СУММЫ КОНЕЧНЫХ МНОЖЕСТВ, ОРБИТЫ КОММУТАТИВНЫХ ПОЛУГРУПП И ФУНКЦИИ ГИЛЬБЕРТА

А. Г. Хованский

1. Введение

Подмножества в полугруппе можно складывать: суммой $A + B$ двух подмножеств A и B в коммутативной полугруппе называется множество точек z, представленных в виде $z = a + b$, где $a \in A$ и $b \in B$. Обозначим через $N * A$ сумму N экземпляров множества A.

В [1] доказана следующая

Теорема. *Для любых конечных подмножеств A и B в коммутативной полугруппе G число точек в множестве $B + N * A$ при достаточно больших натуральных N является полиномом по N. Степень этого полинома меньше, чем число точек в множестве A.*

Этот полином является функцией Гильберта некоторого конечнопорожденного градуированного модуля над кольцом полиномов от нескольких переменных [1], что и доказывает теорему .

Это алгебраическое рассуждение вызывает два естественных вопроса:

1) Какое отношение может иметь кольцо полиномов от нескольких переменных к подсчету числа точек в множестве?
2) Нельзя ли избежать использования теоремы Гильберта для доказательства приведенного комбинаторного факта?

Настоящая статья дает ответ на эти вопросы. Начнем со второго вопроса. Без теоремы Гильберта здесь можно обойтись. Комбинаторные рассуждения позволяют доказать большее. Фиксируем произвольный мультипликативный характер $\chi\colon G \to \mathbb{C}$, $\chi(a + b) = \chi(a) \cdot \chi(b)$.

Обозначим через $f(N)$ сумму значений характера χ по всем точкам множества $B + N * A$.

Теорема 5. *При достаточно больших N функция $f(N)$ является квазиполиномом по N, $f(N) = \sum q_i^N P_i(N)$. Числа q_i в этой формуле являются значениями характера χ на множестве A, а функции P_i — полиномами степени меньшей, чем число точек множества A, в которых значения характера равно q_i.*

При $\chi \equiv 1$ функция f считает число точек в множестве $B + A * N$, и теорема 5 совпадает с приведенным выше комбинаторным фактом. Вообще говоря, функция f не является функцией Гильберта никакого градуированного модуля (значения $f(N)$ этой функции — комплексные числа, которые не обязательно являются целыми), и теорема 5 не может вытекать из теоремы Гильберта.

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX

Теорема 5 является проявлением общих свойств орбит полугруппы $\mathbb{Z}^n_+$, описанных в настоящей статье. Под действием группы множество распадается на орбиты, причем каждая орбита имеет простое описание в групповых терминах. В случае полугруппы орбита не имеет столь простого описания. К тому же орбиты различных точек могут пересекаться. Как в этом случае разрезать X на простые непересекающиеся куски? В п. 2 мы предлагаем частичный ответ на этот вопрос для вполне упорядоченных полугрупп.

Для полугруппы $\mathbb{Z}^n_+$ этот ответ можно уточнить (см. п. 4). Дело в том, что *полугруппа* $\mathbb{Z}^n_+$ *обладает свойством нетеровости* (см. [2]). Этот классический результат играет центральную роль в настоящей статье. Мы приводим его в п. 3 вместе с нужным нам добавлением: *Дополнение до* $\mathbb{Z}^n_+$*-идеала представимо в виде объединения конечного числа непересекающихся сдвинутых координатных полугрупп.*

Орбиты действия полугруппы $\mathbb{Z}^n_+$ устроены достаточно регулярно: они *разбиваются в непересекающиеся объединения конечного числа орбит координатных подполугрупп* (см. п. 4). Теорема 5, приведенная выше — одно из проявлений этой регулярности. В доказатель стве теоремы 5 мы используем также *свойства суммы значений экспоненциальной функции по всем целым точкам стандартного симплекса.* Эти свойства приведены в п. 5.

Вернемся к первому из наших вопросов: какое отношение имеет кольцо полиномов от нескольких переменных к подсчету числа точек в множестве? Подсчет числа точек в множестве $B + N * A$ опирается на свойства полугруппы $\mathbb{Z}^n_+$. А кольцо полиномов от n переменных над полем K является ни чем иным, как полугрупповой алгеброй для $\mathbb{Z}^n_+$ над полем K. (Сопоставление идеалов коммутативных полугрупп и коммутативных колец встречалось уже в [7]. Замечатель ная конструкция базисов Гребнера показывает, что нетеровость полугруппы $\mathbb{Z}^n_+$ влечет за собой нетеровость кольца полиномов.)

Модуль над кольцом полиномов от n переменных является непосредственным обобщением действия полугруппы $\mathbb{Z}^n_+$ на множестве. Теорема о существовании *специаль ного линейного базиса* в модуле над кольцом полиномов от n переменных (см. п. 8) является непосредственным обобщением теоремы о разрезании орбит полугруппы $\mathbb{Z}^n_+$ на орбиты координатных полугрупп. Теорема о структуре орбит вполне упорядоченной полугруппы G (см. п. 2) является следствием теоремы о существовании специального линейного базиса в модуле над полугрупповой алгеброй для G (см. п. 7). Специальный линейный базис в модуле над кольцом полиномов *позволяет охарактеризовать функции Гильберта градуированных модулей.* Фиксируем гомоморфизм $\gamma\colon \mathbb{Z}^n_+ \to \Gamma$, где Γ — некоторая коммутативная полугруппа. Модуль M над кольцом полиномов $K[x_1, \dots, x_n]$ называется γ-градуированным, если линейное пространство M представимо в виде прямой суммы линейных подпространств $M = \sum_{\theta\in\Gamma} M_\theta$, занумерованных элементами полугруппы Γ, и выполнено следующее условие однородности: моном x^a, $a \in \mathbb{Z}^n_+$, отображает однородное пространство M_θ в однородное пространство $M_{\theta+\gamma(a)}$. Функция на полугруппе Γ, сопоставляющая элементу θ размерность однородной компоненты M_θ, называется функцией Гильберта γ-градуированного модуля M. В п. 8 дается *пол-*

ное описание функции Гильберта конечнопорожденных γ-градуированных модулей в терминах гомоморфизма γ. Для классических γ-градуировок (которые встречаются у однородных кординатных колец алгебраических подмногообразий в произведении проективных пространств) это описание легко переводится на аналитический язык и влечет за собой полиномиальность функций Гильберта при больших значениях аргументов.

Для случая общей градуировки $\gamma\colon \mathbb{Z}_+^n \to \mathbb{Z}_+^m$ аналитический характер функции Гильберта оказывается более сложным: *существует конечная стратификация полугруппы $\mathbb{Z}_+^m$ такая, что ограничение функции Гильберта на каждый страт является полиномом с периодическими коэффициентами* (см. п. 10). Отметим, что аналогичное описание функции Гильберта (и их асимптотик) для таких градуировок другим способом получено в статье [6]. Наше описание основано на свойствах чисел целых точек в выпуклых многогранниках с рациональными вершинами, приведенных в п. 9.

Настоящая работа является непосредственным продолжением работы [1]. Ее результаты докладывались в 1991 году на семинарах Арнольда и Гельфанда в Москве и в 1992 году на семинаре Каждана в Гарварде.

2. Действие упорядоченных полугрупп на множествах

В этом пункте мы покажем, как разрезать множество X, на котором действует вполне упорядоченная полугруппа G, на достаточно простые непересекающиеся куски.

Действием полугруппы G на множестве X называется гомоморфизм $\pi\colon G \to S(X)$, где $S(X)$ — полугруппа отображений X в себя. Полугруппу G будем называть вполне упорядоченной, если в ней введен полный порядок (т. е. в каждом подмножестве есть наименьший элемент), выдерживающий левое умножение, т. е. если $g_1 > g_2$, то $gg_1 > gg_2$.

Подмножество $\mathcal{I} \subset G$ назовем *G-идеалом*, если оно инвариантно относительно левого умножения, т. е. если $h \in \mathcal{I}$ и $g \in G$, то $gh \in \mathcal{I}$.

Множество $J \subset G$ назовем *G-коидеалом*, если его дополнение $G \setminus J$ является G-идеалом.

Пусть множество $U \subset X$ инвариантно относительно действия полугруппы G. Задача, которую мы будем сейчас рассматривать, заключается в разрезании множества $X \setminus U$ на возможно более простые части.

Пример. Пусть $\aleph$ — некоторое множество индексов, X — объединение непересекающихся экземпляров G_α полугруппы G, $X = \bigcup_{\alpha\in\aleph} G_\alpha$, U — объединение некоторых G-идеалов $\mathcal{I}_\alpha \subset G_\alpha$, $U = \bigcup_{\alpha\in\aleph} \mathcal{I}_\alpha$. Множество $X \setminus U$ распадается в объединение непересекающихся G-коидеалов $J_\alpha = G_\alpha \setminus \mathcal{I}_\alpha$ относительно умножения слева на элементы полугруппы G.

Покажем, что аналогичное разрезание множества $X \setminus U$ на G-коидеалы существует для любого действия вполне упорядоченной полугруппы G. Пусть множество $X \setminus U$ содержится в объединение орбит O_α некоторых элементов $x_\alpha \in X,\ \alpha \in \aleph$.

Теорема 1. *Множество $X \setminus U$ представимо в виде объединения непересекающихся множеств X_α, $\bigcup X_\alpha = X \setminus U$, $X_\alpha \bigcap X_\beta = \emptyset$ при $\alpha \neq \beta$, обладающих следующим свойством: для любого индекса α множество $X_\alpha \subseteq O_\alpha$ и су-*

ществует G-коидеал J_α такой, что отображение $g \to \pi(g)(x_\alpha)$ осуществляет взаимно однозначное соответствие между J_α и множеством X_α.

Доказательство. Фиксируем полное упорядочивание индексов $\alpha \in \aleph$ элементов x_α. Для каждого индекса α определим инвариантное множество U_α как объединение множества U с орбитами O_β всех элементов x_β, имеющих меньшие индексы $\beta < \alpha$, $U_\alpha = (\bigcup_{\beta<\alpha} O_\beta) \bigcup U$. Определим множество X_α как множество точек орбиты O_α, не попавших в инвариантное множество U_α, $X_\alpha = O_\alpha \setminus U_\alpha$. Ясно, что $\bigcup X_\alpha = X \setminus U$ и $X_\alpha \bigcap X_\beta = \emptyset$ при $\alpha \neq \beta$.

Для каждой точки x, лежащей в X_α, рассмотрим подмножество $G(x) \subset G$, обладающее следующим свойством: $g \in G(x)$, если и только если $\pi(g)(x_\alpha) = x$. Пусть $g(x)$ — минимальный элемент в множестве $G(x)$. (Такой элемент существует, так как полугруппа G вполне упорядочена). Определим J_α как множество элементов $g(x)$ для всех точек $x \in X_\alpha$. По определению естественное отображение $g \to \pi(g)(x_\alpha)$ осуществляет взаимно однозначное отображение множеств J_α и X_α. Покажем, что дополнение $\mathcal{I}_\alpha = G \setminus J_\alpha$ является G-идеалом. Дополнение $\mathcal{I}_\alpha$ представимо в виде объединения следующих двух множеств $\mathcal{I}_\alpha^1$ и $\mathcal{I}_\alpha^2$: $g \in \mathcal{I}_\alpha^1$, если и только если точка $\pi(g)(x_\alpha)$ лежит в инвариантном множестве U_α; $g \in \mathcal{I}_\alpha^2$ если и только если существует элемент $a \in G$ такой, что $a < g$ и $\pi(a)(x_\alpha) = \pi(g)(x_\alpha)$. Покажем, что $\mathcal{I}_\alpha^2$ — G-идеал. Пусть $c \in G$ — любой элемент полугруппы, $g \in \mathcal{I}_\alpha^2$, $a < g$ и $\pi a)(x_\alpha) = \pi(g)(x_\alpha)$. Тогда $ca < cg$ и $\pi(ca)(x_\alpha) = \pi(cg)x_\alpha$. Поэтому $cg \in \mathcal{I}_\alpha^2$. Что и требовалось. Множество $\mathcal{I}_\alpha^1$, очевидно, является G-идеалом. Поэтому $\mathcal{I}_\alpha = \mathcal{I}_\alpha^1 \bigcup \mathcal{I}_\alpha^2$ тоже является G-идеалом. Теорема доказана.

3. Полугруппа $\mathbb{Z}_+^n$

Для полугруппы $\mathbb{Z}_+^n$ теорему 1 можно усилить. Дело в том, что полугруппа $\mathbb{Z}_+^n$ обладает некоторым свойством нетеровости (см. например, [2]). Это свойство было открыто до теоремы Гильберта о нетеровости кольца полиномов. Опишем этот классический результат в нужном нам виде.

Назовем октантом $O^n(a)$ с вершиной в точке $a \in \mathbb{Z}_+^n$, $a = a_1, \dots, a_n$, подмножество целых точек $b = b_1, \dots, b_n$ в $\mathbb{Z}_+^n$, удовлетворяющих неравенствам $b_1 \geq a_1, \dots, b_n \geq a_n$. Ясно, что октант является $\mathbb{Z}_+^n$-идеалом .

Теорема (Нетеровость полугруппы $\mathbb{Z}_+^n$). *Каждый $\mathbb{Z}_+^n$-идеал является объединением конечного числа октантов (другими словами, объединение бесконечного числа октантов на самом деле является объединением конечного числа октантов).*

Доказательво. Индукция по размерности n. Выделим последнюю координату x_n в $\mathbb{Z}_+^n$, т. е. положим $\mathbb{Z}_+^n = \mathbb{Z}_+^{n-1} + \mathbb{Z}_+$. Очевидно, что:

1) сечение октанта горизонтальной плоскостью $x_n = c$, $c \in \mathbb{Z}_+$, есть октант в полугруппе $\mathbb{Z}_+^{n-1}$ (после стирания последней координаты $x_n = c$);.

2) проекция октанта из $\mathbb{Z}_+^n$ есть октант в $\mathbb{Z}_+^{n-1}$.

Переходим к индукции. Спроектируем объединение бесконечного числа октантов $\mathcal{I} \subset \mathbb{Z}_+^n$ на координатную плоскость$\mathbb{Z}_+^{n-1}$. Полученное объединение $(n-1)$-мерных октантов по индукции совпадает с объединением лишь конечного числа из них. Пусть это будут октанты с вершинами $b^1, \dots, b^k$,

($b^i = b^i_1, \ldots, b^i_{n-1}$). По построению эти октанты — проекции n-мерных октантов с некоторыми вершинами $\tilde{b}^i$, ($\tilde{b}^i = b^i_1, \ldots, b^i_{n-1}, b^i_n$). Пусть максимальная из последних координат b^i_n этих вершин равна $c \in \mathbb{Z}^n_+$. Все точки $\mathbb{Z}^n_+$-идеала $\mathcal{I}$, для которых последняя координата не меньше чем c, лежат в объединении октантов $O^n(\tilde{b}^i)$. Остальные точки $\mathbb{Z}^n_+$-идеала $\mathcal{I}$ лежат на конечном числе сечений $x_n = 0, x_n = 1, \ldots, x_n = c - 1$. Каждое из этих сечений по индукционному предположению покрывается конечным числом $(n-1)$-мерных октантов. Теперь видно, что $\mathbb{Z}^n_+$-идеал $\mathcal{I}$ состоит из конечного числа октантов $O^n(\tilde{b}^i)$ и конечного числа n-мерных октантов, вершины которых лежат на конечном числе сечений.

Полугруппа $\mathbb{Z}^n_+$ имеет 2^n координатных полугрупп: для каждого подмножества I отрезка натурального ряда $\{1, \ldots, n\}$ определена подполугруппа $\mathbb{Z}_+(I)$, состоящая из целых точек $a = a_1, \ldots, a_n$, для которых $a_i = 0$ при $i \in I$, и $a_i \geq 0$ при $i \notin I$. Среди полугрупп $\mathbb{Z}_+(I)$ есть нулевая полугруппа (при $I = \{1, \ldots, n\}$) и полугруппа $\mathbb{Z}^n_+$ (при $I = \emptyset$).

Подмножество $\mathbb{Z}^n_+$ назовем сдвинутой координатной подгруппой, если оно имеет вид $a + \mathbb{Z}_+(I)$, где a — некоторый элемент в $\mathbb{Z}^n_+$.

Теорема 2. *Дополнение до $\mathbb{Z}^n_+$-идеала представимо в виде объединения конечного числа непересекающихся сдвинутых координатных полугрупп.*

Доказательство. 1) Предположим сначала, что $\mathbb{Z}^n_+$-идеал является октантом $O^n(a)$ с вершиной a. Представим дополнение $\mathbb{Z}^n_+ \setminus O^n(a)$ в виде объединения сдвинутых полугрупп. Для каждой ненулевой точки a в $\mathbb{Z}^n_+$ определим точку $\pi(a)$ по следующему правилу: если $a = (a_1, \ldots, a_n)$ и $a_1 = \cdots = a_{i-1} = 0$, $a_i > 0$, то $\pi(a) = (a_1, \ldots, a_{i-1}, a_i - 1, a_{i+1}, \ldots a_n)$. Очевидно, что октант с вершиной $\pi(a)$ содержит октант с вершиной a, причем их разность $O^n(\pi(a)) \setminus O^n(a)$ является сдвинутой координатной полугруппой. Для целой точки $a = a_1, \ldots, a_n$ справедливо равенство $\pi^l(a) = 0$, где $l = \|a\| = \sum |a_i|$. Получаем требуемое разложение:

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

.

2) Всякий $\mathbb{Z}^n_+$-идеал является объединением конечного числа октантов. Предположим, что теорема верна в том случае, когда $\mathbb{Z}^n_+$-идеал $\mathcal{I}$ равен объединению k октантов. Докажем теорему для $(k+1)$ октанта. Имеем $\mathcal{I} = \mathcal{I}_0 \bigcup O^n(a)$, где $\mathcal{I}_0$ — объединение k октантов. По индукции дополнение $\mathbb{Z}^n_+$ до $\mathcal{I}_0$ есть объединение сдвинутых координатных полугрупп. В каждой сдвинутой координатной полугруппе $\mathcal{L}$ дополнение до пересечения с октантом $\mathcal{L} \setminus (\mathcal{L} \bigcap O^n(a))$ в свою очередь разбивается в объединение сдвинутых координатных полугрупп (см. шаг 1 доказательства этой теоремы). Теорема доказана.

4. Действие полугруппы $\mathbb{Z}^n_+$ на множестве

Пусть на множестве X задано действие $\pi : \mathbb{Z}^n_+ \to S(X)$ полугруппы $\mathbb{Z}^n_+$ и $U \subset X$ — подмножество, инвариантное относительно этого действия. Пусть множество $X \setminus U$ содержится в объединении орбит некоторых элементов $\{x_\alpha\} \in X$.

Теорема 3. *Существует разбиение множества $X \setminus U$ в объединение непересекающихся множеств $X_{\alpha,i}$, $1 \le i \le l(\alpha)$, где l — некоторая целочисленная функция индекса α, обладающее следующим свойством: для каждой пары индексов (α, i) существует точка $a \in \mathbb{Z}_+^n$ и координатная полугруппа $\mathbb{Z}_+(I)$ такие, что отображение $g \to \pi(g+a)(x_\alpha)$ осуществляет взаимно однозначное соответствие между этой координатной полугруппой и множеством $X_{\alpha,i}$.*

Доказательство. В полугруппе $\mathbb{Z}_+^n$ существует полное упорядочивание (например, лексикографическое). Поэтому к действию полугруппы $\mathbb{Z}_+^n$ применима теорема 1. Для завершения доказательства нужно $\mathbb{Z}_+^n$-коидеалы J_α из этой теоремы разрезать на сдвинутые координатные полугруппы.

5. Сумма экспоненты по стандартному симплексу

Обозначим через $\Delta(m)$ стандартный симплекс в пространстве $\mathbb{R}^n$, определенный условиями $x_1 + \cdots + x_n = m$; $x_1 \ge 0, \ldots, x_n \ge 0$. Определим функцию $F(m,p)$, зависящую от натурального числа m и ковектора $p \in (\mathbb{R}^n)^*$, следующей формулой:

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

Обозначим через e_i базисные векторы пространства $\mathbb{R}^n$. Для каждого $i = 1, \ldots, n$ положим $\mu_i(p) = \prod 1/(1 - \exp(p(e_i - e_j)))$, где произведение берется по всем j таким, что $j \ne i$, $1 \le j \le n$. Функция $\mu_i(p)$ мероморфна на комплексификации пространства $(\mathbb{R}^n)^*$.

Утверждение. *Для всякого $m \ge 0$ и всякого ковектора p такого, что $p(e_i - e_j) \ne 0$ для любых $1 \le i < j \le n$, справедливо равенство*

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

Утверждение — частный случай общего результата ([3],[4]), в котором вместо стандартного симплекса $\Delta(m)$ фигурирует любой целочисленный многогранник. Утверждение полностью определяет функцию $F(m,p)$, если $p(e_i - e_j) \ne 0$ для любых $1 \le i < j \le n$.

Перейдем к общему случаю. Фиксируем ковектор $p = p_0$. Пусть в последовательности $(p_0 e_1), \ldots, (p_0 e_n)$ стречается ровно l различных чисел $q_1, \ldots, q_l$, причем число q_i встречается $k(i)$ раз.

Теорема 4. *Для всякого $m \ge 0$ справедливо равенство $F(p,m) = \sum q_i^m P_i(m)$, где $P_i(m)$ — некоторый полином от m степени $< k(i)$.*

Теорема 4 вытекает из утверждения для $p = p_0 + \lambda p_1$, где p_1 — достаточно общий ковектор и $\lambda \in \mathbb{R}$, при предельном переходе $\lambda \to 0$.

6. Сумма значений характера по множеству $B + N * A$

Подмножества в коммутативной полугруппе можно складывать: суммой $A+B$ двух подмножеств A и B в коммутативной полугруппе G называется множество точек z, представленных в виде $z = a + b$, $a \in A$ и $b \in B$. Фиксируем конечные подмножества A, $B \subset G$. Фиксируем произвольный характер χ полугруппы G, т. е. гомоморфизм $\chi\colon G \to \mathbb{C}$ полугруппы G в мультипликативную полугруппу комплексных чисел, $\chi(a+b) = \chi(a) \cdot \chi(b)$. Пусть $q_1, \dots, q_l \in \mathbb{C} \setminus 0$ — множество ненулевых значений характера χ на множестве A, и пусть $k(i)$ — число точек множества A, в которых характер χ равен q_i.

Обозначим через $N * A$ сумму N экземпляров множества A.

Теорема 5. *Сумма значений характера χ по всем точкам множества $B + N * A$ при достаточно больших натураль ных N равна $\sum_{i=1}^{l} q_i^N P_i(N)$, где P_i — полином от N степени $< k(i)$.*

Доказательство. 1) Занумеруем элементы множества $A = \{a_i\}$, $i = 1, \dots, n$. Рассмотрим полугруппу $\mathbb{Z}_+^n$ и ее гомоморфизм $\pi_1\colon \mathbb{Z}_+^n \to G$, переводящий стандартные образующие $e_1, \dots, e_n$ в элементы $a_1, \dots, a_n \in A$. Обозначим через $\pi_2\colon \mathbb{Z}_+^n \to \mathbb{Z}_+$ стандартный гомоморфизм, определенный равенством $\pi_2(x_1, \dots, x_n) = x_1 + \dots + x_n$.

Обозначим через $\overline{G}$ прямую сумму полугрупп G и $\mathbb{Z}_+$, $\overline{G} = G \oplus \mathbb{Z}_+$, и через $\pi\colon \mathbb{Z}_+^n \to \overline{G}$ — прямую сумму гоморфизмов π_1 и π_2. Обозначим через $\overline{B}$ и $\overline{A}$ следующие подмножества полугруппы $\overline{G}$: $\overline{B} = (B, 0)$, $\overline{A} = (A, 1)$. Полугруппа $\mathbb{Z}_+^n$ действует на $\overline{G}$ по следующему правилу: элемент $c \in \mathbb{Z}_+^n$ переводит точку $g \in \overline{G}$ в точку $g + \pi(c)$. Обозначим через X объединение орбит точек множества $\overline{B}$ относительно этого действия и через X_N — его подмножество, состоящее из точек, у которых вторая координата равна N. Ясно, что множество X_N совпадает с множеством $(B + N * A, N)$.

2) Доопределим характер $\chi\colon G \to \mathbb{C}$ до характера $\overline{\chi}\colon \overline{G} \to \mathbb{C}$ формулой $\overline{\chi}(g, m) = \overline{\chi}(g)$. Обозначим через U множество точек, в которых характер $\overline{\chi}$ равен нулю. Множество U инвариантно относительно действия полугруппы $\overline{G}$ и, следовательно, относительно действия $\mathbb{Z}_+^n$. Нас интересует сумма $\sum_{x \in B + N*A} \chi(x)$. Очевидно, что эта сумма равна $\sum_{x \in X_N \setminus U} \overline{\chi}(x)$.

3) К множеству $X \setminus U$ применима теорема 3. Согласно этой теореме множество $X \setminus U$ является непересекающимся объединением множеств $X_{b,i}$, где $b \in \overline{B}$, $1 \le i \le l(b)$ и $l\colon \overline{B} \to \mathbb{Z}$ — некоторая целочосленная функция на $\overline{B}$. При этом существуют $c \in \mathbb{Z}_+^n$ и координатная полугруппа $\mathbb{Z}_+(I)$, зависящие от индексов (b, i) такие, что отображение $q\colon \mathbb{Z}_+(I) \to X_{b,i}$, определенное формулой $q(x) = \pi(x + c)(b)$, является изоморфизмом.

Прообраз в $\mathbb{Z}_+(I)$ множества $X_{b,i,N} = X_{b,i} \bigcap (X_N \setminus U)$ является стандартным симплексом $\sum x_i = N - \pi_2(c)$, $x_i \ge 0$ при $i \notin I$ и $x_i = 0$ при $i \in I$. Согласно теореме 5 при $N \ge \pi_2(c)$ сумма характера χ по множеству $X_{b,i,N}$ равна $\sum q_j^{N - \pi_2(c)} \cdot P_{j,b,i}(N)$, где $\{q_j\}$ — значения характера χ на элементах подмножества A_I множества A, соответствующих координатной полугруппе $\mathbb{Z}_+(I)$, $P_{j,b,i}$ — полиномы степени меньшей, чем число точек в подмножестве A_I, для которых характер χ равен q_j. Итак, теорема доказана, если под достаточно большими N понимать числа $N \ge \max \pi_2(c)$, где максимум берется по конечному числу точек c.

7. Модули над полугрупповой алгеброй вполне упорядоченной полугруппы

Непосредственным обобщением понятия действия полугруппы на множестве является понятие модуля над полугрупповой алгеброй. В этом пункте мы опишем конструкцию Гребнера для полугрупповой алгебры вполне упорядоченной полугруппы и специальные линейные базисы в модулях над такими полугруппами. Мы также объясним, почему существование этих специальных линейных базисов доказывает теорему 1 о разрезании орбиты вполне упорядоченной полугруппы на простые куски.

С полугруппой G и полем K связана полугрупповая алгебра $K(G)$, состоящая из формальных линейных комбинаций элементов полугруппы G с коэффициентами из поля K. Умножение в G по линейности продолжается до умножения в $K(G)$.

Для упорядоченной полугруппы G существует замечательное отображение Гребнера Grb из $K(G)\setminus 0$ в G, сопоставляющее каждой ненулевой линейной комбинации $a=\sum\lambda(g)g$ наибольший элемент $g\in G$, входящий в a с ненулевым коэффициентом $\lambda(g)\neq 0$. Так как соотношение порядка в G выдерживает левое умножение, то для $g\in G$ и $a\in K(G)$ справедливо равенство $\mathrm{Grb}(g\cdot a)=g\cdot\mathrm{Grb}(a)$. Левому идеалу $\mathcal{I}$ в алгебре $K(G)$ сопоставляются следующие объекты:

1) его гребнеровский G-идеал, являющийся образом ненулевых элементов идеала $\mathcal{I}$ при отображении Гребнера,

2) его гребнеровский G-коидеал — дополнение в G до его гребнеровского идеала,

3) его гребнеровский коидеал в $K(G)$ — линейное подпространство в $K(G)$, порожденное элементами гребнеровского G-коидеала.

Хорошо известно следующее

Утверждение. *Алгебра $K(G)$ как линейное пространство является прямой суммой идеала $\mathcal{I}$ и его гребнеровского коидеала.*

Доказательство. По определению идеал $\mathcal{I}$ и его гребнеровский коидеал L пересекаются лишь по точке 0. Покажем, что каждый элемент $a\in K(G)$ принадлежит сумме $L+\mathcal{I}$. Для каждого элемента $a=\sum\lambda(g)g$, не лежащего в L, обозначим через $\mathrm{Grb}_L(a)$ наибольший из элементов $g\in \mathrm{Grb}(\mathcal{I}\setminus 0)$, входящих в a с ненулевым коэффициентом $\lambda(g)\neq 0$. Вычитая из a элемент $\lambda_1 b_1$ идеала $\mathcal{I}$, для которого $\mathrm{Grb}(\lambda_1 b_1)=\mathrm{Grb}_L(a)$, с подходящим коэффициентом λ_1, можно добиться либо чтобы $a-\lambda_1 b_1\in L$, либо чтобы $\mathrm{Grb}_L(a-\lambda_1 b_1)<\mathrm{Grb}_L(a)$. Если элемент $a_1=a-\lambda_1 b_1$ не лежит в L, то процесс можно повторить. Так как во вполне упорядоченном множестве убывающая цепочка обрывается, за конечное число шагов мы получим включение $a-\sum\lambda_i b_i\in L$, где $b_i\in\mathcal{I}$. Утверждение доказано.

Следствие 1. *Пусть $\mathcal{I}_1$ и $\mathcal{I}_2$ — такие идеалы алгебры $K(G)$, что $\mathcal{I}_1\subseteq\mathcal{I}_2$, и гребнеровские G-идеалы для $\mathcal{I}_1$ и $\mathcal{I}_2$ равны. Тогда $\mathcal{I}_1=\mathcal{I}_2$.*

Действительно, гребнеровские G-коидеалы для идеалов $\mathcal{I}_1$ и $\mathcal{I}_2$ равны. Поэтому $\mathcal{I}_1=\mathcal{I}_2$ согласно утверждению.

Следствие 2. *Элементы $\{g_\alpha\}\subset\mathcal{I}$ порождают идеал $\mathcal{I}$, если и только если их образы при отображении Гребнера порождают гребнеровский G-идеал для $\mathcal{I}$.*

Следствие 2 вытекает из следствия 1.

Рассмотрим $K(G)$ модуль M и его подмодуль M_1. Пусть множество векторов $B = \{m_\alpha\},\ \alpha \in \aleph,\ m_\alpha \in M$, порождает фактор модуль M/M_1.

Теорема 6. *Существует набор G-коидеалов $J_\alpha \subset G$ такой, что элементы $h(m_\alpha),\ \alpha \in \aleph,\ h \in J_\alpha,\ m_\alpha \in B$, являются базисом в линейном фактор пространстве M/M_1.*

Доказательство. Фиксируем любое полное упорядочивание множества индексов $\aleph$. Для каждого индекса $\alpha \in \aleph$ определим подмодули $M_\alpha^<$ и $M_\alpha^\leq$, порожденные подмодулем M_1 и всеми элементами $m_\beta \in B$, для которых, соответственно, $\beta < \alpha$ и $\beta \leq \alpha$. Рассмотрим идеал $\mathcal{I}_\alpha$, состоящий из таких элементов $a \in K(G)$, что для каждого вектора m из модуля $M_\alpha^\leq$ вектор $a(m)$ лежит в модуле $M_\alpha^<$. Согласно утверждению элеменеты $g(m_\alpha),\ g \in J_\alpha$, где J_α — гребнеровский G-коидеал идеала $\mathcal{I}_\alpha$, порождают фактор пространство $M_\alpha^</M_\alpha^\leq$. Откуда и вытекает теорема.

Покажем, что теорема 1 из п. 2 на самом деле является следствием теоремы 6. Действие полугруппы G на X по линейности продолжается до действия полугруппой алгебры $K(G)$ на K-линейном пространстве $C_0(X,K)$, где $C_0(X,K)$ — пространство 0-цепей в множестве X с коэффициентами в поле K.

Нульмерные цепи $C_0(U,K)$ в инвариантном подмножестве U образуют $K(G)$-подмодуль в модуле $C_0(X,K)$. Если множество $X \setminus U$ содержится в объединении орбит O_α элементов $x_\alpha \in X$, то фактормодуль $C_0(X,K)$ по $C_0(U,K)$ порождается векторами m_α, где m_α — 0-цепь, состоящая из точки x_α с кооэффициентом 1. Применяя к модулям $C_0(X,K) \supset C_0(U,K)$ и векторам $\{m_\alpha\}$ теорему 6 получим теорему 1.

8. Модули над кольцами полиномов и их функция Гильберта

Предыдущие комбинаторные рассмотрения дают информацию о модулях над кольцами полиномов. Каждой точке $a \in \mathbb{Z}_+^n,\ a = a_1, \dots, a_n$, соответствует моном $x^a = x_1^{a_1} \cdot \ldots \cdot x_n^{a_n}$. Полугрупповая алгебра $K(\mathbb{Z}_+^n)$ является кольцом $K[x_1, \dots, x_n]$ полиномов от n переменных над полем K. Из нетеровости полугруппы $\mathbb{Z}_+^n$ вытекает нетеровость кольца полиномов (см. п. 3 и следствие 2 п. 7).

Пусть M — конечнопорожденный модуль над кольцом полиномов от n переменных, M_1 — его подмодуль и $\{m_\alpha\}$ — элементы, задающие базис в фактормодуле M/M_1. Для каждого подмножества I в множестве переменных $x_1, \dots, x_n$ обозначим через Ξ_I множество мономов, не зависящих от переменных из подмножества I.

Теорема 7. *Для каждой пары индексов $(\alpha, i),\ 1 \leq i \leq l(\alpha)$, где l — некоторая целочисленная функция индекса α, можно указать точку $a \in \mathbb{Z}_+^n$ и подмножество I в множестве переменных $x_1, \dots, x_n$ такие, что множество всех векторов вида $x^a \cdot x^\mu(m_\alpha)$, где $x^\mu \in \Xi_I$, порождает базис в линейном фактор пространстве M/M_1.*

Доказательство. Так как полугруппу $\mathbb{Z}_+^n$ можно вполне упорядочить, то к модулям $M_1 \subset M$ над кольцом полиномов применима теорема 2. Для завершения доказательства нужно $\mathbb{Z}_+^n$-коидеалы J_α из этой теоремы разрезать на сдвинутые координатные полугруппы.

Отметим, что теорема 3 выводится из теоремы 7 точно так же, как теорема 1 выводится из теоремы 6 (см. п. 7).

Обозначим через $\tilde{N}$ множество натуральных чисел, к которому добавлено число 0 и символ $+\infty$. В $\tilde{N}$ естественным образом определена операция сложения не только конечного, но и бесконечного числа элементов. Размерность линейного пространства принимает значения в $\tilde{N}$. При этом размерность прямой суммы любого числа линейных пространств равна сумме их размерностей.

Фиксируем гомоморфизм $\gamma\colon \mathbb{Z}_+^n \to \Gamma$, где Γ — некоторая коммутативная полугруппа.

Определение. Модуль M над кольцом полиномов $K[x_1,\dots,x_n]$ называется *γ-градуированным*, если линейное пространство M представимо в виде прямой суммы линейных подпространств $M = \sum_{\theta\in\Gamma} M_\theta$, занумерованных элементами полугруппы Γ, и выполнено следующее условие однородности: моном x^a, $a \in \mathbb{Z}_+^n$, отображает однородное пространство M_θ в однородное пространство $M_{\theta+\gamma(a)}$. Функция $H\colon \Gamma \to \tilde{N}$, сопоставляющая элементу θ размерность однородной компоненты M_θ, называется функцией Гильберта γ-градуированного модуля M.

Какие функции $H\colon \Gamma \to \tilde{N}$ могут быть функциями Гильберта конечнопорожденных γ-градуированных модулей M? Ниже мы дадим полный ответ на этот вопрос. Но сначала несколько определений.

В пространстве функций на полугруппе Γ со значениями в $\tilde{N}$ определена операция свертки:

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

С гомоморфизмом $\gamma\colon \mathbb{Z}_+^n \to \Gamma$ связано 2^n функций на Γ, которые будут для нас играть главную роль. С каждым подмножеством $I \subset (1,\dots,n)$ связана координатная подгруппа $\mathbb{Z}_+(I) \subseteq \mathbb{Z}_+^n$ и функция $f_I\colon \Gamma \to \tilde{N}$, сопоставляющая элементу $\theta \in \Gamma$ число точек в множестве $\gamma^{-1}(\theta)\bigcap \mathbb{Z}_+(I)$.

Теорема 8. *Функция Гильберта $H\colon \Gamma \to \tilde{N}$ конечнопорожденного γ-градуированного $K[x_1,\dots,x_n]$-модуля представима в виде*

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

где g_I — неотрицательная целочисленная функция на Γ, равная нулю всюду, кроме конечного числа точек. Обратно, всякая функция H вида (1) *является функцией Гильберта некоторого γ-градуированного модуля.*

Доказательство. 1) Выберем в модуле M конечное число однородных образующих m_α. Согласно теореме 7 градуированное линейное пространство M является прямой суммой конечного числа градуированных подпространств $M(\alpha, i)$, порожденных векторами $x^\alpha \cdot x^\mu(m_\alpha)$, где $\mu \in \mathbb{Z}_+(I)$. Обозначим через b элемент полугруппы Γ, равный $\gamma(a) + g(m_\alpha)$, где $g(m_\alpha)$ — градуировка элемента m_α. Размерность однородной компоненты с градуировкой θ пространства $M(\alpha, i)$ равна $f_I * \delta_b(\theta)$, где δ_b — функция, равная 1 в точке b, и нулю в остальных точках. Отсюда и вытекает первое утверждение теоремы.

2) Для доказательства второго утверждения теоремы рассмотрим следующий пример γ-градуированного $K[x_1,\ldots,x_n]$-модуля. Полиномы P_I, не зависящие от переменных $x_i,\ i\in I$, естественно, являются $K[x_1,\ldots,x_n]$-модулем. Введем в этом модуле γ-градуировку по следующему правилу: градуировка монома $x^\mu,\ \mu\in\mathbb{Z}_+(I)$ равна $b+\gamma(\mu)$, где b — фиксированный элемент в полугруппе γ. Функция Гильберта H этого модуля равна $f_I*\delta_b$, поэтому всякая функция вида (1) является функцией Гильберта прямой суммы модулей описанного вида.

Следствие. *Если полугруппа Γ вкладывается в группу, то функция Гильберта каждого γ-градуированного модуля является линейной комбинацией с натуральными коэффициентами конечного числа функций $f_I(\theta-b)$.*

Пример 1. Самый простой и, безусловно, самый важный пример доставляют $K[x_1,\ldots,x_n]$-модули с обычной целочисленной градуировкой $\gamma:\mathbb{Z}^n\to\mathbb{Z}$, где $\gamma(a_1,\ldots,a_n)=a_1+\cdots+a_n$. Такая градуировка встречается у однородных координатных колец проективных многообразий. Функции $f_I(N)$ в этом случае имеют простой геометрический смысл — это число целых точек в симплексе $a_1+\cdots+a_n=N,\ a_i\ge 0,\ a_j=0$ при $j\in I$. Несложные вычисление показывает, что если число $p=n-|I|$ ненулевых переменных положительно, то $f_I(N)=C^{p-1}_{N+p-1}$. Если же $p=0$, то $f_I(0)=1$ и $f_I(N)=0$ при $N>0$. Поэтому число $f_I(N)$ — полином при $N>0$. Сдвинутые функции $f_I(N-b)$ — полиномы при $N>b$.

Отсюда вытекает замечательная

Теорема Гильберта. *Функция Гильберта H конечнопорожденного модуля с обычной градуировкой — полином, начиная с некоторого места.*

Приведем точное описание функции H. Определим функцию $\overline{C}^k_N$ двух целочисленных аргументов следующей формулой:

1) если $0\le k\le N$, то $\overline{C}^k_N=C^k_N$,
2) если $k=N=-1$, то функция $\overline{C}^k_N$ равна 1,
3) для всех остальных значений $k,\ N$ функция $\overline{C}^k_N$ равна нулю.

Теорема 8 показывает, что функцию Гильберта H конечнопорожденного $K[x_1,\ldots,x_n]$-модуля с градуировкой из примера 1 имеет следующий вид:

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

где $l,\ k$ и $a_{k,l}$ — неотрицательные целые числа, причем $k\le n$.

Пример 2. Чуть более сложный пример доставляет градуировка $\gamma\colon\mathbb{Z}^n_+\to\mathbb{Z}^m_+$, зависящая от параметров $i_1,\ldots,i_m$, связанных соотношением $i_1+\cdots+i_m=n$. Определим числа $c_0=0,\ c_1=i_1,\ c_2=i_1+i_2,\ \ldots,c_m=i_1+\cdots+i_m=n$ и положим $\gamma(a_1,\ldots,a_n)=N_1,\ldots,N_m$, где $N_l=\sum c_{l-1}<j\le c_l a_j$. Такая градуировка встречается у однородных координатных колец подмногообразий в произведении проективных пространств $\mathbb{C}P^{i_1-1}\times\cdots\times\mathbb{C}P^{i_m-1}$. Функция $f_I(N),\ N=N_1,\ldots,N_m$, имеет простой геометрический смысл — это число целых точек в произведении симплексов $\sum_{c_{l-1}<j\le c_l}a_j=N_l,\ a_j\ge 0,\ a_j=0$ при $j\in I$. Это число $f_I(N)$ равно $\overline{C}^{p_1-1}_{N_1+p_1-1}\cdot\ldots\cdot\overline{C}^{p_m-1}_{N_m+p_m-1}$, где p_l — число номеров $j,\ c_{l-1}<j\le c_l$ таких, что $j\notin I$.

Теорема 8 показывает, что функцию Гильберта H конечнопорожденного модуля $K[x_1,\dots,x_n]$-модуля с градуировкой из примера 2 имеет следующий вид:

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

где $k=k_1,\dots,k_m$; $l=l_1,\dots,l_m$; все числа k_j, l_j, $a_{k,l}$ — неотрицательные целые числа и $k_j\le i_j$. В частности, функция $H(N_1,\dots,N_m)$ является полиномом, если все координаты N_j достаточно велики.

9. Целые точки в рациональных многогранниках

С каждой гранью Γ выпуклого ограниченного многогранника $\Delta\subset\mathbb{R}^n$ связан выпуклый конус K_Γ в двойственном пространстве $(\mathbb{R}^n)^*$: ковектор ξ принадлежит K_Γ, если множество точек максимума ограничения линейной функции (ξ,x) на многограннике Δ совпадает с гранью Γ. Конуса K_Γ, соответствующие разным граням Γ, не пересекаются, и их объединение задает разбиение $\Delta^\perp$ двойственного пространства $(\mathbb{R}^n)^*$. Скажем, что многогранники Δ_1 и Δ_2 аналогичны, если соответствующие двойственные разбиения совпадают. Скажем, что многогранник Δ_2 подчинен многограннику Δ_1, если разбиение $\Delta_1^\perp$ более мелко, чем разбиение $\Delta_2^\perp$ (т. е. если каждый конус K_{Γ_1} первого разбиения содержится в некотором конусе K_{Γ_2} второго разбиения). Опорная функция $f_\Delta\colon(\mathbb{R}^n)^*\to\mathbb{R}$ многогранника Δ, определенная равенством $f_\Delta(\xi)=\max_{x\in\Delta}(\xi,x)$, обладает следующими свойствами:

1) f_Δ непрерывна и положительно линейно однородна ($f_\Delta(\lambda\xi)=\lambda f_\Delta(\xi)$, если $\lambda\ge 0$);
2) f_Δ линейна на каждом конусе K_Γ двойственного разбиения;
3) f_Δ выпукла, т. е. $f(\xi_1+\xi_2)\le f_\Delta(\xi_1)+f_\Delta(\xi_2)$.

Множество $L_{\Delta^\perp}$ функций, обладающих свойствами 1) и 2) относительно разбиения $\Delta^\perp$, образуют линейное пространство. Подмножество $L^+_{\Delta^\perp}$ выпуклых функций в $L_{\Delta^\perp}$ является выпуклым конусом. Функция g принадлежит конусу $L^+_{\Delta^\perp}$, если и только если она является опорной функцией выпуклого многогранника, подчиненного многограннику Δ.

Многогранник $\Delta\subset\mathbb{R}^n$ назовем многогранником с рациональными нормалями, если все конусы K_Γ двойственного разбиения $\Delta^\perp$ рациональны. (Отметим, что вершины многогранника Δ с рациональными нормалями не обязательно рациональные.) В пространстве функций $L_{\Delta^\perp}$ существует решетка $\Lambda_{\Delta^\perp}$, определенная следующим условием: кусочно-линейная функция $f\in L_{\Delta^\perp}$ лежит в решетке $\Lambda_{\Delta^\perp}$, если и только если для каждого конуса $K_\Gamma\subset\Delta^\perp$ существует целочисленный вектор $x\in\mathbb{Z}^n\subset\mathbb{R}^n$ такой, что $f(\xi)=(\xi,x)$ при $\xi\in K_\Gamma$.

Пусть $f_1,\dots,f_r$ — образующие решетки $\Lambda_{\Delta^\perp}$.

Теорема 9. *Существует многочлен Q степени $\le n$ от r целочисленных переменных $k=k_1,\dots,k_r$ такой , что если функция $f_\Delta+k_1f_1+\dots+k_rf_r$ является опорной функцией выпуклого многогранника $\Delta(k)$, то число целых точек в этом многограннике равно $Q(k)$.*

Доказательство. Эта теорема легко вытекает из результатов статьи [5]. Действительно, обозначим через $P(\mathbb{Z}^n)$ пространство линейных комбинаций характеристических функций выпуклых целочисленных многогранников. Определим функционал μ на пространстве $P(\mathbb{Z}^n)$ следующей формулой:

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

где $\varphi \in P(\mathbb{Z}^n)$, χ_Δ — характеристическая функция многогранника Δ, $*$ — свертка относительно интеграла по эйлеровой характеристике. Функционал μ инвариантен относительно сдвига на целочисленные вектора, т. е. $\mu(\varphi(\cdot)) = \mu(\varphi(a+\cdot))$, если $a \in \mathbb{Z}^n$. Значение функционала μ на виртуальном многограннике с опорной функцией $k_1f_1 + \cdots + k_rf_r$ полиномиально зависит от $k = k_1, \dots, k_r$ (см. следствие 4 п. 7 [5]). Обозначим этот полином через $Q(k)$. Пусть функция $F = f + k_1f_1 + \cdots + k_rf_r$ является опорной функцией многогранника $\Delta(k)$, $F \in L^+_{\Delta^\perp}$. В этом случае значение функционала μ на характеристической функции многогранника $\Delta(k)$ равняется числу целых точек в этом многограннике. Теорема доказана.

Пусть $A\colon \mathbb{R}^n \to \mathbb{R}^m$ — линейное отображение, обладающее следующим свойством неотрицательности: $A^{-1}(0)\bigcap\mathbb{R}^n_+ = 0$. Нас будет интересовать ограниченный выпуклый многогранник $\Delta(x) = A^{-1}(x)\bigcap\mathbb{R}^n_+$ как функция параметра $x \in \mathbb{R}^m$.

Пусть $e_1, \dots, e_n$ — стандартный базис в $\mathbb{R}^n$ и $a_i \in \mathbb{R}^m$ — образы векторов e_i, $a_i = A(e_i)$, $i = 1, \dots, n$. Подмножество J отрезка натурального ряда $J \subset \{1, \dots, n\}$ назовем существенным, если вектора $a_i = A(e_i)$, $i \in J$, линейно независимы. Для каждого существенного подмножества J обозначим через K_J относительную внутренность натянутого на них конуса, т. е. $x \in K_J$, если $x = \sum_{i\in J}\lambda_i a_i$, $\lambda_i > 0$. С отображением $A\colon \mathbb{R}^n \to \mathbb{R}^m$ свяжем следующую стратификацию $S(A)$ пространства $\mathbb{R}^m$: скажем, что две точки x и y лежат в одном страте, если и только если для каждого множества K_J либо $x \in K_J$ и $y \in K_J$, либо $x \notin K_J$ и $y \notin K_J$. Несложно проверить, что справедливо следующее

Утверждение.

1) *Если точка x лежит в множестве K_J, то многогранник $\Delta(x)$ имеет вершину $O_J = A^{-1}(x)\bigcap\mathbb{R}_J$, где $\mathbb{R}_J$ — координатное подпространство, порожденное векторами e_i, $i \in J$. Обратно, каждая вершина многогранника $\Delta(x)$ совпадает с точкой O_J для некоторого множества K_J, содержащего x.*
2) *Если точки x и y лежат в одном страте, то многогранник $\Delta(x)$ и $\Delta(y)$ аналогичны.*
3) *Если точка y лежит в замыкании страта, содержащего точку x, то многогранник $\Delta(y)$ подчинен многограннику $\Delta(x)$.*

Ниже мы будем предполагать, что матрица отображения A целочисленна, т. е. что $A(e_i) = a_i$, $a_i \in \mathbb{Z}^m$. Для множества независимых целочисленных векторов $\{a_i\}$, $i \in J$, обозначим через $q(J)$ наибольший общий делитель максимальных миноров матрицы, составленной из векторов.

Следствие. *Пусть точка x лежит в множестве K_J. Тогда соответствующая этому множеству вершина O_J многогранника $\Delta(x)$ принадлежит решетке $\frac{1}{q(J)}\mathbb{Z}^n$.*

Действительно, соответствующая вершина O_J имеет вид $A^{-1}(x)\bigcap\mathbb{R}_J$. Пусть q_m — один из ненулевых миноров максимального ранга, составленный из векторов $\{a_i\}$, $i\in J$. Используя этот минор для решения системы линейных уравнений, получим, что точка O_J лежит в решетке $\frac{1}{q_m}\mathbb{Z}^n$. Мы имеем аналогичное включение для любого другого минора q_j. Соединяя все эти включения, получим, что $O_J\in\frac{1}{q(J)}\mathbb{Z}^n$.

Определение. Для целочисленной неотрицатель ний матрицы A определим число $k(A)$ как наименьшее общее кратное чисел $q(J)$ для всех подмножеств J множества столбцов матрицы A.

Определение. Пусть задана полуалгебраическая стратификация пространства $\mathbb{R}^m$ и натуральное число k. Функцию $f\colon\mathbb{Z}^m_+\to\mathbb{R}$ назовем *кусочно-полиномиаль ной* относительно заданной стратификации с коэффициентами, периодическими по модулю k, если выполнено следующее условие: для каждого страта X стратификации и для каждого класса эквивалентности $a\in\mathbb{Z}^m/k\cdot\mathbb{Z}^m$ существует полином $P_{X,a}$ такой, что если целочисленная точка $x\in\mathbb{Z}^m_+$ лежит в замыкании страта X, $x\in\overline{X}$, и при их факторизации $\mathbb{Z}^m\to\mathbb{Z}^m/k\cdot\mathbb{Z}^m$ переходит в точку a, т. е. $\pi(x)=a$, то $f(x)=P_{X,a}(x)$.

Пусть $A\colon\mathbb{R}^n\to\mathbb{R}^m$ — линейное отображение с целочисленной матрицей и $A^{-1}(0)\bigcap\mathbb{R}^n_+=0$. Пусть $f_A\colon\mathbb{Z}^m_+\to\mathbb{Z}_+$ — функция, сопоставляющая каждой целой точке $x\in\mathbb{Z}^m_+$ число целых точек в многограннике $\Delta(x)=A^{-1}(x)\bigcap\mathbb{R}^n_+$.

Теорема 10. *Функция f_A кусочно-полиномиальна относительно стратификации S_A с коэффициентами, периодическими по модулю $k(A)$. Соответствующие полиномы $P_{x,a}$ имеют степени , не превосходящие размерности ядра матрицы A.*

Доказательство. Фиксируем страт X стратификации S_A. Если точка y принадлежит замыканию страта X, а точка x принадлежит страту X, то многогранник $\Delta(y)$ подчинен многограннику $\Delta(x)$. Если к тому же точка y эквивалентна точке x по модулю $k(A)$, т. е. $y=x+k_1k(A)p_1+\dots+k_mk(A)p_m$, где p_i — образующие $\mathbb{Z}^m_+$ и $k_i\in\mathbb{Z}$ — целые числа, то вершины многогранника $\Delta(y)$ отличаются от соответствующих вершин многогранника $\Delta(x)$ на целочисленные векторы. Поэтому согласно теореме 9 число точек в многограннике $\Delta(y)$ — полином от $k_1,\dots,k_m$.

10. Функция Гильберта и целые точки в рациональных многогранниках

В этом параграфе мы будем иметь дело с конечно порожденными A-градуированными $K[x_1,\dots,x_n]$-комодулями, где A — гомоморфизм полугруппы $\mathbb{Z}^n_+$ в полугруппу $\mathbb{Z}^m_+$. Мы будем ниже всегда предполагать, что $A^{-1}(0)=0$. Это условие обеспечивает конечномерность каждой однородной компоненты модуля. Гомоморфизм $A\colon\mathbb{Z}^n_+\to\mathbb{Z}^m_+$ продолжается до линейного отображения $\mathbb{R}^n$ в $\mathbb{R}^m$, которое мы будем обозначать той же буквой A.

Для каждого подмножества I натурального ряда обозначим через $\mathbb{R}_+(I)$ множество точек $(x_1,\dots,x_n)$, $x_i=0$ при $i\in I$, $x_j\geq 0$ при $j\notin I$. Обозначим через $T_{A,I}$ функцию, сопоставляющую каждой точке $x \in \mathbb{Z}_+^m$ число целых точек в многограннике $\Delta_{I,x} = A^{-1}(x) \bigcap \mathbb{R}_+(I)$. Функции f_I, введенные в п. 8, для A-градуированных модулей имеют простой геометрический смысл: $f_I = T_{A,I}$.

Для A-градуированных модулей теорема 8 допускает следующую переформулировку.

Теорема 11. *Функция $H\colon \mathbb{Z}_+^m \to \mathbb{Z}_+$ является функцией Гильберта некоторого конечнопорожденного A-градуированного модуля над кольцом $K[x_1, \dots, x_n]$, если и только если функция H представима в виде следующей конечной суммы:*

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

коэффициенты которой — неотрицательные целые числа.

Нам понадобится обобщение стратификации $S(A)$ пространства $\mathbb{R}^m$, описанной в п. 9.

Для каждого подмножества $J \subset \{1, \dots, n\}$ и каждой точки $b \in \mathbb{Z}_+^m$ обозначим через $K_{J,b}$ множество точек, представимых в виде $x = b + \sum \lambda_i A(e_i)$, где $\lambda_i > 0$, если $i \in J$ и $\lambda_i = 0$, если $i \notin J$.

Рассмотрим следующую конструкцию.

1) Фиксируем конечное число множеств $K_{J,b}$.
2) При помощи множеств пункта 1 определим стратификацию следующим способом: два вектора x и y принадлежат одному страту, если и только если они принадлежат одним и тем же множествам из пункта 1.

Определение. Стратификации, построенные выше, называются *стратификациями, согласованными с отображением A.*

Соединяя теоремы из п. 8 и п. 9, получаем следующий результат.

Теорема 12 (ср. [6]). *Функция Гильберта конечнопорожденного A-градуированного модуля $K[x_1, \dots, x_n]$ является кусочно-полиномиальной относительно некоторой стратификации пространства $\mathbb{R}_+^m$, согласованной с отображением A, с коэффициентами, периодическими по модулю $k(A)$. Соответствующие полиномы $P_{X,a}$ имеют степени, не превосходящие размерности ядра матрицы A.*

Список литературы

1. *Хованский А. Г.* Многогранник Ньютона, полином Гильберта и суммы конечных множеств // Функцион. анализ и его прил.– 1992.–Т. 26, вып. 4.–С. 57–63.
2. *Cox D., Little J., O'Shea D.* Ideals, varieties, and algorithms // Springer-Verlag.–1991.
3. *Brion M.* Points entiers dans les polyedres convexes // Ann. Sci. Ecole Norm. Sup.–1988.–V. 21, N 4.–P. 653–663.
4. *Пухликов А. В., Хованский А. Г.* Теорема Римана-Роха для интегралов и сумм квазиполиномов по виртуальным многогранникам // Алгебра и анализ.– 1992.–Т. 4, вып. 4.–С. 188–216.
5. *Пухликов А. В., Хованский А. Г.* Конечно-аддитивные меры виртуальных многогранников // Алгебра и анализ.– 1992.–Т. 4, вып. 2.–С. 161–185.

6. *Brion M., Procesi C.* Action d'un tore dans une variete projective // Operator Algebras, Unitary Representations, Enveloping Algebras, and Invariant Theory, Birkhauser.–1990.–P. 509–539.
7. *Arnold I. V.* Ideale in kommutativen Halbgruppen // Math. Ann.–1929.–P. 401–407.