Записки научных
семинаров ПОМИ
Том 400, 2012 г.

А. В. Яковлев

О КАНОНИЧЕСКИХ БАЗИСАХ ПРОСТРАНСТВ С ВПОЛНЕ УПОРЯДОЧЕННЫМ БАЗИСОМ И ВЫДЕЛЕННЫМ МНОЖЕСТВОМ ПОДПРОСТРАНСТВ

1. **Введение.** Обычное определение базиса Грёбнера основано на отношении включения для слов, составляющих базис пространства. Однако, обдумывая, как рассказать о базисе Грёбнера студентам, я заметил, что для определения базиса Грёбнера и для доказательства его существования и единственности в нётеровом случае достаточно каким угодно способом вполне упорядочить базис пространства, и этот порядок может быть никак не связан с отношениями включения или делимости старших членов. В частности, аналоги базисов Грёбнера для идеалов алгебры многочленов от нескольких переменных могут быть определены не только для обычных упорядочений одночленов, связанных с лексикографическим порядком, но и для произвольного базиса кольца многочленов, рассматриваемого как векторное пространство над основным полем, и для произвольного полного упорядочения этого базиса. Аналогичная конструкция применима и к любым другим алгебрам и их нетеровым идеалам, и даже в более общей ситуации – лишь бы был задан вполне упорядоченный базис алгебры.

Настоящая заметка посвящена определению в очень общей ситуации базиса, который я называю G-базисом и который в классической ситуации превращается в обычный базис Грёбнера, и доказательству его существования и единственности в нетеровом случае. Отметим, что речь здесь идет только о существовании и единственности, но никак не об алгорифмах; они должны зависеть от того, какими операциями из заданного множества элементов можно построить все элементы порожденного этим множеством "идеала".

2. **Пространства с "идеалами".** Пусть V – векторное пространство над полем k, и пусть $\mathfrak{I}$ – некоторое множество его подпространств, замкнутое относительно любых пересечений (не только конечных). В частности, пересечение V пустого множества подпространств из $\mathfrak{I}$

Ключевые слова: базис Грёбнера.

принадлежит $\mathfrak{I}$. Подпространства из $\mathfrak{I}$ будем называть “идеалами” V (в кавычках). Описанная ситуация достаточно универсальна: V может быть алгеброй (ассоциативной, лиевой, хопфовой или какой угодно другой, в том числе, ещё не изобретенной, с любой сигнатурой), а $\mathfrak{I}$ может быть множеством всех её идеалов, или всех подалгебр, или не всех, а удовлетворяющих каким-то ограничениям. Но V может и не быть алгеброй, а обладать какой-то иной структурой, которая выделяет в V некоторое множество $\mathfrak{I}$ естественных подпространств (как структура алгебры выделяет множество её идеалов). Например, V может быть векторным пространством с линейной топологией, а $\mathfrak{I}$ – множеством всех его замкнутых подпространств.

Для любого подмножества X пространства V будем обозначать через $\langle X\rangle$ пересечение всех “идеалов” V, содержащих X, и будем называть $\langle X\rangle$ “идеалом” V, порожденным множеством X. “Идеал” $U \in \mathfrak{I}$ называем нетеровым, если всякая строго возрастающая цепочка содержащихся в U “идеалов” конечна.

3. Приведенные элементы. Пусть теперь B – базис пространства V, на котором задано отношение $\leq$, превращающее B во вполне упорядоченное множество. Всякий элемент $v \in V$ однозначно представляется в виде линейной комбинации элементов базиса B; носителем $[v]$ элемента v называем (конечное) множество всех тех элементов базиса B, которые входят в эту комбинацию с ненулевыми коэффициентами. Если $v \neq 0$, то в его носителе $[v]$ есть наибольший элемент $w(v) \in B$, который мы будем называть весом v. Тогда

$$v = \alpha w(v) + \sum_{b<w(v)} \beta_b b, \quad \alpha, \beta_b \in k, \quad \alpha \neq 0$$

(почти все β_b равны 0). Коэффициент α при $w(v)$ называем старшим коэффициентом элемента v.

Для каждого элемента $b \in B$ обозначим через V_b линейную оболочку всех элементов $c \in B$, $c < b$. Для “идеала” $U \in \mathfrak{I}$ мы будем обозначать через U_b пересечение $V_b \cap U$; ненулевой элемент $u \in U$ называем приведенным, если старший коэффициент u равен 1 и в носителе $[u]$ элемента u нет весов элементов из $U_{w(u)}$.

Предложение 1. *Если в U есть элемент веса b, то в U есть единственный приведенный элемент веса b.*

Доказательство. Если $u_1, u_2 \in U$ – приведенные элементы веса b, то $u_1 - u_2 \in U_b$, и в носителе элемента $u_1 - u_2$ нет весов элементов из U_b; это возможно только если $u_1 - u_2 = 0$. Таким образом, в U может быть только один приведенный элемент веса b. Покажем, что такой элемент существует.

Пусть M – множество всех элементов $v \in V_b$, таких что $b+v \in U$; по нашему предположению множество M непусто. Если в U нет приведенных элементов веса b, то в (конечном) носителе каждого элемента $v \in M$ есть веса элементов из U_b; пусть $m(v)$ – наибольший из этих весов. Множество $\{m(v) \mid v \in M\} \subseteq B$ непусто вместе с M; пусть c – его наименьший элемент, и пусть $v_0 \in M$ – такой элемент, что $m(v_0) = c$, а β – коэффициент, с которым c входит в v_0. По построению c является весом некоторого элемента $u \in U_b$; пусть γ – коэффициент, с которым c входит в u. Тогда элемент $v_1 = v_0 - \beta\gamma^{-1}u$ тоже принадлежит M, и если в носителе v_1 и есть веса элементов из U_b, то все они меньше c. Это противоречит минимальности c. Следовательно, в U есть приведенный элемент веса b.

4. **G-базисы.** Подмножество S "идеала" U называется базисом U, если $U = \langle S \rangle$. Пусть S – базис U; для каждого $g \in S$ обозначим через S^g подмножество S, состоящее из всех элементов, вес которых больше веса g. S называется G-базисом U, если S состоит из приведенных элементов и все элементы $g \in S$ обладают свойством:

$$g \notin \langle U_{w(g)} \cup S^g \rangle.$$

Поскольку все элементы из S веса, меньшего, чем вес g, принадлежат $U_{w(g)}$, отсюда следует, в частности, что ни один элемент из S не принадлежит "идеалу", порожденному остальными элементами S.

Теорема. *У каждого нетерова идеала $U \in \mathfrak{I}$ есть единственный G-базис.*

Доказательство. ***Единственность.*** Пусть

$$S = \{g_1, \dots, g_m\}, \quad T = \{h_1, \dots, h_n\}$$

– два G-базиса, упорядоченные по убыванию весов. Не ограничивая общности, считаем, что $m \leq n$. Индукцией по i покажем, что $g_i = h_i$ для всех $i \leq m$. Пусть уже доказано, что $g_j = h_j$ для всех $j < i$, так что $S^{g_i} = T^{h_i}$. При $j < i$ элементы g_j принадлежат S^{g_i}, а при $j > i$ элементы g_j принадлежат $U_{w(g_i)}$. Таким образом, все элементы базиса S принадлежат множеству $U_{w(g_i)} \cup \{g_i\} \cup S^{g_i}$, и потому "идеал", порожденный этим множеством, равен U. Если $w(g_i) < w(h_i)$, то $U_{w(g_i)} \cup \{g_i\} \subseteq U_{w(h_i)}$, и потому

$$h_i \in U = \langle U_{w(g_i)} \cup \{g_i\} \cup S^{g_i} \rangle \subseteq \langle U_{w(h_i)} \cup T^{h_i} \rangle,$$

а это противоречит тому, что T – G-базис U. Точно так же приводит к противоречию предположение $w(h_i) < w(g_i)$. Итак, $w(g_i) = w(h_i)$; поскольку приведенные элементы из U, имеющие одинаковый вес, равны, отсюда следует, что $g_i = h_i$.

Осталось показать, что $m = n$. Если это не так, то в T есть элемент h_{m+1}, и $T^{h_{m+1}} = \{h_1, \ldots, h_m\} = \{g_1, \ldots, g_m\} = S$; тогда

$$h_{m+1} \in U = \langle S \rangle \subseteq \langle T^{h_{m+1}} \cup U_{w(h_{m+1})} \rangle$$

в противоречие с тем, что T – G-базис.

Существование. Построим индукцией приведенные элементы $g_1, g_2, \ldots, g_n \in U$, порождающие U и такие что

(1) если $1 \le i < j \le n$, то вес g_i строго больше веса g_j;
(2) если $1 \le i \le n$, то U порождается $U_{w(g_i)}$ и всеми элементами g_j с $j \le i$, но не порождается $U_{w(g_i)}$ и всеми элементами g_j с $j < i$.

Из условия (2) следует, что для каждого i элемент g_i не принадлежит "идеалу", порожденному $U_{w(g_i)}$ и элементами из $\{g_1, \ldots, g_n\}$ с большими весами, чем g_i; поэтому $\{g_1, \ldots, g_n\}$ – G-базис U.

Пусть элементы g_j уже построены для всех $j < i$; обозначим множество этих элементов через X. Если X порождает U, то полагаем $n = i - 1$ и заканчиваем построение. Пусть X не порождает U. Положим $W = U$ при $i = 1$, $W = U_{w(g_{i-1})}$ при $i > 1$; ясно, что $\langle W \cup X \rangle = U$. Пусть M – множество конечных подмножеств P множества W, таких что $\langle P \cup X \rangle = U$; оно непусто, потому что "идеал" $\langle W \rangle \subseteq U$ нетеров, и в порождающем его множестве W есть конечные подмножества, тоже порождающие W. Для каждого $P \in M$ обозначим через m_P наибольший из конечного множества весов элементов, входящих в P. Вместе с P непусто подмножество $\{m_P \mid P \in M\}$ вполне упорядоченного базиса B; пусть b – наименьший элемент этого подмножества, и пусть Q – такое подмножество из M, что $b = m_Q$. Множество Q содержится в U, и в нем есть элемент веса b; значит, в U есть приведенный элемент веса b; его мы и возьмем в качестве g_i.

Проверим, что построенный выше элемент g_i обладает всеми нужными свойствами. Если $1 \leq j < i$, то $g_i \in Q \subseteq W \subseteq V_{w(g_{i-1})}$, и потому $w(g_i) < w(g_{i-1}) \leq w(g_j)$. Далее, пространство, порожденное $U_{w(g_i)} = U_b$ и g_i, содержит все элементы из U, вес которых не больше b; в частности, оно содержит Q, и значит,

$$U = \langle Q \cup X \rangle = \langle U_{w(g_i)} \cup \{g_i\} \cup X \rangle.$$

Наконец, $\langle U_{w(g_i)} \cup X \rangle \neq U$, потому что иначе в нетеровом "идеале" $\langle U_{w(g_i)} \rangle$ было бы конечное подмножество P, вместе с X порождающее U и потому принадлежащее M; но это невозможно, так как в каждом множестве из M есть элементы веса, не меньшего чем $b = w(g_i)$.

Остается заметить, что процесс построения элементов g_i должен остановиться после конечного числа шагов – иначе получилась бы бесконечная строго возрастающая цепочка "идеалов"

$$\langle g_1 \rangle \subset \langle g_1, g_2 \rangle \subset \ldots \subset \langle g_1, g_2, \ldots g_n \rangle \subset \ldots ,$$

содержащихся в нетеровом "идеале" U.

5. Об "идеалах", не являющихся нетеровыми. Следующие примеры показывают, что при отсутствии нетеровости G-базис может не существовать, а если даже G-базис существует, то он может не быть единственным. В этих примерах V – пространство с базисом B, состоящим из элементов b_i, где индексы i пробегают все множество натуральных чисел, причем

$$b_1 < b_2 < b_3 \ldots < b_i < b_{i+1} < \ldots .$$

Пример 1. Множество $\mathfrak{I}$ состоит из пространства V и его подпространств V_i, порожденных начальными отрезками $\{b_1, b_2, \ldots, b_i\}$ базиса B. В этом случае G-базис не существует. Действительно, элементы b_i являются единственными приведенными элементами пространства V. Для любого i будет $\langle b_i \rangle = V_i \neq V$; поэтому базис не может состоять из единственного элемента b_i. Если же два элемента $b_j < b_i$ входят в базис, состоящий из приведенных элементов, то $b_j \in V_i = \langle b_i \rangle$, так что этот базис не может быть G-базисом.

Пример 2. Пусть $\mathfrak{X}$ – множество всех подмножеств X множества натуральных чисел $\mathbb{N}$, дополнения которых являются объединениями отрезков, длина каждого из которых не меньше 2 (один из этих отрезков может быть бесконечным и состоять из всех чисел, больших некоторого числа). Для каждого такого множества X обозначим через V_X подпространство пространства V, порожденное теми из векторов b_i, для которых $i \in X$. Далее, положим $S = \{b_{2i} \,|\, i \in \mathbb{N}\}$, $T = \{b_{2i-1} \,|\, i \in \mathbb{N}\}$.

Предложение 2. *Множество $\mathfrak{I} = \{V_X \,|\, X \in \mathfrak{X}\}$ замкнуто относительно пересечений, а множества $S, T \subseteq B$ составляют два различных G-базиса V.*

Доказательство. Первое утверждение очевидно: дополнение пересечения множеств является объединением дополнений этих множеств, а при объединении длина составляющих эти дополнения отрезков не может уменьшаться. Остается показать, что S и T – G-базисы V.

Дополнение в $\mathbb{N}$ множества четных чисел состоит из отрезков длины 1; поэтому единственным подпространством пространства V, принадлежащим $\mathfrak{I}$ и содержащим S, является само подпространство V. Таким образом, S порождает V. Далее, для любого $i \in \mathbb{N}$ множество $Y = [1, 2i-1] \cup [2i+2, \infty)$ принадлежит $\mathfrak{X}$ и не содержит $2i$; поэтому b_{2i} не принадлежит “идеалу” $V_Y = \langle\{b_y \,|\, y \in Y\}\rangle$ и тем более

$$b_{2i} \notin \langle\{b_j \,|\, 1 \le j < 2i\} \cup \{b_{2s} \,|\, s > i\} = \langle V_{w(b_{2i})} \cup S^{b_{2i}}\rangle.$$

Итак, S – G-базис V.

Аналогично, дополнение в $\mathbb{N}$ множества нечетных чисел состоит из отрезков длины 1; поэтому единственным подпространством пространства V, принадлежащим $\mathfrak{I}$ и содержащим T, является само подпространство V. Таким образом, T порождает V. Далее, для любого $i \in \mathbb{N}$ множество $Z = [1, 2i-2] \cup [2i+1, \infty)$ принадлежит $\mathfrak{X}$ и не содержит $2i-1$; поэтому b_{2i-1} не принадлежит “идеалу” $V_Z = \langle\{b_z \,|\, z \in Z\}\rangle$ и тем более

$$b_{2i-1} \notin \langle\{b_j \,|\, 1 \le j < 2i-1\} \cup \{b_{2s-1} \,|\, s > i\} = \langle V_{w(b_{2i-1})} \cup T^{b_{2i-1}}\rangle.$$

Итак, T – G-базис V.

Yakovlev A. V. On canonical bases of spaces with a well ordered basis and a distinguished family of subspaces.

Let V be a vector space with a well ordered basis and $\mathfrak{I}$ a family of subspaces of V closed under intersections. An analogue of Groebner basis is defined for subspaces from $\mathfrak{I}$. It is shown that in Noetherian case such basis always exists and is unique.

С.-Петербургский
государственный университет
Университетский пр. 28, Петродворец,
198504 Санкт-Петербург, Россия
E-mail: yakovlev.anatoly@gmail.com

Поступило 28 февраля 2012 г.