Б. Я. Казарновский, А. Г. Хованский, Тропическая нетеровость и базисы Грёбнера, *Алгебра и анализ*, 2014, том 26, выпуск 5, 142–163

Алгебра и анализ
Том 26 (2014), №5

ТРОПИЧЕСКАЯ НЕТЕРОВОСТЬ И БАЗИСЫ ГРЁБНЕРА

© Б. Я. КАЗАРНОВСКИЙ, А. Г. ХОВАНСКИЙ

Универсальный базис Грёбнера идеала в кольце полиномов — это конечное подмножество идеала, содержащее его базисы Грёбнера относительно любого порядка Грёбнера. В статье доказывается существование универсального базиса, полиномы в котором имеют контролируемые степени. Теорема о *тропической нетеровости* кольца полиномов Лорана близка к теореме о существовании универсального базиса. Эта теорема — центральный результат статьи, нужный для *тропической теории пересечений* в $(\mathbb{C}^*)^n$, которую мы изложим в последующих работах.

Введение

В статье доказывается свойство тропической нетеровости (см. ниже) кольца $\mathcal{R}$ полиномов Лорана от n переменных над произвольным полем $\mathbf{k}$. Эта теорема из коммутативной алгебры входит в различные описания своеобразного варианта кольца Чжоу, так называемого кольца условий (см. ниже и [1, 2]), для группы $(\mathbb{C}^*)^n$, которые мы подготавливаем для публикации. Статья независима от этого материала и сравнительно элементарна: она не использует теории пересечений, торической геометрии, теории смешанных объемов и конструкций тропической геометрии, нужных для описания кольца условий. Как нам кажется, статья представляет и самостоятельный интерес.

Во введении сформулировано свойство тропической нетеровости, описано расположение материала и (очень кратко) рассказано о кольце условий для группы $(\mathbb{C}^*)^n$.

Полином Лорана $P = \sum c_m z^m \in \mathcal{R}$ — это линейная комбинация мономов $z^m = z_1^{m_1} \dots z_n^{m_n}$, где $m = (m_1, \dots, m_n) \in \mathbb{Z}^n$ и $c_m \in \mathbf{k}$. Носитель $S(P)$ полинома Лорана P — множество точек $m \in \mathbb{Z}^n$, для которых $c_m \neq 0$.

Ключевые слова: полином Лорана, идеал, тропический базис, универсальный базис Грёбнера, теорема Зайденберга.

Первый автор частично поддержан грантом НШ-4850.2012.1, второй автор частично поддержан Канадским грантом 0GP0156833.

С каждой линейной функцией $f\colon \mathbb{R}^n \to \mathbb{R}$ на пространстве $\mathbb{R}^n$, содержащем решетку $\mathbb{Z}^n$, связано *укорочение* $P^{(f)}$ *по порядку* f полинома Лорана $P = \sum c_m z^m$. По определению $P^{(f)} = \sum_{m\in B} c_m z^m$, где B — подмножество носителя $S(P)$ полинома P, на котором достигает максимума линейная функция f. С каждым идеалом $I \subset \mathcal{R}$ и с каждым порядком f свяжем идеал $I^{(f)}$, порожденный укорочениями по порядку f всех полиномов Лорана из идеала I (при $f \equiv 0$ идеалы I и $I^{(f)}$ совпадают).

Конечное множество $\{Q_j\} \subset I$ называется системой *тропических образующих* идеала I, если для всякого порядка f идеал $I^{(f)}$ порожден полиномами Лорана $\{Q_j^{(f)}\}$.

Замечание 1. Понятие тропических образующих идеала близко к понятию H-базиса (см., например, [18, 19]). Мы благодарны рецензенту за это замечание.

Мы доказываем, что кольцо $\mathcal{R}$ обладает свойством *тропической нетеровости*: в каждом идеале I кольца $\mathcal{R}$ существует система тропических образующих. Мы не только доказываем существование тропических образующих, но предъявляем их достаточно явное описание. Отметим, что несколько более слабые аналогичные результаты были известны и раньше (ср. [3, 4]).

Теорема. *По любому конечному множеству $A \subset \mathbb{Z}^n$ можно построить конечное множество $\Phi(A) \subset \mathbb{Z}^n$, обладающее следующим свойством. Для каждого идеала I кольца $\mathcal{R}$, носители образующих которого лежат в множестве A, можно выбрать систему тропических образующих $\{Q_j\}$, носители $S(Q_j)$ которых лежат в множестве $\Phi(A)$.*

В немного более точном виде эта теорема сформулирована и доказана в §7. Доказательство использует теорему Зайденберга (см. §1 и [5, 6]), уточняющую свойство нетеровости кольца полиномов, и технику базисов Грёбнера. Эта техника частично основана на простых результатах о линейных пространствах с вполне упорядоченным базисом (см. §2). Немного более громоздкая часть этой техники связана с определениями порядка Грёбнера (см. п. 2.4) и базиса Грёбнера, с теоремой Бухбергера и с алгоритмом Бухбергера (см. §3).

В п. 5.1 оцениваются степени полиномов, возникающих при применении двухшаговой процедуры из алгоритма Бухбергера. Очень важно, что полученные оценки зависят лишь от степеней полиномов, к которым применяется процедура, но никак не зависят от порядка Грёбнера. Оценки основаны на описании всевозможных линейных порядков на конечных подмножествах решетки $\mathbb{Z}^n$ и используют простые соображения выпуклой геометрии (см. §4).

В п. 5.2 оцениваются степени полиномов в базисе Грёбнера по степеням образующих идеала. Приводимые оценки не зависят от порядка Грёбнера. Они основаны на теореме Зайденберга и на оценках из п. 5.1.

В §6 для всякого идеала в кольце полиномов приводится достаточно явная (хотя и не реализуемая практически) конструкция его *универсального базиса Грёбнера* и оцениваются стенени полиномов в этом базисе по степеням образующих идеала. Этот результат не используется в дальнейшем. Он является прямым следствием оценок из п. 5.2 и демонстрирует их силу.

§7 содержит основную теорему (о тропической нетеровости кольца полиномов Лорана). Она тоже легко вытекает из оценок п. 5.2.

В оставшейся части введения очень кратко рассказывается о кольце условий для группы $(\mathbb{C}^*)^n$. Эту часть введения можно пропустить без ущерба для понимания статьи — в статье кольцо условий больше не фигурирует (но его изучение было главной мотивировкой для полученных в статье результатов).

Известна (см. [1, 2]) следующая версия кольца Чжоу для n-мерной редуктивной группы G. Два k-мерных подмногообразия $X_1, X_2 \subset G$ *эквивалентны* $X_1 \sim X_2$, если для любого $(n-k)$-мерного подмногообразия $Y \subset G$ для почти всех $g_1, g_2 \in G$ выполнено равенство $\#(X_1 \cap g_1 Y g_2) = \#(X_2 \cap g_1 Y g_2)$. Если $X_1 \sim X_2$ и $Y_1 \sim Y_2$, то для почти всех $g_1, g_2, g_3, g_4 \in G$ многообразия $X_1 \cap g_1 Y_1 g_2$ и $X_2 \cap g_3 Y_2 g_4$ эквивалентны. Таким образом корректно определено умножение на классах эквивалентности подмногообразий, сопоставляющее классам пересечение их представителей (приведенных, если надо, в общее положение с помощью лево-правого действия группы). *Кольцо условий* $R(G)$ группы G — это кольцо формальных линейных комбинаций классов эквивалентности вместе с описанным умножением, продолженным по линейности на линейные комбинации.

В [8] дано следующее описание кольца $R((\mathbb{C}^*)^n)$. Каждому k-мерному подмногообразию $X \subset (\mathbb{C}^*)^n$ сопоставлен некоторый k-мерный тропический веер (своеобразный k-мерный вещественный цикл, являющийся линейной комбинацией k-мерных рациональных конусов) C_X в $\mathbb{R}^n$. При этом $(C_X = C_Y) \Leftrightarrow (X \sim Y)$. Приведены геометрическое описание всех тропических вееров вида C_X и геометрическая конструкция тропического веера $C_{X \cap Y}$ по тропическим веерам C_X и C_Y. Таким образом, в [8] описано *кольцо тропических вееров* C_X, изоморфное кольцу $R((\mathbb{C}^*)^n)$. Близкие результаты содержатся в [3]. Ряд красивых и сильных результатов тропической геометрии можно найти в [9–11].

Мы нашли новое описание кольца $R((\mathbb{C}^*)^n)$ в терминах смешанных объемов целочисленных многогранников, полностью пересмотрели результаты статьи [8] и доказали изоморфизм кольца, построенного в терминах смешанных объемов, с кольцом тропических вееров. Эти результаты подготавливаются к печати [12]. Все они используют теорему из коммутативной алгебры, которой и посвящена настоящая статья.

§1. Теорема Зайденберга

В этом параграфе мы формулируем теорему Зайденберга для кольца полиномов и ее аналог для полугруппы $\mathbb{Z}^n_{\geqslant 0}$.

1.1. Кольцо полиномов. Кольцо $R = \mathbf{k}[z_1, \ldots, z_n]$ полиномов от n переменных над любым полем $\mathbf{k}$ обладает *свойством нетеровости*: в кольце R всякая строго возрастающая цепочка идеалов

$$I_1 \subset I_2 \subset \cdots \subset I_i \subset \ldots \tag{1}$$

обрывается за конечное число шагов. Абрахам Зайденберг доказал теорему [5, 6], которую можно сформулировать следующим образом.

Теорема Зайденберга. *Пусть f — заданная строго возрастающая функция на натуральных числах. Пусть идеалы I_i в (1) порождены полиномами степени $\leqslant f(i)$. Тогда число идеалов в цепочке (1) не превосходит числа g_n, которое может быть явно вычислено по функции f и размерности n.*

В исходных статьях [5, 6] словам „g_n может быть явно вычислено по функции f и размерности n“ придан более точный смысл. Замечательная работа Гильермо Морено [7] уточняет теорему Зайденберга. В этой работе, в частности, приведены примеры, показывающие, что даже для простейшей возрастающей функции $f(i) = i$ число g_n как функция от n растет страшно быстро и не является *примитивно рекурсивной функцией от* n (см. [7]). Для дальнейшего нам будет достаточно теоремы Зайденберга в приведенной формулировке. За всеми подробностями мы отсылаем к хорошо написанной статье [7].

1.2. Полугруппа $\mathbb{Z}^n_{\geqslant 0}$. С каждой точкой $m \in \mathbb{Z}^n_{\geqslant 0}$ связан *октант* O_m *с вершиной* m, определенный равенством $O_m = \mathbb{Z}^n_{\geqslant 0} + m$. Напомним важное *свойство конечности* полугруппы $\mathbb{Z}^n_{\geqslant 0}$ (см., например, [13]): объединение любого множества октантов представимо в виде объединения некоторого конечного множества октантов.

Подмножество $J \subset \mathbb{Z}^n_{\geqslant 0}$ называется *идеалом* в полугруппе $\mathbb{Z}^n_{\geqslant 0}$, если для любых $m \in J$, $a \in \mathbb{Z}^n_{\geqslant 0}$ выполнено включение $m + a \in J$. Полугруппа $\mathbb{Z}^n_{\geqslant 0}$

обладает свойством нетеровости: в ней всякая строго возрастающая цепочка идеалов

$$J_1 \subset J_2 \subset \cdots \subset J_i \subset \ldots \tag{2}$$

обрывается за конечное число шагов. Этот факт эквивалентен свойству конечности полугруппы $\mathbb{Z}^n_{\geqslant 0}$. Следующее утверждение тоже эквивалентно свойству конечности полугруппы $\mathbb{Z}^n_{\geqslant 0}$: *в каждом идеале $J \subset \mathbb{Z}^n_{\geqslant 0}$ можно выбрать конечное число образующих*, т.е. существует конечное множество элементов $G \subset J$ таких, что каждый элемент идеала J представлен в виде $m+a$, где $m \in G$ и $a \in \mathbb{Z}^n_{\geqslant 0}$. *Степенью точки* $m = (m_1, \ldots, m_n) \in \mathbb{Z}^n_{\geqslant 0}$ называется число $|m| = m_1 + \cdots + m_n$.

Теорема Зайденберга для $\mathbb{Z}^n_{\geqslant 0}$. *Пусть f — заданная строго возрастающая функция на натуральных числах. Пусть образующие идеалов J_i из* (2) *имеют степени $\leqslant f(i)$. Тогда число идеалов в цепочке* (2) *не превосходит числа g_n, которое может быть явно вычислено по функции f и размерности n.*

Каждой точке $m = (m_1, \ldots, m_n) \in \mathbb{Z}^n_{\geqslant 0}$ можно сопоставить моном $z^m = z_1^{m_1} \cdot \ldots \cdot z_n^{m_n}$. Каждому идеалу $J \subset \mathbb{Z}^n_{\geqslant 0}$ можно сопоставить идеал $I(J)$ в кольце полиномов, состоящий из линейных комбинаций мономов z^m при $m \in J$. Для цепочки (2) теорема Зайденберга для $\mathbb{Z}^n_{\geqslant 0}$ вытекает из теоремы Зайденберга, примененной к цепочке идеалов $I(J_1) \subset I(J_2) \subset \ldots \subset I(J_i) \ldots$

Замечание 2. Используя технику базисов Грёбнера, легко показать, что теорема Зайденберга эквивалентна своему варианту для полугруппы $\mathbb{Z}^n_{\geqslant 0}$. В [7] доказывается именно этот вариант, а теорема Зайденберга выводится из него.

§2. Линейные пространства с упорядоченным базисом

Линейное пространство K (вообще говоря, бесконечномерное) над $\mathbf{k}$ называется *пространством с вполне упорядоченным базисом*, если в нем фиксирован базис $\{e_m\}$, занумерованный элементами множества $\mathcal{M}$, в котором задан порядок $\prec$, превращающий $\mathcal{M}$ во вполне упорядоченное множество.

2.1. Обращение операторов в пространствах с упорядоченным базисом. Начнем с несложного утверждения, справедливого для линейных пространств, не наделенных никакими дополнительными структурами. Оператор $A : L \to L$, действующий в (бесконечномерном) линейном пространстве L над $\mathbf{k}$, называется *обобщенно нильпотентным*, если для

каждого вектора $x \in L$ существует число k (зависящее от x) такое, что $A^k x = 0$.

Утверждение 1. *Пусть E — тождественный и A — обобщенно нильпотентный операторы. Тогда оператор $E - A$ обратим: оператор*

$$B = E + A + A^2 + \dots$$

корректно определен и выполнено тождество $(E - A)B = E$.

Доказательство. Действительно, по определению для каждого $x \in L$ есть k такое, что $A^k x = 0$. Поэтому вектор Bx корректно определен и равен $(E + A + \dots + A^{k-1})x$. Далее, $(E - A)Bx = (E - A^k)x = x$. □

Пусть K — пространство с вполне упорядоченным базисом $\{e_m\}$. Скажем, что оператор $A : K \to K$ *верхнетреугольен* в базисе $\{e_m\}$, если для каждого индекса $m \in \mathcal{M}$ в равенстве $A(e_m) = \sum \mu_p e_p$ при $m \prec p$ и при $m = p$ коэффициент μ_p равен нулю.

Утверждение 2. *Верхнетреугольный оператор обобщенно нильпотентен.*

Доказательство основано на формулируемой ниже лемме 3.

Соответствие C, сопоставляющее каждому элементу $m \in \mathcal{M}$ конечное (возможно, пустое) подмножество $C(m)$ множества $\mathcal{M}$, назовем *конечнозначным убывающим отображением*, если для всяких $m \in \mathcal{M}$ и $g \in C(m) \subset \mathcal{M}$ выполнено неравенство $m \succ g$. Последовательность $m_1, \dots, m_k \in \mathcal{M}$ назовем *C-последовательностью* для конечнозначного убывающего отображения C, если для каждого $i = 1, \dots, k-1$ выполняется включениее $m_{i+1} \in C(m_i)$ (если $C(m_i)$ — пустое множество, то последовательность обрывается на члене m_i).

Лемма 3. *Всякая C-последовательность $m_1, \dots, m_k$ с заданным первым членом $m_1 = m \in \mathcal{M}$ имеет ограниченную сверху длину $k \leqslant N(C, m)$.*

Доказательство. Пусть есть как угодно длинные C-последовательности, начинающиеся в точке $m = m_1$. Тогда (из-за конечности множества $C(m_1)$) существует такая точка $m_2 \in C(m_1)$, что есть как угодно длинные C-последовательности, начинающиеся с членов m_1, m_2. Аналогично существует точка $m_3 \in C(m_2)$ такая, что есть как угодно длинные C-последовательности, начинающиеся с членов m_1, m_2, m_3. Продолжая этот процесс, получим бесконечную последовательность $m_1 \succ m_2 \succ \dots$ Существование такой последовательности противоречит полной упорядоченности множества $\mathcal{M}$. Лемма доказана. □

Доказательство утверждения 2. Пусть A — верхнетреугольный оператор в базисе $\{e_m\}$. С оператором A свяжем многозначное убывающее отображение C, определенное следующим соотношением: множество $C(m)$ равно множеству идексов m_i, для которых коэффициенты μ_i в разложении $Ae_m = \sum \mu_i e_{m_i}$ отличны от нуля (если $Ae_m = 0$, то множество $C(m)$ пусто). По лемме 3 найдется число $N(m, C)$ такое, что длина всякой C-последовательности, начинающейся с члена m, меньше $k = N(m, C)$. Ясно, что $A^k e_m = 0$. Откуда вытекает утверждение 2. □

Теорема 4. *Оператор, равный сумме тождественного и верхнетреугольного операторов, обратим.*

Теорема 4 вытекает из утверждений 1 и 2.

2.2. Отображение $\mathcal{M}$-нормирования и разложение в прямую сумму. Пусть $v = \sum c_m(v)e_m$ — ненулевой вектор в пространстве K с вполне упорядоченным базисом $\{e_m\}$. Коэффициенты $c_m(v)$ отличны от нуля на конечном множестве $S(v) \subset \mathcal{M}$, которое называется *носителем* вектора v.

Определение 1. Отображение $N_{\mathcal{M}} : (K \setminus \{0\}) \to \mathcal{M}$, сопоставляющее вектору $v \in K \setminus \{0\}$ максимальную в смысле порядка $\prec$ точку $N_{\mathcal{M}}(v) \in S(v)$ в носителе вектора v, называется $\mathcal{M}$-*нормированием.*

Опишем конструкцию, использующую $\mathcal{M}$-нормирование, которая сопоставляет каждому линейному пространству $L \subset K$ дополнительное пространство $L^\perp \subset K$ (т.е. такое пространство, что $L \oplus L^\perp = K$). С пространством $L \subset K$ свяжем следующие множества:

образ $N_{\mathcal{M}}(L \setminus \{0\}) = \mathcal{J}$ множества $L \setminus \{0\}$ при $\mathcal{M}$-нормировании;

дополнение $\mathcal{M} \setminus \mathcal{J} = \mathcal{J}^\perp$ к множеству $\mathcal{J}$ в $\mathcal{M}$.

Определим пространство $L^\perp$ как пространство, порожденное векторами e_m при $m \in J^\perp$. Равенство $K = L \bigoplus L^\perp$ доказано ниже в теореме 5.

Для каждой точки $p \in \mathcal{J}$ фиксируем вектор $g_p \in L$ такой, что $N_{\mathcal{M}}(g_p) = e_p$, т.е. $g_p = e_p + \sum \mu_i e_{m_i}$, где $m_i \prec p$. Для каждого индекса $m \in \mathcal{M}$ определим следующий вектор $f_m \in K$:

если $m \in \mathcal{J}$, то $f_m = g_m$;

если $m \in \mathcal{J}^\perp$, то $f_m = e_m$.

Теорема 5. 1) $K = L \bigoplus L^\perp$. 2) *Если* $x = x_1 + x_2$, *где* $x_1 \in L$, $x_2 \in L^\perp$ *и* $x_1, x_2 \neq 0$, *то* $N_{\mathcal{M}}(x) = \max(N_{\mathcal{M}}(x_1), N_{\mathcal{M}}(x_2))$. 3) *Векторы* $\{f_m\}$ *образуют базис в* K. 4) *Векторы* $\{g_p\}$ *при* $p \in \mathcal{J}$ *образуют базис в* L. 5) *Векторы* $\{e_m\}$ *при* $m \in \mathcal{J}^\perp$ *образуют базис* $L^\perp$.

Доказательство. Начнем с доказательства п. 2). Так как $J \bigcap J^{\perp} = \emptyset$, то $N_{\mathcal{M}}(x_1) \neq N_{\mathcal{M}}(x_2)$. Поэтому элемент $N_{\mathcal{M}}(x_1 + x_2)$ равен наибольшему из элементов $N_{\mathcal{M}}(x_1)$ и $N_{\mathcal{M}}(x_2)$. Рассмотрим линейный оператор $\Phi : K \to K$, определенный на базисных векторах $\{e_m\}$ равенством $\Phi(e_m) = f_m$. По определению векторов f_m оператор Φ равен сумме тождественного и верхнетреугольного в базисе $\{e_m\}$ оператора. Согласно теореме 4 оператор Φ обратим. Отсюда немедленно вытекают все остальные пункты теоремы 5. □

Определение 2. Пусть $\{g_p\}$, $p \in \mathcal{J}$, — базис в L из п. 4) теоремы 5. Множество векторов $\{v_p = \lambda_p g_p\}$, где λ_p — любые ненулевые элементы основного поля $\mathbf{k}$, будем называть $(\mathcal{M})$-базисом Грёбнера пространства L.

Из п. 4) теоремы 5 следует, что любой $(\mathcal{M})$-базис Грёбнера является базисом и что размерность конечномерного пространства L равна числу точек в множестве $\mathcal{J}$.

Как с помощью $\mathcal{M}$-нормирования определить, совпадают или не совпадают между собой два вложенных подпространста $L \subset M$ пространства K? Теорема 5 позволяет ответить на этот вопрос.

Следствие 6. *Рассмотрим тройку пространств $L \subset M \subset K$. Соотношение $M \neq L$ выполняется, если и только если существует вектор $v \in M \setminus \{0\}$, носитель $S(v)$ которого не пересекается с множеством $\mathcal{J}$.*

Доказательство. Если $M \neq L$, то существует вектор $x \in M$, представимый в виде $x = x_1 + x_2$, где $x_1 \in L$, $x_2 \in L^{\perp}$ и $x_2 \neq 0$. Так как $x_1 \in L \subset M$, то вектор $v = x_2 = x - x_1$ лежит в M. Его носитель $S(v)$ не пересекается с J. □

2.3. Простейший аналог алгоритма Бухбергера. Пусть задано конечное множество ненулевых векторов $G \subset K$. Рассмотрим две следующие задачи. Как найти образ $\mathcal{J}$ при отображении $\mathcal{M}$-нормирования множества $L \setminus \{0\}$, где $L \subset K$ — пространство, порожденное векторами из G? Как найти $\mathcal{M}$-базис Грёбнера в L?

Опишем алгоритм, решающий эти задачи. Этот алгоритм — простейший аналог алгоритма Бухбергера, нужного нам в дальнейшем.

В качестве первого приближения к множеству $\mathcal{J}$ возьмем множество $\mathcal{J}_G = N_{\mathcal{M}}(G)$. Выберем любое отображение $\mathcal{F}\colon \mathcal{J}_G \to G$ такое, что для $g = \mathcal{F}(p)$ выполняется равенство $N_{\mathcal{M}}(g) = p$. (Равенство $N_{\mathcal{M}}(g) = p$, вообще говоря, не определяет однозначно вектор g, и в выборе отображения $\mathcal{F}$ есть произвол.)

В качестве первого приближения к $(\mathcal{M})$-базису в L возьмем набор векторов $V \subset G$, совпадающий с множеством значений отображения $\mathcal{F}$. По построению $N_{\mathcal{M}}(V) = N_{\mathcal{M}}(G)$ и множество V является $\mathcal{M}$-базисом Грёбнера пространства $L(\mathcal{J}_G, \mathcal{F}) \subset L$, порожденного векторами из V.

Если выполняется включение $G \subset L(\mathcal{J}_G, \mathcal{F})$, то множество $\mathcal{J}$ совпадает со своим первым приближением $\mathcal{J}_G$, пространство L совпадает с $L(\mathcal{J}_G, \mathcal{F})$, множество V является $(\mathcal{M})$-базисом Грёбнера в L. В этом случае обе задачи решены.

Если включение $G \subset L(\mathcal{J}_G, \mathcal{F})$ не выполняется, то существуют векторы $g_j \in G$, не лежащие в $L(\mathcal{J}_G, \mathcal{F})$. Положим $\mathcal{J}_G^{\perp} = \mathcal{M} \setminus \mathcal{J}_G$ и определим пространство $L(\mathcal{J}_G^{\perp})$, порожденное базисными векторами e_q, $q \in \mathcal{J}_G^{\perp}$. По теореме 5 каждый вектор g_j раскладывается в сумму $g_j = g_j^1 + g_j^2$, где $g_j^1 \in L(\mathcal{J}_G, \mathcal{F})$ и $g_j^2 \in L(\mathcal{J}_G^{\perp},)$. Векторы g_j^2 лежат в пространстве L, так как g_j и g_j^1 лежат в L. Обозначим через $G_1 \subset L$ объединение множества V с множеством всех ненулевых векторов g_j^2. Множество G_1 порождает пространство L. Применим к множеству G_1 процедуру, которую мы применяли к множеству G. В результате мы построим множество $\mathcal{J}_{G_1} = N_{\mathcal{M}}(G_1)$, отображение $\mathcal{F}_1 : \mathcal{J}_{G_1} \to G_1$, множество векторов $V_1 = \mathcal{F}(G_1)$ и пространство $L(\mathcal{J}_{G_1}, \mathcal{F}_1)$, порожденное векторами из V_1. Вторым приближением к множеству $\mathcal{J}$ будет множество $\mathcal{J}_{G_1}$. Оно строго больше множества $\mathcal{J}_G$, так как носители ненулевых векторов g_j^2 целиком лежат в дополнении множества $\mathcal{J}_G$. Пространство $L(\mathcal{J}_{G_1}, \mathcal{F}_1) \subset L$ строго больше пространства $L(\mathcal{J}_G, \mathcal{F})$. Если выполняется включение $G_1 \subset L(\mathcal{J}_{G_1}, \mathcal{F}_1)$, то обе задачи решены.

Если включение не выполняется, то опять применим к множеству G_1 нашу процедуру и т.д. Этот процесс не может продолжаться бесконечно, так как множества $\mathcal{J}_{G_i} \subset \mathcal{J}$ строго возрастают с ростом i, а множество $\mathcal{J}$ конечно. В результате за конечное число шагов обе задачи будут решены.

2.4. Порядок Грёбнера, пространство $L(J_G, F)$ и укорочения полиномов. Здесь определяется порядок Грёбнера. С его помощью строится пространство $L(J_G, F)$. Рассматриваются укорочения полиномов из этого пространства по порядку f для линейной функции f, монотонной относительно порядка Грёбнера.

Определение 3. Порядок $\prec$ на решетке $\mathbb{Z}^n$ *согласован с групповой структурой*, если для a, b, $c \in \mathbb{Z}^n$ из $a \prec b$ следует, что $a + c \prec b + c$. Ограничение на $\mathbb{Z}^n_{\geqslant 0}$ порядка на $\mathbb{Z}^n$, согласованного с групповой структурой, называется *порядком Грёбнера* на $\mathbb{Z}^n_{\geqslant 0}$, если относительно этого порядка полугруппа $\mathbb{Z}^n_{\geqslant 0}$ является вполне упорядоченным множеством с минимальным элементом 0.

Каждому моному $z^m = z_1^{m_1} \cdot \ldots \cdot z_n^{m_n}$, где $z = z_1, \ldots, z_n$, $m = (m_1, \ldots, m_n) \in \mathbb{Z}^n_{\geqslant 0}$, можно сопоставить его степень m. Это сопоставление — изоморфизм мультипликативной полугруппы мономов неотрицательных степеней с полугруппой $\mathbb{Z}^n_{\geqslant 0}$. Оно задает нумерацию мономов элементами полугруппы $\mathbb{Z}^n_{\geqslant 0}$. В линейном пространстве $R = \mathbf{k}[z_1, \ldots, z_n]$ мономы образуют базис. Фиксация порядка Грёбнера на полугруппе $\mathbb{Z}^n_{\geqslant 0}$ превращает пространство полиномов в линейное пространство с вполне упорядоченным базисом, к которому применимы результаты п. 2.1–2.3.

Определение 4. Отображение $\mathcal{M}$-нормирования множества ненулевых полиномов $R \setminus \{0\}$ в $\mathbb{Z}^n_{\geqslant 0}$, соответствующее порядку Грёбнера на полугруппе $\mathbb{Z}^n$, называется отображением Грёбнера и обозначается $Gr : R \setminus \{0\} \to \mathbb{Z}^n_{\geqslant 0}$.

Фиксируем некоторый порядок Грёбнера на полугруппе $\mathbb{Z}^n_{\geqslant 0}$. С конечным множеством $G \subset \mathbf{k}[z_1, \ldots, z_n] \setminus \{0\}$ свяжем линейное подпространство $L(J_G, F)$ (зависящее от выбора некоторого отображения F). Пусть

J_G — идеал в полугруппе $\mathbb{Z}^n_{\geqslant 0}$, равный $\bigcup_{m \in A} O_m$, где $A = Gr(G)$;

$J_G^{\perp}$ — коидеал в полугруппе $\mathbb{Z}^n_{\geqslant 0}$, определенный равенством $J_G^{\perp} = \mathbb{Z}^n_{\geqslant 0} \setminus J_G$;

$L(J_G^{\perp})$ — пространство полиномов, порожденное мономами z^j, $j \in J_G^{\perp}$;

$F : J_G \to G$ — любое отображение такое, что если $g = F(p)$, то $p \in O_m$, где $m = Gr(g)$.

По порядку Грёбнера, множеству G и отображению F построим *линейное пространство* $L(J_G, F) \subset R$, порожденное полиномами $g_p = z^{p-m} g$, где $p \in J_G$, $g = F(p) \in G$ и $m = Gr(g)$.

Определение 5. Пусть $f : \mathbb{R}^n \to \mathbb{R}$ — линейная функция на пространстве $\mathbb{R}^n$, содержащем $\mathbb{Z}^n$. С каждым ненулевым полиномом $P = \sum a_m z^m$ связано его *укорочение $P^{(f)}$ по порядку f*: по определению $P^{(f)} = \sum_{m \in B} a_m z^m$, где B — подмножество в носителе $S(P)$ полинома P, на котором достигает максимума функция f. Максимальное значение функции f на $S(P)$ будем обозначать $\deg_f(P)$.

Очевидно, что

1) $(PQ)^{(f)} = P^{(f)} Q^{(f)}$;

2) если $\deg_f P = \deg_f Q$ и $P^{(f)} + Q^{(f)} \neq 0$, то $(P+Q)^{(f)} = P^{(f)} + Q^{(f)}$.

Скажем, что линейная функция f *монотонна относительно порядка Грёбнера* $\prec$, если из $x \prec y$ вытекает, что $f(x) \leqslant f(y)$.

Утверждение 7. *Пусть $L(J_G, F)$ — пространство, построенное по G, F и по некоторому порядку Грёбнера, и f — монотонная функция относительно этого порядка. Тогда укорочение $P^{(f)}$ всякого полинома*

$P \in L(J_G, F)$ лежит в идеале, порожденном укорочениями $g_i^{(f)}$ полиномов $g_i \in G$.

Доказательство. По определению каждый полином $P \in L(J_G, F)$ представим в виде $P = \sum \mu_i g_i z^{a_i - m_i}$, где $g_i = F(a_i)$ и $m_i = Gr(g_i)$. Обозначим через $\tilde{S}(P)$ множество точек a_i, для которых $\mu_i \neq 0$, и через $\tilde{B}(P)$ подмножество в $\tilde{S}(P)$, на котором функция f равна $\deg_f P$. Тогда при $a_i \in \tilde{B}(P)$ имеем $\deg_f g_i z^{a_i - m_i} = \deg_f P$. При этом полином

$$Q = \sum_{a_i \in \tilde{B}} \mu_i g_i^{(f)} z^{a_i - m_i}$$

не равен нулю: легко видеть, что при $a = Gr(P)$ моном z^a входит в полином Q с ненулевым коэффициентом. Поэтому $P^{(f)} = Q$. Утверждение 7 доказано. □

§3. Базис Грёбнера идеала

Здесь обсуждаются базисы Грёбнера, теорема Бухбергера и алгоритм Бухбергера.

3.1. Пространство $L(J_G, F)$ и идеал, содержащий множество G. Пусть $R = \mathbf{k}[z_1, \ldots, z_n]$ и $Gr : R \setminus \{0\} \to \mathbb{Z}^n_{\geqslant 0}$ — отображение Грёбнера для некоторого порядка Грёбнера на $\mathbb{Z}^n_{\geqslant 0}$. Очевидно следующее утверждение.

Утверждение 8. *Для всякого идеала $I \subset K$ множество $J(I) = Gr(I \setminus \{0\})$ является идеалом в полугруппе $\mathbb{Z}^n_{\geqslant 0}$.*

Пусть $G \subset I \setminus \{0\}$ — конечное множество, J_G — идеал в $\mathbb{Z}^n_{\geqslant 0}$, порожденный элементами $Gr(g)$ при $g \in G$, и $L(J_G, F)$ — пространство, соответствующее некоторому отображению $F : J_G \to G$. По определению пространство $L(J_G, F)$ содержится в идеале I.

Вопрос. Совпадает пространство $L(J_G, F)$ с идеалом I или идеал I строго больше, чем пространство $L(J_G, F)$?

Оказывается, что ответ на этот вопрос зависит лишь от ограничения отображения Грёбнера на множество G (т.е. не зависит от ограничения Gr на $I \setminus G$ и не зависит и от выбора отображения F).

Теорема 9. *Равенство $I = L(J_G, F)$ выполняется, если и только если носитель каждого полинома $P \in I$ пересекается с идеалом J_G в полугруппе $\mathbb{Z}^n_{\geqslant 0}$.*

Теорема 9 вытекает из следствия 6.

Определение 6. *Базис Грёбнера идеала* I относительно некоторого порядка Грёбнера — это такое конечное множество G ненулевых полиномов идеала I, что для образа $A = Gr(G)$ множества G при отображении Грёбнера выполнено равенство $\bigcup_{m\in A} O_m = Gr(I \setminus \{0\})$.

Согласно теореме 9 базис Грёбнера идеала является его базисом в обычном смысле этого слова.

Следствие 10. *Пусть* f *— монотонная функция относительно некоторого порядка Грёбнера и* $G = \{g_i\}$ *— базис Грёбнера идеала* I *относительно этого порядка. Тогда укорочение* $P^{(f)}$ *всякого полинома* $P \in I$ *лежит в идеале, порожденном укорочениями* $g_i^{(f)}$ *полиномов* $g_i \in G$.

Следствие 10 вытекает из теоремы 9 и утверждения 7.

3.2. Теорема Бухбергера. Содержит ли данное конечное множество G полиномов базис Грёбнера порожденного ими идеала I? Теорема Бухбергера отвечает на этот вопрос. Она является составной частью алгоритма Бухбергера (см. п. 3.3) и содержит его первый шаг (шаг $1_{(G,F)}$).

Для каждого полинома $g_i \in G$ обозначим через m_i его образ при отображении Грёбнера. Ниже мы считаем, что коэффициент при старшем мономе z^{m_i} полинома g_i равен единице — этого всегда можно добиться, умножая полином g_i на подходящую константу.

Шаг $1_{(G,F)}$. Рассмотрим идеал J_G в полугруппе $\mathbb{Z}^n_{\geqslant 0}$, равный $\bigcup O_{m_i}$, где $m_i = Gr(g_i)$ и $g_i \in G$. Для каждой пары полиномов $g_i, g_j \in G$ обозначим через $m_{i,j}$ вершину октанта $O_{m_i} \cap O_{m_j}$ (очевидно, что $m_{i,j} - m_i \in \mathbb{Z}^n_{\geqslant 0}$; $m_{i,j} - m_j \in \mathbb{Z}^n_{\geqslant 0}$) и определим полином $g_{i,j} = z^{m_{i,j}-m_i} g_i - z^{m_{i,j}-m_j} g_j$. Фиксируем любое отображение $F : J_G \to G$, для которого $a \in O_m$, где $m = Gr(F(a))$, и рассмотрим связанное с ним пространство $L(J_G, F)$.

Теорема 11 (Бухбергер). *Из множества* G *можно выбрать базис Грёбнера идеала* I, *если и только если все полиномы* $g_{i,j}$ *лежат в* $L(J_G, F)$.

Доказательство. Идеал, порожденный полиномами g_i, состоит из всевозможных линейных комбинаций полиномов вида $z^b g_i$. Достаточно проверить, что если все полиномы $g_{i,j}$ лежат в $L(J_G, F)$, то $L(J_G, F)$ содержит все полиномы вида $z^b g_i$. Допустим, что есть полиномы $z^b g_i \notin L(J_G, F)$. Выберем среди них полином, для которого точка $a = Gr(z^b g_i) = b + m_i$ — самая маленькая в смысле порядка Грёбнера. Пространство $L(J_G, F)$ содержит полином $z^{a-m_j} g_j$, где $g_j = F(a)$. Имеем $z^{a-m_i} g_i - z^{a-m_j} g_j = z^{a-m_{i,j}} g_{i,j}$. Так как $g_{i,j} \in L(J_G, F)$, то $g_{i,j} = \sum \lambda(p) z^{p-m_l} g_l$, где $l = F(p)$.

Откуда

$$z^b g_i = z^{a-m_j} g_j - \sum \lambda(p) z^{c(p)} g_l, \text{ где } c(p) = a - m_{i,j} + p - m_l.$$

Порядок любой точки p в носителе полинома $g_{i,j}$ строго меньше порядка точки $m_{i,j}$, поэтому $c(p) - m_l < a$. Следовательно, полиномы $z^{c(p)} g_l$ лежат в пространстве $L(J_G, F)$. Поэтому $z^b g_i \in L(J_G, F)$. Теорема 11 доказана. □

3.3. Алгоритм Бухбергера. Алгоритм решает следующую задачу.

Задача. По конечному множеству полиномов G, порождающему идеал I, построить конечное множество полиномов, содержащее базис Грёбнера этого идеала.

Теорема Бухбергера позволяет проверить, содержит или не содержит множество G базис Грёбнера идеала I. Если содержит, то задача решена. Если нет, то алгоритм Бухбергера позволяет последовательно строить возрастающую цепочку конечных подмножеств $G = G_0 \subset G_1 \subset \ldots$ идеала I, обладающих следующими свойствами:

1) найдется номер i такой, что $G_{i+1} = G_i$;

2) если $G_{i+1} = G_i$, то множество G_i содержит базис Грёбнера идеала I.

Тем самым алгоритм Бухбергера решает приведенную выше задачу.

В алгоритме Бухбергера для перехода от одного конечного множества полиномов к следующему используется двухшаговая процедура. Опишем ее (применяя ее, для определенности, к исходному множеству полиномов G).

Шаг $1_{(G,F)}$. Этот шаг описан в п. 3.2.

Шаг $2_{(G,F)}$. Вместе с пространством $L(J_G, F)$ рассмотрим пространство $L(J_G^\perp)$ и разложение $K = L(J_G, F) \oplus L(J_G^\perp)$. Для каждой пары полиномов $g_i, g_j \in G$ рассмотрим полином $g_{i,j}$ и найдем его разложение $g_{i,j} = g_{i,j}^1 + g_{i,j}^2$, где $g_{i,j}^1 \in L(J_G, F)$ и $g_{i,j}^2 \in L(J_G^\perp)$. Рассмотрим множество H, состоящее из всех ненулевых полиномов $g_{i,j}^2$. Положим $G_1 = G \cup H$.

Сделаем шаги $1_{(G,F)}$ и $2_{(G,F)}$. Если полученное в результате множество G_1 равно G, то G содержит базис Грёбнера и алгоритм окончен. Если же $G \neq G_1$, то переходим от множества G к большему множеству G_1. Двухшаговая процедура описана.

Если $G \neq G_1$, то идеал J_1, порожденный множеством $Gr(G_1)$ в полугруппе $\mathbb{Z}^n_{\geqslant 0}$, строго больше идеала J, так как носители ненулевых полиномов $g_{i,j}^2$ не пересекаются с J. Применим к G_1 ту же процедуру, что и к G, т.е. сделаем шаги $1_{(G_1,F_1)}$ и $2_{(G_1,F_1)}$ и образуем расширенное множество G_2. Если $G_2 = G_1$, то G_2 содержит базис Грёбнера и алгоритм окончен.

Если $G_1 \neq G_2$, то идеал J_2, порожденный множеством $Gr(G_2)$ в полугруппе $\mathbb{Z}^n_{\geqslant 0}$, строго больше идеала J_1. Применим к G_2 ту же процедуру, что и к G. И так далее. Так как всякая возрастающая последовательность идеалов в полугруппы $\mathbb{Z}^n_{\geqslant 0}$ обрывается, мы доказали следующую теорему.

Теорема 12. *Алгоритм Бухбергера останавливается за конечное число шагов и дает решение рассматриваемой задачи.*

Замечание 3. Если два разных порядка Грёбнера задают одинаковые отображения Грёбнера полиномов множества G, то шаги $1_{(G,F)}$ и $2_{(G,F)}$ для таких порядков не различаются. Это замечание играет ключевую роль в последующем (см. п. 5), когда мы будем оценивать степени полиномов, возникающих при применении алгоритма Бухбергера.

§4. Порядки на конечных подмножествах решетки $\mathbb{Z}^n$

С конечным множеством $A \subset \mathbb{Z}^n$ свяжем конечное множество $B \subset \mathbb{Z}^n$, состоящее из всех точек $b = a_i - a_j$, где $a_i, a_j \in A$ и $a_i \neq a_j$, в частности, $0 \notin B$, и если $b \in B$, то $-b \in B$). На решетке $\mathbb{Z}^n$ фиксируем любой порядок $\succ$, согласованный со структурой группы. Определим множество $B_+ \subset B$, состоящее из элементов, больших нуля (в частности, если $b \in B_+$, то $-b \notin B_+$).

Лемма 13. *Выпуклая оболочка $\Delta(B_+)$ множества B_+ не содержит точку 0.*

Доказательство. Если $0 \in \Delta(B_+)$, то 0 содержится строго внутри одного из невырожденных симплексов с вершинами $\{b_0, \ldots, b_k\} \subset B_+$, т.е. существуют $\lambda_i > 0$ такие, что $\sum \lambda_i = 1$ и $\sum \lambda_i b_i = 0$. Но точки $b_0, \ldots, b_k$ имеют целые координаты и аффинно независимы (т.е. минимальное аффинное пространство, содержащее эти точки, имеет размерность $k-1$). Следовательно, все числа λ_i рациональны и после умножения на подходящее натуральное число N становятся натуральными. Однако равенство $\sum (N\lambda_i) b_i = 0$ невозможно, так как $b_i \succ 0$ и соответственно $(N\lambda_i) b_i \succ 0$ и $\sum (N\lambda_i) b_i \succ 0$. Противоречие доказывает лемму. □

Обозначим через $\Delta^c(B_+)$ минимальный конус с вершиной в точке 0, содержащий многогранник $\Delta(B_+)$. Пусть $J = \{b_1, \ldots, b_{n-1}\}$ — любая последовательность точек из множества B_+, содержащая $(n-1)$ элемент. Обозначим через f_J линейную функцию на R^n, значение $f_J(x)$ которой в точке $x \in \mathbb{R}^n$ равно определителю $(n \times n)$-матрицы со столбцами $\{b_1, \ldots, b_{n-1}, x\}$.

Лемма 14. *Если конус $\Delta^c(B_+)$ имеет размерность n, то он задается некоторой системой линейных неравенств $f_{J_i} \geqslant 0$, в которой J_i — последовательность из элементов множества B_+ длины $n-1$.*

Доказательство. Каждая $(n-1)$-мерная грань Γ_i конуса $\Delta^c(B_+)$ содержит $(n-1)$ линейно независимый вектор из множества B_+. Упорядочим эти векторы так, чтобы для полученной последовательности J_i функция f_{J_i} была неотрицательна на конусе $\Delta^c(B_+)$. Для каждой грани Γ_i напишем неравенство $f_{J_i} \geqslant 0$. Полученная система неравенств задает многогранный конус $\Delta^c(B_+)$. □

Функция $f\colon \mathbb{R}^n \to \mathbb{R}$ *монотонна* (*строго монотонна*) на $A \subset \mathbb{Z}^n$ относительно порядка $\succ$, если из $a, b \in A$ и $a \succ b$ вытекает, что $f(a) \geqslant f(b)$ (что $f(a) > f(b)$). Строго монотонная на A функция задает на A тот же порядок, что и $\succ$, т.е. при $a, b \in A$ неравенства $f(a) > f(b)$ и $a \succ b$ эквивалентны.

Пример 1. Функции f_{J_i} из леммы 14 неотрицательны на B_+ и, следовательно, монотонны на множестве A.

Пусть $\mathbb{R}^n$ — пространство с координатами $x_1, \ldots, x_n$ и со стандартной евклидовой метрикой.

Следствие 15. *Если диаметр множества A не превосходит ρ, то конус $\Delta^c(B_+)$ задается некоторой системой неравенств $a_1^i x_1 + \cdots + a_n^i x_n \geqslant 0$, в которых $a_j^i \in \mathbb{Z}$ и $|a_i^j| \leqslant \rho^{n-1}$.*

Доказательство. Если $J_i = \{b_1^i, \ldots, b_{n-1}^i\}$, то коэффициент a_j^i функции f_{J_i} равен определителю матрицы со столбцами $b_1^i, \ldots, b_{n-1}^i, e_j$, где e_j — j-й базисный вектор в $\mathbb{R}^n$. Этот определитель — целое число, модуль которого не превосходит $(n-1)$-мерного объема V_{n-1} параллелепипеда, натянутого на векторы $b_1^i, \ldots, b_{n-1}^i$. По условию длины векторов из B не превосходят ρ, поэтому $V_{n-1} \leqslant \rho^{n-1}$. □

Теорема 16. *Пусть A содержит точку 0 и все базисные векторы e_i, а порядок на A таков, что $e_i \succ 0$ для $i = 1, \ldots, n$. Если при этом диаметр множества A не превосходит ρ, то существует строго монотонная на A линейная функция с целыми коэффициентами, не превосходящими ρ^{n-1}.*

Доказательство. Кэффициенты каждой функции f_{J_i} из следствия 15 — целые числа, не превосходящие по модулю ρ^{n-1}. Так как $\{e_i\} \in B_+$, коэффициенты всех функций f_{J_i} неотрицательны. Нам достаточно показать, что одна из граней Γ_j конуса $\Delta^c(B_+)$ не содержит ни одного базисного вектора: все коэффициенты соответствующей этой грани функции f_{J_j} положительны. Существование такой грани доказано ниже в лемме 18. □

Перенумеровав векторы $\{e_j\}$, можно считать, что $e_1 \prec \cdots \prec e_n$. Для каждой $(n-1)$-мерной грани Γ_i конуса $\Delta^c(B_+)$ выполняется следующая лемма.

Лемма 17. *Если $e_k \in \Gamma_i$ и $m < k$, то $e_m \in \Gamma_i$.*

Доказательство. Функция f_{J_i} равна нулю на Γ_i, монотонна на A и положительна на $\Delta^c(B_+) \setminus \Gamma_i$. Поэтому $f_{J_i}(e_m) \leqslant f_{J_i}(e_k) = 0$. Но $e_m \in B_+$, поэтому $f_{J_i}(e_m) \geqslant 0$. Откуда $f_{J_i}(e_m) = 0$ и, следовательно, $e_m \in \Gamma_i$. □

Лемма 18. *В конусе $\Delta^c(B_+)$ есть $(n-1)$-мерная грань Γ_j, не содержащая ни одного базисного вектора.*

Доказательство. Множество $\mathcal{G}$ всех граней конуса $\Delta^c(B_+)$ (включая сам конус и его вершину 0) частично упорядочено по включению. Определим отображение $\Psi : \{e_i\} \to \mathcal{G}$, сопоставляющее базисному вектору e_m наименьшую грань $\Psi(e_m)$, содержащую вектор e_m. Каждая собственная грань конуса $\Delta^c(B_+)$ является пересечением его $(n-1)$-мерных граней. По лемме 17, если $e_m \prec e_k$, то $\Psi(e_m) \subset \Psi(e_k)$. Поэтому грань $\Psi(e_1)$ содержится в каждой грани $\Psi(e_i)$. Грань $\Psi(e_1)$ не является вершиной. Если $\Psi(e_1) = \Delta^c(B_+)$, то доказывать нечего: в этом случае любая грань не содержит базисных векторов. В противном случае в качестве Γ_j можно взять любую $(n-1)$-мерную грань, не содержащую грань $\Psi(e_1)$. Действительно, если $e_m \in \Gamma_j$, то $\Psi(e_m) \subset \Gamma_j$ и $\Psi(e_1) \subset \Psi(e_m) \subset \Gamma_j$. □

§5. Оценки степеней полиномов

Скажем, что $\alpha\colon \mathbb{R}^n \to \mathbb{R}$ — *допустимая функция*, если α — линейная функция, $\alpha(x_1, \ldots, x_n) = \alpha_1 x_1 + \cdots + \alpha_n x_n$ с положительными коэффициентами $\alpha_1, \ldots, \alpha_n$, линейно-независимыми над $\mathbb{Q}$. Скажем, что x меньше, чем y в смысле α-порядка, если $\alpha(x) < \alpha(y)$. Легко проверить следующее утверждение.

Утверждение 19. *Если $\alpha\colon \mathbb{R}^n \to \mathbb{R}$ — допустимая функция, то на решетке $\mathbb{Z}^n$ α-порядок совместим со структурой группы. На полугруппе $\mathbb{Z}^n_{\geqslant 0}$ α-порядок является порядком Грёбнера.*

Доказательство. В силу линейности функции α, если $\alpha(x) < \alpha(y)$, то $\alpha(x+z) < \alpha(y+z)$. В силу независимости коэффициентов α_i над $\mathbb{Q}$ для векторов $x, y \in \mathbb{Z}^n$ равенство $\alpha(x) = \alpha(y)$ возможно, только если $x = y$. Наконец, α-порядок задает полное упорядочивание полугруппы $\mathbb{Z}^n_{\geqslant 0}$ с минимальным элементом 0 в силу положительности коэффициентов α_i (для данной точки $x \in \mathbb{Z}^n_{\geqslant 0}$ есть лишь конечное число точек $y \in \mathbb{Z}^n_{\geqslant 0}$, для которых $x \succ y$). □

Следующее утверждение 20 нам понадобится ниже в §7.

Утверждение 20. *Для ненулевой линейной функции f, неотрицательной на $\mathbb{Z}^n_{\geqslant 0}$, существует порядок Грёбнера на $\mathbb{Z}^n_{\geqslant 0}$, относительно которого функция f монотонна.*

Доказательство. Приведем пример такого порядка. Фиксируем любую допустимую функцию α. Определим порядок так: если $f(x) > f(y)$, то по определению $x \succ y$; если $f(x) = f(y)$, то по определению $x \succ y$, если $\alpha(x) > \alpha(y)$. □

5.1. Степени полиномов в алгоритме Бухбергера. Пусть G — конечное множество полиномов в $\mathbf{k}[z_1, \ldots, z_n]$, степень каждого из которых $\leqslant N$. Зададим любой порядок Грёбнера на $\mathbb{Z}^n$.

Теорема 21. *Существует допустимая функция α такая, что*

1) *отображение Грёбнера для заданного порядка Грёбнера и для α-порядка на полиномах множества G совпадают*;

2) *коэффициенты α_i функции α удовлетворяют неравенствам $1 \leqslant \alpha_i \leqslant N^{n-1} n^{\frac{n-1}{2}}$.*

Доказательство. Пусть $A \subset \mathbb{Z}^n_{\geqslant 0}$ — множество точек $m = (m_1, \ldots, m_n)$, определенное неравенствами $m_i \geqslant 0$, $|m| = m_1 + \cdots + m_n \leqslant N$. Множество A содержит точку 0, все точки $e_1, \ldots, e_n$ и носители всех полиномов степени $\leqslant N$. Множество A имеет диаметр $\rho = Nn^{1/2}$. По теореме 16 существует линейная функция $l(x) = a_1 x_1 + \cdots + a_n x_n$ с коэффициентами a_i такими, что $1 \leqslant a_i \leqslant N^{n-1} n^{(n-1)/2}$, задающая тот же порядок на множестве A, что и данный порядок Грёбнера. Для построения искомой и функции α достаточно немного возмутить коэффициенты функции l так, чтобы возмущенная функция задавала тот же порядок на множестве A и чтобы ее коэффициенты α_i были независимы над $\mathbb{Q}$ и удовлетворяли тем же неравенствам $1 \leqslant \alpha_i \leqslant \rho^{n-1} = N^{n-1} n^{(n-1)/2}$. Теорема 21 доказана. □

Пусть G — некоторое множество ненулевых полиномов, порождающих идеал I. Пусть степени всех полиномов из G не превосходят некоторого натурального числа N.

Теорема 22. *Вне зависимости от порядка Грёбнера полиномы $g^2_{i,j}$, возникающие в результате применения двухшаговой процедуры Бухбергера к полиномам из множества G, имеют степень, не большую, чем $C(N, n) = 2N^n n^{\frac{n-1}{2}}$.*

Доказательство. Для разных порядков Грёбнера, задающих одинаковые отображения Грёбнера на множестве G, два шага процедуры Бухбергера совпадают между собой. Воспользуемся α-порядком Грёбнера,

где α — функция из теоремы 21. Так как степень полиномов g_i и g_j не превосходит N, то степень полинома $g_{i,j}$ не превосходит $2N$. Поэтому $\alpha(Gr(g_{i,j})) \leqslant N^{n-1}n^{\frac{n-1}{2}}2N$ (так как коэффициенты α_i не превосходят числа $N^{n-1}n^{n-1/2}$), т.е. $\alpha(Gr(g_{i,j})) \leqslant C(N,n)$. Далее $Gr(g_{i,j}^2) \prec Gr(g_{i,j})$, откуда $\alpha(Gr(g_{i,j}^2)) \leqslant C(N,n)$. Так как коэффициенты функции α не меньше единицы, то степень полинома $g_{i,j}^2$ не превосходит числа $C(N,n)$. □

5.2. Степени полиномов в базисе Грёбнера. Справедлива следующая теорема.

Теорема 23. *Пусть идеал I в кольце $\mathbf{k}[z_1,\dots,z_n]$ порожден полиномами степени $\leqslant N$. Тогда для любого порядка Грёбнера существует базис Грёбнера идеала I, в котором все полиномы имеют степень $\leqslant F_1(N)$. Число $F_1(N)$ можно явно вычислить по степени N и размерности n.*

Доказательство. Алгоритм Бухбергера позволяет по заданному множеству образующих G в идеале I и по заданному порядку Грёбнера построить цепочку подмножеств $G \subset G_2 \subset \cdots \subset G_k \subset \dots$, для которой цепочка идеалов $J \subset J_1 \subset J_2 \subset \cdots \subset J_k \subset \dots$ в $\mathbb{Z}^n_{\geqslant 0}$, порожденных образами множеств G_i при отображении Грёбнера, строго возрастает. Определим функцию F_1 натурального аргумента следующими соотношениями: $F_1(1) = N$ при $i > 1, F_1(i) = C(F_1(i),n)$, где C — функция, фигурирующая в теореме 22. По теореме 22 идеал J_k порожден элементами степени не выше, чем $F_1(k)$. Теперь по теореме Зайденберга для полугруппы $\mathbb{Z}^n_{\geqslant 0}$ цепочка идеалов оборвется на некотором идеале J_M. Множество G_M содержит полиномы степени не выше, чем число $F_1(N)$. Из множества G_M можно выбрать базис Грёбнера идеала J. □

§6. Универсальный базис Грёбнера

В дальнейшем материал этого параграфа не используется. Мы приводим его, чтобы продемонстрировать доказанные результаты.

Скажем, что конечное множество полиномов G из идеала I содержит *универсальный базис Грёбнера*, если для любого порядка Грёбнера из множества G можно выбрать подмножество, являющееся базисом Грёбнера относительно этого порядка. Давно и хорошо известно (см. [14, 15, 16]), что у каждого идеала существует универсальный базис Грёбнера. Простое доказательство можно найти в [17]. Ниже мы не только доказываем существование такого базиса, но и приводим его довольно явную конструкцию.

Теорема 24. *Пусть идеал I в кольце $\mathbf{k}[z_1, \dots, z_n]$ порожден полиномами степени $\leqslant N$. Тогда существует универсальный базис Грёбнера идеала I, в котором все полиномы имеют степень не выше, чем $F_1(N)$.*

Доказательство. Рассмотрим конечное подмножество $T(N)$ полугруппы $\mathbb{Z}^n_{\geqslant 0}$, определенное условием: $m \in T(N)$, если и только если $|m| \leqslant F_1(N)$. Построим конечное подмножество G идеала I следующим образом. Для всякого выпуклого многогранника Δ, все вершины которого лежат в $T(N)$, выберем в идеале I один полином P, многогранник Ньютона которого равен Δ. Если в идеале I такого полинома нет, то не будем принимать во внимание многогранник Δ. Определим G как множество всех выбранных полиномов. По построению множество G обладает следующим свойством. Для всякого порядка Грёбнера и всякого полинома $Q \in I$ степени $\leqslant F_1(N)$ найдется полином $P \in G$, имеющий тот же образ при отображении Грёбнера, что и полином Q. Для завершения доказательства осталось воспользоваться теоремой 23. □

Теорема 24 допускает уточнение. Для формулировки более точной теоремы 25 нам понадобятся дополнительные определения.

С точкой $m = (m_1, \dots, m_n) \in \mathbb{Z}^n_{\geqslant 0}$ свяжем параллелепипед $\prod(m)$, определенный соотношениями

$$x = (x_1, \dots, x_n) \in \prod(m) \;\Leftrightarrow\; 0 \leqslant x_1 \leqslant m_1, \dots, 0 \leqslant x_n \leqslant m_n.$$

Скажем, что целочисленный многогранник является $\mathbb{Z}^n_{\geqslant 0}$-выпуклым, если все вершины многогранника лежат в $\mathbb{Z}^n_{\geqslant 0}$ и многогранник с каждой вершиной m содержит параллелепипед $\prod(m)$. С полиномом P свяжем минимальный $\mathbb{Z}^n_{\geqslant 0}$-выпуклый многогранник $\Delta_{\geqslant 0}(P)$, содержащий носитель полинома P. Построим конечное подмножество $\tilde{G}$ идеала I следующим образом. Для всякого $\mathbb{Z}^n_{\geqslant 0}$-выпуклого многогранника Δ, все вершины которого лежат в $T(N)$, выберем в идеале I один полином P, для которого $\Delta_{\geqslant 0}(P) = \Delta$. Если в идеале I такого полинома нет, то не будем принимать во внимание этот $\mathbb{Z}^n_{\geqslant 0}$-выпуклый многогранник. Определим $\tilde{G}$ как множество всех выбранных полиномов.

Теорема 25. *Описанное выше множество полиномов $\tilde{G}$ содержит универсальный базис Грёбнера идеала I.*

Доказательство. Достаточно почти дословно повторить аргументы, доказывающие теорему 24. Дело в том, что если для полиномов P и Q выполнено равенство $\Delta_{\geqslant 0}(P) = \Delta_{\geqslant 0}(Q)$, то для всякого порядка Грёбнера элементы $Gr(P)$ и $Gr(Q)$ совпадают. □

§7. Основная теорема

Для целочисленного многогранника $\Delta \subset \mathbb{R}^n$ определим *множество полиномов Лорана* $M(\Delta)$: полином Лорана P принадлежит множеству $M(\Delta)$, если его многогранник Ньютона $\Delta(P)$ отличается от многогранника Δ сдвигом на целочисленный вектор $\Delta(P) = \Delta + m$. Пусть I — идеал в кольце полиномов Лорана от n переменных и $U \subset \mathbb{R}^n$ — ограниченное множество.

Определение 7. Конечное множество $G \subset I$ полиномов Лорана назовем U-приближением идеала I, если для каждого целочисленного многогранника $\Delta \subset U$ либо $M(\Delta) \bigcap I = \emptyset$, либо $M(\Delta) \bigcap G \neq \emptyset$.

Для всякой ограниченной области U существует некоторое U-приближение G идеала I. Действительно, существует лишь конечное число различных целочисленных многогранников в области U. Достаточно для каждого такого многогранника Δ включить в множество G один из полиномов Лорана $P \in I$ с многогранником $\Delta(P) = \Delta$, если такие полиномы Лорана присутствуют в идеале.

Основная теорема. *Пусть идеал I порожден полиномами Лорана, многогранники Ньютона которых лежат в кубе $-N \leqslant m_i \leqslant N$, при $i = 1, \ldots, n$. Пусть G — U-приближение идеала I, где U — область, определенная неравенствами $|m_1| + \cdots + |m_n| \leqslant F_1(2Nn)$. Тогда полиномы из G задают систему тропических образующих идеала I.*

Доказательство. Пусть $f(m_1, \ldots, m_n) = \alpha_1 m_1 + \cdots + \alpha_n m_n$. Сделаем автоморфизм тора $(\mathbb{C}^*)^n$, переводящий точку $z_1, \ldots, z_n$ в точку $y_1, \ldots, y_n$, где $y_i = z_i$ при $\alpha_i \geqslant 0$ и $y_i = z_i^{-1}$ при $\alpha_i < 0$. При таком преобразовании куб и область U в пространстве степеней мономов перейдут в себя, а линейная функция f перейдет в функцию f^* с неотрицательными коэффициентами. Согласно утверждению 20 такая функция f^* является монотонной функцией относительно некоторого порядка Грёбнера в кольце полиномов от $y_1, \ldots, y_n$. Полиномы Лорана после умножения на подходящие мономы можно сделать полиномами. Полиномы Лорана из множества образующих идеала I можно превратить в полиномы степени $\leqslant 2Nn$. Для завершения доказательства осталось воспользоваться теоремой 23 и следствием 10. □

Список литературы

[1] De Concini C., Procesi C., *Complete symmetric varieties.* II, *Intersection theory*, Algebraic Groups and Related Topics, (Kyoto/Nagoya,

1983), Adv. Stud. Pure Math., vol. 6, North-Holland, Amsterdam, 1985, pp. 481–513.

[2] De Concini C., *Equivariant embeddings of homogeneous spaces*, Proc. Intern. Congress of Mathematicians, vol. 1, 2 (Berkeley, Calif., 1986), Amer. Math. Soc., Providence, RI, 1987, pp. 369–377.

[3] Fulton W., Sturmfels B., *Intersection theory on toric varieties*, Topology **36** (1997), no. 2, 335–353.

[4] Казарновский Б. Я., *Укорочения систем уравнений, идеалов и многообразий*, Изв. РАН. Сер. мат. **28** (1999), №2, 119–132.

[5] Seidenberg A., *On the length of a Hilbert ascending chain*, Proc. Amer. Math. Soc. **29** (1971), 443–450.

[6] Seidenberg A., *Constructive proof of Hilbert's theorem on ascending chains*, Trans. Amer. Math. Soc. **174** (1972), 305–312.

[7] Moreno-Socias G., *Length of polynomial ascending chains and primitive recursiveness*, Math. Scand. **71** (1992), no. 2, 181–205.

[8] Казарновский Б. Я., *с-вееры и многогранники Ньютона алгебраических многообразий*, Изв. РАН. Сер. мат. **67** (2003), №3, 439–460.

[9] Mikhalkin G., *Counting curves via lattice paths in polygons*, C. R. Math. Acad. Sci. Paris **336** (2003), no. 8, 629–634.

[10] Shustin E., *A tropical approach to enumerative geometry*, Алгебра и анализ **17** (2005), №2, 170–214.

[11] Itenberg I., Mikhalkin G., Shustin E., *Tropical algebraic geometry*, 2nd ed., Birkhauser, Basel, 2009.

[12] Казарновский Б., Хованский А., *Алгебра и тропическая геометрия*, 2011–2013, с. 1–42 (готовится к публикации).

[13] Чулков С., Хованский А., *Геометрия полугруппы $\mathbb{Z}^n_{\geqslant 0}$. Приложения к алгебре, комбинаторике и дифференциальным уравнениям*, МЦНМО, М., 2006.

[14] Mora F., Robbiano L., *The Gröbner fan of an ideal. Computational aspects of commutative algebra*, J. Symbolic Comput. **6** (1988), no. 2-3, 183–208.

[15] Weispfenning V., *Constructing universal Gröbner bases*, Lecture Notes in Comput. Sci., vol. 356, Springer, Berlin, 1989, pp. 408–417.

[16] Schwartz N., *Stability of Gröbner bases*, J. Pure Appl. Algebra **53** (1988), no. 1-2, 171–186.

[17] Казарновский Б., Хованский А., *Универсальный базис Грёбнера*, Proc. Intern. Conf. on Polynomial Computer Algebra, St. Peterburg, 2011, pp. 65–69.

[18] Macaulay F. S., *The algebraic theory of modular systems*, Cambridge Tracts in Math. and Math. Phys., vol. 19, Cambridge Univ. Press, Cambridge, 1916.
[19] Sauer Th., *Gröbner bases, H-bases and interpolations*, Trans. Amer. Math. Soc. **353** (2001), no. 6, 2293–2308. (electronic)

Поступило 17 октября 2013 г.

Институт проблем передачи информации
им. А. А. Харкевича РАН
127994, Москва
Бол. Каретный пер., 19, стр. 1
Россия
E-mail: kazbori@gmail.com

Институт системного анализа РАН
117312, Москва
пр. 60-летия Октября, 9
Независимый московский университет
119002, Москва
Бол. Власьевский пер., 11
Россия

Университет Торонто
Канада
E-mail: askold@math.toronto.edu