Сибирский математический журнал
Май—июнь, 2003. Том 44, № 3

УДК 519.48

СВОБОДНАЯ АССОЦИАТИВНАЯ АЛГЕБРА КАК СВОБОДНЫЙ МОДУЛЬ НАД ПОДАЛГЕБРОЙ ШПЕХТА

А. В. Гаврилов

Аннотация: Пусть k — поле характеристики нуль, $k\langle X\rangle$ — свободная ассоциативная алгебра с конечным базисом X. Пусть $R = R(k, X)$ — универсальная обертывающая квадрата $\mathrm{Lie}(X)$, рассматриваемая как подалгебра в $k\langle X\rangle$; она названа подалгеброй Шпехта свободной алгебры. Показано, что $k\langle X\rangle$ является свободным (левым) R-модулем; найдены достаточные условия того, что некоторая система элементов $k\langle X\rangle$ является базисом этого модуля. Получена явная формула, позволяющая вычислять R-коэффициенты элементов свободной алгебры над специальным базисом из «симметризованных мономов».

Ключевые слова: свободная ассоциативная алгебра, свободный модуль над подалгеброй, некоммутативные симметрические многочлены

Пусть k — поле характеристики нуль, $k\langle X\rangle$ — свободная ассоциативная алгебра с конечным базисом $X = \{x_1, \dots, x_n\}$. Будем обозначать через $R = R(k, X)$ подалгебру (с единицей) в $k\langle X\rangle$, порожденную элементами вида $[x_i, x_j]$, $[[x_i, x_j], x_k]$, $[[[x_i, x_j], x_k], x_l]$, и т. д. Иными словами, R — наименьшая подалгебра в $k\langle X\rangle$, содержащая коммутаторы $[x_i, x_j]$, $1 \le i < j \le n$, и замкнутая относительно дифференцирований $\operatorname{ad} x_i$, $1 \le i \le n$. Рассматривавшиеся В. Шпехтом в [1] «собственные формы» совпадают с полилинейными многочленами из R. Более того, в работе [1] фактически сформулированы и доказаны основные свойства этой подалгебры, правда, применительно к полилинейному случаю (см. об этом ниже). Поэтому $R(k, X)$ естественно называть *подалгеброй Шпехта* в $k\langle X\rangle$.

Под R-модулем далее понимается левый модуль над R. Алгебра $k\langle X\rangle$ является свободным R-модулем; как сообщил автору А. Р. Кемер, этот результат считается «фольклорно» известным. Справедливо даже более сильное утверждение. Пусть $Ab : k\langle X\rangle \to k[X]$ — естественный гомоморфизм «абелеанизации».

Теорема 1. *Пусть $\lambda : k[X] \to k\langle X\rangle$ — линейное отображение такое, что*

$$Ab(\lambda(f)) = f, \quad \deg(\lambda(f)) = \deg(f)$$

для всех $f \in k[X]$. Тогда его естественное продолжение

$$\lambda : R \otimes k[X] \to k\langle X\rangle$$

является изоморфизмом R-модулей.

Под естественным продолжением здесь понимается отображение вида

$$\lambda : r \otimes f \mapsto r \cdot \lambda(f).$$

Разложение элемента $k\langle X\rangle$ над R в любом базисе является достаточно нетривиальной процедурой. Однако, как мы увидим, это разложение может быть описано явно в случае специального базиса. Определим линейный оператор симметризации $\sigma : k\langle X\rangle \to k\langle X\rangle$, действующий на мономы следующим образом: если $a_j \in \{x_1, \ldots, x_n\}$, $1 \le j \le m$, то

$$\sigma : a_1 a_2 \ldots a_m \mapsto \frac{1}{m!} \sum_{\pi} a_{\pi(1)} a_{\pi(2)} \ldots a_{\pi(m)}, \tag{1}$$

где сумма берется по всем $m!$ перестановкам $\pi \in S_m$.

Поскольку сумма в правой части (1), очевидно, не зависит от порядка множителей a_j в левой, $\sigma(f)$ при $f \in k\langle X\rangle$ зависит только от $Ab(f)$. Поэтому можно построить (единственным образом) такое отображение $\lambda : k[X] \to k\langle X\rangle$, что $\sigma(f) = \lambda(Ab(f))$. Оно удовлетворяет условиям теоремы 1, поэтому *симметризованные мономы* $s_\alpha = \lambda(x^\alpha)$ образуют базис $k\langle X\rangle$ как R-модуля. Здесь $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ — мультииндекс,

$$x^\alpha = \prod_{i=1}^{n} x_i^{\alpha_i} \in k[X].$$

Например, в $k\langle x_1, x_2\rangle$ будет

$$s_{(2,1)} = \lambda\bigl(x_1^2 x_2\bigr) = \frac{1}{3}\bigl(x_1^2 x_2 + x_1 x_2 x_1 + x_2 x_1^2\bigr).$$

Согласно теореме 1 для всякого элемента $u \in k\langle X\rangle$ однозначно определены коэффициенты $r_\alpha(u) \in R$ такие, что

$$u = \sum_{\alpha} r_\alpha(u) s_\alpha.$$

Оказывается, существует явный алгоритм, позволяющий вычислять эти коэффициенты. Пусть по определению для $u \in k\langle X\rangle$

$$\rho(u) = \sum_{\alpha} r_\alpha(u) y^\alpha \in k\langle X\rangle[Y], \tag{2}$$

где $k\langle X\rangle[Y] = k\langle x_1, \ldots, x_n\rangle[y_1, \ldots, y_n]$,

$$y^\alpha = \prod_{i=1}^{n} y_i^{\alpha_i} \in k\langle X\rangle[Y].$$

Например,

$$\rho(x_1 x_2) = y_1 y_2 + \frac{1}{2}[x_1, x_2],$$

$$\rho(x_1 x_2 x_3) = y_1 y_2 y_3 + \frac{1}{2}([x_1, x_2]y_3 + [x_1, x_3]y_2 + [x_2, x_3]y_1) + \frac{1}{3}([[x_3, x_2], x_1] + [[x_3, x_1], x_2]).$$

Стоит отметить, что при более высоких степенях коэффициенты $r_\alpha(u)$ становятся весьма громоздкими.

Пусть $\frac{\partial}{\partial x_i}$ и $\frac{\partial}{\partial y_i}$ $(1 \le i \le n)$ — дифференцирования алгебры $k\langle X\rangle[Y]$,

$$\frac{\partial}{\partial x_i} x_j = \delta_{ij}, \quad \frac{\partial}{\partial x_i} y_j = 0, \quad \frac{\partial}{\partial y_i} y_j = \delta_{ij}, \quad \frac{\partial}{\partial y_i} x_j = 0,$$

где δ_{ij} — символ Кронекера. Определим линейные операторы D, Δ:

$$Du = \sum_{i=1}^{n} \frac{\partial u}{\partial x_i} y_i, \quad \Delta u = \sum_{i=1}^{n} \frac{\partial u}{\partial y_i} x_i. \tag{3}$$

Теорема 2. *Для всякого* $u \in k\langle X\rangle$

$$\rho(u) = \exp(-\Delta)\exp(D)u. \tag{4}$$

Операторы D, Δ локально нильпотентны в $k\langle X\rangle[Y]$, поэтому правая часть (4) корректно определена.

Перед тем как перейти к доказательствам, автор хотел бы пояснить, почему, по его мнению, рассматриваемые вопросы заслуживают внимания. Пусть $\mathrm{Lie}(X)$ — свободная алгебра Ли, обычным образом вложенная в $k\langle X\rangle$. Если z_i — некоторый линейный базис $\mathrm{Lie}(X)$, то по теореме Пуанкаре — Биркгофа — Витта произведения

$$z_{i_1}z_{i_2}z_{i_3}\dots z_{i_m}, \quad i_1 \geq i_2 \geq i_3 \geq \dots \geq i_m, \tag{5}$$

образуют линейный базис $k\langle X\rangle$.

Известны различные способы построения базиса $\mathrm{Lie}(X)$ [2–5] (см. также [6]). Выбрав один из них, получим два линейных базиса $k\langle X\rangle$: обычный, состоящий из мономов, и «лиевский», состоящий из произведений (5). Естественным образом возникает задача описания матриц перехода от одного базиса к другому (заведомо весьма сложных). Как мы увидим, подалгебра R совпадает с универсальной обертывающей квадрата $\mathrm{Lie}(X)$. Поэтому разложение элемента $k\langle X\rangle$ над R является промежуточным этапом в его разложении по базису (5) независимо от того, какой из однородных базисов $\mathrm{Lie}(X)$ мы используем.

Автор благодарен Л. А. Бокутю за полезные замечания. Также он хотел бы высказать благодарность В. А. Шарафутдинову, чьи вопросы послужили толчком к этой работе.

1. Базисы $k\langle X\rangle$

Пусть z_i, $i \in \mathbb{N}$, — линейный базис $\mathrm{Lie}(X)$, удовлетворяющий следующим условиям:

1) $z_i = x_i$ при $i \leq n$;

2) $z_i = [z_j, z_k]$ для некоторых $k < j < i$ при $i > n$.

Этими свойствами обладают, например, базис Холла [2] и вообще любой (соответствующим образом упорядоченный) базис из лиевских слов. По теореме Пуанкаре — Биркгофа — Витта произведения (5) вместе с единицей образуют линейный базис алгебры $k\langle X\rangle$ (обычно используется обратный порядок, но это несущественно).

Лемма 1. *Произведения вида* $z_{i_1}z_{i_2}z_{i_3}\dots z_{i_m}$, $i_1 \geq i_2 \geq i_3 \geq \dots \geq i_m > n$, *вместе с единицей образуют линейный базис алгебры* R.

Доказательство. Фактически требуется доказать, что элемент из $k\langle X\rangle$ лежит в R тогда и только тогда, когда в его разложении по базису (5) отсутствуют z_i с $i \leq n$. По индукции легко доказывается, что $z_i \in R$, $i > n$. Также по индукции $\frac{\partial}{\partial x_i}R = 0$ для всех $1 \leq i \leq n$.

Пусть $k\langle Z\rangle = k\langle\{z_1, z_2, \dots, z_n, \dots\}\rangle$ — свободная алгебра, $V(Z) \subset k\langle Z\rangle$ — линейная оболочка упорядоченных мономов (5). Рассмотрим гомоморфизм $\theta : k\langle Z\rangle \to k\langle X\rangle$, переводящий z_i в соответствующий элемент $k\langle X\rangle$. Понятно, что ограничение его на $V(Z)$ является линейным изоморфизмом.

Пусть $u \in R$ — некоторый элемент подалгебры Шпехта и $\hat{u} \in V(Z)$ — его прообраз (или, что то же самое, его разложение), т. е. $\theta : \hat{u} \mapsto u$. Легко проверить, что при $i \leq n$ имеет место равенство

$$\frac{\partial\theta(z_j)}{\partial x_i} = \delta_{ij}.$$

Следовательно, при этом условии

$$\theta : \frac{\partial}{\partial z_i} z_j \mapsto \frac{\partial}{\partial x_i} \theta(z_j),$$

поэтому

$$\theta : \frac{\partial}{\partial z_i} \hat{u} \mapsto \frac{\partial}{\partial x_i} u = 0.$$

Но $\frac{\partial}{\partial z_i} \hat{u} \in V(Z)$, тем самым $\frac{\partial}{\partial z_i} \hat{u} = 0$. Для элемента $V(Z)$ это означает, что он не содержит z_i, что и требовалось доказать.

Заметим, что из доказательства также следует равенство

$$R(k, X) = \bigcap_{1 \leq i \leq n} \ker \left(\frac{\partial}{\partial x_i}, k\langle X \rangle \right), \tag{6}$$

которое можно считать еще одним определением R. Фактически и это утверждение, и аналог леммы 1 имеются у В. Шпехта, только в [1] ход рассуждений обратный: «собственные» формы определяются как переходящие в нуль при дифференцированиях, а затем показывается, что они выражаются через коммутаторы.

Из леммы вытекает, что R является универсальной обертывающей квадрата $\mathrm{Lie}(X)$.

Лемма 2. *$k\langle X \rangle$ — свободный R-модуль с базисом, состоящим из произведений*

$$x_{i_1} x_{i_2} x_{i_3} \ldots x_{i_m}, \quad n \geq i_1 \geq i_2 \geq i_3 \geq \cdots \geq i_m. \tag{7}$$

Это сразу следует из предыдущей леммы.

Лемма 3. *Пусть $\varphi_i \in k\langle X \rangle$, $i \in J$, образуют базис $k\langle X \rangle$ как R-модуля. Пусть ψ_i, $i \in J$, — многочлены вида*

$$\psi_i = \varphi_i + \sum_j r_{ij} \varphi_j, \tag{8}$$

где $r_{ij} \in R$, причем $\deg \varphi_j < \deg \varphi_i$ при $r_{ij} \neq 0$. Тогда ψ_i тоже базис модуля.

Здесь J — некоторое множество индексов (которое обязано быть счетным).

Доказательство. Обозначим R-модуль, порожденный ψ_i, через A. Предположим, что φ_k — элемент наименьшей степени, не лежащий в A. Тогда

$$\psi_k - \varphi_k = \sum_j r_{kj} \varphi_j$$

и правая часть принадлежит A, а левая нет. Следовательно, $A = k\langle X \rangle$.

Теперь предположим, что

$$\sum_i q_i \psi_i = 0$$

для некоторых $q_i \in R$, не все из которых равны нулю. Тогда

$$\sum_i q_i \varphi_i + \sum_{ij} q_i r_{ij} \varphi_j = 0.$$

Если полином φ_j присутствует во второй сумме, т. е. для некоторого индекса i $q_i r_{ij} \neq 0$, то по условию $\deg \varphi_j < \deg \varphi_i$. Значит, в левой части равенства элементы φ_i наибольшей степени (из тех, для которых $q_i \neq 0$) присутствуют только в первой сумме. Поэтому коэффициент при них отличен от нуля, что противоречит условиям леммы.

Теперь мы можем доказать теорему 1. Выберем в качестве φ_i упорядоченные мономы (7) из леммы 2. Нетрудно видеть, что $Ab(\varphi_i)$ образуют линейный базис $k[X]$. Тогда полиномы $\psi_i = \lambda(Ab(\varphi_i))$ составят линейный базис $\lambda(k[X])$. Имеет место разложение

$$\psi_i = \varphi_i + \sum_j r_{ij}\varphi_j,$$

причем $\deg\psi_i = \deg Ab(\varphi_i) = \deg\varphi_i$.

Применив к нему гомоморфизм Ab, получим

$$\sum_j Ab(r_{ij})Ab(\varphi_j) = 0.$$

Видно, что $Ab(r) \in k$ для любого $r \in R$. Поскольку $Ab(\varphi_j)$ линейно независимы, все $Ab(r_{ij})$ равны нулю; это означает, что свободные члены r_{ij} равны нулю.

Пусть r_μ, $\mu \in M$, — базис R из леммы 1. Легко видеть, что этот базис однороден. Полиномы φ_i также однородны, поэтому произведения $r_\mu\varphi_i$, $\mu \in M$, $i \in J$, образуют однородный базис $k\langle X\rangle$. Следовательно, в разложении

$$\psi_i - \varphi_i = \sum_j r_{ij}\varphi_j$$

степени слагаемых в правой части не превосходят степени многочлена в левой: $\deg r_{ij} + \deg\varphi_j \leq \deg(\psi_i - \varphi_i) \leq \deg\varphi_i$, $r_{ij} \neq 0$. Поскольку полиномы r_{ij} не могут быть отличными от нуля константами, имеем

$$\deg\varphi_j < \deg\varphi_i, \quad r_{ij} \neq 0.$$

Мы видим, что условия леммы 3 выполнены, и потому ψ_i образуют базис $k\langle X\rangle$ как R-модуля и одновременно линейный базис $\lambda(k[X])$, откуда следует утверждение теоремы.

2. Экспоненциальная формула

Пусть $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$, $\beta = (\beta_1, \beta_2, \ldots, \beta_n)$ — мультииндексы. Ниже мы будем использовать следующие стандартные обозначения:

$$\alpha! = \prod_{i=1}^n \alpha_i!$$

— факториал мультииндекса,

$$\binom{\alpha}{\beta} = \begin{cases} \frac{\alpha!}{\beta!(\alpha-\beta)!}, & \text{если } \beta \leq \alpha, \\ 0 & \text{иначе} \end{cases}$$

— биномиальный коэффициент,

$$|\alpha| = \sum_{i=1}^n \alpha_i$$

— модуль α.

Введем оператор $Q : k\langle X\rangle \to k\langle X\rangle$,

$$Q : u \mapsto \sum_{i=1}^n \frac{\partial u}{\partial x_i} x_i. \tag{9}$$

Лемма 4. *Имеет место равенство*

$$Qs_\alpha = |\alpha| s_\alpha. \tag{10}$$

Доказательство. Пусть $u = a_1 a_2 \dots a_m$, где $a_j \in \{x_1, \dots, x_n\}$, $1 \le j \le m$. Нетрудно видеть, что

$$Qu = \sum_{j=1}^{m} a_1 \dots a_{j-1} a_{j+1} \dots a_m a_j;$$

в каждом мономе справа элемент a_j переставлен в конец. Следовательно,

$$Q\sigma u = \sum_{j=1}^{m} \frac{1}{m!} \sum_{\pi} a_{\pi(1)} \dots a_{\pi(j-1)} a_{\pi(j+1)} \dots a_{\pi(m)} a_{\pi(j)} = m\sigma u,$$

поскольку все внутренние суммы равны. В частности,

$$\sum_{i=1}^{n} \left(\frac{\partial}{\partial x_i} s_\alpha \right) x_i = |\alpha| s_\alpha.$$

Если $\beta = (0, \dots, 0, 1, 0, \dots, 0)$ (единица на i-м месте), то

$$s_\beta = x_i, \quad \binom{\alpha}{\beta} = \alpha_i, \quad \frac{\partial}{\partial x_i} s_\alpha = \alpha_i s_{\alpha-\beta} = s_{\alpha-\beta} \binom{\alpha}{\beta}.$$

Поэтому равенство (10) можно переписать в виде

$$\sum_{|\beta|=1} s_{\alpha-\beta} s_\beta \binom{\alpha}{\beta} = |\alpha| s_\alpha. \tag{11}$$

Имеется интересное следствие формулы (10), которое мы приведем, хотя оно и не имеет отношения к доказательству. Так как для всякого $r \in R$, очевидно, $Qru = rQu$, то

$$Qu = Q \sum_\alpha r_\alpha(u) s_\alpha = \sum_\alpha |\alpha| r_\alpha(u) s_\alpha.$$

Отсюда следует разложение

$$k\langle X \rangle = \bigoplus_{n=0}^{\infty} \ker(Q - nI, k\langle X \rangle),$$

где I — тождественный оператор. Заметим, что полилинейный аналог равенства $R = \ker(Q, k\langle X \rangle)$ имеется у В. Шпехта, но в несколько иной формулировке [1, теорема 13].

Лемма 5. *Имеет место равенство*

$$D^n s_\alpha = n! \sum_{|\beta|=n} s_{\alpha-\beta} y^\beta \binom{\alpha}{\beta}. \tag{12}$$

Доказательство. Нетрудно видеть, что

$$Ds_\alpha = \sum_{i=1}^{n} \left(\frac{\partial}{\partial x_i} s_\alpha \right) y_i = \sum_{|\beta|=1} s_{\alpha-\beta} y^\beta \binom{\alpha}{\beta},$$

так что при $n = 1$ формула (12) верна. Теперь по индукции

$$D^{n+1}s_\alpha = Dn!\sum_{|\delta|=n} s_{\alpha-\delta}y^\delta\binom{\alpha}{\delta} = n!\sum_{|\delta|=n}\sum_{|\gamma|=1} s_{\alpha-\delta-\gamma}y^{\delta+\gamma}\binom{\alpha}{\delta}\binom{\alpha-\delta}{\gamma}$$

$$= n!\sum_{|\delta|=n}\sum_{|\gamma|=1} s_{\alpha-\delta-\gamma}y^{\delta+\gamma}\binom{\alpha}{\delta+\gamma}\binom{\delta+\gamma}{\gamma} = n!\sum_{|\beta|=n+1} s_{\alpha-\beta}y^\beta\binom{\alpha}{\beta}\sum_{|\gamma|=1}\binom{\beta}{\gamma}$$

$$= (n+1)!\sum_{|\beta|=n+1} s_{\alpha-\beta}y^\beta\binom{\alpha}{\beta}.$$

Здесь мы ввели обозначение $\beta = \delta + \gamma$ и воспользовались очевидным соотношением

$$\sum_{|\gamma|=1}\binom{\beta}{\gamma} = |\beta|.$$

Лемма 6. *Имеет место равенство*

$$\Delta^n y^\alpha = n!\sum_{|\beta|=n} y^{\alpha-\beta}s_\beta\binom{\alpha}{\beta}. \tag{13}$$

Доказательство. Аналогично предыдущему

$$\Delta y^\alpha = \sum_{i=1}^{n}\left(\frac{\partial}{\partial y_i}y^\alpha\right)x_i = \sum_{|\beta|=1} y^{\alpha-\beta}s_\beta\binom{\alpha}{\beta}.$$

Теперь по индукции

$$\Delta^{n+1}y^\alpha = \Delta n!\sum_{|\delta|=n} y^{\alpha-\delta}s_\delta\binom{\alpha}{\delta} = n!\sum_{|\delta|=n}\sum_{|\gamma|=1} y^{\alpha-\delta-\gamma}s_\delta s_\gamma\binom{\alpha}{\delta+\gamma}\binom{\delta+\gamma}{\gamma}$$

$$= n!\sum_{|\beta|=n+1} y^{\alpha-\beta}\binom{\alpha}{\beta}\sum_{|\gamma|=1} s_{\beta-\gamma}s_\gamma\binom{\beta}{\gamma} = (n+1)!\sum_{|\beta|=n+1} y^{\alpha-\beta}s_\beta\binom{\alpha}{\beta}$$

согласно (11). Лемма доказана.

Применив лемму 6 к очевидному тождеству $\Delta^{n+m} = \Delta^n\Delta^m$, получим формулу

$$\sum_{|\beta|=n} s_{\alpha-\beta}s_\beta\binom{\alpha}{\beta} = \binom{|\alpha|}{n}s_\alpha, \tag{14}$$

обобщающую (11).

Перейдем к доказательству теоремы 2. Прежде всего по лемме 5

$$\exp(D)s_\alpha = \sum_{n=0}^{\infty}\frac{D^n s_\alpha}{n!} = \sum_{n=0}^{\infty}\sum_{|\beta|=n} s_{\alpha-\beta}y^\beta\binom{\alpha}{\beta} = \sum_\beta s_{\alpha-\beta}y^\beta\binom{\alpha}{\beta}. \tag{15}$$

Аналогично по лемме 6

$$\exp(\Delta)y^\alpha = \sum_{n=0}^{\infty}\frac{\Delta^n y^\alpha}{n!} = \sum_{n=0}^{\infty}\sum_{|\beta|=n} y^{\alpha-\beta}s_\beta\binom{\alpha}{\beta} = \sum_\beta y^{\alpha-\beta}s_\beta\binom{\alpha}{\beta}. \tag{16}$$

Сравнив (15) с (16), мы видим, что

$$\exp(\Delta)y^\alpha = \exp(D)s_\alpha.$$

Поэтому

$$\exp(\Delta)\rho(u) = \sum_\alpha r_\alpha(u)\exp(\Delta)y^\alpha = \sum_\alpha r_\alpha(u)\exp(D)s_\alpha = \exp(D)u,$$

откуда следует утверждение теоремы.

ЛИТЕРАТУРА

1. *Specht W.* Gesetze in Ringen. I // Math. Z. 1950. Bd 52, N 5. S. 557–589.
2. *Hall M.* A basis for free Lie rings and higher commutators in free groups // Proc. Amer. Math. Soc. 1950. V. 1, N 5. P. 575–581.
3. *Ширшов А. И.* О свободных кольцах Ли // Мат. сб. 1958. Т. 45, № 2. С. 113–122.
4. *Ширшов А. И.* О базах свободной алгебры Ли // Алгебра и логика. 1962. Т. 1, № 1. С. 14–19.
5. *Бокуть Л. А.* База свободных полинильпотентных алгебр Ли // Алгебра и логика. 1963. Т. 2, № 4. С. 13–20.
6. *Reutenauer Ch.* Free Lie algebras. Oxford: Clarendon Press, 1993.

Статья поступила 11 декабря 2002 г.

Гаврилов Алексей Владимирович
Институт вычислительной математики и математической геофизики СО РАН, пр. Академика М. А. Лаврентьева, 6, Новосибирск 630090
gavrilov@lapasrv.sscc.ru