Функциональный анализ и его приложения,
1992, т. 26, вып. 4, 57–63

УДК 513.34+513.60

МНОГОГРАННИК НЬЮТОНА, ПОЛИНОМ ГИЛЬБЕРТА И СУММЫ КОНЕЧНЫХ МНОЖЕСТВ

А. Г. Хованский

1. Формулировка результатов

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

Теорема 1. *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.*

Теорема 1 — частный случай теоремы 2, сформулированной в п. 2. Полиномы, встречающиеся в теоремах 1 и 2, являются полиномами Гильберта некоторых градуированных модулей над кольцом полиномов от нескольких переменных.

Если полугруппа G является абелевой группой без элементов конечного порядка, то можно вычислить степень и старший коэффициент полинома, встречающегося в теореме 1. Введем нужные обозначения. Обозначим через $G(A)$ подгруппу группы G, порожденную разностями элементов из множества A (группа $G(A)$ состоит из элементов вида $\sum n_i a_i$, где $a_i\in A$, $n_i\in\mathbb{Z}$ и $\sum n_i=0$). Так как группа G не имеет элементов конечного порядка, то группа $G(A)$ изоморфна группе $\mathbb{Z}^n$, где n — ранг группы $G(A)$. Множество $\bar{A}=A-a$, где a — некоторый элемент множества A, содержится в группе $G(A)$.

Определение. *Приведенным многогранником Ньютона множества $A\subset G$ называется выпуклая оболочка в пространстве $\mathbb{R}^n$, содержащем решетку $\mathbb{Z}^n$, образа множества $\bar{A}$ при изоморфизме групп $G(A)$ и $\mathbb{Z}^n$.*

Приведенный многогранник Ньютона определен с точностью до аффинного преобразования $x\to z\pm Ux$, где $z\in\mathbb{Z}^n$ и U — унимодулярное преобразование. В частности, объем приведенного многогранника Ньютона определен корректно. Обозначим через $i(A, B)$ число классов смежности группы G по подгруппе $G(A)$, содержащих точки множества B.

Теорема 4. *Пусть полугруппа G является абелевой группой без элементов конечного порядка. Тогда при $N\to\infty$ отношение числа точек множества $B+N*A$ к числу N^n, где n — ранг группы $G(A)$, стремится к произведению объема приведенного многогранника Ньютона множества A на число $i(A, B)$.*

Теорема 4 доказывается в п. 3, посвященном в основном группе $G=\mathbb{Z}^n$. Пусть $A\subset\mathbb{Z}^n$ — конечное множество, такое что группа $\mathbb{Z}^n(A)$ равна группе $\mathbb{Z}^n$, и Δ — выпуклая оболочка множества A в $\mathbb{R}^n$, $\mathbb{Z}^n\subset\mathbb{R}^n$. Согласно теореме 3 из п. 2 каждая целая точка многогранника $N\cdot\Delta$, лежащая достаточно далеко от его границы, принадлежит множеству $N*A$.

В п. 4 мы показываем, как, используя полином Гильберта и теорему 3, доказать теорему Кушниренко (теорема Кушниренко вычисляет число решений общей системы из n полиномиальных уравнений от n неизвестных, имеющих одинаковые многогранники Ньютона). Результаты этой статьи возникли из попыток найти наиболее простое доказательство этой теоремы.

В п. 5 вычисляются группы Гротендика полугруппы компактных подмножеств в $\mathbb{R}^n$ и полугруппы конечных подмножеств в $\mathbb{Z}^n$.

Результаты статьи докладывались на Международной топологической конференции 1988 г. в Баку, с тех пор перешли в область фольклора, но так и не были опубликованы. Здесь я восполняю этот пробел.

2. Полином Гильберта и число точек в сумме конечных множеств

Пусть $\bar{G}$ — некоторое множество, $\bar{B}$ — его конечное подмножество и $\bar{A}=\{\bar{a}_i\}$ — множество из m коммутирующих отображений $\bar{G}$ в себя, $\bar{a}_i\circ\bar{a}_j=\bar{a}_j\circ\bar{a}_i$, $1\leqslant i,\ j\leqslant m$. Обозначим через $\bar{B}(N)$ множество $\bigcup\limits_{1\leqslant i_j\leqslant m} \bar{a}_{i_1}\circ\ldots\circ\bar{a}_{i_M}(\bar{B})$.

Теорема 2. *При достаточно большом натуральном N число точек в множестве $\bar{B}(N)$ является полиномом от N. Степень этого полинома меньше числа m.*

Теорема 1, сформулированная в п. 1,— частный случай теоремы 2. Для вывода теоремы 1 из теоремы 2 достаточно рассмотреть множество $\bar{G}$, являющееся множеством точек полугруппы G, множество $\bar{B}$, равное множеству B, и множество отображений $\bar{A}$, состоящее из сдвигов $\bar{a}_i$ полугруппы G на элементы a_i множества A (т. е. $\bar{a}_i(g)=g+a_i$). В этом случае множество $\bar{B}(N)$ совпадает с множеством $B+N*A$, и теорема 1 сводится к теореме 2.

Докажем теорему 2. Рассмотрим счетное число попарно непересекающихся экземпляров G_i, $i=0, 1, \ldots$, множества $\bar{G}$ вместе с взаимно однозначными соответствиями π_i: $\bar{G}\to G_i$. Обозначим через X объединение множеств G_i, $X=\cup G_i$, и через L — пространство комплекснозначных линейных функций на X, отличных от нуля лишь в конечном числе точек. Пространство L порождено функциями δ_x, равными нулю всюду, кроме точки $x\in X$, и равными единице в точке x. В пространстве L есть градуировка: функция имеет градуировку k, если она отлична от нуля лишь на k-м экземпляре G_k множества $\bar{G}$. Пространство L можно превратить в градуированный модуль над кольцом $\mathbb{C}[x_1, \ldots, x_m]$ полиномов от m переменных: образующая x_i по определению переводит функции δ_x, где $x=\pi_j(g)$, $g\in\bar{G}$, $j=0, 1, \ldots$, в функции δ_y, где $y=\pi_{j+1}(\bar{a}_i(g))$. Это действие однозначно продолжается до действия кольца $\mathbb{C}[x_1, \ldots, x_m]$ на пространстве L. Рассмотрим подмодуль $L_{\bar{B}}$ в L, порожденный элементами δ_x, где $x=\pi_0(\bar{b})$, $\bar{b}\in\bar{B}$. Компоненты модуля $L_{\bar{B}}$ с градуировкой N являются линейной комбинацией функций δ_x, где $x=\pi_N(g)$, $g\in\bar{B}(N)$. Размерность этой компоненты равна числу точек в множестве $\bar{B}(N)$. Поэтому теорема 2 вытекает из теоремы Гильберта [1, с. 160, теорема 6.21].

3. Суммы конечных подмножеств в целочисленной решетке

Пусть A — конечное подмножество в $\mathbb{Z}^n$, $\mathbb{Z}^n\subset\mathbb{R}^n$ такое, что подгруппа, порожденная его элементами, совпадает с группой $\mathbb{Z}^n$.

Утверждение 1. *Существует константа C, обладающая следующим свойством: для всякой линейной комбинации $\sum\lambda_i a_i$ векторов $a_i\in A$ с вещественными коэффициентами λ_i, которая является целочисленным вектором, существует равная ей линейная комбинация $\sum n_i a_i$ с целыми коэффициентами n_i такая, что $\sum|n_i-\lambda_i|<C$.*

Доказательство. Для каждого вектора x из конечного множества X целочисленных векторов, представимых в виде $x=\sum\lambda_i a_i$, где $0\leqslant\lambda_i\leqslant 1$, фиксируем представление в виде $x=\sum n_i(x)a_i$, $n_i(x)\in\mathbb{Z}$. Такое представление существует, так как элементы $a_i\in A$ порождают группу $\mathbb{Z}^n$. Достаточно положить $C=m+q$, где m — число элементов множества A и $q=$
$$=\max_{x\in X}\sum_{i=1}^{m}|n_i(x)|.$$
Действительно, для всякого целочисленного вектора $z\in\mathbb{Z}^n$, равного $\sum\lambda_i a_i$, вектор $x=z-\sum[\lambda_i]a_i$ лежит в множестве X. Следовательно, $x=\sum n_i(x)a_i$ и $z=\sum n_i a_i$, где $n_i=[\lambda_i]+n_i(x)$. Утверждение 1 доказано.

Обозначим через Δ выпуклую оболочку множества A в пространстве $\mathbb{R}^n$, содержащем решетку $\mathbb{Z}^n$. Если множество A содержит точку 0 и N — натуральное число, то многогранник $N\cdot\Delta$ можно определить как множество линейных комбинаций $\sum\lambda_i a_i$ векторов $a_i\in A$ таких, что $\lambda_i\geqslant 0$ и $\sum\lambda_i\leqslant N$. Обозначим через $\Delta(N, C)$ многогранник, состоящий из линейных комбинаций $\sum\lambda_i a_i$, где $\lambda_i\geqslant C$, $\sum\lambda_i\leqslant N-C$.

Утверждение 2. *Пусть группа $\mathbb{Z}^n(A)$, порожденная разностями элементов из множества A, совпадает с группой $\mathbb{Z}^n$ и точка 0 принадлежит множеству A. Тогда каждая целочисленная точка из многогранника $\Delta(N, C)$, где C — константа, фигурирующая в утверждении 1, лежит в множестве $N*A$.*

Доказательство. Так как множество A содержит точку 0, то множество $N*A$ состоит из точек вида $\sum n_i a_i$, где $a_i\in A$, $n_i\geqslant 0$ и $\sum n_i\leqslant N$. Согласно утверждению 1 каждая целочисленная точка из многогранника $\Delta(N, C)$ допускает представление в таком виде.

Фиксируем произвольную евклидову метрику в пространстве $\mathbb{R}^n$. Пусть A — конечное подмножество в группе $\mathbb{Z}^n\subset\mathbb{R}^n$ и Δ — его выпуклая оболочка в $\mathbb{R}^n$.

Теорема 3. *Пусть группа $\mathbb{Z}^n(A)$ равна группе $\mathbb{Z}^n$. Тогда существует константа ρ, обладающая следующим свойством: при любом натуральном N каждая целая точка многогранника $N\cdot\Delta$, отстоящая от границы этого многогранника не менее чем на ρ, лежит в множестве $N*A$.*

Доказательство. Не ограничивая общности, можно считать, что множество A содержит точку 0 (в противном случае вместо множества A нужно рассмотреть сдвинутое множество $A-a$, где a — некоторый вектор из множества A). Занумеруем элементы a_i множества A, $i=1, \ldots, m$. Рассмотрим пространство $\mathbb{R}^n$, размерность которого равна числу элементов множества A, и отображение π: $\mathbb{R}^m\to\mathbb{R}^n$, переводящее i-й вектор стандартного базиса в $\mathbb{R}^m$ в вектор $a_i\in\mathbb{R}^n$. Обозначим через $K(N)$ и $K(N, C)$ симплексы в пространстве $\mathbb{R}^m$, определенные соответственно неравенствами $\lambda_i\geqslant 0$, $\sum_{i=1}^{m}\lambda_i\leqslant N$ и $\lambda_i\geqslant C$, $\sum_{i=1}^{m}\lambda_i\leqslant N-C$. Многогранники $N\cdot\Delta$ и $\Delta(N, C)$ являются образами симплексов $K(N)$ и $K(N, C)$ при отображении π. Каждая точка симплекса $K(N)$, удаленная от его границы на расстояние, не меньшее чем $C\sqrt{m}$, лежит в симплексе $K(N, C)$. Поэтому каждая точка многогранника $N\cdot\Delta$, удаленная от его границы на расстояние, не меньшее чем $\rho=C\sqrt{m}\|\pi\|$, где $\|\pi\|$ — норма оператора π, лежит в многограннике $\Delta(N, C)$. Для завершения доказательства теоремы 3 осталось согласиться на утверждение 2.

Ниже мы будем считать, что метрика в пространстве $\mathbb{R}^n$ нормирована следующим условием: объем параллелепипеда $\Pi(e_1, \ldots, e_n)$, натянутого на базис $e_1, \ldots, e_n$ в решетке $\mathbb{Z}^n$ $(x\in\Pi(e_1, \ldots, e_n)\Leftrightarrow x=\sum\lambda_i e_i,\ 0\leqslant\lambda_i\leqslant 1)$, равен единице.

Следствие 1. *Пусть группа $\mathbb{Z}^n(A)$ совпадает с группой $\mathbb{Z}^n$. Тогда отношение числа точек в множестве $N*A$ к числу $N^n\cdot V(\Delta)$, где $V(\Delta)$ — объем выпуклой оболочки Δ множества A, при $N\to\infty$ стремится к единице.*

Доказательство. Множество $N*A$ содержится в множестве целых точек многогранника $N\cdot\Delta$. Это дает верхнюю оценку числа точек в множестве $N*A$. Нижнюю оценку дает теорема 3. Обе эти оценки при $N\to\infty$ имеют порядок $N^n\cdot V(\Delta)$.

Следствие 2. *Пусть группа $\mathbb{Z}(A)$ имеет в группе $\mathbb{Z}^n$ конечный индекс, равный* $\operatorname{ind} A$. *Тогда отношение числа точек в множестве $N*A$ к числу N^n при $N\to\infty$ стремится к числу* $(\operatorname{ind} A)^{-1}V(\Delta)$.

Доказательство. Можно считать, что множество A содержится в группе $\mathbb{Z}^n(A)$ (если это не так, то вместо множества A нужно рассмотреть сдвинутое множество $A-a$, где a — некоторый элемент множества A). В этом случае можно воспользоваться следствием 1, рассматривая вместо решетки $\mathbb{Z}^n$ решетку $\mathbb{Z}^n(A)$. Для этого нужно только перенормировать метрику: отношение объемов параллелепипедов $\Pi(f_1, \ldots, f_n)$ и $\Pi(e_1, \ldots, e_n)$, где $f_1, \ldots, f_n$ и $e_1, \ldots, e_n$ — базисы решеток $\mathbb{Z}^n(A)$ и $\mathbb{Z}^n$, равно числу $\operatorname{ind} A$. Следствие 2 доказано.

Следствие 3. *Пусть A и B — конечные подмножества в $\mathbb{Z}^n$ и группа $\mathbb{Z}^n(A)$ равна группе $\mathbb{Z}^n$. Тогда отношение числа точек в множестве $N*A+B$ к числу $N^n\cdot V(\Delta)$, где $V(\Delta)$ — объем выпуклой оболочки множества A, при $N\to\infty$ стремится к единице.*

Доказательство. Множество $N*A+B$ содержится в множестве целых точек многогранника $N\cdot\Delta+\Delta_B$, где Δ и Δ_B — выпуклые оболочки множеств A и B. Это дает верхнюю оценку числа точек в множестве $N*A+B$. С другой стороны множество $N*A+B$ содержит не меньше точек, чем множество $N*A$. Обе эти оценки при $N\to\infty$ имеют порядок $N^nV(\Delta)$ (для нижней оценки это вытекает из следствия 2). Следствие 3 доказано.

Докажем теперь теорему 4, сформулированную в п. 1.

Прежде всего, множества b_1+N*A и b_2+N*A не пересекаются, если элементы b_1 и b_2 лежат в разных классах смежности группы G по подгруппе $G(A)$. Поэтому достаточно рассмотреть случай, когда все множество B лежит в одном классе смежности. Далее, можно считать, что как множество B, так и множество A лежат в подгруппе $G(A)$. Если это не так, то вместо множеств A и B можно рассмотреть сдвинутые множества $A-a$ и $B=B-b$, где a, b — некоторые элементы множеств A и B. Но в этом случае теорема 4 сводится к следствию 3: группа $G(A)$ по определению не имеет элементов конечного порядка и, следовательно, изоморфна группе $\mathbb{Z}^n$. Теорема 4 доказана.

В заключение этого пункта докажем одно свойство полугрупп в $\mathbb{Z}^n$, вытекающее из утверждения 1. Пусть A — конечное подмножество в $\mathbb{Z}^n$

и $K(A)$ — порожденный этим подмножеством конус в $\mathbb{R}^n$, $x \in K(A)$, $x = \sum \lambda_i a_i$, $\lambda_i \geqslant 0$, $a_i \in A$.

Утверждение 3. *Пусть группа, порожденная множеством A, совпадает с $\mathbb{Z}^n$. Тогда каждая целая точка сдвинутого конуса $K+x$, где $x = C \sum\limits_{a_i \in A} a_i$ и C — константа, фигурирующая в утверждении 1, принадлежит полугруппе, порожденной множеством A.*

Доказательство. Если вектор $z-x$ лежит в конусе K, то этот вектор представим в виде $z-x = \sum \lambda_i a_i$, $\lambda_i \geqslant 0$. Поэтому вектор z представим в виде $z = \sum (\lambda_i + C) a_i$, где $\lambda_i \geqslant 0$. Согласно утверждению 1 каждый целочисленный вектор z такого вида представим линейной комбинацией векторов a_i с натуральными коэффициентами.

Замечание. Утверждение 3 можно рассматривать как многомерное обобщение следующей простой задачи для школьников: показать, что любую достаточно большую (на самом деле бóльшую семи) натуральную сумму рублей можно заплатить без сдачи трех- и пятирублевыми купюрами. (Действительно, группа, порожденная числами 3 и 5, совпадает с группой $\mathbb{Z}$, порожденный ими конус K совпадает с множеством положительных чисел, а сдвинутый конус $K+C$ — с множеством чисел не меньших C.)

4. Число корней общей системы уравнений

Сначала напомним известные факты из алгебраической геометрии (см. [1]), а затем выведем из этих фактов и теоремы 2 теорему Кушниренко.

4.1. Пусть X — открытое по Зарисскому множество в неприводимом n-мерном комплексном алгебраическом многообразии и L — конечномерное линейное пространство регулярных функций на X. Что можно сказать о решениях системы из n уравнений $f_1 = \ldots = f_n = 0$ на X, где f_i — достаточно общие функции из пространства L? Этот вопрос хорошо изучен в алгебраической геометрии. Сформулируем один из вариантов ответа. Обозначим через X_0 подмножество в X, на котором обращаются в нуль все функции из пространства L.

Обозначим через π_L отображение множества $X \backslash X_0$ в проективное пространство $\mathbb{C}P^{|L|-1}$, заданное формулой $\pi_L(x) = e_1(x) : e_2(x) : \ldots : e_m(x)$, где $e_1, \ldots, e_m$ — базис пространства L (отображение π_L определено с точностью до проективного преобразования). Если образ $\pi_L(X \backslash X_0)$ имеет размерность, меньшую чем n, то общая система уравнений $f_1 = \ldots = f_n = 0$ не совместна в $X \backslash X_0$. Предположим, что образ $\pi_L(X \backslash X)$ имеет размерность n. В этом случае корни почти любой системы $f_1 = \ldots = f_n = 0$ лежат лишь в гладких точках множества $X \backslash X_0$ и являются невырожденными. Почти все такие системы имеют одно и то же число корней. Это число корней равно произведению степени отображения π_L: $X \backslash X_0 \to \pi_L(X \backslash X_0)$ множества $X \backslash X_0$ на свой образ $\pi_L(X \backslash X_0)$ на степень замыкания множества $\pi_L(X \backslash X_0)$ в проективном пространстве. Степень отображения π_L: $X \backslash X_0 \to \pi_L(X \backslash X_0)$ равна числу прообразов почти любой точки $y \in \pi_L(X \backslash X_0)$. Степень замыкания множества $\pi_L(X \backslash X_0)$ в проективном пространстве можно вычислить, используя полином Гильберта. Рассмотрим линейное пространство L^N, состоящее из линейных комбинаций функций $f = f_1 \cdot \ldots \cdot f_N$, где $f_i \in L$. Согласно теореме Гильберта размерность пространства L^N при достаточно больших натуральных N является полиномом от N. Степень d этого полинома равна размерности замыкания множества $\pi_L(X\setminus X_0)$, а умноженный на $d!$ коэффициент при N^d этого полинома равен степени в проективном пространстве замыкания множества $\pi_L(X\setminus X_0)$.

4.2. Перейдем к теореме Кушниренко. Введем нужные определения и обозначения. Каждому характеру $\chi=x_1^{m_1}\cdot\ldots\cdot x_n^{m_n}$ тора $(\mathbb{C}\setminus 0)^n$ соответствует точка $m=m_1, \ldots, m_m$ в целочисленной решетке $\mathbb{Z}^n\subset\mathbb{R}^n$. Полиномом Лорана P на торе $(\mathbb{C}\setminus 0)^n$ называется конечная линейная комбинация характеров, $P=\sum\lambda_i\chi_i$. *Носителем* $\operatorname{supp}(P)$ полинома Лорана P называется конечное множество в решетке $\mathbb{Z}^n$, соответствующее характерам χ_i, входящим в полином Лорана P с ненулевым коэффициентом λ_i.

Фиксируем конечное подмножество A в целочисленной решетке $\mathbb{Z}^n$. Сколько корней в $(\mathbb{C}\setminus 0)^n$ имеет общая система уравнений $P_1=\ldots=P_n=0$, в которой P_i — полиномы Лорана с носителем A? Ответ на этот вопрос дает следующая

Теорема Кушниренко ([2]). *Число корней в $(\mathbb{C}\setminus 0)^n$ общей системы уравнений $P_1=\ldots=P_n=0$, $\operatorname{supp}(P)=A$, равно умноженному на $n!$ объему выпуклой оболочки множества A.*

Доказательство. Применим факты из алгебраической геометрии, сформулированные в п. 4.1, в том случае, когда $X=(\mathbb{C}\setminus 0)^n$ и пространство L состоит из линейных комбинаций характеров, соответствующих точкам множества A. Размерность образа пространства $(\mathbb{C}\setminus 0)^n$ при отображении π_L в проективное пространство равна рангу группы $\mathbb{Z}^n(A)$, порожденной разностями элементов множества A. Ранг группы $\mathbb{Z}^n(A)$ меньше, чем n, если и только если объем выпуклой оболочки множества A равен нулю. В этом случае очевидно, что соответствующая общая система уравнений несовместна. Если ранг группы $\mathbb{Z}^n(A)$ равен n, то степень отображения тора $(\mathbb{C}\setminus 0)^n$ на свой образ равна индексу $\operatorname{ind} A$ подгруппы $\mathbb{Z}^n(A)$ в группе $\mathbb{Z}^n$ (любая точка образа имеет ровно $\operatorname{ind} A$ прообразов в торе $(\mathbb{C}\setminus 0)^n$). Пространство L^N состоит из линейных комбинаций характеров, соответствующих точкам множества $N*A$. Размерность пространства L^N равна числу точек в множестве $N*A$. Согласно следствию 2 к теореме 3 (см. п. 3) старший коэффициент полинома Гильберта равен объему $V(\Delta)$ выпуклой оболочки множества A, деленному на число $\operatorname{ind} A$. Поэтому число корней общей системы уравнений $P_1=\ldots=P_n=0$ в $(\mathbb{C}\setminus 0)^n$ равно $n!\operatorname{ind} A\cdot(V(\Delta)/\operatorname{ind} A)=n!V(\Delta)$.

5. Группы Гротендика полугрупп конечных подмножеств в $\mathbb{Z}^n$ и компактных подмножеств в $\mathbb{R}^n$

Пусть A — компактное подмножество в конечномерном линейном пространстве L, а Δ — его выпуклая оболочка размерности k.

Лемма. *Для каждой точки x многогранника $\lambda\cdot\Delta$, где λ любое число, не меньшее чем $k+1$, существует точка $a\in A$ такая, что вектор $x-a$ лежит в многограннике $(\lambda-1)\cdot\Delta$.*

Доказательство. Точка $y=\lambda^{-1}x$ лежит в многограннике Δ. Так как размерность Δ равна k, то точка y лежит в одном из k-мерных симплексов, вершины $a_0, \ldots, a_k$ которого лежат в множестве A, $y=\sum\limits_{0\leqslant i\leqslant k}\lambda_i a_i$, $\lambda_i\geqslant 0$, $\sum\limits_{0\leqslant i\leqslant k}\lambda_i=1$. Коэффициент λ_j при одном из векторов a_j не меньше чем $(k+1)^{-1}$. Точка $x-a_j$ лежит в многограннике $(k-1)\cdot\Delta$.

Следствие 1. *При любом гомоморфизме полугруппы по сложению компактных подмножеств конечномерного линейного пространства в абелеву группу образы подмножеств, имеющих одинаковые выпуклые оболочки, совпадают.*

Доказательство. Пусть Δ — выпуклая оболочка компактных подмножеств A и B. Тогда множества $A+k\cdot\Delta$ и $B+k\cdot\Delta$, где k равно размерности линейного пространства, совпадают: действительно, согласно лемме оба этих множества равны $(k+1)\cdot\Delta$. Так как $A+k\cdot\Delta=B+k\cdot\Delta$, то при гомоморфизме в любую абелеву группу образы элементов A и B совпадают.

Формальные разности $\Delta_1-\Delta_2$ выпуклых тел Δ_1, $\Delta_2\in L$ с естественным отношением эквивалентности $\Delta_1-\Delta_2\sim\Delta_5-\Delta_4\Leftrightarrow\Delta_1+\Delta_2=\Delta_2+\Delta_3$ образуют абелеву группу. Следствие 1 показывает, что эта группа является группой Гротендика полугруппы компактных подмножеств пространства L относительно сложения.

Пусть A, B — конечные подмножества целочисленной решетки $\mathbb{Z}^n$, Δ — выпуклая оболочка множества A и B — множество целых точек многогранника $K\cdot\Delta$, где $K\in\mathbb{Z}$, $K\geqslant n$.

Непосредственно из леммы вытекает следующее

Следствие 2. *Множество $A+B$ состоит из всех целых точек многогранника* $(K+1)\Delta$.

Следствие 3. *Для всякого целочисленного многогранника Δ число целых точек в многограннике $N\cdot\Delta$ является полиномом на множестве достаточно больших натуральных чисел N.*

Следствие 3 вытекает из теоремы 1, примененной к подмножествам A и B в решетке $\mathbb{Z}^n$, где A — множество целых точек многогранника Δ и B — множество целых точек многогранника $n\cdot\Delta$ (см. следствие 2).

Замечание. Справедлива более сильная теорема Макдональда [3]: число целых точек в многограннике $N\cdot\Delta$ является полиномом на множестве всех натуральных чисел N. Алгебраическое доказательство [4] теоремы Макдональда использует не только полином Гильберта, но и равенство нулю когомологий торического многообразия с коэффициентами в некотором пучке, построенном по многограннику Δ.

Следствие 4 доказывается так же, как и следствие 1. Формальные разности целочисленных многогранников с естественным отношением эквивалентности образуют абелеву группу. Следствие 4 показывает, что эта группа является группой Гротендика полугруппы конечных подмножеств решетки.

Замечание. Следствие 4 проясняет, почему дискретные характеристики гиперповерхности $P=0$ в торе $(\mathbb{C}\backslash 0)^n$ зависят не от носителя $\operatorname{supp}(P)$ полинома Лорана P, а от выпуклой оболочки $\Delta(P)$ этого носителя. Доказательство этого факта, основанное на других соображениях, можно найти в [4].

СПИСОК ЛИТЕРАТУРЫ

1. *Мамфорд Д.* Алгебраическая геометрия. Т. 1.– М.: Мир, 1979.
2. *Kouchnirenko A. G.* Polyedres de Newton et pombres de Milnor // Inv. Math.– V. 32.– P. 1–31.
3. *Mc. Mullen P.* Valuations and Euler-type relations on certain classes of convex polytopes // Proc. London Math. Soc. Ser. 3.– 1977 – V. 35. N 1.– P. 113–135.
4. *Хованский А. Г.* Многогранник Ньютона и торические многообразия // Функ. анализ.– 1977.– Т. 11, вып. 4. – С. 56–67.

Институт системного анализа РАН

Поступило в редакцию
10 октября 1991 г.