DEFINING RELATIONS OF NONCOMMUTATIVE ALGEBRAS

Vesselin Drensky

Institute of Mathematics and Informatics
Bulgarian Academy of Sciences
Akad. G. Bonchev Str., Block 8, 1113 Sofia, Bulgaria
e-mail: drensky@math.acad.bg

CONTENTS

INTRODUCTION

These lecture notes are based on several talks which I gave in Sofia at the Joint Seminar on Ring Theory of the Institute of Mathematics and Informatics of the Bulgarian Academy of Sciences and the Department of Mathematics and Informatics of the University of Sofia and on the short graduate course on free associative algebras which I was invite to give in June 1998 at the Department of Mathematics of the University of Palermo, Italy. For most of the ring theorists a big part of the theory of an algebra is the theory of its ideals. For most of the algebraists considering ring theory from combinatorial point of view the ideal theory of an algebra is the theory of the generators of the ideals and different numerical invariants which measure how big are the ideals.

The lecture notes are not a comprehensive survey on algebras with defining relations. Their purpose is to present some main results and to illustrate them by some important examples. The references are given in the end of the chapters. They are restricted to several books and survey articles and the sources of the results included in the text. I have tried to make the notes as selves-closed as possible and I hope that they will be useful for introducing the reader in the topic and will prepare him or her to read other books and papers on combinatorial ring theory.

As a result, the notes are concentrated around several topics: Gröbner bases of ideals of free algebras, graded algebras, growth of algebras and their applications.

In commutative algebra Gröbner bases have proved their efficiency and are applied as a powerful tool in the study of many related fields as invariant theory and algebraic geometry. The noncommutative Gröbner bases are more recent objects of investigations but nevertheless they also have a lot of applications.

From the point of view of generators and defining relations the class of graded algebras is easier to study than the class of all algebras. Concerning the numerical invariants of graded algebras, the most important one is the Hilbert series. The consideration of formal power series has the advantage that one can involve usual calculus and the theory of analytic functions.

The growth function of a finitely generated algebra shows “how big” is the algebra. Studying the asymptotic behaviour of the growth function we can “measure” the algebra even if it is infinite dimensional. We can obtain many important properties of the algebra knowing only this asymptotics.

The theory of symmetric functions and graph theory have proved their efficiency in many branches of mathematics and are considered as one of the standard combinatorial tools in algebra.

Most part of the notes consists of applications of the results to concrete problems and concrete algebras. We have constructed examples of algebras with “bad” properties: graded algebras with nonrational Hilbert series; the famous result of Golod and Shafarevich which shows that the number of defining relations of given degree is not too big then the algebra is infinite dimensional and, as a consequence, an example of finitely generated nil algebra which is not nilpotent and a negative solution of the Burnside problem from group theory; algebras with any prescribed Gelfand-Kirillov dimension; algebras with intermediate growth. On the other hand we give examples of algebras with “nice” properties: universal enveloping algebras of Lie algebras, Clifford algebras, etc. These algebras are important not only in combinatorial ring theory. They appear naturally in other branches of mathematics. We have limited the number of general theorems on these algebras. Instead, we have chosen several important algebras and have worked out their defining relations, the corresponding Gröbner bases and the Hilbert series.

I am very grateful to the Department of Mathematics of the University of Palermo and especially to Antonio Giambruno for the kind invitation to give the course, for the financial support, the hospitality and the friendly and creative atmosphere. I am also very thankful to all students and colleagues who attended my talks in Sofia and lectures in Palermo. I am very grateful to many of my colleagues and friends for the useful discussions on combinatorial ring theory and especially to Tatiana Gateva-Ivanova for the conversations on noncommutative Gröbner bases. Finally I am very much obliged to my wife for the the permanent support and the attention to my work while preparing these notes.

1. DEFINING RELATIONS AND GRÖBNER BASES

During all the lecture notes we fix the notation K for an arbitrary field of any characteristic. All considered vector spaces, algebras, modules, tensor products are over K. As usual, we denote by $\mathbb{C},\mathbb{R},\mathbb{Q},\mathbb{Z},\mathbb{N}$ the sets of complex, real, rational, integer and natural numbers; $\mathbb{R}^+$ is the set of positive real numbers and $\mathbb{N}_0 = \mathbb{N}\cup\{0\}$.

Definition 1.1. A vector space A is called an (associative) algebra (or a K-algebra) if A is an associative ring and for any $a,b\in A$ and any $\alpha\in K$

$$\alpha(ab)=(\alpha a)b=a(\alpha b).$$

If not explicitly stated, we assume that the algebras are unitary (or with 1), finitely generated and reserve the symbol A for an algebra. One defines the notions of subalgebras, ideals, homomorphisms, isomorphisms, etc. in the same way as for rings. □

Examples of algebras are the polynomial algebra $K[x_1,\dots,x_m]$ in m commuting variables and the $n\times n$ matrix algebra $M_n(K)$ with entries from K.

Remark 1.2. If the algebra A has a basis as a vector space $\{a_i \mid i\in I\}$, in order to know the multiplication rule in A it is sufficient to know the multiplication table of the basis elements

$$a_ia_j=\sum_{k\in I}\alpha_{ij}^{(k)}a_k,\ \alpha_{ij}^{(k)}\in K,$$

where for fixed i and j only a finite number of $\alpha_{ij}^{(k)}$ are different from 0. □

Definition 1.3. An algebra A without unit is called nil if for any $a\in A$ there exits an $n=n(a)\in\mathbb{N}$ such that $a^n=0$. It is nilpotent of class n if $a_1\dots a_n=0$ for all $a_i\in A$ and $a_1\dots a_{n-1}\neq 0$ for some $a_1,\dots,a_{n-1}\in A$. □

Definition 1.4. For every set X the free associative algebra $K\langle X\rangle$ is the vector space with basis the set of all words

$$x_{i_1}\dots x_{i_n},\ x_{i_j}\in X,\ n=0,1,2,\dots,$$

and multiplication defined by

$$(x_{i_1}\dots x_{i_p})(x_{j_1}\dots x_{j_q})=x_{i_1}\dots x_{i_p}x_{j_1}\dots x_{j_q},\ x_{i_k},x_{j_l}\in X.$$

Sometimes $K\langle X\rangle$ is called the algebra of polynomials in noncommuting variables. Till the end of these notes we shall fix a positive integer m, the set $X=\{x_1,\dots,x_m\}$ and the notation $F=K\langle X\rangle$. We shall also denote by F^+ the free associative algebra without unit, i.e. the basis of F^+ consists of all words $x_{i_1}\dots x_{i_n}$ of length ≥ 1. Sometimes we shall use other symbols, e.g. x,y,z_i, etc. for the elements of X. □

Proposition 1.5. The algebra $K\langle X\rangle$ has the following universal property. For any algebra A and any mapping $\phi : X\to A$ there exists a unique homomorphism (which we denote also by ϕ) $\phi : K\langle X\rangle\to A$ which extends the given mapping $\phi : X\to A$.

Proof. We define a vector space homomorphism $\phi : K\langle X\rangle\to A$ by

$$\phi\left(\sum\alpha_ix_{i_1}\dots x_{i_n}\right)=\sum\alpha_i\phi(x_{i_1})\dots\phi(x_{i_n}),\ \alpha_i\in K.$$

Using the multiplication rules of $K\langle X\rangle$ and A and the definition of ϕ we obtain

$$\phi\left(\left(\sum\alpha_i x_{i_1}\dots x_{i_p}\right)\left(\sum\beta_j x_{j_1}\dots x_{j_q}\right)\right)=\phi\left(\sum\alpha_i\beta_j x_{i_1}\dots x_{i_p}x_{j_1}\dots x_{j_q}\right)=$$

$$=\sum\alpha_i\beta_j\phi(x_{i_1})\dots\phi(x_{i_p})\phi(x_{j_1})\dots\phi(x_{j_q})=$$

$$=\left(\sum\alpha_i\phi(x_{i_1})\dots\phi(x_{i_p})\right)\left(\sum\beta_j\phi(x_{j_1})\dots\phi(x_{j_q})\right)=$$

$$=\phi\left(\sum\alpha_i x_{i_1}\dots x_{i_p}\right)\phi\left(\sum\beta_j x_{j_1}\dots x_{j_q}\right).\quad\square$$

Corollary 1.6. Let the algebra A be generated by $a_1,\dots,a_m$. Then $A\cong K\langle X\rangle/U$ for some ideal U of $K\langle X\rangle$.

Proof. Let us define $\phi: K\langle X\rangle\to A$ by $\phi(x_i)=a_i$, $i=1,\dots,m$. Since $a_1,\dots,a_m$ generate A, the homomorphism ϕ is onto A. The homomorphisms theorem (which is the same as for rings) gives that $A\cong K\langle X\rangle/U$, where $U=\text{Ker}\phi$ is the kernel of ϕ. □

Definition 1.7. Let $A\cong K\langle X\rangle/U$. Any generating set R of the ideal U is called a set of defining relations of A. We say that A is presented by the generating set X and the set of defining relations R and use the notation $A=K\langle X\mid R\rangle$ for the presentation of A or, allowing some freedom in the notation, $A=K\langle X\mid R=0\rangle$. If both sets X and R are finite, we say that A is finitely presented. □

Example 1.8. The polynomial algebra in two variables has the presentation

$$K[x,y]=K\langle x,y\mid xy=yx\rangle.\quad\square$$

We define the commutator (of length 2) by

$$[u_1,u_2]=u_1u_2-u_2u_1$$

and inductively the left-normed commutator of length n by

$$[u_1,\dots,u_{n-1},u_n]=[[u_1,\dots,u_{n-1}],u_n],\ n\geq 3.$$

Examples 1.9. (i) The matrix algebra $M_n(K)$ has the presentation

$$M_n(K)=K\langle x_{ij},\ i,j=1,\dots,n\mid x_{ij}x_{pq}=\delta_{jp}x_{iq}\rangle,$$

where δ_{jp} is the Kronecker symbol defined by $\delta_{jp}=1$ if $j=p$ and $\delta_{jp}=0$ if $j\neq p$.

(ii) If $\dim A=m$ and $\{a_1,\dots,a_m\}$ is a basis of A and the multiplication is given by

$$a_ia_j=\sum_{k=1}^m\alpha_{ij}^{(k)}a_k,$$

then A has a presentation

$$A=K\langle x_1,\dots,x_m\mid x_ix_j=\sum_{k=1}^m\alpha_{ij}^{(k)}x_k\rangle.\quad\square$$

If A is given with its presentation $A=K\langle X\mid R\rangle$ and we want to do calculations in A we face the following problems:

(i) How to express in some "canonical" way the elements of A?

(ii) How to multiply the elements of A?

The solution of these problems is obvious for finite dimensional algebras provided that we know the basis and the multiplication table of the algebra (as in Example 1.9 (ii)). It is also clear how to work with the polynomial algebra in m variables presented as

$$K[X] = K\langle X \mid [x_i, x_j] = 0, i, j = 1, \dots, m\rangle.$$

In the general case the problem cannot be solved algorithmically (see Kharlampovich and Sapir [KS] for detailed survey on algorithmic problems of algebras, rings, groups and semigroups). One of the simplest examples is due to Tsejtin [T]. Let $m = 5$ and let A be defined by the relations

$$[x_1, x_3] = [x_1, x_4] = [x_2, x_4] = 0,$$

$$x_5x_3x_1 = x_3x_5,\ x_5x_4x_2 = x_4x_5,\ x_3x_3x_1x_5 = x_3x_3x_1.$$

Then there exists no algorithm which determines whether an element of A is equal to 0. In other words A has unsolvable word problem.

We introduce the homogeneous lexicographic (or deg-lex) ordering on

$$\langle X\rangle = \{x_{i_1} \dots x_{i_n} \mid n = 0, 1, 2, \dots\}$$

assuming that

$$x_{i_1} \dots x_{i_p} < x_{j_1} \dots x_{j_q}$$

if

(1) $p < q$;

(2) If $p = q$, then there exists k such that $i_1 = j_1, \dots, i_k = j_k$ and $i_{k+1} < j_{k+1}$.

The introduced ordering has the very important property that the set $\langle X\rangle$ is well ordered. This means that any two elements are comparable and any subset of $\langle X\rangle$ has a minimal element. This allows to apply inductive arguments in our considerations.

Definition 1.10. Let (i) $f \in K\langle X\rangle$,

$$f = \alpha u + \sum_{v<u} \beta_v v,\ u, v \in \langle X\rangle, \alpha, \beta_v \in K, \alpha \neq 0.$$

The word $\hat{f} = u$ is called the leading word of f.

(ii) If $B \subset K\langle X\rangle$ we denote by $\hat{B} = \{\hat{f} \mid 0 \neq f \in B\}$ the set of leading words of B.

(iii) The word $w \in \langle X\rangle$ is called normal with respect to $B \subset K\langle X\rangle$ if w does not contain as a subword a word of $\hat{B}$. $\square$

Obviously $\widehat{fg} = \hat{f}\hat{g}$ for any $f, g \in K\langle X\rangle$, $f, g \neq 0$.

Example 1.11. Let $X = \{x, y\}$ and $x < y$.

(i) The set of normal words with respect to $B = \{y^2 - xy\}$ is

$$\{x^{k_1}yx^{k_2}y \dots x^{k_{n-1}}yx^{k_n} \mid k_1, k_n \geq 0, k_2, \dots, k_{n-1} > 0, n = 1, 2, \dots\}.$$

(ii) The set of normal words with respect to $B = \{yx - x^2\}$ is

$$\{x^k y^l \mid k, l \geq 0\}. \quad \square$$

For any ideal U of $K\langle X\rangle$ we denote

$$N = N(U) = \text{span}\{w \in \langle X\rangle \mid \ w \text{ is normal with respect to } U\}$$

the vector space spanned on the set of normal words.

Theorem 1.12. If $U \triangleleft K\langle X\rangle$, then

$$K\langle X\rangle = N(U) \oplus U$$

as a direct sum of vector spaces.

Proof. The intersection $N \cap U = 0$ is obvious because if $0 \neq f \in N \cap U$ then $\hat{f} \in \hat{U}$ and $\hat{f}$ is not normal with respect to U. In order to show the equality $K\langle X\rangle = N + U$ it is sufficient to present any word $w \in \langle X\rangle$ as $w = \bar{w} + u$, $\bar{w} \in N$, $u \in U$. We apply induction on the ordering. If w is normal, then $w \in N$ and $w = w + 0$ (and $0 \in U$). If w is not normal, then there exist $u \in U$, $a, b \in \langle X\rangle$, such that $w = a\hat{u}b$. Using the trivial presentation $w = (w - aub) + aub$ we apply inductive arguments because $aub \in U$ and $w - aub$ is a linear combination of words which are below w in the ordering. □

Definition 1.13. If $U \triangleleft K\langle X\rangle$, we call

$$N = N(U) = \text{span}\{w \in \langle X\rangle \mid \ w \text{ is normal with respect to } U\}$$

the normal complement to U and if $f = \bar{f} + u \in K\langle X\rangle$, $\bar{f} \in N$, $u \in U$, then $\bar{f}$ is the normal form of f. □

In particular, $\bar{f} = 0$ if and only if $f \in U$.

Corollary 1.14. Let $U \triangleleft K\langle X\rangle$ and let N be the normal complement to U. We define on N the multiplication $\bar{f} * \bar{g} = \overline{fg}$, $\bar{f}, \bar{g} \in N$. Then N is isomorphic as an algebra to $A \cong K\langle X\rangle/U$.

Proof. Let $f = \bar{f} + u_f$, $g = \bar{g} + u_g$ for some $u_f, u_g \in U$. Then

$$fg = \bar{f}.\bar{g} + (\bar{f}u_g + u_f\bar{g} + u_fu_g) = \overline{fg} + u_{fg}, \overline{fg} \in N, fg \in U,$$

and modulo U (i.e. in A), $\bar{f}.\bar{g} = \overline{fg}$. □

Definition 1.15. Let $U \triangleleft K\langle X\rangle$. The set $G \subset U$ is called a Gröbner basis of U (or a complete system of defining relations of the algebra $A = K\langle X\rangle/U$) if the sets of normal words with respect to G and U coincide. □

A trivial example of a Gröbner basis of U is U itself.

Proposition 1.16. For any $U \triangleleft K\langle X\rangle$ there exists a minimal (with respect to the inclusion) Gröbner basis.

Proof. Let $\hat{U} = \{\hat{u} \mid u \in U\}$. We fix one u for each $\hat{u}$ and denote by $G_1 = \{u_i \mid i \in I\}$ the obtained set. Now, starting with the words of minimal length in $\hat{G}_1$, by induction we construct a subset $\hat{G}_2$ of $\hat{G}_1$ such that no word of $\hat{G}_2$ is a proper subword of another word of $\hat{G}_2$ and the sets of normal words with respect to $\hat{G}_1$ and $\hat{G}_2$ are the same. Let $G_2 = \{u_i \mid \hat{u}_i \in \hat{G}_2\}$. Since the set of normal words with respect to G_2 is the same as the set of normal words with respect to $\hat{G}_2$ and G_2 is a Gröbner basis of U which is minimal by construction. □

Definition 1.17. If G is a Gröbner basis of $U \triangleleft K\langle X\rangle$ and every element of G has the form

$$g = u + \sum_{v<u} \beta_v v,\ u, v \in \langle X\rangle, \beta_v \in K,$$

where all words v are normal with respect to G, then G is called a reduced Gröbner basis of U. □

Theorem 1.18. The reduced Gröbner basis of $U \triangleleft K\langle X\rangle$ always exists and is unique.

Proof. Let G be a minimal Gröbner basis of U. If $g \in G$ and

$$g = \alpha u + \sum_{v<u} \beta_v v,\ u, v \in \langle X\rangle, \alpha, \beta_v \in K, \alpha \neq 0,$$

then we replace g with $\frac{1}{\alpha}g$, i.e. we may assume that $g = u + \sum_{v<u} \beta_v v$. If some v is not normal with respect to G, then $v = a\hat{u}_v b$ for some $a, b \in \langle X\rangle$ and $\hat{u}_v \in \hat{G}$. Let $u_v \in G$ be the polynomial corresponding to $\hat{u}_v$. In the expression of u we replace v with $v - a\hat{u}_v b$ (which is also in U) and apply induction on the homogeneous lexicographic ordering. In this way we obtain that the reduced Gröbner basis always exits. In order to prove the uniqueness we assume that G_1 and G_2 are two reduced Gröbner bases and again use induction. If $\hat{g}$ is the minimal element of $\hat{G}_1 \cup \hat{G}_2$ and $\hat{g} \in \hat{G}_1$, then $g \in G_1 \subset U$. Hence there exists an $h \in G_2$ such that $\hat{h} \leq \hat{g}$ and the minimality of $\hat{g}$ gives that $\hat{h} = \hat{g}$. Let $g - h \neq 0$. Since $g - h \in U$ and $\widehat{g - h} < \hat{g}$ we obtain a contradiction. In this way $g - h = 0$ and $g = h$. Now, let g be any element of G_1. We define

$$B_i = \{g_0 \in G_i \mid \hat{g}_0 < \hat{g}\},\ i = 1, 2.$$

By induction, $B_1 = B_2$. Similar arguments show that there exists an $h \in G_2$ such that $\hat{h} \leq \hat{g}$. Since G_1 is a reduced Gröbner basis, we obtain that $\hat{h} \notin B_1 = B_2$ and $\hat{h} = \hat{g}$. Again, $g - h \in U$ and $g - h$ is a linear combination of normal words with respect to B_1 and this gives that $g - h = 0$. □

Recall that an oriented graph is a pair of sets $\Gamma = (V, E)$, where V is the set of vertices and the set E of the (oriented) edges of Γ is a subset of $\{(v_1, v_2) \mid v_1, v_2 \in V\}$. If $e = (v_1, v_2) \in E$ is an edge of Γ we say that v_1 is the beginning and v_2 is the end of e. The vertex v is minimal if it is not a beginning of an edge. We allow infinite sets of vertices in the considered graphs. An oriented path in Γ is a sequence of edges

$$e_1 = (v_1, v_2), e_2 = (v_2, v_3), \ldots, e_k = (v_k, v_{k+1})$$

such that the end of each vertex e_i is the beginning of the next edge e_{i+1}. Similarly, deleting the arrows of the edges (i.e. considering Γ as a unoriented graph) we define unoriented paths. The subgraph $\Gamma_1 = (V_1, E_1)$ is called a connected component of Γ if the set of edges of Γ_1 consists of all vertices $(v_1, v_2) \in E$ such that $v_1, v_2 \in V_1 \subset V$ and V_1 is a maximal subset of V with the property that any two vertices $v', v'' \in V_1$ are connected with a unoriented path.

The following lemma is known as the Diamond lemma (see [N, Sect. 3]).

Lemma 1.19. (The Diamond Lemma) Let $\Gamma = (V, E)$ be an oriented graph such that:

(i) It satisfies the descending chain condition, i.e. every oriented path terminates.

(ii) If two edges e_1 and e_2 begin from one vertex u and end respectively in v_1 and v_2, then there exist oriented paths p_1 and p_2 in Γ beginning respectively from v_1 and v_2 and ending to a common vertex w (the "diamond" condition). Then every connected component of Γ has a unique minimal vertex.

Proof. Let $\Gamma_1 = (V_1, E_1)$ be a connected component of Γ with two different minimal vertices v_1, v_2 and let p be a nonoriented path connecting them. Let $v_1 = w_1, w_2, \dots, w_{k-1}, w_k = v_2$ be the sequence of vertices of the path p. Hence for each $j = 1, \dots, k-1$ one of (w_j, w_{j+1}) and (w_{j+1}, w_j) belongs to E_1. We present p as a disjoint union of subpaths $p = p_1 \cup \dots \cup p_s$, where each component p_i is either positive or negative oriented, i.e. going in positive direction, p_i has one of the forms

$$p_i = (w_{k_i}, w_{k_i+1}), (w_{k_i+1}, w_{k_i+2}), \dots, (w_{k_{i+1}-1}, w_{k_{i+1}}),$$

$$p_i = (w_{k_{i+1}}, w_{k_{i+1}-1}), \dots, (w_{k_i+2}, w_{k_i+1}), (w_{k_i+1}, w_{k_i})$$

and the orientation of $p_1, p_2, \dots, p_s$ changes alternatively. Since v_1, v_2 are minimal vertices, the first p_1 is negative oriented and the last path p_s is positive oriented. Using the diamond condition, it is easy to prove by induction that all oriented paths starting from the same vertex v and leading to minimal vertices end in the same minimal vertex. (The obvious base of the induction is for v being minimal.) Since p_1 starts in w_{k_2} and finishes in v_1, going from w_{k_2} through w_{k_3} and continuing to some minimal vertex, we have the only possibility to reach $w_{k_1} = v_1$. Continuing in this way, we see that all paths from w_{k_s} lead to the same minimal vertex v_1. Since there is a path from w_{k_s} to the minimal vertex v_2, we conclude that $v_1 = v_2$ which contradicts with the assumption $v_1 \neq v_2$. □

Definition 1.20. Let the elements of $G \subset K\langle X\rangle$ have the form

$$g = u + \sum_{v<u} \beta_v v,\ u = \hat{g}, v \in \langle X\rangle, \beta_v \in K.$$

We call a reduction (with respect to G) a transformation of $K\langle X\rangle$ of the following kind. Let $f = \gamma_1 w_1 + \dots \gamma_k w_k \in K\langle X\rangle$, where $w_j \in \langle X\rangle$, $0 \neq \gamma_j \in K$, $j = 1, \dots, k$, and some of the words w_i, w_j may be equal. If w_i contains as a subword some $u = \hat{g}$, $g \in G$, e.g. $w_i = aub$, $a, b \in \langle X\rangle$, then we are allowed to replace f with $f_1 = f - \alpha_i agb$. We denote this graphically as $f \to f_1$. □

Clearly, every nontrivial reduction $f \to f_1$ replaces one of the summands $\gamma_j w_j$ with a sum of monomials $-\sum_{v<u} \gamma_j \beta_v avb$ and all avb are below w_j in the homogeneous lexicographic ordering. For example, let

$$G = \{g_1 = x_3x_2 - x_2^2, g_2 = x_2^2 - x_2x_1\},\ f = x_1x_3x_2 + 2x_1x_2^2 + x_1^2x_3.$$

We denote by capitals the symbols which we replace with a reduction. Applying the reduction corresponding to g_1 we obtain

$$f = x_1X_3X_2 + 2x_1x_2^2 + x_1^2x_3 \to f_1 = x_1x_2^2 + 2x_1x_2^2 + x_1^2x_3.$$

Now we are allowed for example to apply the reduction based on g_2 to the second summand:

$$f_1 = x_1x_2^2 + 2x_1X_2^2 + x_1^2x_3 \to f_2 = x_1x_2^2 + 2x_1x_2x_1 + x_1^2x_3$$

or to present f_1 as $f_1' = 3x_1X_2^2 + x_1^2x_3$ and to bring it to $f_2' = 3x_1x_2x_1 + x_1^2x_3$.

We associate to every polynomial $f = \gamma_1 w_1 + \dots \gamma_k w_k \in K\langle X\rangle$, $w_1 \geq \dots \geq w_k$, a k-tuple $\tilde{f} = (w_1, \dots, w_k)$ (where k depends on f) and order the k-tuples lexicographically, i.e.

$$\tilde{f} = (w_1, \dots, w_k) > \tilde{f}' = (w_1', \dots, w_{k'}')$$

if $w_1 = w_1', \dots, w_s = w_s'$ and $w_{s+1} > w_{s+1}'$ for some s. In our example

$$\tilde{f} = (x_1x_3x_2, x_1x_2^2, x_1^2x_3), \tilde{f}_1 = (x_1x_2^2, x_1x_2^2, x_1^2x_3), \tilde{f}_1' = (x_1x_2^2, x_1^2x_3).$$

Theorem 1.21. Let $U \lhd K\langle X\rangle$ and let the subset G of U have the following property. If g_1, g_2 are two different elements of G such that $\hat{g}_1 = ab$, $\hat{g}_2 = bc$ for some $a, b, c \in \langle X\rangle$, respectively $\hat{g}_1 = a\hat{g}_2 b$, $a, b \in \langle X\rangle$, then there exists a sequence of reductions which brings the elements $f = g_1 c - a g_2$, respectively $f = g_1 - a g_2 b$ to 0. Then G is a Gröbner basis of U.

Proof. Let $\Gamma = (V, E)$ be the oriented graph obtained in the following way. The set of vertices V consists of all expressions $f = \gamma_1 w_1 + \dots \gamma_k w_k \in K\langle X\rangle$. Two vertices $f, f_1 \in K\langle X\rangle$ are connected with an oriented edge (f, f_1) if there exists a nontrivial reduction $f \to f_1$. Since f_1 is obtained from f by replacing one of the monomials participating in f with a sum of smaller monomials, every oriented path terminates. Clearly, the minimal vertices of Γ are the polynomials which are in their normal form with respect to G. Now we shall establish that Γ satisfies the diamond condition. Let

$$f = \gamma_1 w_1 + \dots + \gamma_k w_k \in K\langle X\rangle, 0 \neq \gamma_j \in K, w_j \in \langle X\rangle, w_1 \geq \dots \geq w_k.$$

We apply induction on the lexicographical ordering on $\tilde{f} = (w_1, \dots, w_k)$ assuming that for any $f' \in V$ such that $\tilde{f}' < \tilde{f}$ all sequences of reductions bringing f to a minimal vertex terminate in the same minimal vertex. We also assume that if f' and f'' are two vertices corresponding to the same polynomial of $K\langle X\rangle$ and both $\tilde{f}'$ and $\tilde{f}''$ are below $\tilde{f}$, then the normal forms of f' and f'' obtained as a result of reductions are the same. The base of the induction is for the minimal vertices of Γ and is obvious. If some reduction brings f to f_1 related to a k_1-tuple $\tilde{f}_1 = (w_1', \dots, w_{k_1}')$, then $\tilde{f}_1$ is below in the ordering. Let f be a beginning of two edges $e_1 = (f, f_1)$ and $e_2 = (f, f_2)$. Hence there exist two polynomials $g_1, g_2 \in G$ such that

$$g_1 = u_1 + \sum_{v_1 < u_1} \beta_{v_1}' v_1, \; g_2 = u_2 + \sum_{v_2 < u_2} \beta_{v_2}'' v_2,$$

$u_i = \hat{g}_i$, $v_i \in \langle X\rangle$, $i = 1, 2$, $\beta_{v_1}', \beta_{v_2}'' \in K$, and words $a_i, b_i \in \langle X\rangle$, $i = 1, 2$, such that $w_p = a_1 u_1 b_1$, $w_q = a_2 u_2 b_2$. The result of the reductions are the polynomials

$$f_1 = f - \gamma_p a_1 g_1 b_1, \; f_2 = f - \gamma_q a_2 g_2 b_2.$$

We shall consider several possible cases for w_p, w_q and u_1, u_2.

(i) $p \neq q$, e.g. $p = 1$, $q = 2$. Then

$$f = \gamma_1 a_1 u_1 b_1 + \gamma_2 a_2 u_2 b_2 + \sum_{j=3}^{k} \gamma_j w_j,$$

$$f_1 = f - \gamma_1 a_1 g_1 b_1 = -\gamma_1 \sum_{v_1 < u_1} \beta'_{v_1} a_1 v_1 b_1 + \gamma_2 a_2 u_2 b_2 + \sum_{j=3}^{k} \gamma_j w_j,$$

$$f_2 = f - \gamma_2 a_2 g_2 b_2 = \gamma_1 a_1 u_1 b_1 - \gamma_2 \sum_{v_2 < u_2} \beta''_{v_2} a_2 v_2 b_2 + + \sum_{j=3}^{k} \gamma_j w_j.$$

Now we apply to f_1 and f_2 reductions acting respectively on the summands $\gamma_2 a_2 u_2 b_2$ and $\gamma_1 a_1 u_1 b_1$ and replacing f_1 and f_2 with

$$h_1 = f_1 - \gamma_2 a_2 g_2 b_2,\ h_2 = f_2 - \gamma_1 a_1 g_1 b_1.$$

Hence $h_1 = h_2 = f - \gamma_1 a_1 g_1 b_1 - \gamma_2 a_2 g_2 b_2$ which gives the diamond condition and shows that the two edges (f, f_1) and (f, f_2) can be extended to a path with beginning f and with end the same minimal vertex.

(ii) $p = q$, e.g. $p = 1$, $w_1 = a u_1 b u_2 c$ and

$$f_1 = f - \gamma_1 a g_1 b u_2 c,\ f_2 = f - \gamma_1 a u_1 b g_2 c,$$

i.e. the reductions $f \to f_1$ and $f \to f_2$ concern two subwords u_1 and u_2 of w_1 which have no overlap. Then

$$f_1 = -\gamma_1 \sum_{v_1 < u_1} \beta'_{v_1} a v_1 b u_2 c + \sum_{j=2}^{k} \gamma_j w_j,$$

$$f_2 = -\gamma_1 \sum_{v_2 < u_2} \beta''_{v_2} a u_1 b v_2 c + \sum_{j=2}^{k} \gamma_j w_j.$$

As in (i) we apply reductions $f_1 \to h_1$ and $f_2 \to h_2$ acting respectively on the words $a v_1 b u_2 c$ of f_1 and $a u_1 b v_2 c$ of f_2. Since $\tilde{w}_1 \leq \tilde{f}$ and our reductions concern only w_1 we may assume that $f = w_1$,

$$f_1 = - \sum_{v_1 < u_1} \beta'_{v_1} a v_1 b u_2 c, f_2 = - \sum_{v_2 < u_2} \beta''_{v_2} a u_1 b v_2 c.$$

Now we apply reductions replacing respectively u_2 in f_1 and u_1 in f_2:

$$h_1 = f_1 + \sum_{v_1 < u_1} \beta'_{v_1} a v_1 b g_2 c,$$

$$h_2 = f_2 + \sum_{v_2 < u_2} \beta''_{v_2} a g_1 b v_2 c.$$

Hence the results of the reductions are

$$h_1 = h_2 = \sum_{v_1 < u_1} \sum_{v_2 < u_2} \beta'_{v_1} \beta''_{v_2} a v_1 b v_2 c$$

and this is the diamond condition.

(iii) $p = q$, e.g. $p = 1$, $w_1 = a z_1 z_2 z_3 b$, $u_1 = z_1 z_2$, $u_2 = z_2 z_3$, $z_2 \neq 1$, and

$$f_1 = f - \gamma_1 a g_1 z_3 b,\ f_2 = f - \gamma_1 a z_1 g_2 b,$$

i.e. the reductions $f \to f_1$ and $f \to f_2$ concern two subwords u_1 and u_2 of w_1 which have an overlap. As in (ii) we may assume that $f = z_1 z_2 z_3$,

$$f_1 = -\sum_{v_1 < u_1} \beta_{v_1} v_1 z_3, f_2 = -\sum_{v_2 < u_2} \beta'_{v_2} z_1 v_2.$$

Clearly, $\tilde{f}_1, \tilde{f}_2 < \tilde{f}$ and by inductive arguments any two sequences of reductions which bring f_1, respectively f_2, to normal forms with respect to G give the same result h_1, respectively h_2. By assumption (ii) of the theorem, there exists a sequence of reductions which transfers $g_1 z_3 - z_1 g_2$ to 0. Let us write $f_1 - f_2$ in the form

$$f_1 - f_2 = -\sum_{v_1 < u_1} \beta_{v_1} v_1 z_3 + \sum_{v_2 < u_2} \beta'_{v_2} z_1 v_2,$$

without any adduction of similar monomials. Again $\widetilde{f_1 - f_2} < \tilde{f}$ and the induction gives that the normal form of $f_1 - f_2$ obtained as a result of any sequence of reductions is the same polynomial h. Now, applying to the f_1-part of $f_1 - f_2$ first a sequence of reductions which leads f_1 to h_1 and then to the $-f_2$-part a sequence of reductions which brings $-f_2$ to $-h_2$ we obtain that $h = h_1 - h_2$. On the other hand, $f_1 - f_2 = g_1 z_3 - z_1 g_2$ in $K\langle X \rangle$ and, since $g_1 \widetilde{z_3 - z_1} g_2 < \tilde{f}$, by the inductive assumption the normal form of $g_1 z_3 - z_1 g_2$ which is 0, is equal to the normal form of $f_1 - f_2$ which is equal to $h_1 - h_2$. Hence $h_1 = h_2$ and this checks the diamond condition.

(iv) $p = q$, e.g. $p = 1$, $w_1 = a z_1 z_2 z_3 b$, $u_1 = z_1 z_2 z_3$, $u_2 = z_2$, and

$$f_1 = f - \gamma_1 a g_1 b,\ f_2 = f - \gamma_1 a z_1 g_2 z_3 b.$$

This case is similar to (iii).

Now, by the Diamond lemma, each connected component Γ_1 of Γ has a unique minimal vertex h. In order to complete the proof of the theorem it is sufficient to apply the observation that the vertices of Γ_1 are exactly the elements of $h + U$, where U is the ideal of $K\langle X \rangle$ generated by G. Since the minimal vertices are linear combinations of normal words with respect to G, we establish that every normal word with respect to G is also normal with respect to U, i.e. G is a Gröbner basis of U. □

Theorem 1.21 offers the following algorithm for constructing a Gröbner basis of an ideal U generated in $K\langle X \rangle$ by a finite set R.

Algorithm 1.22. The input is a finite set of relations R (and an algebra presented as $A = K\langle X \mid R = 0\rangle$.) The output is the (maybe infinite) reduced Gröbner basis of the ideal generated by R.

Put $G = R$.

Step 1. (Norming) If

$$g = \alpha u + \sum_{v<u} \beta_v v,\ 0 \neq \alpha, \beta_v \in K, u, v \in \langle X\rangle,$$

then replace g by $\frac{1}{\alpha}g$, i.e. make all leading coefficients of $g \in G$ equal to 1.

Step 2. (Reduction) If

$$f = \sum \gamma_w w \in G,\ \gamma_w \in K, w \in \langle X\rangle,$$

and $\hat{g}$ ($g \in G$, $f \neq g$) is a subword of some $w_0 = a\hat{g}b$ in the expression of f, where $a, b \in \langle X\rangle$, then replace f by $f_1 = f - \gamma_{w_0} agb$. In finite number of steps we obtain either that f reduces to 0 and exclude it from G or that f reduces to a linear combination of $\hat{f}$ and normal with respect to G words. Norm this reduced f.

Step 3. (Composition) Let $f, g \in G$ be such that

$$\hat{f} = ab, \hat{g} = bc,\ a, b, c \in \langle X\rangle, b \neq 1.$$

The result of the composition is the normed element $ag - fc$. Add all these elements to G (if different from 0) and apply Step 2. □

Since one of the main applications of Gröbner bases is to present the elements of the algebra in their normal worm, we give an algorithm for this purpose. It follows easily from the proof of Theorem 1.13.

Algorithm 1.23. Let G be the reduced Gröbner basis of the ideal U of $K\langle X\rangle$ and let

$$A = K\langle X\rangle/U = K\langle X \mid G = 0\rangle.$$

Let the generators of A be denoted by the same symbols X. The input is the Gröbner basis U, a polynomial $f = f(X) \in A$ and the output is the normal form of f.

Let $f = \sum \alpha_w w$, $\alpha_w \in K$, $w \in \langle X\rangle$. If some w_0 in the expression of f is not normal with respect to G and w_0 has the form $w_0 = a\hat{g}b$, $g \in G$, $a, b \in \langle X\rangle$, then replace f by $f - \alpha_{w_0} agb$. Continue this procedure until some of the words of the expression of f are not normal. □

Example 1.24. (i) $A = K\langle X \mid yx = x^2\rangle$, $x < y$. Then $R = \{g = yx - x^2\}$, $\hat{R} = \{\hat{g} = yx\}$. There are no possible overlaps and $G = R$. The set of normal words (the basis of A) is

$$\{x^k y^l \mid k, l \geq 0\}.$$

For bringing the elements of A to their normal form, Algorithm 1.23 advises to replace any yx with x^2. As above, we use capitals for YX subject to the replacement. For example

$$xy^2x^3yxy = xy^2x^3YXy = xy^2x^3x^2y = xyYXx^4y = xyx^6y = xYXx^5y = x^8y.$$

(ii) $A = K\langle X \mid y^2 = xy\rangle$ (the same example with exchanged variables). Then $R = \{g = y^2 - xy\}$, $\hat{R} = \{\hat{g} = y^2\}$. There is an overlap $Y^2y = yY^2$ between the elements of $\hat{R}$. Again we use capitals for the words subject to the reduction $y^2 \to xy$:

$$yg - gy = y(y^2 - xy) - (y^2 - xy)y = -yxy + xY^2.$$

Replacing Y^2 we obtain

$$yg - gy - xg = -yxy + x^2y$$

and add the new relation $g_1 = yxy - x^2y$ to G, i.e.

$$G = \{g = y^2 - xy, g_1 = yxy - x^2y\},\ \hat{G} = \{\hat{g} = y^2, \hat{g}_1 = yxy\}.$$

Now the possible overlaps between the elements of $\hat{G}$ are

$$Y^2xy = y(YXY),\ (YXY)y = yxY^2,\ (YXY)xy = yx(YXY).$$

We calculate

$$gxy - yg_1 = yx^2y - xYXY,\ gxy - yg_1 - xg_1 = yx^2y - x^3y$$

and add $g_2 = yx^2y - x^3y$ to G. Continuing in this way we obtain

$$G = \{g_n = yx^ny - x^{n+1}y \mid n = 0, 1, 2, \dots\},\ (g_0 = g).$$

The possible overlaps between the elements of $\hat{G}$ are

$$(YX^nY)x^py = yx^n(YX^pY),$$

which gives

$$g_nx^py - yx^ng_p = -x^{n+1}YX^pY + YX^{n+p+1}Y.$$

Replacing this expression with

$$(g_nx^py - yx^ng_p) + x^{n+1}g_p - g_{n+p+1} = -x^{n+p+2}y + x^{n+p+2}y = 0$$

we see that G is the reduced Gröbner basis of the ideal generated by R and the set of normal words is

$$\{x^k, x^kyx^l \mid k, l \geq 0\}.$$

The algorithm for presenting the elements of A in their normal form replaces the expressions yx^ny with $x^{n+1}y$. For example

$$x^2yx^4yxy^2x = x^2yx^4yxYYx = x^2yx^4yxxyx =$$

$$= x^2YX^4Yx^2yx = x^7YX^2Yx = x^{10}yx. \quad \square$$

Example 1.25. The algebra A is finite dimensional, with basis $\{a_1, a_2, \dots, a_m\}$, $a_1 = 1$, and multiplication table $a_ia_j = \sum_{k=1}^m \alpha_{ij}^{(k)}a_k$. Hence A has the presentation

$$A = K\langle X \mid x_ix_j = \sum_{k=1}^m \alpha_{ij}^{(k)}x_k, i, j = 1, \dots, m\rangle,$$

$$R = \{x_ix_j - \sum_{k=1}^{m} \alpha_{ij}^{(k)} x_k, i, j = 1, \dots, m\}.$$

The set of normal words with respect to R is $\{1\} \cup X \setminus \{x_1\}$. If there are some additional relations in $G \setminus R$, then we shall obtain that some of the normal words are linearly dependent in A which is impossible. Hence $G = R$. □

Example 1.26. (i) (See [B] for the history of the example.) If A has the presentation

$$A = K\langle x_1, x_2, x_3 \mid x_1^2 = x_1, x_2^2 = x_2, x_3^2 = x_3, (x_1 + x_2 + x_3)^2 = x_1 + x_2 + x_3\rangle,$$

is x_1x_2 equal to 0 in A?

We put $G = R = \{g_i = x_i^2 - x_i, i = 1, 2, 3,\ g_0 = (x_1 + x_2 + x_3)^2 - (x_1 + x_2 + x_3)\}$ and start with reduction of g_0:

$$g_0 \to g = g_0 - (g_1 + g_2 + g_3) = \sum_{i \neq j} x_ix_j.$$

Hence in G we replace g_0 with g. The possible overlaps are $\hat{g}_ix_i = X_i^2x_i = x_iX_i^2 = x_i\hat{g}_i$ (which gives no new relations) and

$$\hat{g}_0x_2 = (X_3X_2)x_2 = x_3X_2^2 = x_3\hat{g}_2,\ \hat{g}_3x_2 = X_3^2x_2 = x_3(X_3X_2) = x_3\hat{g}_0.$$

The new reductions may come from $gx_2 - x_3g_2$ and $g_3x_2 - x_3g$. Now (using capitals to show the reduction) we replace X_i^2 by x_i and X_3X_2 by

$$-(x_3x_1 + x_2x_3 + x_2x_1 + x_1x_3 + x_1x_2)$$

and obtain consecutively

$$gx_2 - x_3g_2 = x_3x_1x_2 + x_2X_3X_2 + x_2x_1x_2 + x_1X_3X_2 + x_1X_2X_2 + X_3X_2 \to$$

$$\to x_3x_1x_2 - (x_2 + x_1 + 1)(x_3x_1 + x_2x_3 + x_2x_1 + x_1x_3 + x_1x_2) + x_2x_1x_2 + x_1x_2 =$$

$$= x_3x_1x_2 - x_2x_3x_1 - X_2^2(x_3 + x_1) - x_2x_1x_3 - x_1x_3x_1 - x_1x_2(x_3 + x_1) -$$

$$-X_1^2(x_3 + x_2) - (x_3x_1 + x_2x_3 + x_2x_1 + x_1x_3) \to$$

$$\to h = x_3x_1x_2 - x_2x_3x_1 - x_2x_1x_3 - x_1x_3x_1 - x_1x_2x_3 - x_1x_2x_1 -$$

$$-x_3x_1 - 2x_2x_3 - 2x_1x_3 - x_1x_2.$$

We add this new polynomial h to G. Direct verification shows that the overlap $\hat{g}_3x_2 = X_3^2x_2 = x_3(X_3X_2) = x_3\hat{g}_0$ does not give a new relation because $g_3x_2 - x_3g$ reduces to 0. Now all possible overlaps are

$$\hat{h}x_2 = (X_3X_1X_2)x_2 = x_3x_1X_2^2 = x_3x_1\hat{g}_2,\ \hat{g}_3x_1x_2 = X_3^2x_1x_2 = x_3(X_3X_1X_2) = x_3\hat{h}$$

and direct calculations again give that $hx_2 - x_3x_1g_2$ and $g_3x_1x_2 - x_3h$ both reduce to 0. Hence the reduced Gröbner basis of A is

$$G = \{g_1, g_2, g_3, g, h\}$$

and the normal words with respect to G are the words which do not contain as subwords x_1^2, x_2^2, x_3^2, x_3x_2 and $x_3x_1x_2$. Therefore $x_1x_2 \neq 0$ in A and even x_1x_2 is not a nil element.

(ii) Let A have the presentation

$$A = K\langle x_1, x_2 \mid x_1^2 = x_1, x_2^2 = x_2, (x_1 + x_2)^2 = x_1 + x_2\rangle,$$

i.e. in (i) we have assumed that $x_3 = 0$. Applying Algorithm 1.22 we obtain consecutively

$$G = R = \{g_1 = x_1^2 - x_1, g_2 = x_2^2 - x_2, g_0 = (x_1 + x_2)^2 - (x_1 + x_2)\},$$

$$g_0 \to g_0 - g_1 - g_2 = x_2x_1 + x_1x_2,\ G = \{g_1, g_2, g\}.$$

The possible overlaps come from $X_2^2x_1 = x_2(X_2X_1)$, and

$$g_2x_1 - x_2g = (x_2^2 - x_2)x_1 - x_2(x_2x_1 + x_1x_2) = -(X_2X_1 + X_2X_1x_2) \to$$

$$\to x_1x_2 + x_1X_2^2 \to 2x_1x_2.$$

If char$K \neq 2$, we add to G x_1x_2 and, after reducing g, we add also x_2x_1. Hence $G = \{g_1, g_2, x_2x_1, x_1x_2\}$. It is easy to see that the further overlaps give no new relations and G is the Gröbner basis. The set of normal words is $\{1, x_1, x_2\}$. A direct verification shows that the algebra A has the following presentation as a direct sum of three subalgebras which of them being isomorphic to the base field K:

$$A = K.x_1 \oplus K.x_2 \oplus K.(1 - x_1 - x_2).$$

If char$K = 2$, then the relation $g = 0$ gives that the algebra A is commutative and $G = \{g_1, g_2, g\}$ is the reduced Gröbner basis. The set of normal words is $\{1, x_1, x_2, x_1x_2\}$. Now A can be presented as a direct sum of four fields

$$A = K.x_1x_2 \oplus K.(x_1 + x_1x_2) \oplus K.(x_2 + x_1x_2) \oplus K.(1 + x_1)(1 + x_2). \quad \square$$

One of the important cases when the procedure of finding the Gröbner basis is trivial and it is very easy to work with the presentation of the algebra is the following.

Definition 1.27. The ideal U of $K\langle X\rangle$ is called a monomial ideal if it is generated by a set R of monomials of $\langle X\rangle$. The corresponding algebra with its presentation

$$A = K\langle X \mid R = 0\rangle,\ R \subset \langle X\rangle,$$

is called a monomial algebra. $\square$

Proposition 1.28. Every set R of monomials is a Gröbner basis of the ideal U generated in $K\langle X\rangle$ by R.

Proof. Let $g_1 = u_1u_2$, $g_2 = u_2u_3$ (respectively $g_1 = u_1u_2u_3$, $g_2 = u_2$) be two monomials from R with an overlap. Since both g_1 and g_2 are monomials, $\hat{g}_i = g_i$, $i = 1, 2$, and $g_1u_3 = u_1g_2$ (respectively $g_1 = u_1g_2u_3$) as words in $\langle X\rangle$. Hence $g_1u_3 - u_1g_2 = 0$ (respectively $g_1 = u_1g_2u_3$) and we obtain no new relations. $\square$

The machinery of Gröbner bases can be also developed for one-sided ideals of $K\langle X\rangle$. We give a sketch of the constructions for right ideals.

Definition 1.29. (i) The word $w \in \langle X \rangle$ is r-normal with respect to $G \subset K\langle X \rangle$, if $w \notin \hat{G}\langle X \rangle$, i.e. there exist no words $\hat{g} \in \hat{G}$ and $v \in \langle X \rangle$ such that $w = \hat{g}v$.

(ii) If U is a right ideal of $K\langle X \rangle$, then $G \subset U$ is an r-Gröbner basis of U if the sets of the r-normal words with respect to U and G coincide. As in the case of two-sided ideals, one can define a reduced r-Gröbner basis of U. $\square$

Remark 1.30. Repeating the arguments of the proof of Theorem 1.18, it is easy to see that the reduced r-Gröbner basis of a right ideal always exists and is unique. It is also clear how to construct an r-Gröbner basis of the right ideal U generated by some $u_1, \dots, u_k$. As in Algorithm 1.22 we start with $G = \{u_1, \dots, u_k\}$, (i) norm the polynomials u_i and (ii) make all possible reductions. (If u_i has a summand $\beta(\hat{u}_j v)$, $i \neq j$, then we replace u_i with $u_i - \beta u_j v$.) (iii) Finally, we consider all $\hat{u}_1, \dots, \hat{u}_k$. If $\hat{u}_i = \hat{u}_j v$ for some $i \neq j$, $v \in \langle X \rangle$, then we add to G the polynomial $u_{k+1} = u_i - u_j v$ and go back to Step (ii). $\square$

As an application we shall prove the following theorem of Cohn (see the book of Cohn [C] for alternative approach).

Theorem 1.31. (Cohn) The free algebra $K\langle X \rangle$ is a FIR (a free ideal ring), i.e. every right ideal U is a free right $K\langle X \rangle$-module.

Proof. Let $U \triangleleft_r K\langle X \rangle$. We choose a minimal subset $G \subset U$ such that the sets of r-normal words with respect to G and U coincide, i.e. G is a minimal r-Gröbner basis of U. Then

$$U = \sum_{g_i \in G} g_i K\langle X \rangle.$$

If $g_1 w_1 + \ldots + g_n w_n = 0$ for some $g_i \in G$ and some $w_i \in K\langle X \rangle$, then we have to show that $w_1 = \ldots = w_n = 0$. Let $\hat{g}_1 > \ldots > \hat{g}_n$ and let all w_i be different from 0. From the minimality of G we obtain that $\hat{g}_i$ is not a beginning of $\hat{g}_j$, $i < j$ and the only words beginning with $\hat{g}_1$ come from $\hat{g}_1 w_1$. Hence $\hat{g}_1 w_1 = 0$ and this implies that $w_1 = 0$ which is a contradiction. $\square$

For further readings we recommend e.g. [AL] and [BW] for commutative Gröbner bases, [B], [L], [M] and [U] for more general approach also in the noncommutative case and [BBL] for monomial algebras and related topics.

References

[AL] W.W. Adams, P. Loustaunau, An Introduction to Gröbner Bases, Graduate Studies in Math. **3**, AMS, Providence, R.I., 1994.

[BW] T. Becker, V. Weispfenning (in co-operation with H. Kredel), Gröbner Bases: A Computational Approach to Commutative Algebra, Grad. Texts in Math. **141**, Springer-Verlag, Berlin-New York, 1993.

[BBL] A.Yu. Belov, V.V. Borisenko, V.N. Latyshev, Monomial algebras, Algebra, 4, J. Math. Sci. (New York) **87** (1997), No. 3, 3463-3575.

[B] G.M. Bergman, The diamond lemma in ring theory, Adv. in Math. **29** (1978), 178-218.

[C] P.M. Cohn, Free Rings and Their Relations, Second Edition, Acad. Press, 1985.

[KS] O.G. Kharlampovich, M.V. Sapir, Algorithmic problems in varieties, Intern. J. Algebra Comp. **5** (1995), 379-602.

[L] V.N. Latyshev, Combinatorial Ring Theory. Standard Bases (Russian), Moscow State University, Moscow, 1988.

[M] T. Mora, A survey on commutative and non-commutative Gröbner bases, Theoret. Comput. Sci **134** (1994), 131-173.

[N] M.H.A. Newman, On theories with a combinatorial definition of "equivalence", Ann. Math. **43** (1942), 223-243.

[T] G.S. Tsejtin, Associative calculation with unsolvable equivalence problem (Russian), Trudy Mat. Inst. AN SSSR **52** (1958), 172-189.

[U] V.A. Ufnarovsky, Combinatorial and asymptotic methods in algebra, in A.I. Kostrikin, I.R. Shafarevich (Eds.), "Algebra VI", Encyclopaedia of Mathematical Sciences **57**, Springer-Verlag, 1995, 1-196.

2. FIRST APPLICATIONS OF GRÖBNER BASES

In this chapter we shall apply the technique of Gröbner bases to universal enveloping algebras of Lie algebras and to some other algebras which are close to them.

Definition 2.1. A vector space L with a binary operation (multiplication) $*$ is called a Lie algebra if

$$a * a = 0 \text{ (anticommutativity law)}$$

$$(a * b) * c + (b * c) * a + (c * a) * b = 0 \text{ (the Jacobi identity)}$$

for all $a, b, c \in L$. $\square$

Since $a * a = 0$, $b * b = 0$,

$$0 = (a + b) * (a + b) = a * a + b * b + (a * b + b * a) = a * b + b * a$$

for $a, b \in L$, we obtain that $a * b + b * a = 0$, i.e. the anticommutativity law does imply that the multiplication in L is anticommutative.

Example 2.2. (i) Let $L = \mathbb{R}^3$ be the three-dimensional vector space over $\mathbb{R}$ equipped with the vector multiplication. Then it is easy to check that L is a Lie algebra.

(ii) Let A be any associative algebra and let L be a subspace of A closed under the multiplication

$$a * b = [a, b] = ab - ba,\ a, b \in L.$$

Obviously, $[a, a] = 0$ and direct verification shows that

$$[[a, b], c] + [[b, c], a] + [[c, a], b] = 0,\ a, b, c \in L.$$

Hence L is a Lie algebra. The algebra A is called an enveloping algebra of L. If $L = A$, we shall use the notation $A^{(-)}$ in order to pay attention that we consider A as a Lie algebra. $\square$

Below we shall show that every Lie algebra can be obtained as a subalgebra of some associative algebra.

Definition 2.3. Let L be a Lie algebra and let the associative algebra $U = U(L)$ be an enveloping algebra of L, i.e. $L \subset U^{(-)}$. The algebra U is called the universal enveloping algebra of L if U has the following universal property. For any associative algebra A and any homomorphism of Lie algebras $\phi : L \to A^{(-)}$ there exists a unique homomorphism of associative algebras $\psi : U \to A$ which extends ϕ, i.e. ψ is equal to ϕ on L. $\square$

Theorem 2.4. (The Poincaré-Birkhoff-Witt Theorem) Every Lie algebra L possesses a unique (up to an isomorphism) universal enveloping algebra $U(L)$. If $\{b_i \mid i \in I\}$ is an ordered basis of L and the multiplication of L is given by the multiplication table

$$b_i * b_j = \sum_{k \in I} \alpha_{ij}^{(k)} b_k,\ i, j \in I,$$

then $U(L)$ has the presentation

$$U(L) = K\langle x_i, i \in I \mid [x_i, x_j] - \sum_{k \in I} \alpha_{ij}^{(k)} x_k = 0,\ i, j \in I\rangle.$$

The set

$$G = \{[x_i, x_j] - \sum_{k\in I} \alpha_{ij}^{(k)} x_k \mid i > j, i, j \in I\}$$

is the reduced Gröbner basis of the corresponding ideal of $K\langle X\rangle$ and as a vector space $U(L)$ has a basis

$$\{b_{i_1}^{n_1} \dots b_{i_p}^{n_p} \mid i_1 < \dots < i_p,\ i_k \in I,\ n_i \geq 0,\ p = 0, 1, 2, \dots\}.$$

Proof. We consider the free associative algebra $K\langle X\rangle$, where $X = \{x_i \mid i \in I\}$ and its ideal J generated by the set

$$G = \{[x_i, x_j] - \sum_{k\in I} \alpha_{ij}^{(k)} x_k \mid i > j, i, j \in I\}.$$

Let $U = U(L) = K\langle X\rangle/J$. We use the symbols $\bar{x}_i$ for the generators of U.

First we shall show the universal property of U. Let $\iota : L \to U^{(-)}$ be the vector space homomorphism defined by

$$\iota : \sum_{i\in I} \beta_i b_i \to \sum_{i\in I} \beta_i \bar{x}_i,\ \beta_i \in K.$$

Clearly, ι is also a Lie algebra homomorphism because for any $b_i * b_j$ (and by linearity for any two elements of L),

$$\iota(b_i * b_j) = \iota\left(\sum_{k\in I} \alpha_{ij}^{(k)} b_k\right) = \sum_{k\in I} \alpha_{ij}^{(k)} \iota(b_k) =$$

$$= \sum_{k\in I} \alpha_{ij}^{(k)} \bar{x}_k = [\bar{x}_i, \bar{x}_j] = [\iota(b_i), \iota(b_j)].$$

Let A be an associative algebra and let $\phi : L \to A^{(-)}$ be any Lie algebra homomorphism. Let $\phi(b_i) = a_i \in A$, $i \in I$. We define a homomorphism $\theta : K\langle X\rangle \to A$ by $\theta(x_i) = a_i$, $i \in I$. Since

$$[a_i, a_j] = [\phi(b_i), \phi(b_j)] = \phi(b_i * b_j) = \sum_{k\in I} \alpha_{ij}^{(k)} \phi(b_k) = \sum_{k\in I} \alpha_{ij}^{(k)} a_k,$$

we obtain that

$$[x_i, x_j] - \sum_{k\in I} \alpha_{ij}^{(k)} x_k \in \mathrm{Ker}\theta,\ J \subseteq \mathrm{Ker}\theta,$$

and we can define $\psi : K\langle X\rangle/J \to A$ such that $\phi = \psi \circ \iota$. The uniqueness of ψ is obvious because U is generated by X.

Now we shall see that G is a reduced Gröbner basis of J. Applying Algorithm 1.22, for

$$g_{ij} = [x_i, x_j] - \sum_{k\in I} \alpha_{ij}^{(k)} x_k,\ i > j, i, j \in I,$$

we obtain that $\hat{g}_{ij} = x_i x_j$ and the only overlaps are $(X_i X_j)x_k = x_i(X_j X_k)$, $i > j > k$. We denote

$$x_i * x_j = \sum_{k\in I} \alpha_{ij}^{(k)} x_k$$

and extend the notation $y_1 * y_2$ by linearity on the vector space spanned by X. In particular, since the Lie algebra L is anticommutative and satisfies the Jacobian identity, we have

$$x_i * x_j = -x_j * x_i, (x_i * x_j) * x_k + (x_j * x_k) * x_i + (x_k * x_i) * x_j = 0.$$

Since $g_{ij} = [x_i, x_j] - x_i * x_j$, the reductions replace $x_i x_j$ by $x_j x_i + x_i * x_j$. Let, for example, $i = 3$, $j = 2$, $k = 1$. Then

$$g_{32}x_1 - x_3 g_{21} = (x_3x_2 - x_2x_3 - x_3 * x_2)x_1 - x_3(x_2x_1 - x_1x_2 - x_2 * x_1) =$$

$$= -x_2X_3X_1 - (x_3 * x_2)x_1 + X_3X_1x_2 + x_3(x_2 * x_1) \to$$

$$\to -X_2X_1x_3 - x_2(x_3 * x_1) - (x_3 * x_2)x_1 + x_1X_3X_2 + (x_3 * x_1)x_2 + x_3(x_2 * x_1) \to$$

$$\to -(x_1x_2 + x_2 * x_1)x_3 - x_2(x_3 * x_1) - (x_3 * x_2)x_1 +$$

$$+ x_1(x_2x_3 + x_3 * x_2) + (x_3 * x_1)x_2 + x_3(x_2 * x_1) =$$

$$= -(x_2 * x_1)x_3 - x_2(x_3 * x_1) - (x_3 * x_2)x_1 + x_1(x_3 * x_2) + (x_3 * x_1)x_2 + x_3(x_2 * x_1) =$$

$$-(x_2 * x_1) * x_3 + (x_3 * x_1) * x_2 - (x_3 * x_2) * x_1 =$$

$$= (x_1 * x_2) * x_3 + (x_3 * x_1) * x_2 + (x_2 * x_3) * x_1 = 0.$$

Hence no new relations have to be added to G and G is a Gröbner basis for J. Clearly it is reduced. A word $w \in \langle X \rangle$ is normal with respect to G if w has no subword $x_i x_j$, $i > j$. Hence the set of normal words is

$$\{x_{i_1} \dots x_{i_n} \mid i_1 \leq \dots \leq i_n, n = 0, 1, 2, \dots\}$$

and U has a basis

$$\{\bar{x}_{i_1} \dots \bar{x}_{i_n} \mid i_1 \leq \dots \leq i_n, n = 0, 1, 2, \dots\}.$$

Hence the words $\bar{x}_i$, $i \in I$, are linearly independent in U and this implies that the vector space homomorphism ι is an embedding of L into U. Therefore, we may identify L with $\iota(L) \subset U$. □

Definition 2.5. The free Lie algebra $L(X)$ freely generated by the set X is defined by the universal property: $L(X)$ is generated by X and for any Lie algebra L any mapping $X \to L$ can be extended to a Lie algebra homomorphism $L(X) \to L$. (Compare with the universal property of $K\langle X \rangle$ in Proposition 1.5.) □

Theorem 2.6. (Witt) The free Lie algebra $L(X)$ is isomorphic to the Lie subalgebra of $K\langle X \rangle^{(-)}$ generated by X and $K\langle X \rangle$ is the universal enveloping algebra of $L(X)$.

Proof. Let L be any Lie algebra and let $U(L)$ be the universal enveloping algebra of L. Let $\phi : X \to L$ be any mapping. We extend ϕ to an associative algebra homomorphism (also denoted by ϕ) $\phi : K\langle X \rangle \to U(L)$. (This is possible because $L \subset U(L)$.) Since $\phi([u, v]) = [\phi(u), \phi(v)]$, $u, v \in K\langle X \rangle$, by induction on the length of the commutators we see that

$$\phi([[x_{i_1}, \dots], [\dots, x_{i_n}]]) = [[\phi(x_{i_1}), \dots], [\dots, \phi(x_{i_n})]]$$

belongs to L for any commutator $[[x_{i_1},\dots],[\dots,x_{i_n}]]\in K\langle X\rangle$. Hence the restriction of ϕ on the Lie subalgebra $L(X)$ generated by X in $K\langle X\rangle$ is a Lie algebra homomorphism from $L(X)$ to L. Hence $L(X)$ has the universal property of Definition 2.5 and is isomorphic to the free Lie algebra. Since the universal property of $U(L(X))$ is also satified by $K\langle X\rangle$, this gives that $K\langle X\rangle = U(L(X))$. □

We shall always assume the free Lie algebra $L(X)$ is a Lie subalgebra of $K\langle X\rangle$.

Combining the Poincaré-Birkhoff-Witt theorem with the Witt theorem we obtain immediately the following important corollary which is very important for different applications: computing the dimensions of the homogeneous components of $L(X)$, for concrete calculations with PI-algebras, etc. (see e.g.[Ba], [Bo], [S], [D]).

Corollary 2.7. If $\{u_1,u_2,\dots\}$ is an ordered basis of $L(X)$, then $K\langle X\rangle$ has a basis

$$\{u_1^{n_1}\dots u_p^{n_p}\mid n_i\geq 0\}.\quad \square$$

By analogy with defining relations of associative algebras we can introduce defining relations of Lie algebras. If $L=L(X)/I$ and the ideal I is generated by some set R, then L has the presentation $L=L(X\mid R=0)$ and R is a set of defining relations for L.

Corollary 2.8. If L has the presentation $L=L(X\mid R=0)$, then its universal enveloping algebra $U(L)$ has the presentation $U(L)=K\langle X\mid R=0\rangle$.

Proof. Let I and J be respectively the ideals of $L(X)$ and $K\langle X\rangle$ generated by R. Let

$$\bar{X}=\{\bar{x}_1,\dots,\bar{x}_m\}=\{x_1+I,\dots,x_m+I\}.$$

Since J contains I, we obtain that $K\langle X\rangle/J$ satisfies all relations of L and is a homomorphic image of $U(L)$. Clearly, both L and $U(L)$ are generated by $\bar{X}$ and we have the homomorphisms

$$\nu: K\langle X\rangle\to U(L),\ \pi: U(L)\to K\langle X\rangle/J.$$

Since $U(L)$ also satisfies the relations R, we derive that the kernel of ν contains $J=K\langle X\rangle RK\langle X\rangle$ and obtain that $\mathrm{Ker}\nu=J$, i.e. π is an isomorphism. □

Definition 2.9. (i) The Lie algebra L is nilpotent of class c if $[a_1,\dots,a_{c+1}]=0$ for all a_i in L and there exit $a_1,\dots,a_c\in L$ such that $[a_1,\dots,a_c]\neq 0$. (Pay attention: If $a_1\dots a_{c+1}=0$ for all a_i in the nonunitary associative algebra A and $a_1\dots a_c\neq 0$ for some $a_1,\dots,a_c\in A$, then the associative algebra is nilpotent of class $c+1$.)

(ii) Let the ideals $L^c(X)$ of $L(X)$ be defined inductively by

$$L^1(X)=L(X),\ L^{c+1}(X)=[L^c(X),L(X)],\ c=1,2,\dots,$$

$(L^1(X)\supset L^2(X)\supset\dots$ is called the lower central series of $L(X)$.) The algebra $L(X)/L^{c+1}(X)$ is called the free nilpotent Lie algebra of class c. (It is easy to see that the algebra $L(X)/L^{c+1}(X)$ has the universal property that for any nilpotent of class $\leq c$ Lie algebra L every mapping $X\to L$ can be extended to a homomorphism $L(X)/L^{c+1}(X)\to L$.) □

Example 2.10. The defining relations of the Lie algebra $L(X)/L^{c+1}(X)$ are

$$R=\{[x_{i_1},\dots,x_{i_{c+1}}]\mid x_{i_j}\in X\}.$$

(Using the anticommutativity and the Jacobi identity one can see that every commutator of length $\geq c$ in $L(X)$ and with any brackets decomposition belongs to $L^c(X)$.) $\square$

Definition 2.11. Let V be a vector space with basis $\{e_1, e_2, \dots\}$ and with a symmetric bilinear form $\langle e_i, e_j\rangle = \alpha_{ij} \in K$, $\alpha_{ij} = \alpha_{ji}$, char$K \neq 2$. The Clifford algebra $C(V)$ of V is the algebra with presentation

$$C(V) = K\langle x_1, x_2, \dots \mid x_ix_j + x_jx_i = \alpha_{ij}, i, j = 1, 2, \dots\rangle. \quad \square$$

Theorem 2.12. The defining relations of the Clifford algebra $C(V)$

$$R = \{g_{ij} = x_ix_j + x_jx_i - \alpha_{ij} \mid i \geq j, i, j = 1, 2, \dots\}$$

form a Gröbner basis and $C(V)$ has a basis

$$\{e_{i_1} \dots e_{i_n} \mid i_1 < \dots < i_n, n = 0, 1, 2, \dots\}.$$

Proof. It is sufficient to apply Algorithm 1.22. The possible overlaps for the leading terms of the relations g_{ij} are $(X_iX_j)x_k = x_i(X_jX_k)$, $i \geq j \geq k$. The reductions replace x_ix_j, $i > j$, with $-x_jx_i + \alpha_{ij}$ and x_i^2 with $\frac{1}{2}\alpha_{ii}$. It is sufficient to consider the cases (i) $(i, j, k) = (3, 2, 1)$, (ii) $(i, j, k) = (2, 2, 1)$ and (iii) $(i, j, k) = (2, 1, 1)$.

(i) $g_{32}x_1 - x_3g_{21} = x_2(X_3X_1) - (X_3X_1)x_2 - \alpha_{23}x_1 + \alpha_{12}x_3 \rightarrow$

$$\rightarrow -x_2(x_1x_3 - \alpha_{13}) + (x_1x_3 - \alpha_{13})x_2 - \alpha_{23}x_1 + \alpha_{12}x_3 =$$

$$= -(X_2X_1)x_3 + x_1(X_3X_2) - \alpha_{23}x_1 + \alpha_{12}x_3 \rightarrow$$

$$\rightarrow (x_1x_2 - \alpha_{12})x_3 - x_1(x_2x_3 - \alpha_{23}) - \alpha_{23}x_1 + \alpha_{12}x_3 = 0.$$

(ii) $\frac{1}{2}g_{22}x_1 - x_2g_{21} = (x_2^2 - \frac{1}{2}\alpha_{22})x_1 - x_2(x_2x_1 + x_1x_2 - \alpha_{12}) =$

$$= -\frac{1}{2}\alpha_{22}x_1 - (X_2X_1)x_2 + \alpha_{12}x_2 \rightarrow -\frac{1}{2}\alpha_{22}x_1 + (x_1x_2 - \alpha_{12})x_2 + \alpha_{12}x_2 =$$

$$= -\frac{1}{2}\alpha_{22}x_1 + x_1X_2^2 \rightarrow 0.$$

(iii) This case is similar to (ii). Hence R is a Gröbner basis. In order to make it reduced it is sufficient to norm the relations for $i = j$. $\square$

Definition 2.13. Let V be a vector space with an ordered basis $\{e_1, e_2, \dots\}$. The Grassmann (or exterior) algebra $E(V)$ of V is the associative algebra with presentation

$$E(V) = K\langle x_1, x_2, \dots \mid x_ix_j + x_jx_i = 0, i, j = 1, 2, \dots\rangle, \text{ char}K \neq 2,$$

and is isomorphic to the Clifford algebra with the trivial form $\langle e_i, e_j\rangle = 0$. Hence $E(V)$ has a basis

$$\{e_{i_1} \dots e_{i_n} \mid i_1 < \dots < i_n, n = 0, 1, 2, \dots\}. \quad \square$$

The Grassmann algebra has numerous applications to the theory of superalgebras, algebraic geometry, geometry, algebras with polynomial identities, etc.

Example 2.14. (For this and other examples see [U, Section 2.11].) Let $f = f(t_1,\dots,t_m) \in K[t_1,\dots,t_m]$ be a homogeneous polynomial of degree n. The generalized Clifford algebra is presented as

$$C(n,m,f) = K\langle x_1,\dots,x_m \mid (t_1x_1+\dots+t_mx_m)^n = f(t_1,\dots,t_m)\rangle.$$

The relations should be read in the following way. Assuming that all t_i commute with X, we write

$$(t_1x_1+\dots+t_mx_m)^n = \sum t_1^{n_1}\dots t_m^{n_m} r_{(n_1,\dots,r_m)}(X),$$

$$f(t_1,\dots,t_m) = \sum \alpha_{(n_1,\dots,r_m)} t_1^{n_1}\dots t_m^{n_m}.$$

Then $R = \{r_{(n_1,\dots,r_m)} - \alpha_{(n_1,\dots,r_m)} \mid n_1+\dots+n_m = n\}$. It is known that R is a Gröbner basis. □

References

[Ba] Yu.A. Bahturin, Identitical Relations in Lie Algebras (Russian), "Nauka", Moscow, 1985. Translation: VNU Science Press, Utrecht, 1987.

[Bo] N. Bourbaki, Lie Groups and Lie Algebras. Chapters 1–3, Elements of Math., Springer-Verlag, 1989.

[D] V. Drensky, Codimensions of T-ideals and Hilbert series of relatively free algebras, J.Algebra **91** (1984), 1-17.

[L] S. Lang, Algebra, Addison-Wesley, Reading, Mass. 1965 (Second Edition 1984).

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

[U] V.A. Ufnarovsky, Combinatorial and asymptotic methods in algebra, in A.I. Kostrikin, I.R. Shafarevich (Eds.), "Algebra VI", Encyclopaedia of Mathematical Sciences **57**, Springer-Verlag, 1995, 1-196.

3. GRADED ALGEBRAS

We start with the necessary background on generating functions.

Definition 3.1. Let $a_0, a_1, a_2, \dots$ (or $\{a_n\}_{n\geq 0}$) be a sequence of real (complex) numbers.

(i) The formal power series

$$a(t) = \sum_{n\geq 0} a_n t^n$$

is called the generating function of $\{a_n\}_{n\geq 0}$.

(ii) If $a(t) = \sum_{n\geq 0} a_n t^n$ converges to the rational function $\frac{p(t)}{q(t)}$ in a neighbourhood of 0 for some $p(t), q(t) \in \mathbb{C}[t]$, we say that $a(t)$ is rational. □

The advantage of studying the generating functions instead of the sequence itself is that we may apply the theory of analytic functions or to find some recurrence relations. In particular, we may find a closed formula for a_n or to estimate its asymptotic behaviour.

Definition 3.2. (i) Two sequences $\{a_n\}_{n\geq 0}$ and $\{b_n\}_{n\geq 0}$ are asymptotically equal (notation $a_n \sim b_n$) if $a_n, b_n \neq 0$ for n sufficiently large and

$$\lim_{n\to\infty} \frac{a_n}{b_n} = 1.$$

(ii) If $a(t) = \sum_{n\geq 0} a_n t^n$ and $b(t) = \sum_{n\geq 0} a_n t^n$ and $a_n \geq b_n$ for all n, we write $a(t) \geq b(t)$. □

Proposition 3.3. Let $\{a_n\}_{n\geq 0}$ and $a(t) = \sum_{n\geq 0} a_n t^n$.

(i) The generating function $a(t)$ is rational if and only if $\{a_n\}_{n\geq 0}$ satisfies a linear recurrence relation, i.e. there exist $c_1, \dots, c_k$ such that

$$a_{n+k} = c_1 a_{n+k-1} + c_2 a_{n+k-2} + \dots + c_k a_n,\ n \geq 0.$$

(ii) If all a_n are rational and $\{a_n\}_{n\geq 0}$ satisfies a linear recurrence relation, then

$$a(t) = \frac{p(t)}{q(t)} \in \mathbb{Q}(t).$$

Proof. (i) Let $a(t) = \frac{p(t)}{q(t)} \in \mathbb{C}(t)$, where

$$p(t) = \sum_{i=0}^{k} p_i t^i,\ q(t) = \sum_{j=0}^{l} q_j t^j,\ q_0 \neq 0.$$

Since $p(t) = q(t)a(t)$, we obtain

$$p(t) = \sum_{i=0}^{k} = \left(\sum_{j=0}^{l} q_j t^j\right)\left(\sum_{n\geq 0} a_n t^n\right) = \sum_{n\geq 0}\left(\sum_{j=0}^{l} q_j a_{n-j}\right) t^n.$$

Hence for $n > k$, $n \geq l$,

$$q_0 a_n + q_1 a_{n-1} + \dots + q_l a_{n-l} = 0,$$

$$a_n = -\frac{1}{q_0}(q_1a_{n-1} + \ldots + q_la_{n-l})$$

which gives the linear recurrence relation.

Now, let

$$a_{n+k} = c_1a_{n+k-1} + \ldots + c_ka_n,\ n = 0, 1, 2, \ldots$$

Multiplying these equations with t^{n+k} and taking their formal sum, we obtain

$$\sum_{n\geq k} a_nt^n = c_1t \sum_{n\geq k-1} a_nt^n + \ldots + c_kt^k \sum_{n\geq 0} a_nt_n,$$

$$a(t) - \sum_{i=0}^{k-1} a_it^i = c_1t\left(a(t) - \sum_{i=0}^{k-2} a_it^i\right) + \ldots + c_{k-1}t^{k-1}(a(t) - a_0) + c_kt^ka(t)$$

and $a(t)(1 - c_1t - c_2t^2 - \ldots - c_kt^k)$ is equal to a polynomial $p(t)$. Hence $a(t)$ is equal to the rational function $\frac{p(t)}{q(t)}$, where $q(t) = 1 - c_1t - c_2t^2 - \ldots - c_kt^k$.

(ii) If all a_n are rational, then in the second part of the proof of (i) we obtain that $p(t), q(t) \in \mathbb{Q}[t]$ and $a(t) \in \mathbb{Q}(t)$. □

Definition 3.4. Let $\{a_n\}_{n\geq 0}$ be a sequence of complex numbers.

(i) If there exist positive b and c such that $|a_n| \leq bn^c$ for all n, we say that the sequence $\{a_n\}_{n\geq 0}$ is with polynomial growth. (We use this terminology although it is more precise to say that the growth of $\{a_n\}_{n\geq 0}$ is polynomially bounded.)

(ii) If there exist $b_1, b_2 > 0$, $c_1, c_2 > 1$ and a subsequence $\{a_{n_k}\}_{k\geq 0}$ such that

$$b_1c_1^{n_k} \leq |a_{n_k}| \leq b_2c_2^{n_k},$$

then $\{a_n\}_{n\geq 0}$ is with exponential growth.

(iii) If for any $b, c > 0$ there exists a subsequence $\{a_{n_k}\}_{k\geq 0}$ such that $|a_{n_k}| > bn_k^c$ and for any $b_1 > 0$, $c_1 > 1$ the inequality $|a_n| < b_1c_1^n$ holds for all sufficiently large n, then $\{a_n\}_{n\geq 0}$ is of intermediate growth. □

Theorem 3.5. If

$$a(t) = \sum_{n\geq 0} a_nt^n = \frac{p(t)}{q(t)} \in \mathbb{C}(t),$$

then the sequence $\{a_n\}_{n\geq 0}$ is either of polynomial or of exponential growth.

Proof. Let $a(t) = \frac{p(t)}{q(t)}$, $p(t), q(t) \in \mathbb{C}[t]$. Since $a(0) = a_0$, we obtain that 0 is not a pole of $a(t)$ and we may assume that $q(0) \neq 0$. Let

$$q(t) = q_0 \prod_{i=1}^{d} (1 - \alpha_it)^{k_i},$$

where $\alpha_1, \ldots, \alpha_d \in \mathbb{C}$ are the different zeros of $q(t)$. Hence

$$a(t) = b(t) + \sum_{i=1}^{d} \sum_{j=1}^{k_j} \frac{\beta_{ij}}{(1 - \alpha_it)^j},\ b(t) \in \mathbb{C}[t], \beta_{ij} \in \mathbb{C}.$$

Using the formula

$$\frac{1}{(1-t)^k} = \sum_{n\geq 0} \binom{n+k-1}{k-1} t^n,$$

we obtain that for $n > \deg b(t)$

$$a_n = b_1(n)\alpha_1^n + \ldots + b_d(n)\alpha_d^n,$$

where $b_i(n)$ are polynomials of n.

(i) If $|\alpha_i| \leq 1$ for all nonzero polynomails $b_i(n)$, then $\{a_n\}_{n\geq 0}$ is with polynomial growth.

(ii) Let $a_n = b_1(n)\alpha_1^n + \ldots + b_k(n)\alpha_k^n$, where all $b_i(n)$ are nonzero polynomials. Let

$$r = |\alpha_1| = \ldots = |\alpha_l| > |\alpha_{l+1}| \geq \ldots \geq |\alpha_k|,\ r > 1,$$

$$s = \deg b_1(n) = \ldots = \deg b_m(n) > \deg b_{m+1}(n) \geq \ldots \geq \deg b_l(n).$$

Then

$$\limsup_{n\to\infty} \left|\frac{a_n}{n^s r^n}\right| =$$

$$\limsup_{n\to\infty} \frac{1}{n^s}\left|b_1(n)\left(\frac{\alpha_1}{r}\right)^n + \ldots + b_m(n)\left(\frac{\alpha_m}{r}\right)^n\right| =$$

$$= \limsup_{n\to\infty} |\beta_1\varepsilon_1^n + \ldots + \beta_m\varepsilon_m^n|$$

for some nonzero $\beta_1, \ldots, \beta_m \in \mathbb{C}$ and where $|\varepsilon_i| = 1$, $i = 1, \ldots, m$. It is sufficient to show that

$$\limsup_{n\to\infty} |\beta_1\varepsilon_1^n + \ldots + \beta_m\varepsilon_m^n| > 0.$$

This will imply that $|a_n| \leq \text{const.}n^s r^n$ and that for every $r_1 \in \mathbb{R}$, $1 < r_1 < r$ we can find a subsequence $\{a_{n_i}\}_{i\geq 0}$ such that $|a_{n_i}| > \text{const.}r_1^n$, which means that the growth of $\{a_n\}_{n\geq 0}$ is exponential. Let

$$c_n = \beta_1\varepsilon_1^n + \ldots + \beta_m\varepsilon_m^n.$$

Since $|c_n|$ is bounded it is sufficient to assume that $\lim_{n\to\infty} c_n = 0$ and to reach a contradiction. Let $\lim_{n\to\infty} c_n = 0$. Hence

$$c_{n+l} = (\beta_1\varepsilon_1^n)\varepsilon_1^l + \ldots + (\beta_m\varepsilon_m^n)\varepsilon_m^l = \delta_{n+l},\ l = 0, 1, \ldots, m-1.$$

We consider these m equations as a linear system with unknowns $\beta_1\varepsilon_1^n, \ldots, \beta_m\varepsilon_m^n$. The determinant of the system is the Vandermonde determinant and is different from 0. Hence the solutions of the system are

$$\beta_i\varepsilon_i^n = \sum_{j=0}^{m-1} \gamma_{ij}\delta_{n+j},$$

where γ_{ij} depends on ε_{ij}^l only, $i = 1, \ldots, m$, $l = 0, 1, \ldots, m-1$. Since $\lim_{n\to\infty} \delta_n = 0$, we obtain that $\lim_{n\to\infty} \beta_i\varepsilon_i^n = 0$. Since $|\varepsilon_i| = 1$, this means that $\lim_{n\to\infty} \beta_i = \beta_i = 0$ which is impossible. □

Corollary 3.6. If $a_n \in \mathbb{Z}$, $n = 0, 1, 2, \ldots$, and

$$a(t) = \sum_{n\geq 0} a_n t^n \in \mathbb{Q}(t),$$

then the radius of convergency r of $a(t)$ is either equal to ∞ or $r \in (0,1]$.

Proof. If $a(t) \in \mathbb{Q}[t]$, then $r = \infty$. If $a(t)$ is not a polynomial, then $\{a_n\}_{n\geq 0}$ satisfies a recurrence relation and for some d and k the coefficients a_{dn+k} are not equal to 0. (Prove it!) Hence

$$\sum_{n\geq 0} |a_n| t^n \geq t^k(1 + t^d + t^{2d} + \dots) = \frac{t^k}{1 - t^d}.$$

Hence $r \leq 1$. The inequality $r > 0$ follows from Theorem 3.6. There exist $b > 0$, $c > 1$ such that $a_n \leq bc^n$ and r is bigger or equal to the radius of convergence $\frac{1}{c}$ of $b(1 + ct + c^2t^2 + \dots)$. $\square$

Definition 3.7. (i) The vector space V is graded if it is a direct sum of subspaces $V = V^{(0)} \oplus V^{(1)} \oplus V^{(2)} \oplus \dots$. The subspace $V^{(n)}$ is the homogeneous component of degree n of V. Similarly, V is multigraded, if for a fixed m it is a direct sum

$$V = \sum{}^{\oplus} V^{(n_1,\dots,n_m)}$$

of its (multi)homogeneous components $V^{(n_1,\dots,n_m)}$, where the summation runs over all $n_i \in \mathbb{Z}$, $n_i \geq 0$. Sometimes it is more convenient to use subscripts V_n instead of $V^{(n)}$ but we prefer the latter notation.

(ii) If $V = \sum^{\oplus} V^{(n)}$, $W \subset V$ and $W = \sum^{\oplus}(W \cap V^{(n)})$, then W is a graded subspace of V and hence V/W inherits the grading of V. We always shall consider W and V/W as graded vector spaces with respect to this grading. $\square$

Example 3.8. (i) The vector space $V = K[X]$ is graded assuming that $V^{(n)}$ is the vector space of all homogeneous polynomials of degree n. Similarly (assuming as usually that $X = \{x_1,\dots,x_m\}$) $V = K[X]$ is multigraded, where $V^{(n_1,\dots,n_m)}$ is the one-dimensional vector space spanned by $x_1^{n_1}\dots x_m^{n_m}$.

(ii) The free algebra $V = K\langle X\rangle$ is graded and multigraded in the same way as $K[X]$, i.e. $V^{(n)}$ is spanned by all products $x_{i_1}\dots x_{i_n}$ and $V^{(n_1,\dots,n_m)} \subset V^{(n)}$, $n_1 + \dots + n_m = n$, is spanned on these $x_{i_1}\dots x_{i_n}$ which contain exactly n_i symbols x_i. $\square$

Definition 3.9. If $V = \sum^{\oplus}_{n\geq 0} V^{(n)}$ is a graded vector space and $\dim V^{(n)} < \infty$ for all $n \geq 0$, then the Hilbert (or Poincaré) series of V is the formal power series

$$H(V,t) = \sum_{n\geq 0} \dim V^{(n)} t^n.$$

Similarly, if $V = \sum^{\oplus} V^{(n_1,\dots,n_m)}$, $\dim V^{(n_1,\dots,n_m)} < \infty$, then we define the Hilbert series in m variables by

$$H(V,t_1,\dots,t_m) = \sum \dim V^{(n_1,\dots,t_m)} t_1^{n_1}\dots t_m^{n_m}. \quad \square$$

Recall that for vector spaces V and W with bases respectively $\{v_i \mid i \in I\}$, $\{w_j \mid j \in J\}$, the tensor product $V \otimes W = V \otimes_K W$ is the vector space with basis $\{v_i \otimes w_j \mid i \in I, j \in J\}$. If $V = \sum^{\oplus}_{n\geq 0} V^{(n)}$, $W = \sum^{\oplus}_{n\geq 0} W^{(n)}$ are graded, then the direct sum $V \oplus W$ and the tensor product $V \otimes W$ are also graded assuming that

$$(V \oplus W)^{(n)} = V^{(n)} \oplus W^{(n)},\ (V \otimes W)^{(n)} = \sum_{k=0}^{n}{}^{\oplus} \left(V^{(k)} \oplus W^{(n-k)}\right).$$

We can easily obtain the following formulas for the Hilbert series of $V \oplus W$ and $V \otimes W$:

$$H(V \oplus W, t) = H(V, t) + H(W, t),\ H(V \otimes W, t) = H(V, t)H(W, t).$$

If $W \subset V$, then

$$H(V, t) = H(W, t) + H(V/W, t).$$

There are also similar definitions of grading and relations for Hilbert series of multigraded vector spaces.

Example 3.10. (i) For the polynomial algebra in one variable

$$K[x] = K \oplus Kx \oplus Kx^2 \oplus \dots$$

Hence $\dim(K[x])^{(n)} = 1$ and

$$H(K[x], t) = 1 + t + t^2 + \dots = \frac{1}{1-t}.$$

Since

$$K[x_1, \dots, x_m] \cong K[x_1, \dots, x_{m-1}] \otimes K[x_m]$$

as graded vector spaces, by easy induction we obtain

$$H(K[x_1, \dots, x_m], t) = H(K[x_1, \dots, x_{m-1}], t)H(K[x_m], t) =$$

$$= \frac{1}{(1-t)^{m-1}} \frac{1}{1-t} = \frac{1}{(1-t)^m},$$

$$H(K[x_1, \dots, x_m], t_1, \dots, t_m) = \prod_{i=1}^{m} \frac{1}{1-t_i}.$$

(ii) The homogeneous component of degree n of free associative algebra $K\langle X\rangle$ has a basis

$$\{x_{i_1} \dots x_{i_n} \mid i_j = 1, \dots, m\}.$$

Hence $\dim(K\langle X\rangle)^{(n)} = m^n$ and the Hilbert series of $K\langle X\rangle$ is

$$H(K\langle X\rangle, t) = 1 + mt + m^2t^2 + \dots = \frac{1}{1-mt}.$$

Since as graded vector spaces

$$K\langle X\rangle = K \oplus x_1K\langle X\rangle \oplus \dots \oplus x_mK\langle X\rangle,$$

$$H(K\langle X\rangle, t_1, \dots, t_m) = 1 + \sum_{i=1}^{m} t_i H(K\langle X\rangle, t_1, \dots, t_m),$$

$$\left(1 - \sum_{i=1}^{m} t_i\right) H(K\langle X\rangle, t_1, \dots, t_m) = 1,$$

$$H(K\langle X\rangle, t_1, \dots, t_m) = \frac{1}{1-(t_1 + \dots + t_m)}. \quad \square$$

Studying the Hilbert series of finitely generated commutative graded algebras A provides a lot of information about the algebras themselves (see e.g. [AM]). In particular, the Hilbert-Serre theorem gives that $H(A,t) \in \mathbb{Q}(t)$.

Now we shall show that in the noncommutative case the situation is more complicated. We shall construct some exotic examples of graded algebras with nonrational Hilbert series.

Theorem 3.11. There exists a two-generated graded algebra with a nonrational Hilbert series.

Proof. Let $X = \{x, y\}$, $I \subset \mathbb{N}_0$,

$$R_I = \{zyx^k y, yx^k yz, yx^i y \mid k \geq 0, z = x, y, i \in I\},$$

$A_i = K\langle x, y \mid R_I = 0\rangle$. Since R_I consists of monomial relations, Proposition 1.28 gives that R_I is a Gröbner basis of the ideal $(R_I) \triangleleft K\langle x, y\rangle$ and the set of normal words with respect to R_I is a basis of A_I. Hence A_I has a homogeneous basis

$$\{x^k, x^k yx^l, yx^j y \mid k, l \geq 0, j \in \mathbb{N}_0 \setminus I\}$$

and the Hilbert series of A_I is

$$H(A,t) = \sum_{k \geq 0} t^k + t \sum_{k,l \geq 0} t^k t^l + t^2 \sum_{j \in \mathbb{N}_0 \setminus I} t^j =$$

$$\frac{1}{1-t} + \frac{t}{(1-t)^2} + \frac{t^2}{1-t} - t^2 \sum_{i \in I} t^i.$$

Clearly, $H(A_I, t)$ is a rational function if and only if $f_I(t) = \sum_{i \in I} t^i$ is rational. Let $f_I(t)$ be rational. Then Proposition 3.3 gives that $f_I(t) \in \mathbb{Q}(t)$. Now we have two possibilities to complete the proof.

Aproach 1. Since the set of rational fuctions with rational coefficients is countable it is sufficient to construct a continuum of different functions $f_I(t)$. Since the functions $f_I(t)$ are in one-to-one correspondence with the subsets I of $\mathbb{N}_0$, we obtain that there exists a set I with a nonrational function $f_I(t)$.

Approach 2. If the formal power series $f_I(t) = \sum_{n \geq 0} \varepsilon_n t^n$, $\varepsilon_n = 0, 1$, is rational, then its coefficients ε_n satisfy a linear recurrence relation

$$\varepsilon_{n+k} = p_1 \varepsilon_{n+k-1} + \ldots + p_k \varepsilon_n$$

for some k and some $p_1, \ldots, p_k$. Now we choose $I = \{1!, 2!, \ldots\}$. Hence $\varepsilon_n = 1$ if and only if $n = q!$ for some q and $\varepsilon_n = 0$ otherwise. Fixing any k, for q sufficiently large (e.g. such that $(q+1)! - q! > k$) we obtain that $\varepsilon_n = 0$ for $n = q! + 1, q! + 2, \ldots, q! + k$. Now the recurrence relation implies that $\varepsilon_n = 0$ for all $n > q!$ which is a contradiction. Hence the function $f_I(t) = \sum_{q \geq 1} t^{q!}$ is not rational. □

Corollary 3.12. There exists a continual set of finitely generated graded algebras with pairwise different Hilbert series.

Proof. From the proof of Theorem 3.11 we obtain that if I_1 and I_2 are different subsets of $\mathbb{N}_0$, then the Hilbert series of the algebras A_{I_1} and A_{I_2} are different. Since the subsets of $\mathbb{N}_0$ are continually many, we complete the proof. □

Using the trick of Olshanskii [O], we can construct the following exotic example.

Corollary 3.13. There exists a continual ascending chain $\{U_\alpha \mid \alpha \in \mathbb{R}\}$ of graded ideals of $K\langle x,y\rangle$ such that $U_\alpha \subset U_\beta$ (and $U_\alpha \neq U_\beta$) if and only if $\alpha < \beta$. Hence, for every $\alpha < \beta$ there is a canonical homomorphism $K\langle x,y\rangle/U_\alpha \to K\langle x,y\rangle/U_\beta$.

Proof. Let $\mathbb{Q} = \{q_1, q_2, \dots\}$ be the set of rationals listed in an arbitrary way. For $\alpha \in \mathbb{R}$ we define the set $I_\alpha = \{i \mid q_i \leq \alpha\}$. Clearly, $I_\alpha \subset I_\beta$ if and only if $\alpha \leq \beta$ and $I_\alpha \neq I_\beta$ for $\alpha \neq \beta$. Hence the ideals U_α of $K\langle x,y\rangle$ from the proof of Theorem 3.11, U_α being generated by the set R_{I_α}, satisfy the condition $U_\alpha \subseteq U_\beta$ for $\alpha \leq \beta$. Since R_{I_α} is the Gröbner basis of U_α, and the sets of normal words with respect to R_{I_α} and R_{I_β} are different for $\alpha \neq \beta$, we obtain that $U_\alpha \neq U_\beta$ for $\alpha \neq \beta$. □

Remark 3.14. If two graded algebras are not isomorphic as graded algebras, this does not mean that they are not isomorphic as algebras without grading. In our case the algebras $A_I = K\langle x, y \mid R_I\rangle$ from the proof of Theorem 3.11 are not isomorphic as algebras. We shall sketch the proof. Let $I_1, I_2 \subseteq \mathbb{N}_0$, $I_1 \neq I_2$, let $x_j = x + (R_{I_j})$, $y_j = y + (R_{I_j})$, $j = 1,2$, be the generators of $A_{I_j} = K\langle x,y\rangle/(R_{I_j})$ and let $\phi : A_{I_1} \to A_{I_2}$ be an isomorphism.

Step 1. The ideal (y_j) generated in A_{I_j} by y_j is nilpotent because $z_j y_j x_j^k y_j = y_j x_j^k y_j z_j = 0$ in A_{I_j}, $z_j = x_j, y_j$, and $A_{I_j}/(y_j) \cong K[x_j]$. Hence (y_j) is the Jacobson radical of A_{I_j} and $\phi((y_1)) = (y_2)$. Hence ϕ induces an isomorphism $\bar{\phi} : K[x_1] \to K[x_2]$. Since all automorphisms of $K[x]$ are the affine defined by $x \to \alpha_0 + \alpha_1 x$, $\alpha_0, \alpha_1 \in K$, $\alpha_1 \neq 0$, we obtain that $\bar{\phi}(x_1) = \alpha_0 + \alpha_1 x_2$, with the same restrictions on α_0, α_1.

Step 2. Let $\phi(y_1) = \beta y_2 + f(x_2, y_2)$, where the polynomial $f(x_2, y_2)$ has no linear component. Since $\phi(x_1)$, $\phi(y_1)$ generate A_{I_2}, and the same holds for $\phi(x_1) - \alpha_0$, $\phi(y_1)$, then $y_2 = g(\phi(x_1) - \alpha_0, \phi(y_1))$ for some $g(u_1, u_2) \in K\langle u_1, u_2\rangle$. This implies that $\beta \neq 0$, i.e.

$$\phi(x_1) = \alpha_0 + \alpha_1 x_2 + \alpha_2 y_2 + u,\ \phi(y_1) = \beta y_2 + v,\ u, v \in \sum_{n\geq 2} {}^{\oplus} A_{I_2}^{(n)}.$$

Step 3. If $I_1 = \mathbb{N}_0$, $I_2 \neq \mathbb{N}_0$, then the Jacobson radical of A_{I_1} is nilpotent of class 2 and the Jacobson radical of A_{I_2} is nilpotent of class 3. Since the class of nilpotency of the Jacobson radical is an invariant of the algebra, we obtain that A_{I_1} and A_{I_2} are not isomorphic.

Step 4. Let $I_1, I_2 \neq \mathbb{N}_0$. Since x_1 annihilates the square of the Jacobson radical of A_{I_1} and ϕ is an automorphism (and hence ϕ sends the Jacobson radical onto the Jacobson radical), $\phi(x_1)$ satisfies the same property for annihilation. This implies $\alpha_0 = 0$.

Step 5. Witout loss of generality we may assume that there exists an i in $I_1 \setminus I_2$. Then $y_2 x_2^i y_2 \neq 0$, $y_1 x_1^i y_1 = 0$ and

$$0 = \phi(y_1)\phi(x_1)^i\phi(y_1) = \alpha_1^i \beta^2 y_2 x_2^i y_2 + w,\ w \in \sum_{n\geq i+3} {}^{\oplus} A_{I_2}^{(n)}.$$

Since $\alpha_1^i \beta^2 y_2 x_2^i y_2 \neq 0$, we reach a contradiction. □

We shall finish this chapter with a theorem of Formanek [F], see also [H].

Theorem 3.15. Let U and V be graded ideals of $K\langle X\rangle$,

$$A = K\langle X\rangle/U,\ B = K\langle X\rangle/V,\ C = K\langle X\rangle/UV.$$

Then the Hilbert series of U, V, UV and A, B, C are related by the equations

$$H(UV,t) = \frac{H(U,t)H(V,t)}{H(K\langle X\rangle,t)},$$

$$H(C,t) = H(A,t) + H(B,t) - \frac{H(A,t)H(B,t)}{H(K\langle X\rangle,t)}.$$

Proof. Let $F = K\langle X\rangle$. By Theorem 1.31, any right (left) ideal of F is a free right (left) F-module. Since U and V are graded, the proof of Theorem 1.31 gives that they have homogeneous sets of free generators, say $\{u_i \mid i \geq 1\}$, $\{v_j \mid j \geq 1\}$, considered respectively as free right and left F-modules. Hence

$$U = \sum_{i\geq 1}{}^{\oplus} u_i F,\ V = \sum_{j\geq 1}{}^{\oplus} F v_j.$$

Let $\deg u_i = p_i$, $\deg v_j = q_j$. Then

$$H(U,t) = \sum_{i\geq 1} t^{p_i} H(F,t),\ H(V,t) = \sum_{j\geq 1} t^{q_j} H(F,t).$$

Since $F^2 = F$, we obtain that

$$UV = \left(\sum_{i\geq 1}{}^{\oplus} u_i F\right)\left(\sum_{j\geq 1}{}^{\oplus} F v_j\right) = \sum_{i,j\geq 1}{}^{\oplus} u_i F v_j,$$

$$H(UV,t) = \sum_{i,j\geq 1} t^{p_i} t^{q_j} H(F,t) = \frac{H(U,t)H(V,t)}{H(F,t)}.$$

Since $H(A,t) + H(U,t) = H(F,t)$ and similar relations hold for B, U and C, UV, the relation between the Hilbert series of A, B, C follows from the relation between the Hilbert series of U, V, UV replacing $H(U,t)$, $H(V,t)$, $H(UV,t)$ respectively with $H(F,t) - H(A,t)$, $H(F,t) - H(B,t)$, $H(F,t) - H(C,t)$. □

Exercise 3.16. Prove a multigraded version of Theorem 3.15. □

References

[AM] M.F. Atiyah, I.G. Macdonald, Introduction to Commutative Algebra, Addison-Wesley, Reading, Mass., 1969.

[F] E. Formanek, Noncommutative invariant theory, Contemp. Math. **43** (1985), 87-119.

[H] P. Halpin, Some Poincaré series related to identities of 2 × 2 matrices, Pacific J. Math. **107** (1983), 107-115.

[O] A.Yu. Ol'shanskii, Some infinite systems of identities (Russian), Trudy Seminara Imeni Petrovskogo **3** (1978), 139-146.

[U] V.A. Ufnarovsky, Combinatorial and asymptotic methods in algebra, in A.I. Kostrikin, I.R. Shafarevich (Eds.), "Algebra VI", Encyclopaedia of Mathematical Sciences **57**, Springer-Verlag, 1995, 1-196.

4. THE THEOREM OF GOLOD-SHAFAREVICH

In 1902 Burnside [B] posed his famous problem which was considered as one of the main problems of the theory of infinite groups for more than 90 years.

Problem 4.1. (Burnside) Let G be a finitely generated group. If every element of G is of finite order, does this imply that G is finite? □

In 1941 Kurosch [K] raised a similar problem in ring theory.

Problem 4.2. (Kurosch) (i) Let A be a finitely generated nonunitary algebra. If every element of A is nil, does this imply that A is nilpotent?

(ii) If every element a of the finitely generated algebra A is algebraic (i.e. there exists a nonzero polynomial $f(x) \in K[x]$ such that $f(a) = 0$), is the algebra finite dimensional. □

The negative solution of the Burnside problem was given by Novikov and Adyan, see the book by Adyan [A]. They proved even more: If p is a fixed sufficiently large prime, then there exists a finitely generated group G which is infinite and every element of G is of exponent p. The construction of Novikov and Adyan is based on purely group theoretical methods. The negative solution of the Kurosh problem was given by Golod and Shafarevich [GS], [G]. They constructed a finitely generated nil algebra which is not nilpotent. As a consequence they also obtained for every prime p a new example of a finitely generated p-group G (i.e. every $g \in G$ is of order g^n for some n) which is infinite. The approach of Golod and Shafarevich is based on Hilbert series and is ring theoretical. A nice exposition close to the original papers [GS], [G] is given in the book of Herstein [H]. Our approach is closer to that in the survey article of Ufnarovsky [U] combined with ideas of the original papers.

Lemma 4.3. Let $r_k \geq 0$, $k = 2, 3, \ldots$, let $m > 0$ and let

$$q(t) = \frac{1}{1 - mt + \sum_{k\geq 2} r_k t^k} = \sum_{k\geq 0} q_k t^k.$$

If $q_k \geq 0$ for all $k \geq 0$, then $q(t)$ cannot be a polynomial.

Proof. Let $q(t) = q_0 + q_1 t + \ldots + q_n t^n$, $q_k \geq 0$, $q_n \neq 0$. Then

$$q(t)\left(1 - mt + \sum_{k\geq 2} r_k t^k\right) = 1,$$

$$q(t)\left(1 + \sum_{k\geq 2} r_k t^k\right) = 1 + mtq(t).$$

Comparing the coefficients of degree $n+2$ of both sides of this equation, we obtain

$$q_0 r_{n+2} + q_1 r_{n+1} + \ldots + q_n r_2 = 0.$$

Since $q_i, r_i \geq 0$, $q_n > 0$, we see that $r_2 = 0$. Now we compare the coefficients of degree $n+3$:

$$q_0 r_{n+3} + q_1 r_{n+2} + \ldots + q_n r_3 = 0$$

and again $r_3 = 0$. Continuing in this way, we obtain that $r_4 = r_5 = \ldots = 0$ and

$$q(t) = \frac{1}{1 - mt} = 1 + mt + m^2 t^2 + \ldots ,$$

i.e. $q(t)$ cannot be a polynomial. □

As usually, we fix an integer $m \geq 2$ and the set $X = \{x_1, \dots, x_m\}$. Let U be a graded ideal of $F = K\langle X\rangle$ generated by a set R of homogeneous polynomials. We denote by r_n the number of elements of degree n in the generating set R and by $r(t) = \sum_{n\geq 2} r_n t^n$ the corresponding generating function.

Lemma 4.4. Let in the above notation N be the vector space spanned by the normal words with respect to U. Then $U = UX + NR$.

Proof. By Theorem 1.12, $F = N \oplus U$ as vector spaces and since $F = FX \oplus K$ and $R \subset FX^2$ (because the relations in R are homogeneous of degree ≥ 2), we obtain

$$U = FRF = FR(FX + K) = FRFX + FR = UX + (N + U)R =$$

$$= UX + NR + UR \subseteq UX + NR + UFX^2 = UX + NR,$$

i.e. $U \subseteq UX + NR$. Since $UX \subseteq U$, $NR \subseteq U$, we obtain $U = UX + NR$. □

Corollary 4.5. Let $A = F/U = K\langle X \mid R = 0\rangle$. Then

$$H(U, t) \leq H(U, t)mt + H(A, t)r(t).$$

Proof. Since N and A are isomorphic as graded vector spaces, we obtain that

$$H(U, t) = H(UX + NR, t) \leq H(UX, t) + H(NR, t) \leq$$

$$\leq H(U, t)mt + H(N, t)r(t) = H(U, t)mt + H(A, t)r(t). \quad \square$$

Theorem 4.6. (Golod-Shafarevich) If all coefficients of the series

$$q(t) = \frac{1}{1 - mt + \sum_{k\geq 2} r_k t^k}$$

are nonnegative, then the algebra $A = K\langle X \mid R = 0\rangle$ is infinite dimensional.

Proof. In the inequality

$$H(U, t)(1 - mt) \leq H(A, t)r(t)$$

in Corollary 4.5 we replace

$$H(U, t) = H(F, t) - H(A, t) = \frac{1}{1 - mt} - H(A, t)$$

and obtain

$$\left(\frac{1}{1 - mt} - H(A, t)\right)(1 - mt) \leq H(A, t)r(t),$$

$$H(A, t)(1 - mt + r(t)) \geq 1.$$

Since the coefficients of $q(t)$ are nonnegative, we derive

$$H(A, t) = H(A, t)(1 - mt + r(t))q(t) =$$

$$= H(A, t)(1 - mt + r(t))\frac{1}{1 - mt + r(t)} \geq \frac{1}{1 - mt + r(t)}.$$

Now, applying Lemma 4.3, we obtain that $q(t)$ is not a polynomial and this implies that infinitely many of the coefficients of $H(A,t)$ are positive. Hence A is not finite dimensional. $\square$

Corollary 4.7. If all coefficients of the series

$$p(t)=\frac{1}{1-mt+\sum_{n\geq 2}s_nt^n}=\sum_{n\geq 0}p_nt^n$$

are nonnegative and $r_n\leq s_n$ for all $n\geq 2$, then the algebra A is also infinite dimensional.

Proof. In the notation of Theorem 4.6 it is sufficient to show that the coefficients of $q(t)=(1-mt+\sum_{n\geq 2}r_nt^n)^{-1}$ are nonnegative. Let

$$u(t)=1-mt+r(t)=1-mt+\sum_{n\geq 2}r_nt^n,$$

$$s(t)=1-mt+\sum_{n\geq 2}s_nt^n.$$

Then $p(t)=\frac{1}{s(t)}$, $q(t)=\frac{1}{u(t)}$. We know that $s(t)\geq u(t)$, $p(t)\geq 0$ and want to show that $q(t)\geq p(t)$, i.e. $\frac{1}{u(t)}\geq\frac{1}{s(t)}$. Hence $v(t)=s(t)-u(t)\geq 0$ and the formal power series $v(t)$ has no constant term. Therefore

$$u(t)=s(t)-v(t)=s(t)-s(t)v(t)\frac{1}{s(t)}=s(t)\left(1-\frac{v(t)}{s(t)}\right),$$

$$\frac{1}{u(t)}=\frac{1}{s(t)}.\frac{1}{1-\frac{v(t)}{s(t)}},$$

$$q(t)=p(t)\frac{1}{1-\frac{v(t)}{s(t)}}.$$

Since $\frac{v(t)}{s(t)}$ has no constant term,

$$\frac{1}{1-\frac{v(t)}{s(t)}}=1+\frac{v(t)}{s(t)}+\frac{v(t)}{s(t)}^2+\dots$$

and the inequalities $v(t)\geq 0$, $\frac{1}{s(t)}\geq 0$ imply that $\frac{v(t)}{s(t)}\geq 0$. Hence

$$\frac{1}{1-\frac{v(t)}{s(t)}}=1+\frac{v(t)}{s(t)}+\frac{v(t)}{s(t)}^2+\dots\geq 1,$$

which gives that $q(t)\geq p(t)$. $\square$

Corollary 4.8. If $0<\varepsilon<\frac{m}{2}$ and $r_n\leq\varepsilon^2(m-2\varepsilon)^{n-2}$ for all $n\geq 2$, then the algebra A is infinite dimensional.

Proof. Using the equation

$$\frac{1}{(1-t)^2}=1+2t+3t^2+\dots$$

we calculate

$$\frac{1}{1-mt+\sum_{n\geq 2}\varepsilon^2(m-2\varepsilon)^{n-2}t^n}=\frac{1}{1-mt+\frac{\varepsilon^2t^2}{1-(m-2\varepsilon)t}}=$$

$$=\frac{1-(m-2\varepsilon)t}{(1-(m-\varepsilon)t)^2}=\frac{m-2\varepsilon}{(m-\varepsilon)(1-(m-\varepsilon)t)}+\frac{\varepsilon}{(m-\varepsilon)(1-(m-\varepsilon)t)^2}=$$

$$=(m-2\varepsilon)\sum_{n\geq 0}(m-\varepsilon)^{n-1}t^n+\varepsilon\sum_{n\geq 0}(n+1)(m-\varepsilon)^{n-1}t^n$$

and the coefficients of the series are positive for all $n\geq 0$. Hence by Corollary 4.7 the algebra A is not finite dimensional. □

Lemma 4.9. Let A be a nilpotent algebra generated by $\{a_1,\dots,a_m\}$. This system of generators is minimal if and only if the set

$$\{\bar{a}_i=a_i+A^2\mid i=1,\dots,m\}$$

is a basis of the vector space $\bar{A}=A/A^2$.

Proof. Let $a\in A$ be such that $a\notin A^2$. Since $a_1,\dots,a_m$ generate A,

$$a=\sum\alpha_i a_{i_1}\dots a_{i_k},\ \alpha_i\in K,k\geq 1.$$

Working modulo A^2 we obtain that $\bar{a}=a+A^2$ is a linear combination of $\bar{a}_i$, $i=1,\dots,m$. Hence $\{\bar{a}_i\mid i=1,\dots,m\}$ is a generating set of A/A^2.

Let $\{\bar{a}_i\mid i=1,\dots,p\}$ be a basis of A/A^2. We shall show that it generates the algebra A. Let A be nilpotent of class n, i.e. $A^n=0$ and $A^{n-1}\neq 0$. We shall use induction on n, the base of the induction $n=2$ being trivial. Assuming that every element of $\tilde{A}=A/A^{n-1}$ is a polynomial of $\tilde{a}_1,\dots,\tilde{a}_m$, $\tilde{a}_i=a_i+A^{n-1}$, it is sufficient to show that every element of A^{n-1} is a polynomial of $a_1,\dots,a_m$. The elements $a_{p+1},\dots,a_m$ have the form $a_i=b_i+c_i$, where b_i is a linear combination of $a_1,\dots,a_p$ and $c_i\in A^2$, $i=p+1,\dots,m$. Since every element $a\in A^{n-1}$ can be presented as

$$a=\sum\alpha_i a_{i_1}\dots a_{i_k},\ \alpha_i\in K,i_j=1,\dots,m,\ k\geq n-1,$$

and $a_{i_1}\dots a_{i_n}=0$, we obtain that it is sufficient to consider only the summands with $k=n-1$. Replacing a_i with b_i+c_i for $i>p$ and expressing b_i as linear combinations of $a_1,\dots,a_p$, we obtain that

$$a=\sum\beta_j a_{j_1}\dots a_{j_{n-1}}+\sum\gamma_{ik}a_{k_1}\dots c_{k_i}\dots a_{k_{n-1}},\ \beta_j,\gamma_{ik}\in K,$$

and the second sum consists of all products containing at least one c_{k_i}. Since $c_{k_i}\in A^2$, we obtain that $a_{k_1}\dots c_{k_i}\dots a_{k_{n-1}}\in A^n=0$ and a is a polynomial of $a_1,\dots,a_p$. □

Theorem 4.10. Let A be a nilpotent algebra with a minimal system of $m>1$ generators and with r defining relations with respect to this minimal generating system. Then $r>\left(\frac{m-1}{2}\right)^2$.

Proof. Let $\{a_1,\dots,a_m\}$ be a minimal system of generators of A and let $F = K\langle X\rangle$, $F^+ = \sum_{n\geq 1} F^{(n)}$. Hence $A \cong F^+/U$ for some ideal U of F^+ and A has the presentation

$$A = (K\langle X \mid R = 0\rangle)^+$$

for some set R of r elements. By Lemma 4.9, the set

$$\{\bar{a}_i = a_i + A^2 \mid i = 1,\dots,m\}$$

is a basis of A modulo A^2. Since $A/A^2 \cong F^+/((F^+)^2 + U)$, this means that $U \subseteq (F^+)^2$ and the relations in R have no linear terms. Every elemet $u_i \in R$, $i = 1,\dots,r$, has the form

$$u_i = u_{i2} + u_{i3} + \ldots + u_{ik},\ u_{ij} \in F^{(j)}.$$

We add all u_{ij} to R as new relations and obtain that the new ideal U' generated in F^+ by

$$R' = \{u_{ij} \mid i = 1,\dots,r,\ j = 1,\dots,k\}$$

contains U. Hence the algebra $A' = F^+/U'$ is a homomorphic image of the original algebra $A = F^+/U$ and is nilpotent. Now the set R' of the generators of U' consists of homogeneous polynomials and U' is a graded vector space. The algebra A' is m-generated, $m \geq 2$, and has $\leq r$ relations of degree 2, $\leq r$ relations of degree 3, etc. Let $r \leq \left(\frac{m-1}{2}\right)^2$. Using the notation of Theorem 4.6, we obtain that $r_n \leq r \leq \left(\frac{m-1}{2}\right)^2$. Hence

$$\sum_{n\geq 2} r_n t^n \leq \sum_{n\geq 2} \left(\frac{m-1}{2}\right)^2 t^n = \left(\frac{m-1}{2}\right)^2 \frac{t^2}{1-t}.$$

The series

$$1 - mt + \sum_{n\geq 2} \left(\frac{m-1}{2}\right)^2 t^n$$

is equal to

$$1 - mt + \left(\frac{m-1}{2}\right)^2 \frac{t^2}{1-t}$$

and its inverse is

$$p(t) = \frac{1}{1 - mt + \left(\frac{m-1}{2}\right)^2 \frac{t^2}{1-t}} = \frac{1-t}{(1-mt)(1-t) + \left(\frac{m-1}{2}\right)^2 t^2} =$$

$$= \frac{1-t}{\left(1 - \frac{m+1}{2}t\right)^2} = \frac{2}{(m+1)\left(1 - \frac{m+1}{2}t\right)} + \frac{m-1}{(m+1)\left(1 - \frac{m+1}{2}t\right)^2}.$$

Since

$$\frac{1}{1 - \frac{m+1}{2}t} = 1 + \frac{m+1}{2}t + \left(\frac{m+1}{2}\right)^2 t^2 + \dots,$$

$$\frac{1}{\left(1 - \frac{m+1}{2}t\right)^2} = 1 + 2\frac{m+1}{2}t + 3\left(\frac{m+1}{2}\right)^2 t^2 + \dots,$$

we obtain that $p(t)$ has positive coefficients and apply Corollary 4.7. Hence A' is not finite dimensional and hence not nilpotent. This is a contradiction with the nilpotency of A'. □

Now we give the negative solution of the Kurosch problem.

Theorem 4.11. For every $m \geq 2$ there exists an m-generated nil algebra which is not nilpotent.

Proof. We fix $\varepsilon \in (0, \frac{1}{2})$. We need a set of homogeneous (and nonlinear) polynomials $R = \{u_1, u_2, \dots\}$ which generates the ideal U of $F = K\langle X\rangle$ with the following properties:

(1) The number r_n of the polynomials u_i of degree n satisfies the inequality $r_n \leq \varepsilon^2(m-2\varepsilon)^{n-2}$.

(2) For every $v \in F^+$ there exists a positive integer $q = q(v)$ such that $v^q \in U$.

Then by Corollary 4.8 the algebra $A = F^+/U$ is infinite dimensional (and hence not nilpotent) and (2) guarantees that A is nil.

We apply induction on the degree k of v. Let the set of homogeneous polynomials $R_{k-1} = \{u_1, \dots, u_{p_{k-1}}\}$ be chosen in such a way that for any $v \in F^+$, $\deg v \leq k-1$, there exists a q such that v^q belongs to the ideal U_{k-1} generated by R_{k-1} and the set R_{k-1} satisfies the inequalities $r_n \leq \varepsilon^2(m-2\varepsilon)^{n-2}$. Now we shall add to R_{k-1} new homogeneous polynomials $u_{p_{k-1}+1}, \dots, u_{p_k}$ such that the set $R_k = \{u_1, \dots, u_{p_k}\}$ satisfies the same conditions as R_{k-1} but for all v of degree $\leq k$. We consider the "generic" polynomial of degree k in F^+

$$v = \sum_{1\leq l\leq k} \alpha_i x_{i_1} \dots x_{i_l},\ \alpha_i \in K.$$

If $\alpha_{j_1}, \dots, \alpha_{j_s}$ are all coefficients of v, then

$$v^q = \sum_{a_1+\dots+a_s=q} \alpha_{j_1}^{a_1} \dots \alpha_{j_s}^{a_s} v_a(x_1, \dots, x_m),$$

where v_a are polynomials which do not depend on α_i. Each v_a is homogeneous of degree $p \in [q, kq]$. We choose q sufficiently large in order to guarantee that the degrees of all v_a are higher than the degrees of the polynomials of R_{k-1} and assume that

$$R_k = R_{k-1} \cup \{v_a \mid a = (a_1, \dots, a_s), a_1 + \dots + a_s = q\}.$$

Then for every $v \in F^+$, $\deg v \leq k$, we obtain that $v^q \in U_k$. Since the degree of v_a is higher than the degree of $u_i \in R_{k-1}$, for small n the integers r_n are the same for R_{k-1} and R_k. We shall estimate the number of v_a. The total number of monomials $x_{i_1} \dots x_{i_l}$ of degree $\leq k$ is $s = m + m^2 + \dots + m^k$ and the number of monomials $\alpha_{j_1}^{a_1} \dots \alpha_{j_s}^{a_s}$ of degree q and in s variables is

$$\binom{s+q-1}{s-1} \leq (s+q-1)^{s-1}.$$

Since k (and hence s) is fixed, for sufficiently large q

$$(s+q-1)^{s-1} \leq \varepsilon^2(m-2\varepsilon)^{q-2}$$

and for all $n \geq q$

$$r_n \leq (s+q-1)^{s-1} \leq \varepsilon^2(m-2\varepsilon)^{q-2} \leq \varepsilon^2(m-2\varepsilon)^{n-2}.$$

Hence we have done the inductive step and this completes the proof. □

Now we shall show how Theorem 4.11 gives the negative solution of the Burnside problem.

Theorem 4.12. For every $m \geq 2$ and every prime p there exists an m-generated p-group which is infinite.

Proof. We consider the algebra $A = F^+/U$ from Theorem 4.10 for the prime field $K = \mathbb{Z}_p$. Then A is m-generated, nil and not nilpotent. Let $A_1 = F/U$ (i.e. $A_1 = \mathbb{Z}_p + A$ is obtained from A by formal adjunction of 1). Since $\mathrm{char}\mathbb{Z}_p = p$ and for any $v \in A$ there exists a $q = q(v)$ such that $v^q = 0$, for some $p^k \geq q$, $k = k(v)$, we have that $(1+v)^{p^k} = 1 + v^{p^k} = 1$ and $1 + v$ is invertible in A_1. Hence the elements $1 + \bar{x}_i = 1 + x_i + U$, $i = 1, \ldots, m$, generate a subgroup G of the multiplicative group of A_1. Let B be the subalgebra of A_1 generated by $1 + \bar{x}_1, \ldots, 1 + \bar{x}_m$. Since $(1 + \bar{x}_i)^{p^k} = 1 \in B$, $\bar{x}_i = (1 + \bar{x}_i) - 1 \in B$, we obtain that $1, \bar{x}_1, \ldots, \bar{x}_m \in B$ and $B = A_1$. Clearly $g_i, g_j \in G$ implies $g_i g_j \in G$ and every element of B is a linear combination of elements of G. If the group G is finite, then $\dim B = |G| < \infty$. This is impossible because $B = A_1$ and the algebra A_1 is infinite dimensional. □

References

[A] S.I. Adyan, The Burnside Problem and Identities in Groups (Russian), "Nauka", Moscow, 1975. Translation: Ergebnisse der Math. und ihrer Grenzgebiete **95**, Springer-Verlag, Berlin-New York, 1979.

[B] W. Burnside, On an unsettled question in the theory of discontinuous groups, Quart. J. Math. **33** (1902), 230-238.

[G] E.S. Golod, On nil-algebras and finitely approximable p-groups (Russian), Izv. Akad. Nauk SSSR, Ser. Mat. **28** (1964), 273-276.

[GS] E.S. Golod, I.R. Shafarevich, On the class field tower (Russian), Izv. Akad. Nauk SSSR, Ser. Mat. **28** (1964), 261-272.

[H] I.N. Herstein, Noncommutative Rings, Carus Math. Monographs **15**, Wiley and Sons, Inc., New York, 1968.

[K] A.G. Kurosch, Ringtheoretische Probleme, die mit dem Burnsideschen Problem über periodische Gruppen in Zusammenhang stehen, Bull. Akad. Sci. URSS Ser. Math. **5** (1941), 233-240.

[U] V.A. Ufnarovsky, Combinatorial and asymptotic methods in algebra, in A.I. Kostrikin, I.R. Shafarevich (Eds.), "Algebra VI", Encyclopaedia of Mathematical Sciences **57**, Springer-Verlag, 1995, 1-196.

5. GELFAND-KIRILLOV DIMENSION

In this chapter we fix an algebra A generated by a finite set $\{a_1, \dots , a_m\}$.

Definition 5.1. Let

$$V^n = \operatorname{span}\{a_{i_1} \dots a_{i_n} \mid i_j = 1, \dots , m\},\ n = 0, 1, 2, \dots ,$$

where we assume that $V^0 = K$ if A is unitary and $V^0 = 0$ if it is not unitary. The growth function of A (with respect to $\{a_1, \dots , a_m\}$ or with respect to V) is defined by

$$g(n) = g_V(n) = \dim(V^0 + V^1 + \dots + V^n),\ n = 0, 1, 2, \dots \quad \square$$

Clearly $g(n)$ is monotone.

Example 5.2. (i) For the polynomial algebra $A = K[X]$ and $V = \operatorname{span}(X)$, $X = \{x_1, \dots , x_m\}$, the growth function $g(n)$ is equal to the number of monomials in m variables and of degree $\leq n$, i.e.

$$g(n) = \binom{n+m}{m}.$$

(ii) For the free algebra $K\langle X\rangle$ and the same $V = \operatorname{span}(X)$ and $m > 1$,

$$g(n) = 1 + m + m^2 + \dots m^n = \frac{m^{n+1} - 1}{m - 1}. \quad \square$$

Exercise 5.3. (Bergman, see [S]) Show that $\lim_{n\to\infty} \left(g(n)^{1/n}\right)$ always exists.

Hint. Step 1. Assume that the fuction $g(n)$ is not bounded, otherwise $0 \leq g(n) < k$ for some $k \in \mathbb{N}$ and $\lim_{n\to\infty} \left(g(n)^{1/n}\right) = 0$.

Step 2. Using that the algebra A is associative, show that $g(n + p) \leq g(n)g(p)$ for all $n, p \geq 1$.

Step 3. Let $n = sp + q$, $s \geq 0$, $0 \leq q < p$. Using Step 1, obtain that

$$g(n)^{1/n} \leq (g(p)^s.g(q))^{1/n} = g(p)^{s/n}.g(q)^{1/n}.$$

Since $g(n)$ is not decreasing, $s/n \leq 1/p$ and $g(p) \geq 1$, derive that

$$g(n)^{1/n} \leq g(p)^{s/n}.g(q)^{1/n} \leq g(p)^{1/p}.g(p)^{1/n}.$$

Step 4. Chose $g(p)^{1/p}$ close to $\liminf_{n\to\infty} g(n)^{1/n}$. Show that the sequence $\{g(n)^{1/n}\}_{n\geq 0}$ converges. $\square$

Lemma 5.4. Let $V = \operatorname{span}\{a_1, \dots , a_m\}$ and $W = \operatorname{span}\{b_1, \dots , b_s\}$ be two generating vector spaces of the algebra A. Then there exists a $k \in \mathbb{N}$ such that

$$g_V(n) \leq g_W(kn),\ n = 0, 1, 2, \dots$$

Proof. Since A is generated by W, there exists a $k \in \mathbb{N}$ such that

$$a_1, \dots , a_m \in W^0 + W^1 + \dots + W^k.$$

Hence

$$V^p \subseteq (W^0 + W^1 + \dots + W^k)^p \subseteq W^0 + W^1 + \dots + W^{kp},$$

$$V^0 + V^1 + \ldots + V^n \subseteq W^0 + W^1 + \ldots + W^{kn},$$

$$g_V(n) \leq g_W(kn),\ n = 0, 1, 2, \ldots \quad \square$$

Definition 5.5. Let A be a finitely generated algebra with growth function $g(n)$ (with respect to the some generating space $\text{span}\{a_1, \ldots, a_m\}$). The Gelfand-Kirillov dimension of A is defined by

$$\text{GKdim}(A) = \limsup_{n\to\infty}(\log_n g(n)) = \limsup_{n\to\infty} \frac{\log g(n)}{\log n}. \quad \square$$

Lemma 5.6. The Gelfand-Kirillov dimension of a finitely generated algebra does not depend on the choice of the set of generators.

Proof. Let $V = \text{span}\{a_1, \ldots, a_m\}$ and $W = \text{span}\{b_1, \ldots, b_s\}$ be two generating spaces of A. Let $\text{GKdim}_V(A)$ and $\text{GKdim}_W(A)$ be the Gelfand-Kirillov dimensions of A defined respectively by means of V and W. By Lemma 5.4, there exists a $k \in \mathbb{N}$ such that $g_V(n) \leq g_W(kn)$, $n = 0, 1, 2, \ldots$, and

$$\text{GKdim}_V(A) = \limsup_{n\to\infty} \frac{\log g_V(n)}{\log n} \leq \limsup_{n\to\infty} \frac{\log g_W(kn)}{\log(kn)} \leq$$

$$\leq \limsup_{n\to\infty} \frac{\log g_W(n)}{\log n} = \text{GKdim}_W(A).$$

Similarly $\text{GKdim}_W(A) \leq \text{GKdim}_V(A)$ and $\text{GKdim}(A)$ is well defined. $\square$

In the sequel, considering an algebra with a presentation $A = K\langle X \mid R = 0\rangle$ we always assume that its growth function is with respect to $V = \text{span}(X)$.

Example 5.7. By Example 5.2 the growth function of the polynomial algebra in m variables is a polynomial of degree m and this gives that

$$\text{GKdim}(K[x_1, \ldots, x_m]) = m.$$

By the same example for the free algebra $K\langle X\rangle$, $m \geq 2$, we obtain that

$$\frac{\log g(n)}{\log n} = \frac{\log(1 + m + m^2 + \ldots + m^n)}{\log n} \geq \frac{\log m^n}{\log n} = \frac{n \log m}{\log n}$$

which tends to infinity for $n \to \infty$. Hence $\text{GKdim}(K\langle X\rangle) = \infty$ for $m > 1$. $\square$

Exercise 5.8. Show that $\text{GKdim}(A) < 1$ implies that $\text{GKdim}(A) = 0$ and $\dim A < \infty$.

Hint. Let $g(n)$ be the growth function of A with respect to some generating vector space V. If $g(n) \geq n$ for all $n \geq 0$, then $\text{GKdim}(A) \geq 1$. Hence $g(n_0) < n_0$ for some n_0. Then in the chain

$$V^0 \subseteq V^0 + V^1 \subseteq V^0 + V^1 + V^2 + \ldots \subseteq V^0 + V^1 + \ldots + V^{n_0}$$

we have $V^0 + V^1 + \ldots + V^k = V^0 + V^1 + \ldots + V^{k+1}$, i.e. $V^{k+1} \subseteq V^0 + V^1 + \ldots + V^k$. This implies that

$$V^{k+2} \subseteq (V^0 + V^1 + \ldots + V^k)V \subseteq V^0 + V^1 + \ldots + V^{k+1} \subseteq V^0 + V^1 + \ldots + V^k,$$

and $V^0+V^1+\ldots+V^n=V^0+V^1+\ldots+V^k$ for all $n\geq k$. Hence $g(n)=g(k)$, $n\geq k$, and

$$\mathrm{GKdim}(A)=\limsup_{n\to\infty}\frac{\log g(k)}{\log n}=0.\quad\square$$

Remark 5.9. By the theorem of Bergman (see [KL]), there is no algebra A with $\mathrm{GKdim}(A)\in(1,2)$. $\square$

Proposition 5.10. Let $A=K\langle X\rangle/U=K\langle X\mid G=0\rangle$, where G is a Gröbner basis of the ideal U and let b_n be the number of normal words of length n with respect to G. Then the growth function $g(n)$ of A (with respect to $V=\mathrm{span}(X)$) satisfies

$$g(n)=b_0+b_1+\ldots+b_n,\ n=0,1,2,\ldots$$

Proof. For every $w\in K\langle X\rangle$ we denote by $\bar{w}=w+U$ its image in A. All normal words $\bar{x}_{i_1}\ldots\bar{x}_{i_n}$ belong to V^n and are linearly independend by Theorem 1.12. Hence $g(n)\geq b_0+b_1+\ldots+b_n$. We shall complete the proof if we establish that for every word $w=x_{j_1}\ldots x_{j_n}\in\langle X\rangle$, its image $\bar{w}$ is a linear combination of normal words of length $\leq n$. We use induction on the homogeneous lexicographic ordering. Since the desired presentation of the normal words is obvious, the base of the induction is trivial. Now let w be not normal, i.e. $w=a\hat{g}b$ for some $g\in G$, $a,b\in\langle X\rangle$. By Algorithm 1.23, in order to present $\bar{w}$ in its normal form, we replace $\bar{w}$ with $\overline{w-agb}$ which is a linear combination of words smaller than w in the ordering. Hence the length of each of these words is bounded by n and we apply inductive arguments. $\square$

Corollary 5.11. Let G be a Gröbner basis of the ideal U of $K\langle X\rangle$ and let $\hat{G}$ be the set of leading words of G. Then the algebra $A=K\langle X\rangle/U=K\langle X\mid G=0\rangle$ and the monomial algebra $B=K\langle X\mid\hat{G}=0\rangle$ have the same growth functions.

Proof. By Proposition 1.28 the set $\hat{G}$ is a Gröbner basis for the ideal generated by $\hat{G}$ in $K\langle X\rangle$. Since the sets of normal words with respect to G and $\hat{G}$ coincide and both G and $\hat{G}$ are Gröbner bases, we apply Proposition 5.10 and complete the proof. $\square$

Sometimes, it is convenient to consider the generalized Hilbert series $H_g(A,t)$ of any (not necessarily graded) algebra $A=K\langle X\mid R=0\rangle$. It is defined by

$$H_g(A,t)=\sum_{n\geq 0}(g(n)-g(n-1))t^n,$$

(where $g(-1)=0$). Clearly, the coefficient $g(n)-g(n-1)$ of t^n is equal to the number of normal words of length n (where the normality is with respect to the ideal U generated by R).

Corollary 5.12. For any m-dimensional Lie algebra L, the Gelfand-Kirillov dimension of the universal enveloping algebra $U(L)$ is equal to m.

Proof. Let $\{a_1,\ldots,a_m\}$ be a basis of L and let the multiplication table of L is given by

$$[a_i,a_j]=\sum_{k=1}^{m}\alpha_{ij}^{(k)}a_k,\ \alpha_{ij}^{(k)}\in K.$$

By the Poincaré-Birkhoff-Witt Theorem 2.4, the set of defining relations of $U(L)$

$$G=\{[x_i,x_j]-\sum_{k=1}^{m}\alpha_{ij}^{(k)}x_k\mid i,j=1,\ldots,m\}$$

is a Gröbner basis and the set of normal words with respect to G is $\{x_1^{n_1}\dots x_m^{n_m} \mid n_i \geq 0\}$. Hence Proposition 5.10 gives that the growth function $g(n)$ of $U(L)$ is equal to the growth function of the polynomial algebra $K[X]$ and $\mathrm{GKdim}(U(L)) = \mathrm{GKdim}(K[X]) = m$. □

In the next chapter we shall show how behave the growth functions of universal enveloping algebras of finitely generated but not finite dimensional Lie albgebras.

It is well known that the Gelfand-Kirillov dimension of any finitely generated commutative algebra A is equal to the transcendence degree of A (and to the Krull dimension of A), see [KL]. Now we shall construct an example of two-generated algebra A with $\mathrm{GKdim}(A) = \alpha$ for any fixed real number $\alpha \geq 2$. The example is a modification of the examle of Borho and Kraft [BK]. On the other hand, Petrogradsky [P] constructed an example of a finitely generated Lie algebra with Gelfand-Kirillov dimension any $\alpha \geq 1$.

Lemma 5.13. Let $f_1(x)$ and $f_2(x)$ be two continuous monotone increasing functions defined for every $x \geq 0$. Let

$$f_1(n) \leq a_n \leq f_2(n),\ n = 1, 2, \dots,$$

where

$$a(t) = \sum_{n\geq 1} a_n t^n,\ b(t) = \frac{a(t)}{1-t} = \sum_{n\geq 1} b_n t^n.$$

Then

$$\int_0^n f_1(x)dx \leq b_n = a_1 + a_2 + \dots + a_n \leq \int_1^{n+1} f_2(x)dx.$$

Proof. For every $k = 1, 2, \dots, n$,

$$f_1(k-1) \leq f_1(x) \leq f_1(k) \leq a_k,\ k-1 \leq x \leq k+1.$$

Hence

$$\int_{k-1}^k f_1(x)dx \leq a_k,\ \int_0^n f_1(x)dx = \sum_{k=1}^n \int_{k-1}^k f(x)dx \leq a_1 + a_2 + \dots + a_n = b_n.$$

The other inequality can be obtained analogously. □

We fix a real number $0 < \beta < 1$ and define a sequence $\{a_n\}_{n\geq 0}$ assuming $a_0 = 0$, $a_1 = 1$, and, inductively,

$$a_n = 0,\ \text{ if }\ a_1 + a_2 + \dots + a_{n-1} = [n^\beta],$$

$$a_n = 1,\ \text{ if }\ a_1 + a_2 + \dots + a_{n-1} < [n^\beta],$$

where $[n^\beta]$ is the integer part of n^β. By the Mean Value Theorem, for every $x \geq 1$

$$\frac{(x+1)^\beta - x^\beta}{(x+1) - x} = \beta\xi^{\beta-1} < 1,$$

for some $\xi \in (x, x+1)$. Hence

$$(n+1)^\beta - n^\beta < (n+1) - n = 1$$

and $[(n+1)^\beta]-[n^\beta]\leq 1$. This means that we can always construct the next element a_{n+1} of the sequence.

Lemma 5.14. Let $0<\beta<1$, let $\{a_n\}_{n\geq 0}$ be the above constructed sequence and $a(t)=\sum_{n\geq 0}a_nt^n$. Then for every $k\in\mathbb{N}$ there exist $\gamma\in\mathbb{R}^+$ and polynomials $h_1(n),h_2(n)$ with real coefficients and of degree $\leq k$ such that the coefficients c_n of the series

$$c(t)=\sum_{n\geq 1}c_nt^n=\frac{a(t)}{(1-t)^k},$$

satisfy the inequality

$$\gamma n^{k+\beta}-h_1(n)\leq c_1+\ldots+c_n\leq\gamma(n+k)^{k+\beta}+h_2(n),\ n=1,2,\ldots$$

Proof. Let

$$b(t)=\sum_{n\geq 1}b_nt^n=\frac{a(t)}{1-t}.$$

Then $b_n=a_1+\ldots+a_n$ and by the construction of a_n we have

$$n^\beta-1<b_n\leq n^\beta,\ n=1,2,\ldots$$

Applying Lemma 5.13, we obtain for the coefficients $b_n^{(2)}$ of the series

$$\sum_{n\geq 1}b_n^{(2)}t^n=\frac{a(t)}{(1-t)^2}$$

$$\frac{1}{\beta+1}n^{\beta+1}-n=\int_0^n x^\beta dx-n\leq\sum_{i=1}^n b_i\leq\int_1^{n+1}x^\beta dx=\frac{1}{\beta+1}((n+1)^{\beta+1}-1).$$

Continuing in this way, we obtain the statement of the lemma. □

Theorem 5.15. For any $\alpha\geq 2$ there exists a two-generated algebra A with $\mathrm{GKdim}(A)=\alpha$.

Proof. Let $\alpha=k+\beta$, where $0\leq\beta<1$. If $\beta=0$, i.e. $\alpha=k$, we consider the algebra $A_\alpha=K\langle x,y\rangle/U_\alpha$, where U_α is the ideal generated by the monomials

$$yx^{p_1}yx^{p_2}\ldots yx^{p_k}y,\ p_j\geq 0.$$

If $\beta>0$, then $A_\alpha=K\langle x,y\rangle/U_\alpha$, where U_α is generated by

$$yx^{p_1}yx^{p_2}\ldots yx^{p_k}y,\ p_j\geq 0,$$

and

$$yx^iyx^{p_2}\ldots yx^{p_{k-1}}y,\ p_j\geq 0, i\in I,$$

where the set I consists of all $i\in\mathbb{N}_0$ such that $a_i=0$ with the above definition of the sequence $\{a_n\}_{n\geq 0}$. We shall consider the case $\beta>0$ only. The case $\beta=0$ is easier and can be handled in a similar way. By Proposition 1.28, the given generating set of the monomial ideal U_α is a Gröbner basis and the set of normal words with respect to U_α consists of

$$x^{p_0}yx^{p_1}y\ldots x^{p_{q-1}}yx^{p_q},\ p_j\geq 0, q\leq k-1,$$

$$x^{p_0}yx^sy\dots x^{p_{k-1}}yx^{p_k},\ p_j\geq 0, s\in J=\mathbb{N}_0\setminus I.$$

Hence the Hilbert series of A_α is

$$H(A_\alpha,t)=\sum_{q=0}^{k-1}t^q(1+t+t^2+\dots)^{q+1}+\sum_{n\in J}t^{k+n}(1+t+t^2+\dots)^k=$$

$$=\frac{1}{1-t}+\frac{t}{(1-t)^2}+\dots+\frac{t^{k-1}}{(1-t)^k}+\frac{a(t)}{(1-t)^k}=\sum_{n\geq 0}b_nt^n.$$

For $q\geq 1$ the series

$$\sum_{n\geq 0}c_n^{(q)}t^n=\frac{1}{(1-t)^q}$$

is the Hilbert series of the polynomial algebra in q variables and

$$g^{(q)}(n)=c_0^{(q)}+c_1^{(q)}+\dots+c_n^{(q)}=\binom{n+q}{q}$$

is a polynomial of degree q. Since the coefficients of the series

$$\sum_{n\geq 0}d_n^{(q)}t^n=\frac{t^{q-1}}{(1-t)^q}$$

satisfy $d_{n+q-1}^{(q)}=c_n^{(q)}$ and $d_n^{(q)}=0$ for $n<q-1$, we obtain that $d_0^{(q)}+d_1^{(q)}+\dots+d_n^{(q)}$ is also a polynomial of degree q. Hence the coefficients of

$$\sum_{n\geq 0}d_nt^n=\frac{1}{1-t}+\frac{t}{(1-t)^2}+\dots+\frac{t^{k-1}}{(1-t)^k}$$

satisfy $d_0+d_1+\dots+d_n=f(n)$ for some polynomial of degree k. By Lemma 5.14 the coefficients c_n of the series

$$c(t)=\sum_{n\geq 0}c_nt^n=\frac{a(t)}{(1-t)^k}$$

satisfy the inequality

$$\gamma n^{k+\beta}-h_1(n)\leq c_1+\dots+c_n\leq\gamma(n+k)^{k+\beta}+h_2(n),\ n=1,2,\dots$$

for some $\gamma\in\mathbb{R}^+$ and some polynomials $h_1(n),h_2(n)$ with real coefficients and of degree $\leq k$. Hence the growth function of A_α

$$g(n)=b_0+b_1+\dots+b_n=(d_0+d_1+\dots+d_n)+(c_0+c_1+\dots+c_n)$$

satisfies the inequality

$$\gamma n^{k+\beta}+f(n)-h_1(n)\leq g(n)\leq\gamma(n+k)^{k+\beta}+f(n)+h_2(n),\ n=1,2,\dots,$$

and for n sufficiently large

$$\gamma(n-1)^{k+\beta} < g(n) < \gamma(n+k+1)^{k+\beta},$$

which means that

$$\mathrm{GKdim}(A) = \lim_{n\to\infty} \frac{\log g(n)}{\log n} = k+\beta = \alpha. \quad \square$$

References

[BK] W. Borho, H. Kraft, Über die Gelfand-Kirillov Dimension, Math. Ann. **220** (1976), 1-24.

[KL] G.R. Krause, T.H. Lenegan, Growth of Algebras and Gelfand-Kirillov Dimension, Pitman Publ., London, 1985.

[P] V.M. Petrogradsky, On Lie algebras with nonintegral q-dimensions, Proc. Amer. Math. Soc. **125** (1997), 649-656.

[S] M.K. Smith, Universal enveloping algebras with subexponential but not polynomially bounded growth, Proc. Amer. Math. Soc. **60** (1976), 22-24.

[U] V.A. Ufnarovsky, Combinatorial and asymptotic methods in algebra, in A.I. Kostrikin, I.R. Shafarevich (Eds.), “Algebra VI”, Encyclopaedia of Mathematical Sciences **57**, Springer-Verlag, 1995, 1-196.

6. ALGEBRAS WITH INTERMEDIATE GROWTH

Let A be a finitely generated algebra with growth function $g(n)$.

Definition 6.1. The algebra A is called an algebra with intermediate growth if its growth function is of intermediate growth. □

By Definition 3.4 and Exercise 5.3 this means that for for any $p \in \mathbb{N}$ and any $\alpha > 1$

$$n^p < g(n) < \alpha^n$$

for all sufficiently large n. Lemma 5.4 easily implies that the property of intermediate growth does not depend on the set of generators of A.

Exercise 6.2. Show that A is with intermediate growth if and only if $g(n)$ grows faster than any polynomial function $p(n)$ and $\lim_{n\to\infty}\left(g(n)^{1/n}\right) = 1$. (See Exercise 5.3 for the existence of $\lim_{n\to\infty}\left(g(n)^{1/n}\right)$.)

Hint. If $g(n)$ grows faster than a polynomial, then $\lim_{n\to\infty}\left(g(n)^{1/n}\right) \geq 1$. The inequality $\lim_{n\to\infty}\left(g(n)^{1/n}\right) > 1$ is equivalent to the fact that $g(n) > \alpha^n$ for some $\alpha > 1$ and n sufficiently large. □

If A is a graded algebra and its Hilbert series is a rational function then by Theorem 3.5 the growth of the coefficients of $H(A,t)$ is either polynomial or exponential and this gives that the growth function of A is also either of polynomial or exponential growth. One may expect that the algebras with intermediate growth are exotic and big exceptions in the class of all algebras. In this chapter we shall show that this is not the case and shall give examples of algebras with intermediate growth obtained with natural constructions. The first examples were obtained by Borho and Kraft [BK] and Martha Smith [Sm], see also [KL]. Lichtman [L] showed that the class of algebras with intermediate growth is quite large and Ufnarovsky [U] found that there exist finitely presented algebras with intermediate growth. Recently Petrogradsky [P] started to build the theory of algebras with intermediate growth introducing a refined scale for measuring the growth.

We shall give a simple example of a two-generated algebra with intermediate growth. The exposition is based on the paper of Smith [Sm]. We fix the following formal products and express them as formal power series

$$c(t) = \prod_{k\geq 1}\frac{1}{1-t^k} = \sum_{n\geq 0} c_n t^n,$$

$$d(t) = \frac{1}{1-t}\prod_{k\geq 1}\frac{1}{1-t^k} = \sum_{n\geq 0} d_n t^n,$$

$$h(t) = \frac{d(t)}{1-t} = \sum_{n\geq 0} h_n t^n.$$

Clearly the series are with positive coefficients and

$$d_n = c_0 + c_1 + \ldots + c_n,\ h_n = d_0 + d_1 + \ldots + d_n,\ 1 = h_0 < h_1 < \ldots$$

Lemma 6.3. The coefficients h_n grow faster than any polynomial function, i.e. for any $p \in \mathbb{N}$ we have $h_n > n^p$ for sufficiently large n.

Proof. We use the formalism of comparing the coefficients of formal power series. Since $(1-t^k)^{-1} > 1$, we obtain

$$h(t) > \prod_{k=1}^{p+2} = \prod_{k+1}^{p+2}(1+t^k+t^{2k}+\dots) >$$

$$> \left(1+t^{(p+2)!}+t^{2(p+2)!}+\dots\right)^{p+2} =$$

$$= \frac{1}{(1-t^{(p+2)!})^{p+2}} = \sum_{n\geq 0}\binom{n+p+1}{p+1}t^{n(p+2)!}$$

and $h_{n(p+2)!} > an^{p+1}$ for some positive $a \in \mathbb{R}$ and sufficiently large n. Since the sequence $\{h_n\}_{n\geq 0}$ is monotone increasing, we obtain that

$$h_n \geq a\left[\frac{n}{(p+2)!}\right]^{p+1} > n^p$$

for sufficiently large n. □

Proposition 6.4. For any $\alpha > 1$ and for n sufficiently large we have $h_n < \alpha^n$.

Proof. If for some $\alpha > 1$ there exists a sequence $1 \leq n_1 < n_2 < \dots$ such that $h_{n_i} \geq \alpha^{n_i}$, then the radius of convergence r of $h(t)$ would be bounded by $\frac{1}{\alpha} < 1$. Since $h(t) > \frac{1}{1-t}$, we know that $r \leq 1$ and we shall show that $r = 1$. It is sufficient to show this for the series $c(t)$. We shall see that the function $c(t)$ is well defined for any $q \in (0,1)$ and this will complete the proof. Let us consider the function

$$f(t) = \frac{\ln(1-t)}{t},\ t \in (0,q), 0 < q < 1.$$

By the L'Hôpitale Rule

$$\lim_{t\to 0} f(t) = \frac{\lim_{t\to 0}(\ln(1-t))'}{t'} = \lim_{t\to 0}\left(\frac{-1}{1-t}\right) = -1.$$

Since $f(t)$ is continuous in $(0,q)$, this implies that $f(t)$ it is bounded and there exist $a,b > 0$ such that $-a < f(t) < -b$, $t \in (0,q)$. Let

$$p_n(t) = \prod_{k=1}^{n}\frac{1}{1-t^k}.$$

Using that $0 < q^k \leq q$, $k = 1,2,\dots,$ we obtain that

$$-aq^k < \ln(1-q^k) < -bq^k,\ bq^k < -\ln(1-q^k) < aq^k,$$

$$\ln p_n(q) = -\sum_{k=1}^{n}\ln(1-q^k),$$

$$b(q+q^2+\dots+q^n) \leq \ln p_n(q) \leq a(q+q^2+\dots+q^n).$$

Since

$$q+q^2+\dots+q^n=\frac{q(1-q^n)}{1-q},$$

$$q=\frac{q(1-q)}{1-q}\leq\frac{q(1-q^n)}{1-q}\leq\frac{q}{1-q},$$

we derive that

$$bq\leq\ln p_n(q)\leq\frac{aq}{1-q},\ e^{bq}\leq p_n(q)\leq e^{\frac{aq}{1-q}}.$$

Since $\{p_n(q)\}_{n\geq 1}$ is a monotone increasing sequence, $\lim_{n\to\infty}p_n(q)$ exists and is finite. Hence $h(q)$ is well defined for any $q\in(0,1)$. Using that the partial sum

$$h_0+h_1q+h_2q^2+\dots+h_nq^n$$

is bounded by

$$\frac{1}{(1-q)^2}\prod_{k=1}^{n}\frac{1}{1-q^k}=\frac{1}{(1-q)^2}p_n(q),$$

we obtain that the radius of convergence of $h(t)$ is equal to 1. □

Lemma 6.3 and Proposition 6.4 immediately give:

Corollary 6.5. The coefficients h_n of the formal power series $h(t)$ are of intermediate growth. □

Let $X=\{x,y\}$ and let L be the Lie algebra with defining relations $w=0$, where $w=[\dots,y,\dots,y,\dots]$ runs on the set of all commutators (with any bracket decomposition) containing two or more symbols y (i.e. $\deg_y w\geq 2$).

Lemma 6.6. The algebra L has a basis

$$\{x,y,[y,\underbrace{x,\dots,x}_{n-1}]\mid n\geq 2\}.$$

Proof. Let W be the ideal generated by all w in the free Lie algebra $L(x,y)$. Since $L(x,y)$ is a multigraded vector space, we obtain that

$$W=\sum_{p\geq 1}\sum_{q\geq 2}L(x,y)^{(p,q)},$$

where $L(x,y)^{(p,q)}$ is the multihomogeneous component of degree (p,q) of $L(x,y)$. Hence as a multigraded vector space

$$L=L(x,y)/W=L(x,y)^{(1,0)}\oplus L(x,y)^{(0,1)}\oplus\sum_{p\geq 1}{}^{\oplus}L(x,y)^{(p,1)}.$$

Since $L(x,y)^{(1,0)}$ and $L(x,y)^{(0,1)}$ are one-dimensional vector spaces spanned respectively on x and y, it is sufficient to see that $L(x,y)^{(p,1)}$, $p\geq 1$, is also one-dimensional and spanned on the commutator $[y,\underbrace{x,\dots,x}_{p}]$. This is obvious because the anticommutativity law gives that $[y,\underbrace{x,\dots,x}_{p}]$ is the only commutator containing a single symbol y and p symbols x. Clearly this commutator is not equal to 0 in $L(x,y)$. □

Theorem 6.7. The universal enveloping algebra of the Lie algebra L defined above is with intermediate growth.

Proof. By the Poincaré-Birkhoff-Witt Theorem 2.4 and by Lemma 6.6, the universal enveloping algebra $U = U(L)$ has a basis

$$\{x^a y^b \prod_{n\geq 2} [y, \underbrace{x, \ldots, x}_{n-1}]^{b_n} \mid a, b, b_n \geq 0\}$$

which is homogeneous with respect to the usual grading of $K\langle x, y\rangle$. Hence the Hilbert series of U is

$$H(U,t) = \frac{1}{1-t} \prod_{k\geq 1} \frac{1}{1-t^k} = d(t) = \sum_{n\geq 0} d_n t^n.$$

Since the growth function $g(n)$ of U satisfies

$$g(n) = d_0 + d_1 + \ldots + d_n,$$

we obtain that $g(n) = h_n$, where

$$h(t) = \sum_{n\geq 0} h_n t^n = \frac{1}{1-t} d(t).$$

Now Corollary 6.5 gives that the coefficients h_n are of intermediate growth. □

Remark 6.8. The coefficient c_n of the series

$$c(t) = \prod_{k\geq 1} \frac{1}{1-t^k} = \sum_{n\geq 0} c_n t^n$$

is equal to the number of partitions of n. The asymptotic behaviour of the sequence $\{c_n\}_{n\geq 0}$ is well know (see e.g. [H, equation (4.2.8)] or [A]) and is

$$c_n \sim \frac{1}{4n\sqrt{3}} \exp\left(\pi\sqrt{\frac{2n}{3}}\right).$$

This gives directly that the growth of $U(L)$ is intermediate. □

There was a conjecture of Borho and Kraft [BK] that the finitely presented associative algebras cannot be with intermediate growth. Repeating the arguments of the proof of Theorem 6.7 (and replacing $H(U(L),t)$ with the generalized Hilbert series of $U(L)$, it is sufficient to show that there exists a finitely presented and infinite dimensional Lie algebra with polynomial growth. The easiest example is the Witt algebra L of the derivations of $K[z]$. The algebra L has a basis $\{a_n \mid n = -1, 0, 1, 2, \ldots\}$ and multiplication table $[a_i, a_j] = (i-j)a_{i+j}$. It is generated by a_{-1} and a_2. A finite set of defining relations of L was found by Stewart [St]. Changing the notation and assuming that L is generated by x_{-1}, x_0, x_1, x_2 and introducing the notation

$$x_{i+1} = \frac{1}{i-1}[x_i, x_1],\ i \geq 2,$$

the defining relations of L are

$$[x_{-1},x_0]=-x_{-1},\ [x_{-1},x_1]=-2x_0,\ [x_{-1},x_2]=-3x_1,$$

$$[x_0,x_1]=-x_1,\ [x_0,x_2]=-2x_2,\ [x_2,x_3]=-x_5,\ [x_2,x_5]=-3x_7.$$

Other examples of finitely presented and infinite dimensional Lie algebras with polynomial growth can be found in the paper of Kac [K]. The simplest example among the algebras of Kac is L generated by e_1,e_2,f_1,f_2,h and with defining relations

$$[e_i,f_j]=\delta_{ij}h,\ [h,e_i]=2e_i,\ [h,f_i]=-2f_i,\ i=1,2,$$

$$[e_2,e_1,e_1,e_1]=[e_1,e_2,e_2,e_2]=0,$$

$$[f_2,f_1,f_1,f_1]=[f_1,f_2,f_2,f_2]=0.$$

By the result of Lichtman [L] the intermediate growth of $U(L)$ holds for every infinite dimensional finitely generated Lie algebra L which has an ideal I such that I is solvable and $\dim L/I<\infty$.

References

[A] G.E. Andrews, The Theory of Partitions, Encyclopedia of Math. and Its Appl. **2**, Addison-Wesley, Reading, Mass., 1976.

[BK] W. Borho, H. Kraft, Über die Gelfand-Kirillov Dimension, Math. Ann. **220** (1976), 1-24.

[H] M. Hall, Combinatorial Theory, Blaisdell Publ. Comp., Watham, Mass.-Toronto-London, 1967.

[K] V.G. Kac, Simple irreducible Lie algebras with finite growth (Russian), Izv. AN SSSR, Ser. Mat. **32** (1968), 1323-1367.

[KL] G.R. Krause, T.H. Lenegan, Growth of Algebras and Gelfand-Kirillov Dimension, Pitman Publ., London, 1985.

[L] A.I. Lichtman, Growth of enveloping algebras, Israel J. Math. **47** (1984), 297-304.

[P] V.M. Petrogradsky, On Lie algebras with nonintegral q-dimensions, Proc. Amer. Math. Soc. **125** (1997), 649-656.

[Sm] M.K. Smith, Universal enveloping algebras with subexponential but not polynomially bounded growth, Proc. Amer. Math. Soc. **60** (1976), 22-24.

[St] I. Stewart, Finitely presented infinite-dimensional simple Lie algebras, Arch. Math. **26** (1975), 504-507.

[U] V.A. Ufnarovsky, On algebras' growth (Russian), Vestnik Moskov. Univ., Ser. Mat. Mekhan. (1978), No. 4, 59-65.