Выпуклые тела и выпуклые многогранники

Лекция 9

1 Базисы Гребнера

Здесь мы изложим конструкцию базисов Гребнера в немного большей общности, чем это необходимо для дальнейшего.

Определение. Пусть G — аддитивная абелева полугруппа. Полугруппа G называется *упорядоченной*, если на ней введено такое отношение частичного порядка $\leqslant$, что

$$(\forall a, b, c \in G) \quad a \leqslant b \quad \Longrightarrow \quad a + c \leqslant b + c.$$

Упорядоченная полугруппа называется *линейно упорядоченной*, если отношение порядка $\leqslant$ линейно.

Предложение 1.1 *Полугруппу $\mathbb{Z}^n_{\geqslant 0}$ можно линейно упорядочить.*

Доказательство.
Один способ — ввести лексикографический порядок. Второй способ — выбрать некоторый вектор w с положительными координатами, линейно независимыми над $\mathbb{Q}$, и положить $a \leqslant b$ в $\mathbb{Z}^n_{\geqslant 0}$, если $(a, w) \leqslant (b, w)$. $\square$

Определение. *Идеалом* упорядоченной полугруппы G называется такое подмножество $I \subseteq G$, что

$$a \in I, b \in G \quad \Longrightarrow \quad a + b \in I.$$

Подмножество $J \subseteq G$ называется *коидеалом*, если $G - J$ — идеал.

Определение. Полугруппа G называется *нетеровой*, если всякий идеал $I \subseteq G$ конечно порожден, то есть найдется конечное число элементов $a_1, \ldots, a_n \in I$, таких что

$$I = (a_1 + G) \cup \cdots \cup (a_n + G).$$

Элементы $a_1, \ldots, a_n$ называются *образующими* идеала I.

Теорема 1.2 *Полугруппа $\mathbb{Z}^n_{\geqslant 0}$ является нетеровой (каждый идеал в группе $\mathbb{Z}^n_{\geqslant 0}$ является объединением конечного числа октантов).*

Доказательство.
Будем вести индукцию по размерности. Пусть I — некоторый идеал в $\mathbb{Z}^n_{\geqslant 0}$. Спроектируем его на координатную гиперплоскость $\mathbb{Z}^{n-1}$ (эту гиперплоскость мы будем себе представлять как горизонтальную). Получится идеал в полугруппе $\mathbb{Z}^{n-1}_{\geqslant 0}$. По предположению индукции, этот идеал конечно порожден. Обозначим через $b_1, \ldots, b_k$ его образующие. Они получаются проекцией из некоторых точек $a_1, \ldots, a_k \in I$. Пусть точка c — максимум высот точек $a_1, \ldots, a_k$. Тогда все элементы идеала, высота которых $\geqslant c$, лежат в объединении октантов, порожденных точками a_i. Остальные элементы идеала лежат в объединении конечного числа горизонтальных слоев. Осталось для каждого из этих слоев воспользоваться предположением индукции. $\square$

Определение. Пусть K — некоторое поле. Со всякой полугруппой G связана *полугрупповая алгебра* $K[G]$, состоящая из всех формальных линейных комбинаций вида

$$\sum_{g \in G} \lambda_g g.$$

Таким образом, сама полугруппа G является базисом векторного пространства $K[G]$. Полугрупповая операция, определенная в G (теперь эту полугрупповую операцию удобней представлять себе как умножение), распространяется по линейности до умножения в алгебре $K[G]$.

Пример. Кольцо многочленов $K[x_1, \ldots, x_n]$ является полугрупповой алгеброй полугруппы $\mathbb{Z}^n_{\geqslant 0}$.

Определение. Пусть G — линейно упорядоченная полугруппа. Тогда определено *отображение Гребнера* $\mathrm{Grb} : (K[G] - 0) \to G$, сопоставляющее каждому элементу $\alpha \in K[G] - 0$ максимальный элемент группы G, входящий в α с ненулевым коэффициентом. Нетрудно проверить, что для всякого $g \in G$ имеет место равенство $\mathrm{Grb}(g\alpha) = g + \mathrm{Grb}(\alpha)$.

Каждому идеалу I в алгебре $K[G]$ соответствуют следующие объекты:

- *Гребнеровский G-идеал* $\mathrm{Grb}(I - 0)$ (это идеал в полугруппе G),
- *Гребнеровский G-коидеал* — дополнение до гребнеровского идеала (это коидеал в полугруппе G),
- *Гребнеровский коидеал* в алгебре $K[G]$ — это векторное подпространство в $K[G]$, порожденное гребнеровским G-коидеалом.

Пусть I — некоторый идеал в алгебре $K[G]$.

Теорема 1.3 *Алгебра $K[G]$ как векторное пространство над K является прямой суммой идеала I и его гребнеровского коидеала.*

Доказательство.
Пусть L — гребнеровский коидеал идеала I. По определению, $I \cap L = \{0\}$. Рассмотрим теперь произвольный элемент $a \in K[G]$. Мы хотим доказать, что $a \in I + L$. Если $a \in L$, то все доказано. Иначе в разложение $a = \sum_{g \in G} \lambda_g g$ входят с ненулевыми коэффициентами некоторые элементы гребреровского G-идеала $\mathrm{Grb}(I - 0)$. Пусть g — максимальный такой элемент. Он является образом при отображении Гребнера некоторого элемента $b \in I$. Вычитая b из a с подходящим коэффициентом, можно уменьшить максимальный элемент из $\mathrm{Grb}(I - 0)$, входящий в разложение a. Повторяя описанный процесс, мы избавимся в разложении элемента a вообще от всех элементов из $\mathrm{Grb}(I-0)$, то есть получим некоторый элемент из L. $\square$

Следствие 1.4 *Пусть I_1 и I_2 — такие идеалы алгебры $K[G]$, что $I_1 \subseteq I_2$ и гребнеровские G-идеалы идеалов I_1 и I_2 совпадают. Тогда $I_1 = I_2$.*

Следствие 1.5 *Элементы идеала $I \subseteq K[G]$ порождают этот идеал тогда и только тогда, когда их образы при отображении Гребнера порождают гребнеровский G-идеал идеала I.*

Отсюда и из нетеровости полугруппы $\mathbb{Z}^n_{\geqslant 0}$ вытекает теорема Гильберта о базисе. На самом деле, конструкция Гребнера позволяет не только доказать теорему Гильберта о базисе, но и дает эффективный способ нахождения базиса для данного идеала I в кольце многочленов. Базисы, полученные при помощи конструкции Гребнера, называются *базисами Гребнера.* Базисы Гребнера являются основным инструментом вычислительной коммутативной алгебры. Кроме того, они полезны и в других разделах математики (например, в комбинаторике и в теории уравнений с частными производными).

2 Функции Гильберта и ряды Пуанкаре

Функция Гильберта осуществляет количественное описание градуированных объектов (например, градуированных алгебр, градуированных полугрупп и т.д.).

Определение. Пусть $V = \bigoplus_{k=0}^{\infty} V_k$ — градуированное векторное пространство, такое что все компоненты V_k конечномерны. Функция $H(k) = \dim V_k$ называется *функцией Гильберта* пространства V.

Аналогичное определение можно дать для градуированных множеств. Пусть $X = \bigoplus_{k=0}^{\infty} X_k$ — градуированное множество, такое что все компоненты X_k конечны. Тогда определена *функция Гильберта* $H(k) = \# X_k$ множества X.

Пример. Полугруппа $G = \mathbb{Z}^n_{\geqslant 0}$ имеет естественную градуировку $G = \bigoplus G_k$, где G_k состоит из всех элементов $(x_1, \ldots, x_n)$, таких что $\sum x_i = k$. Функция Гильберта полугруппы G имеет вид

$$H(k) = \binom{n+k-1}{n-1} = \binom{n+k-1}{k}.$$

Заметим, что полугрупповая алгебра $K[G]$ градуированной полугруппы G наследует градуировку из G. Функция Гильберта алгебры $K[G]$ совпадает с функцией Гильберта полугруппы G.

Определение. Идеал I градуированной алгебры называется *однородным*, если из того что $x \in I$ следует, что все однородные компоненты элемента x также принадлежат I. Нетрудно проверить, что факторалгебра градуированной алгебры по однородному идеалу наследует градуировку.

Пусть G — градуированная полугруппа. Из теоремы 1.3 вытекает следующее

Предложение 2.1 *Функция Гильберта факторалгебры $K[G]/I$ полугрупповой алгебры $K[G]$ по однородному идеалу I совпадает с функцией гильберта G-коидеала идеала I.*

Заметим, что всякая коммутативная градуированная алгебра, порожденная элементами первой степени, является факторалгеброй алгебры многочленов $K[\mathbb{Z}^n_{\geqslant 0}]$ по некоторому однородному идеалу. Следовательно, изучение функций Гильберта таких алгебр сводится к изучению функций Гильберта гораздо более простых объектов: коидеалов группы $\mathbb{Z}^n_{\geqslant 0}$.

Определение. *Рядом Пуанкаре* называется производящий степенной ряд функции Гильберта:

$$P(t) = \sum_{k=0}^{\infty} H(k) t^k.$$

Пример. Нетрудно проверить, что ряд Пуанкаре алгебры многочленов от n переменных имеет вид $1/(1-t)^n$.

Теорема 2.2 *Пусть A — коммутативная градуированная алгебра, порожденная элементами первой степени. Тогда ряд Пуанкаре алгебры A равен*

$$P(t) = \frac{g(t)}{(1-t)^s},$$

где $g(t)$ — некоторый многочлен с целыми неотрицательными коэффициентами, а $s \leqslant \dim A_1$.

Доказательство.
Действительно, пусть алгебра A является фактором кольца многочленов от $n = \dim A_1$ переменных по некоторому однородному идеалу I. Тогда, в силу предложения 2.1, функция Гильберта алгебры A совпадает с функцией Гильберта $\mathbb{Z}^n_{\geqslant 0}$-коидеала M идеала I. Нетрудно проверить, что коидеал M можно представить в виде объединения конечного числа сдвинутых координатных октантов (разных размерностей — в том числе и нульмерных). Функция Гильберта коидеала M складывается из функций Гильберта координатных октантов, составляющих M.

Функция Гильберта координатного октанта $\mathbb{Z}^m_{\geqslant 0}$ имеет вид $H(k) = \binom{m+k-1}{m-1}$. Следовательно, соответствующий ряд Пуанкаре равен

$$P(t) = \sum_{k=0}^{\infty} \binom{m+k-1}{m-1} t^k = \frac{1}{(1-t)^m}.$$

Сдвиг координатного октанта отвечает умножению на t^l. Таким образом, функция Гильберта коидеала M является суммой слагаемых вида $t^l/(1-t)^m$. Приведя эту сумму к общему знаменателю, получим утверждение теоремы. □

Пример. Пусть Δ — простой d-мерный многогранник. Рассмотрим кольцо многочленов $\mathbb{R}[x_1, \ldots, x_n]$ от $n = f_{d-1}(\Delta)$ переменных $x_1, \ldots, x_n$, находящихся во взаимно однозначном соответствии с гиперплоскими гранями $\Gamma_1, \ldots, \Gamma_n$ многогранника Δ. Обозначим через I однородный идеал, порожденный мономами $x_{i_1} \cdots x_{i_k}$, такими что $\Gamma_{i_1} \cap \cdots \cap \Gamma_{i_k} = \varnothing$. *Кольцо граней* (или *кольцо Стенли–Рейзнера*) простого многогранника Δ определяется как факторалгебра алгебры многочленов по идеалу I.

Предложение 2.3 *Ряд Пуанкаре кольца граней простого многогранника Δ имеет вид*

$$P(t) = \frac{H_\Delta(t)}{(1-t)^d},$$

где $H_\Delta(t)$ — H-полином многогранника Δ.

Доказательство.
Пусть F — k-мерная грань многогранника Δ. Грань F представляется в виде пересечения гиперплоских граней: $F = \Gamma_{i_1} \cap \cdots \cap \Gamma_{i_{d-k}}$. Обозначим через V_F векторное пространство, порожденное всеми мономами вида $x_{i_1}^{\alpha_1} \cdots x_{i_{d-k}}^{\alpha_{d-k}}$, такими что все $\alpha_i > 0$. Тогда кольцо граней многогранника Δ распадается (как векторное пространство) в прямую сумму $\bigoplus V_F$ по всем граням F многогранника Δ. В частности, ряд Пуанкаре кольца граней имеет вид $P(t) = \sum P_F(t)$, где $P_F(t)$ — ряд Пуанкаре пространства V_F.

Пусть F — грань размерности k. Векторное пространство V_F изоморфно (как градуированное пространство) пространству многочленов от $d-k$ переменных, сдвинутому на $d-k$. Следовательно, $P_F(t) = t^{d-k}/(1-t)^{d-k}$ и

$$P(t) = \sum_{k=0}^{d} \frac{f_k t^{d-k}}{(1-t)^{d-k}} = \frac{\sum_{k=0}^{d} f_k t^{d-k}(1-t)^k}{(1-t)^d}.$$

Числитель этого выражения равен

$$\sum_{k=0}^{d} f_k t^{d-k}(1-t)^k = t^d \sum_{k=0}^{d} f_k \left(\frac{1}{t} - 1\right)^k = t^d H(1/t).$$

Однако, в силу соотношений Дена–Соммервиля, $t^d H(1/t) = H(t)$. Предложение доказано. $\square$

3 Комбинаторная теорема Маколея

Теорема 2.2 описывает поведение функции Гильберта на бесконечности. Но она не накладывает никаких ограничений на первые несколько членов ряда Пуанкаре. Требуется, чтобы ряд Пуанкаре представлял собой рациональную функцию со знаменателем $(1-t)^s$. Но если к такому ряду прибавить произвольный многочлен, это свойство не нарушится. В частности, для ряда Пуанкаре конечномерной алгебры (который является многочленом), теорема 2.2 не дает ничего нового. Однако не произвольный многочлен с целыми неотрицательными коэффициентами может быть рядом Пуанкаре конечномерной градуированной алгебры, порожденной элементами первой степени. Этот раздел посвящен обсуждению следующей теоремы, описывающей всевозможные функции Гильберта (или, что эквивалентно, ряды Пуанкаре) таких алгебр:

Теорема 3.1 (Маколей) *Пусть A — конечномерная коммутативная градуированная алгебра, порожденная элементами первой степени. Функция Гильберта алгебры A удовлетворяет неравенствам $H(k+1) \leqslant \partial_k(H(k))$ при $k \geqslant 1$. Обратно, если конечная последовательность целых неотрицательных чисел $H(k)$ удовлетворяет приведенным неравенствам, то найдется такая коммутативная градуированная алгебра A, порожденная элементами первой степени, что $H(k) = \dim A_k$.*

Пусть алгебра A является факторалгеброй алгебры многочленов по однородному идеалу I. Обозначим через M соответствующий $\mathbb{Z}^n_{\geqslant 0}$-коидеал. В силу предложения 2.1, достаточно изучить функцию Гильберта коидеала M.

Пусть $<$ обозначает отношение лексикографического порядка на полугруппе $\mathbb{Z}^n_{\geqslant 0}$. Обозначим через $e_1, \ldots, e_n$ стандартный базис этой полугруппы.

Для всякого элемента $m = (m_1, \ldots, m_n)$ полугруппы $\mathbb{Z}^n_{\geqslant 0}$ обозначим $\deg m = m_1 + \cdots + m_n$. Функция $\deg$ задает градуировку полугруппы $\mathbb{Z}^n_{\geqslant 0}$.

Определение. Подмножество M полугруппы $\mathbb{Z}^n_{\geqslant 0}$ называется *уплотненным* (compressed), если для всякого элемента $m \in M$ и для всякого элемента $m' \in \mathbb{Z}^n_{\geqslant 0}$, таких что $\deg m' = \deg m$ и $m' < m$, подмножество M содержит элемент m'.

Следующая лемма описывает геометрический смысл оператора ∂_k.

Лемма 3.2 *Пусть M — некоторое уплотненное подмножество полугруппы $\mathbb{Z}^n_{\geqslant 0}$. Рассмотрим множество*

$$\partial M = \{m + e_i \mid m \in M,\ 1 \leqslant i \leqslant n\}.$$

Множество ∂M уплотнено и $\#(\partial M)_{k+1} = \partial_k(\#M_k)$.

Задача. Докажите сформулированную выше лемму.

Предложение 3.3 *Функция Гильберта всякого уплотненного коидеала полугруппы* $\mathbb{Z}^n_{\geqslant 0}$ *удовлетворяет неравенствам* $H(k+1) \leqslant \partial_k(H(k))$ *при* $k \geqslant 1$. *Обратно, если функция* $H(k)$ *удовлетворяет выписанным неравенствам, то существует уплотненный коидеал* M, *такой что* $H(k) = \#M_k$.

Доказательство.
Действительно, утверждение о том, что множество M является коидеалом, эквивалентно тому, что $\partial M \supseteq M$. Следовательно, для уплотненного коидеала M имеем $\#M_{k+1} \leqslant \#(\partial M)_{k+1} = \partial_k \#M_k$.

Пусть теперь H — функция, удовлетворяющая неравенствам $H(k+1) \leqslant \partial_k H(k)$. Обозначим через M_k совокупность первых $H(k)$ элементов степени k. Нетрудно показать, что (очевидно) уплотненное множество $M = \bigcup M_k$ является коидеалом. $\square$

Теперь для доказательства теоремы Маколея осталось только воспользоваться следующим утверждением:

Предложение 3.4 *Всякий коидеал* M *полугруппы* $\mathbb{Z}^n_{\geqslant 0}$ *можно уплотнить. Другими словами, найдется уплотненный коидеал* M' *с той же функцией Гильберта, что и* M.

Это утверждение верно, но мы не будем его доказывать. Комбинаторное доказательство, приведенное Маколеем, сложно для понимания. Маколей честно признается в этом:

"Note: This proof of the theorem which has been assumed earlier is given only to place it on record. It is too long and complicated to provide any but the most tedious reading."

В настоящее время имеются различные упрощения и обобщения сформулированного комбинаторного факта. Однако все эти упрощения все же еще не настолько просты, чтобы их стоило здесь приводить.

4 Конструкция Биллера–Ли

Биллера и Ли предложили явную конструкцию, при помощи которой для всякого набора неотрицательных целых чисел, удовлетворяющих условиям Макмюллена, можно построить симплициальный многогранник, h-вектор которого совпадает с этим набором. Ниже описана конструкция Биллера–Ли. Доказательств мы не приводим в виду их техничности.

Определение. Пусть Δ — некоторый многогранник. *Проекцией* многогранника Δ относительно точки $x \notin \Delta$ называется линк вершины x в многограннике $\mathrm{conv}(\Delta \cup \{x\})$. Проекция многогранника Δ относительно точки x совпадает с тенью, которую отбрасывает многогранник Δ (на подходящую гиперплоскость), если его освещать из точки x.

Утверждается, что любой допустимый h-вектор можно реализовать проекцией циклического многогранника относительно некоторой точки. Доказательство устроено следующим образом. Сначала строится некоторое множество $\mathcal{B}$ гиперплоских граней циклического многогранника. Затем доказывается, что можно выбрать точку таким образом, чтобы из нее были видны в точности грани множества $\mathcal{B}$. Проекция относительно этой точки и будет искомым многогранником.

Пусть $h_0, \ldots, h_d$ — набор целых неотрицательных чисел, удовлетворяющий условиям Макмюллена. Определим числа $g_0 = 1$, $g_1 = h_1 - h_0$, $\ldots$ так же, как g-вектор многогранника определяется по h-вектору. Если $g_1 = 0$, то, в силу условий Макмюллена, $g_i = 0$ при всех $i > 0$. Тогда все $h_i = 1$ и, следовательно, набор чисел h_i является h-вектором симплекса.

Пусть теперь $g_1 > 0$. Обозначим через $[n]$ множество $\{1, 2, \ldots, n\}$. Далее, положим $V_d = \{1\}$, если d четно, и $V_d = \{1, 2\}$, если d нечетно. Рассмотрим множество $\mathcal{E}$ всех $(d+1)$-элементных подмножеств $A \subseteq [g_1 + d + 1]$, таких что $V_d \subseteq A$, и $A - V_d$ содержит только четные компоненты. В частности, каждое подмножество $A \in \mathcal{E}$ содержит только четные собственные компоненты и, в силу критерия четности Гейла, определяет некоторую гиперплоскую грань циклического многогранника $C(g_1 + d + 1, d + 1)$. Следовательно, множество $\mathcal{E}$ можно рассматривать как некоторое множество граней циклического многогранника.

Представим себе полугруппу $\mathbb{Z}^{g_1}_{\geqslant 0}$ как полугруппу мономов относительно формальных переменных $x_1, \ldots, x_{g_1}$ (полугрупповой опрерацией является умножение мономов). Положим для удобства $x_0 = 1$. Определим отображение $\alpha : \mathcal{E} \to \mathbb{Z}^{g_1}_{\geqslant 0}$ следующим образом. Пусть $A \in \mathcal{E}$. Обозначим через

$\alpha_i(A)$ число элементов множества $[g_1+d+1]$, не принадлежащих A, стоящих перед $2i$-ым по порядку элементом множества $A - V_d$. Положим по определению

$$\alpha(A) = x_{\alpha_1(A)} x_{\alpha_2(A)} \dots x_{\alpha_{[d/2]}(A)}.$$

Очевидно, отображение α является биекцией между множеством $\mathcal{E}$ и множеством всех мономов степени $\leqslant [d/2]$.

Согласно условиям Макмюллена на числа $h_0, \dots, h_d$, существует некоторый уплотненный коидеал M полугруппы $\mathbb{Z}^{g_1}_{\geqslant 0}$, такой что $g_i = \#M_i$. В частности, $\#M_i = 0$ при $i > [d/2]$. Рассмотрим прообраз $\mathcal{B} = \alpha^{-1}(M) \subseteq \mathcal{E}$. Множество $\mathcal{B}$ можно рассматривать как некоторое множество гиперплоских граней циклического многогранника $C(g_1+d+1, d+1)$.

Теперь теорема Биллера–Ли сводится к доказательству следующих утверждений. Найдется точка p вне циклического многогранника $C(g_1+d+1, d+1)$, из которой видны все грани множества $\mathcal{B}$ и только они. Проекция многогранника $C(g_1+d+1, d+1)$ относительно точки p имеет h-вектор с заданными компонентами h_i.

Задача. Докажите эти утверждения.