Sums of Finite Sets, Orbits of Commutative Semigroups, and Hilbert Functions

A. G. Khovanskii[†]

UDC 512.7+514.17

§1. Introduction

We can add subsets of a commutative semigroup: the sum $A+B$ of two subsets A and B of a commutative semigroup is the set of points z representable in the form $z=a+b$, where $a\in A$ and $b\in B$. Denote by $N*A$ the sum of N copies of the set A.

In [1] we proved the following

Theorem. *For any finite subsets A and B in a commutative semigroup G, the number of points of the set $B+N*A$ is a polynomial in N for sufficiently large positive integers N. The degree of this polynomial is less than the number of points of the set A.*

This polynomial is the Hilbert function of a finitely generated graded module over the ring of polynomials in several variables [1], and this proves the theorem.

This algebraic argument implies two natural questions:

(1) what is the relationship between the ring of polynomials in several variables and the calculation of the number of points in a set, and

(2) is it possible to avoid the application of the Hilbert theorem (see §8) in the proof of the above-mentioned combinatorial fact?

The present paper gives an answer to these two problems. We start with the second problem. Here we can do without the Hilbert theorem. Combinatorial arguments can give some more. Let us fix an arbitrary multiplicative character $\chi\colon G\to\mathbb{C}$, $\chi(a+b)=\chi(a)\cdot\chi(b)$.

Denote by $f(N)$ the sum of values of the character χ over all points of the set $B+N*A$.

Theorem 5. *For sufficiently large N, the function $f(N)$ is a quasipolynomial in N of the form $f(N)=\sum q_i^N P_i(N)$. The numbers q_i in this formula are the values of the character χ on the set A, and the functions P_i are polynomials of degree less than the number of points of the set A at which the values of this character are equal to q_i.*

For $\chi\equiv 1$ the function f calculates the number of points of the set $B+A*N$, and Theorem 5 coincides with the above-mentioned combinatorial fact. Generally speaking, the function f is not the Hilbert function of a graded module (the values $f(N)$ of this function are complex numbers that are not necessarily integers), and Theorem 5 cannot follow from the Hilbert theorem.

Theorem 5 is a manifestation of general properties of orbits of the semigroup $\mathbb{Z}_+^n$ that are described in this paper. Under the action of a group a set is decomposed into orbits, and each orbit has a simple description in group terms. For the case of a semigroup an orbit has no equally simple description. Moreover, the orbits of distinct points can intersect. How can we cut the set on which the semigroup acts into simple disjoint pieces? In §2 we give a partial answer to this question for well ordered semigroups.

For the semigroup $\mathbb{Z}_+^n$ this answer can be refined (see §4). The point is that *the semigroup $\mathbb{Z}_+^n$ is Noetherian* (see [2, 7]). This classical result plays the central role in the present paper. We present it in §3 together with an addition we need: *the complement of a $\mathbb{Z}_+^n$-ideal is representable in the form of the union of a finite number of disjoint shifted coordinate semigroups.*

The orbits of the action of the semigroup $\mathbb{Z}_+^n$ are sufficiently regular: they *decompose into disjoint unions of finite sets of orbits of coordinate semigroups* (see §4). Theorem 5 is a manifestation of this

[†] The research was partially supported by NSERS grant OGP01563833.

Institute for System Studies of the Russian Academy of Sciences and University of Toronto, Canada. Translated from Funktsional'nyi Analiz i Ego Prilozheniya, Vol. 29, No. 2, pp. 36–50, April–June, 1995. Original article submitted July 15, 1994.

regularity. In the proof of Theorem 5 we also use some *properties of the sum of values of an exponential function over all integral points of the standard simplex.* These properties are presented in §5.

Now let us come back to the first problem: what is the relationship between the ring of polynomials in several variables and the calculation of the number of points in a set? The calculation of the number of points in the set $B + N * A$ is based on some properties of the semigroup $\mathbb{Z}^n_+$. However, the ring of polynomials in n variables over a field K is just the semigroup algebra for $\mathbb{Z}^n_+$ over the field K. (As the remarkable construction of Gröbner bases shows, the Noetherian property of the semigroup $\mathbb{Z}^n_+$ implies the Noetherian property of the polynomial ring.)

A module over the ring of polynomials in n variables is a direct generalization of the action of the semigroup $\mathbb{Z}^n_+$ on a set. The existence theorem for a *special linear basis* in a module over the ring of polynomials in n variables (see §8) is a direct generalization of the theorem on the decomposition of orbits of the semigroup $\mathbb{Z}^n_+$ into orbits of coordinate semigroups. The theorem on the structure of orbits of a well ordered semigroup G (see §2) is a consequence of the theorem on the existence of a special linear basis in a module over the semigroup algebra of G (see §7). The special linear basis in a module over the polynomial ring *permits us to characterize the Hilbert functions of graded modules.* Let us fix a homomorphism $\gamma\colon \mathbb{Z}^n_+ \to \Gamma$, where Γ is a commutative semigroup. A module M over the polynomial ring $K[x_1, \dots, x_n]$ is said to be γ-graded if M as a linear space is representable as the direct sum $M = \sum_{\theta\in\Gamma} M_\theta$ of linear subspaces indexed by the elements of the semigroup Γ and if the following homogeneity condition holds: the monomial x^a, $a \in \mathbb{Z}^n_+$, maps the homogeneous space M_θ into the homogeneous space $M_{\theta+\gamma(a)}$. The function on the semigroup Γ that assigns the dimension of the homogeneous component M_θ to the element θ is called the Hilbert function of the γ-graded module M. In §8 we give a *complete description of the Hilbert function* for finitely generated γ-graded modules in terms of the homomorphism γ. For classical γ-gradations (which occur in homogeneous coordinate rings of algebraic subvarieties in the products of projective spaces) this description can easily be translated into analytical language and implies the fact that for large values of the arguments the Hilbert functions are polynomials.

For the case of a general gradation $\gamma\colon \mathbb{Z}^n_+ \to \mathbb{Z}^m_+$ the analytical nature of the Hilbert function turns out to be more complicated: *there exists a finite stratification of the semigroup $\mathbb{Z}^m_+$ such that the restriction of the Hilbert function to each stratum is a polynomial with periodic coefficients* (see §10). Note that a similar description of the Hilbert functions (and their asymptotic behavior) for these gradations was obtained in [6] in a different way. Our description is based on some properties (see §9) of the number of integral points in convex polytopes with rational vertices.

The present paper is an immediate continuation of [1]. The results of this paper were presented in 1991 at the seminars of V. I. Arnold and I. M. Gelfand in Moscow and in 1992 at the seminar of D. Kazhdan at Harvard.

§2. Action of Ordered Semigroups on Sets

In this section we show how a set X on which a well ordered semigroup G acts can be decomposed into sufficiently simple disjoint pieces.

By an action of a semigroup G on a set X we mean a homomorphism $\pi\colon G \to S(X)$, where $S(X)$ is the semigroup of mappings of X into itself. The semigroup G is said to be well ordered if on G a well ordering is introduced (i.e., every nonempty subset has the least element) that admits left multiplication (i.e., $g_1 > g_2$ implies $gg_1 > gg_2$).

A subset $\mathfrak{J} \subset G$ is called a *G-ideal* if it is invariant under the left multiplication, i.e., if the relations $h \in \mathfrak{J}$ and $g \in G$ imply $gh \in \mathfrak{J}$.

A set $J \subset G$ is called a *G-coideal* if its complement $G \setminus J$ is a G-ideal.

Let a set $U \subset X$ be invariant under the action of the semigroup G. The problem to be considered is to cut the set $X \setminus U$ into the simplest possible parts.

Example. Let $\aleph$ be a set of indices, let X be the union of disjoint copies G_α, $\alpha \in \aleph$, of the semigroup G, $X = \bigcup_{\alpha\in\aleph} G_\alpha$, and let $U = \bigcup_{\alpha\in\aleph} \mathfrak{J}_\alpha$, where $\mathfrak{J}_\alpha \subset G_\alpha$ is a G-ideal. The set $X \setminus U$ is decomposed into the union of disjoint G-coideals $J_\alpha = G_\alpha \setminus \mathfrak{J}_\alpha$.

Let us show that a similar decomposition of the set $X \setminus U$ into G-coideals exists for each action of a well ordered semigroup G. Suppose that the set $X \setminus U$ is contained in the union of orbits O_α of some elements $x_\alpha \in X$, $\alpha \in \aleph$.

Theorem 1. *The set $X \setminus U$ is representable in the form of the union of disjoint sets X_α, $\bigcup X_\alpha = X \setminus U$, $X_\alpha \cap X_\beta = \varnothing$ for $\alpha \neq \beta$, with the following property: for each index α the set X_α belongs to O_α and there exists a G-coideal J_α such that the mapping $g \to \pi(g)(x_\alpha)$ determines a one-to-one correspondence between J_α and the set X_α.*

Proof. We fix a well ordering of the indices $\alpha \in \aleph$ of the elements x_α. For each index α let us define an invariant set U_α as the union of the set U and the orbits O_β of all elements x_β with indices β less than α, $U_\alpha = (\bigcup_{\beta<\alpha} O_\beta) \cup U$. Let us define X_α as the set of points of the orbit O_α that do not belong to the invariant set U_α, $X_\alpha = O_\alpha \setminus U_\alpha$. Clearly, $\bigcup X_\alpha = X \setminus U$ and $X_\alpha \cap X_\beta = \varnothing$ for $\alpha \neq \beta$.

For each point x belonging to X_α we consider the subset $G(x) \subset G$ with the following property: $g \in G(x)$ if and only if $\pi(g)(x_\alpha) = x$. Let $g(x)$ be a minimal element of the set $G(x)$. (Such an element exists because the semigroup G is well ordered.) Define J_α as the set of elements $g(x)$ for all points $x \in X_\alpha$. By definition, the natural mapping $g \to \pi(g)(x_\alpha)$ is a one-to-one mapping of the set J_α onto X_α. Let us show that the complement $\mathfrak{J}_\alpha = G \setminus J_\alpha$ is a G-ideal. Note that the complement $\mathfrak{J}_\alpha$ is representable in the form of the union of the following sets $\mathfrak{J}_\alpha^1$ and $\mathfrak{J}_\alpha^2$: $g \in \mathfrak{J}_\alpha^1$ if and only if the point $\pi(g)(x_\alpha)$ belongs to the invariant set U_α, and $g \in \mathfrak{J}_\alpha^2$ if and only if there exists an element $a \in G$ such that $a < g$ and $\pi(a)(x_\alpha) = \pi(g)(x_\alpha)$. We will show that $\mathfrak{J}_\alpha^2$ is a G-ideal. Let $c \in G$ be an arbitrary element of the semigroup, let $g \in \mathfrak{J}_\alpha^2$, $a < g$, and let $\pi(a)(x_\alpha) = \pi(g)(x_\alpha)$. Then $ca < cg$ and $\pi(ca)(x_\alpha) = \pi(cg)x_\alpha$. Therefore, $cg \in \mathfrak{J}_\alpha^2$, and this proves the required assertion. Clearly, the set $\mathfrak{J}_\alpha^1$ is an G-ideal. Thus, $\mathfrak{J}_\alpha = \mathfrak{J}_\alpha^1 \cup \mathfrak{J}_\alpha^2$ is also a G-ideal. The theorem is proved.

§3. Semigroup $\mathbb{Z}_+^n$

Theorem 1 can be strengthened for the semigroup $\mathbb{Z}_+^n$. The point is that the semigroup $\mathbb{Z}_+^n$ possesses a kind of Noetherian property (e.g., see [2]). This property was discovered before the Hilbert theorem on the Noetherian property of the polynomial ring. Let us describe this classical result in the form we will need in the sequel.

By the octant $O^n(a)$ with vertex at a point $a \in \mathbb{Z}_+^n$, $a = (a_1, \dots, a_n)$, we mean the subset of integral points $b = (b_1, \dots, b_n)$ of $\mathbb{Z}_+^n$ that satisfy the inequalities $b_1 \geq a_1$, $\dots$, $b_n \geq a_n$. Clearly, an octant is a $\mathbb{Z}_+^n$-ideal.

Theorem (on the Noetherian property of the semigroup $\mathbb{Z}_+^n$). *Each $\mathbb{Z}_+^n$-ideal is the union of a finite number of octants (in other words, the union of an infinite family of octants is in fact the union of a finite number of octants).*

Proof. Induction on the dimension n. Let us isolate out the last coordinate x_n in $\mathbb{Z}_+^n$, i.e., put $\mathbb{Z}_+^n = \mathbb{Z}_+^{n-1} + \mathbb{Z}_+$. It is clear that

(1) the intersection of an octant by a horizontal plane $x_n = c$, $c \in \mathbb{Z}_+$, is an octant in the semigroup $\mathbb{Z}_+^{n-1}$ (after the last coordinate $x_n = c$ is deleted);

(2) the projection of an octant belonging to $\mathbb{Z}_+^n$ is an octant in $\mathbb{Z}_+^{n-1}$.

We now proceed to induction. Take the projection of the union of an infinite family of octants $\mathfrak{J} \subset \mathbb{Z}_+^n$ onto the coordinate plane $\mathbb{Z}_+^{n-1}$. By the induction assumption, the resulting union of $(n-1)$-dimensional octants coincides with the union of a finite number of octants. Let these be the octants with vertices $b^1, \dots, b^k$ $(b^i = (b_1^i, \dots, b_{n-1}^i))$. By construction, the octants are the projections of n-dimensional octants with some vertices $\tilde{b}^i$ $(\tilde{b}^i = (b_1^i, \dots, b_{n-1}^i, b_n^i))$. Let the maximal value of the last coordinates b_n^i of these vertices be $c \in \mathbb{Z}_+^n$. All points of the $\mathbb{Z}_+^n$-ideal $\mathfrak{J}$ for which the last coordinate is no less than c belong to the union of the octants $O^n(\tilde{b}^i)$. The remaining points of the $\mathbb{Z}_+^n$-ideal $\mathfrak{J}$ belong to the finite number of sections $x_n = 0$, $x_n = 1$, $\dots$, $x_n = c - 1$. By the induction assumption, each of these sections is covered by a finite number of $(n-1)$-dimensional octants. Now we see that the $\mathbb{Z}_+^n$-ideal $\mathfrak{J}$ consists of a finite number of octants $O^n(\tilde{b}^i)$ and a finite number of n-dimensional octants whose vertices belong to a finite set of sections.

The semigroup $\mathbb{Z}_+^n$ has 2^n *coordinate semigroups*: for each subset I of the segment $\{1, \dots, n\}$ of positive integers there is a subsemigroup $\mathbb{Z}_+(I)$ consisting of integral points $a = (a_1, \dots, a_n)$ such that $a_i = 0$ for $i \in I$ and $a_i \geq 0$ for $i \notin I$. The semigroups $\mathbb{Z}_+(I)$ include the zero semigroup (for $I = \{1, \dots, n\}$) and the semigroup $\mathbb{Z}_+^n$ (for $I = \varnothing$).

A subset of $\mathbb{Z}_+^n$ will be called a *shifted coordinate semigroup* if it has the form $a + \mathbb{Z}_+(I)$, where a is an element of $\mathbb{Z}_+^n$.

Theorem 2. *The complement of a $\mathbb{Z}_+^n$-ideal can be represented as the union of a finite number of disjoint shifted coordinate semigroups.*

Proof. 1) We first assume that the $\mathbb{Z}_+^n$-ideal is an octant $O^n(a)$ with vertex a. Let us represent the complement $\mathbb{Z}_+^n \setminus O^n(a)$ as the union of shifted coordinate semigroups. For each nonzero point a of $\mathbb{Z}_+^n$ we define the point $\pi(a)$ by the following rule: if $a = (a_1, \dots, a_n)$ and $a_1 = \dots = a_{i-1} = 0$, $a_i > 0$, then $\pi(a) = (a_1, \dots, a_{i-1}, a_i - 1, a_{i+1}, \dots, a_n)$. Obviously, the octant with vertex $\pi(a)$ contains the octant with vertex a, and their difference $O^n(\pi(a)) \setminus O^n(a)$ is a shifted coordinate semigroup. For the integral point $a = (a_1, \dots, a_n)$ we have $\pi^l(a) = 0$, where $l = \|a\| = \sum |a_i|$. Thus, we obtain the required decomposition

$$\mathbb{Z}_+^n \setminus O^n(a) = \bigcup_{l=1}^{\|a\|} O^n(\pi^l(a)) \setminus O^n(\pi^{l-1}(a)).$$

2) Each $\mathbb{Z}_+^n$-ideal is the union of a finite number of octants. Assume that the theorem holds when the $\mathbb{Z}_+^n$-ideal $\mathfrak{J}$ is the union of k octants. Let us prove the theorem for $k+1$ octants. We have $\mathfrak{J} = \mathfrak{J}_0 \cup O^n(a)$, where $\mathfrak{J}_0$ is the union of k octants. By induction, the complement of $\mathfrak{J}_0$ in $\mathbb{Z}_+^n$ is the union of shifted coordinate semigroups. In turn, in each shifted coordinate semigroup $\mathfrak{L}$ the complement of its intersection with the octant $\mathfrak{L} \setminus (\mathfrak{L} \cap O^n(a))$ can be decomposed into the union of shifted coordinate semigroups (see step 1 in the proof of this theorem). The theorem is proved.

§4. Action of the Semigroup $\mathbb{Z}_+^n$ on a Set

Suppose that on the set X an action $\pi \colon \mathbb{Z}_+^n \to S(X)$ of the semigroup $\mathbb{Z}_+^n$ is defined; let $U \subset X$ be a subset invariant with respect to this action. Let the set $X \setminus U$ belong to the union of orbits of some elements $x_\alpha \in X$.

Theorem 3. *There exists a decomposition of the set $X \setminus U$ into the union of disjoint sets $X_{\alpha,i}$, $1 \leq i \leq l(\alpha)$, where l is an integer-valued function of the index α, with the following property: for each pair of indices (α, i) there exists a point $a \in \mathbb{Z}_+^n$ and a coordinate semigroup $\mathbb{Z}_+(I)$ such that the mapping $g \to \pi(g+a)(x_\alpha)$ determines a one-to-one correspondence between this coordinate semigroup and the set $X_{\alpha,i}$.*

Proof. In the semigroup $\mathbb{Z}_+^n$ there is a well ordering (e.g., lexicographical). Therefore we can apply Theorem 1 to the action of this semigroup. To complete the proof, the $\mathbb{Z}_+^n$-coideals J_α in this theorem must be cut into shifted coordinate semigroups.

§5. Exponential Sums

Denote by $\Delta(m)$ the standard simplex $\{x = (x_1, \dots, x_n);\ x_1 + \dots + x_n = m;\ x_1 \geq 0, \dots, x_n \geq 0\}$ in the space $\mathbb{R}^n$. We define the function $F(m,p)$ depending on a positive integer m and a covector $p \in (\mathbb{R}^n)^*$ by the formula

$$F(m,p) = \sum_{x \in \Delta(m) \cap \mathbb{Z}^n} e^{px}.$$

Let e_i denote the basis vectors of the space $\mathbb{R}^n$. For each $i = 1, \dots, n$ we set

$$\mu_i(p) = \prod 1/(1 - \exp(p(e_i - e_j))),$$

where the multiplication extends over all j such that $j \neq i$, $1 \leq j \leq n$. The function $\mu_i(p)$ is meromorphic on the complexification of the space $(\mathbb{R}^n)^*$.

Proposition. *For each $m \geq 0$ and each covector p such that $p(e_i - e_j) \neq 0$ for any $1 \leq i < j \leq n$ we have*

$$F(m,p) = \sum_{1 \leq i \leq n} e^{m(pe_i)} \cdot \mu_i(p).$$

This proposition is a special case of a general result [3, 4] in which an arbitrary integral polytope is considered instead of the standard simplex $\Delta(m)$. It completely determines the function $F(m,p)$ if $p(e_i - e_j) \neq 0$ for any $1 \leq i < j \leq n$.

Let us pass to the general case. We fix a covector $p = p_0$. Let the sequence $(p_0 e_1), \dots, (p_0 e_n)$ contain exactly l distinct numbers $q_1, \dots, q_l$ and let the number q_i occur $k(i)$ times.

Theorem 4. *For each $m \geq 0$ the relation $F(p,m) = \sum q_i^m P_i(m)$ holds, where $P_i(m)$ is a polynomial in m of degree $< k(i)$.*

Theorem 4 follows from the above proposition for $p = p_0 + \lambda p_1$, where p_1 is a sufficiently generic covector and $\lambda \in \mathbb{R}$, under the passage to the limit as $\lambda \to 0$.

§6. Sum of Values of a Character Over the Set $B + N * A$

We can add subsets of a commutative semigroup: the sum $A + B$ of two subsets A and B of a commutative semigroup G is the set of points z representable in the form $z = a + b$, where $a \in A$ and $b \in B$. Let us fix some finite subsets $A, B \subset G$. Choose an arbitrary character χ of the semigroup G, i.e., a homomorphism $\chi\colon G \to \mathbb{C}$ of the semigroup G into the multiplicative semigroup of complex numbers, $\chi(a+b) = \chi(a) \cdot \chi(b)$. Let $q_1, \dots, q_l \in \mathbb{C} \setminus 0$ be the set of nonzero values of the character χ on the set A and let $k(i)$ be the number of points in the set A at which the character χ is equal to q_i.

We denote by $N * A$ the sum of N copies of the set A.

Theorem 5. *For sufficiently large positive integers N the sum of values of the character χ over all points of the set $B + N * A$ is equal to $\sum_{i=1}^{l} q_i^N P_i(N)$, where P_i is a polynomial in N of degree $< k(i)$.*

Proof. 1) Let us index the elements of the set A, i.e., let $A = \{a_i\,;\, i = 1, \dots, n\}$. Consider the semigroup $\mathbb{Z}_+^n$ and the homomorphism $\pi_1\colon \mathbb{Z}_+^n \to G$ that maps the standard generators $e_1, \dots, e_n$ into the elements $a_1, \dots, a_n \in A$. Denote by $\pi_2\colon \mathbb{Z}_+^n \to \mathbb{Z}_+$ the standard homomorphism defined by the relation $\pi_2(x_1, \dots, x_n) = x_1 + \dots + x_n$, $x_i \in \mathbb{Z}_+$.

We denote by $\overline{G}$ the direct sum of the semigroups G and $\mathbb{Z}_+$, $\overline{G} = G \oplus \mathbb{Z}_+$, and by $\pi\colon \mathbb{Z}_+^n \to \overline{G}$ the direct sum of the homomorphisms π_1 and π_2. Let $\overline{B}$ and $\overline{A}$ be the following subsets of the semigroup $\overline{G}$: $\overline{B} = (B, 0)$, $\overline{A} = (A, 1)$. The semigroup $\mathbb{Z}_+^n$ acts on $\overline{G}$ according to the following rule: an element $c \in \mathbb{Z}_+^n$ maps a point $g \in \overline{G}$ into the point $g + \pi(c)$. Denote by X the union of the orbits for the points of the set $\overline{B}$ with respect to this action and by X_N the subset of X consisting of the points whose second coordinate is N. Clearly, X_N coincides with the set $(B + N * A, N)$.

2) Let us extend the character $\chi\colon G \to \mathbb{C}$ to a character $\overline{\chi}\colon \overline{G} \to \mathbb{C}$ by the formula $\overline{\chi}(g, m) = \overline{\chi}(g)$. Denote by U the set of points at which the character $\overline{\chi}$ vanishes. The set U is invariant under the action of the semigroup $\overline{G}$ and, consequently, under the action of $\mathbb{Z}_+^n$. We are interested in the sum $\sum_{x \in B+N*A} \chi(x)$. It is clear that this sum is equal to $\sum_{x \in X_N \setminus U} \overline{\chi}(x)$.

3) We can apply Theorem 3 to the set $X \setminus U$. By this theorem, the set $X \setminus U$ is the disjoint union of some sets $X_{b,i}$, where $b \in \overline{B}$, $1 \leq i \leq l(b)$, and $l\colon \overline{B} \to \mathbb{Z}$ is an integer-valued function on $\overline{B}$. Moreover, there exist $c \in \mathbb{Z}_+^n$ and a coordinate semigroup $\mathbb{Z}_+(I)$ (that depend on the indices (b, i)) for which the mapping $q\colon \mathbb{Z}_+(I) \to X_{b,i}$ determined by the formula $q(x) = \pi(x + c)(b)$ is an isomorphism.

The preimage of the set $X_{b,i,N} = X_{b,i} \cap (X_N \setminus U)$ in $\mathbb{Z}_+(I)$ is the standard simplex $\{x = (x_1, \dots, x_n)\,;$ $\sum x_k = N - \pi_2(c)$, $x_k \geq 0$ for $k \notin I$ and $x_k = 0$ for $k \in I\}$. By Theorem 4, for $N \geq \pi_2(c)$ the sum of values of the character χ over the set $X_{b,i,N}$ is equal to $\sum q_j^{N - \pi_2(c)} \cdot P_{j,b,i}(N)$, where $\{q_j\}$ is the set of values of the character χ on the elements $a_k \in A$ for $k \notin I$ and $P_{j,b,i}$ are polynomials of degree less than the number of points $a_k \in A$ with $k \in I$ for which the character χ is equal to q_j. Thus, the theorem is proved if "sufficiently large" numbers N are understood as the numbers $N \geq \max \pi_2(c)$, where the maximum is taken over a finite set of points c.

§7. Modules Over the Semigroup Algebra of a Well Ordered Semigroup

The notion of a module over a semigroup algebra is a straightforward generalization of the notion of action of a semigroup on a set. In this section we describe the Gröbner construction for the semigroup algebra of a well ordered semigroup and the special linear bases in modules over such semigroups. We will also explain why the existence of these special linear bases proves Theorem 1 on the decomposition of an orbit of a well ordered semigroup into simple pieces.

With a semigroup G and a field K the semigroup algebra $K(G)$ consisting of formal linear combinations of elements of the semigroup G with coefficients belonging to the field K is associated. The multiplication in G is extended to the multiplication in $K(G)$ by linearity.

For an ordered semigroup G there exists the remarkable Gröbner mapping Grb from $K(G) \setminus 0$ into G that assigns to each nonzero linear combination $a = \sum \lambda(g)g$ the greatest element $g \in G$ that enters a with a nonzero coefficient $\lambda(g)$. Because the ordering in G is preserved under left multiplication, for $g \in G$ and $a \in K(G)$ we have $\mathrm{Grb}(g \cdot a) = g \cdot \mathrm{Grb}(a)$. With a left ideal $\mathfrak{J}$ of the algebra $K(G)$ the following objects are associated:

(1) its Gröbner G-ideal, which is the image of the set of nonzero elements of the ideal $\mathfrak{J}$ under the Gröbner mapping,

(2) its Gröbner G-coideal, which is the complement in G of the Gröbner ideal of $\mathfrak{J}$,

(3) its Gröbner coideal in $K(G)$, which is the linear subspace of $K(G)$ spanned by the elements of the Gröbner G-coideal.

The following assertion is well known.

Proposition. *The algebra $K(G)$ as a linear space is the direct sum of the ideal $\mathfrak{J}$ and its Gröbner coideal.*

Proof. By definition, the ideal $\mathfrak{J}$ and its Gröbner coideal L intersect only at the point 0. Let us show that each element $a \in K(G)$ belongs to the sum $L + \mathfrak{J}$. For every element $a = \sum \lambda(g)g$ not belonging to L we denote by $\mathrm{Grb}_L(a)$ the greatest of the elements $g \in \mathrm{Grb}(\mathfrak{J} \setminus 0)$ that enter a with nonzero coefficients $\lambda(g)$. By subtracting from a an element $\lambda_1 b_1$ of the ideal $\mathfrak{J}$ for which $\mathrm{Grb}(\lambda_1 b_1) = \mathrm{Grb}_L(a)$, where λ_1 is an appropriate coefficient, we can obtain either $a - \lambda_1 b_1 \in L$ or $\mathrm{Grb}_L(a - \lambda_1 b_1) < \mathrm{Grb}_L(a)$. If the element $a_1 = a - \lambda_1 b_1$ does not belong to L, then the process can be iterated. Since in a well-ordered set any descending chain terminates, after a finite number of steps we obtain the relation $a - \sum \lambda_i b_i \in L$, where $b_i \in \mathfrak{J}$. The proposition is proved.

Corollary 1. *Let $\mathfrak{J}_1$ and $\mathfrak{J}_2$ be ideals of the algebra $K(G)$ such that $\mathfrak{J}_1 \subseteq \mathfrak{J}_2$ and the Gröbner G-ideals for $\mathfrak{J}_1$ and $\mathfrak{J}_2$ coincide. Then $\mathfrak{J}_1 = \mathfrak{J}_2$.*

Indeed, the Gröbner G-coideals for the ideals $\mathfrak{J}_1$ and $\mathfrak{J}_2$ coincide. Therefore, $\mathfrak{J}_1 = \mathfrak{J}_2$ by the proposition.

Corollary 2. *The elements $g_\alpha \in \mathfrak{J}$ generate the ideal $\mathfrak{J}$ if and only if their images under the Gröbner mapping generate the Gröbner G-ideal for $\mathfrak{J}$.*

Corollary 2 follows from Corollary 1.

Consider a $K(G)$-module M and its submodule M_1. Let a set $B = \{m_\alpha\}$ of vectors $m_\alpha \in M$, $\alpha \in \aleph$, generate the quotient module M/M_1.

Theorem 6. *There exists a set of G-coideals $J_\alpha \subset G$ such that the elements $h(m_\alpha)$, $\alpha \in \aleph$, $h \in J_\alpha$, $m_\alpha \in B$, form a basis in the linear quotient space M/M_1.*

Proof. Let us choose an arbitrary well ordering of the set $\aleph$ of indices. For each index $\alpha \in \aleph$ we define the submodules $M_\alpha^{<}$ and $M_\alpha^{\leqq}$ generated by the submodule M_1 and all elements $m_\beta \in B$ such that $\beta < \alpha$ and $\beta \leq \alpha$, respectively. Consider the ideal $\mathfrak{J}_\alpha$ that consists of elements $a \in K(G)$ such that for each vector m belonging to the module $M_\alpha^{\leqq}$ the vector $a(m)$ belongs to the module $M_\alpha^{<}$. By the foregoing proposition, the elements $g(m_\alpha)$, $g \in J_\alpha$, where J_α is the Gröbner G-coideal of the ideal $\mathfrak{J}_\alpha$, span the quotient space $M_\alpha^{<}/M_\alpha^{\leqq}$. This implies the theorem.

Let us show that Theorem 1 in §2 is in fact a consequence of Theorem 6. The action of the semigroup G on X is extended by linearity to the action of the semigroup algebra $K(G)$ on the K-linear space

$C_0(X, K)$, where $C_0(X, K)$ is the space of zero-dimensional chains in the set X with coefficients belonging to the field K.

In the invariant subset U the zero-dimensional chains $C_0(U, K)$ form a $K(G)$-submodule of the module $C_0(X, K)$. If the set $X \setminus U$ belongs to the union of the orbits O_α of elements $x_\alpha \in X$, then the quotient module of $C_0(X, K)$ by $C_0(U, K)$ is generated by the vectors m_α, where m_α is the zero-dimensional chain that consists of the point x_α with coefficient 1. Applying Theorem 6 to the modules $C_0(X, K) \supset C_0(U, K)$ and the vector set $\{m_\alpha\}$, we obtain Theorem 1.

§8. Modules Over Polynomial Rings and Their Hilbert Functions

The foregoing combinatorial considerations give some information about modules over polynomial rings. To each point $a \in \mathbb{Z}_+^n$, $a = (a_1, \ldots, a_n)$, there corresponds a monomial $x^a = x_1^{a_1} \cdots x_n^{a_n}$. The semigroup algebra $K(\mathbb{Z}_+^n)$ is the ring $K[x_1, \ldots, x_n]$ of polynomials in n variables over the field K. Since the semigroup $\mathbb{Z}_+^n$ is Noetherian, the polynomial ring is also Noetherian (see §3 and Corollary 2 §7).

Let M be a finitely generated module over the polynomial ring in n variables, let M_1 be submodule of M, and let $\{m_\alpha\}$ be the set of elements determining a basis in the quotient module M/M_1. For each subset I in the set of the variables $x_1, \ldots, x_n$ we denote by Ξ_I the set of monomials that do not depend on the variables belonging to the subset I.

Theorem 7. *For each pair of indices (α, i), $1 \le i \le l(\alpha)$, where l is an integer-valued function of the index α, there is a point $a \in \mathbb{Z}_+^n$ and a subset I of the set of the variables $x_1, \ldots, x_n$ such that the set of all vectors of the form $x^a \cdot x^\mu(m_\alpha)$, where $x^\mu \in \Xi_I$, generates a basis in the linear quotient space M/M_1.*

Proof. Because the semigroup $\mathbb{Z}_+^n$ can be well ordered, we can apply Theorem 2 to the modules $M_1 \subset M$ over the polynomial ring. To complete the proof we must cut the $\mathbb{Z}_+^n$-coideals J_α in this theorem into shifted coordinate semigroups.

Note that Theorem 3 can be derived from Theorem 7 in just the same way as Theorem 1 is derived from Theorem 6 (see §7).

Denote by $\widetilde{N}$ the set of positive integers supplemented with the number 0 and the symbol $+\infty$. In $\widetilde{N}$ a natural operation of addition is defined not only for a finite but also for an infinite set of elements. The dimensions of linear spaces take on the values belonging to $\widetilde{N}$. Moreover, the dimension of the direct sum of any set of linear spaces is equal to the sum of their dimensions.

Let us choose a homomorphism $\gamma\colon \mathbb{Z}_+^n \to \Gamma$, where Γ is a commutative semigroup.

Definition. A module M over the polynomial ring $K[x_1, \ldots, x_n]$ is said to be *γ-graded* if M as a linear space can be represented in the form of the direct sum of linear subspaces, $M = \sum_{\theta \in \Gamma} M_\theta$, indexed by the elements of the semigroup Γ and the following homogeneity condition holds: the monomial x^a, $a \in \mathbb{Z}_+^n$, maps the homogeneous space M_θ into the homogeneous space $M_{\theta + \gamma(a)}$. The function $H : \Gamma \to \widetilde{N}$ that assigns the dimension of the homogeneous component M_θ to the element θ is called the *Hilbert function* of the γ-graded module M.

What functions $H : \Gamma \to \widetilde{N}$ can be Hilbert functions of finitely generated γ-graded modules M? Below we give a complete answer to this question, but first we state some definitions.

In the space of functions on the semigroup Γ with values in $\widetilde{N}$ the convolution operation can be defined:

$$f * g(\theta) = \sum_{\theta_1 + \theta_2 = \theta} f(\theta_1) \cdot g(\theta_2).$$

With a homomorphism $\gamma\colon \mathbb{Z}_+^n \to \Gamma$ we associate 2^n functions on Γ, which will play the key role in our study. With each subset $I \subset (1, \ldots, n)$ we associate a coordinate semigroup $\mathbb{Z}_+(I) \subseteq \mathbb{Z}_+^n$ and the function $f_I\colon \Gamma \to \widetilde{N}$ that assigns the number of points of the set $\gamma^{-1}(\theta) \cap \mathbb{Z}_+(I)$ to the element $\theta \in \Gamma$.

Theorem 8. *The Hilbert function $H\colon \Gamma \to \widetilde{N}$ of a finitely generated γ-graded $K[x_1, \ldots, x_n]$-module is representable in the form*

$$H = \sum_I f_I * g_I, \tag{1}$$

where g_I is a nonnegative integer-valued function on Γ that vanishes everywhere except for a finite number of points. Conversely, each function H of the form (1) is the Hilbert function of a γ-graded module.

Proof. 1) Let us choose a finite number of homogeneous generators m_α in the module M. By Theorem 7, the graded linear space M is the direct sum of a finite number of graded subspaces $M(\alpha, i)$ generated by the vectors $x^\alpha \cdot x^\mu(m_\alpha)$, where $\mu \in \mathbb{Z}_+(I)$. Denote by b the element of the semigroup Γ which is equal to $\gamma(a) + g(m_\alpha)$, where $g(m_\alpha)$ is the gradation of the element m_α. The dimension of the homogeneous component of the space $M(\alpha, i)$ with gradation θ is equal to $f_I * \delta_b(\theta)$, where δ_b is the function that is equal to 1 at the point b and vanishes at the other points. This implies the first assertion of the theorem.

2) To prove the other assertion of the theorem, consider the following example of a γ-graded module over the ring $K[x_1, \dots, x_n]$. We take the quotient ring of the polynomial ring $K[x_1, \dots, x_n]$ by the ideal generated by the variables x_i, $i \in I$. Let us endow this module with γ-gradation by the following rule: the gradation of the equivalence class of the monomial x^μ, $\mu \in \mathbb{Z}_+(I)$, is equal to $b + \gamma(\mu)$, where b is a fixed element of the semigroup Γ. The Hilbert function H of this module is equal to $f_I * \delta_b$; therefore each function of the form (1) is the Hilbert function of the direct sum of modules of this type.

Corollary. *If the semigroup Γ can be embedded into a group, then the Hilbert function of each γ-graded module is a linear combination of a finite number of functions $f_I(\theta - b)$ with positive integral coefficients.*

Example 1. The simplest and, of course, the most important example is the $K[x_1, \dots, x_n]$-modules with ordinary integer-valued gradation $\gamma\colon \mathbb{Z}^n \to \mathbb{Z}$, where $\gamma(a_1, \dots, a_n) = a_1 + \dots + a_n$. This gradation occurs in homogeneous coordinate rings of projective varieties. In this case the functions $f_I(N)$ have a simple geometric meaning: they are the numbers of integral points in the simplex $\{a = (a_1, \dots, a_n);\ a_1 + \dots + a_n = N,\ a_j \geq 0,\ a_j = 0 \text{ for } j \in I\}$. Simple calculation shows that if the number $p = n - |I|$ of nonzero variables is positive, then $f_I(N) = C^{p-1}_{N+p-1}$. If $p = 0$, then $f_I(0) = 1$ and $f_I(N) = 0$ for $N > 0$. Therefore the number $f_I(N)$ is a polynomial for $N > 0$. The shifted functions $f_I(N - b)$ are polynomials for $N > b$.

This implies the following remarkable

Hilbert Theorem. *Beginning with some positive integer, the Hilbert function H of a finitely generated module with ordinary gradation is a polynomial.*

Now we present a complete description of the function H. Let us define the function $\overline{C}^k_N$ of two integral variables by the following formula:

(1) if $0 \leq k \leq N$, then $\overline{C}^k_N = C^k_N$,

(2) if $k = N = -1$, then the function $\overline{C}^k_N$ is equal to 1,

(3) for the other values of k and N the function $\overline{C}^k_N$ is equal to zero.

Theorem 8 shows that the Hilbert function H of a finitely generated $K[x_1, \dots, x_n]$-module with the gradation in Example 1 has the following form:

$$H(N) = \sum a_{k,l} \overline{C}^{k-1}_{N+k-l-1},$$

where l, k, and $a_{k,l}$ are nonnegative integers and $k \leq n$.

Example 2. A somewhat more complicated example is the gradation $\gamma\colon \mathbb{Z}^n_+ \to \mathbb{Z}^m_+$ that depends on the parameters $i_1, \dots, i_m$ related by the condition $i_1 + \dots + i_m = n$. Let $c_0 = 0$, $c_1 = i_1$, $c_2 = i_1 + i_2$, $\dots$, $c_m = i_1 + \dots + i_m = n$, and let $\gamma(a_1, \dots, a_n) = (N_1, \dots, N_m)$, where $N_l = \sum_{c_{l-1} < j \leq c_l} a_j$. This gradation occurs in homogeneous coordinate rings of subvarieties in the product of projective spaces $\mathbb{C}P^{i_1 - 1} \times \dots \times \mathbb{C}P^{i_m - 1}$. The function $f_I(N)$, $N = (N_1, \dots, N_m)$, has a simple geometric meaning: it is the number of integral points in the product of simplexes $\{(a_{c_{l-1}+1}, \dots, a_{c_l});\ \sum_{c_{l-1} < j \leq c_l} a_j = N_l,\ a_j \geq 0,\ a_j = 0 \text{ for } j \in I\}$. This number $f_I(N)$ is equal to $\overline{C}^{p_1 - 1}_{N_1 + p_1 - 1} \cdots \overline{C}^{p_m - 1}_{N_m + p_m - 1}$, where p_l is the number of indices j, $c_{l-1} < j \leq c_l$, such that $j \notin I$.

Theorem 8 shows that the Hilbert function H of a finitely generated $K[x_1, \dots, x_n]$-module with the gradation in Example 2 has the following form:

$$H(N_1, \dots, N_m) = \sum a_{k,l} \prod \overline{C}^{k_j-1}_{N_j+k_j-l_j-1},$$

where $k = (k_1, \dots, k_m)$, $l = (l_1, \dots, l_m)$; all numbers k_j, l_j, $a_{k,l}$ are nonnegative integers and $k_j \leq l_j$. In particular, the function $H(N_1, \dots, N_m)$ is a polynomial if all coordinates N_j are sufficiently large.

§9. Integral Points in Rational Polytopes

To each face Γ of a convex bounded polytope $\Delta \subset \mathbb{R}^n$ there corresponds a convex cone K_Γ in the dual space $(\mathbb{R}^n)^*$. Namely, a covector ξ belongs to K_Γ if and only if the set of points of maximum for the restriction of the linear function (ξ, x) on the polytope Δ coincides with the face Γ. The cones K_Γ corresponding to different faces Γ are disjoint, and their union determines a decomposition $\Delta^\perp$ of the dual space $(\mathbb{R}^n)^*$. Two polytopes Δ_1 and Δ_2 are said to be analogous if the corresponding dual decompositions coincide. A polytope Δ_2 is said to be subordinated to a polytope Δ_1 if the decomposition $\Delta_1^\perp$ is finer than the decomposition $\Delta_2^\perp$ (i.e., if each cone K_{Γ_1} of the first decomposition is contained in some cone K_{Γ_2} of the other decomposition). The support function $f_\Delta \colon (\mathbb{R}^n)^* \to \mathbb{R}$ of the polytope Δ defined by the relation $f_\Delta(\xi) = \max_{x\in\Delta}(\xi, x)$ possesses the following properties:

(1) f_Δ is continuous and positive linearly homogeneous ($f_\Delta(\lambda\xi) = \lambda f_\Delta(\xi)$ for $\lambda \geq 0$);

(2) f_Δ is linear on each cone K_Γ of the dual decomposition;

(3) f_Δ is convex, i.e., $f(\xi_1 + \xi_2) \leq f_\Delta(\xi_1) + f_\Delta(\xi_2)$.

The set $L_{\Delta^\perp}$ of functions with properties (1) and (2) with respect to the decomposition $\Delta^\perp$ forms a linear space. The subset $L^+_{\Delta^\perp}$ of convex functions in $L_{\Delta^\perp}$ is a convex cone. A function g belongs to the cone $L^+_{\Delta^\perp}$ if and only if it is the support function of a convex polytope subordinated to the polytope Δ.

A polytope $\Delta \subset \mathbb{R}^n$ will be called a polytope with rational normals if all cones K_Γ of the dual decomposition $\Delta^\perp$ are rational. (Note that the vertices of a polytope Δ with rational normals are not necessarily rational.) In the space of functions $L_{\Delta^\perp}$ there is a lattice $\Lambda_{\Delta^\perp}$ determined by the following condition: a piecewise linear function $f \in L_{\Delta^\perp}$ belongs to the lattice $\Lambda_{\Delta^\perp}$ if and only if for each cone $K_\Gamma \subset \Delta^\perp$ there exists an integral vector $x \in \mathbb{Z}^n \subset \mathbb{R}^n$ such that $f(\xi) = (\xi, x)$ for $\xi \in K_\Gamma$.

Let $f_1, \dots, f_r$ be the generators of the lattice $\Lambda_{\Delta^\perp}$.

Theorem 9. *There exists a polynomial Q of degree $\leq n$ in r integral variables $k_1, \dots, k_r$ such that if the function $f_\Delta = k_1 f_1 + \dots + k_r f_r$ is the support function of a convex polytope Δ_k, then the number of integral points in this polytope is equal to $Q(k)$.*

Proof. This theorem readily follows from results in [5]. Indeed, denote by $P(\mathbb{Z}^n)$ the space of linear combinations of the characteristic functions of convex integral polytopes. Define a functional μ on $P(\mathbb{Z}^n)$ by the following formula:

$$\mu(\varphi) = \sum_{x\in\mathbb{Z}^n} \varphi * \chi_\Delta(x),$$

where $\varphi \in P(\mathbb{Z}^n)$, χ_Δ is the characteristic function of the polytope Δ and $*$ is the convolution with respect to the integral over the Euler characteristic. The functional μ is invariant with respect to the shifts by integral vectors, i.e., $\mu(\varphi(\,\cdot\,)) = \mu(\varphi(a + \,\cdot\,))$ for $a \in \mathbb{Z}^n$. The value of the functional μ on a virtual polytope with support function $k_1 f_1 + \dots + k_r f_r$ is a polynomial in $k = (k_1, \dots, k_r)$ (see [5, §7, Corollary 4]). Denote this polynomial as $Q(k)$. Let the function $f_\Delta = k_1 f_1 + \dots + k_r f_r$ be the support function of the polytope Δ_k, $f_\Delta \in L^+_{\Delta^\perp}$. In this case the value of the functional μ on the characteristic function of the polytope Δ_k is equal to the number of integral points in this polytope. The theorem is proved.

Let $A \colon \mathbb{R}^n \to \mathbb{R}^m$ be a linear mapping with the following nonnegativity property: $A^{-1}(0) \cap \mathbb{R}^n_+ = 0$. We are interested in the bounded convex polytope $\Delta(x) = A^{-1}(x) \cap \mathbb{R}^n_+$ as a function of the parameter $x \in \mathbb{R}^m$.

Let $e_1, \dots, e_n$ be the standard basis in $\mathbb{R}^n$ and let $a_i \in \mathbb{R}^m$ be the images of the vectors e_i, $a_i = A(e_i)$, $i = 1, \dots, n$. A subset J of the segment $J \subset \{1, \dots, n\}$ of positive integers is said to be essential if the vectors $a_i = A(e_i)$, $i \in J$, are linearly independent. For each essential subset J denote by K_J the relative interior of the cone spanned by these vectors, i.e., $x \in K_J$ if $x = \sum_{i \in J} \lambda_i a_i$, $\lambda_i > 0$. With the mapping $A\colon \mathbb{R}^n \to \mathbb{R}^m$ we associate the following stratification $S(A)$ of the space $\mathbb{R}^m$: two points x and y are said to belong to the same stratum if and only if for each set K_J we have either $x \in K_J$ and $y \in K_J$ or $x \notin K_J$ and $y \notin K_J$. It is easy to show that the following assertion holds.

Proposition. (1) *If a point x belongs to the set K_J, then the polytope $\Delta(x)$ has the vertex $O_J = A^{-1}(x) \cap \mathbb{R}_J$, where $\mathbb{R}_J$ is the coordinate subspace generated by the vectors e_i, $i \in J$. Conversely, each vertex of the polytope $\Delta(x)$ coincides with the point O_J for some set K_J containing x.*

(2) *If two points x and y belong to the same stratum, then the polytopes $\Delta(x)$ and $\Delta(y)$ are analogous.*

(3) *If a point y belongs to the closure of a stratum containing a point x, then the polytope $\Delta(y)$ is subordinated to the polytope $\Delta(x)$.*

Below we assume that the matrix of the mapping A is integral, i.e., $A(e_i) = a_i$, $a_i \in \mathbb{Z}^m$. For the set of independent integral vectors $\{a_i\,; i \in J\}$, we denote by $q(J)$ the greatest common divisor of the maximal minors of the matrix composed of these vectors.

Corollary. *Let a point x belong to the set K_J. Then the vertex O_J of $\Delta(x)$ corresponding to this set belongs to the lattice $\frac{1}{q(J)}\mathbb{Z}^n$.*

Indeed, the corresponding vertex O_J has the form $A^{-1}(x) \cap \mathbb{R}_J$. Let q_m be a nonzero minor of maximum rank composed of the vectors a_i, $i \in J$. Applying this minor for solving the system of linear equations, we see that the point O_J belongs to the lattice $\frac{1}{q_m}\mathbb{Z}^n$. We have a similar relation for any other minor q_j. Combining all these relations we obtain $O_J \in \frac{1}{q(J)}\mathbb{Z}^n$.

Definition. For an integral nonnegative matrix A the number $k(A)$ is the least common multiple of the numbers $q(J)$ for all subsets J of the set of columns of the matrix A.

Definition. Let a semialgebraic stratification of the space $\mathbb{R}^m$ and a positive integer k be given. A function $f\colon \mathbb{Z}^m_+ \to \mathbb{R}$ is said to be *piecewise polynomial with respect to the given stratification with coefficients periodic modulo* k if the following condition holds: for each stratum X of the stratification and for each equivalence class $a \in \mathbb{Z}^m/k\cdot\mathbb{Z}^m$ there exists a polynomial $P_{X,a}$ such that if an integral point $x \in \mathbb{Z}^m_+$ belongs to the closure of the stratum X, $x \in \overline{X}$, and under their factorization $\pi\colon \mathbb{Z}^m \to \mathbb{Z}^m/k\cdot\mathbb{Z}^m$ this point goes into the point a, i.e., $\pi(x) = a$, then $f(x) = P_{X,a}(x)$.

Let $A\colon \mathbb{R}^n \to \mathbb{R}^m$ be a linear mapping with an integral matrix and let $A^{-1}(0) \cap \mathbb{R}^n_+ = 0$. Let $f_A\colon \mathbb{Z}^m_+ \to \mathbb{Z}_+$ be the function that associates the number of integral points in the polytope $\Delta(x) = A^{-1}(x) \cap \mathbb{R}^n_+$ with each integral point $x \in \mathbb{Z}^m_+$.

Theorem 10. *The function f_A is piecewise polynomial with respect to the stratification S_A with coefficients periodic modulo $k(A)$. The degrees of the corresponding polynomials $P_{x,a}$ do not exceed the dimension of the kernel of the matrix A.*

Proof. Let us choose a stratum X of the stratification S_A. If a point y belongs to the closure of the stratum X and a point x belongs to the stratum X, then the polytope $\Delta(y)$ is subordinated to the polytope $\Delta(x)$. If, in addition, the point y is equivalent to the point x modulo $k(A)$, i.e., $y = x + k_1 k(A) p_1 + \cdots + k_m k(A) p_m$, where p_i are the generators of the semigroup $\mathbb{Z}^m_+$ and $k_i \in \mathbb{Z}$ are integers, then the vertices of the polytope $\Delta(y)$ differ from the corresponding vertices of the polytope $\Delta(x)$ by integral vectors. Therefore, by Theorem 9, the number of points in the polytope $\Delta(y)$ is a polynomial in $k_1, \dots, k_m$.

§10. Hilbert Function and Integral Points in Rational Polytopes

In this section we deal with finitely generated A-graded $K[x_1, \dots, x_n]$-comodules, where A is a homomorphism of the semigroup $\mathbb{Z}^n_+$ into the semigroup $\mathbb{Z}^m_+$. Below we always assume that $A^{-1}(0) = 0$. This condition guarantees that each homogeneous component of the module is finite-dimensional. The homomorphism $A\colon \mathbb{Z}_+^n \to \mathbb{Z}_+^m$ can be extended to a linear mapping of $\mathbb{R}^n$ into $\mathbb{R}^m$, which will be denoted by the same letter A.

For each segment I of the natural scale denote by $\mathbb{R}_+(I)$ the set of points $(x_1, \dots, x_n)$, $x_i = 0$ for $i \in I$ and $x_i \geq 0$ for $i \notin I$. Denote by $T_{A,I}$ the function that associates the number of integral points in the polytope $\Delta_{I,x} = A^{-1}(x) \cap \mathbb{R}_+(I)$ with each point $x \in \mathbb{Z}_+^m$. The functions f_I introduced in §8 have a simple geometric meaning for A-graded modules: $f_I = T_{A,I}$.

Theorem 8 has the following version for A-graded modules.

Theorem 11. *A function $H: \mathbb{Z}_+^m \to \mathbb{Z}_+$ is the Hilbert function of a finitely generated A-graded module over the ring $K[x_1, \dots, x_n]$ if and only if it is representable in the form of the following finite sum:*

$$H(x) = \sum a_{I,b} T_{A,I}(x - b), \qquad b \in \mathbb{Z}_+^m \text{ and } I \subset \{1, \dots, n\},$$

whose coefficients are nonnegative integers.

We will need a generalization of the stratification $S(A)$ of the space $\mathbb{R}^m$ described in §9.

For each subset $J \subset \{1, \dots, n\}$ and each point $b \in \mathbb{Z}_+^m$ denote by $K_{J,b}$ the set of points representable in the form $x = b + \sum \lambda_i A(e_i)$, where $\lambda_i > 0$ for $i \in J$ and $\lambda_i = 0$ for $i \notin J$.

Consider the following construction.

(1) Let us choose a finite number of sets $K_{J,b}$.

(2) With the help of the sets in (1) we define the stratification as follows: two vectors x and y belong to the same stratum if and only if they belong to the same sets in (1).

Definition. The above stratifications are called *stratifications compatible with the mapping A*.

Combining the theorems from in §§8 and 9 we obtain the following result.

Theorem 12 (cf. [6]). *The Hilbert function of a finitely generated A-graded module over $K[x_1, \dots, x_n]$ is piecewise polynomial with respect to some stratification of the space $\mathbb{R}_+^m$ compatible with the mapping A, with coefficients periodic modulo $k(A)$. The degrees of the corresponding polynomials $P_{X,a}$ do not exceed the dimension of the kernel of the matrix A.*

References

1. A. G. Khovanskii, "The Newton polytope, the Hilbert polynomial, and sums of finite sets," Funkts. Anal. Prilozhen., **26**, No. 4, 57–63 (1992).
2. D. Cox, J. Little, and D. O'Shea, Ideals, Varieties, and Algorithms, Springer-Verlag (1991).
3. M. Brion, "Points entiers dans les polyedres convexes," Ann. Sci. Ecole Norm. Sup., **21**, No. 4, 653–663 (1988).
4. A. V. Pukhlikov and A. G. Khovanskii, "The Riemann–Roch theorem for integrals and sums of quasipolynomials on virtual polytopes," Algebra Analiz, **4**, No. 4, 188–216 (1992).
5. A. V. Pukhlikov and A. G. Khovanskii, "Finitely additive measures of virtual polyhedra," Algebra Analiz, 4, No. 2, 161–185 (1992).
6. M. Brion and C. Procesi, "Action d'un tore dans une variete projective," in: Operator Algebras, Unitary Representations, Enveloping Algebras, and Invariant Theory, Birkhauser (1990), pp. 509–539.
7. I. V. Arnold, "Ideale in kommutativen Halbgruppen," Math. Ann., 401–407 (1929).

Translated by A. I. Shtern