mathcal{L}$, $\mathcal{B}$ and $\mathcal{J}$ denote the locally nilpotent Levitsky radical, the Baer radical and the Jacobson radical respectively, where we will apply the first two to semigroups as well. The following theorem is attributed to Okniński (Okniński, 1987):

Theorem 3. *The following relations hold:*

a) $\mathcal{L}(A) = K[\mathcal{L}(S)]$;
b) $\mathcal{B}(A) = K[\mathcal{B}(S)]$;
c) $\mathcal{J}(A) \subseteq K[\mathcal{N}(S)]$ *(the question about the equality is open);*
d) S *is (semi-)primary* $\iff$ A *is (semi-)primary.*

We say that a semigroup T has the *permutation property* $\mathcal{P}_n$ if, for any n elements $a_1, \dots, a_n$ there exists a non-identity permutation π, such that $a_1 a_2 \dots a_n = a_{\pi(1)} \dots a_{\pi(n)}$. For instance, if $K[T]$ is a PI-algebra, then it satisfies some standard identity S_n and thus $\mathcal{P}_n$ is satisfied in T. The reverse implication is not true, however. Nonetheless, it is true in the monomial case, which was proved in the same paper (Okniński, 1987).

Theorem 4. *An algebra A is a PI-algebra if and only if the semigroup S has the permutation property. In addition, $\mathcal{N}(S) = \mathcal{B}(S)$; $\mathcal{J}(A) = K[\mathcal{N}(S)]$ and the Gel'fand-Kirillov dimension* Dim $A/\mathcal{J}(A) \leqslant 1$. *In particular, the dimension* Dim A *does not exceed the nilpotency index of* $\mathcal{N}(S)$.

We single out one more characterization of PI-algebras (oral communication of A.Ya. Belov); it is equivalent to the Height Theorem.

He also announced that there exist presentable monomial algebras with a transcendental Hilbert series (however, cf. 7.4 and 7.6) as well as that the following holds:

Theorem 5. *Let A be a monomial PI-algebra. Then*

i) A *is primary* $\iff$ $A = A_f$, *for some word* f.
ii) A *is semiprimary* $\iff$ $A = A_{f_1, f_2, \dots, f_k}$, *where* $A_{f_1, \dots, f_k} = \langle X \mid F \rangle$, *and the set F consists of all the words that are not subwords of any of the infinite words* f_i^∞.

7.8. Examples of Growth of Algebras. Properties of the Gel'fand-Kirillov Dimension. We will give here examples of algebras of practically every growth. It is most suitable to demonstrate this on monomial algebras. Moreover, we will briefly discuss simple properties of the Gel'fand-Kirillov dimension. These properties are described deeper and in more detail in a monograph by Krause and Lenagan (Krause, Lenagan, 1985). We will also follow the presentation of a paper by Borho and Kraft (Borho, Kraft, 1976). At the beginning however, we give two examples by V.T. Markov, refuting some natural hypotheses (Markov, 1988).

Example. The algebra $A = \langle x, y \mid xy^m xy^n x;\ (m \neq n \geqslant 0), (xy^n)^{2n-1}; (n \geqslant 1)\rangle$ has a finite Gel'fand-Kirillov dimension (Dim $A = 3$), but its primary ideal is not nilpotent.

Example. The algebra A with the generators x, y and the relations $yx^m yx^n y = 0$, for all $m, n \geqslant 0$; $yx^n y = 0$, for a non-square $n \geqslant 1$, and $yx^n y = x^{2^n} y^2 x^{2^n}$, for n square, is weakly Noetherian, but Dim $A = \frac{5}{2}$ is not an integer (cf. 7.4).

We go on now to study growth.

Theorem 1. *Assume that the third derivative of a function f satisfies the condition $0 \leqslant f'''(x) \leqslant 1$, for $x > 0$. We assume also that its growth is greater than $[n^2]$ and that the function $\frac{f(n)}{n^2}$ is monotonous. Then there exists a monomial algebra A such that $r(A) = [f]$.*

Proof. Let $h(x)$ be the function inverse to $x - f''(x)$. Taking its integer part, we easily see that we get a monotonous function $g(n)$. The required algebra is defined in the following way:

$$A = \langle x, y \mid (AyA)^3 = 0, \quad yx^{g(m)-1}y = 0, \quad (m = 1, 2, \ldots)\rangle. \qquad \square$$

The details are in (Borho, Kraft, 1976).

Corollary. *There exists an algebra A for which $\underline{Dim}\, A \neq Dim\ A$. For every $d \geqslant 2$, there exists an algebra with the growth equal to $[n^d]$, thus the Gel'fand-Kirillov dimension can be any real number greater than two.*

Proof. For the first claim, it suffices to construct the corresponding function. The second is guaranteed by the following:

Theorem 2. *The growth of the tensor product of two finitely generated algebras equals to the product of the growths of the two algebras. The Gel'fand-Kirillov dimension has the following properties:*

a) $\max(Dim\, A, Dim\, B) \leqslant Dim\, A \otimes B \leqslant Dim\, A + Dim\, B$.
b) $Dim\,(A \oplus B) = \max(Dim\, A, Dim\, B)$.
c) $Dim\, A[x] = Dim\, A + 1$.
d) $Dim\, C \leqslant Dim\, A$, *for every subalgebra or a quotient algebra C of the algebra A.*
e) $Dim\,(A/I_1 \cap I_2 \cap \cdots \cap I_r) = \max_j Dim\, A/I_j$, *for some ideals I_j.*
f) $Dim\, S^{-1}A = Dim\, A$, *for localization at a multiplicatively closed central subset without nilpotent elements.*

Proof. If $A = \langle U\rangle$, $B = \langle V\rangle$, then $A \otimes B = \langle W\rangle$, where $W = U \otimes \mathbf{1} + \mathbf{1} \otimes V$ and $U^{(n)} \otimes V^{(n)} \subseteq W^{(2n)} \subseteq U^{(2n)} \otimes V^{(2n)} \Rightarrow r(A \otimes B) = r(A)r(B)$. Then, a) – d) are obvious and e) is their consequence, since the inclusion $A/I_1 \cap I_2 \subseteq A/I_1 \oplus A/I_2$ holds. Finally, if V is a finite-dimensional subspace generating $S^{-1}A$, then $sV \subseteq U^{(k)}$, for some $k \in \mathbb{N}$, $s \in S$, thus $V^{(n)} \subseteq s^{-n}U^{(kn)} \Rightarrow [d_V] \leqslant [d_U]$. $\square$

We point out that it would be erroneous to make a conclusion that the equality holds in the right-hand part in a) (although this error occurred in (Borho, Kraft, 1976)). The equality holds however, if $\operatorname{Dim} A = \underline{\operatorname{Dim}} A$, $\operatorname{Dim} B = \underline{\operatorname{Dim}} B$ (this and other interesting facts on the tensor product may be found in the paper by Krempa and Okniński (Krempa, Okniński, 1987)).

How small can the Gel'fand-Kirillov dimension be? It is zero for a finite-dimensional algebra and for a finitely generated, infinite-dimensional algebra it is not smaller than 1. Thus, it cannot be between zero and one. It is surprising that it cannot fall into the interval between 1 and 2 either. It follows from the following simple lemma of Bergman (cf. Krause, Lenagan, 1985):

Lemma. *If A is a monomial algebra in the natural graduation and $\dim A_m \leqslant m$, for some m, then $r(A) \leqslant [n]$.*

The simplest way to carry out the proof is with the aid of 5.6, considering the graph from Theorem 3 in 5.7. Another approach is to show explicitly that, for $k \geqslant m$, the number of normal words is not greater than m^2.

If, on the other hand, $\dim A_m > m$, for all m, then the growth is already not smaller than $[1 + 2 + \cdots + n] = \left[\frac{n(n-1)}{2}\right] = [n^2]$.

Reasoning as in 4.2, we may conclude that, for a fixed number of generators and relations and their powers, the question whether an algebra has the polynomial growth of the first degree is algorithmically solvable. A rather interesting is the question on the existence of a similar algorithm for answering the question on the polynomial or the exponential growth.

We go on to superdimension now.

Lemma. *Let $\mathfrak{M}$ be an infinite set of natural numbers $1 = m_1 < m_2 < m_3 < \ldots$ Let us denote by $P_{\mathfrak{M}}(n)$ the number of solutions of the equation $x_1 + \cdots + x_s = m$, where $s \in \mathbb{N}$, $x_i \in \mathfrak{M}$, $x_1 \leqslant x_2 \leqslant \ldots \leqslant x_s$; $m \leqslant n$. Let the limit $\lim_{k\to\infty} \frac{\log m_k}{\log k} = t$ exist. Then $\operatorname{DIM}[P_{\mathfrak{M}}] = \frac{1}{1+t}$.*

Example. If $\mathfrak{M} = \{[k^\alpha]\}$, then $\operatorname{DIM} P_{\mathfrak{M}} = \frac{1}{1+\alpha}$, $(\alpha \geqslant 1)$.

Theorem 3. *For every $\beta \leqslant \frac{1}{2}$, there exists a monomial algebra A, such that $\operatorname{Dim} A = \beta$.*

Proof. Define $\mathfrak{M}$ as in the example and consider $\alpha = \beta^{-1} - 1$, $A = \langle x, y \mid x^i y^{i-1} x^i, y^i x^{i-1} y^i \ (i > 1), xy^m x, yx^m y, (m \notin \mathfrak{M})\rangle$. Then it is not difficult to check that $[P_{\mathfrak{M}}] \leqslant r(A) \leqslant [m^2 P_{\mathfrak{M}}^2]$. □

We state a number of other results from (Borho, Kraft, 1976).

Theorem 4. *Let A be a commutative algebra. Then:*

a) *If A is finitely generated, then the dimension* $\operatorname{Dim} A$ *is an integer, coinciding with the Krull dimension, if A is finitely generated.*
b) *If I is a nilideal, then* Dim =Dim A/I.

Without commutativity both claims are false. The first is refuted by the Weyl algebra W_n (2.11). Its Krull dimension equals n and its Gel'fand-Kirillov dimension equals $2n$. A counterexample for the second one is the algebra A from Theorem 1, with the ideal I, generated by y.

Theorem 5. *Let I contain an element that is neither left nor right zero divisor. Then* $\mathrm{Dim}\, A/I \leqslant \mathrm{Dim}\, A - 1$.

Corollary. *Let $I_0 \subsetneqq I_1 \subsetneqq I_2 \subsetneqq \cdots \subsetneqq I_r$ be an ascending chain of non-primary ideals in a left Noetherian algebra. Then*

$$Dim\, A \geqslant r.$$

Theorem 6. *Let L be a finite-dimensional Lie algebra and let A be its universal enveloping algebra, with an ideal I of A. Then $n = \mathrm{Dim}\, A/I$ is an integer. Moreover, if L is a semisimple algebra over an algebraically closed field of characteristic zero and if I is primitive, then n is an even number* (cf. Borho, Kraft, 1976, for all the necessary definitions).

7.9. Finite Gröbner Basis and Strictly Ordered Algebras. We have already seen that the presence of a finite Gröbner basis implies many important properties. For instance we automatically know how to solve the equality problem, we know that the algebra has alternative growth and its Hilbert series (if the algebra is graded) is a rational function. How can one find out whether a given algebra have a finite Gröbner basis (algebras of this kind are sometimes called *standard finitely presented*)? As a matter of fact, even for fixed generators and relations, we do not know whether the process of constructing a Gröbner basis terminates or not. And what about if we are allowed to change the generators? We have already seen in the examples considered earlier (for instance $A = \langle x, y \mid xy = y^2 \rangle \cong \langle x, y \mid x^2 = yx \rangle$) that one algebra can have a finite Gröbner basis in one set of generators and not in another and besides, much depends on the choice of the order $>$. Is it possible that changing generators does not affect the automaton property (which is however unlikely, although the author does not know counterexamples)?

Nevertheless, let us assume, finally, that a finite Gröbner basis is given from the very beginning. Are there algorithms solving the question on the existence of zero divisors, on the Noetherian algebras or on other of its purely algebraic properties?

Finally, is it possible to introduce a notion of a Gröbner basis, for ideal I of an arbitrary algebra A, such as a commutative algebra, rather than only for the free algebra as we have done? If it is possible, then how and when is it finite?

This is only a small list of questions which could be extended substantially. We will give some partial answers in the sequel, some others may be found in (Golod, 1988), (Kandri-Rody, Weispfenning, 1987), (Mora, 1988, 1989), but on the whole, all of this subject is still at the formative level.

Let us discuss at the beginning, the question on a Gröbner basis of an ideal I in an arbitrary (not necessarily free) algebra A. Let N be a basis of normal words of the algebra A, that has been presented as a homomorphic image of a free algebra. For an arbitrary element u in the free algebra $\mathfrak{A}$, such that $A = \mathfrak{A}/J$, its normal form $\overline{u}$ modulo the ideal I has been defined in (2.3). Recall that we may assume that multiplication in A is given by the rule $f * g = \overline{fg}$, for $f, g \in N$. We may carry over to A the order $>$ from the free algebra $\mathfrak{A}$, since it is defined on the basis N of normal words. Thus, the notion of the leading word is defined in A and, as before it will be denoted by $\hat{u}$. Sometimes it will be suitable to represent the elements of A not only as linear combinations of normal words. In this case, we will use the operation $*$; for instance $f \hat{*} g = \hat{\overline{fg}}$.

In order to be able to talk about a Gröbner basis, starting from A, we need some restrictions on $>$, that are satisfied automatically in a free algebra.

Definition. We will call an algebra A *strictly ordered*, if the total order $>$, defined on its set of normal words N, satisfies the following conditions:

a) $0 < 1 < f; \quad (\forall f \in N \setminus \mathbf{1});$
b) $f < g \Rightarrow f * h < g * h, \quad h * f < h * g; \quad (f, g, h \in N);$
c) $\deg(f * g) = \deg f + \deg g; \quad (f, g \in n).$

Note that these conditions imply that A has no zero divisors. (Indeed, if f, g are normal words, then $f > \mathbf{1} \Rightarrow fg > g > 0$.)

The Weyl algebra, all the universal enveloping algebras (in particular the polynomial algebra $K[X]$ and the free algebra $K\langle X\rangle$) are examples of strictly ordered algebras.

Latyshev called these algebras algebras of the polynomial type in (Latyshev, 1982), which is justified by the following result of his:

Theorem 1. *Let A be a strictly ordered* PI-*algebra, where the order $>$ in A is inherited from the homogeneous lexicographic order in $\mathfrak{A}$. Then A is commutative.*

Now we can almost literally repeat the definition from 2.3.

Definition. Let I be an ideal in a strictly ordered algebra A. A set $B \subset I$ is called its *Gröbner basis* if, for every $u \in I$, there exists a $g \in G$, such that $\deg_{\hat{g}} u > 0$ (i.e. the leading word of u contains the leading word of g as a subword).

Algorithms for construction and use of Gröbner basis in strictly ordered algebras may be found in (Kandri-Rody, Weispfenning, 1987), (Mora, 1988, 1989). Sufficient conditions for the Noetherian property are obtained there too. The main condition imposed on algebras is the requirement of the existence of finite Gröbner basis of the form $x_j x_i - \alpha_{ij} x_i x_j - P_{ij}$ ($P_{ij} < x_i x_j$; $i < j$), for the algebra A (algebras of this type, with the condition $\alpha_{ij} \neq 0$, have been called the *algebras of solvable type* in (Kandri-Rody, Weispfenning, 1987)). It is obvious that they are strictly ordered.

Let A be a strictly ordered algebra whose order has been inherited from the homogeneous lexicographic order. Let us introduce the notion of equivalence on A: $f \sim g \iff$ the leading words coincide $\hat{f} = \hat{g}$. For example, in an algebra of solvable type, $x_j x_i \sim x_i x_j$, for any generators $x_1, \dots, x_n$, i.e. it is *almost commutative*. Let us assume that the generators are ordered like this: $x_n > x_{n-1} > \cdots > x_1$. Under these conditions, the following non-trivial result of Gateva-Ivanova (Gateva-Ivanova, 1989a) holds:

Theorem 2. *The following conditions are equivalent:*

a) *The word $x_n x_{n-1}$ is not normal.*
b) *The algebra A is almost commutative.*

Corollary. *Let $A = \mathfrak{A}/I$ be a strictly ordered algebra, where the ideal I is homogeneous and has a finite Gröbner basis. Then the following conditions are equivalent:*

a) *The algebra A is almost commutative.*
b) *The algebra A is left Noetherian.*
c) *The algebra A is right Noetherian.*
d) *The algebra A has the polynomial growth.*

When these conditions are satisfied, every two-sided ideal in A has a finite Gröbner basis.

Recall that the *Noetherian property* means that every ideal (left or right respectively) is finitely generated as a module. If every two-sided ideal is generated by a finite number of elements, then we speak of the *weak Noetherian property*.

7.10. Lie Algebras of Polynomial Growth. The growth of a Lie algebra shows rather substantially through its properties. See for instance a series of papers by A.A. Kirillov and his colleagues, where the properties of growth of Lie algebras of vector fields have been studied (Kirillov, 1989), (Kirillov, Kontsovich, Molev, 1983), (Kirillov, Ovsienko, Udalova, 1984) and others. It is interesting that, for instance, two vector fields on a line in a "general position" generate a Lie algebra of intermediate growth, i.e. for such algebras, the intermediate growth is not an exception, but rather a rule.

We would like to state without a proof (and even not in a very strict formulation), a result of Kac that shows how rigid the structure of a Lie algebra becomes under the requirement of the polynomial growth. The main object of our attention will be the $\mathbb{Z}$-graded Lie algebras, i.e. those of the form $L = \bigoplus_{-\infty}^{\infty} L_n$, where, as usual, $[L_i, L_j] \subseteq L_{i+j}$ and L_i are finite-dimensional. Firstly, we will be interested in *simple $\mathbb{Z}$-graded Lie algebras*, i.e. algebras without homogeneous ideals different from L and the algebra itself. Examples of such algebras are four Cartan series of Lie algebras of vector fields:

W_n, S_n, H_n, K_n (cf. definition in (Kac, 1968)). Note that all of them have the polynomial growth. There are also other examples.

Definition. Let $A = (\alpha_{ij})$ be the *generalized Cartan matrix* of dimension n, i.e. $\alpha_{ii} = 2, \alpha_{ij} \leqslant 0$ and $\alpha_{ij} < 0 \iff \alpha_{ji} < 0$ $(i \neq j)$. The *Kac-Moody algebra* $g'(A)$ is a complex Lie algebra with $3n$ generators e_i, f_i, h_i and the following relations:

$$[h_i h_j] = 0, \quad [e_i f_i] = h_i \quad [e_i f_j] = 0; \quad (i \neq j),$$
$$[h_i e_j] = \alpha_{ij} e_j, \quad [h_i f_j] = -\alpha_{ij} f_j; \quad (i, j = 1, \ldots, n),$$
$$e_j(\text{ad } e_i)^{1-\alpha_{ij}} = 0, \quad f_j(\text{ad } f_i)^{1-\alpha_{ij}} = 0; \quad (i \neq j).$$

The Kac-Moody algebras are divided into three non-intersecting classes. In order to describe them, it is suitable to assume that the matrix A is indecomposable, i.e. that it is impossible to break up the set $\{1, 2, \ldots, n\}$ into two non-intersecting subsets I and J, such that $a_{ij} = 0$, for every $i \in I$, $j \in J$. Under this assumption, there are three mutually exclusive possibilities:

a) There exists a column vector v with natural (i.e. positive integer) entries, such that all the entries of the vector Av are also positive. In this case, the Lie algebra $g'(A)$ is finite-dimensional and is isomorphic to one of the classical algebras $A_n - E_8$.
b) There exists a vector v with natural entries, such that $Av = 0$. In this case, the Lie algebra $g'(A)$ is infinite-dimensional, but of the polynomial growth. The algebras in this class are called *affine*.
c) There exists a vector v with natural entries, such that all the entries of Av are negative. In this case, the growth of $g'(A)$ is exponential.

Theorem 1. *Under certain technical restrictions, every simple $\mathbb{Z}$-graded Lie algebra of the polynomial growth is isomorphic either to one of Lie algebras in the Cartan series $\mathbb{H}_n, S_n, W_n, K_n$ or to a quotient over the center of an affine algebra.*

A strict formulation and proof are in (Kac, 1968); for more details on Kac-Moody algebras cf. (Kac, 1983) whose presentation in its introduction we followed.

7.11. Comments. We have discussed the questions about PI-algebras only in a rather limited scope. The details for Lie algebras may be found in the monograph (Bakhturin, 1985). We have touched upon semigroups only fragmentarily. The question about the equality $J(A) = K[\mathcal{N}(S)]$ for monomial algebras is still open and it is not even clear whether it is always possible to choose a basis of letters in $J(A)$. The algebras of small growth are of special interest (cf. for instance a result by A.T. Kolotov (Kolotov, 1981)). The Kac-Moody algebras are defined not only for complex numbers, but are mainly studied over algebraically closed fields of zero characteristic.

§8. Problems of Rationality

8.1. Introduction. One of the most powerful stimuli that contributed to the development of the theory connected with the Hilbert and Poincaré series had been posing the problems on rationality of the corresponding series. We formulate some of them.

1. The Kostrikin-Shafarevich problem (Kostrikin, Shafarevich, 1957). Is it true that the Poincaré series of a finite-dimensional nilpotent associative algebra (cf. 1.8) is always rational?
2. The Kaplansky-Serre problem (cf. Gulliksen, Levin, 1969 and Serre, 1965). Is it true that the Poincaré series of a commutative local Noetherian ring is always rational?
3. The Serre problem. Let X be a finite singly connected CW-complex. Is it true that its Poincaré series (cf. definitions in the sequel, 9.5) is always rational (Serre, 1965)?
4. The Govorov problem (Govorov, 1972). Is it true that the Hilbert series of a finitely presented graded algebra is always rational?

It turned out that these problems of rationality and others closely related to them are closely related with each other and that the series defined by each of the four classes of objects, are rationally expressible by the corresponding series of another class. In particular, since we have already seen that there exist finitely presented graded algebras with non-rational Hilbert series (cf. for instance 4.6; we will give simpler examples later, cf. 8.3), all of these problems are answered negatively. This and the following section will be devoted to establishing those relations. The next section is devoted to the series indicated in the first three problems, whereas in this section we consider other connections.

8.2. Rational Dependence. Formulation of the Fundamental Theorem

Definition. We call two series $H_1(t)$ and $H_2(t)$ *rationally dependent* if there are four polynomials $P_i(t), 1 \leqslant i \leqslant 4$, such that

$$P_4 P_1 \neq P_2 P_3$$

and

$$H_1 = \frac{P_1 H_2 + P_2}{P_3 H_2 + P_4}.$$

Rational dependence is obviously an equivalence relation and we will denote it by $H_1 \sim H_2$. Let $\mathcal{A}$ and $\mathcal{B}$ be two sets of formal series. We will say that $\mathcal{A}$ *rationally depends* on $\mathcal{B}$ (and denote it by $\mathcal{A} \to \mathcal{B}$), if every series in $\mathcal{A}$ is rationally dependent on some series in $\mathcal{B}$.

For example, it follows from Theorem 3 in 4.6 that, the set of the Hilbert series of a system of Diophantine equations rationally depends on the set of Hilbert series of the Roos algebras.

We have already considered several different types of series and their sets. In the first place these were the Hilbert and the Poincaré series. We will now considerably widen possible types of series, by introducing a number of new objects and their series. All of them have been enumerated in Fig. 1, which we have borrowed from (Anick, Gulliksen, 1985), with minor changes. All those objects will be discussed in the course of this and the next section, thus we will not give their definitions now, but rather only decipher the abbreviations:

g.a. – graded algebra
f.p. – finitely presented
f.g. – finitely generated
d.g.a. – differential graded algebra
c.d.g.a. – commutative d.g.a. (commutativity is meant in the graduated sense: $ab = (-1)^{|a||b|}ba$).

Fundamental Theorem. *All of the 18 sets of series in Fig. 1 rationally depend on each other, if the ground field is prime. For an arbitrary field, the 14 sets of series, not related to the complexes X are rationally dependent, i.e. all except L_X.*

A scheme of a proof is depicted in the diagram on the following page. Every arrow denotes rational dependence of one set on the other. References over and under an arrow indicate where the corresponding dependence had been proved and where it will be discussed. Obvious and undepicted arrows are dependencies of every small rectangle on all the small rectangles, placed above, that are a part of the same greater rectangle – it is simply the dependence of a subset on the whole set. For instance, it is obvious that the set of Hilbert series of quadratic algebras rationally depends on the set of all Hilbert series of f.p. graded algebras.

It is obvious from the diagram that this theorem is the result of work of vast number of mathematicians from different countries. The value of transition arrows is not only in the presence of exact formulas expressing one series through the other, but is also in the fact that many of the constructed correspondences have functorial character, thanks to which it was possible to connect many questions from perfectly different areas of mathematics and conversely, to carry over the results obtained, for instance for local rings, to finite complexes. It is clear that the size of this book does not allow us to have detailed proofs, but we will at least state the most important constructions and relations among the series, whereas the reader may use the references to study deeper any of the classes he is interested in. Throughout this and the next section we will be at the stage of proving the fundamental theorem, and in the course of discussion, many other results of independent value will be obtained.

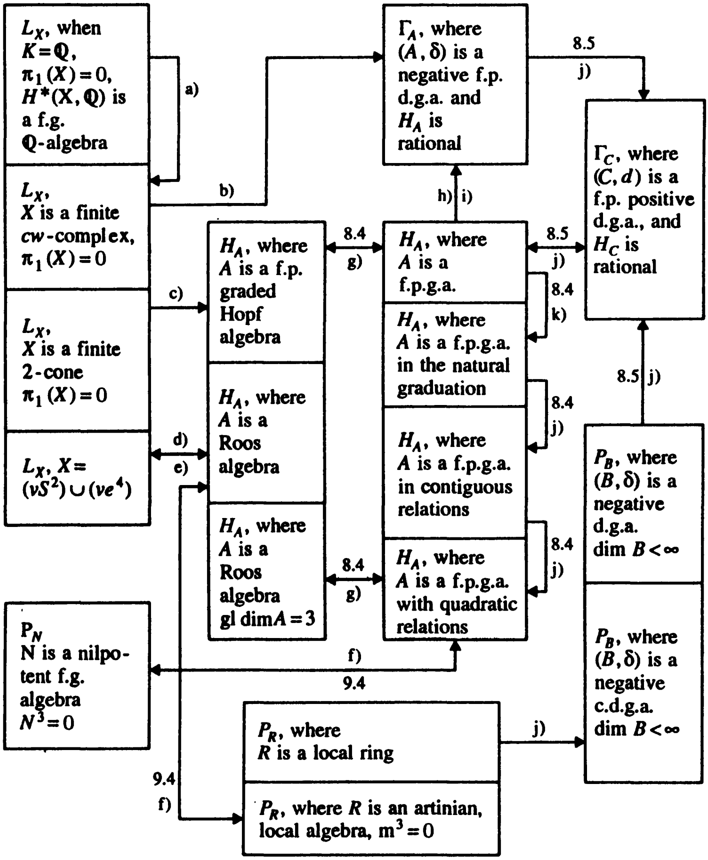


Fig. 1. a) (Halperin, Levin, 1986), b) (Adams, Hilton, 1955), c) (Lemaire, 1971), d) (Anick, 1984), e) (Roos, 1979), f) (Löfwall, 1979), g) (Jacobson, 1985), h) (Anick, 1982b), i) (Lemaire, 1982), j) (Anick, Gulliksen, 1985), k) (Anick, Löfwall, 1986)

8.3. Examples of Non-rational Series. Before we begin the proof of the fundamental theorem, we state the main consequences, the more so as exactly they were the main stimulus for its proof.

Theorem 1. *All the 18 sets of series enumerated in Fig. 1 contain series that are not rational functions (i.e. not representable in the form of a ratio of two polynomials).*

Proof. It is sufficient to give examples of non-rational series in one of those classes. We have already seen such examples in 4.6 (Theorem 4). It is useful however, to give also more explicit examples. The simplest of them is the universal enveloping algebra of a Lie algebra with the basis $e_1, e_2, \ldots$ and the multiplication $[e_ie_j] = (i-j)e_{i+j}$. We have seen at the end of 5.5, that its superdimension equals 1/2, hence, by the corollary in 5.4, its Hilbert series cannot be rational; moreover we know its exact form: $\prod_1^\infty(1-t^i)^{-1}$ – cf. 5.5. Thus, the only thing that remains to be done is to prove that the given Lie algebra is finitely presented, and thus the same will be true for its universal enveloping algebra. It turns out that the given Lie algebra is defined with only two relations. Its generators are e_1 and e_2 (we point out that $|e_2| = 2$, hence the graduation is not natural). If we now define e_k by induction as $e_{k+1} = \frac{1}{k-1}[e_ke_1]$ and impose two relations $[e_3e_2] = e_5$, $[e_5e_2] = 3e_7$, then it is not difficult to prove the equality $[e_ie_j] = (i-j)e_{i+j}$ by induction. □

Remark. The counterexample to problems in 7.1, constructed in the course of the proof, works only in characteristic zero, but there are other more complicated examples that do not depend on this premise, first of all an example by Shearer (Shearer, 1980), given by semigroup relations of second degree; historically, it was the first example of non-rationality of a Hilbert series of a finitely presented algebra. The first example of a finitely presented Hopf algebra was constructed by Anick (Anick, 1982b) and it deserves a separate study. We can also obtain examples of this kind by Theorem 4 in 4.5. Finally, in characteristic zero, we can construct infinitely many examples with the aid of universal enveloping algebras. For instance, the following holds:

Theorem 2. *Let $\mathfrak{L} = \bigoplus_{-1}^\infty \mathfrak{L}_m$ be one of Lie algebras of the Cartan series W_n, H_n, S_n, K_n* (cf. Kac, 1968), *and let $\overline{\mathfrak{L}} = \bigoplus_1^\infty \mathfrak{L}_m$ be its "nilpotent" part. Then $\mathfrak{L}$ and $\overline{\mathfrak{L}}$ are finitely presented Lie algebras. In particular, since they have the polynomial growth, their universal enveloping algebras have the intermediate growth* (Fejgin, Fuks, 1988), (Ufnarovskij, 1987).

Theorem 3. *For each of the 18 classes of objects, enumerated in Fig. 1, there is no algorithm that would give an answer to the following question (in a finite number of steps), for every object of that class and any series H: Is it true that the series corresponding to the given object (the Hilbert series, the Poincaré series etc.) equals to H.*

Proof. Since all the interrelationships among the series in the fundamental theorem are constructive, everything follows from Theorem 5 in 4.6. □

Understandably, we may strengthen this theorem, using the specifics of every class and make it more precise. For instance, for the case of local rings R with $\mathfrak{M}^3 = 0$, edim$R = g$, $\dim \mathfrak{M}^2 = r$, the problem of equality of the Poincaré series to the series $(1-gt+rt^2)^{-1}$ is algorithmically unsolvable and, as a corollary, the question whether it is true that $\mathrm{Ext}\,^1_R(K,K)$ generates $\mathrm{Ext}\,^*_R(K,K)$ is unsolvable (cf. 9.4). For CW-complexes X and their loop space ΩX, this leads to algorithmic insolubility of the question about the equality of their rational homotopic types, even if the complexes consist only of two-dimensional and four-dimensional cells. Finally, for the four-dimensional CW-complexes, it has been proved that there exists a recursive sequence c_n such that establishing the isomorphism $\pi_n(X) \otimes \mathbb{Q} \cong \mathbb{Q}^{c_n}$, for all n, is an algorithmically undecidable problem. All these details may be found in the foundational paper (Anick, 1985a).

8.4. Contiguous Sets. Quadratic Algebras. Relation with Hopf Algebras. Let us start a voyage along the figure 1. We will descend through the stories of rectangles corresponding to Hilbert series of finitely presented algebras and show how we can go down from an arbitrary algebra to a quadratic one and then we will establish connections with the rectangle of the Hopf algebra.

It would be possible to realize the descent from the highest story of an arbitrary graduation to the natural one, with the aid of Theorem 5 in 4.5, but since we have not given an explicit construction there, we will give a simpler, but less accurate way which does not preserve growth.

Lemma. *Let the algebra A have a generator x of degree $d > 1$. Let us consider the algebra B, where the generator x is replaced by d generators $t_1, \dots, t_d$ of degree 1, and in every relation, every occurrence of x is replaced by the word $t_1 t_2 \dots t_d$. Then*

$$H_B^{-1} = H_A^{-1} + t^d - dt.$$

Proof. The algebra B is obtained from A by introducing new generators as well as an additional relation $t_1 t_2 \dots t_d = x$. On the other hand, if we consider an order such that $t_1 t_2 \dots t_d > x$, then according to the Composition Lemma, the set of normal words is same as with the relation $t_1 t_2 \dots t_d = 0$. In this case, however, we have the ordinary free product of the algebra A and the algebra $\langle t_1, \dots, t_d \mid t_1 t_2 \dots t_d \rangle$. Now use 3.4 and 3.7. □

So called contiguous relations will have an auxiliary role in further descent to quadratic algebras.

Before going to the next story we first give a definition. Let $\mathfrak{A}$ be a free algebra with the set of generators X, in the natural graduation, let R be a set of homogeneous elements of degree $\geqslant 2$, let R_n denote those among them that are of degree n, let $|R_n|$ denote their number, let d denote a maximal number for which $|R_d| \neq 0$ and let I be the ideal generated by R.

Definition. We call a set R *contiguous* if, for every $2 \leqslant m < d$ the following equality holds:

$$\left(\sum_{n=m+1}^{d} R_n \mathfrak{A} \right) \cap \mathfrak{A}_m I = \sum_{n=m+1}^{d} R_n I. \tag{1}$$

Example. The set $vx - xw, xy, uxw$ is contiguous for $X = \{u, v, w, x, y\}$. Since $d = 3$, it is sufficient to check (1) for $m = 2$. Indeed, $(R_3 \mathfrak{A}) \cap \mathfrak{A}_2 I = (uxw\mathfrak{A}) \cap \mathfrak{A}_2 I = ux(w\mathfrak{A} \cap I) = uxwI = \sum_3^3 R_3 I$.

With the same set of generators, the set $vx - xw, xy, uvx$ will not be contiguous any more, since $(R_3\mathfrak{A}) \cap \mathfrak{A}_2 I \ni uvxy$, but $\sum_3^3 R_3 I = uvxI$ does not contain non-zero elements of degree 4. We point out that contiguity of relations of an algebra $\langle X \mid R \rangle$ is not its invariant, since for the two indicated sets, the corresponding algebras are isomorphic.

Every set of elements of second degree in the natural graduation is a contiguous set in an obvious way, since the possible m simply do not exist. By the same token, the lower story – the quadratic algebras are justifyably placed below the algebras defined by contiguous relations, i.e. the former rationally depend on the latter, as a subset. We will now make the reverse descent.

Theorem 1. *Let $A = \langle X \mid R \rangle$ be an algebra defined by a contiguous set of relations and g generators in the natural graduation. Then there exists a quadratic algebra B such that*

$$H_B = \frac{1}{1-t} H_A [1 + (g^2 + g^3 + \cdots + g^{d-1})t - \sum_{n=3}^{d} |R_n|(t^2 + t^3 + \cdots + t^{n-1})].$$

Proof. Let $X = \{x_1, \ldots, x_g\}$. For every m, denote by S_m the set of all the words of length m in the alphabet X. Set $S = \bigcup_2^{d-1} S_m$ and consider the set of symbols u_f enumerated by words in S. The new set of generators will be the union

$$\{u_f \mid f \in S\} \cup X \cup \{v\},$$

where the graduation is assumed to be natural, so that $|v| = |u_f| = 1$. Let us first construct a somewhat larger algebra C defined by that set of generators and the following set of defining relations:

$$u_f u_h = 0; \quad (f, h \in S); \quad x u_f = 0; \quad (x \in X, f \in S);$$
$$vx = 0; \quad (x \in X);$$
$$v u_{xy} = xy; \quad (x, y \in X \Rightarrow xy \in S_2)$$
$$v u_{hx} = u_h x; \quad (h \in S_m,\ 2 \leqslant m < d-1,\ x \in X \Rightarrow hx \in S_{m+1}).$$

It is not difficult to prove, with the aid of the Composition Lemma, that this is a complete set of relations, so that the set of normal words will consist of the words of the form fv^j and $u_h f v^j$ and that, as a graded space, C is isomorphic to $(K \oplus U) \otimes \mathfrak{A} \otimes K[v]$, where U is the space generated by all u_f. It is easy to prove that, for every word $f \in S_m$, $f = v^{m-1} u_f$, for $2 \leqslant m < d$ holds. Thus we can assign an element $y^* \in C_2$, to every $y \in \mathfrak{A}_m$, for $2 \leqslant m \leqslant d$, such that $y = v^{m-2} y^*$ (we give the exact formula: $(fx)^* = u_f x$, if $f \in S_{m-1}, x \in X$ and we must extend $*$ further by linearity).

We can also define the algebra B now: it is obtained from C by imposing additional conditions $y^* = 0$ $(y \in R)$. B is a quadratic algebra since $y^* \in C_2$

and it remains only to convince ourselves in regularity of computation of its Hilbert series. The details of this computation will be left to the reader (for references we can turn to (Anick, Gulliksen, 1985)) and we only note that we can easily compute the Hilbert series for C with the aid of Theorem 1 in 3.3, and that the main idea is in showing (using contiguity of the relations) that A embeds into B the same way as the free algebra $\mathfrak{A}$ embeds into C. □

The only step that remains to be done is the descent from stage of finitely presented algebras with the natural graduation, to the algebras with contiguous relations.

Theorem 2. *Let A be a finitely presented algebra with the natural graduation. Then there exists an algebra B, defined by a contiguous set of relations, such that*

$$H_B = (1 - gt)^{-2}(2 - H_A)^{-1},$$

where $g = \dim(\mathrm{Tor}_1^A(K, K))$ is the minimal number of generators of A.

Proof. Let $A = \langle X \mid R \rangle$. Let us consider two copies of the set X: X' and X'', as well as two copies of the free algebra: $K\langle X' \rangle$ and $K\langle X'' \rangle$. Let $V = \bigoplus_1^\infty A_n$. Let us consider the tensor graded algebra $T\langle V \rangle$ (cf. 1.6). Recall that $T\langle V \rangle$ is essentially a free algebra whose generators are words in the alphabet X, with the corresponding graduation.

As a graded vector space, the algebra B represents the tensor product $K\langle X' \rangle \otimes T\langle V \rangle \otimes K\langle X'' \rangle$, but the multiplication is defined differently: $(a' \otimes (f_1)(f_2)\dots(f_n) \otimes b'') \cdot (c' \otimes (g_1)(g_2)\dots(g_m) \otimes d'') = a' \otimes (f_1)(f_2)\dots(f_n c)(b g_1)(g_2)\dots(g_m) \otimes d''$, for $n, m \neq 0$. In addition, for $n = 0$, we set $(a' \otimes \mathbf{1} \otimes b'')(c' \otimes (g_1)\dots(g_m) \otimes d)'' = a'c' \otimes (bg_1)(g_2)\dots \otimes d''$ and analogously for $m = 0$. It is not too complicated to check the validity of the formula for the Hilbert series H_B, using computations in 3.3.

It turns out that the algebra B is finitely presented: its generators are the union of the three sets of generators: $X' \cup X \cup X''$ (naturally identified in B), and the relations are the following:

$$xy' = x''y; \quad x'y'' = y''x'; \quad (x, y \in X, x' \text{ is a copy of } x \text{ etc. });$$
$$\phi(r) = 0; \quad (r \in R),$$

where ϕ is the linear map $\phi : K\langle X \rangle \longrightarrow K\langle X', X, X'' \rangle$, defined by the rule $\phi(x_{i_1} \dots x_{i_n}) = x_{i_1} x'_{i_2} \dots x'_{i_n}$.

It is purely a technical matter to check this as well as contiguity of the relations; if desired we may familiarize ourselves about it in (Anick, Gulliksen, 1985). □

We point out that passage to the second Hilbert series in both theorems was accompanied by the loss of growth, but, while in Theorem 1, the polynomial growth turns into polynomial, in Theorem 2, the growth of B is always exponential, since B contains a free subalgebra.

We now establish dependencies among the Hilbert series of a Hopf algebra. The fact that the set of Hilbert series of a finitely presented Hopf algebras rationally depends on the set of the Hilbert series of finitely presented graded algebras is clear. Much less trivial and more important is the reverse dependence.

Theorem 3. *Let $A = \langle X \mid R\rangle$ be a finitely presented graded algebra with g generators and r relations. Then there exists a finitely presented Lie superalgebra $L = L(A)$, such that* gl.dim $U(L) \leqslant 3$ *(and the strict inequality is possible only for $r = 0$), and the Hilbert series of the universal enveloping algebra $U(L)$ equals*

$$H_{U(L)} = (1 - H_X)^{-2}(2 - H_A^{-1}).$$

If the algebra A has the natural graduation, then L and $U(L)$ also have natural graduations and the correspondence $A \longrightarrow U(L(A))$ is a covariant functor from the category of finitely generated algebras graded in the natural graduation into the category of Hopf algebras.

Proof. After noting that, in the natural graduation, the formula for the Hilbert series does not differ from the analogous formula in Theorem 2, we do not find it surprising that the construction too is made perfectly analogously.

Thus, let us make two copies X' and X'' of the set of generators. The set of generators of L as well as its universal enveloping algebra $U(L)$ will be the union $X' \cup X \cup X''$; as for generating relations, we consider the following: $[x'y''] = 0$; $[x', y] = [xy'']$ ($x, y \in X, x', y', y''$ are their copies); $\phi(r) = 0\,(r \in R)$, where ϕ is a linear mapping defined by $\phi(x_{i_1} \dots x_{i_n}) = [x'_{i_1}[\dots[x'_{i_n}x_{i_n}]\dots]]$. We emphasize that, since we are talking about Lie superalgebras, the commutators are assumed to be graded (cf. 1.1). Thus, there are exactly $2g^2 + r$ relations.

In principle, it is possible to repeat further the proof of Theorem 2.

The reader may try to do this by himself, however it should be noted that, in the original paper (Jacobson, 1985), the rest of the proof had been carried out in the spirit of homological algebra, with the aid of so-called Hochschild-Serre spectral sequence. □

Theorem 3 finalizes the dependencies between the rectangle of finitely presented algebras and the rectangle of Hopf algebras, both over the upper as well as the lower stories.

8.5. Differential Algebras. We will consider here all the dependencies in Fig. 1 related to the differential algebras, excluding their connections with local rings and complexes.

Definition. We will say that *differentiation* of degree $|d| = m$ is defined on a graded superalgebra A, if a linear map $d : A \longrightarrow A$ is defined, such that it maps every A_n into A_{n+m} and satisfies the condition

$$d(xy) = (dx)y + (-1)^{|d||x|}x(dy),$$

for all the homogeneous elements (Leibniz rule).

An example of typical differentiation is the map $\operatorname{ad} u, \operatorname{ad} u : x \to [ux]$, in a Lie superalgebra, for every element u. However, we will be interested primarily in the associative case.

Definition. A graded algebra A, together with a differentiation d (i.e. the ordered pair (A, d)) will be called *differential*, if $d^2 = 0$ (due to this, differentiation is often called a differential) and if the degree $|d|$ equals to ± 1. We will speak of a positive d.g.a., in the case $|d| = 1$ and of a negative one, in the case $|d| = -1$. In both cases we speak of commutative d.g.a. if, for all the homogeneous elements, the equality $xy = (-1)^{|x||y|}yx$ holds (the graded commutator equals to zero).

Example. Let the algebra A consist of differential forms of the first degree, i.e. of the expressions of the form $f(x)dx$, where $f(x)$ is a polynomial of one variable x, as well as of the forms of the zero degree, i.e. of polynomials $f(x)$ respectively. This algebra becomes commutative (both in the ordinary and in the graded case), if we set $(dx)^2 = 0$.

Defining the differential d by the natural rule $d : x \to dx$ and $d^2x = 0$, we arrive at the familiar rules of differentiation

$$d : f(x) \to f'(x)dx; \quad d : f(x)dx \to 0$$

and the structure of a (negative) differential algebra.

Example. The tensor product of two differential algebras (A_1, d_1) and (A_2, d_2) becomes a differential algebra, if the structure of the differential is defined by the following rule:

$$d(x \otimes y) = dx \otimes y + (-1)^{|x||y|} x \otimes dy.$$

Applying this to the previous example, we get the structure of a differential algebra on the set of differential forms in several variables. We emphasize that we have in mind here the graded tensor product of algebras, i.e. we assume that $(x \otimes y)(x' \otimes y') = (-1)^{|y||x'|}(xx' \otimes yy')$, so that we can view that set also as the tensor product of the polynomial algebra $K[x_1, \ldots, x_m]$ with the exterior algebra $\Lambda K[dx_1, \ldots, dx_m]$, where the differential is defined according to the following rules:

$$d(f(x_1, \ldots, x_m) \otimes \mathbf{1}) = \sum \frac{\partial f_i}{\partial x_i} \otimes dx_i; \quad d(\mathbf{1} \otimes dx_i) = 0.$$

Since the differential d displaces graduation, we will often suitably change graduation, for the homogeneity reasons; to this end, we introduce the following

Notation. If V is a graded vector space, then tV will denote the same space, but with a different graduation: $(tV)_0 = 0; \quad (tV)_{n+1} = V_n$. Obviously $H_{tV} = tH_V$.

We return to the study of differential algebras (A, d). $\operatorname{Im} d \subset \operatorname{Ker} d$, since $d^2 = 0$ and, since both of the spaces are graded, we may consider the graded quotient space $H(A) = \operatorname{Ker} d / \operatorname{Im} d$ and its generating function $\Gamma_A(t)$, obviously equal to $H_{\operatorname{Ker} d} - H_{\operatorname{Im} d}$, which we will call the *homological series* of the differential algebra (A, d). The meaning of the notion will be clarified, if we see a differential algebra as an algebra which is a complex at the same time:

$$0 \xleftarrow{d} A_0 \xleftarrow{d} A_1 \xleftarrow{d} A_2 \dots$$

(we have presented the case $|d| = -1$ here). Then, Γ_A is simply a generating function of the dimensions of the homologies H_n of this complex (cf. 1.8). We may consider one more point of view. The Leibniz rule shows that, since $\operatorname{Ker} d \cdot \operatorname{Ker} d \subset \operatorname{Ker} d, \quad \operatorname{Im} d \cdot \operatorname{Ker} d \subseteq \operatorname{Im} d$, the operation of multiplication, induced by multiplication on A is correctly defined on the set of homologies $H(A)$. The Hilbert series of the algebra $H(A)$ is exactly the homological series. Let us now establish some dependencies among different series.

Lemma. *Let (A, d) be a differential algebra. Then:*

$$H_{\operatorname{Im} d} = \frac{t}{1+t}(H_A - \Gamma_A),$$

for $|d| = 1$ and

$$H_{\operatorname{Im} d} = \frac{1}{1+t}(H_A - \Gamma_A),$$

for $|d| = -1$.

Proof. Let us for instance consider the case $|d| = -1$. By using the notation $t\operatorname{Im} d$, we may assume that the mappings $d : A \longrightarrow t\operatorname{Im} d$ are homogeneous, and then, according to 3.3, we have

$$H_A = H_{\operatorname{Ker} d} + tH_{\operatorname{Im} d}.$$

Subtracting from this equality, the equality $\Gamma_A = H_{\operatorname{Ker} d} - H_{\operatorname{Im} d}$, we get the desired result. □

Let us show now how to go from negative d.g.a. to the positive ones.

Theorem 1. *Let (A, δ) be a negative d.g.a. Then there exists a positive d.g.a., such that its Hilbert series is calculated by the formula*

$$H_C = \frac{H_A}{1 - t^2},$$

and the homological series by the formula

$$\Gamma_C = \frac{H_A}{1+t} + \frac{t}{1-t^2}\Gamma_A$$

(in particular, for rational H_A, we have $\Gamma_C \sim \Gamma_A$). Finite presentability of A is equivalent to finite presentability of C and the correspondence $(A,\delta) \longrightarrow (C,d)$ is functorial.

Proof. Define C to be $A \otimes K[y]$, stipulating the degree of y to be two. Then the formula $H_C = H_A(1-t^2)^{-1}$ immediately follows from the two theorems in 3.3. After defining the differential d by the rule $d(ay^n) = \delta(a)y^{n+1}$, for $a \in A$, we easily see that C becomes a positive differential algebra and we find that the image $\operatorname{Im} d$ is generated by the elements of the form uy^m, where $u \in \operatorname{Im}\delta, m \geqslant 1$. Consequently, according to 3.3,

$$H_{\operatorname{Im} d} = H_{\operatorname{Im}\delta} H_{\{y,y^2,y^3,\dots\}} = H_{\operatorname{Im}\delta} \cdot \frac{t^2}{1-t^2}.$$

After substituting both of the formulas from the lemma into the equality $(1-t^2)H_{\operatorname{Im} d} = t^2 H_{\operatorname{Im}\delta}$ and using the already calculated value for H_C, we easily obtain the desired equality for Γ_C. Functoriality is checked straightforwardly, after extending the homomorphism to y in the identity manner. □

Let us show now how to go from a positive d.g.a. of the homological series of a finitely presented algebra to the Hilbert series of a finitely presented algebra.

Theorem 2. *For every positive differential algebra (A,d), there exists a graded algebra $\tilde{A}$, such that*

$$H_{\tilde{A}} = (1+t)H_A + \frac{t(1+t)H_A^2}{(1+t)^2 - tH_A - t^2\Gamma_A}.$$

In addition, A finitely presented is equivalent to $\tilde{A}$ being finitely presented, just as A quadratic is equivalent to $\tilde{A}$ being quadratic. The correspondence $(A,d) \to \tilde{A}$ is functorial.

Proof. We take the set X of generators of the algebra A, together with two new generators, denoted by a and b, to be the generators of the algebra $\tilde{A}$. For the relations, we will take the whole set of relations R of the algebra A, together with the following relations:

$$a^2 = ab = ba = b^2 = 0 \text{ and } [ax] = d(x); \quad (x \in X)$$

Graduation of $\tilde{A}$ is ensured by the fact that $d(x) \in A_2$, for $x \in X$, and $\tilde{A}$ quadratic is ensured by A being quadratic, if we set $|a| = |b| = 1$. Note that $\tilde{A}$ may be seen as the free product of the algebras A and $K\langle a,b\rangle$, factored out by the new relations (cf. 3.4), which easily establishes the functoriality of the mapping $(A,d) \to \tilde{A}$. We emphasize, that the commutator $[ax]$ is assumed to be graded, as usual, thus the mapping $D : c \to [ac] - d(c)$ is a differentiation and therefore, the property $[a, c] = d(c)$, for $c \in A$ holds in the whole of the algebra A.

It remains to calculate the Hilbert series. To this end, we introduce some notation. Set $V = A/K \oplus \operatorname{Im} d$ and consider the vector space

$$M = A \oplus tA \oplus (A \otimes T(tV) \otimes tA),$$

where, as usual, T symbolises the tensor algebra. The main idea is to introduce an action of $\tilde{A}$ on M, turning the latter into a left module and then showing that it is cyclic and establishing its isomorphism with $\tilde{A}$ (as a graded space). We will leave the technical realization of this plan to the reader, directing him to (Anick, Gulliksen, 1985) for help.

Computation of the Hilbert series reduces to 3.3 and to the lemma. □

It remains to pass from finite-dimensional negative differential graded algebra and its Poincaré series to the homological series of a positive algebra.

Theorem 3. *For every finite-dimensional differential algebra* (A, δ), *there exists a finitely generated free positive d.g.a.* (C, d), *such that* $P_A = \Gamma_C$.

Proof. In fact, this is rather a question of defining of the Poincaré series of a differential algebra (it should be defined through the resolution in the corresponding category: all the modules should also have differentiation). Without going into details, let us say that the required resolution, in this case, will be a slightly modified bar resolution. For exact formulas and definitions, see (Anick, Gulliksen, 1985). □

We have not discussed only one connection: from the Hilbert series of graded algebras to the homological series of the negative differential algebras. Those who wish to see this connection explicitly, should turn to (Anick, 1982b) or to (Lemaire, 1982).

8.6. Comments. The fundamental theorem is a result of a colective effort of many mathematicians from different countries of the world. This can be seen already in the diagram, although the central organizational role of J.E. Roos should be emphasized; mainly thanks to his efforts a collective attack was organized, after it became clear that the problems of rationality were closely connected with each other. We can read about this also in (Anick, Halperin, 1985).

Note that there are no connections between growths. For instance, for the local rings, the growth is always alternative, whereas for the graded algebras and topological series, the growth is not alternative.

The aforementioned four problems have stimulated an immense number of investigations. It is practically impossible to encompass many sufficient conditions of rationality in one picture. Nevertheless, for the graded algebras, a greater portion of results has essentially been proved only for the automaton algebras. The unique large class, that is interesting from that point of view is the class of algebras with one relation, as long as it is not clear whether it is an automaton class of algebras.

A sufficiently large list of known results on rationality for local rings is given in 9.2.

§9. Local Rings. CW-complexes

9.1. Introduction. Recall that a commutative ring R is called *local* if it has a proper ideal $\mathfrak{M}$, containing all other proper ideals of R. The quotient ring $K = R/\mathfrak{M}$ is a field. As a rule, we will consider only Noetherian local rings, thus R will be tacitly assumed to be Noetherian everywhere in the sequel. Our approach to the local rings will be based on studying their Poincaré series P_R. It turns out that, given the context, it is most suitably studied through the functor Ext, since it is possible to introduce a structure of an algebra on the set $\operatorname{Ext}(K, K)$. Moreover, in reality it has the structure of a Hopf algebra that could be associated with the corresponding structure of a Lie superalgebra. The presence of the differential makes it possible to see this Hopf algebra as a differential algebra as well. Thanks to this fact, we can establish connections among various series that were discussed in the previous section. Finally, the case $\mathfrak{M}^3 = 0$ will play a specific role, since it will enable us to relate the Poincaré series of local rings, nilpotent algebras and topological series.

9.2. Regularity. Complete Intersection. Rationality. Let $K = R/\mathfrak{M}$. Note that, for every $n \geqslant 0$, the quotient $\mathfrak{M}^n/\mathfrak{M}^{n+1}$ is a vestor space over K. The dimension $\operatorname{edim} R = \dim_K \mathfrak{M}/\mathfrak{M}^2$ is called the *embedding dimension* and equals to the minimal number of generators of the ideal $\mathfrak{M}$ (as a module over R). The *dimension* $\dim R$ is a number n minimal with the property that there are n elements in $\mathfrak{M}$ such that the ideal generated by them contains some power $\mathfrak{M}^k$ of the ideal $\mathfrak{M}$. It is obvious that $\dim R \leqslant \operatorname{edim} \mathrm{R}$, but if these two dimensions coincide, the ring is called *regular*.

The multiplication in R induces a natural structure of an algebra in the associated ring $\operatorname{gr} R = \bigoplus_0^\infty \mathfrak{M}^n/\mathfrak{M}^{n+1}$. The Hilbert series $H_{\operatorname{gr} R} = \sum_0^\infty \dim_K(\mathfrak{M}^n/\mathfrak{M}^{n+1})t^n$ of this algebra is naturally also called the Hilbert series of the ring R and is denoted by H_R. We point out that the ring R itself, generaly speaking, may not be an algebra over K. Since $\operatorname{gr} R$ is a commutative algebra, its Hilbert series is of the form $H_R = f(t)/(1-t)^d$, where $f(t)$ is a polynomial with integer coefficients. The number d coincides with the dimension $\dim R$ of the ring R. Note that R regular $\iff \operatorname{gr} R \cong K[X]$.

Example 1. The ring of formal power series $K[[z]]$ is local and regular. Its ideal $\mathfrak{M}$ is formed by the series without the constant term (since all the other series are invertible). The ring associated to it is the polynomial algebra of one variable, thus its Hilbert series is $H_R = 1 + t + t^2 + \cdots = (1-t)^{-1}$.

Example 2. Let A be a commutative ring and let $\mathcal{P}$ be its prime ideal (i.e. the quotient over it does not have zero divisors). Let us consider the set of ordered pairs (f,g) where $f, g \in A, g \notin \mathcal{P}$, as well as the equivalence relation: $(f,g) \sim (f',g') \iff \exists h \notin \mathcal{P}$ with $h(fg' - f'g) = 0$. After denoting the equivalence classes by the symbols f/g, we may well define addition and multiplication on them:

$$f/g + f'/g' = fg' + f'g/gg'; \quad (f/g)(f'/g') = ff'/gg'.$$

In this way we obtain a local ring $A_{\mathcal{P}}$ called the *localization at* $\mathcal{P}$. For our purposees, it is important to note that if A is Noetherian, then $A_{\mathcal{P}}$ is also Noetherian. This example plays a rather important role in algebraic geometry. Let, for instance, X be an affine variety and let A be the ring of regular functions over it (cf. definition in Shafarevich, 1972). If $\mathcal{P}$ consists of all those functions which equal zero at the point $x \in X$, then $\mathcal{P}$ is a prime ideal and $A_{\mathcal{P}}$ is denoted by $\mathcal{O}_x$ and is called the local ring of the point x. The variety will be smooth if and only if all the local rings of its points are regular.

Regularity may be defined in a different way. Recall that the sequence of elements $x_1, \ldots x_n \in \mathfrak{M}$ is called *regular*, if x_i is not a zero divisor in $R/(x_1, \ldots, x_{i-1})R$, for $i = 1, 2, \ldots, n$ (assume $X_0 = 0$; $(x_1, \ldots, x_{i-1})R$ is the ideal generated by x_j, $j < i$). It turns out that a ring is regular if and only if its maximal ideal $\mathfrak{M}$ may be generated by a regular sequence.

Local rings have yet another structure. The fact is that the powers $\mathfrak{M}^k$ define the structure of a topological space on them: these powers are taken to be a base of the open neighbourhoods of zero. We may naturally consider completeness and completions in this topology. A deep statement holds: every complete local ring is a homomorphic image of a regular one; for details see (Zariski, Samuel, 1958, 1960). We emphasize that the passage to completion does not change basic characteristics of a ring: (non-)regularity, the dimension, the Poincaré series. Thus a standard beginning of many proofs is: "without loss of generality we may assume R to be complete".

The following definition singles out one more important class.

Definition. The ring R is called a (local) *complete intersection*, if its completion is a quotient of a regular ring, mod the ideal generated by some regular sequence.

These rings have originated in algebraic geometry (where they acquired the name, under geometric considerations). However, they turned out to be exceptionally important in homological algebra too, which will be seen somewhat later.

In general, if $(S, \mathfrak{N})$ is a regular ring such that, for some ideal I, the quotient ring S/I is isomorphic to the completion of R, then the number

$d(R) = \dim_K(I/\mathfrak{M}I) - (\dim S - \dim R)$ is called the *defect of the complete intersection* of the ring R. It is not difficult to prove that $d(R) \geqslant 0$, where the equality holds if and only if the ring is a complete intersection ring.

It turns out that these properties are fully characterized by the Poincaré series (Avramov, 1984a). Recall that the growth of R is the growth of the series P_R.

Theorem 1. *The growth of a local ring R is alternative. It is polynomial if and only if R is a complete intersection. In addition, R will be a regular ring if and only if P_R is a polynomial.*

Note that L. Avramov has proved even a little more: the Betti numbers are either given by polynomials or they are bounded below and above by powers, so that the radius of convergence of the Poincaré series is always positive.

It would appear that this theorem would allow for hope for rationality of the Poincaré series, but this is not the case, as we have already noted. Nonetheless it is appropriate to list a summary of results on rationality. Let us denote by depth R the maximal length of a regular sequence in the ideal $\mathfrak{M}$.

Rationality holds if one of the following conditions holds:

1) R is a complete intersection (Tate, 1957);
2) $\operatorname{edim} R - \dim R \leqslant 1$ (Shamash, 1969);
3) $\operatorname{edim} R - \operatorname{depth} R \leqslant 3$ (a series of authors who studied these rings, cf. (Avramov, Kustin, Miller, 1988); the last word was (Weiman, 1985));
4) $\operatorname{edim} R - \operatorname{depth} R = 4$ and R is Gorenstein (Jacobson, Kustin, Miller, 1985).

A more complete list is in (Avramov, Kustin, Miller, 1988).

In fact, more has been proved in (Avramov, Kustin, Miller, 1988). Let M be a finitely generated R-module. The series $P_R^M(t) = \sum_{i=0}^{\infty} b_i(M)t^i$ was called the *Poincaré series* of M (cf. 1.8).

Theorem 2. *Let R be any of the rings 1)–4) listed above and let M be any finitely generated R-module. Then, its Poincaré series $P_R^M(t)$ is rational.*

9.3. Koszul Complex. Let R be a local ring and let $x_1, x_2, \dots, x_m$ be a minimal generating set of $\mathfrak{M}$, so that $\operatorname{edim} R = m$; let $L = L^R = \Lambda R[X_1, \dots, X_m]$ be the exterior algebra over R of m generators $X_1, \dots, X_m$ (more precisely, it is a free R-module). Let us define the differential d on words by the following rule:

$$d(X_{i_1} \dots X_{i_r}) = \sum_{j=1}^{r} (-1)^j x_{i_j} X_{i_1} \dots \hat{X}_{i_j} \dots X_{i_r},$$

where the little hat denotes that the marked factor is omitted; for instance

$$d(X_2X_3) = -x_2X_3 + x_3X_2.$$

It is easy to see that $d^2 = 0$. Thus L becomes a complex, called the *Koszul complex* (1.8). In fact, L is a negative differential graded algebra (cf. 8.5), not over the field K, but over R. On the other hand, the homology algebra $H_*(L)$ is the already existing graded algebra over K.

It turns out that many properties of the ring R may be characterized in terms of the Koszul complex. Let $c_i = \dim_K H_i(L)$, so that $\sum c_k t^k$ is the Hilbert series of the algebra $H_*(L)$.

Theorem 1. i) *The ring R is regular if and only if $c_1 = 0$. In this case, L is a minimal R-free resolution (3.9), hence* $\mathrm{Tor}_*^R(K,K) = H(K \otimes_R L) = K \otimes_R L = \Lambda K[\mathrm{Tor}_1^R(K,K)]$.

ii) *The ring R is a complete intersection if and only if $H_2(L) = [H_1(L)]^2$.*

iii) *Let $R = S/I$, where $(S, \mathfrak{N})$ is a regular ring and* $\dim S = n$. *Then $c_1 \geqslant n - \dim R$, where the equality holds if and only if R is a complete intersection. Note that R is called an almost complete intersection, if $c_1 = n - \dim R + 1$.*

iv) *The defect $d(R)$ of the complete intersection equals*

$$c_1 - \operatorname{edim} R + \dim A$$

((Tate, 1957), (Auslander, Buchsbaum, 1957, 1958), (Babenko, 1986a)).

Theorem 2 (Serre, 1965). *Let R be a local ring and $n =$* edim R. *Then the following inequality for the series holds:*

$$P_R(t) \leqslant \frac{(1+t)^n}{1 - \sum_{i=1}^n c_i t^{i+1}}.$$

The rings, where the equality holds are called the Golod rings (he proved that the equality holds if and only if $H_*(L)$ has a zero multiplication and the so-called ternary Massey operations equal to zero too (Golod, 1962)*).*

This theorem enables us to estimate the radius of convergence of the series P_R, when necessary.

Another similar condition was obtained in (Avramov, Lescot, 1982). The following dimensions are called the Bass numbers of a local ring R:

$$\mu_i(R) = \dim_K \mathrm{Ext}_R^i(K, R).$$

Let

$$I_R(t) = \sum \mu_i t^i$$

be the corresponding generating function.

Theorem 3. *The following inequality holds, for every non-regular ring R of embedding dimension $n =$* edim R:

$$I_R(t) \leqslant \frac{\sum_{i=0}^{n-1} c_{n-i} t^i - t^{n+1}}{1 - \sum_{i=1}^n c_i t^{i+1}}.$$

The equality holds if and only if R is a non-regular Golod ring.

Lescot's paper (Lescot, 1985) is devoted to the asymptotic behavior of the Bass numbers $\mu_i(M) = \dim_K \mathrm{Ext}_R^i(K, M)$, for an arbitrary module M. Another of his papers (Lescot, 1986) is devoted to the syzygy module.

Another application of the Bass numbers is the following. A ring R is called a *Gorenstein ring*, if it has a finite injective resolution. It is a natural generalization of the notion of complete intersection. It is interesting that the rationality of the Poincaré series fails already in the class of the Gorenstein rings. However, the following holds:

Theorem 4. *The ring R is Gorenstein* $\iff I_R(t) = t^n$.

9.4. Nilpotent Algebras and Rings with the Condition $\mathfrak{M}^3 = 0$. Let N be a finite-dimensional nilpotent algebra of index $\leqslant 3$. Our goal is to study its Poincaré series P_N and to learn better the structure of its Yoneda algebra $E = \operatorname{Ext}^*_{\tilde{N}}(K, K)$ (cf. definitions in 1.8).

If $N^2 = 0$, it is easy to see that E is a free associative algebra, generated by the set $W = \operatorname{Ext}^*_{\tilde{N}}(K, K)$, while the converse is true too. In general, the subalgebra E^1, generated in E by W, does not necessarily coincide with E (more details about this, somewhat later). Thus, let $N^3 = 0$.

Multiplication in N defines a mapping $\phi : V \otimes V \longrightarrow N^2$, where $V = N/N^2$, by the rule $(a + N^2) \otimes (b + N^2) \to ab$. Let us consider the conjugate mapping $\phi^* : (N^2)^* \longrightarrow (V \otimes V)^* = V^* \otimes V^*$ and let $A(N)$ be the algebra obtained from the tensor (thus also the free) algebra, factoring out by the ideal generated by the image $\phi^*((N^2)^*)$. It is a quadratic algebra, since $\operatorname{Im} \phi^* \subset V^* \otimes V^*$. The mapping indicated is invertible.

Let A be a quadratic algebra. Then it may be represented in the form $A = T(V)/(F)$, where $F \subset V \otimes V$. Set $\tilde{F} = \{f \in V^* \otimes V^* \mid f(F) = 0\}$ and $V^* = Hom(V, K)$. Then $N(A) = T(V^*)/(\tilde{F} \oplus V^* \otimes V^* \otimes V^*)$.

Theorem 1 (Löfwall, 1979). *The mappings $A \to N(A)$ and $N \to A(N)$ are mutually inverse and they map isomorphic algebras into isomorphic ones. Moreover, the following relation, between the Hilbert series of the quadratic algebra A and the Poincaré series of the corresponding nilpotent algebra N, holds:*

$$P_N^{-1}(t) = (1 + t^{-1})H_A^{-1}(t) - t^{-1}H_N(-t).$$

Example. Let $N = \langle x, y \mid x^2 = y^2, xy = 2yx, y^2x = y^3 = 0\rangle$. It can be checked by the Composition Lemma that this is a complete system of relations, thus $N^3 = 0$. We define the mapping ϕ as follows: let $\{x, y\}$ (we use same symbols) be a basis in $V = N/N^2$. Then ϕ is defined by the correspondence:

$$\phi : \begin{cases} x \otimes x \to y^2; \\ x \otimes y \to 2yx; \\ y \otimes x \to yx; \\ y \otimes y \to y^2. \end{cases}$$

If we use an asterisk for the dual elements, then

$$\phi^* : \begin{cases} (y^2)^* \to x^* \otimes x^* + y^* \otimes y^*; \\ (yx)^* \to y^* \otimes x^* + (1/2)x^* \otimes y^*. \end{cases}$$

Consequently $A(N) \cong \langle a, b \mid a^2 + b^2, ab + (1/2)ba \rangle$.

Since the Hilbert series of a finite-dimensional algebra N is a polynomial, we have established one of the connections indicated in Fig. 1.

What do we get in application to the local rings with $\mathfrak{M}^3 = 0$ – another rectangle in our picture? First of all, Levin has shown that $P_R = P_{\mathrm{gr}\, R}$ and Löfwall has shown that the subalgebras generated by $\mathrm{Ext}^1_R(K, K)$ and $\mathrm{Ext}^1_{\mathrm{gr}\, R}(K, K)$ in $\mathrm{Ext}^*_R(K, K)$ and $\mathrm{Ext}^*_{\mathrm{gr}\, R}(K, K)$ respectively are isomorphic. Hence we may use the previous theorem. Even a stronger result holds (Löfwall, 1986):

Theorem 2. *Let R be a local ring with $\mathfrak{M}^3 = 0$ and let E^1 be a subalgebra of the Yoneda algebra $E = \mathrm{Ext}^*_R(K, K)$, generated by $\mathrm{Ext}^1_R(K, K)$. Then*

(i) *In the correspondence $R \to \mathrm{gr}\, R \to A(\mathrm{gr}\, R)$, from the previous theorem, the Roos algebras correspond to the commutative nilpotent algebras, so that the following formula holds:*

$$P_R^{-1}(t) = (1 + t^{-1})H_{E^1}(t) - t^{-1}H_R(-t).$$

(ii) *$E = E^1$ if and only the Fröberg formula holds: $P_R(t)H_R(-t) = 1$.*

Note that the Roos algebras are a special case of the Hopf algebras (1.7) and that we have established one more connection in Fig. 1.

Example. Let R be a local ring defined by the relations $\langle x_1, x_2, x_3, x_4, x_5 \mid x_1^2, x_2^2, x_3^2, x_5^2, x_1x_2, x_3x_5, x_1x_3 + x_2x_4 + x_4x_5, \mathfrak{M}^3 \rangle$.

The corresponding Roos algebra will be the universal enveloping algebra for the following Lie superalgebra:

$$L = \langle T_1, T_2, T_3, T_4, T_5 \mid T_4^2, [T_4T_2] - [T_4T_5], [T_4T_2] - [T_1T_3], \\ [T_1T_4], [T_1T_5], [T_2T_3], [T_3T_4], [T_2T_5] \rangle; \quad (|T_i| = 1).$$

We can check that the Hilbert series $H_{U(L)}$ is not rational, and then the same is true for P_R (Löfwall, Roos, 1980)

We point out that from the point of view of questions on rationality, everything reduces to nilpotent rings, since the following holds:

Theorem 3 (Levin, 1975). *For every local ring R, there exists an integer n, such that, for all $k \geqslant n$:*

$$P_R^{-1}(t) = P_{R/\mathfrak{M}^k}^{-1}(t) + (-1)^k t^{2-k} H_R(-t)|_{\geqslant k},$$

where

$$H_R(t)|_{\geqslant k} = \sum_{i \geqslant k} \dim_K(\mathfrak{M}^i/\mathfrak{M}^{i+1})t^i.$$

9.5. Hopf Algebras, Differential Algebras and CW-complexes. We have seen in 9.4, that it was possible to relate naturally a Lie superalgebra with a local ring with $\mathfrak{M}^3 = 0$. This connection is not accidental. It turns out that, for a local ring R, its Yoneda algebra $\mathrm{Ext}^*_R(K, K)$ may be equipped with the structure of a Hopf algebra (Gulliksen, Levin, 1969) with divided powers, thus Theorem 2 from 1.7 holds as well as its analogue for finite characteristic, and the following holds:

Theorem 1. *For a local ring R, the Yoneda algebra $\mathrm{Ext}^*_R(K, K)$ is a universal enveloping algebra of the uniquely determined Lie superalgebra $\pi_*(R)$.*

We will call this Lie superalgebra the *algebra of homotopic groups of a local ring.* This term is dictated by considerations in differential geometry and topology (we will not introduce the corresponding notions and notation that will be used in the sequel). For all the information about the content of this part we refer the reader to (Babenko, 1986a), where the necessary references can be found too.

An analogy with topology is the following. For every complex X, the linear space $\pi^{\mathbf{Q}}_*(X) = \pi_{*+1}(X) \otimes \mathbb{Q}$ is a Lie superalgebra with respect to Whitehead multiplication. If X is a singly connected complex, then the Pontryagin ring $H_*(\Omega X)$ and the Whitehead superalgebra $\pi^{\mathbf{Q}}_*(X)$ are related by the equality $H_*(\Omega X) = U(\pi^{\mathbf{Q}}_*(X))$.

The corresponding generating function is also introduced. The series $L_X = \sum \dim_K H_i(\Omega X, \mathbb{Q}) t^i$ is called *the Poincaré series of the loop space* of the given space. After all, it equals to the Hilbert series of the Pontryagin algebra $H_*(\Omega X)$, however note that, even for finite singly connected complexes, the latter may not be finitely generated. We refer the reader to the papers indicated in Fig. 1, in relation to different questions of rational dependence. It is important to emphasize that the connection between the local rings and the CW-complexes, that we only hinted at, has a rather deep, categorical content. A connection between two classes of objects is realized through the differential algebras according to the Quillen principle: "Differential graded algebras should be used not only as an instrument of calculating (co)homologies. In reality, an appropriate category of differential graded algebras will carry a "homotopic theory" and a series of other invariants with it". A marvelous realization of the Quillen principle may be found in (Avramov, Halperin, 1986). Unfortunately, the volume of this book does not allow us to go deeper in that direction, but the reader may familiarize himself with this theory through an expository paper (Babenko, 1986a).

§10. Other Combinatorial Questions

10.1. Introduction. In this short section we consider briefly two important new directions of research that, in our opinion, should not be passed by in silence. We have in mind hyperbolic and quantum groups.

10.2. Hyperbolic Groups. We will consider here, from a purely philosophical point of view, an important notion introduced by Gromov (Gromov, 1987). We begin by a somewhat ill-posed problem. Let us assume that we would like to obtain an algebra of sufficiently general position, with some imposed condition that cannot be guaranteed by a finite number of defining relations or we simply do not know how to do it. For instance we may need an infinite nilalgebra. Going back to Golod's example (3.5), we recall how it was achieved: every succeeding relation was simply taken to be of considerably greater degree than the preceeding. In addition, the infinity was ensured by the Golod-Shafarevich theorem. The question is, however, what to do if the relations are not homogeneous, such as when we want to construct a simple nilalgebra. In principle, it is perfectly unclear that it will be possible to add even one relation at some stage – it is enough to recall that the Kac-Moody algebras (7.10) turned out to be simple, up to the center, although finitely presented, thus no relations can be added to them. On the other hand, note that we are dealing here with the polynomial growth, which obviously does not correspond to a "general position". On the other hand, it is purely intuitively clear, that if the relations are chosen fairly randomly, then the infinite-dimensionality should not be altered. What are the means to express this intuitive "clarity". We would like to have some wide class of finitely presented algebras of the exponential growth from which we would not exit after imposing one more relation of a sufficiently general form. An example of such a class were graded algebras with three generators and not more than one relation in every degree (5.3). Unfortunately, such an effective description of a class of algebras, in the non-homogeneous case, has not been found yet. A similar problem for groups has been solved however – Gromov investigated *hyperbolic groups* in (Gromov, 1987). Let X be a finite set of generators of the group G and, for every $g \in G$, let the symbol $|g|$ denote the length of the shortest presentation of g through the generators and their inverses. If $d_X(n)$ is the number of the elements $g \in G$, such that $|g| \leqslant n$, then it is not difficult to understand that the equivalence class $[d_X]$ is exactly the growth of the group G. For $x, y \in G$ set

$$(x \cdot y) = \frac{1}{2}(|x| + |y| - |x^{-1}y|).$$

Definition. A group G is called *hyperbolic,* if there exists a constant $\delta \geqslant 0$, such that, for all $x, y, z \in G$:

$$(x \cdot y) \geqslant \min((x \cdot z), (y \cdot z)) - \delta.$$

It turns out that this definition does not depend on the choice of generators (only the constant δ changes) and that all the groups whose defining relations do not link more than 1/6 of their lengths are hyperbolic, but represent only a small fraction of the hyperbolic groups.

It is more striking however that the hyperbolic groups are always finitely presented. As every finitely presented group, a hyperbolic group may be realized as a fundamental group of the corresponding smoothly bounded region V. The hyperbolicity of the fundamental group is equivalent to the following purely geometrical property: there exists a constant C such that every smooth closed curve S contractible in V and enclosing a smoothly embedded disk D, satisfies the inequality:

$$\text{the area of } D \leqslant C \cdot \text{length of } S.$$

This allows for a study of hyperbolic groups by geometrical methods: In reality, it turns out that the hyperbolic groups are exactly fundamental groups of spaces of negative curvature. We may view them as the groups of isometries of the spaces of negative curvature. Let $F = F(X)$ be a free group, $W \subseteq X$ and let $N(W)$ be the normal subgroup of F generated by W; let also $f \in N(W)$, let $L(f)$ be the length of minimal representation of f through the generators and let $S(f)$ be the minimal number A with the property that

$$f = \rho_1 w_1^{b_1} \rho_1^{-1} \rho_2 w_2^{b_2} \rho_2^{-1} \dots w_n^{b_n} \rho_n^{-1},$$

for some $\rho_i \in F, w_i \in W$, where

$$\sum L(\rho_i) \leqslant A, \quad \sum |b_i| L^2(W_i) \leqslant A.$$

Theorem 1. *Let G be a hyperbolic group and let $d \geqslant 8(\delta+2)$ (δ comes from the definition of a hyperbolic group). Let W be the set of all the words in G of length not greater than 3d that are equal to the unity. Then:*

a) $G = F/N(W)$.

b) *For every $f \in N(W)$, $S(f) \leqslant 27d^2 L(f)$.*

Corollary. *The equality problem is decidable in G.*

The converse holds too.

Theorem 3. *If $G = \langle X \mid W \rangle$ and if there exists a constant $C > 0$ such that, for every $f \in N(W)$, $S(f) \leqslant CL(f)$, then G is a hyperbolic group.*

If all the words in W have the length not greater than three (and it is always possible to achieve), then in reality, it is sufficient to check the condition of Theorem 3 only for a finite number of words. By the same token, there exists (at least theoretically) an algorithm for checking whether a group is hyperbolic.

Theorem 4. *The generating function (cf. 3.3 for non-invariantly defined Hilbert series)*

$$\sum d_X(n)t^n$$

for a hyperbolic group is a rational function. The growth of a hyperbolic group is either constant (in case the group is finite) or exponential. Moreover, it is an automatic group.

This is derived from the fact that the set of normal words is a Markov set. For details and definitions see (Gromov, 1987). A few other rational generating functions for the corresponding interesting sets may be found in the same paper, and most importantly, some deep geometric and combinatorial ideas that deserve thorough investigation.

10.3. Quantum Groups and Quadratic Algebras. This part has an almost advertising goal: to attract attention of the specialists in the area of combinatorial algebra to some new questions and problems that were born in areas fairly remote from them. Thus the content of this part will consist of several examples that should arise the readers curiosity.

What is the meaning of the word "quantum"? "Quantizing is something similar to replacing commutative algebras by non-commutative" (Drinfel'd, 1986). Let us try to illustrate this claim. We start with a quantum plane. To this end, let us at the beginning adopt the point of view of algebraic geometry, namely that the properties of objects are given by the properties of its coordinate ring. For instance, the ordinary affine plane may be uniquely established by its ring $K[x, y]$. A further development of this point of view is an assumption that every algebra A is a coordinate ring, i.e. the ring of functions on some imaginary "quantum" space $\operatorname{Spec} A$.

Let now q be an element of the base field, such that $q^2 \neq 0, -1$. The quantum plane $\operatorname{Spec} A_q(2|0)$ is defined by the ring

$$A_q(2|0) = \langle x, y \mid xy = q^{-1}yx \rangle. \tag{1}$$

There is also a "behind-the-mirror" analogue – the second quantum plane defined by

$$A_q(0|2) = \langle \xi, \eta \mid \xi^2 = 0, \eta^2 = 0, \xi\eta = -q\eta\xi \rangle. \tag{2}$$

And now we want to define quantum matrices. Again, we define instead the coordinate ring of the variety of all quantum matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$. They form the quadratic algebra:

$$\begin{aligned} M_q(2) = &\langle a, b, c, d \mid ab = q^{-1}ba, ac = q^{-1}ca, cd = q^{-1}dc, \\ &bd = q^{-1}, bc = cb, ad - da = (q^{-1} - q)bc \rangle. \end{aligned} \tag{3}$$

A justification of these definitions is the following

Theorem 1. *Let (x, y) and (ξ, η) satisfy (1) and (2) respectively. Let a, b, c, d commute with x, y, ξ, η. Set*

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}, \quad \begin{pmatrix} x'' \\ y'' \end{pmatrix} = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}, \quad \begin{pmatrix} \xi' \\ \eta' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \xi \\ \eta \end{pmatrix}.$$

Then the following conditions are equivalent:

a) (x', y') *and* (x'', y'') *satisfy the relations in (1).*
b) (x', y') *satisfy (1) and* (ξ', η') *satisfy (2).*
c) (a, b, c, d) *satisfy relations in (3).*

Corollary. *If the quadruples* (a, b, c, d) *and* (a', b', c', d') *satisfy (3) and if their elements mutually commute, then the matrix entries of the product* $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$ *also satisfy (3).*

Both the theorem and the corollary are easily checked by direct computations. The next stage is to introduce the determinant. Let (a, b, c, d) satisfy (3). Then set

$$\mathrm{DET}_q \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - q^{-1}bc = da - qcb,$$

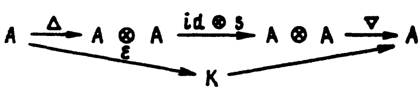
and it is not difficult to check that the determinant of the product equals to the product of the determinants of the factors. And now let us reach the quantum groups. For instance, setting $\mathrm{DET}_q = 1$, we obtain the quantum group $\mathrm{SL}_q(2)$ (more precisely, its coordinate ring). What corresponds to the quantum group $\mathrm{GL}_q(2)$? And, generally, what is a quantum group? Let us again try to get onto a more general point of view and to define not the notion we have singled out, but rather to describe all the family of quantum groups.

Let us return to groups. Let G be a group and let $A = \mathrm{Fun}\,(G)$ be the algebra of functions on G that are assumed to be smooth, if G is a Lie group, regular, if G is an algebraic group etc. Since $\mathrm{Fun}\,(G \times G) = A \otimes A$, if the tensor product is interpreted in the corresponding sense (for instance, as a topological tensor product in the case of Lie groups), the multiplication in the group induces a comultiplication $\Delta : A \longrightarrow A \otimes A$. As a result, A turns into a commutative Hopf algebra. Thus, the category of groups is dual to the category of commutative Hopf algebras.

And let us now "unroll" our point of view and define at the first place the category of quantum spaces as the category dual to the category of associative algebras, of course not necessarily commutative, whenever we mentioned the word "quantum". Let us denote by $\mathrm{Spec}\, A$ the quantum space corresponding to the algebra A, and call it the spectrum of A. From this point of view, all our previous examples are examples of quantum spaces. What is specific about $\mathrm{Spec} M_q(2)$? It is the presence of multiplication. It translates, with the aid of Theorem 1 and its corollary, as follows: the comultiplication

$$\Delta : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \to \begin{pmatrix} a & b \\ c & d \end{pmatrix} \otimes \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

turns $M_q(2)$ into a bialgebra. It is now clear how to define quantum semigroups: they are spectra of bialgebras. Finally, the quantum groups are spectra of the Hopf algebras. Now the reader can independently define the latter notion, introducing antipodes as the reflection of the property of having the inverse element. Here is one of the necessary diagrams: (s is an antipode):



In addition, we need to take into account that, in the non-commutative case, the existence of a "skew" antipode s' is required; it is in fact an antipode for the opposite multiplication and the same comultiplication. More details about this cf. (Drinfel'd, 1986) and (Manin, 1988).

Thus, the notions of a quantum group and a Hopf algebra are in fact equivalent. Let us emphasize that, generally speaking, a quantum group is not a group in the ordinary sense.

Let us turn our attention to the following aspect of our examples: all of them were examples of quadratic algebras. Recall that they are not appearing for the first time – cf. 3.10 and 8.4. Let us try to consider quadratic algebras from the categorical point of view. First of all let us represent a quadratic algebra A as a quotient of the tensor algebra $T(A_1)$ mod an ideal generated by $R(A) \subset A_1 \otimes A_1$. Such a pair $\{A_1, R(A)\}$ uniquely determines A. For instance, $A_q(0|2) = \{K\xi \oplus K\eta, K(\xi \otimes \xi) + K(\eta \otimes \eta) + K(\xi \otimes \eta - q\eta \otimes \xi)\}$, whereas the dual algebra $A^!$ (cf. 3.10) is defined by the pair $\{A_1^*, R(A)^\perp\}$.

Quadratic algebras form a category. It is interesting that, besides the tensor product, this category is also closed under two other operations. Let A, B be quadratic algebras, defined by the relations $R(A) \subset A_1 \otimes A_1$ and $R(B) \subset B_1 \otimes B_1$ respectively. Let T be the mapping that carries

$$a_1 \otimes a_2 \otimes b_1 \otimes b_2, \text{ to } a_1 \otimes b_1 \otimes a_2 \otimes b_2.$$

Let us define the algebras $A \circ B$ and $A \bullet B$ by the following pairs:

$$A \circ B = \{A_1 \otimes B_1, T(R(A) \otimes B_1 \otimes B_1 + A_1 \otimes A_1 \otimes R(B)\},$$
$$A \bullet B = \{A_1 \otimes B_1, T(R(A) \otimes R(B)\}.$$

The following isomorphisms hold:

$$(A \circ B) \circ C \cong A \circ (B \circ C), \quad (A \bullet B) \bullet C \cong A \bullet (B \bullet C),$$
$$(A \bullet B)^! \cong A^! \circ B^!, \quad (A \circ B)^! = A^! \bullet B^!.$$

We point out that if A is a Hopf algebra (thus, also a Roos algebra), then the comultiplication leads to a natural morphism $A \to A \circ A$.

Theorem 2. *The following factorial isomorphism holds:*

$$\mathrm{Hom}\,(A \bullet B, C) \cong \mathrm{Hom}\,(A, B^! \circ C).$$

If we introduce an inner Hom by the rule $\mathrm{Hom}(B, C) = B^! \circ C$ and dually $\mathrm{hom}(B, C) = B^! \bullet C$, then $\mathrm{hom}(A, A) = \mathrm{end}(A)$ is provided by a structure of a Hopf algebra. These properties open up the way to generalizing examples discussed at the begining of this part (cf. Manin, 1987).

Let us consider our quantum examples from one more viewpoint. Their defining relations form a complete system of relations and, by the same token, their Hilbert series are same as in the corresponding polynomial algebras. These algebras are called the Poincaré-Birkhoff-Witt algebras (PBW in a short form), thus extending this definition to non-graded algebras with non-invariantly defined Hilbert series. Thus, if A is a graded PBW algebra (with the natural gradation), and if $d = \dim A_1$ is the number of generators, then $\dim A_n = \binom{n+d-1}{n}$.

We are interested in the quadratic PBW algebras. First of all, they are homogeneous Koszul algebras (cf. 3.10) and, in particular, $\mathrm{Ext}^*_A(K, K) \cong A^!$ (Priddy). In an unexpected way, the PBW property is essentially defined in the third component: the generic algebras (in the sense analogous to that considered in section 4), for which $\dim A_2 = \frac{d(d+1)}{2}, \dim A_3 = \binom{d+2}{3}$ are all PBW algebras (this is a result of V.G. Drinfel'd, cf. (Vershik, 1984) where other interesting properties of quadratic algebras can be found too).

10.4. Comments. In our presentation we have followed (Gromov, 1987), (Manin, 1988) and (Drinfel'd, 1986), not at all pretending that we have shed light on the most meaningful moments of these works. In (Vershik, 1984) we can also find discussions on Sklyanin's algebras, for which the defining relations have the form of equality of a commutator to an anticommutator. The contents of the last part is connected to the classical methods of the inverse problem and this connection after all deserves a special attention, however this discussion and many other interesting questions will remain beyond the scope of this work.

§11. Appendix

11.1. Computer Algebra. Although the main subject of the preceeding chapters consisted of non-commutative algebras, a significant progress in the commutative case should be mentioned before everything else.

The major part of this progress stems from a new era of Computer Algebra. There has been an emergence of a number of powerful software packages for hardest calculations in algebra. The concept of a Gröbner basis is certainly very useful by itself, but with the help of a computer, it really becomes a diamond.

We are nowadays offered a possibility of a selection among the many first class Computer Algebra systems. One can use both very convenient universal packages such as MAPLE and MATHEMATICA, or the more specialized (and more effective) ones such as MACAULAY, COCOA (commutative algebra), GROEBNER (non-commutative, especially path algebras), BERGMAN (both commutative and non-commutative case), GAP (group theory) and so on. The full list is too long to give here (the author mentions only those that he is familiar with); one of the ways to get a more complete and up-to-date information on the variety and availability is by anonymous ftp from math.berkeley.edu, where it is in the directory: pub/Symbolic_Soft.

Let us now assume that we have one of these remarkable instruments available in our computer and that we want to use them for our routine calculations. What are our new possibilities to prove purely mathematical results?

11.2. Commutative Gröbner Basis. First of all we have a possibility to calculate a Gröbner basis. In fact, it gives much more than it can be hoped for. Here is a short list of questions that can be easily dealt with in the commutative case. As usual, K denotes the ground field. Assume that we are given an algebra $A = \langle X \mid R \rangle$ (always finite in the commutative case), and, in the following five items, let I be an ideal of $K[X]$, generated by R.

1. *Ideal membership.* Using the Gröbner basis of the given algebra A, we can find a basis of A, consisting of normal words as well as find out whether a given element u belongs to the ideal I. More importantly we can find the exact expression for u, if this is the case!

Example. $A = \langle x, y \mid xy = y, y^2 = x \rangle$. If $x > y$, then the set $\{f_1 = xy - y, f_2 = y^2 - x, f_3 = x^2 - x\}$ is the (commutative) Gröbner basis. Note, that $f_3 = yf_1 + (1-x)f_2$ (because it was obtained as a result of a reduction of the composition $f_1y - f_2x$ by f_2.)

Suppose we test the element $u = -x^3 + xy^2 + x^2 - xy - y^2 + y$. Applying reductions we get

$$u \xrightarrow{-xf_3} xy^2 - xy - y^2 + y \xrightarrow{yf_1} -xy + y = -f_1.$$

So, $u = -xf_3 + yf_1 - f_1$, and $u = (-xy + y - 1)f_1 + (x^2 - x)f_2$.

2. *Ideal equality.* Two ideals are equal iff their reduced Gröbner bases are equal.

3. *Inverses.* An element f has an inverse iff the ideal, generated by I and f in $K[X]$ contains 1. On the other hand, we know already how to solve the problem of membership and how to express $1 = af + \sum a_i f_i$, whenever possible. The element a will be the inverse.

4. *Radical membership.* Let y be an additional variable. Then f belongs to the radical of I (i.e. it is a nil-element in the factor algebra) iff the ideal, generated by I and $1 - yf$ in $K[X, y]$, contains 1.

5. *Lexicographic ordering.* We have already mentioned that, in the commutative case the pure lexicographic ordering is possible as well as useful

(although it is hardest from the computational point of view). The following fundamental fact is valid only in the pure lexicographic ordering:

Theorem. *Let $x_1 < x_2 < \cdots < x_n$ be the pure lexicographic ordering and $m \leq n$. If G is the Gröbner basis for the ideal I, then $G \cap K[x_1, x_2, \dots, x_m]$ is the Gröbner basis for $I \cap K[x_1, x_2, \dots, x_m]$.*

6. *Intersection.* In the remaining two items we assume that I, J are arbitrary ideals in $K[X]$. Let y be an additional variable, such that $X < y$ (in the pure lexicographic ordering). Then, in order to find the Gröbner basis for the intersection, it is sufficient to use the following fact

Theorem. $I \cap J = \langle yI, (1-y)J\rangle \cap K[X]$.

Example. Let $I = \langle x^2 - y^2\rangle, J = \langle y\rangle$ and $x > y$. Introducing a new variable $z, z > x$, we need to calculate the Gröbner basis for the ideal, generated by $z(x^2 - y^2)$ and $(1-z)y$. In addition to these elements it contains one more: $x^2y - y^3$. Exactly this element generates $I \cap J$.

Of course the answer here was evident from the beginning, for we have $\langle f\rangle \cap \langle g\rangle = lcm\,(f, g)$.

7. *Homomorphism.*

Theorem. *Let $\phi : K[Y]/J \longrightarrow K[X]/I$ be a homomorphism, such that $\phi y_i = u_i(X), i = 1, \dots m$. Let $Y < X$ be a pure lexicographic ordering. Then*

$$\ker \phi = (\langle I, y_i - u_i\,(i = 1, \dots, m)\rangle \cap K[Y])/J.$$

Thus, it is easy to find for example the subalgebras, generated by the given set of elements (by considering them as an image of $K[Y]$.)

The list can be (and should be) continued for long, but even this list is sufficient for understanding the role of computer applications today. Moreover, these basic constructions are already included in the modern computer algebra systems and we need only one line to call them. More importantly, the procedures following Gröbner basis calculations, such as syzygies, have become an important part of Computer Algebra and it is sufficient to refer to the corresponding manuals for completing the calculations (for example the manual for GAP contains more than 1000 pages and has procedures for almost all necessary calculations in finite groups). As to publications, there are many and the following are only a few among them: (Becker, Weispfenning, 1993), (Davenport, Siret, Tournier, 1988), (Mora, 1986), (Robbiano, 1989), (Almkvist, 1990), (Sturmfels, 1993) (the last two authors are concerned with invariant theory – a subject we have reluctantly omitted).

11.3. n-cyclic Systems of Equations. Let us discuss a nice example of a modern application of computers, where several different ideas come together. For a given natural number n the n-cyclic system is of the following form:

$$\begin{cases} x_1 + x_2 + x_3 + \cdots + x_{n-1} + x_n & = 0 \\ x_1x_2 + x_2x_3 + x_3x_4 + \cdots + x_{n-1}x_n + x_nx_1 & = 0 \\ \cdots \\ x_1x_2\cdots x_{n-1} + x_2x_3\cdots x_n + \cdots + x_nx_1\cdots x_{n-2} & = 0 \\ x_1x_2\cdots x_n & = 1 \end{cases}$$

Note, that only the last equation has a non-zero right-hand side and that all other equations have exactly n summands (as well as that they are not all elementary symmetric functions).

This system represents a good test for computer algebra programs and it has appeared independently in a rather different areas such as orthogonal decompositions of Lie algebras (Kostrikin, Kostrikin, Ufnarovskij, 1981) and Fourier transforms (Björck, 1985). The program's rating is the last n, for which it is able to find all solutions; rating increases with increasing n. The highest rating is achieved when men and computers cooperate (Björck, Fröberg, 1991), (Björck, Fröberg, 1994), (Backelin, Fröberg, 1991).

Here we give the main idea of their approach:

Theorem. *Let*

$$\begin{cases} f_1(x_1, x_2, x_3, \dots, x_n) = 0 \\ f_2(x_1, x_2, x_3, \dots, x_n) = 0 \\ \cdots \\ f_m(x_1, x_2, x_3, \dots, x_n) = 0 \end{cases}$$

be any (non-homogeneous) system of polynomial equations.

Let $g_i(x_1, x_2, x_3, \dots, x_n, z) = z^{\deg f_i} f_i(x_1/z, \dots, x_n/z)$ be homogenizations and let I be an ideal, generated by $g_1, \dots, g_m$ in $A = K[x_1, x_2, x_3 \dots x_n, z]$ Let $B = A/I$ and $B_m = A/(I, z^m)$. Then

1. The sequence of power series $H_m(t) = (H_B - H_{B_m})/t^m$ first strictly decreases (coefficient-wise) with increasing m, then stabilizes, after some index m_0, to a series $H(t)$.

2. The original system has finitely many solutions iff $H(t) = p(t)/(1-t)$, for some polynomial p. If this is the case, the number of solutions does not exceed $p(1)$ (the equality holds over an algebraically closed field, if multiplicity is counted).

This theorem allows us to decide, even for very complicated systems, whether we have found all the solutions or at least to estimate how many we have not found. All we need to do is calculate the Hilbert series for some commutative algebras. Computers do it perfectly well. For example, the 7-cyclic system has 924 solutions (Backelin, Fröberg, 1991). The 8-cyclic system has infinitely many solutions (this is the case for arbitrary square multiples of n, (Backelin, 1989)), and one can find them all in (Björck, Fröberg, 1994). For a prime p, Fröberg communicated to the author a nice formula as a conjecture for the number of roots of $p-$cyclic system, namely $\binom{2p-2}{p-1}$.

11.4. Commutative Algebras with the Quadratic Relations. The powerful computer programs have opened a new era of investigations in commutative ring theory. The best way to get to appreciate these new possibilities would be through reading a paper by Jan-Eric Roos (Roos, 1994). It contains not only mathematical theorems, but programs as well as typical computer science arguments. For example, one can find there a computer investigation of commutative algebras with 3 quadratic relations in four variables. Based on 22 different cases of 2 relations (see Jordan, 1906), we can consider 255 different variants for the third relation with the coefficients 0 or 1. Of course, this does not exhaust all the cases, however there are sufficiently many for understanding the general case. The whole picture of 5610 rings consists of 6 classes; the possible Hilbert series are as follows:

$(1+t)/(1-t)^3$ – the largest class; example: (x^2, y^2, z^2);
$(1+2t-t^3)/(1-t)^2$ – about 600 cases; example: (xy, y^2, z^2);
$(1+2t-2t^3)/(1-t)^2$ – about 200 cases; example: $(xy+z^2, y^2, xz)$;
$(1+2t)/(1-t)^2$ – about 50 cases; example: (xy, y^2, xz);
$(1+2t-2t^3+t^4)/(1-t)^2$ – 18 cases; example: $(x^2, y^2, xz+yu)$;
$(1+2t-2t^2+t^3)/(1-t)^2$ – 6 cases; example: (xy, y^2, yz).

Especially interesting are the Poincaré series calculations. Although it is impossible to calculate infinite number of Betti numbers, there are some ways to predict the remaining infinite part (once again, using computers!) – refer to (Roos, 1994). Some other ideas about possible prediction of Hilbert series in the non-commutative case can be found in (Ufnarovskij, 1993). Nevertheless it should be noted that these kinds of predictions are rather restricted even for sufficiently nice classes of algebras. One of these classes is that of the (homogeneous) Koszul algebras. One can define them as commutative quadratic algebras for which the double Poincaré series can be obtained from the Hilbert series:

$$P_A^{-1}(s,t) = H_A(-st) \quad (*).$$

Other equivalent definitions and examples can be found in the sequel.

Since we always know the Hilbert series in the commutative case, we know its Poincaré series too. The problem is that we cannot predict whether our algebra is Koszul, even if we know a sufficiently large part of its Poincaré series, and even in the case when the algebra is finite-dimensional:

Theorem (Roos, 1993). *Let*

$$A = \langle x, y, z, u, v, w \mid x^2, xy, yz, z^2, zu, u^2, uv, vw, w^2,$$

$$y^2, v^2, xz + \alpha zw - uw, zw + xu + (\alpha - 2)uw\rangle$$

be a commutative quadratic algebra over a field K of characteristic 0, where $\alpha \in K$. Then $H_A(t) = 1 + 6t + 8t^2$, but

$$H_A(-st) - P_A^{-1}(s,t) = (st)^{\alpha+1}(t + st).$$

11.5. Koszul Algebras and Veronese Subalgebras. A (homogeneous) Koszul algebra A (also called the Fröberg algebra, or the Priddy algebra, or even a "wonderful algebra") can be defined by one of the following equivalent properties; see (Backelin, Fröberg, 1985a), (Löfwall, 1986), (Priddy, 1970), (Backelin, 1982), (Kempf, 1992):

$P_A(t)H_A(-t) = 1$;
$P_A(s,t)H_A(-st) = 1$ (this was used in (*), above);
$\operatorname{Ext}^1_A(K,K)$ generates $\operatorname{Ext}^*_A(K,K)$ as an algebra with the Yoneda multiplication;
$\operatorname{Ext}^{p,q}_A(K,K) = 0$ for $p \neq q$;
$\operatorname{Tor}^A_{p,q}(K,K) = 0$ for $p \neq q$;
A is quadratic and its associated lattice $L(A)$ is distributive (see 3.10);
A is quadratic and $A^!$ is a Koszul algebra.

The main difference from Theorem 4 in 3.10 is that we do not assume in the first three cases the algebra to be quadratic; this property is rather a consequence of any of the above equivalent properties.

We list here some examples of Koszul algebras:

Monomial quadratic algebras;
Monomial commutative quadratic algebras;
Algebras defined by some special classes of monomial and binomial quadratic relations (Kobayashi, 1978)
Generic algebras where the number of relations is not large (both for commutative and non-commutative cases), such as quadratic algebras of global dimension 2, in the non-commutative case. This does not necessarily provide an example, if the number of relations is large.

Some other examples and the following result can be found in (Backelin, Fröberg, 1985a).

Theorem. *Let A, B be graded augmented algebras. Then:*

1. *The following conditions are equivalent:*
   Both A and B are Koszul algebras;
   $A * B$ is a Koszul algebra;
   $A \otimes B$ is a Koszul algebra

If the conditions are satisfied, the Segre product (see (4.4)) $A \circ B$ is a Koszul algebra too.

2. *Assume that $B = A/(f)$, where f is a quadratic element, not a zero-divisor, in the commutative case, and strongly free in the non-commutative case. Then B is a Koszul algebra if and only if A is.*
3. *If $A \longrightarrow B$ is a small homomorphism and B is a Koszul algebra, then A is also a Koszul algebra.*
4. *If A is a Koszul algebra then all its Veronese subalgebras $A^{(d)}$ are also Koszul algebras.*

The following two definitions will clarify the last two statements:

Definition. Following (Avramov, 1978), we say that an epimorphism $f : A \longrightarrow B$ is a small homomorphism if either of the following two equivalent conditions is satisfied:

the induced homomorphism $f_* = \operatorname{Tor}^f_*(K,K)$ is injective;
the induced homomorphism $f^* = \operatorname{Ext}^*_f(K,K)$ is surjective;

An ideal I is called small, if the natural epimorphism $A \longrightarrow A/I$ is small.

Thus, in order for a homomorphism to be small it should be surjective and both algebras should be augmented. It is natural that subideals of small ideals are small. Note that an algebra is a Koszul algebra iff the square of its augmented ideal is small (Löfwall, 1986).

Definition. Let $A = \oplus A_n$ be a graded algebra; then, for any d, its d-th Veronese subalgebra (or subring) is defined by

$$A^{(d)} = \oplus_{k\geq 0} A_{kd}.$$

These algebras are important, for they are related to the Veronese embeddings in algebraic geometry.

An important and nontrivial fact is the following

Theorem (Backelin, 1986). *If A is a graded commutative algebra and d is sufficiently large, then $A^{(d)}$ is a homogeneous Koszul algebra.*

According to the previous theorem this is the case for all d, if A itself is a Koszul algebra. Note that, as a corollary, we get the result of Mumford (Mumford, 1970) that for sufficiently large d, the Veronese subalgebra $A^{(d)}$ is quadratic.

More information about this topic can be found in (Avramov, 1992), (Bakelin, Fröberg, 1985b), (Backelin, 1992), (Priddy, 1970), (Kempf, 1992), (Fröberg, Löfwall, 1991), (Stanley, 1978).

11.6. Lie Algebras and Rationality. The following interesting results show that the growth in Lie algebras is rather unexpected:

Theorem (Kobayashi, Sanami, 1990). *Let L be a solvable Lie algebra of degree 2. Then its growth is polynomial.*

Theorem (Lichtman, Ufnarovskij, to appear). *Let L be a free solvable Lie algebra of degree d, and let $A = U(L)$ be its universal enveloping algebra. If $d > 2$ then the growth of L as well as of A is almost exponential (this means, that it is less than the exponential growth $[2^m]$ but more than the growth $[2^{m^\alpha}]$ for any $\alpha < 1$).*

More exactly, this theorem is a straightforward consequence of the following two results:

Theorem. *Let L be an arbitrary Lie algebra with a growth $r(L) > [2^{m^\alpha}]$ for some $\alpha > 0$. Then* $\underline{\text{DIM}}\ U(L) = 1$.

This shows that, the hypothesis in 5.5 fails.

Theorem. *Let L_d be a free solvable Lie algebra of degree d and let $A_d = U(L_d)$ be its universal enveloping algebra. If $d > 1$ then the growth of L_d is equal to the growth of A_{d-1} (the number of the generators $n > 1$ is fixed); see also (Lichtman, 1984a,b), (Shmel'kin, 1973) on this topic.*

It is interesting to compare this result with, in a sense, an opposite case, when a free subalgebra exists. Note that a consequence of the last theorem is that the universal enveloping algebra of a solvable Lie algebra has no free subalgebras of rank 2. On the other hand the following holds:

Theorem (Avramov, 1994). *Let R be a commutative noetherian local ring and let L be its homotopy Lie superalgebra (see (9.5)). If L contains a Lie subsuperalgebra of finite codimension, then there exists a polynomial $D(t)$ with integer coefficients such that, for any finitely generated R-module M, the series $D(t)P_M^R(t)$ is a polynomial with integer coefficients.*

The following theorem looks especially simple for the graded case.

Theorem. *Let R be a graded commutative noetherian local ring. A necessary condition for all finitely generated R-modules to have eventually polynomial Betti functions is for R to be a complete intersection with at most one non-quadratic relation, and a sufficient condition is that it be a complete intersection of quadrics.*

The reader can also find the nongraded version of the last theorem in (Avramov, 1994) as well as many other interesting results and references. Some additional useful information on Lie algebras may be found in some of the new books as well as in the references they contain as follows: (Vaughan-Lee, 1993) gives a nice discussion on the topic of the Burnside problem; (Reutenauer, 1993) treats free Lie algebras and related topics; (Bokut', Kukin, 1993) gives advanced applications of the theory of non-commutative Gröbner bases as well as many other nice combinatorial results in Lie and associative algebras; (Bahturin, Mikhalev, Petrogradsky, Zaicev, 1992) discuss infinite-dimensional Lie superalgebras; (Mathieu, 1992) treats classification of simple graded Lie algebras of polynomial growth. This has already led us into a new topic.

11.7. Gelfand-Kirillov Dimension, Growth and monomial algebras. Among the many new results, that could be placed in this section, we mention only a few. Perhaps the most elegant of them are the following two, connecting different notions discussed earlier.

Theorem (Felix, Halperin, Thomas, 1989). *Let A be a graded Hopf cocommutative algebra of polynomial growth (we mean here the growth of its*

Hilbert series). If $\mathrm{Ext}_A(K, A) \neq 0$, *then* A *is a finitely generated nilpotent Hopf algebra.*

Theorem (Small, Staford, Warfield, 1985). *Finitely generated algebras of linear growth are PI.*

Algebras with linear growth were investigated using graphs; they were also described in 5.6. Here we give some new applications. First of all there is an exact bound for the Bergman theorem (see the first Lemma in 7.8):

Theorem. *Let* A *be a graded algebra such that* $\dim A_m \leq m$ *for some* m *(in the natural grading). Then*
1. $\dim A_{m+h} \leq \frac{m(m+2)}{4}$, *if* m *is even,*
2. $\dim A_{m+h} \leq \frac{(m+1)^2}{4}$, *if* m *is odd.*

This result was proved in (Kobayashi, Kobayashi, 1993), where one can find some other results and examples of algebras of Gelfand-Kirillov dimension 1. Another approach to those algebras and the following result can be found in (Ellingsen, 1993):

Theorem. *Let* A *be a finitely presented monomial algebra (in the natural grading). If* $\dim A_{m-1} \leq m + d - 2$, *for some* m *greater than or equal to the maximal length of the defining words, then the growth of the algebra is either exponential or bounded by a polynomial of degree* d.

The reader, interested in C^*-algebras, can find out how the property of linear growth is reflected in their structure (Kirchberg, Vaillant, 1992).
As to the monomial algebras we mention the following uniqueness theorem:

Theorem (Shirayanagi, 1991). *Every finite-dimensional monomial algebra has a unique irredundant presentation up to permutations of the generators.*

See also (Gateva-Ivanova, 1994), (Fröberg, 1985), (Fröberg, Hoa, 1992), (Green, Kirkman, Kuzmanovich, 1991), (Chiswell, 1994), (Shneerson, 1993).

11.8. The Burnside Problem and Semigroups. This section could be easily skipped, for the most recent results are covered perfectly well by the following references (Ivanov, 1994), (Vaughan-Lee, 1993), (Vaughan-Lee, Zelmanov, 1993), (Okniński, 1990), (Kharlampovich, Sapir); we especially recommend the last one since it contains many ideas and methods.
At least one result, once again relating different notions in this book, should be mentioned.
Let us define words Z_n in a free group by induction:

$$Z_1 = x_1, \; Z_{n+1} = (Z_n, x_{n+1}, Z_n);$$

where $(x, y, z) = ((x, y), z)$ and $(x, y) = x^{-1}y^{-1}xy$ (compare this with 6.2!)

Theorem (Zel'manov, 1993). *For every prime number p there exists a natural number n such that a group of exponent p is locally finite if and only if it satisfies the identity* $Z_n = 1$.

11.9. The Generatingfunctionology. The name of this section as well as most of its content have been borrowed from (Wilf, 1990). We think it is appropriate to exhibit in this book some methods for manipulating generating functions. Let us start from the list of the most important generating functions. An underlined quantity is defined by the expression on the other side of the equality sign. We emphasize that these are only abbreviation for the most commonly used series, not the corresponding functions as they are known in analysis. For example, the expression $e^{(t+1)}$ has no meaning for the formal series, because the composition $f(g(t))$ is defined only in the case when f is a polynomial or g is a constant or has a zero free term.

The classical series:

$$\underline{-\log(1-t)} = \sum_{n\geq 1} \frac{t^n}{n}$$

$$\underline{e^t} = \sum_{n\geq 0} \frac{t^n}{n!}$$

$$\underline{\sin t} = \sum_{n\geq 0} (-1)^n \frac{t^{2n+1}}{(2n+1)!}$$

$$\underline{\cos t} = \sum_{n\geq 0} (-1)^n \frac{t^{2n}}{(2n)!}$$

$$e^t \sin t = \sum_{n\geq 1} \frac{2^{n/2} \sin \frac{\pi n}{4} t^n}{(n)!}$$

$$\underline{(1+t)^\alpha} = \sum_{n\geq 0} \binom{\alpha}{n} t^n$$

$$\underline{\arctan t} = \sum_{n\geq 0} (-1)^n \frac{t^{2n+1}}{2n+1}$$

$$\underline{\arcsin t} = t + \frac{1}{2}\frac{t^3}{3} + \frac{1\cdot 3}{2\cdot 4}\frac{t^5}{5} + \frac{1\cdot 3\cdot 5}{2\cdot 4\cdot 6}\frac{t^7}{7} + \cdots$$

The series with binomial coefficients:

$$\frac{1}{(1-t)^{k+1}} = \sum_{n\geq 0} \binom{n+k}{n} t^n$$

$$\frac{t^k}{(1-t)^{k+1}} = \sum_{n\geq 0} \binom{n}{k} t^n$$

$$\frac{1}{\sqrt{1-4t}} = \sum_{n\geq 0} \binom{2n}{n} t^n$$

$$\frac{1-\sqrt{1-4t}}{2t} = \sum_{n\geq 0} \frac{1}{n+1} \binom{2n}{n} t^n$$

$$\frac{1}{\sqrt{1-4t}} \left(\frac{1-\sqrt{1-4t}}{2t}\right)^k = \sum_{n\geq 0} \binom{2n+k}{n} t^n$$

$$\left(\frac{1-\sqrt{1-4t}}{2t}\right)^k = \sum_{n\geq 0} \frac{k}{2n+k} \binom{2n+k}{n} t^n$$

The series with the Bernoulli numbers.

$$\frac{t}{e^t - 1} = \sum_{n\geq 0} B_n \frac{t^n}{n!}$$

$$t \cot t = \sum_{n\geq 0} (-4)^n \frac{B_{2n} t^{2n}}{(2n)!}$$

$$\tan t = \sum_{n\geq 1} (-1)^{n-1} \frac{2^{2n}(2^{2n}-1)B_{2n}}{(2n)!} t^{2n-1}$$

$$\frac{t}{\sin t} = \sum_{n\geq 0} (-1)^{n-1} \frac{(4^n - 2) B_{2n} t^{(2n)}}{(2n)!}$$

The series with the Stirling numbers of the first kind.

$$\frac{1}{k!} (\log \frac{1}{1-t})^k = \sum_n \frac{t^n}{n!} \underline{s(n,k)}$$

The hypergeometric series:

$$_pF_q \left[\begin{matrix} a_1 & a_2 & \dots & a_p \\ b_1 & b_2 & \dots & b_q \end{matrix} \middle| \, t \right] = \sum_{n\geq 0} \frac{(a_1)_n (a_2)_n \cdots (a_p)_n}{(b_1)_n (b_2)_n \cdots (b_q)_n} \frac{t^n}{n!},$$

where

$$(a)_n = a(a+1)(a+2)\dots(a+n-1)$$

for $n \geq 1$ and $(a)_0 = 1$. One can easily check whether a given series $\sum f_k$ can be represented in a hypergeometric form: the ratio of consecutive terms f_{n+1}/f_n should be a rational function of the summation index n. If this is the case, then the ratio can be expressed in the form

$$\frac{f_{n+1}}{f_n} = \frac{(n+a_1)(n+a_2)\cdots(n+a_p)t}{(n+b_1)(n+b_2)\cdots(n+b_q)(n+1)}$$

(here t is an expression, that does not depend on n, and the presence of the factor $(n+1)$ is traditional). Then

$$\sum_{n=0}^{\infty} f_n = {}_pF_q\left[\begin{matrix} a_1 & a_2 & \dots & a_p \\ b_1 & b_2 & \dots & b_q \end{matrix}\middle| t\right].$$

Example. Does the Bessel function

$$J_p(x) = \sum_{n=0}^{\infty} \frac{(-1)^n(\frac{x}{2})^{2n+p}}{n!(n+p)!}$$

have a hypergeometric form? The ratio of the consecutive terms is

$$\frac{-(\frac{x^2}{4})}{(n+p+1)(n+1)}.$$

Taking into the account that the first term is not equal to 1, we can rewrite the Bessel function as follows:

$$J_p(x) = \frac{(\frac{x}{2})^p}{(p+1)!}\,{}_0F_1\left[\begin{matrix} \\ p+1 \end{matrix}\middle| -\frac{x^2}{4}\right].$$

Note that most series above can be expressed in the hypergeometric form, e.g.

$$e^t = {}_0F_0\left[\begin{matrix} \\ \end{matrix}\middle| t\right],$$

$$\sin t = {}_0F_1\left[\begin{matrix} \\ 3/2 \end{matrix}\middle| -\frac{t^2}{4}\right],$$

$$\frac{1}{\sqrt{1-4t}} = {}_1F_0\left[\begin{matrix} 1/2 \\ \end{matrix}\middle| 4t\right].$$

One can also easily recognize the hypergeometric series by "Mathematica's" Algebra "SymbolicSum" package, or "Maple's" "convert/hypergeom".

In addition, the following list contains the rules for some elementary operations with generating functions. Let $a(t) = \sum_{n=0}^{\infty} a_n t^n, b(t) = \sum_{n=0}^{\infty} b_n t^n; \beta \in K$; h – a natural number, P – a polynomial. Then we have:

Linearity:

$$\beta a(t) = \sum_{n=0}^{\infty} \beta a_n t^n,$$

$$a(t) + b(t) = \sum_{n=0}^{\infty} (a_n + b_n) t^n,$$

Products and summation:

$$a(\beta t) = \sum_{n=0}^{\infty} a_n \beta^n t^n,$$

$$\frac{a(t)}{1-t} = \sum_{n=0}^{\infty} (a_0 + a_1 + \cdots + a_n) t^n,$$

$$a(t)b(t) = \sum_{n=0}^{\infty} (a_0 b_n + a_1 b_{n-1} + a_2 b_{n-2} + \cdots + a_n b_0) t^n,$$

Shift:

$$\frac{a(t) - a_0 - a_1 t - \cdots - a_{h-1} t^{h-1}}{t^h} = \sum_{n=0}^{\infty} a_{n+h} t^n,$$

Differential:

$$D(a(t)) = \sum_{n=0}^{\infty} (n+1) a_{n+1} t^n,$$

$$P(tD)(a(t)) = \sum_{n=0}^{\infty} P(n) a_n t^n.$$

Example. Suppose, we have arrived at the following recurrent inequality:

$$a_{n+1} \le a_n + n^2.$$

How can we estimate the coefficients a_n? Let $a(t) = \sum_{n=0}^{\infty} a_n t^n$ be the generating function. Then, according to our rules we have:

$$\frac{a(t) - a_0}{t} \le a(t) + (tD)^2 (\frac{1}{1-t}).$$

or

$$a(t)(1-t) \le a_0 + t \frac{t + t^2}{(1-t)^3}.$$

We can multiply both sides of the inequality by the series $(1-t)^{-1}$ (with positive coefficients) and conclude that the generating function series has at most polynomial growth of degree 4 and its coefficients a_n are growing polynomially by degree at most 3.

We now give some methods; we start with some rather simple but useful cases. The first is the method of translating the "at least" information into the "exact" one. By this, we mean the following:

Suppose that we are given a finite set of objects and a set P of properties that any of these objects may or may not satisfy. We would like to know the exact number e_k of objects, which satisfy exactly k properties from the set P. The main assumption made here is that, for any subset $S \subseteq P$, we can calculate sufficiently easily the number $N(S)$ of objects which have at least these S properties. The question is whether we can find the exact numbers e_k? The answer is as follows:

The Sieve Method. Let

$$l_k = \sum_{S \subseteq P, |S|=k} N(S)$$

(note that in this sum some objects may be calculated more than once). Let $l(t) = \sum l_k t^k, e(t) = \sum e_k t^k$ be the corresponding generating functions. Then

$$e(t) = l(t-1).$$

Example. Another question usually posed is: How many objects have none of the given properties? The answer is clear (and well-known; we usually see it as the method of inclusion-exclusion):

$$e_0 = l(-1) = \sum (-1)^k l_k.$$

Example. How many of the $n!$ permutations of n symbols have exactly k fixed points? This is easy to answer if we replace the word "exact" by the phrase "at least": there are $\binom{n}{k}$ possibilities to select k symbols among n, and, for every of these possibilities there are $(n-k)!$ different permutations with at least those k symbols fixed. Thus the sieve formula produces,

$$l_k = (n-k)!\binom{n}{k} = \frac{n!}{k!}$$

and

$$l(t) = \sum_{k \le n} \frac{n!}{k!} t^k = n! \sum_{k \le n} \frac{t^k}{k!}.$$

The latter series looks like an exponential series, thus after introducing notation for "truncated" exponential series:

$$exp_{\leq n}(t) = \sum_{k \leq n} \frac{t^k}{k!},$$

we obtain the following generating function as an answer to our question:

$$e(t) = n! exp_{\leq n}(t-1).$$

We now give a simple, but highly effective method of summing series. It combines two familiar procedures frequently used in mathematics. The first procedure embeds the object in question into a more intricate structure, such as seeing the real numbers as part of the larger structure of complex numbers or embedding a (single) summation or a definite integral into the double ones. Once in a wider structure one can view the original object with more freedom, from different angles, so that real numbers for instance can be identified with any line through the origin, in the complex plane, whereas the order in the double summation or integration may be interchanged (just as in Fubini's theorem). This extend-and-interchange method is called the "snake oil method" in (Wilf, 1990). We leave it up to the reader's imagination to decide as to why this name was chosen.

A Method for Series Summation. Suppose that we need to do some summation and that the result will depend on some variable n. The method is to multiply the sum by t^n or by $\frac{t^n}{n!}$ and then sum over n. In other words, we first create a generating function, thus arriving at a double sum. In the final step we interchange the order of summation and use our lists to get the answer!

Example. Let

$$a_n = \sum_k s(n,k) B_k.$$

Thus, we have

$$a(t) = \sum_n \frac{a_n t^n}{n!} = \sum_n \sum_k \frac{s(n,k) B_k t^n}{n!} = \sum_k B_k \sum_n \frac{s(n,k) t^n}{n!} =$$

(see the list of series!)

$$\sum_k B_k \left\{ \frac{1}{k!} (\log \frac{1}{1-t})^k \right\} = \sum \frac{B_k}{k!} u^k,$$

where $u = \log \frac{1}{1-t}$. After using the list one more time, we get

$$a(t) = \frac{u}{e^u - 1} = \frac{\log \frac{1}{1-t}}{\frac{1}{1-t} - 1} = \frac{1-t}{t} \log \frac{1}{1-t}.$$

After writing the first fraction in the last expression as $\frac{1}{t} - 1$, we get the sum of the two series, then we look into the lists for the last time and finally get the result:

$$\frac{a_n}{n!} = \frac{1}{n+1} - \frac{1}{n},$$

therefore

$$\sum_k s(n,k) B_k = -\frac{(n-1)!}{n+1}.$$

The Wilf-Zeilberger Method. Let us assume that we want to prove an identity of the form $\sum_k \cdots = \cdots$. The Wilf-Zeilberger method is a powerful procedure that produces proofs with a stencil-like ease. We start from two examples of such proofs and give some explanations of these wonderful proofs later.

Example. The following Dixon's identity holds:

$$\sum_k (-1)^k \binom{a+b}{a+k} \binom{b+c}{b+k} \binom{a+c}{c+k} = \frac{(a+b+c)!}{a!b!c!}.$$

Proof. Dividing both sides of the equation by the right-hand side and denoting every new summand on the left-hand side by $F(a,k)$, we arrive at a new form of the identity we would like to prove:

$$\sum_k F(a,k) = 1 \quad (*)$$

Let

$$R(a,k) = \frac{(c+1-k)(b+1-k)}{2((a+k)(a+b+c+1))}$$

and $G(a,k) = R(a,k)F(a,k-1)$. It is easy to check that

$$F(a+1,k) - F(a,k) = G(a,k+1) - G(a,k)$$

and that

$$\lim_{k \to \pm\infty} G(a,k) = 0$$

Consequently, we have

$$\sum_{k=-\infty}^{+\infty} (F(a+1,k) - F(a,k)) = 0,$$

thus, the sum on the left-hand side of $(*)$ has a constant value. It is easy to check that for $a = 0$ it equals 1, hence the identity has been proved. □

Example. The following identity holds:

$$\sum_k (-1)^k \binom{n}{k}\binom{2k}{k} 4^{n-k} = \binom{2n}{n}$$

Proof. Dividing both sides of the equation by the right-hand side and denoting every new summand on the left-hand side by $F(n,k)$, we arrive at a new form of the identity we would like to prove:

$$\sum_k F(n,k) = 1 \quad (*)$$

Let

$$R(n,k) = \frac{2k-1}{2n+1}$$

and $G(n,k) = R(n,k)F(n,k-1)$. It is easy to check that

$$F(n+1,k) - F(n,k) = G(n,k+1) - G(n,k) \tag{1}$$

and that

$$\lim_{k\to\pm\infty} G(n,k) = 0 \tag{2}$$

Consequently, we have

$$\sum_{k=-\infty}^{+\infty} (F(n+1,k) - F(n,k)) = 0,$$

thus, the sum on the left-hand side of $(*)$ has a constant value. It is easy to check that for $n = 0$ it equals 1, hence the identity has been proved. □

Comparing these two examples we can conclude that they are almost identical: if we replace a by n in the first example the difference will be only in the identities in question and the definitions of functions $R(n,k)$. Thus the key of the method is to choose a function $R(n,k)$ (called a "WZ certificate") in such a way that it reflects the identity we are proving and satisfies the equalities (1) and (2) above. Usually it can be done only with the aid of a computer program. We will discuss this procedure in more detail in the sequel; first, we list some examples of identities and their WZ certificates.

The following identity holds:

$$\sum_k (-1)^k \frac{\binom{n}{k}}{\binom{k+a}{k}} = \frac{a}{n+a}$$

WZ certificate:

$$R(n,k) = \frac{k}{n+a}$$

The following identity holds:

$$\sum_k (-1)^{n-k} \binom{2n}{k}^2 = \binom{2n}{n}$$

WZ certificate:

$$R(n,k) = -\frac{10n^2 - 6kn + 17n + k^2 - 5k + 7}{2(2n-k+2)^2}$$

If b is a nonpositive integer or $c-a-b$ has a positive real part, then the following Gauss's ${}_2F_1$–identity holds:

$${}_2F_1\left[\begin{matrix} a & b \\ c & \end{matrix}\middle| 1\right] = \frac{\Gamma(c-a-b)\Gamma(c)}{\Gamma(c-a)\Gamma(c-b)}.$$

WZ certificate:

$$R(n,k) = \frac{(k+1)(k+c)}{n(n-c+1)}.$$

If $a-b+c=1$ and real part of a is less than 1, then the following Kummer's ${}_2F_1$–identity holds:

$${}_2F_1\left[\begin{matrix} a & b \\ c & \end{matrix}\middle| -1\right] = \frac{\Gamma(\frac{b}{2}+1)\Gamma(b-a+1)}{\Gamma(b+1)\Gamma(\frac{b}{2}-a+1)}.$$

If $a+b+c+1 = d+e$ and c is a negative integer then the following Saalschütz's ${}_3F_2$–identity holds:

$${}_3F_2\left[\begin{matrix} a & b & c \\ d & e & \end{matrix}\middle| 1\right] = \frac{(d-a)_{|c|}(d-b)_{|c|}}{(d)_{|c|}(d-a-b)_{|c|}}.$$

If $a+b+c = d+\frac{1}{2}$, $e = a+b+\frac{1}{2}$, $a+f = b+g = d+1$ and if d is a non-positive integer then the following Clausen's ${}_4F_3$–identity holds:

$${}_4F_3\left[\begin{matrix} a & b & c & d \\ e & f & g & \end{matrix}\middle| 1\right] = \frac{(2a)_{|d|}(2b)_{|d|}(a+b)_{|d|}}{(a)_{|d|}(b)_{|d|}(2a+2b)_{|d|}}.$$

Now let us return to the crucial problem of choosing WZ certificate. The reader can find a remarkable algorithm in (Gosper, 1978) that takes hypergeometric series $\sum f_k$ as input and either gives a hypergeometric series $\sum g_k$ such that $f_k = g_{k+1} - g_k$ as output or informs us that such a g does not exist. Of course, this algorithm solves our problem in the hypergeometric case. Much more importantly, this algorithm is already implemented in the modern computer algebra programs! An important by-product of the use of these programs, is a possibility to create our own examples of proofs without any knowledge of Gosper's algorithm.

Let us illustrate this through the following trivial identity:

$$\sum_{k=0}^{n} \frac{\binom{n}{k}}{2^n} = 1.$$

We want to find the function $G(n,k)$ by computer calculations. We list a program for use in "Mathematica" (the comments come after the code and the actual verbatim listing may differ for different implementations of "Mathematica"):

```
In[1]:= <<DiscreteMath'RSolve'

In[2]:= rhs=Binomial[n+1,k]/2^(n+1)-Binomial[n,k]/2^(n)

         Binomial[n, k]     Binomial[1+n, k]
Out[2]= -(--------------) + ----------------
                n                -(-1-n)
               2                2

In[3]:= eqn=g[k+1]==g[k]+rhs

                        Binomial[n, k]     Binomial[1+n, k]
Out[3]= g[1+k] == -(--------------) + ---------------- + g[k]
                               n                -(-1-n)
                              2                2

In[4]:= RSolve[eqn,g[k],k]


Out[4]= {{g[k] ->

                       Binomial[-2+k-n, -1+k]
       If[n <= -1, ----------------------, Binomial[n, -1+k]]
                              -(-1+k)
                          (-1)
g[0] - ---------------------------------------------------------}}
                                     n
                                  2 2
```

We now give some comments about the listing above:

1) In the first line, we include the library containing the programs needed.

2) In the second line we define our function $F(n+1,k) - F(n,k)$. But what is "rhs?" It is simply an abbreviation for the right-hand side we will use later. Out[2] in the third line is the result, though in an unusual (but correct) form.

3) In line four, we have defined the kind of function g we need: it should be a solution to the equation. Note that in the equation we use == instead of = and "eqn" is a new abbreviation (this time for the equation). In the "Out" part, we see the equation itself.

4) We arrive to the central point in the sixth line. We ask "Mathematica" to find the solution to our recurrence equation. Note that we have specified k to be the main parameter. Now what do we have in Out[4]? We have expected something else... This means only that "Mathematica" has investigated the problem slightly deeper than we expected. First of all, it has taken into account that the result should depend on $g(0)$, so our formula starts with $g(0)$, instead of "If[...", as one might expect. The rest is a big (and strange) fraction. The second thing we learn is that there are two different cases: $n < 0$ and $n \geq 0$. "Mathematica" presents both of them and has written it in a rather understandable way: first the condition (If $n \leq -1$), then the solution if the condition is valid (we do not need it) and at last the case when the condition is not satisfied. Aha, the last case is needed! What is it? After translating from "Mathematica's" language we can write it down as

$$g(0) - \frac{\binom{n}{k-1}}{2 \cdot 2^n};$$

this is O.K. with the computer!

To learn more about the WZ-method and the Gosper's algorithm, which is the core of this approach, the reader is recommended to begin from (Wilf, 1990), (Wilf, Zeilberger, 1992), (Gosper, 1978). It will be especially useful to look into *The Electronic Journal of Combinatorics* and *The World Combinatorics Exchange* via information retrieval tools such as Gopher, WAIS (Wide Area Information Servers) or WWW (World Wide Web) – accessible through "Mosaic".

Let us end the section and the book by giving example of an advanced, up-to-date short proof of a classical result; it is taken from (Andrews, Ekhad, Zeilberger, 1993).

Theorem. *Every positive integer can be represented as a sum of four perfect squares of integers (Lagrange). Moreover, the number of ways (counting different order of summands as different representations) to represent a positive integer in this fashion equals eight times the sum of its divisors which are not multiples of 4 (Jacobi).*

Proof. Clearly it is sufficient to prove Jacobi's claim, because any number has at least one divisor (namely 1), not divisible by 4.

Let

$$H_n = H_n(q) = \frac{1+q}{1-q}\frac{1+q^2}{1-q^2}\cdots\frac{1+q^n}{1-q^n}.$$

According to the WZ-method the following two identities hold:

$$\sum_{k=-n}^{n} \frac{4(-q)^k}{(1+q^k)^2} H_n^2 H_{n+k} H_{n-k} = 1, \tag{3}$$

with the WZ certificate:

$$\frac{q^{n-k+2}(1+q^{2n+2})(1+q^{k-1})^2(1+q^{n+k})}{(1-q^{n+1})^3(1-q^{n+k})(1+q^{n+1})}$$

and

$$\sum_{k=0}^{n} \frac{2(-q^{n+1})^k}{1+q^k} \frac{H_k}{H_n} = \sum_{k=-n}^{n} (-q)^{k^2}, \tag{4}$$

with the WZ certificate (for the left-hand part):

$$\frac{(-q^{n+1})(1+q^{k-1})}{1+q^{n+1}}.$$

Dividing both sides of the identity (3) by H_n^4 and letting $n \longrightarrow \infty$ in both identities (3) and (4) gives the following two identities:

$$1 + 8\sum_{k=1}^{\infty} \frac{(-q)^k}{(1+q^k)^2} = H_\infty^{-4},$$

$$\sum_{k=-\infty}^{\infty} (-q)^{k^2} = H_\infty^{-1},$$

where, of course,

$$H_\infty = \lim_{n\to\infty} H_n = \prod_{1}^{\infty} \frac{1+q^n}{1-q^n}.$$

Now it is sufficient to combine the two new identities and to change $-q$ to t to prove another nice identity:

$$\left(\sum_{k=-\infty}^{\infty} t^{k^2}\right)^4 = 1 + 8\sum_{k=1}^{\infty} \frac{t^k}{(1+(-t)^k)^2}. \tag{5}$$

The rest of the proof of the theorem is simply a pleasure.

It is important to note that we count the number of vectors (not sets) (a, b, c, d), where the components a, b, c, d are integers, such that $a^2 + b^2 + c^2 + d^2 = n$. Therefore, the number of representations of number n is equal exactly to the coefficient of t^n on the left-hand side of our identity (5). Let us now calculate the right-hand side of the identity. With a little help of our list of series, we can deduce the following equality:

$$\frac{z}{(1+z)^2} = \sum_{m=1}^{\infty} (-1)^{m+1} m z^m.$$

Setting $z = -t^k$ we get

$$\frac{(-1)^k t^k}{(1+(-t)^k)^2} = \sum_{m=1}^{\infty} (-1)^{m+1} m (-1)^{km} t^{km}$$

and after trivial tricks with the signs, we can rewrite the $\sum$ on the right-hand side of identity (5) as follows:

$$\sum_{k=1}^{\infty}\sum_{m=1}^{\infty} (-1)^{(k+1)(m+1)} m t^{km} = \sum_{n=1}^{\infty} t^n \sum_{m|n} (-1)^{(n/m+1)(m+1)} m.$$

Thus, the desired coefficient of t^n is a weighted sum of divisors m of n, where the weight of m equals 1, if at least one of $m, n/m$ is odd, and it equals (-1), if both of them are even. On the other hand, $-1 = 1 - 2$ (this identity is the central point!), hence we can find our coefficient as the following difference:

$$\sum_{m|n} m - \sum_{\substack{m|n; \\ m, \frac{n}{m} \text{ even}}} 2m = \sum_{m|n} m - \sum_{m|n; 4|m} m.$$

This finishes the proof of Jacobi's claim. □

References*

Adams, J., Hilton, P. (1955): On the chain algebra of a loop space. Comment. Math. Helv. *30*, 305–330. Zbl. 71,164

Adyan, S.I. (1975): Burnside Problem and Group Identities. Moscow, Nauka. English transl.: Berlin-Heidelberg-New York, Springer-Verlag 1979. Zbl. 306.20045

Adyan, S.I., Razborov, A.A. (1987): Periodic Lie groups and algebras. Usp. Mat. Nauk *42*, No. 2, 3–68. English transl.: Russ. Math. Surv. *42*, No. 2, 1–81 (1987). Zbl. 627.17008

Adyan, S.I., Repin, N.N. (1986): Exponential lower estimate of the nilpotency degree of Engel Lie algebras. Mat. Zametki *39*, No. 3, 444–452. English transl.: Math. Notes *39*, 244–249 (1986). Zbl. 599.17009

* For the convenience of the reader, references to reviews in Zentralblatt für Mathematik (Zbl.), compiled using the MATH database, and Jahrbuch über die Fortschritte in der Mathematik (FdM.) have, as far as possible, been included in this bibliography.

Adyan, S.I., Repin, N.N. (1988): Lower estimates of orders of maximal periodic groups of prime order. Mat. Zametki *44*, No. 2, 161–176. English transl.: Math. Notes *44*, No. 1/2, 571–579 (1988). Zbl. 669.20030

Anan'in, A.Z. (1977): Locally finitely approximable and locally representable varieties of algebras. Algebra Logika *16*, 3–23. English transl.: Algebra Logic *16*, 1–16 (1978). Zbl. 381.16010

Anan'in, A.Z. (1987): Representability of K. P. algebras with a chain condition. XIX Vses. Alg. Konf., Abstracts I, L'vov, p.7. Zbl. 699.00006

André, M. (1971): Hopf algebras with divided powers. J. Algebra *18*, No. 1, 19–50. Zbl. 217,71

Andrunakievich, V.A., Ryabukhin, Yu. M. (1979): Radicals of Algebras and Structure Theory. Moscow, Nauka. Zbl. 507.16009

Anick, D. (1980): Construction d'espaces de lacets et d'anneaux locaux à séries de Poincaré-Betti non rationnelles. C. R. Acad. Sci., Paris, Ser. A *290*, 729–732. Zbl. 466.13006

Anick, D. (1982a): The smallest singularity of a Hilbert series. Math. Scand. *51*, 35–44. Zbl. 492.16003

Anick, D. (1982b): A counterexample to a conjecture of Serre. Ann. Math., II. Ser. *115*, No. 1, 1–33. Zbl. 454.55004

Anick, D. (1982c): Non-commutative graded algebras and their Hilbert series. J. Algebra *78*, No. 1, 120–140. Zbl. 502.16002

Anick, D. (1984): Connection between Yoneda and Pontryagin algebras. Lect. Notes Math. *1051*, 331–350. Zbl. 542.57035

Anick, D. (1985a): Diophantine equations, Hilbert series and undecidable spaces. Ann. Math., II. Ser. *122*, 87–112. Zbl. 584.13012

Anick, D. (1985b): On monomial algebras of finite global dimension. Trans. Am. Math. Soc. *291*, No. 1, 291–310. Zbl. 575.16002

Anick, D. (1986): On the homology of associative algebras. Trans. Am. Math. Soc. *296*, No. 2, 641–659. Zbl. 598.16028

Anick, D. (1988a): Generic algebras and CW-complexes. Proc. Conf. Alg. Topol. and K-theory in honor of John Moore, Princeton Univ. 1983, 247–331. Zbl. 681.55002

Anick, D. (1988b): Recent progress in Hilbert and Poincaré series. Lect. Notes Math. *1318*, 1–25. Zbl. 666.13008

Anick, D. (1989): The computation of rational homotopy groups in $\sharp P$-hard. Comp. Geometry Topol., Lect. Notes Pure Appl. Math. *114*, 1–56. Zbl. 691.55009

Anick, D., Green, E.L. (1987): On the homology of quotients of path algebras. Commun. Algebra *15*, No. 1, 2, 309–341. Zbl. 608.16029

Anick, D., Gulliksen, T.H. (1985): Rational dependence among Hilbert and Poincaré series. J. Pure Appl. Algebra *38*, 135–157. Zbl. 575.13008

Anick, D., Halperin, S. (1985): Commutative rings, algebraic topology, graded Lie algebras and the work of Jan-Eric Roos. J. Pure Appl. Algebra *38*, 103–109. Zbl. 574.18008

Anick, D., Löfwall, C. (1986): Hilbert series of finitely presented algebras. Lect. Notes Math. *1183*, 32–55. Zbl. 592.13015

Arbib, Michael A. (1968): Algebraic Theory of Machines, Languages and Semigroups. New York and London, Academic Press. Zbl. 181,15

Assmus, E.F. (1959): On the homology of the local ring. Ill. J. Math. *3*, 187–199. Zbl. 85,24

Aubry, M., Lemaire, J.-M. (1985): Zero divisors in enveloping algebras of graded Lie algebras. J. Pure Appl. Algebra *38*, No. 2–3, 159–166. Zbl. 587.55006

Auslander M., Buchsbaum, D.A. (1956): Homological dimension in Noetherian rings. Proc. Natl. Acad. Sci. USA *42*, 36–38. Zbl. 70,35

Auslander M., Buchsbaum, D.A. (1957): Homological dimension in local rings. Trans. Am. Math. Soc. *85*, 390–405. Zbl. 78,28

Auslander M., Buchsbaum, D.A. (1958): Codimension and multiplicity. Ann. Mat., II. Ser. *68*, No. 2, 625–627. Zbl. 92,39

Avramov, L.L. (1974): On a Hopf algebra of a local ring. Izv. Akad. Nauk SSSR, Ser. Mat. *38*, No. 2, 253–277. English transl.: Math. USSR, Izv. *8*, 259–284 (1975). Zbl. 295.13005

Avramov, L.L. (1975a): Flat morphisms of complete intersections. Dokl. Akad. Nauk SSSR *225*, No. 1, 11–14. English transl.: Sov. Math., Dokl. *15*, 1413–1417 (1976). Zbl. 334.13009

Avramov, L.L. (1975b): On the homology of the tensor product of local rings. Izv. Akad. Nauk. SSSR, Ser. Mat. *39*, No. 1, 3–14. English transl.: Math. USSR, Izv. *9*, 1–12 (1976). Zbl. 295.13006

Avramov, L. (1977): Homology of local flat extensions and complete intersection defects. Math. Ann. *228*, No. 1, 27–37. Zbl. 333.13011

Avramov, L. (1978): Small homomorphisms of local rings. J. Algebra *50*, No. 2, 400–453. Zbl. 395.13005

Avramov, L. (1979): On the convergence radius of Poincaré series of local rings. Rept. Dep. Math. Univ. Stockholm *4*, 17 pp. Zbl. 433.13010

Avramov, L. (1981a): Complete intersections and symmetric algebras. J. Algebra *73*, No. 1, 248–263. Zbl. 516.13001

Avramov, L. (1981b): Obstructions to the existence of multiplicative structures on minimal free resolutions. Am. J. Math. *103*, No. 1, 1–31. Zbl. 447.13006

Avramov, L. (1984a): Local algebras and rational homotopy. Homotopie algébrique et algèbre locale. Journ. Luminy/France 1982, Astérisque No. 113–114, 15–43. Zbl. 552.13003

Avramov, L. (1984b): Local rings of finite simplicial dimension. Bull. Am. Math. Soc. *10*, No. 2, 289–291. Zbl. 552.13005

Avramov, L.L., Golod, E.S. (1971): On the homology algebra of a Koszul complex of a local Gorenstein ring. Mat. Zametki *9*, No. 1, 53–58. English transl.: Math. Notes *9*, 30–32 (1971). Zbl. 213,49

Avramov, L., Halperin, S. (1986): Through the looking glass: a dictionary between rational homotopy theory and local algebra. Lect. Notes Math. *1183*, 1–27. Zbl. 588.13010

Avramov, L., Herzog, J. (1980): The Koszul algebra of a codimension 2 embedding. Math. Z. *175*, 249–260. Zbl. 461.14014

Avramov, L., Kustin, A., Miller, M. (1988): Poincaré series of modules over local rings of small embedding codepth or small linking number. J. Algebra *118*, No. 1, 162–204. Zbl. 648.13008

Avramov, L., Lescot, J. (1982): Bass number and Golod rings. Math. Scand. *51*, 199–211. Zbl. 509.13009

Avramov, L., Levin, G. (1978): Factoring out the socle of a Gorenstein ring. J. Algebra *55*, No. 1, 74–83. Zbl. 407.13018

Babenko, I.K. (1979a): On Poincaré series of iterated loop spaces. Usp. Mat. Nauk *34*, No. 3, 191–192. English transl.: Russ. Math. Surv. *34*, No. 3, 193–194 (1979). Zbl. 411.55005

Babenko, I.K. (1979b): Some Questions on Rational Homotopic Type. Author's PhD Dissertation review, Moscow, MGU

Babenko, I.K. (1979c): On real homotopic properties of complete intersections. Izv. Akad. Nauk SSSR, Ser. Mat. *43*, No. 5, 1004–1024. English transl.: Math. USSR, Izv. *15*, 241–258 (1980). Zbl. 423.14011

Babenko, I.K. (1980): On analytic properties of Poincaré series of loop spaces. Mat. Zametki *27*, No. 5, 751–765. English transl.: Math. Notes *27*, 359–367 (1980). Zbl. 447.55007

Babenko, I.K. (1981): On generating functions in the rational homotopy theory. Preprint, Novosibirsk, appeared in: Vestn. Mosk. Univ., Ser. I 1985, No. 1, 15–19 (1985). English transl.: Mosc. Univ. Math. Bull. *40*, No. 1, 21–27 (1985). Zbl. 597.55005

Babenko, I.K. (1986a): Problems of growth and rationality in algebra and topology. Usp. Mat. Nauk *41*, No. 2, 95–142. English transl.: Russ. Math. Surv. *41*, No. 2, 117–175 (1986). Zbl. 607.55007

Babenko, I.K. (1986b): Closed geodesics, asymptotic volume and characteristics of group growth. Izv. Akad. Nauk SSSR, Ser. Mat. *52*, No. 4, 675–711. English transl.: Math. USSR, Izv. *33*, No. 1, 1–37 (1989). Zbl. 657.53024

Backelin, J. (1975): On the rationality of some Hilbert series 1. Preprints Univ. Stockholm No. 16

Backelin, J. (1978): La série de Poincaré-Betti d'une algébre graduée de type fini à une relation est rationnelle. C. R. Acad. Sci., Paris, Ser. A *287*, 843–846. Zbl. 395.16025

Backelin, J. (1980): Monomial rings of embedding dimension four have rational Poincaré series. Rept. Dep. Math. Univ. Stockholm No. 14, 15

Backelin, J. (1981): A distributiveness property of augmented algebras and some related homological results. Preprints Univ. Stockholm

Bakhturin, Yu.A. (1985): Identities in Lie Algebras. Moscow, Nauka. English transl.: Utrecht (1987). Zbl. 571.17001

Bakhturin, Yu.A., Ol'shanskij, A.Yu. (1988): Identities. Itogi Nauki Tekh., Ser. Sovrem. Probl. Mat., Fundam. Napravleniya *18*, 117–240. English transl.: Encycl. Math. Sci. *18*, Berlin-Heidelberg-New York, Springer-Verlag, 107–221, 1991. Zbl. 673.16001

Bakhturin, Yu.A., Slin'ko, A.M., Shestakov, I.P. (1981): Nonassociative rings. Itogi Nauki Tekh., Ser. Algebra Topologiya. Geom. *18*, 3–72. English transl.: J. Sov. Math. *18*, 169–211 (1982). Zbl. 486.17001

Bass, H. (1972): The degree of polynomial growth of finitely generated nilpotent groups. Proc. London Math. Soc., III. Ser. *25*, No. 4, 603–614. Zbl. 259.20045

Bejdar, K.I., Latyshev, V.N., Markov, V.T., Mikhalev, A.V., Skornyakov, L.A., Tuganbaev, A.A. (1984): Associative rings. Itogi Nauki Tekh., Ser. Algebra Topologiya Geom. *22*, 3–115. English transl.: J. Sov. Math. *38*, 1855–1929 (1987). Zbl. 564.16002

Belov, A. Ya. (1988): On a Shirshov basis of relative free algebras of complexity n. Mat. Sb., Nov. Ser. *135*, No. 3, 373–384. English transl.: Math. USSR, Sb. *63*, No. 2, 363–374 (1989). Zbl. 659.16012

Belyaev, V. Ya. (1978): Subrings of finitely generated associative rings. Algebra Logika *17*, No. 6, 627–638. English transl.: Algebra Logic *17*, 407–414 (1979). Zbl. 429.16017

Bergman, G. (1978): The diamond lemma for ring theory. Adv. Math. *29*, No. 2, 178–218. Zbl. 326.16019

Birkhoff, G. (1967): Lattice Theory. 3rd edition. Am. Math. Soc., Providence. Zbl. 153,25

Bokut', L.A. (1976): Embeddings in simple associative algebras. Algebra Logika *15*, No. 2, 117–142. English transl.: Algebra Logic *15*, 73–90 (1977). Zbl. 349.16007

Bokut', L.A. (1978): On algebraically closed and simple Lie algebras. Tr. Mat. Inst. Steklova *148*, 30–42. English transl.: Proc. Steklov Inst. Math. *148*, 27–39. Zbl. 443.17007

Bokut', L.A., L'vov, I.V., Kharchenko, V.K. (1988): Non-commutative rings. Itogi Nauki Tekh., Ser. Sovrem. Probl. Mat., Fundam. Napravleniya *18*, 5–116. English transl.: Encycl. Math. Sci. *18*, Berlin-Heidelberg-New York, Springer-Verlag, 1–106, 1991. Zbl. 725.16003

Borho, W., Kraft, H. (1976): Über die Gelfand-Kirillov Dimension. Math. Ann. *220*, No. 1, 1–24. Zbl. 306.17005

Borisenko, V.V. (1985): On matrix representation of finitely generated algebras, given by a finite number of relations. Vestn. Mosk. Univ., Ser. I 1985, No. 4, 75–77. English transl.: Mosc. Univ. Math. Bull. *40*, No. 4, 80–83 (1985). Zbl. 579.16012

Braun, A. (1982): The radical in a finitely generated PI-algebra. Bull. Am. Math. Soc., New Ser. *7*, No. 2, 385–386. Zbl. 493.16011

Buchberger, B. (1983): Grobner Bases: An algorithmic method in polynomial ideal theory. CAMP Bull. *290*, No. 83. See also: Math. Appl., D. Reidel Publ. Co. *16*, 184–232 (1985). Zbl. 587.13009

Buchberger, B., Collins, G.E., Loos, R. (1982): Computer Algebra. Symbolic and Algebraic Computation. Wien, New York, Springer-Verlag. Zbl. 491.00019

Chekanu, G.P. (1988): On local finiteness of algebras. Mat. Issled. *105*, 153–171. Zbl. 681.16010

Cohn, P.M. (1971): Free Rings and Their Relations. London, New York, Academic Press. Zbl. 232.16003

Dejean, F. (1972): Sur un theorem de Thue. J. Comb. Theor., Ser. A *13*, 90–99. Zbl. 245.20052

Dicks, W. (1985): On the cohomology of one-relator associative algebras. J. Algebra *97*, 79–100. Zbl. 588.16014

Drenski, V.S. (1974): On identities in Lie algebras. Algebra Logika *13*, No. 3, 265–290. English transl.: Algebra Logic *13*, 150–165 (1975). Zbl. 298.17011

Drenski, V.S. (1981a): Representations of the Symmetric group and varieties of linear algebras. Mat. Sb., Nov. Ser. *115*, 98–115. English transl.: Math. USSR, Sb. *43*, 85–101 (1982). Zbl. 465.17007

Drenski, V.S. (1981b): A minimal base of identities of a matrix algebra of second order over the field of characteristic zero. Algebra Logika *20*, 282–290. English transl.: Algebra Logic *20*, 188–194 (1982). Zbl. 496.16017

Drensky, V. (1984a): Codimensions of T-ideals and Hilbert series of relatively free algebras. J. Algebra *91*, No. 1, 1–17. Zbl. 552.16006

Drensky, V. (1984b): On the Hilbert series of relatively free algebras. Commun. Algebra *12*, No. 19, 2335–2347. Zbl. 549.16009

Drensky, V. (1985): T-ideals containing all matrix polynomial identities. Commun. Algebra *13*, 2037–2072. Zbl. 578.16005

Drensky, V., Popov, A. (1987): Prime varieties of associative algebras. Proc. 16th Spring Conf., Sunny Beach/Bulg. 1987, 35–52 (1987). Zbl. 632.16015

Drinfel'd, V.G. (1986): Quantum groups. Zap. Nauchn. Semin. Leningr. Otd. Mat. Inst. Steklova *155*, 18–49. English transl.: J. Sov. Math. *41*, 898–915 (1988). Zbl. 617.16004

Dubnov, Ya. S., Ivanov, V.K. (1943): On reducing the degree of affinor polynomials. Dokl. Akad. Nauk SSSR *41*, 95–98. Zbl. 60,33

Fejgin, B.L., Fuks, D.B. (1988): Cohomology of groups and Lie algebras. Itogi Nauki Tekh., Ser. Sovrem. Probl. Mat., Fundam. Napravleniya *21*, 121–209. English transl. in: Encycl. Math. Sciences *21*, Berlin-Heidelberg-New York, Springer-Verlag (in preparation). Zbl. 653.17008

Fröberg, T., Gulliksen, T., Löfwall, C. (1986): Flat families of local, artinian algebras with an infinite number of Poincaré series. Algebra, algebraic topology and their interactions, Proc. Conf. Stockholm 1983, Lect. Notes Math. *1183*, 170–191. Zbl. 588.13012

Furstenberg, H. (1981): Poincaré recurrence and number theory. Bull. Am. Math. Soc., New Ser. *5*, No. 3, 211–234. Zbl. 481.28013

Gateva-Ivanova, T. (1983): On the PI-degree of the tensor product of PI-algebras. C. R. Acad. Bulg. Sci. *36*, 1367–1370. Zbl. 532.16013

Gateva-Ivanova, T. (1987): Algorithmic determination of the Jacobson radical of monomial algebras. Preprint, Sofiya

Gateva-Ivanova, T. (1989a): On Noetherianity of some associative finitely presented algebras. Internat. Conference on Algebra. Abstracts on theory of rings, algebras and modules. Novosibirsk, 1989, 179. See also: J. Algebra *138*, No. 1, 13–35 (1991). Zbl. 723.16012

Gateva-Ivanova, T. (1989b): Global dimension of associative algebras. Lect. Notes Comput. Sci. *357*, 213–229. Zbl. 679.16020

Gateva-Ivanova, T., Latyshev, V. (1988): On the recognizable properties of associative algebras. Spec. volume J.S.C. On Computational Aspects in Commutative Algebras. London, Acad. Press, 237–254. See also: J. Symb. Comput. *6*, No. 2/3, 371–388 (1988). Zbl. 663.68045

Gel'fand, I.M., Kirillov, A.A. (1966): Sur les corps liés aux algèbres enveloppantes des algèbres de Lie. Publ. Math., Inst. Hautes Étud. Sci. *31*, 509–523. Zbl. 144,21

Gel'fand, S.I., Manin, Yu. I. (1989): Homological Algebra. Itogi Nauki Tekh., Ser. Sovrem. Probl. Mat., Fundam. Napravleniya *38*, 5–238. English transl. in: Encycl. Math. Sciences *38*, Berlin-Heidelberg-New York, Springer-Verlag (in preparation). Zbl. 718.18007

Gerasimov, V.N. (1976): Distributive lattices of subspaces and the problem of equality for algebras with one relation. Algebra Logika *15*, No. 4, 384–435. English transl.: Algebra Logic *15*, 238–274 (1977). Zbl. 372.08001

Golod, E.S. (1959): On the cohomology ring of a finite p-group. Dokl. Akad. Nauk SSSR *125*, No. 4, 703–706. Zbl. 99,388

Golod, E.S. (1962): On homologies of some local rings. Dokl. Akad. Nauk SSSR *144*, No. 3, 479–482. English transl.: Sov. Math., Dokl. *3*, 745–749 (1962). Zbl. 122,42

Golod, E.S. (1964): On nil-algebras and finitely approximable p-groups. Izv. Akad. Nauk SSSR, Ser. Mat *28*, No. 2, 273–276. English transl.: Am. Math. Soc., Transl., II. Ser. *48*, 103–106 (1965). Zbl. 215,392

Golod, E.S. (1978): On homologies of some local rings. Usp. Mat. Nauk *33*, No. 5, 177–178. English transl.: Russ. Math. Surv. *33*, 185–186 (1978). Zbl. 417.13010

Golod, E.S. (1988): Standard bases and homology. Lect. Notes. Math. *1352*, 88–95. Zbl. 657.13013

Golod, E.S., Shafarevich, I.R. (1964): On tower of class fields. Izv. Akad. Nauk SSSR, Ser. Mat. *28*, No. 2, 261–272

Govorov, V.E. (1972): On graded algebras. Mat. Zametki *12*, No. 2, 197–204. English transl.: Math. Notes *12*, 552–556 (1973). Zbl. 239.16002

Govorov, V.E. (1973a): On the dimension of graded algebras. Mat. Zametki *14*, No. 2, 209–216. English transl.: Math. Notes *14*, 678–682 (1974). Zbl. 277.16016

Govorov, V.E. (1973b): Dimension and multiplicity of graded algebras. Sib. Mat. Zh. *14*, No. 6, 1200–1206. English transl.: Sib. Math. J. *14*, 840–845 (1974). Zbl. 277.16017

Grigorchuk, R.I. (1978): Symmetric random walks on discrete groups. Multicomponent random systems, Adv. Probab. rel. Topics, Vol. 6, 285–325 (1980). Zbl. 475.60007

Grigorchuk, R.I. (1980): The Burnside problem on periodic groups. Funkts. Anal. Prilozh. *14*, No. 1, 53–54. English transl.: Funct. Anal. Appl. *14*, 41–43 (1980). Zbl. 595.20029

Grigorchuk, R.I. (1983): On Milnor's problem of group growth. Dokl. Akad. Nauk SSSR *271*, No. 1, 30–33. English transl.: Sov. Math., Dokl. *28*, 23–26 (1983). Zbl. 547.20025

Grigorchuk, R.I. (1984a): Degrees of growth of finitely generated groups and the theory of invariant means. Izv. Akad. Nauk SSSR, Ser. Mat. *48*, No. 5, 939–985. English transl.: Math. USSR, Izv. *25*, 259–300 (1985). Zbl. 583.20023

Grigorchuk, R.I. (1984b): Construction of p-groups of intermediate growth, with a continuum of quotient groups. Algebra Logika *23*, No. 4, 383–394. English transl.: Algebra Logic *23*, 265–273 (1984). Zbl. 573.20037

Grigorchuk, R.I. (1985): On the growth rates of p-groups and torsion-free groups. Mat. Sb., Nov. Ser. *126*, No. 2, 194–214. English transl.: Math. USSR, Sb. *54*, 185–205 (1986). Zbl. 568.20033

Grigorchuk, R.I. (1989): On the Hilbert-Poincaré series of graded algebras associated with groups. Mat. Sb. *180*, No. 2, 207–225. English transl.: Math. USSR, Sb. *66*, No. 1, 211–229 (1990). Zbl. 695.16009

Gromov, M. (1981): Groups of polynomial growth and expanding maps. Publ. Math. Inst. Hautes Étud. Sci. *53*, 53–78. Zbl. 474.20018

Gromov, M. (1987): Hyperbolic groups. Essays Group Theory, Publ., Math. Sci. Res. Inst. *8*, 75–263. Zbl. 634.20015

Gulliksen, T.H. (1972): Massey operations and the Poincaré series of certain local rings. J. Algebra *22*, 225–232. Zbl. 243.13015

Gulliksen, T.H., Levin, G. (1969): Homology of Local Rings. Queen's Papers Pure and Appl. Math., No. 20. Zbl. 208,303

Green, E.L. (1983): Graphs with relations, coverings and group graded algebras. Trans. Am. Math. Soc. *279*, 297–310. Zbl. 536.16001

Hall, M.J. (1967): Combinatorial Theory. Waltham (Massachusetts), Toronto-London, Blaisdell Publishing Company. Zbl. 196,24

Hall, P., Higman, G. (1956): On the p-length of p-solvable groups and reduction theorem for Burnside's problem. Proc. Lond. Math. Soc., III. Ser. *6*, No. 3, 1–42. Zbl. 73,255

Halperin, S. (1977): Finiteness in the minimal models of Sullivan. Trans. Am. Math. Soc. *230*, 173–199. Zbl. 364.55014
Halperin, S., Levin, G. (1986): High sheleta of CW complexes. Lect. Notes Math. *1183*, 211–217. Zbl. 607.55006
Halperin, S., Stasheff, J. (1979): Obstructions to homotopy equivalences. Adv. Math. *32*, 233–279. Zbl. 408.55009
Herstein, I. (1968): Noncommutative Rings. New York, Wiley. Zbl. 177,58
Higman, G. (1957): Groups and rings having automorphisms without non-trivial fixed points. J. Lond. Math. Soc. *32*, No. 3, 321–334. Zbl. 79,32
Higman, G. (1960): Lie ring methods in the theory of finite nilpotent groups. Proc. Int. Congr. Math. 1958, 307–312. Zbl. 122,274
Higman, G. (1961): Subgroups of finitely presented groups. Proc. R. Soc. Lond., Ser. A *262*, 455–475. Zbl. 104,21
Jacobson, C. (1985): Finitely presented graded Lie algebras and homomorphisms of local rings. J. Pure Appl. Algebra *38*, 243–253. Zbl. 575.13010
Jacobson, C., Kustin, R., Miller, M. (1985): The Poincaré series of a codimension four Gorenstein ring is rational. J. Pure Appl. Algebra *38*, 255–275. Zbl. 575.13007
Kac, V.G. (1968): Simple irreducible graded Lie algebras of finite growth. Izv. Akad. Nauk SSSR, Ser. Mat. *32*, 1323–1367. English transl.: Math. USSR, Izv. *2*, 1271–1311 (1970). Zbl. 222.17007
Kac, V.G. (1983): Infinite Dimensional Lie Algebras. Boston-Basel-Stuttgart, Birkhäuser. Zbl. 537.17001
Kandri-Rody, A., Weispfenning, V. (1987): Non-commutative Gröbner bases in algebras of solvable type. Preprint, Univ. Passau, appeared in: J. Symb. Comput. *9*, No. 1, 1–26 (1990). Zbl. 715.16010
Kegel, O. (1963): Zur Nilpotenz gewisser assoziativer Ringe. Math. Ann. *149*, 258–260. Zbl. 106,254
Kemer, A.R. (1980a): Non-matrix varieties. Algebra Logika *19*, No. 3, 255–283. English transl.: Algebra Logic *19*, 157–178 (1981). Zbl. 467.16025
Kemer, A.R. (1980b): Kapelli identities and nilpotency of the radical of a finitely generated PI-algebra. Dokl. Akad. Nauk SSSR *225*, No. 4, 793–797. English transl.: Sov. Math., Dokl. *22*, 750–753 (1980). Zbl. 489.16011
Kemer, A.R. (1984): Varieties and $\mathbb{Z}_2$-graded algebras. Izv. Akad. Nauk SSSR, Ser. Mat. *48*, No. 5, 1042–1059. English transl.: Math. USSR, Izv. *25*, 359–374 (1985). Zbl. 586.16010
Kemer, A.R. (1987): Finite basis property of identities of associative algebras. Algebra Logika *26*, No. 5, 597–641. English transl.: Algebra Logic *26*, No. 5, 362–397 (1987). Zbl. 646.16013
Kemer, A.R. (1988): Representability of reduced free algebras. Algebra Logika *27*, No. 2, 274–294. English transl.: Algebra Logic *27*, No. 3, 274–294 (1988). Zbl. 678.16012
Kharlampovich, O.G. (1989): Equality problem for solvable Lie algebras and groups. Mat. Sb. *180*, No. 8, 1033–1066. English transl.: Math. USSR, Sb. *67*, No. 2, 489–525 (1990)
Kirillov, A.A. (1989) On identities in Lie algebras of vector fields. Vestn. Mosk. Univ., Ser. I 1989, No. 2, 11–13. English transl.: Mosc. Univ. Math. Bull. *44*, No. 2, 14–17 (1989). Zbl. 707.17004
Kirillov, A.A., Kontsovich, M.L., Molev, A.I. (1983): Algebras of intermediate growth. Preprint. Inst. Prikl. Mat. Akad. Nauk SSSR, No. 39. English transl.: Sel. Math. Sov. *9*, No. 2, 137–153 (1990). Zbl. 684.17008
Kirillov, A.A., Ovsienko, V.Yu., Udalova, O.D. (1984): On identities in the Lie algebra of vector fields on the real line. Preprint. Inst. Prikl. Mat. Akad. Nauk SSSR, No. 135. English transl.: Sel. Math. Sov. *10*, No. 1, 7–17 (1991). Zbl. 748.17017
Kobayashi, Y. (1978): The Hilbert series of some graded algebras and the Poincaré series of some local rings. Math. Scand. *42*, No. 1, 19–33. Zbl. 388.13016

Kolotov, A.T. (1981): Aperiodic sequences and functions of growth of algebras. Algebra Logika *20*, No. 2, 138–154. English transl.: Algebra Logic *20*, 95–105 (1982). Zbl. 535.16020

Kostrikin, A.I. (1974): Some related questions in the theory of groups and Lie algebras. Lect. Notes Math. *372*, 409–416. Zbl. 297.20046

Kostrikin, A.I. (1986): Around Burnside. Moscow, Nauka. English transl.: Berlin-Heidelberg-New York, Springer-Verlag 1990. Zbl. 702.17001

Kostrikin, A.I., Shafarevich, I.R. (1957): Homology groups of nilpotent algebras. Dokl. Akad. Nauk SSSR *115*, No. 6, 1066–1069. Zbl. 83,30

Koszul, J.L. (1951): Sur un type d'algèbres differentielles en rapport avec la transgression. Colloque topologie, Bruxelles 1950, 73–81. Zbl. 45,308

Krause, G.R., Lenagan, T.H. (1985): Growth of Algebras and Gelfand-Kirillov Dimension. London, Pitman Publ. Zbl. 564.16001

Kreknin, V.A., Kostrikin A.I. (1963): On Lie algebras with regular automorphism. Dokl. Akad. Nauk SSSR *149*, No. 2, 249–251. English transl.: Sov. Math., Dokl. *4*, 355–358 (1963). Zbl. 125,289

Krempa, J. (1972): Logical connections between some open problems, concerning nil-rings. Fundam. Math. *76*, 121–130. Zbl. 214,292

Krempa, J., Okniński, J. (1987): Gelfand-Kirillov dimension of a tensor product. Math. Z. *194*, 487–494. Zbl. 595.16019

Kukin, G.P. (1977): On the equality problem for Lie algebras. Sib. Mat. Zh. *18*, No. 5, 1194–1197. English transl.: Sib. Math. J. *18*, 849–851 (1978). Zbl. 383.17006

Kukin, G.P. (1978): Bases of a free Lie algebra. Mat. Zametki *24*, No. 3, 375–382. English transl.: Math. Notes *24*, 700–704 (1979). Zbl. 404.17013

Kukin, G.P. (1980): On embeddings of recursively defined Lie algebras and groups. Dokl. Akad. Nauk SSSR *251*, No. 1, 37–39. English transl.: Sov. Math., Dokl. *21*, 378–381 (1980). Zbl. 447.20026

Kukin, G.P. (1983): Problems of equalities and free products of Lie algebras and associative algebras. Sib. Mat. Zh. *24*, No. 2, 85–96. English transl.: Sib. Math. J. *24*, 221–231 (1983). Zbl. 519.17009

Kuz'min, E.N. (1975): On Nagata-Higman theorem. Mathematical structures, Sofiya, 101–107

Latyshev, V.N. (1972): On the Regev theorem on identities of the tensor product of PI-algebras. Usp. Mat. Nauk *27*, No. 4, 213–214. Zbl. 254.16013

Latyshev, V.N. (1976): Partially ordered sets and non-matrix identities of associative algebras. Algebra Logika *15*, No. 1, 53–70. English transl.: Algebra Logic *15*, 34–45 (1977). Zbl. 358.16012

Latyshev, V.N. (1982): Commutativity of PI-algebras of polynomial type. Algebra. Collection of papers devoted to the 90th anniversary of birth of O.Yu. Shmidt, Moscow, 86–94. Zbl. 529.16026

Latyshev, V.N. (1988): Combinatorial Ring Theory. Standard Bases. Moscow, MGU. Zbl. 668.13001

Le Bruyn, L. (1985): The functional equations for Poincaré series of trace rings of generic 2×2 matrices. Isr. J. Math. *52*, 355–360. Zbl. 587.16014

Lejtes, D.A. (1984): Lie superalgebras. Itogi Nauki Tekh., Ser. Sovrem. Probl. Mat. *25*, 3–49. English transl.: J. Sov. Math. *30*, 2481–2512 (1985). Zbl. 567.17003

Lemaire, J.-M. (1971): A finite complex whose rational homotopy is not finitely generated. Lect. Notes Math. *196*, 114–120. Zbl. 216,449

Lemaire, J.-M. (1974): Algèbres connexes et homologie des espaces de lacets. Lect. Notes Math. *422*. Zbl. 293.55004

Lemaire, J.-M. (1982): Anneaux locaux et espaces de lacets a séries de Poincaré irrationelles. Lect. Notes Math. *901*, 145–156. Zbl. 481.13008

Lemaire, J.-M., Sigrist, F. (1978): Dénombrement de types d'homotopie rationelle. C. R. Acad. Sci., Paris, Ser. A *287*, 109–112. Zbl. 382.55005

Lescot, J. (1985): Asymptotic properties of Betti numbers of modules over certain rings. J. Pure Appl. Algebra *38*, 287–298. Zbl. 602.13004

Lescot, J. (1986): Series de Bass des modules de syzygie. Lect. Notes Math. *1183*, 277–290. Zbl. 594.13012

Levin, G. (1974): Two conjectures in the homology of local rings. J. Algebra *30*, No. 1, 56–74. Zbl. 284.13015

Levin, G. (1975): Local rings and Golod homomorphisms. J. Algebra *37*, No. 2, 266–289. Zbl. 324.13022

Levin, G. (1978): Poincaré series of modules over local rings. Proc. Am. Math. Soc. *72*, No. 1, 6–10. Zbl. 407.13020

Levin, G. (1980): Large homomorphisms of local rings. Math. Scand. *46*, No. 2, 209–215. Zbl. 472.13010

Löfwall, C. (1975): On the Poincaré series for a class of local rings. Preprint, Dept. Math. Univ. Stockholm, No. 8

Löfwall, C. (1979): Une algèbre nilpotent dont la série de Poincaré-Betti est non-rationelle. C. R. Acad. Sci., Paris, Ser. A *288*, 327–330. Zbl. 408.16021

Löfwall, C. (1986): On the subalgebra generated by the one-dimensional elements in the Yoneda Ext-algebra. Lect Notes Math. *1183*, 291–338. Zbl. 595.16020

Löfwall, C., Roos, J.-E. (1980): Cohomologie des algèbres de Lie graduées et séries de Poincaré-Betti non-rationnelles. C. R. Acad. Sci., Paris, Ser. A *290*, 733–736. Zbl. 449.13011

Lyndon, R.C., Schupp, P.E. (1977): Combinatorial Group Theory. Berlin-Heidelberg-New York, Springer-Verlag. Zbl. 368.20023

MacLane, S. (1963): Homology. Berlin-Heidelberg-New York, Springer-Verlag. Zbl. 133,265

Magnus, W. (1950): A connection between the Baker-Hausdorff formula and a problem of Burnside. Ann. Math., II. Ser. *52*, 111–126. Zbl. 37,304

Mahler, K. (1930): Arithmetische Eigenschaften einer Klasse transzendental-transzendenter Funktionen. Math. Z. *32*, 545–585. FdM. 56,186

Manin, Yu.I. (1987): Some remarks on Koszul algebras and quantum groups. Ann. Inst. Fourier *37*, No. 4, 191–205. Zbl.625.58040

Manin, Yu.I. (1988): Quantum Groups and Non-commutative Geometry. Centre de Recherches Math. (CRM), Montreal, Univ. de Montreal C.P. Zbl. 724.17006

Markov, V.T. (1988): The Gel'fand-Kirillov dimension: nilpotency, representability, non-matrix varieties. Siberian school on varieties of algebraic systems. Abstracts, Barnaul, 43–45. Zbl. 685.00002

Mikhalev, A.A. (1989): A composition lemma and the equality problem for colored Lie superalgebras. Vestn. Mosk. Univ., Ser. I 1989 No. 5, 88–91. English transl.: Mosc. Univ. Math. Bull. *44*, No. 5, 87–90 (1989). Zbl. 705.17004

Milnor, J. (1968a): Growth of finitely generated solvable groups. J. Differ. Geom. *2*, No. 4, 447–449. Zbl. 176,298

Milnor, J. (1968b): Problem 5603. Am. Math. Mon. *75*, No. 6, 685–686

Milnor, J. (1968c): A note on curvature and fundamental groups. J. Differ. Geom. *2*, 1–7. Zbl. 162,254

Milnor, J., Moore, J. (1965): On the structure of Hopf algebras. Ann. Math., II. Ser. *81*, No. 2, 211–264. Zbl. 163,282

Mora, F. (1985): Gröbner bases for noncommutative polynomial rings. Lect. Notes Comput. Sci. *229*, 353–362. Zbl. 659.16003

Mora, F. (1988): Seven variations on standard bases. Preprint, No. 45, Genova

Mora, F. (1989): Gröbner bases in noncommutative algebras. Proc. ISSAC 88, Lect. Notes Comput. Sci. *358*, 150–161. Zbl. 706.68006

Nesterenko, N.S. (1983): Determining a base of a generalized Clifford algebra. In the book: VII All-union Algebraic Conference, Minsk

Novikov, P.S., Adyan, S.I. (1968): On infinite periodic groups I, II, III. Izv. Akad. Nauk SSSR, Ser. Mat. *32*, No. 1, 212–244, No. 2, 251–524, No. 3, 709–731. English transl.: Math. USSR, Izv. *2*, 209–236, 241–480, 665–685 (1969). Zbl. 194,33

Okniński, J. (1987): On monomial algebras. Arch. Math. *50*, 417–423. Zbl. 627.20042

Ol'shanskij, A.Yu. (1970): On the problem of finite basis of identities in groups. Izv. Akad. Nauk SSSR, Ser. Mat. *34*, No. 2, 376–384. Zbl. 215,105

Ol'shanskij, A. Yu. (1982): Groups of bounded period with subgroups of prime order. Algebra Logika *21*, No. 5, 553–618. English transl.: Algebra Logic *21*, 369–418 (1983). Zbl. 524.20024

Ol'shanskij, A.Yu., Shmel'kin, A.L. (1989): Infinite groups. Itogi Nauki Tekh., Ser. Sovrem. Probl. Mat., Fundam. Napravleniya *37*, 5–113. English transl. in: Encycl. Math. Sc. *37*. Berlin-Heidelberg-New York, Springer-Verlag (in preparation). Zbl. 715.20002

Passi, Inder Bir S. (1979): Group rings and their augmentation ideals. Lect. Notes Math. *715*. Zbl. 405.20007

Razmyslov, Yu.P. (1971): On Engel Lie algebras. Algebra Logika *10*, No. 1, 33–34. English transl.: Algebra Logic *10*, 21–29 (1972). Zbl. 253.17005

Razmyslov, Yu.P. (1973a): On finite basing of identities of a matrix algebra of second order over a field of characteristic zero. Algebra Logika *12*, No. 1, 83–113. English transl.: Algebra Logic *12*, 47–63 (1974). Zbl. 282.17003

Razmyslov, Yu.P. (1973b): On a problem of Kaplansky. Izv. Akad. Nauk SSSR, Ser. Mat. *37*, No. 3, 483–501. English transl.: Math. USSR, Izv. *7*, 479–496 (1974). Zbl. 314.16016

Razmyslov, Yu.P. (1974): On the Jacobson radical in PI-algebras. Algebra Logika *13*, No. 3, 337–360. English transl.: Algebra Logic *13*, 192–204 (1975). Zbl. 354.16008

Razmyslov, Yu.P. (1978): On a problem of Hall and Higman. Izv. Akad. Nauk SSSR, Ser. Mat. *42*, No. 4, 833–847. English transl.: Math. USSR, Izv. *13*, 133–146 (1979). Zbl. 394.20030

Regev, A. (1971): Existence of polynomial identities in $A \otimes B$. Bull. Am. Math. Soc. *77*, No. 6, 1067–1069. Zbl. 225.16012

Roos, J.E. (1978): Sur l'algèbre Ext de Yoneda d'un anneau local de Golod. C. R. Acad. Sci., Paris, Ser. A *286*, 9–12. Zbl. 374.13018

Roos, J.E. (1979): Relations between the Poincaré-Betti series of loop spaces and of local rings. Lect. Notes Math. *740*, 285–322. Zbl. 415.13012

Roos, J.E. (1981): Homology of loop spaces and of local rings. 18th Scand. Congr. Math. Aarhus 1980, Prog. Math. *11*, 441–468. Zbl. 512.13015

Salomaa, A. (1981): Jewels of Formal Language Theory. Rockville: Comput. Sci. Press and London, Pitman. Zbl. 487.68064

Sanov, I.N. (1951): On a system of relations in periodic groups with the period equal to a prime power. Izv. Akad. Nauk SSSR, Ser. Mat. *15*, No. 1, 477–502. Zbl. 45,302

Sapir, M.V. (1987): Problems of Burnside type and finite based in varieties of semigroups. Izv. Akad. Nauk SSSR, Ser. Mat. *51*, No. 2, 319–340. English transl.: Math. USSR, Izv. *30*, No. 2, 295–314 (1988). Zbl. 646.20047

Sapir, M.V. (1989): A minimal variety of associative algebras with unsolvable equality problem. Mat. Sb. *180*, No. 12, 1691–1708. English transl.: Math. USSR, Sb. *68*, No. 2, 567–584 (1990). Zbl. 694.16014

Serre, J-P. (1951): Homologie singulière des espaces fibrés. Ann. Math., II. Ser. *54*, 425–505. Zbl. 45,260

Serre, J-P. (1965): Algèbre locale. Multiplicités. Lect. Notes Math. *11*. Zbl. 142,286

Shafarevich, I.R. (1972): Foundations of Algebraic Geometry. Moscow, Nauka. English transl.: Berlin-Heidelberg-New York, Springer-Verlag 1974. Zbl. 258.14001. 2nd ed. (1988). Zbl. 675.14001

Shafarevich, I.R. (1986): Basic notions of algebra. Itogi Nauki Tekh., Ser. Sovrem. Probl. Mat., Fundam. Napravleniya *11*, 290 p. English transl. in: Encyclopaedia of Mathematical Sciences *11*, Berlin-Heidelberg-New York, Springer-Verlag 1990. Zbl. 655.00002, Zbl. 711.16001

Shamash, J. (1969): The Poincaré series of a local ring. J. Algebra *12*, 453–470. Zbl. 189,40
Shearer, J.B. (1980): A graded algebra with non-rational Hilbert series. J. Algebra *62*, No. 1, 228–231. Zbl. 436.16001
Shirshov, A.I. (1957) On rings with identity relations. Mat. Sb., Nov. Ser. *41*, No. 3, 277–283. Zbl. 78,24
Shirshov, A.I. (1957): On some non-associative nil rings and algebraic algebras. Mat. Sb. *44*, No. 3, 381–394. Zbl. 78,22
Shirshov, A.I. (1962a): Some algorithmic problems for Lie algebras. Sib. Mat. Zh. *3*, No. 2, 292–296. Zbl. 104,260
Shirshov, A.I. (1962b): On bases of free Lie algebras. Algebra Logika *1*, No. 1, 14–19. Zbl. 145,258
Shirshov, A.I. (1984): Rings and Algebras. Moscow, Nauka. Zbl. 565.01015
Sjödin, G. (1980): Hopf algebras and derivations. J. Algebra *64*, No. 1, 218–229. Zbl. 429.16008
Small, L.W., Stafford, J., Warfield, R. (1985): Affine algebras of Gelfand-Kirillov dimension one are PI. Math. Proc. Camb. Philos. Soc. *97*, 407–414. Zbl. 561.16005
Tate, J. (1957): Homology of Noetherian rings and local rings. Ill. J. Math. *1*, 14–27. Zbl. 79,55
Tits, J. (1972): Free subgroups in linear groups. J. Algebra *20*, No. 2, 250–270. Zbl. 236.20032
Trofimov, V.I. (1980): The growth function of finitely generated semigroups. Semigroup Forum *21*, 351–360. Zbl. 453.20047
Trofimov, V.I. (1983): Bounded graph automorphisms and a characterization of lattices. Izv. Akad. Nauk SSSR, Ser. Mat. *47*, No. 2, 407–420. English transl.: Math. USSR, Izv. *22*, 379–391. Zbl. 519.05037
Trofimov, V.I. (1984a): Graphs with polynomial growth. Mat. Sb., Nov. Ser. *123*, No. 3, 407–421. English transl.: Math. USSR, Sb. *51*, 405–417 (1985). Zbl. 548.05033
Trofimov, V.I. (1984b): Growth functions of the permutation groups. Tr. Inst. Mat. *4*, 118–138. Zbl. 604.20003
Trofimov, V.I. (1985): Groups of graph automorphisms as topological groups. Mat. Zametki *38*, No. 3, 378–385. English transl.: Math. Notes *38*, 717–720 (1985). Zbl. 596.05033
Trofimov, V.I. (1986): Action of a group on a graph. Izv. Akad. Nauk SSSR, Ser. Mat. *50*, No. 5, 1077–1096. English transl.: Math. USSR, Izv. *29*, 429–447 (1987). Zbl. 616.05040
Tsejtin, G.S. (1958): Associative computations with unsolvable equivalency problem. Tr. Mat. Inst. Steklova *52*, 172–189. Zbl. 87,253
Ufnarovskij, V.A. (1978): The growth of algebras. Vestn. Mosk. Univ., Ser. I 1978, No. 4, 59–65. English transl.: Mosc. Univ. Math. Bull. *33*, No. 4, 47–52 (1978). Zbl. 392.16025
Ufnarovskij, V.A. (1980): Poincaré series of graded algebras. Mat. Zametki *27*, No. 1, 21–32. English transl.: Math. Notes *27*, 12–18 (1980). Zbl. 432.16018
Ufnarovskij, V.A. (1982): A growth criterion for graphs and algebras defined by words. Mat. Zametki *31*, No. 3, 465–472. English transl.: Math. Notes *31*, 238–241 (1982). Zbl. 491.05041
Ufnarovskij, V.A. (1984): Algebras, defined by two quadratic relations. Mat. Issled. *76*, 148–171. Zbl. 566.16010
Ufnarovskij, V.A. (1985): An independence theorem and its consequences. Mat. Sb., Nov. Ser. *128*, No. 1, 124–132. English transl.: Math. USSR, Sb. *56*, 121–129 (1987). Zbl. 598.15002
Ufnarovskij, V.A. (1987): On finite-definiteness of Hamiltonian algebras. Mat. Issled. *91*, 103–112. Zbl. 631.17009
Ufnarovskij, V.A. (1989a): The use of graphs for computing basis, growth and Hilbert series of associative algebras. Mat. Sb. *180*, No. 11, 1548–1550. English transl.: Math. USSR, Sb. *68*, No. 2, 417–428 (1990). Zbl. 685.16007

Ufnarovskij, V.A. (1989b): On regular words in the sense of Shirshov. International Conference on Algebra; Abstracts in theory of rings, algebras and modules, Novosibirsk, 140

Vershik, A.M. (1984): Algebras with quadratic relations. Spectral theory of operators and infinite-dimensional analysis, Collect. Sci. Works, Kiev 1984, 32–57 (1984). Zbl. 581.16017

Weyman, J. (1985): On the structure of free resolutions of length 3. Preprint, appeared in: J. Algebra *126*, 1–33 (1989). Zbl. 705.13008

Wisliceny, J. (1979): Optimalitätsuntersuchung zum Satz von Golod-Schafarewitsch. Preprint Zentralinstitut für Mathematik und Mechanik, Berlin. Zbl. 418.20032

Wolf, J. (1968): Growth of finitely generated solvable groups and curvature of Riemannian manifolds. J. Differ. Geom. *2*, No. 4, 421–446. Zbl. 207,518

Zariski, O., Samuel, P. (1958, 1960): Commutative Algebra. Vol. I, II. Toronto, London, New York, Van Nostrand. Zbl. 81,265; Zbl. 121,278

Zel'manov, E.I. (1983): Lie algebras with algebraic adjoint representation. Mat. Sb., Nov. Ser. *121*, No. 4, 545–561. English transl.: Math. USSR, Sb. *49*, 537–552 (1984). Zbl. 544.17003

Zel'manov, E.I. (1984): Lie algebras with finite grading. Mat. Sb., Nov. Ser. *124*, No. 3, 353–392. English transl.: Math. USSR, Sb. *52*, 347–385 (1985). Zbl. 546.17005

Zel'manov, E.I. (1988): On the nilpotency of nil algebras. Lect. Notes Math. *1352*, 227–240. Zbl. 657.17001

Zel'manov, E.I. (1989): On some problems of Lie groups and algebras. Mat. Sb. *180*, No. 2, 159–167. English transl.: Math. USSR, Sb. *66*, No. 1, 159–168 (1990). Zbl. 673.17007

Zel'manov, E.I. (1990): A solution of the restricted Burnside problem for groups of odd exponent. Izv. Akad. Nauk SSSR, Ser. Mat. *1*, 42–59. English transl.: Math. USSR, Izv. *36*, No. 1, 41–60 (1991). Zbl. 704.20030

Zel'manov, E.I., Kostrikin, A.I. (1990): A theorem on sandwich algebras. Tr. Mat. Inst. Steklova *183*, 106–111. English transl.: Proc. Steklov Inst. Math. *183*, 121–126 (1991). Zbl. 729.17006

Zhevlakov, K.A., Slin'ko, A.M., Shestakov I.P., Shirshov, A.I. (1978): Nearly Associative Rings. Moscow, Nauka. English transl.: New York etc., Academic Press 1982. Zbl. 445.17001

Zimin, A.I. (1980): Semigroup varieties with finiteness conditions for finitely generated semigroups. Ivanov Univ., Ivanovo. Deposited in VINITI 27.10.80, No. 4519-B

Zimin, A.I. (1982): Blocking sets of terms. Mat. Sb., Nov. Ser. *119*, No. 3, 363–375. English transl.: Math. USSR, Sb. *47*, 353–364 (1984). Zbl. 599.20106

Additional References

Almkvist, G. (1990): Commutative and noncommutative invariant theory. Banach Cent. Publ., **26**, Part 2, 259–268. Zbl. 768.20017

Andrews, G.E., Ekhad, S.B., Zeilberger, D. (1993): A short proof of Jacobi's formula for the number of representations of an integer as a sum of four squares. Am. Math. Mon. **100**, 274–276. Zbl. 769.11020

Avramov, L. (1978): Small homomorphisms of local rings. J. Algebra **50**, 400–453. Zbl. 395.13005

Avramov, L. (1992): Problems on infinite free resolutions. Free Resolutions in Commutative Algebra and Algebraic Geometry. Edited by Eisenbud D., Huneke C., Res. Notes Math., 2, Jones and Barlett Publishers, Boston, London, 3–23

Avramov, L. (1994): Local rings over which all modules have rational Poincaré series. J. Pure Appl. Algebra **91**, 29–48

Backelin, J. (1982): A distributiveness property of augmented algebras and some related homological results. Ph. D. Thesis, Stockholm University, Stockholm, 1982

Backelin, J. (1986): On the rates of growth of the homologies of Veronese subrings. Lect. Notes Math. **1183**, 79–100. Zbl. 588.13011

Backelin, J. (1989): Square multiples n give infinitely many cyclic n–roots. Reports Matematiska Institutionen, Stockholms Universitet, No 8

Backelin, J. (1992): Some Homological Properties of "High" Veronese Subrings. J. Algebra **146**, No. 1, 1–17. Zbl. 758.13006

Backelin, J., Fröberg, R. (1985a): Koszul algebras, Veronese subrings and rings with linear resolutions. Rev. Roum. Math. Pures Appl. **30**, 85–97. Zbl. 583.16017

Backelin, J., Fröberg, R. (1985b): Poincaré series of short artinian rings. J. Algebra **96**, No. 2, 495–498. Zbl. 572.13001

Backelin, J., Fröberg, R. (1991): How we proved that there are exactly 924 cyclic 7-roots. Proc. ISAAC'91 (S. M. Watt, ed.), ACM, 103–111

Bakhturin, Yu.A., Mikhalev, A.A., Petrogradskij, V.M., Zaitsev, M.V. (1992): Infinite Dimensional Lie Superalgebras. Walter de Gruyter, De Gruyter expositions in Math. 7. Zbl. 762.17001

Becker, T., Weispfenning, V. (1993): Gröbner Bases. Springer-Verlag, New York Berlin Heidelberg. Zbl. 772.13010

Björck, G. (1985): Functions of modulus one on Z_p whose Fourier transforms have constant modulus. Proc. A. Haar Memorial Conf., Budapest, Colloquia Mathematica Societatis János Bolyai **49**, 193–197. Zbl. 619.43004

Björck, G., Fröberg, R. (1991): A faster way to count the solutions of inhomogeneous systems of algebraic equations, with applications to cyclic n-roots. J.Symb. Comput., **12**, 329–336. Zbl. 751.12001

Björck, G., Fröberg, R. (1994): Methods to "divide out" certain solutions from systems of algebraic equations, applied to find all cyclic 8-roots. Analysis, Algebra and Computers in Mathematics Research. Proc. 21st Nordic Congress of Mathematicians, M. Gyllenberg and L.E. Person, Eds. Lecture Notes Pure and Appl. Math., Marcel Dekker, **156**, 57–70

Bokut', L.A., Kukin, G.P. (1993): Algorithmic and Combinatorial Algebra. Kluwer, Math. Appl. 225

Chiswell, I. (1994): The growth series of HNN extensions. Commun. Algebra **22**, No 8, 2969–2981

Davenport, J.H., Siret, Y., Tournier, E. (1988): Computer Algebra. Academic Press, Harcourt Brace Jovanovich Publishers (2nd ed., Academic Press 1993). Zbl. 679.68058

Ellingsen, Jr., H.W. (1993): Graphs and the growth of monomial algebras. Lect. Notes Pure Appl. Math. **151**, 99–109

Felix, Y., Halperin, S., Thomas, J.-C. (1989): Hopf algebras of polynomial growth. J. Algebra **125**, No. 2, 408–417. Zbl. 676.16008

Fröberg, R. (1985): Rings with monomial relations having linear resolutions. J. Pure Appl. Algebra **38**, 235–241. Zbl. 573.13012

Fröberg, R., Hoa, L.T. (1992): Segre products and Rees algebras of face rings. Commun. Algebra **20**(11), 3369–3380. Zbl. 768.13005

Fröberg, R., Löfwall, C. (1991): On Hilbert series for commutative and noncommutative graded algebras. J. Pure Appl. Algebra **76**, 33–38. Zbl. 741.13007

Gateva-Ivanova, T. (1994): Noetherian properties of skew polynomial rings with binomial relations. Trans. Am. Math. Soc. **343**, No. 1, 203–219

Gosper, R.W. (1978): Decision procedures for indefinite hypergeometric summation. Proc. Natl. Acad. Sci. U.S.A. **75**, 40–42. Zbl. 384.40001

Green, E., Kirkman, E., Kuzmanovich, J. (1991): Finitistic Dimensions of Finite Dimensional Monomial Algebras. J. Algebra **136**, No. 1, 37–50. Zbl. 727.16003

Ivanov, S.V. (1994): The Burnside problem for all sufficiently large exponents. Inter. J. Algebra Comput. **4**, No. 1,2, 1–300

Jordan, C. (1906): Réduction d'un réseau de formes quadratiques ou bilinéaires. J. de Math. (6) **2**, 403–438. FdM 37,136

Kempf G. (1992): Wonderful rings and awesome modules. In: Free Resolutions in Commutative Algebra and Algebraic Geometry. Eisenbud D., Huneke C. (Eds.), Research Notes Math., 2, 47–48, Jones and Barlett Publishers, Boston, London

Kharlampovich, O., Sapir, M. (to appear): Algorithmic problems in varieties

Kirchberg, E., Vaillant, G. (1992): On C^*−algebras having linear, polynomial and subexponential growth. Invent. Math., **108**, 635–652. Zbl. 782.46047

Kobayashi, S., Kobayashi, Y. (1993): On algebras with Gelfand-Kirillov dimension one. Proc. Am. Math. Soc., **119**, No. 4, 1095–1104

Kobayashi, S., Sanami, M. (1990): Growth of two-step solvable Lie algebras. Proc. Am. Math. Soc., **109**, No. 4, 859–863. Zbl. 701.17012

Kobayashi, Y. (1978): The Hilbert series of some graded algebras and the Poincaré series of some local rings. Math. Scand. **42**, 19–33. Zbl. 388.13016

Kostrikin, A.I, Kostrikin, I.A., Ufnarovskij, V.A. (1981): Orthogonal decompositions of simple Lie algebras (type A_n). Tr. Mat. Inst. Steklova **158**, 105–120. English transl.: Proc. Steklov Inst. Math. 4 (1983), 113–129. Zbl. 526.17003

Lichtman, A.I. (1984): Growth in enveloping algebras. Isr. J. Math. **47**, No. 4, 296–304. Zbl. 552.17006

Lichtman, A.I. (1984): Matrix Rings and Linear Groups over a Field of Fractions of Enveloping Algebras and Group Rings. Int. J. Algebra **88**, No. 1, 1–37. Zbl. 536.16023

Lichtman, A., Ufnarovskij, V. (to appear): On Growth of Lie Algebras. To appear in Algebra Colloquium

Löfwall, C. (1986): On the subalgebra, generated by one-dimensional elements in the Yoneda Ext-algebra. Lect. Notes Math. **1183**, 291–338. Zbl. 595.16020

Mathieu, O. (1992): Classification of simple graded Lie algebras of finite growth. Invent. Math. **108**, No. 3, 455–519. Zbl. 769.17018

Mora, T. (1986): Gröbner bases for non-commutative polynomial rings. In: J.Calmet (ed.), AAECC-3, Lect. Notes Comp. Sc. **229**, 353–362. Zbl. 659.16003

Mumford, D. (1970): Varieties defined by quadratic equations. In: Questions on Algebraic Varieties. Marchionna E. (ed.), C.I.M.E. III, Ciclo, Varenna, 1969, 29–100. Zbl. 198.258

Okniński, J. (1990): Semigroup Algebras. Marcel Dekker, New York, Pure and Appl. Math. **138**. Zbl. 725.16001

Priddy, S.B. (1970): Koszul resolution. Trans. Am.Math.Soc. **152**, 39–60. Zbl. 261.18016

Reutenauer, Ch. (1993): Free Lie Algebras. Oxford Sc. Publ., London Math. Soc. Monographs, New series **7**, Clarendon Press, Oxford

Robbiano, L. (ed. (1988): Computational Aspects of Commutative Algebras. J. Symbolic Comput. 6, No. 2–3, 133–388

Roos, J.-E. (1993): Commutative non Koszul algebras having a linear resolution of arbitrary high order. Applications to torsion in loop space homology. C.R.Acad. Sci. Paris **316**, Série I, 1123–1128. Zbl. 785.13004

Roos, J.-E. (1994): A computer-aided study of the graded Lie algebra of a local commutative noetherian ring. J. Pure Appl. Algebra **91**, 255–315

Shirayanagi, K. (1991): A classification of finite-dimensional monomial algebras. Effective methods in algebraic geometry. Prog. Math. **94**, Birkhäuser Boston, 469–481. Zbl. 737.16006

Shmel'kin, A.L. (1973): Wreath products of Lie algebras and their application in the theory of groups. Tr. Mosk. Mat. O-V. **29**, 247–260. English transl.: Trans. Moscow Math. Soc. **29** (1973), 239–252. Zbl. 286.17012

Shneerson, L. (1993): Identities in Finitely Generated Semigroups of Polynomial Growth. J. Algebra **154**, 67–85. Zbl. 770.20024

Small, L. W., Stafford, J.T., Warfield, Jr., R.B. (1985): Affine algebras of Gelfand-Kirillov dimension one are PI. Math. Proc. Soc. Camb. Philos. Soc. **97**, 407–414. Zbl. 561.16005

Stanley, R. (1978): Hilbert Functions of Graded Algebras. Adv. Math. **28**, 57–83. Zbl. 384.13012

Sturmfels, B. (1993): Algorithms in Invariant Theory. Springer-Verlag, Vienna

Ufnarovskij, V.A. (1993): Calculations of growth and Hilbert series by computer. Lect. Notes Pure Appl. Math. **151**, 247–256

Vaughan-Lee, M. (1993): The restricted Burnside problem. Second ed., Oxford Sc. Publications, London Math. Soc. Monographs, New series 8, Clarendon Press, Oxford. Zbl. 713.20001 (1st ed.)

Vaughan-Lee, M., Zelmanov, E.I. (1993): Upper bounds in the restricted Burnside problem. J. Algebra **162**, No. 1, 107–146

Wilf, H.S. (1990): Generatingfunctionology. Academic Press, Inc, Harcourt Brace Jovanovich Publishers, Boston

Wilf, H.S., Zeilberger, D. (1992): An algorithmic proof theory for hypergeometric (ordinary and "q") multisum/integral identities. Invent. Math. **103**, 575–634. Zbl. 782.05009

Zelmanov, E.I. (1993): On additional laws in the Burnside problem for periodic groups. Int. J. Algebra Comput. **3**, No. 4, 583–600

II. Non-Associative Structures

E. N. Kuz'min, I. P. Shestakov

Translated from the Russian
by R. M. Dimitrić

Contents

Both mathematics of the 20th century and theoretical physics include the methods of non-associative algebras in their arsenals more and more actively. It suffices to mention the Jordan algebras that had grown as an apparatus of quantum mechanics. On the other hand, Lie algebras, being non-associative, reflect fundamental properties of such associative objects as Lie groups. The present survey includes basic classes of non-associative algebras, close to a certain degree to the associative algebras: alternative, Jordan and Malcev algebras. We tried, as much as possible, to point out their applications in different areas of mathematics. A separate section is devoted to the survey of the theory of quasigroups and loops. Sections 1–4 have been written by I.P. Shestakov, whereas Sect. 5 and 6 have been written by E.N. Kuz'min. The authors are genuinely grateful to V.D. Belousov who has given them essential assistance in the work on Sect. 6. The authors are also grateful to A.I. Kostrikin and to I.R. Shafarevich for their constructive remarks directed towards the improvement of the manuscript of this survey.

Enumeration of formulas in different sections is independent; when refering to a formula from a different section, the section number is added in front of the formula number.

Note that the references cited with the results are not necessarily pointing to the first authors of those results.

§1. Introduction to Non-Associative Algebras

1.1. The Main Classes of Non-Associative Algebras. Let A be a vector space over a field F. Let us assume that a bilinear multiplication of vectors is defined on A, i.e. the mapping $(u,v) \mapsto uv$ from $A \times A$ into A is given, with the following conditions:

$$(\alpha u + \beta v)w = \alpha(uw) + \beta(vw); \quad u(\alpha v + \beta w) = \alpha(uv) + \beta(uw), \tag{1}$$

for all $\alpha, \beta \in F$; $u, v, w \in A$. In this case, the vector space A, together with the multiplication defined on it is called an *algebra* over the field F.

An algebra over an associative-commutative ring Φ, with unity is defined analogously. It is a left unitary Φ-module A with the product $uv \in A$, satisfying conditions (1), for $\alpha, \beta \in \Phi$. One of the advantages of the notion of an algebra over Φ (or a Φ-algebra) is that it allows for a study of algebras over fields and rings at the same time; the latter are obtained from a Φ-algebra when $\Phi = \mathbb{Z}$ is the ring of integers. We will be primarily interested in algebras over fields.

Every finite-dimensional algebra A over the field F may be defined by a "multiplication table" $e_i e_j = \sum_{k=1}^{n} \gamma_{ij}^k e_k$, where $e_1, \ldots, e_n$ is an arbitrary basis of A and $\gamma_{ij}^k \in F$ are the so-called *structural constants of the algebra*, corresponding to the given basis. Every collection γ_{ij}^k defines an algebra.

The just introduced notion of an algebra is too general to lead to interesting structural results (cf. examples in 1.2). In order to get such results, we need to impose some additional conditions on the operation of multiplication. Depending on the form of the imposed restrictions, different classes of algebras are obtained.

One of the most natural restrictions is that of *associativity* of multiplication

$$(xy)z = x(yz) \tag{2}$$

This is obviously satisfied when the elements of the algebra A are mappings of a set into itself and when the composition of mappings is taken as multiplication. One can show that every associative algebra is isomorphic to an algebra of linear transformations of an appropriate vector space. Thus, the condition of associativity of multiplication characterizes the algebras of linear transformations (with composition as multiplication).

The class of associative algebras assumes an important place in the theory of algebras and it is most thoroughly studied. In mathematics and its applications, however, other classes of algebras where condition (2) is not satisfied arise often. Such algebras are called *non-associative.*

The first class of non-associative algebras that was subject to serious and systematic study, was that of Lie algebras, that first arising in the theory of Lie groups. An algebra L is called a *Lie algebra,* if its operation of multiplication is *anticommutative,* i.e.

$$x^2 = 0 \tag{3}$$

and if it satisfies the *Jacobi identity*

$$J(x, y, z) \equiv (xy)z + (yz)x + (zx)y = 0. \tag{4}$$

If A is an associative algebra, then the algebra $A^{(-)}$ obtained by introducing a new multiplication on the vector space A, with the aid of the *commutator*

$$[x, y] \equiv xy - yx,$$

satisfies conditions (3) and (4) and consequently is a Lie algebra. This example is quite general, since the Poincaré-Birkhoff-Witt theorem implies that every Lie algebra over a field is isomorphic to a subalgebra of the algebra $A^{(-)}$, for a suitable associative algebra A.

Lie algebras have a rather developed theory, finding applications in different areas of mathematics. An extensive literature is devoted to them, and among them a sequence of surveys in this series. In our paper they will play a secondary role, appearing only marginally, basically as algebras of derivations of other algebras.

In analogy with the commutator or the Lie multiplication $[x, y]$ in an associative algebra A, we may introduce a symmetric *(Jordan) multiplication*

$$x \circ y = xy + yx.$$

Over the fields of characteristic $\neq 2$, however, it is more suitable to consider the operation

$$x \cdot y = \frac{1}{2}(xy + yx),$$

since in this case, the powers of an element x in the algebra A coincide with its powers with respect to the operation $(\cdot)$. The algebra obtained after introducing the multiplication $x \cdot y$ on the vector space A is denoted by $A^{(+)}$. We note that the mapping $x \mapsto \frac{1}{2}x$ establishes an isomorphism between the algebra $A^{(+)}$ with the corresponding algebra and the multiplication operation $x \circ y$.

The algebra $A^{(+)}$ is *commutative* i.e. satisfies the equality

$$xy = yx, \tag{5}$$

and generally speaking is not associative, although it satisfies the following weak associativity law

$$x^2(yx) = (x^2y)x. \tag{6}$$

The algebras satisfying identities (5) and (6) are called *Jordan algebras.*

Jordan algebras appeared first in 1934 in the joint paper by Jordan, von Neumann and Wigner (1934). In the ordinary interpretation of quantum mechanics the observables are Hermitian matrices or the Hermitian operators on a Hilbert space. The linear space of Hermitian matrices is not closed with respect to the ordinary product xy, but it is closed with respect to the symmetrized product $x \cdot y$. The program suggested by Jordan, consisted in at first singling out basic algebraic properties of Hermitian matrices in terms of the operation $x \cdot y$, and then in studying all the algebraic systems satisfying those properties. The authors hoped that in this process, new algebraic systems would be found, that would give a more suitable interpretation of quantum mechanics. They had chosen identities (5) and (6), satisfied by the operation $x \cdot y$, to be the basic properties. Although this path did not give any intrinsic generalizations of the matrix formalism of quantum mechanics, the class of algebras introduced by these authors had attracted attention of algebraists. The theory of Jordan algebras had started developing fast and soon thereafter its interesting applications in real and complex analysis, in the theory of symmetric spaces, in Lie groups and algebras had been found. In recent times the Jordan algebras again attract physicists in searching for models for explanations of properties of elementary particles. In relation to the physical theory of supersymmetry, Jordan superalgebras have appeared and studies have begun on them.

For an associative algebra A, the algebras of the form $A^{(+)}$ and their subalgebras are called *special Jordan algebras*. They are already not as such universal examples of Jordan algebras as the algebras $A^{(-)}$ and their subalgebras in the case of Lie algebras. There exist Jordan algebras, not isomorphic to subalgebras of the algebra $A^{(+)}$, for any associative algebra A. Such algebras are called *exceptional*.

The study of exceptional Jordan algebras intrinsically relies on the knowledge of properties of algebras of another class which is somewhat wider than the class of associative algebras. These are so-called *alternative algebras* defined by the identities

$$x^2y = x(xy), \tag{7}$$
$$yx^2 = (yx)x, \tag{8}$$

first of which is called the identity of *left alternativity* and the second – the identity of *right alternativity*. It is clear that every associative algebra is alternative. On the other hand, according to Artin's theorem (see 2.3 in the sequel), every two elements in an alternative algebra generate an associative subalgebra, thus alternative algebras are sufficiently close to the associative ones. A classical example of an alternative non-associative algebra is the famous algebra of Cayley numbers, that was constructed as far back as in 1845 by A. Cayley. This algebra and its generalizations – so-called Cayley-Dickson algebras – play an important role in the theory of alternative algebras and their applications in algebra and geometry.

If A is an alternative non-associative algebra, then the commutator algebra $A^{(-)}$ is not a Lie algebra. However, it is not difficult to show that, in this case, the algebra $A^{(-)}$ satisfies the following *Malcev identity*:

$$J(x, y, xz) = J(x, y, z)x, \tag{9}$$

where $J(x, y, z) \equiv (xy)z + (yz)x + (zx)y$ is the Jacobian of the elements x, y, z. An anticommutative algebra satisfying identity (9), is called a ***Malcev algebra***. This class of algebras was first introduced by A. I. Malcev in 1955 (under the name of "Moufang-Lie algebras") in studies on analytic Moufang loops; the Malcev algebras are related to them in approximately the same way as the Lie algebras are to Lie groups. Every Lie algebra is a Malcev algebra; on the other hand, every two-generated Malcev algebra is a Lie algebra. The latter condition defines the class of *binary Lie algebras*, wider than the class of Malcev algebras. If the characteristic is not equal to 2, this class may be defined by the following identities

$$x^2 = 0, \quad J(xy, x, y) = 0.$$

Alternative algebras, Jordan algebras as well as Malcev algebras, along with Lie algebras are the main and the best researched classes of non-associative algebras. All of them are in one or another way closely related to associative algebras (the Malcev algebras, through the alternative algebras), and for this reason they are sometimes united under the general name of "almost associative algebras". The main portion of this survey is exactly devoted to these classes of algebras (except of Lie algebras). There are, after all, other classes of non-associative algebras with quite satisfactory structure theories. We will consider some of them in Sect. 4. Nonetheless, the almost associative algebras that arose on the meeting of ring theory with other mathematical areas remain still the richest, from the point of view of applications and relations. Besides, the methods of their research are fairly universal and may be applied (and are being applied successfully) in the studies of other classes of algebras.

1.2. General Properties of Non-Associative Algebras. Numerous notions and results in the theory of associative algebras in fact do not use the associativity property and carry over without changes to arbitrary algebras. Some notions of this kind are definitions of subalgebras, one- and two-sided ideals, simple algebras, direct sums of algebras, homomorphisms, quotient algebras etc. The fundamental homomorphism theorems remain valid for arbitrary algebras too.

At the same time, there is a series of important notions, whose definitions intrinsically use the associativity property, thus not allowing for automatic expansion to arbitrary algebras. For instance, the power a^n of an element a and the power A^n of an algebra A is not, in general, a uniquely definable notion because, in a non-associative algebra, the result of multiplication of n elements depends on the arrangement of the brackets in the product. In particular, this product may equal to zero with one arrangement of the brackets and non-zero with another (even if all the elements are equal). Thus there are several analogues of nilpotency in the theory of non-associative algebras. The most important of them all are solvability and nilpotency.

Let A be an arbitrary algebra. If B and C are subspaces of A, then BC will denote the linear subspace generated by all the products bc, where $b \in B$, $c \in C$. We set $A^1 = A^{(0)} = A$, and further by induction

$$A^{n+1} = \sum_{i+j=n+1} A^i \cdot A^j, \quad A^{(n+1)} = A^{(n)} \cdot A^{(n)}.$$

An algebra A is called *nilpotent*, if there is an n such that $A^n = 0$ and is called *solvable*, if $A^{(m)} = 0$, for some m. The smallest numbers n and m with these properties are respectively called the *nilpotency index* and the *solvability index* of the algebra A. It is easy to see that the algebra A is nilpotent of index n, if and only if the product of any n of its elements, with any arrangement of the brackets equals zero and if there exists a non-zero product of $n-1$ elements. Every nilpotent algebra is solvable, but the converse is not generally true.

Proposition. *The sum of two solvable (two-sided) ideals of the algebra A is again a solvable ideal. If A is finite-dimensional, then A contains the greatest solvable ideal $S = S(A)$. Moreover, the factor algebra A/S does not contain non-zero solvable ideals.*

The ideal $S(A)$ defined in the proposition, is called the *solvable radical* of the finite-dimensional algebra A. In general, an ideal I of a (not necessarily finite-dimensional) algebra A, with certain property $\mathcal{R}$, is called an *$\mathcal{R}$-radical* of the algebra A and is denoted by $I = \mathcal{R}(A)$, if I contains all the ideals of the algebra A with the property $\mathcal{R}$ and the quotient algebra A/I does not contain such non-zero ideals (i.e. $\mathcal{R}(A/I) = 0$). In addition, it is assumed that the property $\mathcal{R}$ is preserved under homomorphisms (the class of $\mathcal{R}$-algebras is homomorphically closed).

The notion of a radical is one of fundamental instruments in constructing the structure theory of various classes of algebras. After a successful choice of a radical, everything reduces to description of the *radical algebras* (i.e. algebras A for which $A = \mathcal{R}(A)$) and the *semisimple algebras* (i.e. algebras A for which $\mathcal{R}(A) = 0$); arbitrary algebras are then described as extensions of the semisimple ones, by the radical ones. At first this method was used by Molien and Wedderburn, the founders of the structure theory of finite-dimensional associative algebras. They have considered a maximal nilpotent ideal of an algebra A as the radical $\mathcal{R}(A)$; the semisimple algebras were described as the direct sums of the full matrix algebras over division rings.

In the non-associative case, the class of nilpotent algebras, unlike the solvable case, is not closed under extensions (i.e. an algebra A may contain a nilpotent ideal I with a nilpotent quotient algebra A/I, but not be nilpotent itself.). Hence, the *nilpotent radical* does not exist in all the finite-dimensional algebras (for instance it does not exist in Lie algebras). Moreover, a finite-dimensional algebra may in general contain several different maximal nilpotent ideals. In those cases, the solvable radical $S(A)$ comes out to play the major role. It lies in the essence of the structure theories of finite-dimensional Lie algebras and finite-dimensional Malcev algebras of zero characteristic; on the other hand, in the cases of finite-dimensional alternative and Jordan algebras, where the nilpotent radical exists, $S(A)$ coincides with this radical.

Let us consider a few examples showing that in general it is difficult to count on a satisfactory structure theory of finite-dimensional algebras.

Example 1. Let A be an algebra over a field F, with a basis e_1, e_2, a, b and the following non-zero products of basis elements: $ae_1 = \epsilon e_1 a = e_2, be_2 = \epsilon e_2 b = e_1$, where $0 \neq \epsilon \in F$. Then $I_1 = Fe_1 + Fe_2 + Fa, I_2 = Fe_1 + Fe_2 + Fb$ are different maximal nilpotent ideals in A. By choosing $\epsilon = 1$ or $\epsilon = -1$ we obtain a commutative or anticommutative algebra A.

Example 2. Let $A_1, \ldots, A_k$ be simple algebras over a field F with bases $\{v_i^{(1)} \mid i \in I_1\}, \ldots, \{v_i^{(k)} \mid i \in I_k\}$. Let us consider the algebra $A = Fe + A_1 + \cdots + A_k$ with multiplication, defined by the following conditions: a) A_i are subalgebras of A; b) $A_i A_j = 0$, for $i \neq j$; c) $ev_i^{(j)} = v_i^{(j)} e = e$, for all i, j; d) $e^2 = e$. Then $I = Fe$ is the unique minimal ideal in A, and $I^2 = I$. In particular, $S(A) = 0$, but A does not decompose into a direct sum.

We point out that if all the algebras A_i in this example are commutative, then A is commutative too. If all the A_i are anticommutative, then we may consider $\tilde{A} = A \dotplus Ff$ and replace conditions c) and d) by the following: c') $ev_i^{(j)} = -v_i^{(j)} e = f$, $v_i^{(j)} f = -fv_i^{(j)} = e$; d') $ef = -fe = f$. Then $\tilde{A}$ is an anticommutative algebra with a unique minimal ideal $I = Fe + Ff$, $I^2 \neq 0$ and again $S(\tilde{A}) = 0$, but $\tilde{A}$ does not decompose into a direct sum.

One more approach to the notion of a radical of a non-associative algebra is possible: we can take the radical of an algebra A to be the smallest ideal $\tilde{N}$, for which the quotient algebra $A/\tilde{N}$ decomposes into the direct sum of simple algebras. Such a radical exists in every finite-dimensional algebra A and, satisfies the condition $\tilde{N}(A/\tilde{N}) = 0$; moreover $\tilde{N}(A) = S(A)$ in the algebras we have mentioned above, while in general $\tilde{N}(A) \supseteq S(A)$. However, this radical is not only necessarily nilpotent or solvable, but can even be a simple algebra. For example, for the algebra A in Example 2, $\tilde{N}(A) = Fe \cong F$.

The following example shows that the simple finite-dimensional algebras also form a rather big class, which implies that their complete description can hardly be done, even in the case of small dimensions and an algebraically closed field.

Example 3. Let us consider the algebra $A = A(\alpha_{ij})$ over the field F with a basis $e_1, \ldots, e_n$ and the multiplication table of the form $e_i e_j = \alpha_{ij} e_j$, where $0 \neq \alpha_{ij} \in F, i, j = 1, \ldots, n$ and all the columns in the matrix (α_{ij}) are different. A peculiarity of the algebra $A(\alpha_{ij})$ consists in the fact that in a given basis, the matrices of operators of left multiplications $L_x : y \mapsto xy$ have a diagonal form and are therefore commuting. Consequently all the algebras $A(\alpha_{ij})$ satisfy the identity

$$x(yz) = y(xz).$$

It is not difficult to show that $A(\alpha_{ij})$ is a simple algebra: in addition $A(\alpha_{ij}) \cong A(\beta_{ij})$ if and only if, $\alpha_{ij} = \lambda_i \beta_{\sigma(i)\sigma(j)}$, where $0 \neq \lambda_i \in F, i = 1, \dots, n; \sigma \in S_n$. If, in addition, we set $\alpha_{i1} = 1, i = 1, \dots, n$, then to every matrix (α_{ij}) there corresponds only a finite number ($\leqslant n!$) of matrices (β_{ij}) of the same type, for which $A(\alpha_{ij}) \cong A(\beta_{ij})$. Consequently, the aforementioned simple algebras form a family that depends on $n^2 - n$ "independent" parameters.

An element a of an algebra A is called *nilpotent* if the algebra generated by it in A is nilpotent. If all the elements of an algebra (ideal) are nilpotent, then such an algebra (ideal) is called a *nilalgebra* (a *nilideal*). In general the class of nilalgebras is not closed with respect to extensions. On the other hand, this condition is satisfied under the additional conditions of associativity of powers or power-associativity, defined in the sequel.

An algebra A is called a *power-associative algebra*, if its every element lies in an associative subalgebra. It is not difficult to show that all the algebras considered in 1.1 are power-associative. Over a field of characteristic 0, the class of power-associative algebras may be defined by identities

$$(x^2)x = x(x^2), \quad (x^2x)x = x^2x^2.$$

The powers a^n ($n \geqslant 1$) of an element a are defined in a natural way in every power-associative algebra; in addition the equalities $(a^n)^m = a^{nm}, a^n a^m = a^{n+m}$ hold, and the element a is nilpotent if and only if $a^n = 0$, for some n.

Just as for the associative algebras, the following is proved in a standard way:

Proposition. *Every power-associative algebra A contains a unique maximal two-sided nilideal $Nil(A)$; moreover, the quotient algebra $A/Nil A$ does not contain two sided non-zero nilideals (i.e. it is a nilsemisimple algebra).*

The ideal $\operatorname{Nil} A$ is called the *nilradical* of the algebra A. If A is a finite dimensional power-associative algebra, then $S(A) \subseteq \operatorname{Nil} A$; the inclusion may be strict, as the example of a Lie algebra shows, where $\operatorname{Nil} A = A$. We will see in the sequel that, for finite-dimensional alternative and Jordan algebras the ideal $\operatorname{Nil} A$ is nilpotent. In particular, in these cases $\operatorname{Nil} A = S(A)$. In the case of finite-dimensional commutative power-associative algebras the question on equality of the radicals $S(A)$ and $\operatorname{Nil} A$ is open and is known as Albert's problem. The following example shows that in this case the ideal $\operatorname{Nil} A$ is not necessarily nilpotent.

Example 4 (Suttles, 1972). Let A be a commutative algebra over a field of characteristic $\neq 2$, with the basis $\{e_1, e_2, e_3, e_4, e_5\}$ and the following multiplication table:

$$e_1e_2 = e_2e_4 = -e_1e_5 = e_3, \quad e_1e_3 = e_4, \quad e_2e_3 = e_5;$$

and all the other products are zero. Then A is a solvable power-associative nilalgebra of index 4, which is not nilpotent.

It is not difficult to see that Albert's problem is equivalent to the following question: are there any simple finite-dimensional commutative power-associative nilalgebras? The answer to this question is not known even without the assumption on power-associativity. The structure of nilsemisimple finite-dimensional commutative power-associative algebras is known.

Theorem (Albert, 1950, Kokoris, 1956). *Every nilsemisimple finite-dimensional commutative power-associative algebra over a field of characteristic* $\neq 2, \neq 3, \neq 5$ *has a unity and decomposes into the direct sum of simple algebras, such that each of them is either a Jordan algebra or an algebra of degree 2, over a field of positive characteristic.*

We clarify that the *degree of an algebra* A over a field F is a maximal number of mutually orthogonal idempotents in the scalar extension $\overline{F} \otimes_F A$, where $\overline{F}$ is the algebraic closure of the field F. Exceptional algebras of degree 2 from the conclusion of the theorem have been described in (Oehmke, 1962); their construction is fairly complex and we will not state it here. A description of simple Jordan algebras will be given in Sect. 3.

In general, the structure of nilsemisimple finite-dimensional power-associative algebras remains unknown. It is possible to get the description of these algebras only under some additional restrictions (cf. Sect 4). An effective method of studying power-associative algebras is a passage to the associated commutative power-associative algebra $A^{(+)}$, since properties of the algebra $A^{(+)}$ often give an essential information about the properties of A.

Let A be an algebra and let $a \in A$. Let us denote by R_a and L_a respectively the operators of the right and left multiplication by the element a:

$$R_a : x \mapsto xa, \quad L_a : x \mapsto ax.$$

The subalgebra of the algebra $\operatorname{End} A$ of the endomorphisms of the linear space A, generated by all the operators R_a, where $a \in A$ is called the *algebra of right multiplications* of the algebra A and is denoted by $R(A)$. The *algebra of left multiplications* $L(A)$ of the algebra A is defined analogously. The subalgebra of $\operatorname{End} A$ generated by all the operators R_a, L_a, $a \in A$ is called the *multiplication algebra* of the algebra A and is denoted by $M(A)$. If B is a subalgebra of A, then $M^A(B)$ will denote a subalgebra of the algebra $M(A)$, generated by all the operators R_b, L_b, where $b \in B$.

Properties of an algebra A are reflected in a certain way in the properties of its multiplication algebra $M(A)$. For example, the algebra A is nilpotent if and only if its associative algebra $M(A)$ is nilpotent. If a finite-dimensional algebra A is semisimple (is a direct sum of simple algebras), then the algebra $M(A)$ has the same property; and if A is simple, then $M(A)$ is also simple and is isomorphic to the full matrix algebra over its center.

Along with associative multiplication algebras, it is sometimes suitable to consider also the *Lie multiplication algebra* Lie(A) defined as the subalgebra of the Lie algebra $(\operatorname{End} A)^{(-)}$, generated by all the operators R_a, L_a, where $a \in A$. It is clear that $\operatorname{Lie}(A) \subseteq (M(A))^{(-)}$. Another Lie algebra naturally connected with every algebra A is the *derivation algebra* Der A.

Recall that the *derivation* of an algebra A is a linear operator $D \in \operatorname{End} A$ which satisfies the equality

$$(xy)D = (xD)y + x(yD), \text{ for all } x, y \in A. \tag{10}$$

The set Der A of all derivations of an algebra A is a subspace of the vector space End A; moreover, it is not difficult to see that if $D_1, D_2 \in \operatorname{Der} A$, then the commutator $[D_1, D_2] \in \operatorname{Der} A$ too, thus Der A is also a subalgebra of the Lie algebra $(\operatorname{End} A)^{(-)}$.

Equality (10) may be rewritten in terms of right and left multiplications: the operator $D \in \operatorname{End} A$ is a derivation if and only if any of the following two equalities is satisfied:

$$[R_y, D] = R_{yD}, \text{ for every } y \in A, \tag{11}$$
$$[L_x, D] = L_{xD}, \text{ for every } x \in A, \tag{12}$$

A derivation D of an algebra A is called an *inner derivation*, if $D \in \operatorname{Lie}(A)$. Equalities (11) and (12) easily imply that the set Inder A of all inner derivations of the algebra A is an ideal of the algebra Der A.

Inner derivations play an important role in the theory of associative and Lie algebras. It is well known that every derivation of a finite-dimensional semisimple associative or Lie algebra of zero characteristic is inner. More generally, the following hold:

Proposition (Schafer, 1966). *Let A be a finite-dimensional algebra, over a field of characteristic 0, which is the direct sum of simple algebras, and A has either right or left unity. Then every derivation of the algebra A is inner.*

This proposition is not valid without the assumption on the existence of an one-sided unity (Walcher, 1987).

We know from the theory of Lie groups that there is a close connection between derivations and automorphisms of finite-dimensional algebras over the field of real numbers. Namely, the algebra Der A, in this case, is nothing else but the Lie algebra of the automorphism group of the algebra A. The correspondence between derivations and automorphisms is established by $D \mapsto \exp D = 1 + D + \frac{D^2}{2!} + \ldots$; in the core of the proof that $\exp D$ is an automorphism lies the well-known Leibniz' formula:

$$(xy)D^n = \sum_{i=0}^{n} \binom{n}{i} (xD^i)(yD^{n-i}).$$

If A is an arbitrary algebra over a field of characteristic 0 and if D is a nilpotent derivation of A, then the operator $G = \exp D$ makes sense too; moreover, it is not difficult to show, with the aid of the Leibniz formula, that G is an automorphism of the algebra A.

In considering non-associative algebras, the following notion of an *associator* turns out to be useful

$$(x, y, z) \equiv (xy)z - x(yz).$$

The ideal $D(A)$ of an algebra A, generated by all the associators is called an *associator ideal* of the algebra A. A dual to this notion is the notion of the *associative center* $N(A)$ of an algebra A:

$$N(A) = \{n \in A \mid (n, A, A) = (A, n, A) = (A, A, n) = 0\}.$$

An algebra A is associative if and only if $D(A) = 0$ (or $N(A) = A$). The *center* $Z(A)$ *of an algebra* A is the set

$$Z(A) = \{z \in N(A) \mid [z, A] = 0\}.$$

Proposition. *For every algebra A, the associative center as well as the center are subalgebras. Moreover,*

$$D(A) = (A, A, A) + (A, A, A)A = (A, A, A) + A(A, A, A).$$

The proof follows from the following two identities valid in every algebra:

$$x(y, z, t) + (x, y, z)t = (xy, z, t) - (x, yz, t) + (x, y, zt), \tag{13}$$
$$[xy, z] - x[y, z] - [x, z]y = (x, y, z) - (x, z, y) + (z, x, y), \tag{14}$$

The notions of a bimodule and a birepresentation play an important role in the theory of algebras.

Let $\mathfrak{M}$ be a class of algebras over a field F. Let us assume that, for an algebra A in $\mathfrak{M}$ and a vector space M over F, the bilinear compositions $A \times M \longrightarrow M$, $M \times A \longrightarrow M$, written as am and ma, for $a \in A$ and $m \in M$ have been defined. Then the direct sum $A \dotplus M$ of the vector spaces A and M may be made into an algebra by defining multiplication via the following rule:

$$(a_1 + m_1)(a_2 + m_2) = a_1a_2 + (m_1a_2 + a_1m_2),$$

where $a_i \in A$, $m_i \in M$. This algebra is called the *split null extension* of the algebra A, by M. If the algebra $A \dotplus M$ again belongs to the class $\mathfrak{M}$, then M is called a *bimodule over the algebra A* (or an *A-bimodule*) *in the class $\mathfrak{M}$*.

For instance, if $\mathfrak{M}$ is the class of all algebras over F, then, no conditions are required in the definition of a bimodule in the class $\mathfrak{M}$, except that the operations am and ma are bilinear. If $\mathfrak{M}$ is the class of all the associative algebras, then the bimodule operations must satisfy the following conditions:

$$(ma)b = m(ab), \quad (am)b = a(mb), \quad (ab)m = a(bm),$$

for all $a, b \in A, m \in M$; in other words, we arrive at the usual well-known definition of an associative bimodule.

In the class of Lie algebras, the corresponding conditions for bimodule operations are of the form

$$am = -ma, \quad m(ab) = (ma)b - (mb)a.$$

In general, if a class $\mathfrak{M}$ is defined by a set of multilinear identities $\{f_i(x_1, \ldots, x_{n_i}) = 0 \mid i \in I\}$, then it is not difficult to see that M is a bimodule over an algebra $A \in \mathfrak{M}$ in the class $\mathfrak{M}$, if and only if the following conditions are satisfied:

$$f_i(a_1, \ldots, a_{k-1}, m, a_{k+1}, \ldots, a_{n_i}) = 0, \quad k = 1, \ldots, n_i; \quad i \in I,$$

for every $a_j \in A, m \in M$. In case when the relations f_i are not multilinear, the corresponding conditions for bimodules may also be written down fairly simply, with the aid of the operators of *"partial linearizations"* (cf. for instance Jacobson, 1968); if the class $\mathfrak{M}$ is defined by a finite number of identities, then bimodules in the class $\mathfrak{M}$ are also defined by a finite number of relations. For a concrete class $\mathfrak{M}$, defined by identities of small degree, it is simpler to find the conditions for bimodules directly. Let us show this through the examples of the alternative and Jordan algebras.

1) Let $\mathfrak{M}$ be the class of alternative algebras.

In terms of the associators, the class $\mathfrak{M}$ is defined via the following identities:

$$(x, x, y) = 0, \quad (x, y, y) = 0. \tag{15}$$

Thus a *bimodule* M over an alternative algebra A is *alternative* if and only if the following relations hold in the split null extension $A \dotplus M$:

$$(a + m, a + m, b + n) = 0, \quad (a + m, b + n, b + n) = 0,$$

for all $a, b \in A$; $m, n \in M$. Because of $M^2 = 0$ (in the algebra $A \dotplus M$), these relations give us the following conditions for a bimodule M to be alternative:

$$\begin{aligned} (a, a, m) = 0, \quad (a, m, b) + (m, a, b) = 0 \\ (m, b, b) = 0, \quad (a, m, b) + (a, b, m) = 0. \end{aligned} \tag{16}$$

2) Let $\mathfrak{M}$ be the class of Jordan algebras.

The defining relations for the class $\mathfrak{M}$ are of the following form:

$$xy = yx, \quad (x^2, y, x) = 0.$$

If A is a Jordan algebra and M is a bimodule over A, then the algebra $A \dotplus M$ is Jordan if and only if the following relations hold there:

$$(a+m)(b+n) = (b+n)(a+m), \quad ((a+m)^2, b+n, a+m) = 0,$$

for all $a, b \in A; m, n \in M$. It is easy to see that these relations are equivalent to the following:

$$am = ma, \quad (a^2, m, a) = 0, \quad (a^2, b, m) + 2(am, b, a) = 0, \tag{17}$$

for all $a, b \in A, m \in M$.

If M is an A-bimodule, then the mappings $\rho(a) : m \to ma$ and $\lambda(a) : m \to am$ are linear operators on M and the mappings $a \to \rho(a)$, $a \to \lambda(a)$ are linear mappings from A into the algebra End M. The pair (ρ, λ) of linear mappings from A into the algebra End M of endomorphisms of some vector space M is called a *birepresentation of the algebra A in the class $\mathfrak{M}$*, if M, equipped with the compositions $ma = m\rho(a), am = m\lambda(a)$, is a bimodule over A in the class $\mathfrak{M}$. It is obvious that the notions of a bimodule and a birepresentation define each other. Using relations (16) and (17) which define alternative and Jordan bimodules, we can easily write down the conditions defining birepresentations in these classes. For instance the alternative birepresentations are defined by the following conditions

$$\begin{aligned} \lambda(a^2) - \lambda(a)^2 = 0, \quad [\lambda(a), \rho(b)] + \rho(a)\rho(b) - \rho(ab) = 0, \\ \rho(a^2) - \rho(a)^2 = 0, \quad [\lambda(a), \rho(b)] + \lambda(ab) - \lambda(b)\lambda(a) = 0. \end{aligned} \tag{18}$$

Every algebra A may be considered in a natural way to be a bimodule over itself, interpreting ma and am as multiplication in the algebra A. Bimodules of this kind along with the corresponding birepresentations $a \mapsto R_a$, $a \mapsto L_a$ are called *regular bimodules*. Note that subbimodules of a regular bimodule A are the two-sided ideals of the algebra A.

If a class $\mathfrak{M}$ is defined via a system of identities $\{f_i\}$, then the regular bimodule for an algebra $A \in \mathfrak{M}$, generally speaking, may be not a bimodule in the class $\mathfrak{M}$. Indeed, it is evident from the examples considered above that, for this property to hold, the algebra A must not only satisfy the identities $\{f_i\}$, but also some new identities (for instance, in case of Jordan algebras the identity $(a^2, b, c) + 2(ac, b, a) = 0$ should hold in A). These new identities, called partial linearizations of the identities $\{f_i\}$, do not in general follow from $\{f_i\}$. However, this is the case if all the f_i are homogeneous and the number of elements in the field F is not smaller than the degree of every f_i in its every participating variable. In particular, every regular bimodule over an alternative algebra is alternative. The same is valid for Jordan algebras over a field F of characteristic $\neq 2$.

In considerations on a family of linear transformations it is often useful to pass to the enveloping associative algebra of this family. For instance, the enveloping algebra of the family $\{R_a, L_a \mid a \in A\}$ is the multiplication algebra $M(A)$. In the case of arbitrary birepresentations, a study of the enveloping algebra of the family $\{\rho(a), \lambda(a) \mid a \in A\}$ is largely facilitated by introducing the universal enveloping algebra. Let us show how to construct this algebra through the example of alternative algebras.

Let A be an alternative algebra and let $B = A \dotplus A^0$ be the direct sum of vector spaces, where A^0 is a vector space isomorphic to A under the isomorphism $a \mapsto a^0$. Let us consider the tensor algebra $T(B) = F \dotplus B \dotplus B \otimes B \dotplus B \otimes B \otimes B \dotplus \dots$ For every pair (ρ, λ) of linear transformations from A to $\operatorname{End} M$, we can constract a linear transformation $\phi : B \longrightarrow \operatorname{End} M$, setting $\phi(a + b^0) = \rho(a) + \lambda(b)$. Because of the properties of the tensor algebra, ϕ is uniquely extendable to the homomorphism of associative algebras: $\tilde{\phi} : T(B) \longrightarrow \operatorname{End} M$. It is not difficult to see that the pair (ρ, λ) is an alternative birepresentation (i.e. satisfies identities (18)), if and only if $\operatorname{Ker} \tilde{\phi}$ contains the following set of elements:

$$\begin{gathered} (a^2)^0 - a^0 \otimes a^0, \quad a^0 \otimes b - b \otimes a^0 + a \otimes b - ab, \\ a^2 - a \otimes a, \quad a^0 \otimes b - b \otimes a^0 + (ab)^0 - b^0 \otimes a^0; a, b \in A. \end{gathered} \tag{19}$$

For instance, we have

$$\begin{gathered} \lambda(a^2) - \lambda(a)^2 = \phi((a^2)^0) - (\phi(a^0))^2 = \tilde{\phi}((a^2)^0) - (\tilde{\phi}(a^0))^2 = \\ \tilde{\phi}((a^2)^0) - \tilde{\phi}(a^0 \otimes a^0) = \tilde{\phi}((a^2)^0 - a^0 \otimes a^0). \end{gathered}$$

Denote by I the ideal of the algebra $T(B)$ generated by the set of elements (19), denote by $U(A)$ the quotient algebra $T(B)/I$ and let $\mathcal{R} : a \mapsto a + I, \mathcal{L} : a \mapsto a^0 + I$ be linear transformations from A to $U(A)$. It is clear that the pair $(\mathcal{R}, \mathcal{L})$ satisfies the equalities in (18); in addition, it is not difficult to see that, for every alternative birepresentation $(\rho, \lambda) : A \longrightarrow \operatorname{End} M$ there exists a unique homomorphism of associative algebras $\phi : U(A) \longrightarrow \operatorname{End} M$, such that $\rho = \mathcal{R} \circ \phi, \lambda = \mathcal{L} \circ \phi$. In this way, M may be considered as a right (associative) $U(A)$-module. Conversely, every right $U(A)$-module is an alternative A-bimodule with respect to the compositions $ma = m\mathcal{R}(a), am = m\mathcal{L}(a)$. The algebra $U(A)$ is called the *universal multiplicative enveloping algebra* of the algebra A (in the class of alternative algebras).

We can also construct, in an analogous way, multiplicative enveloping algebras for other classes of algebras. Note that, for a Lie algebra L, the algebra $U(A)$ is the ordinary universal (Birkhoff-Witt) enveloping algebra; if A is associative, then $U(A) \cong A^\sharp \otimes (A^\sharp)^0$, where $A^\sharp = F \cdot 1 + A$ and the algebra $(A^\sharp)^0$ is anti-isomorphic to $A^\sharp$.

If (ρ, λ) is an arbitrary birepresentation of the algebra A (in the class $\mathfrak{M}$), then the enveloping algebra of the family $\{\rho(a), \lambda(a) \mid a \in A\}$ is a homomorphic image of the algebra $U(A)$. In particular, if regular bimodules for algebras in $\mathfrak{M}$ are bimodules in the class $\mathfrak{M}$, then the multiplication algebra $M(A)$ and, more generally, the algebra $M^B(A)$, for every algebra $B \in$

$\mathfrak{M}$ containing the algebra A, are homomorphic images of the algebra $U(A)$. Generally, introduction of the algebra $U(A)$ reduces the problem of describing birepresentations of the algebra A to determination of the structure of $U(A)$ and to the description of the right (associative) representations of $U(A)$.

As the concluding remark, we point out that the notions of a right module and a right representation, which play a fundamental role in the theory of associative algebras, do not always yield to such simple and natural definitions in other classes of algebras (except the cases of commutative and anticommutative algebras, where the notions of representation and birepresentation coincide by default). It is still unknown whether a right alternative module may be defined by a finite number of relations. On this matter see (Slin'ko, Shestakov, 1974), where the notion of the right representation in an arbitrary class of algebras has been defined and studied, and the theory of right representations of alternative algebras has been constructed.

Non-associative superalgebras have been studied more and more actively in recent times. They first arose in physics and geometry and turned out to be rather useful in algebra. An algebra A is called a *$\mathbb{Z}_2$-graded algebra* or a *superalgebra*, if $A = A_0 \dotplus A_1$, where $A_iA_j \subseteq A_{i+j}, i, j \in \mathbb{Z}_2$. For example, the Grassmann algebra $G = G_0 \dotplus G_1$ is a superalgebra, where G_0 (G_1) denotes a subspace, generated by the words of even (odd) length, on the generators of the algebra G. Let $\mathfrak{M}$ be a class of algebras over an infinite field, defined by some system of identities. The superalgebra $A = A_0 \dotplus A_1$ is called an $\mathfrak{M}$-superalgebra if its *Grassmann envelope* $G(A) = G_0 \otimes A_0 + G_1 \otimes A_1$ belongs to $\mathfrak{M}$. The $\mathfrak{M}$-superalgebra A, generally speaking, does not itself belong to the class $\mathfrak{M}$; its even part A_0 is a subalgebra contained in $\mathfrak{M}$ and its odd part A_1 is an $\mathfrak{M}$-bimodule over A_0. If the identities defining $\mathfrak{M}$ are known, then it is possible to write down "superidentities" defining $\mathfrak{M}$-superalgebras. For example, the superalgebra $A = A_0 \dotplus A_1$ is a *Lie superalgebra*, if the following identities hold there:

$$a_ia_j + (-1)^{ij}a_ja_i = 0,$$
$$(a_ia_j)a_k - a_i(a_ja_k) - (-1)^{jk}(a_ia_k)a_j = 0;$$

the *alternative superalgebras* are defined by the following identities:

$$(a_i, a_j, a_k) + (-1)^{jk}(a_i, a_k, a_j) = 0,$$
$$(a_i, a_j, a_k) + (-1)^{ij}(a_j, a_i, a_k);$$

and the *Jordan superalgebras* are defined by the following identities.

$$a_ia_j - (-1)^{ij} \cdot a_ja_i = 0,$$
$$(-1)^{l(i+k)}(a_ia_j, a_k, a_l) + (-1)^{i(j+k)}(a_ja_l, a_k, a_i) +$$
$$(-1)^{j(l+k)}(a_la_i, a_k, a_j) = 0,$$

where $a_s \in A_s$, $s = i, j, k, l \in \{0, 1\}$, everywhere.

§2. Alternative Algebras

2.1. Composition Algebras. We begin presentation of the theory of alternative algebras with consideration of the most important class of these algebras, namely the composition algebras. An algebra A with unity 1 over a field F of characteristic $\neq 2$ is called a *composition algebra* if a non-degenerate quadratic form $n(x)$ has been defined on the vector space A such that

$$n(xy) = n(x)n(y) \tag{1}$$

In this case, we also say that the form $n(x)$ allows composition on A. Typical representatives of composition algebras are fields of real numbers $\mathbb{R}$ and complex numbers $\mathbb{C}$, the quaternion skew-field $\mathbb{Q}$ as well as the algebra of Cayley numbers (octonions) $\mathbb{O}$, with the Euclidean norm $n(x) = (x, x) = |x|^2$. The first three among them are associative and the algebra $\mathbb{O}$ provides us with the first and most important example of an alternative non-associative algebra. Equality (1), written down in an orthonormal basis, for each of those algebras, gives an identity of the following form:

$$(x_1^2 + \cdots + x_k^2)(y_1^2 + \cdots + y_k^2) = z_1^2 + \cdots + z_k^2, \quad k = 1, 2, 4, 8,$$

where z_i are bilinearly expressible through x_r, y_s. The efforts of many mathematicians of the last century were devoted to finding all the k for which these identities were valid, and only in 1898, Hurwitz had shown that the values $k = 1, 2, 4, 8$ were the only possible. We will see in the sequel that this claim is a consequence of a general fact that the dimension of a composition algebra may only be equal to 1, 2, 4, 8.

Proposition. *Let A be a composition algebra. Then A is alternative and every element of the algebra A satisfies a quadratic equation with the coefficients in F (i.e. the* algebra A is quadratic *over F).*

Proof. Substituting $y + w$ for y in (1) we get $n(x)n(y + w) = n(xy + xw)$. Subtracting the identity (1) from this equality as well as subtracting the identity obtained from (1) by substituting y by w, we get

$$n(x)f(y, w) = f(xy, xw), \tag{2}$$

where $f(x, y) = n(x + y) - n(x) - n(y)$ is a non-singular symmetric bilinear form associated with the quadratic form $n(x)$. Running the same procedure with x, we obtain

$$f(x, z)f(y, w) = f(xy, zw) + f(zy, xw) \tag{3}$$

The procedure just performed is called the *linearization of identity* (1) in y and x respectively. The idea of this procedure is in lessening the degree of the identity in a given variable, through introduction of new variables, and in arriving after all to a multilinear identity. We will apply this procedure in the sequel, without detailed explanations. Now set $z = 1, y = xu$ in (3):

$$f(x,1)f(xu,w) = f(x \cdot xu, w) + f(xu, xw). \tag{4}$$

Since $f(xu, xw) = n(x)f(u, w)$, and because of (2), (4) may be rewritten in the following way

$$f(x \cdot xu + n(x)u - f(x,1)xu, w) = 0,$$

which implies that

$$x \cdot xu + n(x)u - f(x,1)xu = 0, \tag{5}$$

because the form $f(x, y)$ is non-degenerate and w is arbitrary. Setting here $u = 1$, we obtain

$$x^2 - f(x,1)x + n(x) = 0 \tag{6}$$

which proves the second half of the proposition. It remains to prove that the algebra A is alternative.

Multiplying (6) on the right by u and comparing with (5) we obtain $x^2u = x(xu)$. The proof that $u \cdot x^2 = (ux)x$ is analogous. Thus, the algebra A is alternative and the proof is complete. □

Recall that an endomorphism ϕ of a vector space A is called an *involution of the algebra* A, if $\phi(\phi(x)) = x$ and $\phi(xy) = \phi(y)\phi(x)$, for all $x, y \in A$.

Proposition. *In the composition algebra A, the mapping $x \mapsto \overline{x} = f(1,x) - x$ is an involution, fixing the elements of the field $F = F \cdot 1$; in addition, the elements $t(x) = x + \overline{x}$ and $n(x) = x\overline{x}$ are in F, for all x in A.*

We prove only the equality $\overline{x}\,\overline{y} = \overline{yx}$, as the other claims are fairly obvious. Linearising relation (6) in x, we obtain

$$xy + yx - f(1,x)y - f(1,y)x + f(x,y) = 0. \tag{7}$$

Moreover, for $w = z = 1$ in (3), we obtain the following:

$$f(x,1)f(y,1) = f(xy,1) + f(y,x). \tag{8}$$

Substituting it in (7), we get

$$xy + yx - f(1,x)y - f(1,y)x + f(1,x)f(1,y) - f(1,xy) = 0.$$

therefore

$$(f(1,x) - x)(f(1,y) - y) = f(1,xy) - yx.$$

We infer from (8) that $f(1,xy) = f(1,yx)$. Thus $\overline{x}\,\overline{y} = \overline{yx}$. □

Let us show now that the condition of the algebra A being alternative is not only necessary but also sufficient for the relation (1) to hold.

Proposition. *Let A be an alternative algebra over a field F with unity 1 and involution $x \mapsto \overline{x}$, such that the elements $t(x) = x + \overline{x}$ and $n(x) = x\overline{x} \in F$, for all $x \in A$. Then the quadratic form $n(x)$ satisfies condition (1).*

Proof. Note first of all that the following equalities hold in A:

$$x(\overline{x}y) = (y\overline{x})x = n(x)y, \tag{9}$$

which is easily implied by the alternativity conditions. Furthermore, by linearizing the alternativity identities (1.15) in x and y respectively, we obtain

$$(x, y, z) + (y, x, z) = 0, \tag{10}$$
$$(x, y, z) + (x, z, y) = 0, \tag{11}$$

which imply that, in an alternative algebra, the associator (x, y, z) is an alternating function of its arguments. In particular, we have the identity

$$(x, y, z) = (z, x, y). \tag{12}$$

Finally, in view of (9) and (12) we obtain the following:

$$\begin{gathered} n(xy) = (xy)(\overline{xy}) = (xy)(\overline{y}\,\overline{x}) = (xy \cdot \overline{y})\overline{x} - (xy, \overline{y}, \overline{x}) = \\ n(x)n(y) - (\overline{x}, xy, \overline{y}) = n(x)n(y) - (\overline{x} \cdot xy)\overline{y} + \overline{x}(xy \cdot \overline{y}) = \\ n(x)n(y) - n(x)n(y) + n(x)n(y) = n(x)n(y). \end{gathered}$$

□

Now let A be an algebra with the unity 1, over a field F and an involution $a \mapsto \overline{a}$, where $a + \overline{a}, a\overline{a} \in F$, for every $a \in A$. Let us fix $0 \neq \alpha \in F$ and let us define on the vector space $A \dotplus A$ the following operation of multiplication:

$$(a_1, a_2) \cdot (a_3, a_4) = (a_1 a_3 - \alpha a_4 \overline{a_2}, \overline{a_1} a_4 + a_3 a_2).$$

The resulting algebra (A, α) is called the algebra derived from the algebra A by the *Cayley-Dickson process.* It is clear that A is isomorphically embeddable into (A, α) and that $\dim(A, \alpha) = 2 \dim A$. Let $v = (0, 1)$; then $v^2 = -\alpha \cdot 1$ and $(A, \alpha) = A \dotplus vA$. For an arbitrary element $x = a_1 + va_2 \in (A, \alpha)$, set $\overline{x} = \overline{a_1} - va_2$. Then $x + \overline{x} = a_1 + \overline{a_1}, x\overline{x} = a_1\overline{a_1} + \alpha a_2 \overline{a_2} \in F$ and the mapping $x \mapsto \overline{x}$ is an involution of the algebra (A, α) extending the involution $a \mapsto \overline{a}$ of the algebra A. If the quadratic form $n(a) = a\overline{a}$ is non-degenerate on A, then the quadratic form $n(x) = x\overline{x}$ is non-degenerate on (A, α).

The Cayley-Dickson process may be applied to every composition algebra A; furthermore, the algebra (A, α) will again be a composition algebra, if and only if it is alternative. Let us clarify under what conditions this is the case. Let $x, y \in (A, \alpha), x = a + vb, y = c + vd$. We have

$$(x, x, y) = (a + vb, a + vb, c + vd) = \alpha(\overline{a}, d, \overline{b}) - v(a, c, b).$$

Since $\overline{(y, x, x)} = -(\overline{x}, \overline{x}, \overline{y})$, the algebra (A, α) is alternative if and only A is associative.

We can now give the following examples of composition algebras over F:

I. A field F of characteristic $\neq 2$.

II. $\mathbb{C}(\alpha) = (F, \alpha), \alpha \neq 0$. If the polynomial $x^2 + \alpha$ is irreducible over F, then $\mathbb{C}(\alpha)$ is a field; otherwise, $\mathbb{C}(\alpha) = F \oplus F$.

III. $\mathbb{H}(\alpha, \beta) = (\mathbb{C}(\alpha), \beta), \beta \neq 0$ – the *algebra of generalized quaternions*. It is easy to check that the algebra $\mathbb{H}(\alpha, \beta)$ is associative, but not commutative.

IV. $\mathbb{O}(\alpha, \beta, \gamma) = (\mathbb{H}(\alpha, \beta), \gamma), \gamma \neq 0$ – the *Cayley-Dickson algebra*. It is not difficult to get convinced that the algebra $\mathbb{O}(\alpha, \beta, \gamma)$ is not associative, thus our inductive process of constructing composition algebras breaks up.

If $F = \mathbb{R}$ is the field of real numbers, then the construction described above gives, for $\alpha = \beta = \gamma = 1$, the classical algebras of complex numbers $\mathbb{C} = \mathbb{C}(1)$, the quaternions $\mathbb{H} = \mathbb{H}(1, 1)$ and the *Cayley numbers* $\mathbb{O} = \mathbb{O}(1, 1, 1)$.

Let us show now that the examples I–IV exhaust all the composition algebras.

Let A be a composition algebra with the quadratic form $n(x) = x\overline{x}$; $f(x, y) = x\overline{y} + y\overline{x}$ be the bilinear form associated with $n(x)$. If B is a subspace in A, then we will denote by $B^{\perp}$ the orthogonal complement of B with respect to the form $f(x, y)$.

Lemma. *Let B be a subalgebra of A containing the unity 1 of the algebra A. Then, if the restriction of the form f to B is non-degenerate and if $B \neq A$, then for a suitable $v \in B^{\perp}$, the subspace $B_1 = B + vB$ is a subalgebra of A, obtained from B by the Cayley-Dickson process.*

The following theorem is easy to prove with the aid of the lemma.

Theorem. *Every composition algebra is isomorphic to one of the algebras of types I–IV, given above.*

Indeed we may set $B = F$, since the subalgebra F is non-degenerate with respect to $f(x, y)$. If $F \neq A$, then A contains the subalgebra $B_1 = (F, \alpha)$ of type II. If $B_1 \neq A$, then A contains the subalgebra $B_2 = (B_1, \beta)$ of type III. If finaly, $B_2 \neq A$, then A contains the subalgebra $B_3 = (B_2, \gamma)$ of type IV. The process must stop here, since, in the opposite case, the algebra A would contain a non-alternative subalgebra $B_4 = (B_3, \delta)$, which is impossible. Thus, A coincides with one of its subalgebras F, B_1, B_2, B_3 which proves the theorem. □

Corollary. *A non-degenerate quadratic form $n(x)$, defined on a finite-dimensional vector space V over a field F of characteristic $\neq 2$, allows composition* *if and only if,* $\dim_F V = 1, 2, 4, 8$ *and, in some basis of the space* V, *the form* $n(x)$ *is respectively of one of the following forms:*

1) $n(x) = x_0^2$;
2) $n(x) = x_0^2 + \alpha x_1^2$;
3) $n(x) = (x_0^2 + \alpha x_1^2) + \beta(x_2^2 + \alpha x_3^2)$;
4) $n(x) = [(x_0^2 + \alpha x_1^2) + \beta(x_2^2 + \alpha x_3^2)] + \gamma[(x_4^2 + \alpha x_5^2) + \beta(x_6^2 + \alpha x_7^2)]$, *where* $\alpha, \beta, \gamma \in F, \alpha\beta\gamma \neq 0$.

We can choose a canonical basis in every composition algebra for which the form $n(x)$ is of one of the forms 1)–4). Let $\mathbb{C}(\alpha) = F \dot{+} Fv_1, \mathbb{H}(\alpha, \beta) = \mathbb{C}(\alpha) \dot{+} \mathbb{C}(\alpha)v_2, \mathbb{O}(\alpha, \beta, \gamma) = \mathbb{H}(\alpha, \beta) \oplus \mathbb{H}(\alpha, \beta)v_3$; then $v_1^2 = -\alpha, v_2^2 = -\beta, v_3^2 = -\gamma, \overline{v_i} = -v_i, v_i v_j = -v_j v_i$, for $i \neq j$ and the elements $e_0 = 1, e_1 = v_1, e_2 = v_2, e_3 = v_3, e_4 = v_1 v_2, e_5 = v_2 v_3, e_6 = v_1(v_2 v_3), e_7 = v_1 v_3$ form a canonical basis of the algebra $\mathbb{O}(\alpha, \beta, \gamma)$. Note that $\overline{e_i} = -e_i, e_i e_j = -e_j e_i$, for $i, j \geqslant 1, i \neq j$. If $\mathbb{O} = \mathbb{O}(1, 1, 1)$ is the algebra of Cayley numbers, then $e_i^2 = -1$, for all $i \geqslant 1$ and $e_i e_j = \lambda e_k, \lambda = \pm 1$, for all $i, j \geqslant 1, i \neq j$ and a suitable $k \geqslant 1$; in addition, for every cyclic permutation σ of the symbols i, j, k, $e_{\sigma(i)} e_{\sigma(j)} = \lambda e_{\sigma(k)}$. With these properties in hand, the multiplication table in the algebra $\mathbb{O}$ is fully determined by the following conditions:

$$e_i e_{i+1} = e_{i+3}, \quad i = 1, \ldots, 7; \quad e_{7+j} = e_j, \text{ for } j > 0. \tag{13}$$

In case of arbitrary $\alpha, \beta, \gamma \in F$, we set formally $e_1 = \sqrt{\alpha} e_1', e_2 = \sqrt{\beta} e_2', e_3 = \sqrt{\gamma} e_3', e_4 = \sqrt{\alpha\beta} e_4', e_5 = \sqrt{\beta\gamma} e_5', e_6 = \sqrt{\alpha\beta\gamma} e_6', e_7 = \sqrt{\alpha\gamma} e_7'$; then multiplication of the elements e_i' is according the formulas analogous to those in (13) and, the multiplication table for the elements e_i will contain only positive integer powers of the parameters α, β, γ:

$$e_1 e_2 = e_4, e_2 e_4 = \beta e_1, e_5 e_6 = \beta\gamma e_1, \ldots$$

The multiplication table of the algebra of Cayley numbers may be also defined with the aid of the scheme in Fig. 1 below. The enumeration of the vertices may be arbitrary since different enumerations give isomorphic algebras. The indicated enumeration is in accordance with the choice of a basis satisfying conditions (13).

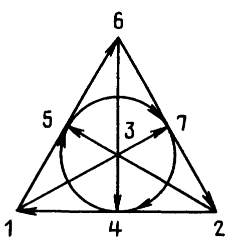


Fig. 1

A composition algebra A is called a *split composition algebra* if it satisfies one of the following equivalent conditions:

a) $n(x) = 0$, for some $x \neq 0$ in A;
b) $xy = 0$, for some $x \neq 0, y \neq 0$ in A;
c) A contains a non-trivial idempotent (i.e. an element $e \neq 0, 1$ such that $e^2 = e$).

Recall that an algebra A is called a *division algebra*, if, for every a, b $(a \neq 0)$ in A, the following equations are solvable in A:

$$ax = b, \quad ya = b.$$

If, for $a \neq 0$, each of these equations has a unique solution and A contains a unity, then A is called a *(skew) field*. It is easy to see that every finite-dimensional algebra without zero divisors is a division algebra, thus every composition algebra is either split or else is a division algebra (and therefore a skew-field).

Let us give examples of split composition algebras over a field F.

1. $n = \dim_F A = 2, A = F \oplus F$, with the involution $\overline{(\alpha, \beta)} = (\beta, \alpha)$.
2. $n = 4, A = F_2$ – the algebra of 2×2 matrices over F with the simplectic involution $\overline{\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}} = \begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix}$.
3. $n = 8, A = \mathbb{O}(F)$ – the so-called *"Cayley-Dickson matrix algebra"* consists of all the matrices of the form $\begin{pmatrix} \alpha & u \\ v & \beta \end{pmatrix}$, where $\alpha, \beta \in F$ and u, v are vectors in the three-dimensional vector space F^3, with ordinary matrix operations of addition and multiplication by a scalar and the following multiplication:

$$\begin{pmatrix} \alpha & u \\ v & \beta \end{pmatrix} \begin{pmatrix} \gamma & z \\ w & \delta \end{pmatrix} = \begin{pmatrix} \alpha\gamma + (u, w) & \alpha z + \delta u - v \times w \\ \gamma v + \beta w + u \times z & \beta\delta + (v, z) \end{pmatrix},$$

where (x, y) denotes the scalar product of vectors $x, y \in F^3$ and $x \times y$ denotes their "vector" product. Involution in the algebra $\mathbb{O}(F)$ is defined in the same way as in the algebra F_2 and, for the element $a = \begin{pmatrix} \alpha & u \\ v & \beta \end{pmatrix}$, we have $n(a) = a\bar{a} = \alpha\beta - (u, v), t(a) = a + \bar{a} = \alpha + \beta$.

Theorem (Jacobson, 1958, Zhevlakov, Slin'ko, Shestakov, Shirshov, 1978). *Every split composition algebra over a field F is isomorphic to one of these algebras: $F \oplus F$, $F_2, \mathbb{O}(F)$.*

Note that condition a) in the definition of a split algebra is always satisfied in a composition algebra over an algebraically closed field, thus the following holds:

Corollary. *There are only four non-isomorphic composition algebras over an algebraically closed field F.*

Classification of the composition algebras over the fields $\mathbb{Q}_p$ of p-adic numbers is the same, since every quadratic form in 5 and more variables over $\mathbb{Q}_p$ represents zero. Over the field $\mathbb{R}$ of real numbers, there exist only 7 non-isomorphic composition algebras: 3 split and 4 division algebras: $\mathbb{R}, \mathbb{C}, \mathbb{H}, \mathbb{O}$. The latter 4 algebras are unique finite-dimensional alternative division algebras over $\mathbb{R}$. There are also non-alternative, finite-dimensional division algebras over $\mathbb{R}$ (Kuz'min, 1966). In general, they have not been described, but the following fundamental result holds:

Theorem (Bott, Milnor, 1958). *Finite-dimensional division algebras over $\mathbb{R}$ exist only in dimensions 1, 2, 4, 8.*

An algebraic proof of this result is not yet known. The known proof is topological and is based on investigations of topological properties of the mapping of the sphere S^{n-1} into itself, induced by multiplication in an n-dimensional division algebra. With the aid of the methods of mathematical logic, using the completeness of the elementary theory of real closed fields, it can be shown that an analogous result holds for finite-dimensional division algebras over an arbitrary real closed field.

In the conclusion we note that the classification of the composition algebras over the fields of algebraic numbers is also known (Jacobson, 1958).

2.2. Projective Planes and Alternative Skew-Fields. We have seen that the alternative algebras have naturally risen from the study of quadratic forms, admitting composition. Another factor that stimulated the development of alternative algebras was their relation with the theory of projective planes, established at the beginning of the thirties in papers by Moufang.

We note that the ordered pair of sets $\pi = (\pi_0, \pi^0)$ is called a *projective plane* with the set of points π_0 and the set of lines π^0, if a relation of incidence (i.e. belonging of a point P to a line l) exists between these two sets, subject to the following conditions:

1. If $P_1, P_2 \in \pi_0, P_1 \neq P_2$, then there exists a unique line $l \in \pi^0$, containing P_1 and P_2 (denoted by $l = P_1P_2$).
2. If $l_1, l_2 \in \pi^0, l_1 \neq l_2$, then there exists a unique point $P \in \pi_0$ that belongs both to l_1 and to l_2 ($P = l_1 \cap l_2$).
3. There exist 4 point in a general position, i.e. a position such that no three of these points belong to one line.

A classical example of a projective plane is a two-dimensional projective space PF^2, over a field F, whose points are one-dimensional subspaces of the linear space F^3 and whose lines are the two-dimensional subspaces. If $F = F_q$ is a field with q elements, then PF^2 is a finite plane, containing $q^2 + q + 1$ points and lines. In particular, for $q = 2$ we get the smallest projective plane, the so-called *Fano plane*. It may be pictured as in Fig. 1, if the arrows there are removed and if the "lines" are considered to be the sides and the altitudes of the triangle as well as its inscribed circle.

Let P be a point and l be a line in the projective plane π. The plane π is called a (P,l)-*Desargues plane*, if for any of its different points A, B, C, A', B', C', such that (1) $AA' \cap BB' \cap CC' = P$, (2) $AB \neq A'B'$, $AC \neq A'C'$, $BC \neq B'C'$, (3) $AB \cap A'B' \in l$, $AC \cap A'C' \in l$, the intersection $BC \cap B'C'$ also belongs to l.

The two resulting configurations (depending on whether the point P belongs to the line l or not) are pictured in Fig. 2 and 3:

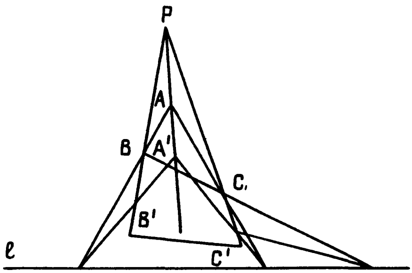


Fig. 2

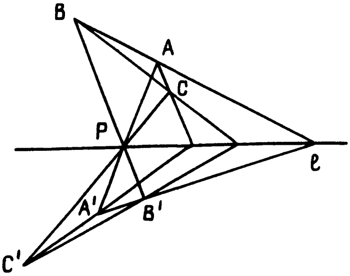


Fig. 3

If a plane π is (P,l)-Desargues, for every point $P \in l$, then π is called l-*Desargues* (or else we speak of π as of the translation plane, with respect to the line l). A plane π is called a *Desargues plane*, if it is a (P,l)-Desargues plane, for every P and l. In this case we say that the *Desargues theorem* holds in π. An example of a Desargues projective plane is the aforementioned plane PF^2. If the plane π is l-Desargues, for every line l, then we say that the *little Desargues theorem* holds in π and π is called a *Moufang plane* in this case.

Coordinates may be introduced into every projective plane in the following way. Let X, Y, O, I be four points in a general position. Let us call the line XY – the line at infinity l_∞ and, call the line OI – the line $y = x$. On the line OI, assign the coordinates $(0,0)$ to the point O, the coordinates $(1,1)$ to the point I, and assign the single coordinate (1) to the point Z of the intersection of the lines OI and XY. We assign the coordinates (b,b) to other points of the line OI, where b are symbols different for different points. Let now $P \notin l_\infty$ and $XP \cap OI = (b,b)$, $YP \cap OI = (a,a)$. Then we assign the coordinates (a,b) to the point P. By this rule, the previous coordinates are assigned to the points of the line OI. Let the line connecting $(0,0)$ and $(1,m)$ intersect l_∞ in a point M. Assign a unique coordinate (m) to the point M; it may be interpreted as a characterization of the slope of the line OM. Finally, assign the symbol (∞) as the coordinate of the point Y (cf. Fig. 4).

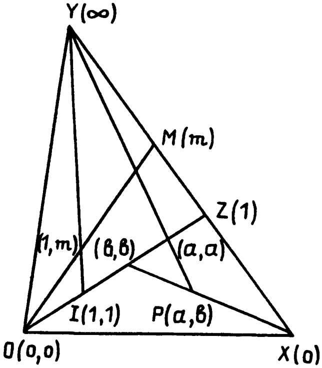


Fig. 4

We point out that by this very construction we may obtain the Cartesian coordinates in the ordinary real plane. In doing this, the point X should be considered to be the point at infinity of the axis x, and Y – the point at infinity of the axis y, O is the coordinate origin and I is the point $(1,1)$.

Let us define now algebraic operations of addition and multiplication on the set R of the coordinate symbols b. Set $a+b=c$, for some elements $a,b,c \in R$, if the point (a,c) belongs to the line connecting the points $(0,b)$ and (1) and $a \cdot b = c$, if the point (a,c) lies on the line connecting the point $(0,0)$ with (b). It is easy to see that the following equalities are satisfied:

$$a+0=0+a=a,$$
$$0 \cdot a = a \cdot 0 = 0,$$
$$1 \cdot a = a \cdot 1 = a.$$

Moreover, the following equations in R are uniquely solvable in x, y:

$$y+a=b, \quad a+x=b, \quad c \cdot x = a, \quad y \cdot c = a,$$

for every a,b,c $(c \neq 0)$ in R.

The algebraic system $\langle R, +, \cdot \rangle$ does not in general satisfy the axioms of a (non-associative) ring and, generaly speaking, does not define the plane π. Moreover, in choosing different coordinates, one plane π may be assigned several different coordinatizing systems $\langle R, +, \cdot \rangle$, which may be non-isomorphic. The situation changes if we impose some Desargues conditions on π.

Theorem 1 (Skornyakov, 1951), (Pickert, 1955). *A projective plane π is an l-Desargues plane, for two different lines l, containing the point $Y = (\infty)$, if and only if the corresponding coordinatizing system $\langle R, +, \cdot \rangle$ is a left alternative skew-field. A plane π is a Moufang (Desargues) plane if and only if every of its coordinatizing systems is an alternative (respectively, associative) skew-field. Every two skew-fields coordinatizing a Desargues plane are mutually isomorphic.*

Conversely, given a (non-associative) skew-field R, then we can always construct a projective plane π by it, whose one of the coordinatizing skew-fields is R. In addition, if R is alternative (associative), then π is Moufang (respectively, Desargues).

In the case of an arbitrary projective plane it is more suitable to consider one ternary operation, instead of the binary operations of addition and multiplication, on the set of the coordinate symbols R. If $a, b, c, d \in R$, then set $d = a \cdot b \circ c$, if the point (a, d) lies on the line connecting the points (b) and $(0, c)$. It is easy to see, that $a + b = a \cdot 1 \circ b$, $a \cdot b = a \cdot b \circ 0$, i.e. the former binary operations are expressible in terms of the ternary ones. The set R, together with the introduced operation $a \cdot b \circ c$ is called *ternary of the plane* π. The advantage of a ternary is in the fact that the plane it coordinatizes may be uniquely restored by the ternary. However, in this case too, several non-isomorphic ternaries may correspond to one plane.

Relation of the theory of projective planes with the alternative rings has initiated a series of algebraic questions on their structure. First of all, the question of description of alternative skew-fields had risen. A study on them was initiated by Zorn and Moufang. One of the results obtained by Zorn was the following:

Theorem 2. *A finite alternative skew-field is associative and is the Galois field* F_q.

This theorem easily follows from Artin's theorem on associativity of two-generated alternative ring (cf. 2.3 in the sequel) and the classical Wedderburn theorem on finite associative skew-fields, which states that every such skew-field is a field and is generated by one element.

Because of Theorem 1, Theorem 2 implies the following

Corollary. *Every finite Moufang plane is a Desargues plane.*

A final description of alternative skew-fields was obtained at the beginning of the fifties by Bruck and Kleinfeld and independently by L.A Skornyakov, who proved that every alternative, non-associative skew-field is a Cayley-Dickson algebra over its center. This result had enabled them to prove, in particular, that every two alternative skew-fields coordinatizing the same Moufang plane π are mutually isomorphic. Somewhat later, L.A. Skornyakov had proved that every right alternative (or left alternative) skew-field is alternative. In view of Theorem 1, the latter means that if a projective plane π is an l-Desargues plane, for two different lines l, then π is a Moufang plane.

Thus, the Moufang (non-Desargues) planes are exactly the planes that can be coordinatized by the Cayley-Dickson division algebras (Cayley-Dickson skew-fields). By the corollary of Theorem 2, they are all infinite. We will give another realization of these planes in 3.5.

In the conclusion we add a few words about finite planes. It is not difficult to show that, in a finite projective plane π, every line contains exactly as many points as the number of lines passing through an arbitrary point. If this number equals $n+1$, then we say that π is of order n. In this case, the number of all the points in π equals n^2+n+1. For instance, PF_q^2 is of order $q = p^r$ (where p is prime). It turns out that, not for every n are there planes of order n. At this time, no finite plane is known of order different from p^r. It has been proved for instance that there are no planes of orders 6 and 14. The question for $n = 10$ remains open. It is known that there exist non-Desargues planes of orders p^r, for all $r \geqslant 2$ and all $p \neq 2$, and also of orders 2^{2r}, where $r \geqslant 2$. For $n = p^r < 9$, there exist only Desargues planes.

2.3. Moufang's Identities and Artin's Theorem. Let A be an alternative algebra (a. a.) over a field F. We have already observed that the associator $(x, y, z) = (xy)z - x(yz)$ in the algebra A is an alternating function of its arguments. In particular, the following identity holds in A:

$$(x, y, x) = 0. \tag{14}$$

The algebras satisfying (14) are called *flexible algebras*. It is easy to see that, for instance, every commutative or anticommutative algebra is flexible.

Let us prove that the following identities are satisfied in an a. a. A:

$$(x, y, yz) = (x, y, z)y \tag{15}$$

$$(x, y, zy) = y(x, y, z). \tag{16}$$

By (1.13), we have

$$(x, y, xy) = -(x, xy, y) = x(x, y, y) + (x, x, y)y - (x^2, y, y) - (x, x, y^2) = 0.$$

Linearizing this identity in x, we get

$$(xy, z, y) + (zy, x, y) = 0,$$

which implies, by (1.13) and (14), the following identity:

$$0 = (xy, z, y) + (x, y, zy) = (x, y, z)y + (x, yz, y).$$

This proves (15). Identity (16) is proved analogously.

Well known *Moufang identities* are easily provable using (15) and (16):

$$(xy \cdot z)y = x(y \cdot zy) - \textit{the right Moufang identity},$$

$$(yz \cdot y)x = y(z \cdot yx) - \textit{the left Moufang identity},$$

$$(xy)(zx) = x(yz)x - \textit{the central Moufang identity}.$$

For instance, $(xy \cdot z)y - x(yzy) = (x \cdot yz)y + (x, y, z)y - (x \cdot yz)y + (x, yz, y) = 0$.

We can now prove the following theorem we mentioned earlier:

Artin's Theorem. *In an a. a. A, any two elements generate an associative subalgebra.*

Proof. Let A_0 be the subalgebra generated by elements $a, b \in A$. In order to prove its associativity, it is enough to prove, because of the distributivity of multiplication, that, for arbitrary finite products u_1, u_2, u_3, of the elements a, b, the identity $(u_1, u_2, u_3) = 0$ holds. We will prove this claim by induction on the total number of factors in the products u_1, u_2, u_3. The basis of induction consists in the alternativity and flexibility conditions. By the inductive hypothesis, we may assume that u_1, u_2, u_3 are associative products of the elements a, b. In this case, in two of them, the rightmost factors must coincide. Let, for instance, $u_1 = v_1 a$, $u_2 = v_2 a$. If either v_1 or v_2 are absent then, by the inductive hypothesis and (15) and (16), $(u_1, u_2, u_3) = 0$. We can therefore assume that v_1 and v_2 are non-empty. Let us linearize identity (16) in y:

$$(x, y, zw) + (x, w, zy) = y(x, w, z) + w(x, y, z).$$

Setting here $x = u_1, y = u_3, z = v_2, w = a$, we get the following, by the inductive hypothesis:

$$(u_1, u_2, u_3) = -(v_1 a, u_3, v_2 a) = (v_1 a, a, v_2 u_3) - a(v_1 a, u_3, v_2) - \\ u_3(v_1 a, a, v_2) = (v_1 a, a, v_2 u_3) = a(v_1, a, v_2 u_3) = 0.$$

The theorem has been proved. □

The following more general claim may be proved by similar arguments: any three elements a, b, c in an a. a. A that satisfy the relation $(ab)c = a(bc)$, generate in A an associative subalgebra (compare with Moufang's theorem in 6.2).

Corollary. *Every a. a. is power-associative.*

In particular, in every a. a. A, there is a uniquely defined nilradical $\operatorname{Nil} A$.

2.4. Finite-Dimensional Alternative Algebras (Schafer, 1966). Let A be an a. a., let M be an alternative A-bimodule and let (ρ, λ) be the corresponding birepresentation of the algebra A (cf. 1.2). It is said that the algebra A acts nilpotently on M, if the algebra $\langle \rho(A) \cup \lambda(A) \rangle$, generated in $\operatorname{End} M$ by the set $\rho(A) \cup \lambda(A)$ is nilpotent. If $x \in A$, then it is said that x acts nilpotently on M, if the subalgebra $\langle \rho(x), \lambda(x) \rangle$ is nilpotent. (1.18) implies that the algebra $\langle \rho(x), \lambda(x) \rangle$ is commutative and that $\rho(x^k), \lambda(x^k) \in \langle \rho(x), \lambda(x) \rangle$, for every $k \geqslant 1$.

Theorem. *Let A be an a. a. over the field F and let M be a finite-dimensional alternative A-bimodule. Let, in addition, C be a multiplicatively closed subset in A generating the algebra A. Then, if every element $c \in C$ acts nilpotently on M, A too acts nilpotently on M.*

Proof. Note that there are multiplicatively closed subsets $B \subseteq C$, such that the algebra $\langle B \rangle$, generated by B acts nilpotently on M. For instance the set $\{x^k \mid k \geqslant 1\}$, for every $x \in C$. Moreover, the set $\{x \in A \mid Mx = xM = 0\}$ is an ideal in A (it easily follows from the fact that the split null extension $A \dotplus M$ is alternative). Consequently, we may assume, without loss of generality, that the birepresentation (ρ, λ) is exact (i.e. $\operatorname{Ker} \lambda \cap \operatorname{Ker} \rho = 0$) as well as that the algebra A is finite-dimensional over F. Let D be a maximal multiplicatively closed subset in C, such that the subalgebra $\langle D \rangle$ acts nilpotently on M. We may assume that $D \subsetneqq C$. By assumption, there is an n such that $M\sigma_1 \dots \sigma_n = 0$, for all $\sigma_1, \dots, \sigma_n$ from the set $\{\rho(x), \lambda(x) \mid x \in D\}$. Let $M_i = \{m \in M \mid m\sigma_1 \dots \sigma_i = 0, \text{ for all } \sigma_1, \dots, \sigma_i\}$; then $0 = M_0 \subseteq M_1 \subseteq \dots \subseteq M_n = M$.

Let us consider an arbitrary element w of the form

$$w = \sigma_1 \dots \sigma_{i-1} \tau \sigma_{i+1} \dots \sigma_{2n}, \tag{$*$}$$

where σ_i are same as above, $\tau = \rho(a)$ or $\tau = \lambda(a)$, $i = 1, \dots, 2n-1$. It is clear that $w = 0$. Let now y be an arbitrary element in A, which is a product of $2n+1$ factors, $2n$ of which belong to D. It follows easily from (1.18) that $\rho(y)$ and $\lambda(y)$ are linear combinations of elements of the form (*), thus $\rho(y) = \lambda(y) = 0$ and $y = 0$. Hence, $\langle D \rangle$ acts nilpotently on A (and, in particular, on C), thus there exists an element $z \in C$, such that $z \notin D, zD \cup Dz \subseteq D$. Clearly $z^k D \cup Dz^k \subseteq D$, for all $k \geqslant 1$, thus the set $E = D \cup \{z^k \mid k \geqslant 1\}$ is multiplicatively closed and properly contains D.

It only remains to prove that $\langle E \rangle$ acts nilpotently on M. (1.18) implies that every M_i is invariant with respect to $\rho(z)$ and $\lambda(z)$, hence M_i is a $\langle E \rangle$-bimodule. The algebra $\langle E \rangle$ acts nilpotently on every quotient M_i/M_{i-1}, hence it acts nilpotently on M too. This contradiction finishes the proof. □

Note that the explicit form of the alternativity condition has not been used in the proof of the theorem. The same proof is applicable in case when A is, for instance, a Lie algebra and M a Lie bimodule. Moreover, the reasoning used is still valid in every class $\mathfrak{M}$ of algebras, defined by the homogeneous identities of the third degree, such that, for every algebra A and its every ideal I, the set I^2 is again an ideal of A. The necessary changes, related to the possible non-associativity of powers in A are fairly obvious (Stitzinger, 1983).

The right and left Moufang identities imply that every alternative birepresentation (ρ, λ) satisfies the following relations

$$\rho(xyx) = \rho(x)\rho(y)\rho(x), \quad \lambda(xyx) = \lambda(x)\lambda(y)\lambda(x).$$

This and the relations $\rho(x^2) = \rho(x)^2, \lambda(x^2) = \lambda(x)^2$ imply easily that $\rho(x^k) = \rho(x)^k, \lambda(x^k) = \lambda(x)^k$, for all $k \geqslant 1$. In particular, if the element x is nilpotent, then it acts nilpotently on every alternative bimodule.

Using a regular birepresentation, we obtain the following

Corollary 1. *Let A be a finite-dimensional a. a. and C be a multiplicatively closed nilsubset of A. Then the subalgebra $\langle C \rangle$ acts nilpotently on A and, in particular, is itself nilpotent.*

Corollary 2. *The nilradical $\mathrm{Nil}\, A$ of a finite-dimensional a. a. A is nilpotent.*

The quotient algebra $A/\mathrm{Nil}\, A$ does not contain non-zero nilideals, i.e. it is semisimple. The structure of semisimple a. a. is described by the following

Theorem. *A finite-dimensional semisimple a. a. is isomorphic to the direct sum of simple algebras, each of which is either associative and is a matrix algebra over a skew-field or is a Cayley-Dickson algebra over its center.*

A finite-dimensional a. a. A over the field F is called a *separable algebra* if, for every extension K of the field F, the algebra $A_K = K \otimes_F A$ is semisimple. As in the case of the associative algebras, this is equivalent to the property that the algebra A is semisimple and the center of its every simple component is a separable extension of the field F.

The following theorem generalizes the classical Wedderburn-Malcev theorem in the theory of associative algebras to the a. a.

Theorem. *Let A be a finite-dimensional a. a. over the field F and let $N = \mathrm{Nil}\, A$ be its nilradical. If the quotient algebra A/N is separable over F, then $A = B \dotplus N$ (the direct sum of vector spaces), where B is a subalgebra of the algebra A, isomorphic to A/N. If F is a field of characteristic $\neq 2, \neq 3$ and B_1 is another subalgebra of A, isomorphic to A/N, then there exists an inner automorphism ϕ of the algebra A, such that $B_1 = B^{\phi}$.*

We will not specify the form of these inner automorphisms of the a. a., since they look fairly complicated in general. We only point out that, over a field of characteristic zero, ϕ may be chosen to be in the subgroup generated by the automorphisms of the form $\exp(D)$, where D is a nilpotent inner derivation of the algebra A lying in the radical of its multiplication algebra $M(A)$.

Let us clarify now how the inner derivations of the a. a. look, over the fields of characteristics $\neq 2, \neq 3$.

First of all it is not difficult to see that the mapping $R_a - L_a$ is a derivation of an a. a. A, for some $a \in A$, if and only if the element a is in the center $N(A)$ of the algebra A. Furthermore, the fact that the associator (x, y, z) is skew-symmetric implies the following relations:

$$-R_{xy}+R_xR_y = L_{xy}-L_yL_x = [L_y, R_x] = [R_y, L_x] = L_xL_y-L_{yx} = R_{yx}-R_yR_x$$

for all $x, y \in A$. This, in particular implies that

$$[R_x, R_y] = R_{[x,y]} - 2[L_x, R_y]. \tag{17}$$

Furthermore, in view of the relation $R_x \circ R_y = R_{x \circ y}$, we get

$$[R_y,[R_x,R_z]] = (R_x \circ R_y)\circ R_z - (R_z \circ R_y)\circ R_x = R_{(x\circ y)\circ z-(z\circ y)\circ x} = R_{[y,[x,z]]-2(x,y,z)} \tag{18}$$

Let us consider the following mapping, for arbitrary $x, y \in A$:

$$D_{x,y} = R_{[x,y]} - L_{[x,y]} - 3[L_x, R_y]. \tag{19}$$

For every $z \in A$, by (17) and (18) we have

$$2[R_z, D_{x,y}] = 3[R_z, R_{[x,y]} - 2[L_x,R_y]] - [R_z, R_{[x,y]}] - 2[R_z, L_{[x,y]}] = 3[R_z,[R_x,R_y]] - R_{[z,[x,y]]} = R_{2[z,[x,y]]-6(x,z,y)} = 2R_{zD_{x,y}},$$

which implies that $D_{x,y}$ is a derivation of the algebra A. Clearly the derivations $R_a - L_a$ ($a \in N(A)$) and $D_{z,y}$ ($x, y \in A$) are inner. Let us show now that if A contains 1, then every inner derivation D of the algebra A is of the form

$$D = R_a - L_a + \sum_i D_{x_i,y_i}, \quad a \in N(A), x_i, y_i \in A. \tag{20}$$

Indeed relations (17) and (18) and their left analogues easily imply that the Lie algebra Lie(A) of multiplications of the algebra A consists of elements of the form $R_x + L_y + \sum_i [L_{x_i}, R_{y_i}]$, $x, y, x_i, y_i \in A$. It is clear that every such an element may be represented in the form $T = R_g + L_h + \sum_i D_{u_i,v_i}$. Now, if T is a derivation, then $0 = 1T = g + h$, hence $R_g - L_g = T - \sum_i D_{u_i,v_i}$ is a derivation of the algebra A, and $g \in N(A)$. This finishes the proof.

We have already pointed out in Sect. 1 that every derivation of a finite-dimensional central simple associative algebra is inner. Let us clarify now what does the derivation algebra Der $\mathbb{O}$ of the Cayley-Dickson algebra $\mathbb{O}$ look like.

Let $\mathbb{O}$ be a Cayley-Dickson algebra over a field F of characteristic $\neq 2, \neq 3$, let $n(x)$ be the norm of an element $x \in \mathbb{O}$ and let $f(x,y)$ be the bilinear form on $\mathbb{O}$, associated with $n(x)$. Let us represent $\mathbb{O}$ in the form $\mathbb{O} = F\cdot 1 \dotplus \mathbb{O}_0$, where $\mathbb{O}_0$ is the set of elements in $\mathbb{O}$ with the zero trace. It is not difficult to show that every element in $\mathbb{O}_0$ is the sum of commutators, thus $\mathbb{O}D \subseteq \mathbb{O}_0$, for every $D \in$ Der $\mathbb{O}$. In addition, for every $x \in \mathbb{O}$ we have $(x+\overline{x})D = (t(x)\cdot 1)D = 0$, hence $\overline{x}D = -xD = \overline{xD}$. Now

$$f(xD,y) + f(x,yD) = xD\cdot\overline{y} + y\cdot\overline{xD} + x\cdot\overline{yD} + yD\cdot\overline{x} = t(xD\cdot\overline{y} + x\cdot\overline{yD}) = t(xD\cdot\overline{y} + x\cdot\overline{y}D) = t((x\overline{y})D) = 0,$$

i.e. D is skew-symmetric, with respect to the form f. It is easy to see, that the operators of multiplication by elements in $\mathbb{O}_0$ are skew-symmetric with respect to f. The set $o(8,f)$ of all the skew-symmetric linear transformations of $\mathbb{O}$ with respect to f, form a subalgebra of the Lie algebra (End $\mathbb{O})^{(-)}$ – an orthogonal Lie algebra of dimension $\frac{1}{2}\cdot 8\cdot(8-1) = 28$ over F. The elements of the form $D + R_x + L_y$, where $D \in$ Der $\mathbb{O}$, $x, y \in \mathbb{O}_0$ form a subspace of

$o(8, f)$, which is the direct sum of the spaces $\operatorname{Der}\mathbb{O}$, $R_{\mathbb{O}_0} = \{R_x \mid x \in \mathbb{O}_0\}$ and $L_{\mathbb{O}_0} = \{L_x \mid x \in \mathbb{O}_0\}$. In fact the following equality holds:

$$\operatorname{Der}\mathbb{O} \dotplus R_{\mathbb{O}_0} \dotplus L_{\mathbb{O}_0} = o(8, f),$$

thus, $\dim \operatorname{Der}\mathbb{O} = 28 - 7 - 7 = 14$. In addition, the algebra $\operatorname{Der}\mathbb{O}$ is simple. Thus the following theorem holds:

Theorem. *Let $\mathbb{O}$ be the Cayley-Dickson algebra, over a field of characteristic $\neq 2, \neq 3$. Then the derivation algebra $\operatorname{Der}\mathbb{O}$ is a 14-dimensional central simple Lie algebra.*

According to the classification of finite-dimensional simple Lie algebras over an algebraically closed field K of characteristic 0, only one of them is of dimension 14 – it is the exceptional algebra $\mathbb{G}_2$. The theorem implies that $\mathbb{G}_2 \cong \operatorname{Der}\mathbb{O}$, where $\mathbb{O}$ is the (split) Cayley-Dickson algebra over K. Let $\overline{F}$ be the algebraic closure of the field F. A central simple Lie algebra L over F is called an algebra of type $\mathbb{G}_2$, if $\overline{F} \otimes_F L \cong \operatorname{Der}\mathbb{O}$, where $\mathbb{O}$ is the (split) Cayley-Dickson algebra over $\overline{F}$. It is clear that for every Cayley-Dickson algebra $\mathbb{O}$, the algebra $\operatorname{Der}\mathbb{O}$ is an algebra of type $\mathbb{G}_2$. Conversely, every central simple Lie algebra of type $\mathbb{G}_2$ over the field of characteristic $\neq 2, \neq 3$, is isomorphic to the algebra $\operatorname{Der}\mathbb{O}$, for an appropriate Cayley-Dickson algebra $\mathbb{O}$; in addition, $\operatorname{Der}\mathbb{O}_1 \cong \operatorname{Der}\mathbb{O}_2$, if and only if $\mathbb{O}_1 \cong \mathbb{O}_2$.

Corollary. *Every derivation D of a Cayley-Dickson algebra $\mathbb{O}$ of characteristic $\neq 2, \neq 3$ is inner and is of the form $D = \sum_i D_{x_i, y_i}$, where $x_i, y_i \in \mathbb{O}$.*

Indeed, for every a. a. A the derivations of the form $\sum_i D_{x_i, y_i}$ form an ideal in the algebra $\operatorname{Der} A$, and since this ideal is non-zero in the algebra $\operatorname{Der}\mathbb{O}$, everything follows from the fact that $\operatorname{Der}\mathbb{O}$ is simple.

Combining this result with known facts on derivations of central simple associative algebras, we arrive, in a standard way, to the fact that every derivation D of a finite-dimensional separable a. a. A of characteristic $\neq 2, \neq 3$, is inner and is of the form (20). Furthermore, in case of characteristic 0, we may choose $a = 0$.

We also point out that a finite-dimensional a. a. A of characteristic 0 is semisimple if and only if the Lie algebra $\operatorname{Der} A$ is semisimple.

At the conclusion let us shortly look into the structure of the bimodules over finite-dimensional a. a. Just as in the case of the associative algebras, every alternative bimodule over a separable a. a. is completely reducible. The structure of irreducible bimodules is described in the following

Theorem (Schafer, 1952). *Let A be a finite-dimensional a. a., let M be a faithful irreducible alternative A-bimodule and let (ρ, λ) be the corresponding birepresentation of the algebra A. Then either M is an associative bimodule over the (associative) algebra A or one of the following cases holds:*

1) *A is the algebra of generalized quaternions, λ is a (right) associative irreducible representation of A and $\rho(a) = \lambda(\overline{a})$, for every $a \in A$;*

2) *A is the Cayley-Dickson algebra and $M = A$ is a regular A-bimodule.*

A few words about the methods of study of finite-dimensional a. a. These methods have a lot in common for different classes of algebras that are nearly associative (except the Lie algebras and their generalizations). In investigating simple and semisimple algebras the methods consist in passing to an algebraically closed field, in finding a sufficient number of orthogonal idempotents, and using the properties of Pierce decomposition of algebras. In studying solvable and nilalgebras the methods consist in the passage to the associative enveloping algebras. Apart from these, all the cases explore the traditional methods of finite-dimensional linear algebra: eigen vectors, minimal polynomials, the trace bilinear form etc.

2.5. Structure of Infinite-Dimensional Alternative Algebras (Zhevlakov, Slin'ko, Shestakov, Shirshov, 1978). We have already mentioned in Sect.1 that the fundamental instrument in building a structure theory of one or another class of algebras is the notion of a radical. In the case of infinite-dimensional a. a., the most important role is played by the quasi-regular and prime radicals.

The quasi-regular radical $\operatorname{Rad} A$ of an a. a. A is a direct generalization of the corresponding notion from the theory of associative algebras and allows several equivalent characterizations:

1) $\operatorname{Rad} A$ is the largest right (left) quasi-regular ideal of the algebra A;
2) $\operatorname{Rad} A$ is the intersection of all maximal modular right (left) ideals of the algebra A;
3) $\operatorname{Rad} A$ is the intersection of the kernels of all of the irreducible right (left) representations of the algebra A.

Here, just as in the case of associative algebras, an ideal I is called a *quasi-regular ideal* if every element $x \in I$ is *quasi-invertible* (i.e. the element $1-x$ is invertible in the algebra $A^\sharp$, obtained from A by adjoining an external unity); a right ideal I is a *modular right ideal*, if there exists an element $e \in A$ such that $x - ex \in I$, for every $x \in A$.

An algebra A is called *semisimple*, if $\operatorname{Rad} A = 0$ and is called (right) *primitive*, if A contains a maximal modular right ideal that does not contain non-zero two-sided ideals.

Construction of semisimple a. a. is described in the following

Theorem. *Every semisimple a. a. is isomorphic to a subdirect sum of primitive algebras, each of which is either associative or is the Cayley-Dickson algebra.*

The *prime radical* of an a. a. A is defined as the smallest ideal $P(A)$ for which the quotient algebra $A/P(A)$ is *semiprime* (i.e. does not contain non-zero nilpotent ideals). The ideal $P(A)$ may be not nilpotent in general, although it is a nilideal. Every semiprime algebra is isomorphic to a subdirect sum of *prime algebras* (i.e. algebras where the product of every two non-zero two-sided ideals is always different from 0). Simple algebras and algebras without zero divisors are examples of prime algebras.

The problem of describing the simple algebras is one of the central questions in studying every class of algebras. In a difference from the associative algebras, where this problem is practicably invisible (since every associative algebra may be embedded into a simple one), simple a. a. have an exhaustive description, modulo associative algebras.

Theorem. *Every simple non-associative a. a. is the Cayley-Dickson algebra over its center.*

This theorem generalizes, in particular, the Bruck-Kleinfeld-Skornyakov theorem on the structure of alternative skew-fields that was mentioned in 2.2.

One can relate a series of prime algebras with every central simple algebra. Let A be a central algebra over a field F. A subring $B \subseteq A$ is called a *central order* in A, if its center Z is contained in F and the ring of fractions $Z^{-1}B = \{z^{-1}b \mid 0 \neq z \in Z, b \in B\}$ coincides with A. It is easy to see that every central order of a simple algebra is a prime algebra. The central orders in Cayley-Dickson algebras are called the *Cayley-Dickson rings.* Prime a. a. are exhausted by these rings, with the exception of some "pathological" cases.

Theorem. *Every prime non-associative a. a. of characteristic* $\neq 3$ *is a Cayley-Dickson ring.*

The restriction on the characteristic is, generally speaking, essential. But it may be replaced, for instance, by the condition of A not having *absolute zero divisors* (i.e. elements a for which $aAa = 0$) or by the condition of A not having non-zero locally nilpotent ideals. Recall that an algebra A is called a *locally nilpotent algebra,* if every finitely generated subalgebra of A is nilpotent. Every a. a. A contains the largest locally nilpotent ideal $LN(A)$, which is called the *locally nilpotent radical* of the algebra A. The radical $LN(A)$ contains all the one-sided locally nilpotent ideals of the algebra A and all the absolute zero divisors; the quotient algebra $A/LN(A)$ is LN-semisimple and is isomorphic to a subdirect sum of prime LN-semisimple algebras.

The radicals $\operatorname{Nil} A$ (cf. 1.2), $\operatorname{Rad} A$, $LN(A)$ and $P(A)$ are related by the following inclusions:

$$\operatorname{Rad} A \supseteq \operatorname{Nil} A \supseteq LN(A) \supseteq P(A), \tag{21}$$

which are strict, in general, already in the case of the associative algebras. In finite-dimensional a. a. all these radicals coincide with the ordinary nilpotent radical (see 2.4). Moreover, they coincide within the class of *Artinian* a. a. (i.e. the algebras satisfying the minimality condition for the right ideals), for which the generalization of the classical associative theory is valid.

Theorem. *The Rad A is nilpotent in every Artinian a. a. A. An algebra A is Artinian semisimple if and only if it is a finite direct sum of full matrix algebras over skew-fields and the Cayley-Dickson algebras.*

It is not difficult to derive from here that, in an Artinian a. a., every nil-subalgebra is nilpotent. In particular, the properties of solvability and nilpotency are equivalent within the class of Artinian algebras. With some constraints on the characteristic, these properties are equivalent for finitely generated algebras and their subalgebras too. This is not the case in general – there exist examples of solvable, non-nilpotent a. a. over every field. Nevertheless, solvability and nilpotency are closely related within the class of a. a., as the following result shows:

Theorem (Pchelintsev, 1984, Shestakov, 1989). *Let A be a solvable alternative Φ-algebra. Then the subalgebra A^2 is nilpotent and, if $\frac{1}{6} \in \Phi$, then $(A^n)^3 = 0$, for some n.*

We also point out that over a field of characteristic 0, every alternative nilalgebra of bounded index is solvable.

Free algebras play an important role in the theory of every class of algebras: free non-associative algebra, free alternative algebra, free Lie algebra etc. Recall that the algebra $F_{\mathfrak{M}}[X]$ from the class $\mathfrak{M}$, with the set of generators X is called a *free algebra in the class* $\mathfrak{M}$ (or $\mathfrak{M}$-free), if every mapping from the set X into an arbitrary algebra A in $\mathfrak{M}$ is uniquely extendable to a homomorphism $F_{\mathfrak{M}}[X]$ to A.

The set of all the non-associative words made up out of elements of the set X forms the *basis of the free non-associative algebra* $F\{X\}$, over a field F; its elements may be viewed as non-associative, non-commutative polynomials in variables from X. If the class $\mathfrak{M}$ is defined by a system of identities $\{f_\alpha\}$, then the $\mathfrak{M}$-free algebra $F_{\mathfrak{M}}[X]$ is isomorphic to the quotient algebra $F\{X\}/I_{\mathfrak{M}}$, where $I_{\mathfrak{M}}$ is the ideal of the algebra $F\{X\}$, generated by the set $\{f_\alpha(y_1, \dots, y_{n_\alpha})/y_i \in F\{X\}\}$. Thus, the *free alternative algebra* $F_{\text{Alt}}[X]$ is isomorphic to the quotient algebra $F\{X\}$, mod the ideal I_{Alt}, generated by all the elements of the form (f_1, f_1, f_2), (f_1, f_2, f_2), where $f_1, f_2 \in F\{X\}$.

Many questions in the theory of a. a. are reduced to the study of the structure of free and PI-*algebras*, i.e. the algebras satisfying *essential polynomial identities*, namely identities which are not consequences of associativity. A general scheme of this reduction is as follows: In the free algebra, one looks for fully invariant (i.e. stable under endomorphisms) ideals, subalgebras or subspaces with certain nice properties (for instance being contained in some center). If, in an algebra A, the value of the elements from this ideal (or the subalgebra) are not all equal to zero, then A has a series of nice properties; otherwise, A is a PI-algebra.

Some basic properties of a free a. a. are described in the following

Theorem (Zhevlakov, Slin'ko, Shestakov, Shirshov, 1978; Il'tyakov, 1984; Filippov, 1984; Shestakov, 1976, 1977, 1983; Zel'manov, Shestakov, 1990).

Let $A = Alt[X]$ be the free a. a. over a field F of characteristic $\neq 2,3$ on the set of free generators X; let $Z(A)$ be its center and $N(A)$ its associative center. Then $[x,y]^4 \in N(A), (x,y,z)^4 \in Z(A)$, for all $x,y,z \in A$; for $|X| > 2$ the algebra A is not prime and for $|X| > 3$ it is not semiprime; $Rad A = \{x \in A \mid x^{n(x)} = 0\} = T(\mathbb{O}) \cap D(A)$, where $T(\mathbb{O})$ is the ideal of identities of the split Cayley-Dickson algebra over F and $D(A)$ is the associator ideal of A; if either $|X| < \infty$ or F is a field of characteristic 0, then $Rad A$ is nilpotent, and if $|X| \leqslant 3$, then $Rad A = 0$; if $|X| < |Y|$, then there is an identity in $Alt[X]$ which does not hold in $Alt[Y]$.

The study of structure of PI-algebras goes mainly by the pattern of the associative PI-theory. At this time, many principal results of that theory have been transfered to a. a. One of effective methods of investigation of alternative PI-algebras is a passage to algebras from other classes which are in one way or another connected with the given PI-algebra A. For instance, it is not difficult to check that, for an a. a. A, the algebra $A^{(+)}$ is a special Jordan algebra (see 3.1), where, if A is a PI-algebra, then $A^{(+)}$ is a Jordan PI-algebra. The most brilliant example of utilization of this connection are the results of A. I. Shirshov, devoted to solving the well known *Kurosh problem* inside the class of alternative PI-algebras. This problem, which is a typical example of a problem of the "Burnside" type, is formulated as follows: if in an algebra A, every singly generated subalgebra is finite-dimensional, then is every finitely generated subalgebra of A finite-dimensional? In general the answer is negative, already for the associative algebras (although for skew-fields the answer is not known), but if A is a PI-algebra, the answer is affirmative both for the associative as well as for the alternative and Jordan algebras. Furthermore, the solution of the problem for the a. a. relies essentially on the case of special Jordan algebras. Let us state an important partial case of this result.

Theorem. *An a. a. with the identity $x^n = 0$ is locally nilpotent.*

Along with the Jordan algebra $A^{(+)}$, it is useful to draw the algebra of right multiplications $R(A)$ into the study of properties of an a. a. A; this algebra inherits many properties of A. For instance, if A is a finitely generated PI-algebra, then the algebra $R(A)$ is of the same kind, and in this case we may apply the well developed associative PI-theory for studying A. On this path, we for example prove the following

Theorem (Shestakov, 1983). *The radical $Rad A$ of a finitely generated alternative PI-algebra A over a field is nilpotent.*

In investigating properties of free a. a., alternative superalgebras (cf. 1.2) proved to be useful; they satisfy the following classification theorem which has been proved recently (E. I. Zel'manov, I. P. Shestakov, 1990): every prime alternative superalgebra $A = A_0 \dotplus A_1$ of a characteristic $\neq 2,3$ is either associative or $A_1 = 0$ and A_0 is the Cayley-Dickson ring.

§3. Jordan Algebras

3.1. Examples of Jordan Algebras. Recall that an algebra is called a *Jordan algebra* (J. a.), if it satisfies the following identities:

$$xy = yx$$
$$(x^2 y)x = x^2(yx).$$

In this section we assume that the base field F is of characteristic not equal to 2.

Example 1. Let A be an associative algebra. Then, the algebra $A^{(+)}$ is a J. a., as noted in 1.1. Every subspace J in A, closed with respect to the operation $x \cdot y = \frac{1}{2}(xy + yx)$, forms a subalgebra of the algebra $A^{(+)}$ and is consequently a J. a. Such a J. a. J is called a *special Jordan algebra* and the subalgebra A_0 in A generated by J is called the *associative enveloping algebra* of J. Properties of the algebras A and $A^{(+)}$ are closely related: A is simple (prime, nilpotent), if and only if $A^{(+)}$ has the corresponding properties. The algebra $A^{(+)}$ may happen to be a Jordan algebra for non-associative A too. For instance, if A is a right alternative (in particular, alternative) algebra, then $A^{(+)}$ is a special J. a. (cf. 4.2).

Example 2. Let X be a vector space of dimension greater than 1 over F, with a symmetric nondegenerate bilinear form $f(x, y)$. Let us consider the direct sum of vector spaces $J(X, f) = F \dotplus X$ and let us define multiplication there in the following way:

$$(\alpha + x)(\beta + y) = (\alpha\beta + f(x, y)) + (\alpha y + \beta x).$$

Then $J(X, f)$ is a simple special J. a.; its enveloping algebra is the Clifford algebra $\mathrm{Cl}\,(X, f)$ of the bilinear form f. In case when $F = \mathbb{R}$ and $f(x, y)$ is the ordinary scalar product on X, the algebra $J(X, f)$ is called the *spin-factor* and is denoted by V_n, where $n - 1 = \dim X$.

Example 3. Let A be an associative algebra with involution $*$. The set $H(A, *) = \{h \in A \mid h^* = h\}$ of $*$-symmetric elements is closed with respect to Jordan multiplication $x \cdot y$, and therefore, is a special J. a. For instance, if D is a composition associative algebra over F, with involution $d \to \overline{d}$ (cf. 2.1) and if D_n is the algebra of $n \times n$ matrices over D, then the mapping $S : (a_{ij}) \mapsto (\overline{a_{ji}})$ is an involution in D_n and the set of the D-Hermitian matrices $H(D_n) = H(D_n, S)$ is a special J. a. If the algebra A is $*$-simple (i.e. does not contain proper ideals I, such that $I^* \subseteq I$), then $H(A, *)$ is simple; if A is $*$-prime, then $H(A, *)$ is prime. In particular, all the algebras $H(D_n)$ are simple. Every algebra of the form $A^{(+)}$ is isomorphic to the algebra $H(B, *)$, where $B = A \oplus A^0$, the algebra A^0 is anti-isomorphic to A, and $(a_1, a_2)^* = (a_2, a_1)$.

Example 4. If $D = \mathbb{O}$ is the Cayley-Dickson algebra, then the corresponding algebra $H(\mathbb{O}_n)$ of Hermitian matrices is a J. a., only for $n \leqslant 3$. In cases $n = 1, 2$, the algebras obtained in this way are isomorphic to some algebras in Example 2, and thus are special. The algebra $H(\mathbb{O}_3)$ is not special and gives us an example of a simple exceptional J. a. Albert was the first to prove that the algebra $H(\mathbb{O}_3)$ is exceptional. We will call a J. a. J the *Albert algebra*, if $J \otimes_F K \cong H(\mathbb{O}_3)$, for some extension K of the field F. Every Albert algebra is simple, exceptional and is of dimension 27 over its center.

We will see in the sequel, in 3.7 that the stated examples exhaust all the simple J. a.

3.2. Finite-Dimensional Jordan Algebras (Braun, Koecher, 1966), (Jacobson, 1968). Let J be a J. a. and let $a, b, c \in J$. Consider a the following regular birepresentation of the algebra J: $a \mapsto L_a, a \mapsto R_a$ (cf. 1.2). In view of (1. 17), we have

$$L_a = R_a, \quad [R_{a^2}, R_a] = 0,$$
$$R_{a^2b} - R_bR_{a^2} + 2R_aR_bR_a - 2R_aR_{ba} = 0. \tag{1}$$

Linearizing the last relation in a, we get the following:

$$R_{ac\cdot b} - R_bR_{ac} + R_aR_bR_c + R_cR_bR_a - R_aR_{bc} - R_cR_{ba} = 0. \tag{2}$$

It easily follows from (2) that, for every $k \geqslant 1$, the operator R_{a^k} belongs to the subalgebra $A \subseteq \operatorname{End} J$ generated by the operators R_a, R_{a^2}. In view of (1), A is commutative, thus we have $[R_{a^k}, R_{a^n}] = 0$, for all $k, n \geqslant 1$, or $(a^k, J, a^n) = 0$. In particular, every J. a. J is power-associative and the nilradical $\operatorname{Nil} J$ is uniquely defined. Just as in the case of the alternative algebras, the following theorem holds:

Theorem. *Let J be a finite-dimensional J. a. Then the radical $\operatorname{Nil} J$ is nilpotent and the quotient algebra $J/\operatorname{Nil} J$ is isomorphic to the direct sum of simple algebras.*

An important example of semisimple J. a. over $\mathbb{R}$ are so-called *formally real J. a.*, i.e. algebras where the equality $x^2 + y^2 = 0$ implies $x = y = 0$. In the foundational paper (Jordan, von Neumann, Wigner, 1934), the finite-dimensional formally real J. a. were characterized as the direct sums of simple algebras of one of the following forms: $\mathbb{R}, V_n, H(\mathbb{R}_n), H(\mathbb{C}_n), H(\mathbb{H}_n), H(\mathbb{O}_3)$, where $\mathbb{C}$ is the field of complex numbers, $\mathbb{H}$ is the quaternion skew-field and $\mathbb{O}$ is the algebra of Cayley numbers and $n \geqslant 3$. Simple finite-dimensional algebras over an algebraically closed field F are described in a similar fashion:

Theorem. *Every simple finite-dimensional J. a. over an algebraically closed field F is isomorphic either to F or to the algebra $J(X, f)$, or to the algebra of Hermitian matrices $H(D_n), n \geqslant 3$, over a composition algebra D, associative for $n > 3$.*

Recall (see 1.2) that every finite-dimensional commutative power-associative nilsemisimple algebra over a field of characteristic 0 is a Jordan algebra, thus this theorem at the same time gives a description of simple finite-dimensional commutative power-associative algebras of characteristic 0, which are not nilalgebras.

In a finite-dimensional J. a. J with the separable quotient algebra $J/\mathrm{Nil}\, J$ an analogue of the classical Wedderburn-Malcev theorem on splitting off of the radical and conjugation of semisimple factors holds.

Structure of Jordan bimodules over a J. a. J is defined by its *universal multiplicative enveloping algebra* $U(J)$, which is defined as the quotient algebra of the tensor algebra $T(J)$ over the ideal generated by the set of the elements of the forms

$$a^2 \otimes a - a \otimes a^2, a^2b - b \otimes a^2 - 2a \otimes ba + 2a \otimes b \otimes a, \text{ where } a, b \in J$$

(see 1.2). A linear mapping $\rho : J \longrightarrow \mathrm{End}\, M$ is a representation of a J. a. J (or, equivalently, the pair (ρ, ρ) is a birepresentation of J) if and only if there exists a homomorphism of associative algebras $\phi : U(J) \longrightarrow \mathrm{End}\, M$, coinciding with ρ on the elements in J, identified with its cannonical images in $U(J)$. Thus descriptions of Jordan J-bimodules reduce to determining the structure of the algebra $U(J)$ and to a study of its associative representations. A finite-dimensional J. a. J is separable if and only if $U(J)$ is separable. This implies that every Jordan bimodule over a separable finite-dimensional J. a. is completely reducible. The construction of the algebra $U(J)$ is known for all central simple finite-dimensional J. a. J. This also determines irreducible J-bimodules (they correspond to simple components of the algebra $U(J)$).

Example 1. Let J be the Albert algebra. Then $U(J) = F \oplus F_{27}$. The component F corresponds to the trivial one-dimensional J-bimodule, and F_{27} to a regular J-bimodule. Since we usually do not consider trivial bimodules to be irreducible, every irreducible J-bimodule is isomorphic to a regular bimodule.

Example 2. $J = J(X, f)$. Then $U(J) = F \oplus \mathrm{Cl}\,(X, f) \oplus D(X, f)$, where $D(X, f)$, is the so-called "meson algebra", defined as the quotient algebra $T(X)/I$, where $T(X)$ is the tensor algebra of the space X and I is the ideal in $T(X)$ generated by all the elements of the form $x \otimes y \otimes x - f(x, y)x$, where $x, y \in X$. One can show that $D(X, f)$ is isomorphic to the subalgebra of the algebra $\mathrm{Cl}\,(X, f) \otimes \mathrm{Cl}\,(X, f)$, generated by elements of the form $x \otimes 1 + 1 \otimes x$, $x \in J$. We will not give the decomposition of $D(X, f)$ into simple components, since it is fairly complicated: it depends on the parity of the dimension of X and the discriminant of the form f.

3.3. Derivations of Jordan Algebras and Relations with Lie Algebras (Braun, Koecher, 1966; Schafer, 1966; Jacobson, 1966). With every J. a. J one can associate several interesting Lie algebras. We already know some of them: It is the derivation algebra Der J, the Lie multiplication algebra Lie (J) and the algebra of inner derivations Inder J = Der $J \cap$ Lie (J). We introduce two more algebras below: the structure algebra Strl J and the superstructure algebra (or the Tits-Kantor-Koecher construction) $K(J)$.

Let J be a J. a. with unity 1 and $a, b, c \in J$. By skewsymmetrizing (2) in a and b we get the following:

$$R_{(a,c,b)} = [R_c, [R_a, R_b]]. \tag{3}$$

Since $(a, c, b) = c[R_a, R_b]$, then, in view of (1. 11), (3) implies that the operator $[R_a, R_b]$ is a derivation of the algebra J. Moreover, (3) implies that $\mathrm{Lie}\,(J) = R_J + [R_J, R_J]$, where $R_J = \{R_a \mid a \in J\}$. Since $\mathrm{Der}\, J \cap R_J = 0$ (if $R_a \in \mathrm{Der}\, J$, then $0 = 1R_a = a$), we have $\mathrm{Inder}\, J = \mathrm{Der}\, J \cap \mathrm{Lie}\,(J) = \mathrm{Der}\, J \cap (R_J + [R_J, R_J]) = (\mathrm{Der}\, J \cap R_J) + [R_J, R_J] = [R_J, R_J]$, i.e. every inner derivation in J is of the form $D = \sum_i [R_{a_i}, R_{b_i}]$, $a_i b_i \in J$. At the same time, it has been proved that $\mathrm{Lie}\,(J) = R_J \dotplus \mathrm{Inder}\, J$ is the direct sum of vector spaces with multiplication

$$[R_a + D, R_b + D'] = R_{aD' - bD} + ([R_a, R_b] + [D, D']), \tag{4}$$

where $a, b \in J; D, D' \in \mathrm{Inder}\, J$. If D and D' in (4) are taken from the algebra Der J, then this formula will define multiplication on the vector space $R_J \dotplus \mathrm{Der}\, J$. The resulting algebra is again a Lie algebra, called the *structure algebra* of the algebra J and is denoted by Strl J.

Theorem. *Let J be a finite-dimensional semisimple J. a. over a field of characteristic 0. Then Der J = Inder J is a completely reducible Lie algebra. If J does not contain simple summands of dimension 3 over the center, then the algebra Der J is semisimple.*

The stated restriction is essential since Der V_3 is an one-dimensional Lie algebra. For the central simple J. a. J the algebra Der J is simple with the exception of the algebra $J(X, f)$, $\dim X = 2, 3, 5$, and the algebra $H(F_4)$. If $J = H(D_n)$, where $n \geqslant 3$ and if D is a composition algebra of dimension d over F, then the dimension of the algebra Der J is given by the following table:

d	1	2	4	8
dim(Der J)	$\frac{n(n-1)}{2}$	$n^2 - 1$	$n(2n+1)$	52 ($n = 3$)

In particular, the algebra Der $(H(\mathbb{O}_3))$ is a simple 52-dimensional Lie algebra. According to the classification of finite-dimensional simple Lie algebras, over an algebraically closed field K of characteristic 0, only one of them has dimension 52, namely the exceptional algebra $\mathbb{F}_4$. Thus, over the field K, we have $\mathbb{F}_4 = \mathrm{Der}\,(H(\mathbb{O}_3))$. For every Albert algebra J, the algebra Der J is an algebra of type $\mathbb{F}_4$ and, conversely, every Lie algebra of type $\mathbb{F}_4$ is isomorphic to the algebra $\operatorname{Der} J$, for a suitable Albert algebra J; furthermore, $\operatorname{Der} J \cong \operatorname{Der} J_1$, if and only if $J \cong J_1$.

For a semisimple J. a. J, the structure algebra $\operatorname{Strl} J$ is not semisimple since its center contains the element $R_1 = \operatorname{Id}_J$, where 1 is the unity of J. Let $J_0 = \{x \in J \mid \operatorname{tr}(R_x) = 0\}$; then $J = F \cdot 1 + J_0$ and $\operatorname{Strl} J = F \cdot R_1 \dotplus R_{J_0} \dotplus \operatorname{Der} J$. It is easy to see that $(\operatorname{Strl} J)' = R_{J_0} \dotplus \operatorname{Der} J$. The subalgebra $\operatorname{Strl}_0 J = R_{J_0} \dotplus \operatorname{Der} J$ of codimension 1 in $\operatorname{Strl} J$ is called the *reduced structure algebra* of the algebra J.

Theorem. *Let J be a central simple J. a. of finite dimension $n > 1$, over a field of characteristic 0. Then $\operatorname{Strl}_0 J$ is a semisimple Lie algebra.*

If $J = H(D_n)$, where $n \geqslant 3$ and D is a composition algebra of dimension d over F, then the algebra $\operatorname{Strl}_0 J$ is simple for $d = 1, 4, 8$, and for $d = 2$ it is the direct sum of two isomorphic simple algebras.

Example. The algebra $\operatorname{Strl}_0(H(\mathbb{O}_3))$ is a simple Lie algebra of dimension (27-1)+52=78 and it acts irreducibly on $H(\mathbb{O}_3)$. There are three non-isomorphic simple Lie algebras of dimension 78, over an algebraically closed field K of characteristic 0: the algebra $\mathbb{E}_6$, the orthogonal Lie algebra $o(13)$ and the simplectic Lie algebra $\operatorname{sp}(12)$. However, the two latter algebras do not have irreducible representations of dimension 27. Thus, over the field K, we have $\mathbb{E}_6 = \operatorname{Strl}_0(H(\mathbb{O}_3))$. If now J is an arbitrary Albert's algebra, then the algebra $\operatorname{Strl}_0 J$ is a simple Lie algebra of type $\mathbb{E}_6$; in addition, the algebras $\operatorname{Strl}_0 J$ and $\operatorname{Strl}_0 J_1$, for Albert's algebras J and J_1, are isomorphic if and only if J and J_1 are isotopic (cf. 3.4 in the sequel).

We need a notion of the *triple Jordan product*, which plays an important role in the theory of J. a., in order to define the superstructure algebra $K(J)$. Let $a, b, c \in J$; set $\{abc\} = (a \cdot b) \cdot c + (c \cdot b) \cdot a - b \cdot (a \cdot c)$. Let us also define the linear operators $U_{a,b} : x \mapsto \{axb\}, V_{a,b} : x \mapsto \{abx\}, U_a = U_{a,a}$. If $J = A^{(+)}$, where A is an associative algebra with multiplication ab, then $\{aba\} = aba$. There are many arguments showing that the ternary operation $\{abc\}$ is more natural for J. a., then the ordinary multiplication. We will return later to properties of this operation. Let us point out now only that, if J has the unity, then the ordinary multiplication is expressible through the ternary by $V_{1,a} = R_a$.

Let us again consider the structure algebra $\operatorname{Strl} J = R_J \dotplus \operatorname{Der} J$. We define a mapping $*$ of the algebra $\operatorname{Strl} J$ into itself, by setting $(R_a + D)^* = -R_a + D$. It is easy to see that $*$ is an automorphism of order 2 of the algebra $\operatorname{Strl} J$. We form the vector space $K(J) = J \dotplus \operatorname{Strl} J \dotplus \overline{J}$, where $\overline{J}$ is isomorphic to J under the isomorphism $a \mapsto \overline{a}$. Let us now define multiplication on $K(J)$, by setting

$$[a_1 + T_1 + \overline{b_1}, a_2 + T_2 + \overline{b_2}] = (a_1 T_2 - a_2 T_1) + (V_{a_1,b_2} - V_{a_2,b_1} + [T_1, T_2]) + (\overline{b_1 T_2^*} - \overline{b_2 T_1^*}).$$

The resulting algebra $K(J)$ is a Lie algebra, called the ***superstructure algebra*** or the *Tits-Kantor-Koecher construction* for the algebra J.

The correspondence $J \mapsto K(J)$ is functorial and there is a close relation between the properties of the algebras J and $K(J)$. The algebra J is simple (semisimple, solvable), if and only if $K(J)$ is of the same kind.

The algebra $K(J)$ has a less formal interpretation too. Let $\mathrm{Pol}\,(J)$ be the vector space of the polynomial transformations J into J. It is known that $\mathrm{Pol}\,(J)$ forms a Lie algebra with respect to the brackets

$$[p,q](x) \equiv \frac{\partial p(x)}{\partial x} q(x) - \frac{\partial q(x)}{\partial x} p(x),$$

the so-called "Lie algebra of polynomial vector fields on J". It is not difficult to ascertain that $K(J)$ is isomorphic to the subalgebra of the algebra $\mathrm{Pol}\,(J)$, which consists of quadratic polynomials of the form $a + Tx + \{xbx\}$, where $a, b \in J, T \in \mathrm{Strl}\, J$.

Example 1. Let $J = \mathbb{R}$. Then $K(\mathbb{R})$ consists of the polynomials of the form $p(x) = p_1 + p_2 x + p_3 x^2$, where $p_i \in \mathbb{R}$; furthermore

$$[p,q](x) = p'(x)q(x) - q'(x)p(x) =$$
$$(p_2 q_1 - q_2 p_1) + 2(p_3 q_1 - q_3 p_1)x + (p_3 q_2 - q_3 p_2)x^2.$$

Thus, $K(\mathbb{R}) \cong \mathrm{sl}\,(2, \mathbb{R})$.

Example 2. Let J be the Albert algebra. Then $K(J)$ is a simple Lie algebra of dimension 27+79+27=133, i.e. $K(J)$ is an algebra of type $\mathbb{E}_7$.

The Tits-Kantor-Koecher construction results in fact not only in one Lie algebra, but the whole series. Namely, let H be an arbitrary subalgebra of the algebra $\mathrm{Strl}\, J$ which contains the subalgebra $R_J \dot{+} \mathrm{Inder}\, J$; then the vector space $K_H(J) = J \dot{+} H \dot{+} \overline{J}$ is a subalgebra of $K(J)$. All the algebras $K_H(J)$ are 3-graduated, i.e. are of the form $L = L_{-1} \dot{+} L_0 \dot{+} L_1$, where $L_i L_j \subseteq L_{i+j}, L_i = 0$, for $|i| > 1$; in addition $L_{-1} = J, L_1 = J, L_0 = H$.

In the conclusion of this part we give the *Tits construction* which brings about exceptional simple Lie algebras of every type, with the aid of the composition algebras and Jordan matrix algebras of order 3.

Let F be a field of characteristic $\neq 2, \neq 3$ and let A be a composition algebra over F; J is either F or is the algebra $H(D_3)$, where D is the composition algebra over F. Let us denote by $t(a)$ the trace of the element a in the algebra A and by $\mathrm{tr}\,(x)$ denote the ordinary trace of the matrix x in the algebra $H(D_3)$. Let $A_0 = \{a \in A \mid t(a) = 0\}$, $J_0 = \{x \in J \mid \mathrm{tr}\,(x) = 0\}$ ($J_0 = 0$, for $J = F$). For $a, b \in A$ and $x, y \in J$, set

$$a * b = ab - \frac{1}{2} t(ab), \quad x * y = xy - \frac{1}{3} \mathrm{tr}\,(xy);$$

then $a * b \in A_0, x * y \in J_0$. Let us define an anticommutative multiplication on the direct sum of vector spaces $\mathrm{Der}\, A \dot{+} A_0 \otimes J_0 \dot{+} \mathrm{Der}\, J$, according to the following rules:

1) $\operatorname{Der} A$ and $\operatorname{Der} J$ are commuting subalgebras in L;

2) $[a\otimes x, D] = aD\otimes x, [a\otimes x, E] = a\otimes xE$, for all $D \in \operatorname{Der} A, E \in \operatorname{Der} J, a \in A_0, x \in J_0$;

3) $[a \otimes x, b \otimes y] = \frac{1}{12}\operatorname{tr}(xy)D_{a,b} + (a * b) \otimes (x * y) + \frac{1}{2}t(ab)[R_x, R_y]$, for all $a, b \in A_0, x, y \in J_0$, where $D_{a,b} \in \operatorname{Der} A$ is of the form (2.19).

The resulting algebra L is a Lie algebra. For brevity, we denote $\mathbb{C}(\alpha) = \mathbb{C}, \mathbb{H}(\alpha, \beta) = \mathbb{H}$; then the type of the algebra L depending on the form of the algebras A and J is determined by the following table:

$A \backslash J$	F	$H(F_3)$	$H(\mathbb{C}_3)$	$H(\mathbb{H}_3)$	$H(\mathbb{O}_3)$
$\mathbb{F}$	0	A_1	A_2	C_3	F_4
$\mathbb{C}$	0	A_2	$A_2 \oplus A_2$	A_5	E_6
$\mathbb{H}$	A_1	C_3	A_5	A_6	E_7
$\mathbb{O}$	G_2	F_4	E_6	E_7	E_8

For instance, if $A = \mathbb{O}, J = H(\mathbb{O}_3)$, then the algebra $L = \operatorname{Der} A \dotplus A_0 \otimes J_0 \dotplus \operatorname{Der} J$ is of dimension 14+7·26+52=248 and is a simple Lie algebra of type $\mathbb{E}_8$.

3.4. Isotopies of Jordan Algebras, Jordan Structures (Braun, Koecher, 1966; Jacobson, 1968; Meyberg, 1972; Springer, 1973; Loos, 1975). An element a in a J. a. J with unity 1 is called *invertible*, if the operator $U_a = 2R_a^2 - R_{a^2}$ is invertible in $\operatorname{End} J$. It is easy to see that a is invertible if and only if 1 is in the image of U_a. Set $a^{-1} = aU_a^{-1}$; then a^{-1} is also invertible and $(a^{-1})^{-1} = a$. If A is an associative algebra, then a is invertible in A if and only if it is invertible in $A^{(+)}$ and a^{-1} is same in A and in $A^{(+)}$. If every element in a J. a. J is invertible, then J is called a *division* J. a. We point out that the invertibility of an element a in a J. a., does not, generally speaking imply invertibility of the operator R_a, thus the equations $ax = b$ $(a \neq 0)$ are not necessarily solvable in a division J. a.

The notion of isotopy, whose sources lie in the associative theory, plays an important role in the theory of J. a. If an invertible element c is fixed in an associative algebra A, and if a new c-multiplication $a_c b = ac^{-1}b$ is defined, then the resulting algebra $A^{(c)}$ will again be associative, where the element c will be the unity in $A^{(c)}$. Analogously, for a J. a. J with an invertible element c, the algebra $J^{(c)}$ obtained from J by introduction of a c-multiplication $a_c \cdot b = \{ac^{-1}b\}$, will be a J. a. with the unity c. The algebra $J^{(c)}$ is called the *c-isotope* of the algebra J. Two J. a. are called *isotopic*, if one of them is isomorphic to an isotope of the other; the corresponding isomorphism is called an *isotopy*. In the associative case, the algebras A and $A^{(c)}$ are always isomorphic: the mapping $x \mapsto xc$ is an isomorphism of A and $A^{(c)}$, thus the notion of isotopy does not play a special role here. In the Jordan case, the situation is different: the algebra $J^{(c)}$ may be non-isomorphic to J. For instance, the algebra $J = H(\mathbb{R}_2)$ does not contain nilpotent elements, while its isotope $J^{(c)}$, for $c = e_{12}+e_{21}$ contains the nilpotent element e_{11}: $e_{11}\cdot e_{11} = e_{11}(e_{12}+e_{21})^{-1}e_{11} = 0$. Nevertheless, many important properties of J. a., such as the properties of being simple or special, are invariant with respect to isotopy; isotopic J. a have isomorphic structure and superstructure Lie algebras.

An isotopy of a J. a. J with itself is called an *autotopy* (in other words, an autotopy is an isomorphism of an algebra with its isotop). The family of all the autotopies of J. a. J form a group, which is called the *structure group* of the algebra J and is denoted by $\operatorname{Str} J$. The group $\operatorname{Str} J$ is an algebraic group and its Lie algebra is the structure algebra $\operatorname{Strl} J$. The automorphisms of J are autotopies which fix the unity 1 of the algebra J. More generally, two isotopes $J^{(a)}$ and $J^{(b)}$ are isomorphic if and only if there is an autotopy carrying a to b.

A series of important theorems in the theory of J. a. hold "up to an isotopy", i.e. their conclusions do not apply to the algebras in question, but only to some of their isotopies. In this respect the group $\operatorname{Str} J$ often turns out to be more useful than the automorphism group $\operatorname{Aut} J$. For instance, there is no natural notion of an inner automorphism for a J. a., while at the same time, for every invertible $a \in J$, the operator U_a is an "inner autotopy" from J to $J^{(a^2)}$. All this suggests a thought about the existence of some algebraic object which unifies the J. a. J and all its isotopies and which has the group $\operatorname{Str} J$ as its automorphism group. Such an object exists indeed and it is the Jordan pair (J, J).

The *Jordan pair* (J. p.) over a field F of characteristic $\neq 2, \neq 3$ is the pair $V = (V^+, V^-)$ of vector spaces, with two trilinear mappings $V^\sigma \times V^{-\sigma} \times V^\sigma \mapsto V^\sigma, \sigma = \pm$, written as $(x, y, z) \mapsto \{xyz\}$ and which satisfying the following identities

$$\{xyz\} = \{zyx\}, \tag{5}$$

$$\{xy\{uvz\}\} - \{uv\{xyz\}\} = \{\{xyu\}vz\} - \{u\{yxv\}z\}. \tag{6}$$

Examples of J. p.:

Example 1. $V(J) = (J, J)$, where J is a J. a. and $\{xyz\}$ is the triple Jordan product in J. For this J. p., $\operatorname{Aut} V(J) \cong \operatorname{Str} J$. If $V = (V^+, V^-)$ is an arbitrary J. p., then for every $a \in V^\sigma$, the space $V^{-\sigma}$, with the multiplication operation $x_a\cdot y = \{xay\}$ is a J. a. J_a. If, in addition, the element a is invertible, then $V \cong V(J_a)$. Thus the (unital) J. a. may be seen, "up to an isotopy", to be a J. p. with invertible elements.

Example 2. A vector space T with a trilinear operation $\{xyz\}$, satisfying (5) and (6), is called a *Jordan triple system* (J. t. s.). For instance, every J. a. is a J. t. s. with respect to the triple Jordan product; the rectangular $p\times q$ matrices $M_{p,q}(F)$ form a J. t. s. with respect to the operation $\{xyx\} = xy^tx$ (in view of (5), the trilinear operation $\{xyz\}$ in J. p. and J. t. s. is obtained by linearization of the quadratic operation $\{xyx\}$, thus it suffices to give the latter). With every J. t. s. T, one can relate in a natural way the J. p. $V(T) = (T,T)$. Not every J. p. is obtainable in this fashion, since there exist J. p. for which $\dim V^+ \neq \dim V^-$. The pair $V(T)$ has the involution $(t_1, t_2) \mapsto (t_2, t_1)$; conversely, every J. p. with involution is of the form $V(T)$, for an appropriate J. t. s. T. Thus J. t. s. may be viewed as a J. p. with involution.

Example 3. $V = (M_{p,q}(F), M_{q,p}(F)), \{xyx\} = xyx$. It is easy to see that $V \cong V(T)$, for the J. t. s. $T = M_{p,q}(F)$ from Example 2.

Example 4. $V(R) = (R_{-1}, R_1)$, where $R = R_{-1} \dotplus R_0 \dotplus R_1$ is an associative 3-graded algebra ($R_i R_j \subseteq R_{i+j}$, $R_i = 0$, for $|i| > 1$); $\{xyx\} = xyx$. If, in addition, R is a simple algebra and $R_{-1} + R_1 \neq 0$, then $V(R)$ is a simple J. p.

Example 5. $V(L) = (L_{-1}, L_1)$, where $L = L_{-1} \dotplus L_0 \dotplus L_1$ is a 3-graded Lie algebra; $\{xyz\} = [[x,y],z]$. An example of such a Lie algebra is the superstructure algebra $L = K(J)$, for a J. a. J; furthermore $V(L) \cong V(J)$. If L_0 acts faithfully on $L_{-1} + L_1$, then we may assume that $\operatorname{Inder} V(L) \subseteq L_0 \subseteq \operatorname{Der} V(L)$. The algebra L will be called faithful in this case. A subalgebra H of derivations of a J. p. V will be called large, if $\operatorname{Inder} V \subseteq H$.

The Tits-Kantor-Koecher construction has a generalization to J. p., by assigning, to every J. p. $V = (V^+, V^-)$ with a large subalgebra of derivations H, the faithful 3-graded Lie algebra $K_H(V) = V^- \dotplus H \dotplus V^+$; furthermore, there is a bijective correspondence between faithful 3-graded Lie algebras and J. p. with fixed large derivation subalgebras.

The simple Lie algebras $A_n, B_n, C_n, D_n, E_6, E_7$ have a non-trivial faithful 3-grading, thus they allow construction and study with the aid of J. p. The algebras G_2, F_4, E_8 do not have such a grading, but have a grading of the form $L = L_{-2} \dotplus L_{-1} \dotplus L_0 \dotplus L_1 \dotplus L_2$. Jordan methods are effectively applicable in studying these algebras, as well as the Lie algebras with an arbitrary finite $\mathbb{Z}$-grading (Kantor, 1974; Allison, 1976, 1978; Zel'manov, 1984).

Another important kind of Jordan structures has been studied in recent times, namely *Jordan superalgebras* (cf. 1.2). Just as in the case of ordinary algebras, there is a close tie between Jordan and Lie superalgebras; in particular, the Tits-Kantor-Koecher construction generalizes to Jordan superalgebras. With help of this connection, on the basis of a known classification of simple finite-dimensional Lie superalgebras over an algebraically closed field of characteristic 0, a classification of simple Jordan superalgebras with the same conditions had been obtained in (Kac, 1977). I. L. Kantor and E. I. Zel'manov have pointed out recently that the classification given in (Kac, 1977) has a gap: a series of simple Jordan superalgebras, connected with gradings of Hamiltonian Lie superalgebras has been omitted.

A typical example of a Jordan superalgebra is the algebra $A^{(+)s}$, obtained by introducing *Jordan supermultiplication* $x \cdot^s y = \frac{1}{2}(xy + (-1)^{ij} yx)$, $x \in A_i, y \in A_j$, on the vector space of the associative superalgebra $A = A_0 \dotplus A_1$. The superalgebra J is called special if it is embeddable in a suitable algebra

$A^{(+)s}$. For instance, if A has a superinvolution $*$ (i.e. $A_i^* \subseteq A_i$ and $(xy)^* = (-1)^{ij}y^*x^*$, for $x \in A_i, y \in A_j$), then the set of supersymmetric elements $H(A, *) = \{x \in A \mid x^* = x\}$ forms a subalgebra in $A^{(+)s}$. If $X = X_0 \dotplus X_1$ is a vector space with a supersymmetric bilinear form f (f is symmetric on X_0 and skewsymmetric on X_1, $f(X_i, X_j) = 0$, for $i \neq j$), then the algebra of the bilinear form $J(X, f) = F \dotplus X$ is a Jordan superalgebra with $J_0 = F + X_0, J_1 = X_1$. For every $\mathbb{Z}_2$-graded J. a. $J = J_0 + J_1$, its Grassmann envelope $G(J) = G_0 \otimes J_0 + G_1 \otimes J_1$ is a Jordan superalgebra.

An important class of Jordan superalgebras is connected with the algebras of Poison brackets. Let A be an associative and commutative algebra with a skew symmetric bilinear operation $\{x, y\}$ (Poison brackets), such that A is a Lie algebra under this operation and such that, for every $a \in A$, the mapping $x \to \{a, x\}$ is a derivation of the algebra A. Then the superalgebra $J = J_0 \dotplus J_1$, where $J_0 = J_1 = A$ with the multiplication

$$(a_0 + b_1)(c_0 + d_1) = (ac + \{b, d\})_0 + (ad + bc)_1, \text{where } a, b, c, d \in A,$$

is a Jordan superalgebra. This construction has a generalization to the case when A is a commutative superalgebra.

There are two more types of Jordan structures that we have not mentioned. These are the *quadratic J. a.* (q. J. a.) and so-called *J-structures*. In the definition of a q. J. a., the bilinear operation of multiplication $x \cdot y$ is substituted by the quadratic operation $yU_x = \{xyx\}$, with the following axioms:

1) $U_1 = \mathrm{Id}$,
2) $U_x V_{y,x} = V_{x,y} U_x$,
3) $U_{yU_x} = U_x U_y U_x$,

where $zV_{x,y} \equiv \{zyx\} \equiv y(U_{x+z} - U_x - U_z)$. The advantage of the q. J. a. is in the fact that they cover the case of characteristic 2; in the case of characteristic $\neq 2$, they are equivalent to ordinary J. a. At present, almost all the fundamental theorems of J. a. have been carried over to q. J. a (McCrimmon, 1966; Jacobson, 1981; Zelmanov, McCrimmon, 1988)

The notion of a J-structure is based on the operation of inversion $x \mapsto x^{-1}$. The Hua identity $\{xyx\} = x - (x^{-1} - (x - y^{-1})^{-1})^{-1}$, which holds for any elements of an arbitrary J. a., for which the right-hand-side is defined, shows that, if a J. a. has "many" invertible elements, then the operation of inversion contains all the information about the algebra. In particular, this is so in the finite-dimensional case. A finite-dimensional space V, with a fixed element 1 and a birational mapping $x \mapsto x^{-1}$ is called a *J-structure* if 1) $1^{-1} = 1, (x^{-1})^{-1} = x, (\lambda x)^{-1} = \lambda^{-1}x^{-1}$, for $\lambda \in F$; 2) $(1+x)^{-1} + (1+x^{-1})^{-1} = 1$; 3) the orbit of 1, under the action of the structure group $G = \{g \in \mathrm{GL}(V) \mid (xg)^{-1} = (x^{-1})h$, for some $h \in \mathrm{GL}(V)\}$ is a Zariski open set in V. Over the fields of characteristic $\neq 2$, the J-structures are categorically equivalent to finite-dimensional J. a. with unity. This approach was used in (Springer, 1973), for a classification of simple finite-dimensional J. a., on the basis of the Cartan-Shevalley theory of semisimple linear algebraic groups.

3.5. Jordan Algebras in Projective Geometry. We have established in 2.2 that every Moufang plane may be coordinatized by a Cayley-Dickson skew-field, uniquely determined up to isomorphism. This coordinatization is still insufficient for describing isomorphisms (collineations) of Moufang planes in algebraic language – in the spirit of "geometric algebra". The latter is achievable with the aid of representations of Moufang planes in simple exceptional J. a.

Let $J = (H(D_3))^{(\gamma)}$, where D is the Cayley-Dickson skew-field and γ is an invertible diagonal element in J. Let us denote by P the set of all the elements of "rank 1" in J: $P = \{0 \neq x \in J \mid JU_x = Fx\}$. If $a \in P$, then either $a^2 = 0$, or $a = \alpha e$, where e is a primitive idempotent. Let $[a] = aF^*$ be the "ray" spanned over the element a. Denote by a^* and a_* two samples of the set $[a]$. We define the plane $\pi(J)$ with the set of points $\pi_0 = \{a_* \mid a \in P\}$ and the set of lines $\pi^0 = \{a^* \mid a \in P\}$, regarding a_* to be incident to b^*, if $\operatorname{tr}(ab) = 0$, where $\operatorname{tr}(x)$ is the trace of the matrix x. Then $\pi(J)$ is a projective Moufang plane, coordinatized by the skew-field D.

Fundamental theorem of projective geometry for Moufang planes $\pi(J)$ (Jacobson, 1968; Faulkner, 1970). *Every collineation of the projective Moufang plane $\pi(J)$ is induced by a semilinear autotopy of the algebra J, defined uniquely up to some factors in F^*. The planes $\pi(J)$ and $\pi(J_1)$ are isomorphic if and only if J and J_1 are isotopic (as rings).*

Another interesting application of J. a. in projective geometry concerns so-called Moufang polygonal geometries, where J. a. arise as the coordinatizing algebras (Faulkner, 1977).

3.6. Jordan Algebras in Analysis. J. a. have various and deep applications in differential geometry, in real, complex and functional analysis, in theory of automorphic functions (Koecher, 1962, 1971; Loos, 1969; McCrimmon, 1978; Iordanesku, 1979; Hanche-Olsen, Stormer, 1984; Ayupov, 1985; Upmeier, 1985). The essence of the majority of them is in close relations among formally real J. a., self-dual convex cones and the Hermitian symmetric spaces.

An analytic Riemannian manifold M is called a *Riemannian symmetric space*, if every point $p \in M$ is an isolated fixed point of some involutive isometry (a geodesic symmetry with respect to p). Important examples of such spaces are *self-dual convex cones*, i.e. open subsets Y of an Euclidean space X such that: 1) $(x, y) > 0$, for every $x, y \in Y$; 2) if $(x, y) > 0$, for all $0 \neq y \in \overline{Y}$, then $x \in Y$. Let $\operatorname{Aut} Y = \{A \in \mathrm{GL}(X) \mid A(Y) = Y\}$; the cone Y is called homogeneous, if the group $\operatorname{Aut} Y$ acts transitively on it. It is not difficult to see that, for every formally real J. a. J, the set $C(J) = \{x^2 \mid$

$0 \neq x \in J\} = \{\exp x \mid x \in J\}$ is a homogeneous self-dual convex cone (with respect to the form $(x, y) = \operatorname{tr} R_{xy}$). Conversely, the following holds:

Theorem (Vinberg, 1965; Iochum, 1984; Koecher, 1962). *Every homogeneous self-dual convex cone Y is of the form $Y = C(J)$, for some formally real J. a. J.*

Geometric structure of the cone $C(J)$ is quite compatible with the algebraic structure of J: the geodesic symmetry at a point p is the operation of inversion in the isotope $J^{(p)}$; the coefficients $\Gamma^k_{ij}(p)$ of affine connectedness coincide with the structural constants γ^k_{ij} of the algebra $J^{(p)}$. If J is simple, then $\operatorname{Str} J = \{\pm A \mid A \in \operatorname{Aut} C(J)\}$.

A complex analogue of a Riemann symmetric space is a *Hermitian symmetric space*, defined as a real Riemann symmetric space with complex structure, invariant with respect to geodesic symmetry. Examples of Hermitian symmetric spaces are *bounded symmetric domains*, i.e. bounded domains in $\mathbb{C}^n$ such that their every point is isolated fixed point of some involutive automorphism. A metric, the so-called Bergman metric, may be introduced in every such a domain, and the following theorem holds:

Theorem (Helgason, 1962; Loos, 1969). *A bounded symmetric domain with Bergman metric is a Hermitian symmetric space of a non-compact type. Conversely, every Hermitian symmetric space of a non-compact type is isomorphic to a bounded symmetric domain.*

The simplest examples of a Hermitian symmetric space of non-compact type and a bounded symmetric domain are respectively the upper half-plane and the unit disc in $\mathbb{C}$. An isomorphism between them is realized through the Cayley transformation $z \mapsto \frac{z-i}{z+i}$. Let now J be a formal real J. a. and let $C(J)$ be its related convex cone. Consider the set $H(J) = \{x + iy \mid x \in J, y \in C(J)\}$ in the complexification J_C of the algebra J and call it the half-space associated with the algebra J.

Theorem (Koecher, 1962). *The half-space $H = H(J)$ is a Hermitian symmetric space of a non-compact type, and the mapping $\phi : z \mapsto (z - i \cdot 1)(z + i \cdot 1)^{-1}$ defines an isomorphism of H with the bounded symmetric domain $D = \phi(H) = \{z \in J_C \mid 1 - z\bar{z} \in C(J)\}$.*

Example 1. $J = \mathbb{R}$, H is the upper half-plane and D – the unit disc.

Example 2. $J = H(\mathbb{R}_n)$, $H = \{A + iB \mid A, B \in J$ and B is positive definite$\}$ is the Siegel generalized upper half-plane (Helgason, 1962) and $D = \{z \in J_C \mid 1 - z\bar{z} \in C(J)\}$ is a generalized unit disc.

The geometry of the half-space $H(J)$ is described well in Jordan terms: for instance, the group $\operatorname{Aut}(H(J))$ consists of linear-fractional transformations, generated by the inversion $z \mapsto -z^{-1}$, by the translations $z \mapsto z + a$, $a \in J$, and the transformations in $\operatorname{Aut} C(J)$.

The bounded symmetric domains allow for another reduction to "nicer" objects – to so-called *bounded homogeneous circular domains*. These are defined as homogeneous bounded domains in $\mathbb{C}^n$ which contain the origin, and for which the transformation $x \mapsto e^{it}x$ is an automorphism for every $t \in \mathbb{R}$. These domains are symmetric: at the origin, the symmetry is given by the automorphism $x \mapsto -x = e^{i\pi}x$, and the symmetry exists in other points because of homogeneity. Examples of such domains are the domains $D = \phi(H)$, for the half-planes H considered above.

Theorem (Koecher, 1969; Upmeier, 1985). *Every bounded symmetric domain is biholomorphically equivalent to a bounded homogeneous circular domain.*

The circular domains of the stated form are in turn categorically equivalent to the *Hermitian Jordan triple systems*, i.e. to the real J. t. s. with a complex structure such that the triple product $\{xyz\}$ is $\mathbb{C}$-linear in x, z and is $\mathbb{C}$-antilinear in y, and the bilinear form $\langle x, y\rangle = \operatorname{tr} V_{x,y}$ is Hermitian and positive definite.

Theorem (Koecher, 1969; Upmeier, 1985). *There is a bijective correspondence between bounded homogeneous circular domains and the Hermitian J. t. s. If D is a domain with Bergman kernel $K(z,w)$, then the operation of multiplication in the J. t. s. $J = J(D)$ is defined by the following equality:*

$$\{uvw\} = \sum c_{ijkl} u_i \overline{v_j} w_k \overrightarrow{e_l}, \text{ where } c_{ijkl} = \frac{\partial^4 \ln K(z,z)}{\partial z_i \partial \overline{z_j} \partial z_k \partial \overline{z_l}}\Big|_{z=0}.$$

Conversely, for a given J. t. s J, the domain is obtained as follows:

$$D(J) = \{x \in J \mid 2Id - V_{x,x} > 0\}.$$

Relation between the geometric and the algebraic structures can be seen in further results: the Bergman kernel is

$$K(z,w) = \frac{1}{\mu(D)} \cdot \det{}^{-1}(\mathrm{Id} - 2V_{x,y} + U_x U_y);$$

the Bergman metric at the origin is $\langle u, v\rangle = \operatorname{tr} V_{u,v}$; the Shilov boundary of the closure $\overline{D}$ coincides with the set of maximal idempotents of J; a decomposition of J into the direct sum of simple J. t. s. corresponds to a decomposition of D into irreducible domains. We may easily get a classification of irreducible domains by using the description of simple Hermitian J. t. s.

The aforementioned approach is also successfully applicable in studying infinite-dimensional (Banach) symmetric domains (Kaup, 1981; Upmeier, 1985), where the role of formal real J. a. is played by the so-called *JB*-algebras, defined as real J. a. with complete norm which satisfy the following conditions: 1) $\|ab\| \leqslant \|a\| \cdot \|b\|$, 2) $\|a^2\| = \|a\|^2$, 3) $\|a^2\| \leqslant \|a^2 + b^2\|$. Finite-dimensional JB-algebras are exactly the formal real J. a. Examples of infinite-dimensional JB-algebras are the algebra $B(H)_{sa}$ of selfadjoint bounded operators in a Hilbert space H (with Jordan multiplication) and the algebra $C(S, H(\mathbb{O}_3))$ of all the continuous functions on a compact S, with values in $H(\mathbb{O}_3)$, where $\mathbb{O}$ is the algebra of Cayley numbers. These examples are fairly general, as is seen in the following theorem, which is analogous to a Gel'fand-Najmark theorem for C^*-algebras:

Theorem (Alfsen, Shultz, Stormer, 1978). *For every JB-algebra J, there exist a complex Hilbert space H and a compact topological space S, such that J is isometrically isomorphic to a closed subalgebra of the algebra $B(H)_{sa} \oplus C(S, H(\mathbb{O}_3))$.*

3.7. Structure of Infinite-Dimensional Jordan Algebras. The basic notions of the modern structure theory of J. a. are that of an absolute zero divisor, a non-degenerate algebra and a non-degenerate radical.

An element $a \neq 0$ of a J. a. J is called an *absolute zero divisor*, if $JU_a = 0$; if the algebra J does not contain absolute zero divisors, then it is called a *non-degenerate algebra*. The smallest ideal I of an algebra J such that the quotient algebra J/I is non-degenerate is called the *non-degenerate radical* of the algebra J. We will denote it by $\operatorname{rad} J$.

Example 1. Let $J = A^{(+)}$, where A is associative. Then the absolute zero divisors in $A^{(+)}$ are elements a such that $aAa = 0$; $A^{(+)}$ is non-degenerate if and only if A is semiprime; $\operatorname{rad} A^{(+)}$ coincides with prime radical of the algebra A.

Example 2. Let J be a finite-dimensional J. a. Then $\operatorname{rad} J = \operatorname{Nil} J$ is the greatest nilpotent ideal in J (cf. 3.2) and J is non-degenerate if and only if it is semisimple.

Every non-degenerate J. a. is isomorphic to a subdirect sum of prime non-degenerate algebras. The structure of the latter is described in

Theorem (Zel'manov, 1983a). *A J. a. J is prime non-degenerate, if and only if one of the following cases holds:*

1) *J is a central order* (cf. p. 203) *in the J. a. of the bilinear form $J(X, f)$;*
2) *$A^{(+)} \triangleleft J \subseteq (Q(A))^{(+)}$, where A is a prime associative algebra and $Q(A)$ is its Martindale's quotient ring* (Bokut', L'vov, Kharchenko, 1988)*;*
3) *$H(A, *) \triangleleft J \subseteq H(Q(A), *)$, where A is an associative prime algebra with involution $*$;*
4) *J is Albert's ring (a central order in Albert's algebra).*

Corollary. *Every prime non-degenerate J. a. is either special or is the Albert ring.*

The non-degeneracy condition in the theorem is essential: An example has been constructed in (Pchelintsev, 1986) of a (special) prime J. a. with a basis of absolute zero divisors and, naturally, not being an algebra of any of the types 1)–4). The question on validity of the corollary of the theorem, without the non-degeneracy condition, remains open.

Every simple J. a. is non-degenerate (see below), thus description of simple J. a. follows from the following description of prime non-degenerate J. a.:

Theorem (Zel'manov, 1983a). *Simple J. a. are exactly the algebras of one of the following types:*

1) $J = J(X, f)$;
2) $J = A^{(+)}$, *where* A *is an associative simple algebra;*
3) $J = H(A, *)$, *where* A *is a simple associative algebra, with involution* $*$;
4) J *is the Albert algebra.*

Division J. a. are described analogously: it is necessary only to assume that A is a skew-field, in cases 2) and 3) and, in cases 1) and 4), to impose natural restrictions on J.

The notions of absolute zero divisors and non-degeneracy carry over to J. p. and J. t. s., naturally. Prime, non-degenerate and simple J. p. and J. t. s. are also described in (Zel'manov, 1983b). We now give classification of simple J. p.:

Theorem (Zel'manov, 1983b). *A Jordan pair* V *is simple if and only if it is of one of the following forms: 1)* $V = (R_{-1}, R_1)$, *where* $R = R_{-1} \dot{+} R_0 \dot{+} R_1$ *is a simple 3-graded associative algebra with* $R_{-1} + R_1 \neq 0$*; 2)* $V = (H(R_{-1}, *), H(R_1, *))$, *where* R *is same as in 1), with the involution* $*$ *that preserves graduation; 3)* $V = (J(X, f), J(X, f))$*; 4)* $V = (M_{1,2}(\mathbb{O}), M_{1,2}(\mathbb{O}^0))$ *– a pair of* 1×2 *matrices over the Cayley-Dickson algebra* $\mathbb{O}$, *with the multiplication* $\{xyx\} = x(y^t x)$, *and* $\mathbb{O}^0$ *is anti-isomorphic to* $\mathbb{O}$*; 5)* $V = (J, J)$, *where* J *is Albert's algebra.*

We now turn to studying the properties of the radical $\operatorname{rad} J$. In every J. a. J, just as in the case of alternative algebras, the quasiregular radical $\operatorname{Rad} J$ (the greatest quasiregular ideal), the nilradical $\operatorname{Nil} J$, the locally nilpotent $LN(J)$ and prime radicals $P(J)$ are defined, and they are related by inclusions (2. 21). (However, it is still unclear, whether the ideal $P(J)$ is a "real radical", since it is not known whether a semiprime J. a. can contain P-radical ideals.) The place of the radical $\operatorname{rad} J$, among those radicals is shown in the following theorem:

Theorem (Zel'manov, 1982; Pchelintsev, 1986). *In every J. a.* J *the inclusions* $LN(J) \supseteq \operatorname{rad} J \supseteq P(J)$, *hold, and in general, each of them may be strict.*

Corollary 1. *In every J. a.* J, *every set of absolute zero divisors generates a locally nilpotent ideal.*

Since simple locally nilpotent algebras do not exist, the following holds:

Corollary 2. *Every simple J. a. is non-degenerate.*

For finite-dimensional J. a., all the aforementioned radicals coincide. Moreover, they all coincide in the class of J. a. with the minimal condition for so-called *inner* (or *quadratic*) *ideals.* The latter are analogues of one-sided ideals of associative algebras and are defined as a subspaces K of J. a. J such that $\{kak\} \in K$, for all $k \in K$ and $a \in J$.

Example 1. Let $J = A^{(+)}$, where A is associative. Then every one-sided ideal of the algebra A is an inner ideal in $A^{(+)}$.

Example 2. For every $a \in J$, the set $JU_a = \{xU_a \mid x \in J\}$ is an inner ideal of a J. a. J.

Example 3. Let $J = H(\mathbb{O}_3)$. Then, for every element a of rank 1 (cf. 3.5), the subspace $F \cdot a$ is a quadratic ideal of J.

For a J. a., the following analogue of the classical Wedderburn-Artin theorem holds:

Theorem (Jacobson, 1968; Zhevlakov, Slin'ko, Shestakov, Shirshov, 1978). *Let a J. a. J satisfy the minimal condition for inner ideals. Then $Rad\, J$ is nilpotent and finite-dimensional, and the quotient algebra $J/Rad\, J$ decomposes into a finite direct sum of simple J. a. of one of the following forms:* 1) *a division J. a.;* 2) *$H(A, *)$, for an associative artinian $*$-simple algebra A, with involution $*$;* 3) *$J(X, f)$;* 4) *The Albert algebra.*

Many results from the theory of alternative algebras on relations between solvability and nilpotence are valid for J. a. too. For instance, every finitely generated solvable J. a. is nilpotent; if J is solvable, then J^2 is nilpotent; over a field of characteristic 0, a Jordan nilalgebra of bounded index is solvable. At the same time, in contrast to alternative algebras, finitely generated J. a. may contain solvable, but not nilpotent subalgebras.

Free J. a. have been studied relatively poorly. One of the deepest results about their structure is a theorem by Shirshov, which ascertains that a free J. a. with two generators is special. The free J. a. $J[X]$, for $|X| \geqslant 3$ is not special and contains zero divisors and, for a sufficiently large number of generators, rad $J[X] \neq 0$ (Medvedev, 1985). For special J. a., the role of a free algebra is played by the so-called *free special J. a.* $SJ[X]$, which is defined as the smallest subspace in the free associative algebra Ass $[X]$, containing X and closed with respect to the Jordan multiplication. The elements of the J. a. $SJ[X]$ are called the *Jordan elements* of the algebra Ass $[X]$. It is easy to see that $SJ[X] \subseteq H(\text{Ass}\,[X], *)$, where $*$ is the involution of the algebra Ass $[X]$, which is identity on X: $(x_1x_2 \dots x_n)^* = x_n \dots x_2x_1$. The J. a. $H(\text{Ass}\,[X], *)$ is generated by the set X and by all the possible "tetrades" $\{x_ix_jx_kx_l\} = x_ix_jx_kx_l + x_lx_kx_jx_i$; for $|X| \leqslant 3$, it coincides with the J. a. $SJ[X]$, and for $|X| > 3$ it properly contains it (since the tetrades are not

Jordan elements). For $|X| > 3$, no criteria for elements in Ass $[X]$ to be Jordan have been found, up to now. Every special J. a. is a homomorphic image of the algebra $SJ[X]$, but the converse is not always true. For instance, the quotient algebra $SJ[x,y,z]/I$, where I is an ideal generated by the element $x^2 - y^2$, is exceptional. This implies that it is impossible to define the class SJord of all special J. a. by identities. Let $\pi : J[X] \longrightarrow SJ[X]$ be a canonical epimorphism; then $\operatorname{Ker}\pi \neq 0$, for $|X| \geqslant 3$. The elements in $\operatorname{Ker}\pi$ are called *s-identities*; they are satisfied in all special J. a., but are not identities in the class of all J. a. An example of such an identity is a well-known Glennie s-identity $G(x,y,z) = K(x,y,z) - K(y,x,z)$, where

$$K(x,y,z) = 2\{\{y\{xzx\}y\}z(xy)\} - \{y\{x\{z(xy)z\}x\}y\}.$$

Let us denote by $\overline{\text{SJord}}$ the class of all J. a. satisfying all the s-identities, and by Jord – the class of all the J. a.; then the following proper inclusions hold: SJord $\subset \overline{\text{SJord}} \subset$ Jord (Albert's algebra does not satisfy the Glennie identity, thus it does not belong to $\overline{\text{SJord}}$). The question of describing all the s-identities is still open. It is not clear even whether they all follow from a finite number of s-identities.

Note that the class SJord may be defined by quasi-identities, i.e. by the expressions of the form $(f(x) = 0 \Rightarrow g(x) = 0)$. This is however impossible to achieve with finite number of quasi-identities. Moreover, any number of quasi-identities in a bounded collection of variables does not suffice (Sverchkov, 1983).

A J. a. is called a *Jordan* PI-*algebra*, if it satisfies an identity, which is not an s-identity. For Jordan PI-algebras analogues of main structure theorems from the theory of associative PI-algebras hold:

Theorem (Zel'manov, 1983a; Medvedev, 1988). *Let J be a Jordan PI-algebra over a field F. Then* 1) $\mathit{Nil}\,J = LN(J) = \mathit{rad}\,J$; 2) *if J is prime and non-degenerate, then it is a central order in a simple J. a. with the same identity;* 3) *if J is simple, then either J is finite-dimensional over the center or $J = J(X,f)$;* 4) *if J is finitely generated, then $\mathit{Rad}\,J$ is nilpotent.*

We point out that the non-degeneracy condition on J in 2) and the condition of J being finitely generated in 4) are essential.

As in the case of alternative algebras, an effective method of studying Jordan PI-algebras is a passage to different enveloping algebras. With regard to this, we mention the following result:

Theorem (Shestakov, 1983; Medvedev, 1988). *Let J be a finitely generated Jordan PI-algebra over a field F. Then* 1) *the universal multiplicative enveloping algebra $U(J)$ is an associative PI-algebra;* 2) *if J is special, then its associative enveloping algebra is also a PI-algebra.*

§4. Generalizations of Jordan and Alternative Algebras and Other Classes of Algebras

Just as in the previous section, F will be a field of characteristic $\neq 2$, in the sequel.

4.1. Non-Commutative Jordan Algebras (Schafer, 1966). A natural generalization of the class of Jordan algebras to the non-commutative case is a class of algebras satisfying the following Jordan identity:

$$(x^2y)x = x^2(yx). \tag{1}$$

If the algebra has a unity, then the identity (1) easily implies the following flexibility identity:

$$(xy)x = x(yx). \tag{2}$$

Thus, if we want the class of algebras we are introducing to be stable with respect to adjoining a unity to an algebra, then we need to add the flexibility identity (2) to the identity (1). Algebras satisfying identities (1) and (2) are called *non-commutative Jordan algebras* (n. J.).

It is not difficult to see that identity (1) in the definition of a n. J. algebra may be replaced by any of the following identities:

$$x^2(xy) = x(x^2y), \quad (yx)x^2 = (yx^2)x, \quad (xy)x^2 = (x^2y)x.$$

We have seen in 3.1 that, in case of a Jordan algebra J, the operators $R_{x^k}, k = 1, 2, \dots$, for every $x \in J$ are in the commutative subalgebra, generated by the operators R_x and R_{x^2}. For a n. J. algebra the following analogue of this result holds:

Proposition. *Let A be a n. J. algebra and $a \in A$. Then the operators R_a, L_a, L_{a^2} generate a commutative subalgebra of the multiplication algebra $M(A)$, containing all the operators $R_{a^k}, L_{a^m}; k, m = 1, 2, \dots$*

Corollary. *Every n. J. algebra is power-associative.*

The condition of commuting of multiplication operators with the powers of an element fully characterizes n. J. algebras, since the identities (1) and (2) are just special cases of this condition ($[L_{x^2}, R_x] = [L_x, R_x] = 0$).

Another characterization of n. J. algebras is this: they are flexible algebras A, such that the associatied algebra $A^{(+)}$ (see 1.1 and 3.1) is a Jordan algebra.

The class of n. J. is rather large. Apart from Jordan algebras, it contains all the alternative algebras, as well as arbitrary anti-commutative algebras. Let us give additional examples of n. J. algebras.

Example 1. Let A be an algebra over a field $F, \lambda \in F, \lambda \neq \frac{1}{2}$. Let us define new multiplication on the vector space A:

$$a_\lambda \cdot b = \lambda ab + (1 - \lambda)ba.$$

We denote the resulting algebra by $A^{(\lambda)}$. The passage from the algebra A to $A^{(\lambda)}$ is reversible: $A = (A^{(\lambda)})^{(\mu)}$, for $\mu = \frac{\lambda}{2\lambda-1}$. Properties of algebras A and $A^{(\lambda)}$ are fairly closely related: the ideals (subalgebras) of the algebra A are ideals (subalgebras) of $A^{(\lambda)}$; the algebra $A^{(\lambda)}$ is nilpotent, solvable, simple if and only if A has the corresponding property. If A is an associative algebra, then it is easy to check that $A^{(\lambda)}$ is a n. J. algebra; furthermore, if the identity $[[x, y], z] = 0$ does not hold in A, then $A^{(\lambda)}$ is non-associative. In particular, if A is simple non-commutative associative algebra, then $A^{(\lambda)}$ gives us an example of a simple non-associative n. J. algebra. The algebras of the form $A^{(\lambda)}$, for an associative algebra A, are called the split quasi-associative algebras. More generally, an algebra A is called a *quasi-associative algebra*, if it has a scalar extensions which is a split quasi-associative algebra. Clearly, every quasi-associative algebra is also a n. J. algebra.

Example 2. Let $0 \neq \alpha_1, \dots, 0 \neq \alpha_n \in F$ and let $A(\alpha_1) = (F, \alpha_1), \dots, A(\alpha_1, \dots, \alpha_n) = (A(\alpha_1, \dots, \alpha_{n-1}), \alpha_n)$ be the algebras obtained from F by sequential application of the Cayley-Dickson process (cf. 2.1). Then $A(\alpha_1, \dots, \alpha_n)$ is a simple central quadratic n. J. algebra of dimension 2^n.

In general, every quadratic flexible algebra is a n. J. algebra. The following theorem shows that, under some restrictions, the nilsemisimple (i.e. with zero nilradical) finite-dimensional, power-associative algebras are also n. J. algebras.

Theorem 1. *Let A be a finite-dimensional power-associative algebra, with a bilinear symmetric form (x, y), satisfying the following conditions:* 1) $(xy, z) = (x, yz)$, *for all* $x, y, z \in A$; 2) $(e, e) \neq 0$, *if* $0 \neq e = e^2$; 3) $(x, y) = 0$, *if* xy *is a nilpotent element. Then* $Nil\,A = Nil\,A^{(+)} = \{x \in A \mid (x, A) = 0\}$, *and, if characteristic of the field F is not equal to 5, then the quotient algebra $A/Nil\,A$ is a n. J. algebra.*

The following theorem describes the structure of the nilsemisimple, n. J. algebras:

Theorem 2. *Let A be a finite-dimensional nilsemisimple n. J. algebra over F. Then A has a unity and decomposes into a direct sum of simple algebras; in addition, if characteristic of the field F equals to zero, then each of the simple summands is an algebra of one of the following forms: a (commutative) Jordan algebra; a quasi-associative algebra; a quadratic flexible algebra.*

Over the field of positive characteristic, there is another type of simple n. J. algebra, the so-called nodal algebras. An algebra A with unity 1 is called a *nodal algebra*, if every element in A is representable in the form $\alpha \cdot 1 + n$, where $\alpha \in F$ and n is nilpotent, and if furthermore, the nilpotent elements do not form a subalgebra in A. Nodal algebras do not exist either in the classes of alternative and Jordan algebras, or in the class of n. J. algebras of characteristic 0. Every nodal algebra maps homomorphically onto some simple nodal algebra.

Theorem 3. *Let A be a simple finite-dimensional n. J. algebra over F. Then A is either anti-commutative, or satisfies the conclusion of Theorem 2, or is a nodal algebra. In the latter case,* $\operatorname{char} F = p > 0$, *the algebra* $A^{(+)}$ *is isomorphic to the* p^n*-dimensional associative-commutative algebra of truncated polynomials* $F[x_1, \ldots, x_n], x_i^p = 0$, *and multiplication in A is defined by the following formula:*

$$fg = f \cdot g + \sum_{i,j=1}^{n} \frac{\partial f}{\partial x_i} \cdot \frac{\partial g}{\partial x_j} \cdot c_{ij},$$

where $(\cdot)$ *is the multiplication in* $A^{(+)}$, *and* $c_{ij} = -c_{ji}$ *are arbitrary elements in A, among which at least one is invertible in* $A^{(+)}$.

The construction described in Theorem 3 does not always result in a simple algebra. However, all such algebras of dimension p^2 are simple and, for every even n, there exist simple algebras of that form of dimension p^n. The derivation algebras of the nodal n. J. algebras are related to the simple (nonclassical) modular Lie algebras (Schafer, 1966; Strade, 1972).

In a difference from the case of alternative and Jordan algebras, an analogue of the main Wedderburn theorem on splitting of the nilradical, does not in general hold in the class of n. J. algebras.

The flexible power-associative algebras occupy an intermediate position between arbitrary power-associative algebras and n. J. algebras. Let A be a finite-dimensional algebra of that form, over a field of characteristic 0. The mapping $x \mapsto [a, x]$ is a derivation of the associated commutative power-associative algebra $A^{(+)}$, and, since the nilradical of a power-associative algebra of characteristic 0 is stable with respect to the derivations (Slin'ko, 1972), the inclusion $[A, \operatorname{Nil}(A^{(+)})] \subseteq \operatorname{Nil}(A^{(+)})$ holds, therefore $\operatorname{Nil}(A^{(+)}) \triangleleft A$ and $\operatorname{Nil}(A^{(+)}) = \operatorname{Nil} A$. This means that $(A/\operatorname{Nil} A)^{(+)} = A^{(+)}/\operatorname{Nil}(A^{(+)})$ is a nilsemisimple finite-dimensional commutative power-associative algebra. Over a field of characteristic 0, all such algebras are Jordan algebras (cf. 1.2), thus $A/\operatorname{Nil} A$ is a n. J. algebra. Thus, every finite-dimensional nilsemisimple flexible power-associative algebra over a field of characteristic 0 is a n. J. algebra. In the general case, the following holds:

Theorem 4 (Oehmke, 1958, 1962). *Let A be a finite-dimensional nilsemisimple flexible power-associative algebra over an infinite field of characteristic* $\neq 2, 3$. *Then A has unity and decomposes into the direct sum of simple algebras, each of which is either a n. J. algebra, or is an algebra of degree 2* (cf. p. 179) *over a field of positive characteristic.*

The algebras of the latter form have not been described up to date. A method of their description was given in (Block, 1968), where it was proved that, for every such algebra A, the algebra $A^{(+)}$ is also a simple algebra (of a known structure). An example of an flexible power-associative simple algebra of degree 2 which is neither commutative nor a n. J. algebra was given in (Mayne, 1973).

In the conclusion we point out that structure of arbitrary finite-dimensional nilsemisimple power-associative algebras is still unclear. It is known that in this case new simple algebras arise, among them the nodal algebras, even over an algebraically closed field of characteristic 0.

Example 3. Let V be a vector space of dimension $2n$ over a field F with a non-degenerate skew-symmetric bilinear form (x, y). Let us define multiplication on the vector space $A = F \dot{+} V$, by the rule $(\alpha + v)(\beta + u) = (\alpha\beta + (v, u)) + (\alpha u + \beta v)$. Then A is a quadratic algebra over F, (hence, it is also power-associative), and it is simple and nodal. It is interesting that A turns out to be a Jordan superalgebra (cf. 3.4), if we set $A_0 = F, A_1 = V$.

4.2. Right-Alternative Algebras (Bakhturin, Slin'ko, Shestakov, 1981; Zhevlakov, Slin'ko, Shestakov, Shirshov, 1982; Skosyrskij, 1984). Among the algebras that do not satisfy the flexibility identity (2), right alternative algebras are the most well researched. Recall that an algebra is called *a right alternative algebra* (r. a.), if it satisfies the identity

$$(xy)y = x(yy). \tag{3}$$

Let A be a r. a. algebra over F; then (3) implies that the following relations hold in the algebra of its right multiplications $R(A)$, for all $a, b \in A$:

$$R_{a^2} = R_a^2, \quad R_{a \cdot b} = R_a \cdot R_b, \tag{4}$$

where $a \cdot b = \frac{1}{2}(ab + ba)$ is the multiplication in the associated algebra $A^{(+)}$. Thus, the transformation $a \mapsto R_a$ is a homomorphism of the algebra $A^{(+)}$ into the special Jordan algebra $(R(A))^{(+)}$ (cf. 3.1). If A has unity, then this transformation is injective. Since the class of r. a. algebras is closed with respect to adjoining a unity to the algebra, we have the following:

Proposition. *For every r. a. algebra A, the associated algebra $A^{(+)}$ is a special Jordan algebra.*

This proposition allows for application of the well-developed apparatus of the Jordan algebras to studies of r. a. algebras. The strongest results in the theory of r. a. algebras have been obtained exactly along this road.

Relations (4) easily imply that

$$R_{a^k} R_{a^n} = R_{a^{k+n}},$$

for every $a \in A, k, n = 1, 2, \ldots$ In particular, every r. a. algebra A is power-associative and it has a uniquely defined nilradical $\mathrm{Nil}\, A$

Theorem (Skosyrskij, 1984). *Let A be an arbitrary r. a. algebra. Then the quotient algebra $A/\mathit{Nil}\,A$ is alternative.*

Corollary 1. *Every simple r. a. algebra that is not a nilalgebra is alternative (and consequently, is either associative or a Cayley-Dickson algebra).*

Corollary 2. *Every r. a. algebra without nilpotent elements is alternative.*

Corollary 2 implies, in particular, Skornyakov's theorem on right alternative skew-fields, that we mentioned in 2.2.

Corollary 3. *Let A be a r. a. algebra and $a, b \in A$. Then the element (a, a, b) generates a nilideal in A.*

In general, the ideal generated by the associator (a, a, b) is not solvable. It is not clear however, whether it is a nilalgebra of fixed finite index. It is known only that $(a, a, b)^4 = 0$.

A subspace L of an algebra A is called right nilpotent, if $L^{\langle n \rangle} = 0$, for some n, where $L^{\langle 1 \rangle} = L$, $L^{\langle i+1 \rangle} = L^{\langle i \rangle} L$.

Theorem. *Let A be a r. a. nilalgebra of bounded index. Then every finite-dimensional subspace in A is right nilpotent.*

Corollary 4. *A finite-dimensional r. a. nilalgebra is right nilpotent.*

In particular, every finite-dimensional r. a. nilalgebra is solvable and therefore cannot be a simple algebra. At the same time, it can be non-nilpotent.

The "non-nil" restriction in Corollary 1 is essential in general: an example of a non-alternative, simple r. a. nilalgebra (with the identity $x^3 = 0$) was constructed in (Miheev, 1977). There are no examples of that kind among right artinian r. a. algebras, as is shown in the following

Theorem (Skosyrskij, 1985). *Let A be a r. a. algebra satisfying the minimal condition for right ideals. Then the ideal $N = \mathit{Nil}\,A$ is right nilpotent and the quotient algebra A/N is a semisimple artinian alternative algebra.*

The right artinian condition cannot be replaced by the left artinian: the simple algebra constructed in (Miheev, 1977) does not even contain proper left ideals.

Just as in the case of non-commutative Jordan algebras, the main Wedderburn theorem on splitting off of the radical, is not satisfied in general, in the class of r. a. algebras (Thedy, 1978).

4.3. Algebras of (γ, δ)-Type (Albert, 1949; Nikitin, 1974; Markovichev, 1978; Ng Seong Nam, 1984). Besides the alternative algebras, an important example of non-flexible power-associative algebras is given by the so-called algebras of (γ, δ)-type that arise in studies of classes of algebras A with the following structural property: $(*)$ if I is an ideal of the algebra A, then I^2 is also an ideal of A. Despite its generality, this property enables proofs of fairly meaningful structural results (cf. for instance, 2.4). At the same time, there are not so many generalizations of the associative algebras with property (*).

Proposition. *Let a class $\mathcal{K}$ of power-associative algebras, defined by a system of identities over an infinite field, is such that all of its algebras satisfy condition (*), and let $\mathcal{K}$ contain all the associative algebras. Then $\mathcal{K}$ is either the class of alternative algebras, or $\mathcal{K}$ is defined by the following identities*

$$(x,x,x)=0, \tag{5}$$

$$S(x,y,z)\equiv(x,y,z)+(y,z,x)+(z,x,y)=0, \tag{6}$$

$$(x,y,z)+\gamma(y,x,z)+\delta(z,x,y)=0, \tag{7}$$

where γ and δ are fixed scalars such that $\gamma^2-\delta^2+\delta=1$.

The algebras satisfying identities (5)–(7) are called the *algebras of* (γ,δ)-type. Their structure in the finite-dimensional case is described by the following

Theorem. *Let A be a finite-dimensional algebra of type (γ,δ), over a field F of characteristic $\neq 2,3,5$. Then the radical $Nil\,A$ is nilpotent and the quotient algebra $A/Nil\,A=\overline{A}$ is associative. If, in addition, the algebra $\overline{A}$ is separable over F, then $A=B\dotplus Nil\,A$, where B is a subalgebra of A isomorphic to $\overline{A}$.*

The class of algebras of (γ,δ)-type does not give new examples of simple algebras.

Theorem (Markovichev, 1978; Ng Seong Nam, 1984). *Every simple (not necessarily finite-dimensional) algebra of type (γ,δ) and characteristic $\neq 2,3,5$ is associative.*

At the same time, there exist prime non-associative algebras of type (γ,δ) of arbitrary characteristic (Pchelintsev, 1984). These algebras, just as in general, every non-associative algebra of type (γ,δ), contain non-zero locally nilpotent ideals.

4.4. Lie-Admissible Algebras (Myung, 1982, 1986). Studies of one more class of algebras have been fairly intensively initiated in recent times, under the influence of papers by a physicist Santilli (1978, 1982); these are the so-called *Lie-admissible algebras*, i.e. algebras A such that their commutator algebra $A^{(-)}$ is a Lie algebra. Apart from the associative and Lie algebras, this class for instance contains quasi-associative algebras and algebras of (γ,δ)-type. If L is a Lie algebra with multiplication $[x,y]$, then after defining an arbitrary commutative multiplication $x\circ y$ on L and setting $x*y=\frac{1}{2}([x,y]+x\circ y)$, we arrive at a Lie-admissible algebra $\tilde{L}$ (with respect to the multiplication $x*y$), for which $L^{(-)}\cong L$. It is clear that every Lie-admissible algebra allows such a realization; furthermore, if L is a simple algebra, then $\tilde{L}$ is also simple. Since the commutative multiplication $x\circ y$ was arbitrary, it is also clear that, in general, the problem of describing simple Lie-admissible algebras, even modulo Lie algebras, is hardly feasible. However, under some additional restrictions, it is possible to obtain such a description.

Theorem. *Let A be a finite-dimensional Lie admissible algebra with multiplication $*$ over an algebraically closed field of characteristic 0, such that $A^{(-)}$ is a simple Lie algebra. Then if A satisfies the identity $(x, x, x) = 0$, then there exists a linear form τ on A and a scalar $\beta \in F$, such that*

$$x * y = \frac{1}{2}[x, y] + \tau(x)y + \tau(y)x + \beta x \# y, \tag{8}$$

where $x\#y$ is either equal to zero, for all $x, y \in A$, or $A^{(-)} \cong sl(n+1, F)$ and

$$x\#y = xy + yx - \frac{2}{n+1} tr(xy)E,$$

where E is the identity matrix. Furthermore, A is power-associative, if and only if $\beta = 0$ in (8).

Corollary. *If, the algebra A from the hypotheses of the theorem is flexible, then*

$$x * y = \frac{1}{2}[x, y] + \beta x \# y;$$

if, in addition, A is power-associative, then A is a Lie algebra.

§5. Malcev Algebras and Binary Lie Algebras

5.1. Structure and Representation of Finite-Dimensional Malcev Algebras. We have defined Malcev algebras and binary Lie algebras in §1, which arose in (Malcev, 1955) as two natural generalizations of Lie algebras. After expanding the Jacobian in identity (1.9), it may be rewritten (in view of anticommutativity) in the following form:

$$xyzx + yzx^2 + zx^2y = xy \cdot xz, \tag{1}$$

where parentheses were omitted in left normalized products $xyzx = (xy \cdot z)x$, $yzx^2 = (yz \cdot x)x$, etc, for the convenience of notation. If the characteristic of the base field F is different from 2, then the following identity follows from (1):

$$xyzt + yztx + ztxy + txyz = ty \cdot xz, \tag{2}$$

which, together with the anticommutativity identity $x^2 = 0$, is appropriate to take as a definition of Malcev algebras in the case char $F = 2$ too, since first of all, for $t = x$ it again turns into identity (1), and secondly, it has a number of advantages: it is multilinear and transforms into itself after cyclic permutations of the variables x, y, z, t, hence all the variables participate equally in (2). Every Lie algebra satisfies identity (2); on the other hand, an anticommutative algebra satisfying identity (1) or (2) is a binary Lie algebra. Thus, the class of Malcev algebras is placed between Lie algebras and binary Lie algebras.

Up to now, the theory of finite-dimensional Malcev algebras has almost as a completed form as the theory of Lie algebras. We will give here only basic facts on the structure theory of Malcev algebras.

In studying various classes of algebras one of the most essential questions is the question of describing simple algebras of that class. In case of Malcev algebras it is natural to ask the question about classification of simple Malcev algebras that are not Lie algebras, and there is almost complete answer to this question: non-Lie simple Malcev algebras over an arbitrary field F of characteristic different from 2 have been described, even without the assumption of finite-dimensionality (Kuz'min, 1971; Filippov, 1976a).

Let $\mathbb{O} = \mathbb{O}(\alpha, \beta, \gamma)$ be the Cayley-Dickson algebra over F (cf. 2.1). Then $\mathbb{O} = F \dot{+} M$, where $M = \{x \in \mathbb{O} \mid t(x) = 0\}$ and multiplication in $\mathbb{O}$, for elements $a, b \in M$ is defined by the following formula:

$$a \cdot b = -(a, b) + a \times b, \tag{3}$$

where $(,)$ is a symmetric non-degenerate bilinear form on M and $(\times)$ is anticommutative multiplication on M. We denote the constructed 7-dimensional anticommutative algebra $(M, \times)$ by $M(\alpha, \beta, \gamma)$; it is defined in the case when $\operatorname{char} F = 2$ too, and it is a central simple Malcev algebra over F; if $\operatorname{char} F \neq 3$, then the algebra $M(\alpha, \beta, \gamma)$ is not a Lie algebra.

Theorem. *Every central simple Malcev algebra over a field F of characteristic $\neq 2$ is either a Lie algebra or an algebra of type $M(\alpha, \beta, \gamma)$. In particular, there are no non-Lie simple Malcev algebras of characteristic 3.*

Using the right alternativity of the Cayley-Dickson algebra $\mathbb{O}(\alpha, \beta, \gamma) = F \dot{+} M$, we obtain the following $(a, b \in M)$:

$$(a \cdot b) \cdot b = -(a, b)b - (a \times b, b) + (a \times b) \times b = a \cdot b^2 = -(b, b)a,$$

hence

$$(a \times b) \times b = -(b, b)a + (a, b)b, \quad (a \times b, b) = 0. \tag{4}$$

In particular, (4) implies that the bilinear form $(,)$ is uniquely determined by the multiplication operation $(\times)$ on M, and then, by formula (3), multiplication on $\mathbb{O}$ is defined too. Thus, two Malcev algebras of types $M(\alpha, \beta, \gamma)$ and $M(\alpha', \beta', \gamma')$ over F are isomorphic if and only if the corresponding Cayley-Dickson algebras $\mathbb{O}(\alpha, \beta, \gamma)$ and $\mathbb{O}(\alpha', \beta', \gamma')$ are isomorphic. Another useful criterion for isomorphism of the algebras of type $M(\alpha, \beta, \gamma)$ consists in equivalence of bilinear forms $(,)$ defined on them.

For every $n \geqslant 3$ there exist central simple anticommutative algebras of dimension $2^n - 1$, over the field F of characteristic 2, satisfying identity (1), but only for $n = 3$ do they satisfy identity (2) (Kuz'min, 1967a).

In case $\operatorname{char} F = 0$ the structure of finite-dimensional Malcev algebras has been studied in more depth. We define a Killing form K on the space of Malcev algebras A, by setting $K(x, y) = \operatorname{tr}(R_x R_y)$, where R_x is the operator of right multiplication by x in A. The form K is symmetric and associative: $K(x, y) = K(y, x), K(xy, z) = K(x, yz)$. The algebra A is semisimple (i.e. its solvable radical $S(A)$ equals 0), if and only if its Killing form is non-degenerate. In case of Lie algebras, this claim becomes the well-known Cartan criterion for semisimplicity of Lie algebras. A semisimple algebra A decomposes into the direct sum of simple algebras, which are, by what has been said, either simple Lie algebras or 7-dimensional algebras of type $M(\alpha, \beta, \gamma)$, over its centroid $\Gamma \supseteq F$ $(\alpha, \beta, \gamma \in \Gamma)$.

The radical $S(A)$ coincides with the orthogonal complement of A^2, with respect to K. In particular, the algebra A is solvable if and only if $K(A, A^2) = 0$. In addition, the inclusions $S \cdot A \subseteq N, SD \subseteq N$ hold, where D is an arbitrary derivation of the algebra A, and $N = N(A)$ is the greatest nilpotent ideal (nilradical) in A. Both the radical and nilradical of a Malcev algebra have the property of ideal heredity: if $B \triangleleft A$, then $S(B) = B \cap S(A), N(B) = B \cap N(A)$.

An automorphism $\phi \in \operatorname{Aut} A$ is called special, if it is a product of automorphisms of the form $\exp D$, where D is a nilpotent inner derivation of the form $R_{xy} + [R_x, R_y]$. Just as in the case of alternative and Jordan algebras, a theorem on splitting off of the radical and conjugacy of semisimple quotients with respect to special automorphisms holds for Malcev algebras of characteristic 0. This result generalizes the classical Levi-Malcev-Harish-Chandra theorem for Lie algebras.

A Cartan subalgebra of a Malcev algebra A over an arbitrary field F is defined in the same fashion as in the case of Lie algebras: it is a nilpotent subalgebra H that coincides with its normalizer $\mathfrak{N}(H) = \{x \in A \mid H \cdot x \subseteq H\}$. Such subalgebras necessarily exist if $|F| \geqslant \dim A$. If $\operatorname{char} F = 0$ and F is algebraically closed, then the Cartan subalgebras are mutually conjugated via special automorphisms.

An effective way to study finite-dimensional Malcev algebras of arbitrary characteristic is through the representations theory or Malcev modules. In agreement with identity (2), a linear transformation $\rho : A \longrightarrow \operatorname{End} V$ is called a (right) representation of a Malcev algebra A if, for all $a, b, c \in A$, the following relation holds:

$$\rho(ab \cdot c) = \rho(a)\rho(b)\rho(c) - \rho(c)\rho(a)\rho(b) + \rho(b)\rho(ca) - \rho(bc)\rho(a); \qquad (5)$$

in this case, V is called a *Malcev A-module*. Since the algebra A is anticommutative, the notion of a Malcev A-module is equivalent to the notion of a bimodule: it suffices to set $am = -ma$ $(a \in A, m \in V)$. A special case of a representation is a regular representation $x \mapsto R_x$.

The representation theory of nilpotent Malcev algebras is fully analogous to the corresponding theory for Lie algebras. An important role here is played by a theorem on nilpotency of the associative algebra A_ρ^*, generated by the operators $\rho(x)$, with the condition that $\rho(x)$ are nilpotent (an analogue of Engel's theorem). If, in addition, ρ is an almost exact representation (i.e. the kernel of ρ does not contain non-zero ideal of the algebra A), then the algebra A is also nilpotent.

The representation ρ is called split if, for every $x \in A$, the eigenvalues of the matrix $\rho(x)$ are in F. For split representations of solvable Malcev algebras of characteristic 0, an analogue of a Lie theorem on triangularization holds, i.e. on the existence of an A-invariant flag of subspaces (submodules) of the module V. The following claim is an analogue of the classical Weil theorem: every representation of a semisimple Malcev algebra of characteristic 0 is completely reducible. If V is an exact irreducible A-module ($\operatorname{char} F = 0$), then the algebra A is simple, and one of the following cases holds: 1) $A \cong M(\alpha, \beta, \gamma)$ and V is a regular A-module, 2) A is a Lie algebra and V is a Lie module, 3) $A \dotplus V \cong A_1 \dotplus V_1$, where $A_1 = \mathrm{sl}(2, F), \dim M_1 = 2, \rho(a) = a^*$, where a^* is the matrix adjoint to the matrix $a \in A_1$.

A well known first Whitehead lemma on derivation of a semisimple Lie algebra to a bimodule generalizes to representations of semisimple Malcev algebras; this implies, in particular, that every derivation of a semisimple Malcev algebra is inner.

5.2. Finite-Dimensional Binary Lie Algebras (*BL*-Algebras). Engel's theorem in its classical formulation remains valid for a BL-algebra A of arbitrary characteristic: if every operator R_x is nilpotent, then the algebra A is nilpotent (Kuz'min, 1967b). As in the case of Malcev algebras, a BL-algebra A contains the greatest nilpotent ideal $N(A)$ – the nilradical of the algebra A. If A is a nilpotent algebra and ρ is a finite-dimensional binary Lie representation of A by nilpotent operators, then the enveloping associative algebra A_ρ^* of the representation ρ is nilpotent. However, the majority of the results on finite-dimensional BL-algebras relates to the case of characteristic 0. In the sequel, A will denote a finite-dimensional BL-algebra of characteristic 0. If A is solvable and V is a binary Lie A-module, then the algebra A^2 is nilpotent and acts nilpotently on V. The solvable algebra $A \neq 0$ contains an abelian ideal $I \neq 0$, and if the base field is algebraically closed, then A contains an one-dimensional ideal. Semisimple BL-algebras and their representations are described in the following

Theorem (Grishkov, 1980). *If A is semisimple, V is a binary Lie A-module and if V_0 is the annihilator of the algebra A in module V, then A is a Malcev algebra and V/V_0 is a Malcev A-module.*

In general, A does not necessarily decomposes into a semidirect sum of a semisimple subalgebra and the solvable radical S, but, among all the subalgebras $B \leqslant A$, for which $A = B + S$, there exists a subalgebra B_0, which is a semidirect sum of a semisimple Lie subalgebra L and an ideal C, whose radical R is in the center (the annihilator) of A, $C^2 = C, \overline{C} = C/R$ is the direct sum of 7-dimensional simple Malcev algebras (the base field is algebraically closed); if V is a binary Lie A-module, then $VR = 0$. In particular, the Levi decomposition for A exists, if A/S is a Lie algebra.

Example. Let M be a simple 7-dimensional Malcev algebra over F, let V be a finite-dimensional space with $1 \leqslant \dim V \leqslant 14$ and let $\sigma : M \times M \longrightarrow V$ be an arbitrary skew-symmetric function. Then the algebra $(M, V, \sigma) = M \dot{+} V$ with the multiplication $(a_1 + v_1) \cdot (a_2 + v_2) = a_1 a_2 + \sigma(a_1, a_2)$ $(a_i \in M, v_i \in V, i = 1, 2)$ is a binary Lie algebra. Since the radical V of the algebra $A = (M, V, \sigma)$ coincides with its center, then it obviously does not split off if $A^2 = A$, which is easily achievable for an appropriate choice of σ.

5.3. Infinite-Dimensional Malcev Algebras. Studies of Malcev algebras, without the assumption of finite-dimensionality are mainly based on the analysis of identities of the free Malcev algebra with finite or countable number of generators. Since the structure of the identities in Malcev algebras essentially depends on the characteristic, we will consistently assume here that char $F \neq 2$.

A number of properties of infinite-dimensional algebras, such as local nilpotency, local finiteness, being algebraic (every subsequent notion is weaker than the preceeding one) brings them closer to finite-dimensional algebras. An algebra A is called locally finite, if every finite set of of its elements generates a finite-dimensional subalgebra. An algebra A is called an *algebraic algebra* if, for all $x, y \in A$, there exists a natural number n dependent on x, y, such that xy^n belongs to a subalgebra with the generators $x, xy, \ldots, xy^{n-1}$. A special case of the algebraic property is the weak Engel condition $E : xy^{n(x,y)} = 0$. Every Malcev algebra A contains the greatest locally finite ideal $L(A)$ as well as the greatest locally nilpotent ideal $LN(A)$ (Kuz'min, 1968a). In the class of algebraic Malcev algebras, the extension of locally finite algebra by a locally finite is again a locally finite algebra, thus $L(A/L(A)) = 0$. If A is weakly Engel, then $L(A) = LN(A)$ (Kuz'min, 1968a). The following theorem reduces the question of local nilpotency for Malcev algebras to the corresponding question for Lie algebras. For a Malcev algebra A to be locally nilpotent, it is necessary and sufficient that condition E holds in A and that every Lie homomorphic image of A is locally nilpotent (Filippov, 1976b). In particular, a Malcev algebra of characteristic $p > 2$, satisfying the condition E_{p+1}, i.e. the identity $xy^{p+1} = 0$ is locally nilpotent, since this holds for Lie algebras. As in the case of Lie algebras, this implies an affirmative solution of the weak Burnside problem for Moufang loops of prime period (Grishkov, 1985; Kostrikin, 1986, cf. also §6).

If char $F \neq 2, 3$, then, along with the Jacobians $J(x, y, z) = xy \cdot z + yz \cdot x + zx \cdot y$, we consider the function $g(x, y, z, t, u)$ with a number of remarkable properties:

$$g(x,y,z,t,u) = J([x,y,xz],t,u) + J([x,t,yz],x,u),$$

where $[x,y,z] = 3xy \cdot z - J(x,y,z)$. The function $g(x,y,z,t,u)$ is skew-symmetric in y,z,t,u and equals 0, if $y,z \in A^3$ or $y,z,t \in A^2$; in particular, the algebra A^2 satisfies the identity $g = 0$. Since the function g is non-zero in the free Malcev algebra M_k, with $k \geqslant 5$ generators, for $A = M_k$ $(k \geqslant 5)$, the identities for A and A^2 differ. The algebra M_4 satisfies the identity $g = 0$ and, for $k \geqslant 5$, M_k satisfies the identity $g(x_1,\ldots,x_5)x_6\ldots x_{k+2} = 0$, but does not satisfy the identity $g(x_1,\ldots x_5)x_6\ldots x_{k+1} = 0$, thus, for every $k \geqslant 4$ the identities for M_k and M_{k+1} are different (Filippov, 1984). Moreover, the algebras M_k, for $k \geqslant 5$ have a non-trivial center and thus, trivially, they are not prime. A free Malcev algebra with countable number of generators also has a non-trivial center: it contains for instance the elements of the form $g(x_1,\ldots x_5)y^2$, which are in general different from 0. The semiprime Malcev algebras satisfy the identity $g = 0$.

Prime and semiprime Malcev algebras of characteristic 3 are Lie algebras, thus, in particular, non-Lie simple Malcev algebras of characteristic 3 do not exist. Let A be a prime non-Lie Malcev algebra of characteristic $\neq 2,3$. Then the center Z of the algebra of right multiplications $R(A)$ is different from 0 and is naturally contained in the centroid Γ. Since Γ is a commutative integral domain, there exists the quotient field Q of Z (coinciding with the quotient field of Γ) and the canonical embedding $A \longrightarrow A_Q = Q \otimes_Z A$. The algebra A_Q turns out to be a 7-dimensional central simple algebra over the field Q.

The commutator algebra $A^{(-)}$ of an arbitrary alternative algebra A is a Malcev algebra. In this regard, there arises a question: is it true that every Malcev algebra of characteristic $\neq 2,3$ is embeddable into a commutator algebra of a suitable alternative algebra? The answer to this question is affirmative for semiprime Malcev algebras, but the problem remains open in the general case.

§6. Quasigroups and Loops

6.1. Basic Notions. A non-empty set Q with a binary operation $(\cdot)$ is called a *quasigroup*, if the equations $a \cdot x = b$, $y \cdot a = b$ are uniquely solvable, for all $a, b \in Q$. The solutions of these equations are denoted as $x = a \setminus b$, $y = b/a$, and the binary operations $\setminus, /$ are respectively called the left and the right division. They are related to the multiplication $(\cdot)$, via the following identities:

$$x \cdot (x \setminus y) = x \setminus (x \cdot y) = y, \quad (x/y) \cdot y = (x \cdot y)/y = x. \tag{1}$$

It is clear that the notion of a quasigroup generalizes the notion of a group: group is a quasigroup for which the operation of multiplication is associative. A quasigroup with unity is called a *loop*.

A quasigroup may be equivalently defined as a set with three basic operations $(\cdot), \backslash, /$, related via identities (1). Then a loop is a quasigroup with the additional identity $x \backslash x = y/y$.

Finite quasigroups may be defined with the aid of Cayley tables.

Example.

G_1	e	a	b	c	d
e	e	a	b	c	d
a	a	e	d	b	c
b	b	c	e	d	a
c	c	d	a	e	b
d	d	b	c	a	e

G_2	e	a	b	c	d
e	e	a	b	c	d
a	a	e	d	b	c
b	b	c	a	d	e
c	c	d	e	a	b
d	d	b	c	e	a

G_3	e	a	b	c	d
e	e	a	b	c	d
a	a	b	d	e	c
b	b	c	a	d	e
c	c	d	e	a	b
d	d	e	c	b	a

G_4	e	a	b	c	d
e	e	a	b	c	d
a	a	e	c	d	b
b	b	c	d	a	e
c	c	d	e	b	a
d	d	b	a	e	c

These are apparently mutually non-isomorphic non-associative loops. Incidentally, the smallest order of a non-associative loop is 5.

If we omit the borders in the Cayley table of a finite quasigroup, the resulting square has the property that the elements in every row and every column (their number equals the order of the quasigroup) do not repeat. Squares with this property are called *latin squares.* They have been apparently studied by Euler. Thus, quasigroups and latin squares are closely linked. Shuffling around rows and columns of a latin square or renaming its entries (i.e. applying a permutation of the set Q, where the entries of the square come from) does not change the latin property of the square. Algebraically this leads to an important property, namely that of isotopy of quasigroups. Quasigroups Q, Q' are said to be isotopic, if there is a triple of bijective transformations $\alpha, \beta, \gamma : Q \longrightarrow Q'$, such that $(xy)\gamma = x\alpha \cdot y\beta$, for all $x, y \in Q$. The triple (α, β, γ) is called an *isotopy* of Q to Q'. Composition of isotopies is defined in a natural way: $(\alpha, \beta, \gamma) \cdot (\alpha_1, \beta_1, \gamma_1) = (\alpha\alpha_1, \beta\beta_1, \gamma\gamma_1)$. If $Q = Q'$, then the isotopy is called an *autotopy*; the autotopies form a group with respect to the given operation. The transformations $R_a : x \mapsto xa$, $L_a : x \mapsto ax$ are called the right and the left translation respectively. Let us fix an arbitrary pair of elements $a, b \in Q$ and let us define a new operation $(\circ)$ on Q, by setting $xy = xb \circ ay$. Then $Q(\circ)$ is a quasigroup and $(R_a, L_a, 1)$ is an isotopy of Q to $Q(\circ)$. It is clear that $e = ab$ is the unity of the quasigroup $Q(\circ)$, i.e. $Q(\circ)$ is a loop. Thus, every quasigroup is isotopic to a loop. For $b = a$, the loop $Q(\circ)$ is called an LP-isotope of the quasigroup Q.

The notion of isotopy does not play a special role for groups, because of Albert's theorem: if two groups are isotopic, they are isomorphic. This statement is a consequence of a more general statement: if a loop is isotopic to a group, then they are isomorphic. Loop properties preserved under isotopies are called *universal*; the aforementioned implies that associativity is an example of a universal property. Universal identities in quasigroups may be described in the language of the so-called $*$-automata (Gvaramiya, 1985). The category of quasigroups is embeddable into the category of invertible

$*$-automata, and a quasigroup formula, in particular an identity, is universal, if and only if it is expressible in terms of the automata category containing it.

By using isotopies, a number of quasigroups may be obtained from a given quasigroup. Another way consists in passing to the anti-isomorphic quasigroup or in substituting multiplication operation on Q by the operation of the left or the right division. The resulting quasigroups are called parastrophs of the quasigroup Q.

6.2. Analytic Loops and Their Tangent Algebras. Let us first recall some basic facts from the theory of Lie groups and Lie algebras. First of all, there are different variants of definitions of Lie groups, depending on requirements of topological nature. The topological space of a Lie group G is an n-dimensional manifold – topological, differentiable, or analytic, and the group operations (multiplication and inversion) are assumed to be respectively continuous, differentiable appropriately many times, or analytic. The question of equivalence of the weakest of these definitions with the strongest was the essence of the fifth Hilbert problem, which was affirmatively solved in 1952 (Gleason, Montgomery, Zippin, (cf. Kaplansky, 1971)).

Every neighbourhood U of the identity element $e \in G$, homeomorphic to the Euclidean space $\mathbb{R}^n$, is a local Lie group: there exists a neighbourhood $U_1 \subseteq U$ of e, such that, for $x, y \in U_1$, the operations of multiplication and inversion are defined (with the values in U); the functions $f^i(x,y)$, where $f^i(x,y)$ is the i-th coordinate of the vector $f(x,y) = x \cdot y$ are either continuous, or differentiable, or analytic, depending on the initial requirements.

We will hold on to an intermediate variant and assume that the functions $f^i(x,y)$ are twice continuously differentiable in U_1. The point e is taken to be the coordinate origin; thus $f(x,0) = f(0,x) = x$. The set of all the tangent vectors at e, to all the differential paths $g(t)$ starting at e, forms the *tangent space* $T_e = \mathbb{R}^n$. Let $a, b \in T_e$ be the tangent vectors for the paths $g(t), h(t)$. Then the tangent vector to the path $k(t)$, where $k(t^2) = g(t)h(t)[h(t)g(t)]^{-1}$ is a bilinear function of the vectors a, b; in this way, T_e becomes an n-dimensional algebra over the field $\mathbb{R}$, called the *tangent algebra* of the (local) Lie group G. The algebra $T_e = L(G)$ is obviously anticommutative (satisfies the identity $x^2 = 0$); associativity of multiplication in G implies that $L(G)$ satisfies the Jacobi identity $xy \cdot z + yz \cdot x + zx \cdot y = 0$, i.e. $L(G)$ is a Lie algebra. Another way of constructing the Lie algebra $L(G)$ is possible too. To this end, expand the functions $f^i(x,y)$ into the Taylor series in a neighbourhood of the coordinate origin $|x|, |y| < \epsilon$

$$f^i(x,y) = x^i + y^i + a^i_{jk} x^j y^k + o(\epsilon^2)$$

(the summation is over the repeating indices) and set $c^i_{jk} = a^i_{jk} - a^i_{kj}$. Then $L(G)$ is defined as the algebra with a basis $e_1, \dots, e_n$ and the multiplication table $e_i e_j = c^k_{ij} e_k$.

A. I. Malcev has pointed out that neither of the two ways of defining the tangent algebra really needs associativity of multiplication in G, as well as that they can be applied to differentiable and, in particular, to *analytic loops*. The curve $k(t)$, considered above may be defined in case of loops by the equality $k(t^2) = g(t)h(t)/[h(t)g(t)]$.

There is a close relation between Lie groups and their tangent algebras. For instance, two connected Lie groups are locally isomorphic if and only if, their Lie algebras are isomorphic; connected simply connected Lie group is uniquely determined by its Lie algebra. Thus it is clear why Lie algebras are one of the main instruments in studying Lie groups. However, in a more general case of loops, without associativity, the notion of a tangent algebra turns out to be not very meaningful, if at least power-associativity is not assumed.

A continuous curve $g(t)$, defined for sufficiently small values of t is called a *locally one-parameter subgroup*, if the following identity $g(t+s) = g(t)\cdot g(s)$ holds in its domain. Such a curve is always differentiable and if a is its tangent vector in e, then the coordinates $g^i(t)$ satisfy the following system of ordinary differential equations

$$\frac{dg^i(t)}{dt} = v^i_j(g)a^j, \quad i = 1, \ldots, n, \tag{2}$$

where $v^i_j(x) = \frac{\partial}{\partial y^j} f^i(x, 0)$. A crucial moment for the theory of local Lie groups is the theorem about the existence of the local one-parameter subgroups $g(t) = g(a;t)$ with a given arbitrary tangent vector $a \in T_e$. Because of $g(\alpha a; t) = g(a; \alpha t), \alpha > 0$, the vector $g(a;1)$ is defined, for sufficiently small a. The transformation $\exp : a \mapsto g(a;1)$ defines a diffeomorphism of a neighbourhood V of the coordinate origin in T_e to some neighbourhood U of the element e in G. The inverse transformation $\log : U \mapsto V$ introduces the so-called canonical coordinates of the 1st kind. The formula $a \circ b = \log(\exp a \cdot \exp b)$ provides V with a structure of a local Lie group, isomorphic to the local group U; the one-parameter subgroups in V are defined by the equations $\tilde{g}(a;t) = at$.

A natural boundary of generality of the assumptions, under which a similar situation occurs is the condition of power-associativity. And, in fact, this condition turns out to be sufficient too. Let $g(t)$ be a solution of the system (2) with the initial condition $g(0) = (0, \ldots, 0) = e$, defined for $|t| < \alpha$. By approximating the curve $g(t)$ by the cyclic subgroups with generators $g(u), u \to 0$, we can show that $g(t)$ is a one-parameter subgroup in its whole domain. Thus it is in the class of power-associative loops where the exponential transformation makes sense and where the canonical coordinates of 1st kind are defined (Kuz'min, 1971).

The fact that a passage from one system of canonical coordinates of 1st kind to another system of canonical coordinates of 1st kind is given by analytic functions (in fact even linear) implies, for instance, invariance of the differentiable structure in a local differentiable power-associative loop.

If G is a Lie group, then, in the canonical coordinates of the 1st kind the multiplication operation on G (more exactly, in a neighbourhood of the unity of G) is expressible through the operations of addition and multiplication in the Lie algebra, with the aid of the so-called *Campbell-Hausdorff series*

$$x \circ y = x + y + \frac{1}{2}xy + \frac{1}{12}(xy^2 + yx^2) + \frac{1}{24}yx^2y + \dots, \tag{3}$$

where parentheses have been left out in the left normalized products of elements of $L(G)$. Hausdorff gave a constructive method of finding the summands of the series (3) (cf. Chebotarev, 1940). Consider x, y to be generators of the free Lie algebra (or the free anti-commutative algebra) and denote the right-hand-side of (3) by $u(x, y)$. Then $u(x, y)$ satisfies a symbolic differential equation

$$x\frac{\partial u}{\partial x} - xV^{-1}(y)\frac{\partial u}{\partial y} = 0,$$

where the operator $s\frac{\partial}{\partial t}$ stands for the differential replacement of occurrences of t by occurrences of s, $xV^{-1}(y) = \sum_{n=0}^{\infty}(-1)^n b_n xy^n$ and b_n are rational numbers with the derived function $\sum b_n t^n = t/(e^t - 1)$ ($b_k = B_k/k!$, where B_k are the so-called Bernoulli numbers). Arranging $u(x, y)$ in powers of x: $u = u_0 + u_1 + \dots$, we get a system of recurrent relations for determining u_i: $u_0 = y$, $ku_k = xV^{-1}(y)\frac{\partial u_{k-1}}{\partial y}$, $k \geqslant 1$. In particular,

$$u_1 = xV^{-1}(y) = x + \frac{1}{2}xy + \frac{1}{12}xy^2 - \frac{1}{6!}xy^4 + \frac{1}{6 \cdot 7!}xy^6 + \dots$$

Alternative (dissociative) loops where every two elements generate a subgroup, occupy an intermediate place between power-associative loops and groups. If G is an alternative differentiable loop and if $g(t), h(t)$ are its local one-parametric subgroups, then the products of the form $g(t_1)h(s_1)\dots g(t_n)\,h(s_n)$, for small t_i, s_i do not depend on the distribution of the parentheses (initially it is checked for rational t_i, s_i). Thus, $g(t_i), h(s_i)$ lie in a local Lie subgroup. After switching to the canonical coordinates of the 1st kind, we find that the multiplication in G, in the neighbourhood of the coordinate origin is expressible by the ordinary Campbell-Hausdorff formula (3), and that the tangent algebra $L(G)$ is a binary Lie algebra: every two of its elements generate a Lie subalgebra. Formula (3) shows that G is determined uniquely, up to a local isomorphism, by its tangent algebra, and since the right-hand-side of (3) is an analytic function of its coordinates x, y, G has a structure of a local analytic loop, compatible with the initial differential structure.

For every finite-dimensional binary Lie algebra L over $\mathbb{R}$, with the aid of the Campbell-Hausdorff series, a local analytic alternative loop is constructed, whose tangent algebra is isomorphic to L.

For a long time the attention of algebraists has been attracted by the so-called *Moufang loops*, defined by any of the following mutually equivalent identities:

$$(xy \cdot z)y = x(y \cdot zy), \tag{4}$$
$$(yz \cdot y)x = y(z \cdot yx), \tag{5}$$
$$xy \cdot zx = (x \cdot yz)x. \tag{6}$$

They have been first considered by Moufang, in whose honor they have been named, in connection to studies on non-Desarguesian projective planes. The following fundamental theorem is due to her: if G is a Moufang loop, then every three elements $a, b, c \in G$, connected with the relation $ab \cdot c = a \cdot bc$, generate a subgroup. In particular, for $c = e$, this implies the statement about the alternativeness of the Moufang loops. Let us give two examples of analytic Moufang loops.

Alternative rings and algebras satisfy the identities (4)–(6) (cf. 2.3). If A is a finite-dimensional alternative algebra with unity, over the field $\mathbb{R}$ and if a is its invertible element, then a^{-1} is a polynomial in a (over $\mathbb{R}$). Thus, the set $W(A)$ of invertible elements of the algebra A is closed with respect to multiplication and forms an analytic Moufang loop globally. Its tangent algebra is isomorphic to the commutator algebra $A^{(-)}$, whose space coincides with A and the multiplication $[,]$ is related to the multiplication in A by the formula $[a, b] = ab - ba$.

Multiplicativity of the norm in the Cayley-Dickson algebra $\mathbb{O} = \mathbb{O}(\alpha, \beta, \gamma)$ over $\mathbb{R}$ implies that the elements in $\mathbb{O}$, with the norm equal to 1 also form an analytic Moufang loop H, globally. If $\mathbb{O}$ is a division algebra, then the space of this loop is a 7-dimensional sphere S^7, and if $\mathbb{O}$ is a split Cayley-Dickson algebra, then the space H is analytically isomorphic to the direct product $S^3 \times \mathbb{R}^4$. The tangent algebra of this loop is isomorphic to a 7-dimensional simple Malcev algebra $M(\alpha, \beta, \gamma)$ (cf. 5.1).

By writing down operation of multiplication in an arbitrary analytic Moufang loop G with the aid of the Campbell-Hausdorff series (in canonical coordinates of the 1st kind), A. I. Malcev discovered that the tangent algebra $L(G)$ satisfies identity (4.1), i.e. turns out to be a Malcev algebra (in modern terminology). Thus, a Malcev algebra is associated to every analytic (or differentiable) Moufang loop, in the same way as a Lie algebra is associated to a Lie group. The question arose, however, about the existence of the inverse correspondence: Is there any analytic Moufang loop, even local, corresponding to any finite-dimensional real Malcev algebra? For an arbitrary Lie algebra L, the multiplication defined in the neighbourhood of the coordinate origin, via the Campbell-Hausdorff series, produces a local Lie group $g(L)$. An analogous result turned out to be true for Malcev algebras too (Kuz'min, 1971).

Let L be a finite-dimensional Malcev algebra over $\mathbb{R}$ and let G be a local analytic loop, constructed on L, by the Campbell-Hausdorff formula. G is alternative, because L is a binary Lie algebra. Substituting y by $x^{-1}y$ in (6) and multiplying both sides of that equality by x^{-1} on the right, we conclude that, in the class of alternative loops, the Moufang identities are equivalent to the following identity

$$(y \cdot zx)x^{-1} = x(x^{-1}y \cdot z). \tag{6'}$$

Assume that x, y, z are generators of the free Malcev algebra and define a formal alternative loop by series (3), and then denote the left-hand-side of (6′) by $\theta_1(x, y, z)$ and the right-hand-side by $\theta_2(x, y, z)$. Then, we can show that each function θ_i satisfies the following symbolic differential equation

$$y\frac{\partial\theta}{\partial y} - \left[yV^{-1}(z) - \frac{1}{6}J(x, y, z)V(x)\right]\frac{\partial\theta}{\partial z} = 0; \tag{7}$$

this equation induces a system of recurrent relations for the participating functions θ, homogeneous in y. Since the components of the zero power (computable as the values of the functions θ_i, for $y = 0$) also coincide for both functions ($\theta_i(x, 0, z) = (zx)x^{-1} = z$, $\theta_2(x, 0, z) = x(x^{-1}z) = z$), all the other components of these functions are equal, and $\theta_1 = \theta_2$. Thus, a formal Moufang loop is assigned via the Campbell-Hausdorff series to a free Malcev algebra, while a local analytic Moufang loop G corresponds to a finite-dimensional Malcev algebra L; this gives the affirmative answer to the question posed above. Note that, for $x = 0$, equation (7) turns into the defining equation for the functions $\theta(0, y, z) = y \circ z$.

The fundamental results about relations between local Lie groups and global Lie groups carry over to analytic Moufang loops. Namely, every local analytic Moufang loop is locally isomorphic to an analytic global Moufang loop. If G and G' are connected analytic Moufang loops where G is simply connected and if ϕ is a local homomorphism of G to G', then ϕ is uniquely extendable to a homomorphism $\tilde{\phi}$ globally, and if G' is also simply connected and ϕ is a local isomorphism, then $\tilde{\phi}$ is an isomorphism of G to G'. Thus, there exists an up to isomorphism unique simply connected analytic global Moufang loop G with a given tangent Malcev algebra, and every connected analytic Moufang loop G' with the same tangent algebra can be obtained from G by factoring out mod a discrete central normal subgroup. The space of a simply connected analytic Moufang loop, with a solvable tangent Malcev algebra, is homeomorphic to the Euclidean space $\mathbb{R}^n$ (Kerdman, 1979).

The analogous statements in the more general case of binary Lie algebras and analytic alternative loops are incorrect: a finite-dimensional binary Lie algebra over $\mathbb{R}$ may be not a tangent algebra of any global analytic alternative loop.

Example. The unique non-Lie Malcev algebra A of dimension 4 has the following multiplication table: $e_1e_2 = e_3, e_1e_4 = e_1, e_2e_4 = e_2, e_3e_4 = -e_3, e_1e_3 = e_2e_3 = 0$. The algebra A is solvable and is the tangent algebra of an analytic Moufang loop whose space coincides with $\mathbb{R}^4$, while the multiplication in the coordinate form is defined by the following formulas:

$$z_1 = x_1e^{y_4} + y_1, z_2 = x_2e^{y_4} + y_2, z_3 = x_3 + y_3e^{x_4} + x_1y_2 - x_2y_1, z_4 = x_4 + y_4.$$

An interesting generalization of the theory of local analytic Moufang loops is connected with the notion of a Bol loop. A loop G is called a *left Bol loop*, if it satisfies the following identity:

$$(y \cdot zy)x = y(z \cdot yx) \tag{8}$$

(compare with (5)). The loop anti-isomorphic to it satisfies the following identity:

$$(xy \cdot z)y = x(yz \cdot y) \tag{8'}$$

and is called the right Bol loop. Moufang loops are both left and right Bol loops; conversely, the set of identities (8), (8′) implies the identity $xy{\cdot}x = x{\cdot}yx$ (flexibility), therefore left and right Bol loop is a Moufang loop. In the sequel, we mean a left Bol loop, when we speak of a Bol loop.

Example. The set of positive definite Hermitian matrices of order n with the operation of "multiplication" $a \circ b = \sqrt{ab^2a}$ is an analytic global Bol loop. The inversion operation in this loop is an automorphism: $(x \circ y)^{-1} = x^{-1} \circ y^{-1}$. More generally, let G be a group with an involutive automorphism ϕ and assume that the set $\{x \cdot (x\phi)^{-1} \mid x \in G\}$ allows taking unique square roots. Then A is a Bol loop with respect to the operation $a \circ b = \sqrt{ab^2a}$. We remark also that in this case, every element $x \in G$ is uniquely representable in the form $x = ah$, where $a \in A$, $h \in H = \{y \in G \mid y\phi = y\}$, thus A can be identified in a natural way with the space of the left conjugacy classes of G mod H.

The Bol loops are power-associative, thus, they have canonical coordinates of the 1st kind. If G is a local differentiable Bol loop of class $C^k, k \geqslant 5$, then the multiplication operation in G is analytic with respect to the canonical coordinates of the 1st kind. The tangent space T_e of a locally analytic Bol loop is a binary-ternary algebra with anticommutative multiplication and a trilinear operation $[,,]$ satisfying the following identities:

$$[x, x, y] = 0, \tag{9}$$
$$[x, y, z] + [y, z, x] + [z, x, y] = 0, \tag{10}$$
$$[a, b, [x, y, z]] = [[a, b, x], y, z] + [x, [a, b, y], z] + [x, y, [a, b, z]], \tag{11}$$
$$xy \cdot zt = [x, y, zt] - [z, t, xy] + [x, y, t]z - [x, y, z]t. \tag{12}$$

Identities (9)–(12) define the class of *Bol algebras*. In canonical coordinates of 1st kind multiplication in G is expressible through the mentioned operations in $T_e = B(G)$ by the following formula:

$$a \circ b = a + b + \frac{1}{2}ab - \frac{1}{4}(ab^2 - ba^2) + \frac{1}{3}[a, b, b] - \frac{1}{6}[b, a, a] + \dots \tag{13}$$

Thus, to every locally analytic Bol loop G, the tangent Bol algebra $B(G)$ is assigned uniquely. Conversely, every finite-dimensional Bol algebra over the field $\mathbb{R}$ is a tangent algebra of some local analytic Bol loop and two such loops are locally isomorphic if and only if their tangent algebras are isomorphic (Sabinin, Miheev, 1982). In case of Moufang loops, the ternary operation $[,,]$ is expressible through the binary, as follows:

$$[x, y, z] = \frac{1}{3}(2xy \cdot z - yz \cdot x - zx \cdot y), \tag{14}$$

and the series on the right-hand-side of (13) turns into the Campbell-Hausdorff series. Identities (9)–(11) define the so-called class of *Lie triple systems* (L. t. s.). Any Lie algebra is a Lie triple system with respect to the operation of double multiplication or, any of its subspaces closed under this operation; every L. t. s. has a standard embedding into a Lie algebra. Every Jordan algebra is a L. t. s. with respect to the operation $[x, y, z] = (x, z, y)$. A Malcev algebra A is a L. t. s. T_A with respect to operation (14), thus L. t. s. is one of the means of studying Malcev algebras.

Bol loops have an intrinsic application in differential geometry. For example, every locally symmetric affinely connected space X (cf. Helgason, 1962, p. 163; Sabinin, Mikheev, 1985), can be provided, in a natural way, with the structure of a local Bol loop X_e, in a neighbourhood of an arbitrary point $e \in X$; furthermore, e is the unity of the loop X_e and the geodesics, through e, are local one-parameter subgroups. A special role in this case is played by analytic Moufang loops and Malcev algebras: a solution of the problem of describing n-dimensional torsion-free affinely connected spaces, with n independent infinitely small translations is related to them (Sabinin, Mikheev, 1985).

6.3. Some Classes of Loops and Quasigroups. The class of loops closest to groups and most researched is that of Moufang loops. The loop property to be a Moufang loop is universal in the sense of 6.1. The Moufang loops also have the following invariant under isotopy. We introduce a derived operation $x + y = xy^{-1}x$ in a Moufang loop $Q(\cdot)$ and we call $Q(+)$ the core of Q. If two Moufang loops are isotopic, then their cores are isomorphic. The loop property of being a left Bol loop is also universal.

Commutative Moufang loops (CML) have been studied specially thoroughly. They arise in studying rational points on cubic hyperplanes (Manin, 1972) and are characterized by one identity $x^2 \cdot yz = xy \cdot xz$.

Let k be an infinite field and let V be a cubic hypersurface defined over k. By definition, V is defined by a homogeneous equation of the third degree $F(T_0, \ldots, T_n) = 0$, where $(T_0, \ldots, T_n)$ is the system of homogeneous coordinates in the projective space P^n over k. We will assume that the form F is irreducible over the algebraic closure $\overline{k}$ of the field k. Let V_r be the set of non-singular k-points of V (the tangent hyperplane to V is defined in such points). A ternary relation of collineation is introduced on the set V_r: the triple of points (x, y, z) is collinear, if x, y, z are on one line l defined over k which is either contained in V or intersects V only in the points x, y, z (each of the points x, y, z appears as many times as the order of osculation of V with line l at that point). It is obvious that the relation of collineation is symmetric, i.e. is preserved under any permutations of x, y, z; moreover, for every $x, y \in V_r$ there exists a point $z \in V_r$, such that x, y, z are collinear. If z is uniquely determined by given x and y, then by setting $x \circ y = z$ we can define a structure of a totally-symmetric quasigroup on V_r (the equality $a \circ b = c$ is preserved under all the permutations of the symbols a, b, c). For $n > 1$ however, the set V_r does not in general have this property, hence one performs an additional factorization mod a "permissible" equivalence relation S, with a totally-symmetric quasigroup $Q = V_r/S$ as a result. Fixing an arbitrary element E in Q and introducing a new multiplication $(\cdot)$ in Q by the formula $X \cdot Y = E \circ (X \circ Y)$, we get a CML $Q(\cdot)$ with unity E and the identity $x^6 = 1$. The loop $Q(\cdot)$ is locally finite.

Let G be an arbitrary CML and let $(x, y, z) = (xy \cdot z)(x \cdot yz)^{-1}$ be the *associator* of the elements $x, y, z \in G$. We define the descending central series $G = G_0 \geqslant G_1 \geqslant \ldots$ of the loop G, by taking $G_{i+1} (i \geqslant 0)$ to be the subloop generated by the associators of the form $(x, y, z), x \in G_i, y, z \in G$. The loop G is said to be centrally nilpotent of class k, if $G_k = (e)$ and if k is the smallest number with this property.

By the Bruck-Slaby theorem, every n-generated CML is centrally nilpotent of class $\leqslant n-1$ (cf. Bruck, 1958). The intriguing question about the exactness of this estimate had been open for a long time; the affirmative answer was given in 1978 (Malbos, 1978; Smith, 1978; cf. also Bénéteau, 1980).

If two CML are isotopic, then they are isomorphic.

We can arrive at the notion of a Moufang loop in the following way. Let ${}^{-1}x, x^{-1}$ be defined by the equalities ${}^{-1}x \cdot x = x \cdot x^{-1} = e$. A loop G is called an IP-loop (a loop with the inversion property), if it satisfies the identity ${}^{-1}x \cdot xy = yx \cdot x^{-1} = y$ (in this case ${}^{-1}x = x^{-1}$). Every Moufang loop is an IP-loop, because of the alternativity property. If all the LP-isotopes of G (cf. 6.1) are IP-loops, then G is a Moufang loop.

Medial quasigroups, defined by the identity $xu \cdot vy = xv \cdot uy$, appear in various applications. The main theorem for them is the Bruck-Toyoda theorem: Let $Q(\cdot)$ be a medial quasigroup; then there exists an abelian group $Q(+)$ such that $x \cdot y = x\phi + y\psi + c$, where ϕ, ψ are commuting automorphisms of the group $Q(+)$ and c is a fixed element.

Another type of quasigroups has apparently first attracted attention of the algebraists; these are the *distributive quasigroups* satisfying the following identities of the left and the right distributivity:

$$x \cdot yz = xy \cdot xz, \quad yz \cdot x = yz \cdot zx.$$

There is an interesting relation between the distributive quasigroups and the CML: every LP-isotop $Q(\circ)$ of a distributive quasigroup $Q(\cdot)$ is a CML and isomorphic LP-isotopes $Q(\circ)$ correspond to different elements $a \in Q$.

The defining identities of a distributive quasigroup Q mean that the left and the right translations are automorphisms of Q, and they generate respectively the left and the right associated groups. The left associated group of a finite distributive quasigroup is solvable and, moreover, its commutator is nilpotent; furthermore, a finite distributive quasigroup decomposes into the direct product of its maximal p-subquasigroups. The latter result carries over to locally finite distributive quasigroups too.

The following analogue of Moufang's theorem holds for distributive quasigroups: if four elements a, b, c, d are related by the medial law $ab \cdot cd = ac \cdot bd$, then they generate a medial subsemigroup. A distributive quasigroup may be not medial globally. The left distributive identity does not imply the right distributivity. Let $Q(\cdot)$ be a Moufang loop, where the mapping $x \to x^2$ is a permutation, and $Q(+)$ is its core (i.e. $x + y = xy^{-1}x$). Then $Q(+)$ is a left distributive quasigroup, isotopic to a left Bol loop. $Q(+)$ is a distributive quasigroup if and only if $Q(\cdot)$ satisfies the identity $xy^2x = yx^2y$.

Example. Let G be the free group with the identity $x^3 = 1$ and with $r \geqslant 3$ generators. Then G is a finite group of order $3^{m(r)}$, where $m(r) = r + \binom{r}{2} + \binom{r}{3}$; G is a non-associative CML with respect to the operation $x \circ y = x^{-1}yx^{-1}$, and it is a distributive quasigroup, with respect to the operation $x + y = xy^{-1}x$; it is non-medial for $r \geqslant 4$.

A special place in the theory of quasigroups is occupied by the direction related to finding fairly general conditions on the identity of the quasigroup $Q(\cdot)$, so that the operation of multiplication on Q is representable in the form $x \cdot y = x\alpha + y\beta + c$, where $Q(+)$ is a group, α, β are its automorphisms and c is a fixed element. A typical example of such an identity is the medial identity to which the aforementioned Bruck-Toyoda theorem applies. The identity $w_1 = w_2$ is called balanced, if w_1, w_2 are non-associative words of the same composition and every variable occurs in w_1, w_2 only once. A balanced identity $w_1 = w_2$ is called completely cancellable, if w_i contains a subword $u_i, i = 1, 2$, where u_1, u_2 are of the same composition and of length > 1. If a quasigroup satisfies a balanced identity, which is not completely cancellable, then it is isotopic to a group.

6.4. Combinatorial Questions of the Theory of Quasigroups. The class of totally-symmetric quasigroups (TS-quasigroups) that we encountered in 6.3 is interesting from the point of view of combinatorics. It is obvious that this class is defined by the identities $xy = yx$, $x \cdot xy = y$. An idempotent ($x^2 = x$) TS-quasigroup is called a *Steiner quasigroup*. Steiner quasigroups arise in connection to the so-called *Steiner triple systems* studied in combinatorial analysis. A system S of unordered triples (a, b, c) of elements of the set Q is called a Steiner triple system, if the elements of every triple are mutually different and if every pair of elements $a, b \in Q$ occurs in a unique triple $(a, b, c) \in S$. Setting $a \cdot b = c$, if $(a, b, c) \in S$ and $a^2 = a$, we get a Steiner quasigroup; conversely, every Steiner quasigroup $Q(\cdot)$ determines a Steiner triple system S on Q. A finite Steiner quasigroup of order n exists if and only if n is either of the form $6k + 1$ or $6k + 3$. Every distributive quasigroup is an extension of a normal Steiner subquasigroup, by a medial quasigroup. In the above example of a distributive quasigroup, related to the group G of period 3, $G(+)$ is a Steiner quasigroup.

Steiner quadruples are defined analogously to Steiner triplets: every pair of elements $a, b \in Q$ occurs in a unique quadruple $(a, b, c, d) \in S$. The *Stein quasigroups*, satisfying the identities $x \cdot xy = yx, xy \cdot yx = x$ are related to them. Every two different elements a, b of a Stein quasigroup Q generate a subquasigroup of order 4 with the following Cayley table

	a	b	c	d
a	a	c	d	b
b	d	b	a	c
c	b	d	c	a
d	c	a	b	d

Thus, 2-generated subquasigroups in the Stein quasigroup Q form a quadruple Steiner system Q. Conversely, the Stein quasigroup $Q(\cdot)$ is easily constructible on every quadruple Steiner system, with the aid of the Cayley table above. A finite Stein quasigroup of order n exists if and only if n is either of the form $12k + 1$ or $12k + 4$ (Stein, 1964).

If a Stein quasigroup is isomorphic to a group, then the latter must be of nilpotence degree 2.

A number of applications of the theory of quasigroups to the solution of combinatorial questions is based on the close relation between finite quasigroups and the latin squares, mentioned in 6.1. One of the questions of this kind concerns investigations of orthogonal latin squares. Two latin squares of order n are called *orthogonal*, if in their superposition, there are exactly n^2 different ordered pairs of elements. A pair of orthogonal quasigroups corresponds to a pair of orthogonal latin squares. The quasigroups $Q(A)$ and $Q(B)$ (A, B are the multiplication operations on Q) are called orthogonal, if the system of equations $A(x, y) = a$, $B(x, y) = b$ is uniquely solvable, for all $a, b \in Q$. By joint efforts of Bose, Shrikhande and Parker (1960), it was shown that there are orthogonal latin squares of every order $n \neq 2, 6$. Latin squares form an orthogonal system, if they are mutually orthogonal. An orthogonal system of quasigroups (OSQ) corresponds to an orthogonal system of latin squares. The following theorem holds: If $A_1, \ldots A_t$ is an orthogonal set of latin squares of order $n \geqslant 3$, then $t \leqslant n - 1$. For $t = n - 1$, this orthogonal system and the corresponding system of quasigroups are called full. The full OSQ may be constructed with the aid of Galois fields, setting for instance, $A_i(x, y) = x + \lambda_i y$, where $\lambda_i \neq 0$. Thus, for every $n = p^\alpha \geqslant 3$, where p is a prime number, there exists a full OSQ of order n. Full OSQ are related to projective planes (cf. 2.2), since every projective plane may be coordinatized by a full OSQ. Furthermore the following holds:

Theorem. *A projective plane of order $n \geqslant 3$ may be constructed if and only if there exists a full OSQ of order n.*

The OSQ with $k \leqslant n-1$ quasigroups of order n correspond to algebraic k-nets (cf. 6.5), which are generalizations of projective planes.

The multiplication operation in the Stein quasigroup $Q(\cdot)$ is orthogonal to the operation $x \circ y = y \cdot x$. There are six more classes of quasigroups that are definable by identities of the Stein identity type, for which some conditions of orthogonality are satisfied.

The notion of orthogonality is closely related to the notion of a transversal in a latin square. A transversal of a latin square of order n is a sequence of n different elements in different rows and columns of the latin square. A quasigroup is called admissible, if the corresponding latin square contains at least one transversal. In this case the quasigroup has the so-called complete permutation. A permutation θ of elements of $Q(\cdot)$ is called complete, if the mapping $\theta' : x \mapsto x \cdot x\theta$ is also a permutation. For instance, the identity permutation in any group of odd order or, more generally, in a power-associative loop of odd order, is a complete permutation. In the Klein group $K_4 = \{e, a, b, c\}$ the permutation $\theta = \begin{pmatrix} e & a & b & c \\ e & b & c & a \end{pmatrix}$ is a complete permutation, since $\theta' = \begin{pmatrix} e & a & b & c \\ e & c & a & b \end{pmatrix}$. On the other hand, the cyclic groups of even order have no complete permutations, i.e. are not admissible. It is known that the number of different transversals in a group is a multiple of the order of the group.

A quasigroup with an orthogonal quasigroup has a complete permutation. Two permutations ϕ_1, ϕ_2 on the set Q are non-intersecting, if $x\phi_1 \neq x\phi_2$, for every $x \in Q$. The following holds:

Theorem. *A quasigroup Q of order n has an orthogonal quasigroup, if and only if, Q contains n mutually non-intersecting complete permutations.*

A group, on the other hand, has an orthogonal quasigroup if and only if it is admissible.

The existence of a transversal in a quasigroup Q of order n gives a possibility to go from Q to a quasigroup of order $n+1$, if we project the elements of this transversal onto an additional row and column indexed by k, where $k \notin Q$, and place the new element k in their place and in the cell (k, k). This passage from a semigroup of order n to a quasigroup of order $n+1$ is called extension and allows for different generalizations.

The notion of orthogonality of latin squares of order n may be generalized requiring that in their superposition there are exactly r different ordered pairs, $n \leqslant r \leqslant n^2$. In this case the latin squares and the corresponding quasigroups are called r-orthogonal (for $r = n^2$ we get the ordinary orthogonality). In relation to the notion of r-orthogonality, there is a question of describing the spectrum R_n of partial orthogonality of the class of quasigroups of order n, i.e., for every n, finding all the values of r such that there are r-orthogonal quasigroups of order n. This question remains open in general. There are descriptions of the spectrum R_n, for small n: $R_3 = \{3, 9\}, R_4 = \{4, 6, 8, 9, 12, 16\}, R_5 = \{5, 7, 10 - 19, 21, 25\}$.

Example. The following two squares are 12-orthogonal:

1	2	3	4
3	4	1	2
2	1	4	3
4	3	2	1

3	4	2	1
1	3	4	2
4	2	1	3
2	1	3	4

A notion of r-orthogonal systems of quasigroups is introduced in analogy with the OSQ. Up to now, only the $(n+2)$-orthogonal systems of quasigroups of order n have been investigated. It has been proved that the number of quasigroups in systems of this kind does not exceed $2^{[\frac{n}{2}]-1}$ and possibilites of constructing full systems of this kind (i.e. systems with $2^{[\frac{n}{2}]-1}$ quasigroups) over groups have been investigated.

The theory of quasigroups has practical applications, through its combinatorial aspect: in the theory of information coding and in planning experiments.

6.5. Quasigroups and Nets. The notion of a 3-web has a significant role in differential geometry; the algebraic analogue of this notion is that of a 3-net. A family N consisting of objects of two forms – lines l and points p with the incidence relation $p \in l$ is called an *(algebraic) 3-net*, if the set of all the lines $\mathcal{L}$ is divided into three mutually non-intersecting classes $\mathcal{L}_1, \mathcal{L}_2, \mathcal{L}_3$ and if the following conditions hold: 1) every point p is incident to one and only one line in every class; 2) every two lines in different classes are incident to some point p. Instead of "p is incident to l" we will say "p belongs to l", "l contains p". If $P(l) = \{p \mid p \in l\}$, then all the classes $\mathcal{L}_i$ are of the same cardinality as $P(l)$ and are of the same cardinality as some "index" set Q. Let $\phi_i : Q \longrightarrow \mathcal{L}_i$ be some bijective transformations, $i = 1, 2, 3$. Let us introduce the coordinates of lines and points in N. If $\phi_i(a) = l \in \mathcal{L}_i$, then assign the pair $[a, i]$ to the line l. If the lines $[a, 1], [b, 2]$ contain the point p, then assign the pair (a, b) to the point p. Let us define a multiplication operation $(\cdot)$ on Q, setting $a \cdot b = c$, if the line $[c, 3]$ contains the point (a, b). Q is a quasigroup with respect to this operation; mutually isotopic quasigroups correspond to different triples of "index transformations" ϕ_i. Thus a class of isotopic quasigroups uniquely corresponds to every 3-net. Conversely, one can relate with any given quasigroup $Q(\cdot)$ (and its isotopes) the algebraic 3-net N whose lines are the pairs $[a, i]$, $a \in Q$, $i = 1, 2, 3$, and whose points are the pairs (a, b), $a, b \in Q$ with the incidence relation $(a, b) \in [a, 1], [b, 2], [a \cdot b, 3]$.

The closure conditions, that also arose in differential geometry, play a great role in the theory of 3-nets. The points $(a, b), (c, d)$ are called collinear if $a \cdot b = c \cdot d$. It is said that a 3-net N satisfies some closure condition, if collinearity of some pairs of points implies the collinearity of another pair of points. Thus, the closure conditions are equivalent to some quasi-identities of a special form, in the coordinate quasigroup Q. Since the closure conditions do not depend on notation of the lines, they are preserved under isotopy of quasigroups (i.e. have the universal property). In some cases, the closure conditions (quasi identities) are equivalent to the identities in $Q(\cdot)$, which are also universal, i.e. are invariant with respect to the isotopies of loops. An algorithm for constructing the closure figures, corresponding to the universal identities is known (Belousov, Ryzhkov, 1966).

Example 1. The Thomsen condition is of the form $x_1y_2 = x_2y_1$, $x_1y_3 = x_3y_1 \Rightarrow x_2y_3 = x_3y_2$. It is satisfied if and only if $Q(\cdot)$ is isotopic to an abelian group.

Example 2. The Reidemeister condition is of the form $x_1y_2 = x_2y_1$, $x_1y_4 = x_2y_3$, $x_3y_2 = x_4y_1 \Rightarrow x_4y_3 = x_3y_4$. It is satisfied if and only if $Q(\cdot)$ is isotopic to a group.

The notion of a 3-net generalizes to that of k-nets ($k \geqslant 3$), which differ from 3-nets in that there are exactly k lines passing through every point and those lines belong to k different classes $\mathcal{L}_1, \dots, \mathcal{L}_k$. The number k is called the genus of the net. The points and lines of the k-net N may be denoted again as the pairs (a, b), $[a, i]$, where a, b run through the base set $Q, i = 1, \dots, k, [a, i] \in \mathcal{L}_i$. If $[c, i]$ is a line in $\mathcal{L}_i$ passing through the point (a, b), we set $A_i(a, b) = c$; the outcome of this is that we assign the binary operation A_i on Q to every family $\mathcal{L}_i$. Since, for $i \neq j$ the system of equations $A_i(x, y) = a$, $A_j(x, y) = b$ is uniquely solvable for every $a, b \in Q$, the operations $A_1, \dots, A_k$ form an orthogonal system (OSO), which, in particular, may be OSQ. Change of the coordinates of points and lines of k-nets corresponds to an isostrophy of the corresponding OSO (or OSQ); isostrophy is a generalization of isotopy. The order of a k-net is the number of points on every line, i.e. the order of the set Q. The genus k and the order n are connected by the relation $k \leqslant n + 1$. If $k = n + 1$, then such a net is nothing else but an affine plane.

Let $\sum = \{A_i \mid i = 1, \dots, k\}$ be the coordinate OSO. We have a bijective correspondence $\theta_{ij} : (a, b) \longrightarrow (x, y)$, if we assign, to every point (a, b) the intersection point (x, y) of the lines $[a, i]$, $[b, j]$ $(i \neq j)$. Let us denote $A_m\theta_{ij}(a, b) = V_{ijm}(a, b)$; then V_{ijm} is a quasigroup operation on Q. The system $\sum$ of all the quasigroups V_{ijm} is called a covering for $\sum$. A family of points and lines of a k-net N is called a configuration, if there are three lines (edges) of this configuration passing through every point (vertex) of this configuration and if every edge contains at least two vertices. It turns out that some functional equation on the quasigroups in $\overline{\sum}$ corresponds to every configuration in N and conversely. Thus, the configuration with 4 vertices corresponds to the equation of general associativity, the configuration with 5 vertices corresponds to the equation of general distributivity etc.

Even a more general notion of a spacial net is considered in the theory of nets; an orthogonal system of n-ary operations (n-quasigroups) corresponds to them. Such nets have not been studied much up to now and it is partly related to the fact that there are different variants of defining orthogonality for n-quasigroups.

Formation of the quasigroup theory goes back to the beginning of the thirties. It has recently intensively developed in a number of countries (USSR, USA, France, Hungary, etc.) and has become one of the independent parts of modern algebra.

References*

Aczel, J. (1965): Quasigroups, nets and nomograms. Adv. Math. *1*, No. 3, 383–450. Zbl. 135,36

Albert, A.A. (1949): Almost alternative algebras. Portugal Math. *8*, No. 1, 23–36. Zbl. 33,154

Albert, A.A. (1950): A theory of power-associative commutative algebras. Trans. Am. Math. Soc. *69*, 503–527. Zbl. 39,265

Alfsen, E.M., Shultz, F.W., Stormer, E. (1978): A Gelfand-Neumark theorem for Jordan algebras. Adv. Math. *28*, No. 1, 11–56. Zbl. 397.46065

Allison, B.N. (1976): A construction of Lie algebras from J-ternary algebras. Am. J. Math. *98*, No. 2, 285–294. Zbl. 342.17008

Allison, B.N. (1978): A class of nonassociative algebras with involution containing the class of Jordan algebras. Math. Ann. *237*, No. 2, 133–156. Zbl. 368.17001

Ayupov, Sh.A. (1985): Jordan operator algebras. Itogi Nauki Tekh., Ser. Sovrem. Probl. Mat. *27*, 67–98. English transl.: J. Sov. Math. *37*, 1422–1448 (1987). Zbl. 615.46064

Bakhturin, Yu.A., Slin'ko, A.M., Shestakov, I.P. (1981): Non-associative rings. Itogi Nauki Tekh., Ser. Algebra Topologiya Geom. *18*, 3–72. English transl.: J. Sov. Math. *18*, 169–211 (1982). Zbl. 486.17001

Belousov, V.D. (1967): Fundamentals of the theory of quasigroups and loops. Moscow, Nauka. Zbl. 163,18

Belousov, V.D. (1971): Algebraic Nets and Quasigroups. Kishinev, Shtiintsa. Zbl. 245.50005

Belousov, V.D. (1979): Configurations in Algebraic Nets. Kishinev, Shtiintsa. Zbl. 447.94058

Belousov, V.D., Ryzhkov, V.V. (1966): On a way of obtaining closure configurations. Mat. Issled. *1*, No. 2, 140–150. Zbl. 226.20074

Bénéteau, L. (1980): Free commutative Moufang loops and anticommutative graded rings. J. Algebra *67*, No. 1, 1–35. Zbl. 451.20063

Block, R.E. (1968): Determination of A^+ for the simple flexible algebras. Proc. Natl. Acad. Sci. USA *61*, No. 2, 394–397 . Zbl. 198,355

Bokut', L.A., L'vov, I.V., Kharchenko, V.K. (1988): Noncommutative rings. Itogi Nauki Tekh., Ser. Sovrem. Probl. Mat., Fundam. Napravleniya *18*, 5–116. English transl.: Encycl. Math. Sci. *18*, Berlin-Heidelberg-New York, Springer-Verlag, 1–106, 1991. Zbl. 687.16001

Bose, R.C., Shrikhande, S.S., Parker, E.T. (1960): Further results on the construction of mutually orthogonal Latin squares and the falsity of Euler's conjecture. Can. J. Math. *12*, No. 2, 189–203. Zbl. 93,319

* For the convenience of the reader, references to reviews in Zentralblatt für Mathematik (Zbl.), compiled using the MATH database, and Jahrbuch über die Fortschritte in der Mathematik (FdM.) have, as far as possible, been included in this bibliography.

Bott, R., Milnor, J. (1958): On the parallelizability of the spheres, Bull. Am. Math. Soc. *64*, 87–89. Zbl. 82,166

Braun, H., Koecher, M. (1966): Jordan-Algebren. Berlin-Heidelberg-New York, Springer-Verlag. Zbl. 145,260

Bruck, R.H. (1958): A Survey of Binary Systems. Ergebn. Math. *20*, Berlin-Heidelberg-New York, Springer-Verlag. Zbl. 81,17

Bruck, R.H. (1963): What is a loop? Stud. Math. *2*, 59–99. Zbl. 199,52

Chebotarev, N.G. (1940): Theory of Lie Groups. Moscow-Leningrad, Gostekhizdat

Faulkner, J.R. (1970): Octonion planes defined by quadratic Jordan algebras. Mem. Am. Math. Soc. *104*, 1–71. Zbl. 206,233

Faulkner, J.R. (1977): Group with Steinberg Relations and Coordinatization of Polygonal Geometries. Mem. Am. Math. Soc. *185*. Zbl. 391.17002

Filippov, V.T. (1976a): Central simple Malcev algebras. Algebra Logika *15*, No. 2, 235–242. English transl.: Algebra Logic *15*, 147–151 (1977). Zbl. 346.17019

Filippov, V.T. (1976b): On Engel Malcev algebras. Algebra Logika *15*, No. 1, 89–109. English transl.: Algebra Logic *15*, 57–71 (1977). Zbl. 345.17001

Filippov, V.T. (1977): Malcev algebras. Algebra Logika *16*, No. 1, 101–108. English transl.: Algebra Logic *16*, 70–74 (1978). Zbl. 391.17011

Filippov, V.T. (1984): On varieties of Malcev and alternative algebras, generated by the algebras of finite rank. Tr. Inst. Mat. *4*, 139–156. Zbl. 559.17013

Grishkov, A.N. (1980): Structure and representations of binary Lie algebras. Izv. Akad. Nauk SSSR, Ser. Mat. *44*, No. 5, 999–1030. English transl.: Math. USSR, Izv. *17*, 243–269 (1981). Zbl. 468.17007

Grishkov, A.N. (1985): The restricted Burnside problem for Moufang loops of prime exponent. Dokl. Akad. Nauk SSSR *285*, No. 3, 534–536. English transl.: Sov. Math., Dokl. *32*, 714–716 (1985). Zbl. 599.20109

Gvaramiya, A.A. (1985): Classes of quasigroups, invariant under isotopy and abstract classes of reversible automata. Dokl. Akad. Nauk SSSR *282*, No. 5, 1047–1051. English transl.: Sov. Math., Dokl. *31*, 545–549 (1985). Zbl. 601.20064

Hanche-Olsen, H., Störmer, E. (1984): Jordan Operator Algebras. Boston, Pitman, VIII. Zbl. 561.46031

Helgason, S. (1962): Differential geometry and symmetric spaces. New York and London, Academic Press. Zbl. 111,181

Il'tyakov, A.V. (1984): Free alternative algebras of rank 3. Algebra Logika *23*, No. 2, 136–158. English transl.: Algebra Logic *23*, 98–113 (1984). Zbl. 588.17020

Iochum, B. (1984): Cônes Autopolaires et Algèbres de Jordan. Lect. Notes Math. *1049*. Zbl. 556.46040

Iordanescu, R. (1979): Jordan Algebras with Applications. Bucarest

Jacobson, N. (1958): Composition algebras and their automorphisms. Rend. Circ. Mat. Palermo, II. Ser. *7*, No. 1, 55–80. Zbl. 83,27

Jacobson, N. (1968): Structure and Representation of Jordan Algebras. Providence RI, X. Zbl. 218,124

Jacobson, N. (1981): Structure theory of Jordan algebras. The University of Arkansas Lect. Notes Math., Vol. *5*. Zbl. 492.17009

Jordan, P., von Neumann, J., Wigner, E. (1934): On an algebraic generalization of the quantum mechanical formalism. Ann. Math., II. Ser. *35*, 29–64. Zbl. 8,421

Kac, V.G. (1977): Classification of the simple $\mathbb{Z}$-graded Lie superalgebras and simple Jordan superalgebras. Commun. Algebra *5*, No. 13, 1375–1400. Zbl. 367.17007

Kantor, I.L. (1974): Some generalizations of Jordan algebras. Tr. Semin. Vektorn. Tenzorn. Anal. *16*, 406–499. Zbl. 272.17001

Kaplansky, I. (1971): Lie algebras and locally compact groups. The University of Chicago Press, Chicago and London. Zbl. 223.17001

Kaup, W. (1981): Jordan algebras and holomorphy. Lect. Notes Math. *843*, 341–365. Zbl. 466.32014

Kerdman, F.S. (1979): On global analytic Moufang loops. Dokl. Akad. Nauk SSSR *249*, No. 3, 533–536. English transl.: Sov. Math., Dokl. *20*, 1297–1300 (1979). Zbl. 457.22003

Koecher, M. (1962): Jordan algebras and their applications. Univ. Mionnesota Lect. Notes, Minneapolis. Zbl. 128,31

Koecher, M. (1969): An elementary approach to bounded symmetric domains. Rice Univ. Lect. Notes, Houston. Zbl. 217,109

Koecher, M. (1971): Jordan algebras and differential geometry. Actes Congr. Int. Math. 1970 *1*, 279–283. Zbl. 229.17009

Kokoris, L.A. (1956): Simple power-associative algebras of degree two. Ann. Math., II. Ser. *64*, No. 3, 544–550. Zbl. 72,262

Kostrikin, A.I. (1986): Around Burnside. Moscow, Nauka. English transl.: Berlin-Heidelberg-New York, Springer-Verlag 1990. Zbl. 624.17001

Kuz'min, E.N. (1966): On some classes of algebras with division. Algebra Logika *5*, No. 2, 57–102. Zbl. 199,71

Kuz'min, E.N. (1967a): On a class of anticommutative algebras. Algebra Logika *6*, No. 4, 31–50. Zbl. 207,341

Kuz'min E.N. (1967b): On anticommutative algebras satisfying the Engel condition. Sib. Mat. Zh. *8*, No. 5, 1026–1034. English transl.: Sib. Math. J. *8*, 779–785 (1968). Zbl. 172,317

Kuz'min E.N. (1968a): Algebraic sets in Malcev algebras. Algebra Logika *7*, No. 2, 42–47. English transl.: Algebra Logic *7*, 95–97 (1970). Zbl. 204,361

Kuz'min, E.N. (1968b): Malcev algebras and their representations. Algebra Logika *7*, No. 4, 48–69. English transl.: Algebra Logic *7*, 233–244 (1970). Zbl. 204,361

Kuz'min, E.N. (1971): On a relation between Malcev algebras and analytic Moufang loops. Algebra Logika *10*, No. 1, 3–22. English transl.: Algebra Logic *10*, 1–14 (1972). Zbl. 244.17019

Loos, O. (1966): Über eine Beziehung zwischen Malcev-Algebren und Lie-Tripelsystemen. Pac. J. Math. *18*, No. 3, 553–562. Zbl. 145,42

Loos, O. (1975): Jordan Pairs. Lect. Notes Math. *460*. Zbl. 301.17003

Loos, O. (1977): Bounded symmetric domains and Jordan pairs. Univ. California Lecture Notes, Irvine

Loos, O. (1969): Symmetric Spaces. New York-Amsterdam, W.A. Benjamin, Inc. Zbl. 175,486

Mal'tsev, A.I. (= Malcev, A.I.) (1955): Analytic loops. Mat. Sb., Nov. Ser. *36*, No. 3, 569–576. Zbl. 65,7

Malbos, J.-P. (1978): Sur la classe de nilpotence des boucles commutatives de Moufang et des espaces médiaux. C. R. Acad. Sci., Paris, Ser. A *287*, 691–693. Zbl. 409.20051

Manin, Yu.I. (1972): Cubic Forms: Algebra, Geometry, Arithmetic. Moscow, Nauka. English transl.: Amsterdam, North-Holland 1974. Zbl. 255.14002

Markovichev, A.S. (1978): Nilrings of (γ, δ)-type. Algebra Logika *17*, No. 2, 181–200. English transl.: Algebra Logic *17*, 128–142 (1979). Zbl. 412.17002

Mayne, J.H. (1973): Flexible algebras of degree two. Trans. Am. Math. Soc. *172*, 69–81. Zbl. 253.17001

McCrimmon, K. (1966): A general theory of Jordan rings. Proc. Natl. Acad. Sci. USA *56*, No. 4, 1072–1079. Zbl. 139,255

McCrimmon, K. (1978): Jordan algebras and their applications. Bull. Am. Math. Soc. *84*, No. 4, 612–627. Zbl. 421.17010

McCrimmon, K. (1984): The Russian revolution in Jordan algebras. Algebras Groups Geom. *1*, No. 1, 1–61. Zbl. 543.17011

Medvedev, Yu. A. (1985): On nilpotent elements of a free Jordan algebra. Sib. Mat. Zh. *26*, No. 2, 140–148. English transl.: Sib. Math. J. *26*, 271–277 (1985). Zbl. 582.17012

Medvedev, Yu.A. (1988): Representations of finitely generated Jordan PI-algebras. Izv. Akad. Nauk SSSR, Ser. Mat. *52*, No. 1, 64–78. English transl.: Math. USSR, Izv. *32*, No. 1, 63–76 (1989). Zbl. 662.17014

Meyberg, K. (1972): Lectures on algebras and triple systems. Univ. Virginia Lecture Notes, Charlottesville

Mikheev, I.M. (1977): On simple right alternative rings. Algebra Logika *16*, No. 6, 682–710. English transl.: Algebra Logic *16*, 456–476 (1978). Zbl. 401.17009

Myung, H.C. (1982): Lie algebras and flexible Lie-admissible algebras. Nonantum (Mass.), Hadronic Press. Zbl. 533.17001

Myung, H.C. (1986): Malcev-Admissible Algebras. Boston e.a., Birkhäuser, XVI. Zbl. 609.17009

Ng Seong Nam (1984): Local nilpotence of the associator ideal of a (1, 1) algebra. Commun. Algebra *12*, 1125–1137. Zbl. 543.17014

Nikitin, A.A. (1974): Almost alternative algebras. Algebra Logika *13*, No. 5, 501–533. English transl.: Algebra Logic *13*, 287–305 (1975). Zbl. 314.17002

Oehmke, R.H. (1958): On flexible algebras. Ann. Math., II. Ser. *68*, No. 2, 221–230. Zbl. 83,256

Oehmke, R.H. (1962): On commutative algebras of degree two. Trans. Am. Math. Soc. *105*, No. 2, 295–313. Zbl. 133,289

Pchelintsev, S.V. (1984): Solvability and nilpotency of alternative algebras of type $(-1, 1)$. Tr. Inst. Mat. *4*, 81–101. Zbl. 554.17005

Pchelintsev, S.V. (1986): Prime algebras and absolute zero divisors. Izv. Akad. Nauk SSSR, Ser. Mat. *50*, No. 1, 79–100. English transl.: Math. USSR, Izv. *28*, 79–98 (1987). Zbl. 609.17008

Pickert, G. (1955): Projektive Ebenen. Berlin-Göttingen-Heidelberg, Springer-Verlag, VIII, 343 S. Zbl. 66,387

Sabinin, L.V., Mikheev, P.O. (1982): Analytic Bol loops. Webs and quasigroups, Interuniv. Collect. Kalinin 1982, 102–109. Zbl. 499.20044

Sabinin, L.V., Mikheev, P.O. (1985): Theory of Smooth Bol Loops. Moscow, Izdatel'. Zbl. 584.53001

Sagle, A. (1961): Malcev algebras. Trans. Am. Math. Soc. *101*, No. 3, 426–458. Zbl. 101,23

Santilli, R.M. (1978, 1982): Lie-admissible approach to the hadronic structure. Vol. 1 and 2. Nonantum (Mass.), Hadronic Press. Zbl. 455.70001, Zbl. 599.70001

Schafer, R.D. (1952): Representation of alternative algebras. Trans. Am. Math. Soc. *72*, 1–17. Zbl. 46,35

Schafer, R.D. (1966): An Introduction to Nonassociative Algebras. New York, Academic Press, X. Zbl. 145,256

Shestakov, I.P. (1976): Centers of alternative algebras. Algebra Logika *15*, No. 3, 343–362. English transl.: Algebra Logic *15*, 214–226 (1977). Zbl. 402.17019

Shestakov, I.P. (1977): On a problem of Shirshov. Algebra Logika *16*, No. 2, 227–246. English transl.: Algebra Logic *16*, 153-166 (1978). Zbl. 399.17006

Shestakov, I.P. (1983): Finitely generated special Jordan and alternative PI-algebras. Mat. Sb., Nov. Ser. *122*, No. 1, 31–40. English transl.: Math. USSR, Sb. *50*, 31–40 (1985). Zbl. 524.17008

Shestakov, I.P. (1989): Solvable alternative algebras. Sib. Mat. Zh. *30*, No. 6, 219–222. English transl.: Sib. Math. J. *30*, 1019–1022 (1989). Zbl. 708.17029

Shirshov, A.I. (1958): Some questions of theory of near associative rings. Usp. Mat. Nauk *13*, No. 6, 3–20. Zbl. 88,32

Skornyakov, L.A. (1951): Projective planes. Usp. Mat. Nauk *4*, No. 6, 112–154. Zbl. 45,99

Skosyrskij, V.G. (1984): Right alternative algebras. Algebra Logika *23*, No. 2, 185–192. English transl.: Algebra Logic *23*, 131–136 (1984). Zbl. 572.17013

Skosyrskij, V.G. (1985): Right alternative algebras with the minimality condition for the right ideals. Algebra Logika *24*, No. 2, 205–210. English transl.: Algebra Logic *24*, 126–129 (1985). Zbl. 577.17014

Slin'ko, A.M. (1972): A note on radicals and the differentiation of rings. Sib. Mat. Zh. *13*, No. 6, 1395–1397. English transl.: Sib. Math. J. *13*, 984–986 (1973). Zbl. 281.17001

Slin'ko, A.M., Shestakov, I.P. (1974): Right representations of algebras. Algebra Logika *13*, No. 5, 544–588. English transl.: Algebra Logic *13*, 312–333 (1975). Zbl. 342.17003

Smith, J.D.H. (1978): On the nilpotence class of commutative Moufang loops. Math. Proc. Camb. Philos. Soc. *84*, No. 3, 387–404. Zbl. 393.20054

Springer, T.A. (1973): Jordan Algebras and Algebraic Groups. Berlin-Heidelberg-New York, Springer-Verlag, VII. Zbl. 259.17003

Stein, S.K. (1964): Homogeneous quasigroups. Pac. J. Math. *14*, No. 3, 1091–1102. Zbl. 132,265

Stitzinger, E.L. (1983): Engel's theorem for a class of algebras. Pac. J. Math. *107*, No. 1, 245–249. Zbl. 517.17010

Strade, H. (1972): Nodale nichtkommutative Jordanalgebren und Lie-Algebren bei Charakteristik $p > 2$. J. Algebra *21*, No. 3, 353–377. Zbl. 235.17002

Suttles, D.A. (1972): A counterexample to a conjecture of Albert. Notices Am. Math. Soc. *19*, A566

Sverchkov, S.R. (1983): Quasivarieties of special Jordan algebras. Algebra Logika *22*, No. 5, 563–573. English transl.: Algebra Logic *22*, 406–414 (1983). Zbl. 542.17009

Thedy, A. (1978): Right alternative algebras and Wedderburn principal theorem. Proc. Am. Math. Soc. *72*, No. 3, 427–435. Zbl. 405.17002

Tits, J. (1966): Algèbres alternatives, algèbres de Jordan et algèbres de Lie exceptionnelles. Indagationes Math. *28*, No. 2, 223–237. Zbl. 139,32

Tomber, M.L. (1979): A short history of nonassociative algebras. Hadronic J. *2*, No. 6, 1252–1265, 1366–1387. Zbl. 417.17001

Upmeier, H. (1985): Symmetric Banach manifolds and Jordan C^*-algebras. Amsterdam etc., North-Holland. Zbl. 561.46032

Vinberg, Eh.B. (1965): Structure of the automorphism group of a homogeneous convex cone. Tr. Mosk. Mat. O.-va *13*, 56–83. English transl.: Trans. Mosc. Math. Soc. *13*, 63–93 (1967). Zbl. 224.17010

Walcher, S. (1987): On derivations of simple algebras. Algebras Groups Geom. *4*, No. 3, 379–382. Zbl. 643.17002

Zel'manov, E.I. (1982): Absolute zero divisors and the algebraic Jordan algebras. Sib. Mat. Zh. *23*, No. 6, 100–116. English transl.: Sib. Math. J. *23*, 841–854 (1983). Zbl. 526.17012

Zel'manov, E.I. (1983a): On prime Jordan algebras II. Sib. Mat. Zh. *24*, No. 1, 89–104. English transl.: Sib. Math. J. *24*, 73–85 (1983). Zbl. 534.17009

Zel'manov, E.I. (1983b): On prime Jordan triple systems. Sib. Mat. Zh. *24*, No. 4, 23–37. English transl.: Sib. Math. J. *24*, 509–520 (1983). Zbl. 516.17009

Zel'manov (1984): Lie algebras with finite grading. Mat. Sb., Nov. Ser. *124*, No. 3, 353–392. English transl.: Math. USSR, Sb. *52*, 347–385 (1985). Zbl. 546.17005

Zelmanov, E.I., McCrimmon, K. (1988): The structure of strongly prime quadratic Jordan algebras. Adv. Math. *69*, No. 2, 133–222. Zbl. 656.17015

Zelmanov, E.I., Shestakov, I.P. (1990): Prime alternative superalgebras and nilpotence of the radical of a free alternative algebra. Izv. Akad. Nauk SSSR *54*, 676–693. English transl.: Math. USSR, Izv. *37*, No. 1, 19–36 (1991). Zbl. 713.17020

Zhevlakov, K.A., Slin'ko, A.M., Shestakov, I.P., Shirshov, A.I. (1978): Rings that are Nearly Associative. Moscow, Nauka. English transl.: New York, Academic Press 1982. Zbl. 445.17001

Author Index

Subject Index

Kostrikin · Shafarevich (Eds.)

Algebra VI

Combinatorial and Asymptotic Methods of Algebra.
Non-Associative Structures

This book contains two contributions: "Combinatorial and Asymptotic Methods in Algebra" by V. A. Ufnarovskij is a survey of various combinatorial methods in infinite-dimensional algebras, widely interpreted to contain homological algebra and vigorously developing computer algebra, and narrowly interpreted as the study of algebraic objects defined by generators and their relations. The author shows how objects like words, graphs and automata provide valuable information in asymptotic studies. The main methods emply the notions of Gröbner bases, generating functions, growth and those of homological algebra. Treated are also problems of relationships between different series, such as Hilbert, Poincaré and Poincaré-Betti series. Hyperbolic and quantum groups are also discussed. The reader does not need much of background material for he can find definitions and simple properties of the defined notions introduced along the way.

"Non-Associative Structures" by E. N. Kuz'min and I. P. Shestakov surveys the modern state of the theory of non-associative structures that are nearly associative. Jordan, alternative, Malcev, and quasigroup algebras are discussed as well as applications of these structures in various areas of mathematics and primarily their relationship with the associative algebras. Quasigroups and loops are treated too. The survey is self-contained and complete with references to proofs in the literature.

The book will be of great interest to graduate students and researchers in mathematics, computer science and theoretical physics.

ISBN 3-540-54699-5
ISBN 0-387-54699-5