О некоммутативных базисах Грёбнера над кольцами

Е. С. ГОЛОД
Московский государственный университет им. М. В. Ломоносова

УДК 512.664.2+512.713+512.552.4

Ключевые слова: некоммутативные базисы Грёбнера над кольцами, S-многочлены, арифметическое кольцо.

Аннотация

Пусть R — коммутативное кольцо. Доказывается, что для проверки того, что некоторое множество элементов $\{f_\alpha\}$ свободной ассоциативной алгебры над R образует базис Грёбнера (относительно некоторого допустимого порядка на мономах) (двустороннего) идеала, который эти элементы порождают, достаточно проверять редуцируемость к нулю S-многочленов относительно $\{f_\alpha\}$ в том и только том случае, если R — арифметическое кольцо. Обсуждаются также некоторые связанные с этим открытые вопросы и примеры.

Abstract

E. S. Golod, On noncommutative Gröbner bases over rings, Fundamentalnaya i prikladnaya matematika, vol. 10 (2004), no. 4, pp. 91—96.

Let R be a commutative ring. It is proved that for verification whether a set of elements $\{f_\alpha\}$ of the free associative algebra over R is a Gröbner basis (with respect to some admissible monomial order) of the (bilateral) ideal that the elements f_α generate it is sufficient to check reducibility to zero of S-polynomials with respect to $\{f_\alpha\}$ iff R is an arithmetical ring. Some related open questions and examples are also discussed.

Пусть R — коммутативное кольцо (с единицей). В [1] было показано, что если рассматриваются идеалы в кольце многочленов $R[X_1, \ldots, X_n]$, то для проверки того, что некоторое множество многочленов $\{f_\alpha\}$ является базисом Грёбнера (для некоторого допустимого порядка на мономах) порождаемого им идеала, достаточно редуцируемости к нулю S-многочленов относительно $\{f_\alpha\}$ в том и только том случае, если кольцо R арифметическое. Цель настоящей заметки — получить аналогичное утверждение для (двусторонних) идеалов в кольце некоммутативных многочленов (т. е. в свободной ассоциативной алгебре с единицей) над R.

Сначала уточним понятие S-многочлена в рассматриваемой ситуации. Пусть $T = R\langle X_1, \ldots, X_n\rangle$ — свободная ассоциативная алгебра с единицей над R и задан некоторый допустимый порядок на (некоммутативных) мономах от $X_1, \ldots, X_n$. Если $f \in T$, то через $\omega(f)$ обозначается старший член f относительно заданного порядка. Пусть выбраны два элемента $f_1, f_2 \in T$ и $\omega(f_i) = a_i W_i$,

Фундаментальная и прикладная математика, 2004, том 10, № 4, с. 91—96.

где W_i — мономы, $a_i \in R$, $i = 1, 2$. Пусть $\{(\lambda_\alpha^{(1)}, \lambda_\alpha^{(2)})\}$ — некоторое множество порождающих модуля соотношений $\{(\lambda^{(1)}, \lambda^{(2)}) \in R^2 \colon \lambda^{(1)} a_1 + \lambda^{(2)} a_2 = 0\}$ между элементами a_1, a_2. Каждому представлению мономов W_1 и W_2 в виде

$$W_i = MD, \quad W_j = DN \tag{1}$$

или

$$W_i = M' W_j N', \tag{2}$$

где $\{i, j\} = \{1, 2\}$, M, N, D — непустые мономы и M', N' — произвольные мономы, и любому соотношению $\{\lambda_\alpha^{(1)}, \lambda_\alpha^{(2)}\}$ ставится в соответствие, как и в случае, когда R — поле, S-многочлен $\lambda_\alpha^{(i)} f_i N + \lambda_\alpha^{(j)} M f_j$ (соответственно $\lambda_\alpha^{(i)} f_i + \lambda_\alpha^{(j)} M' f_j N'$). Кроме того, в отличие от случая поля, всякому моному M и всякому соотношению $(\lambda_\alpha^{(1)}, \lambda_\alpha^{(2)})$, не являющемуся кратным тривиального соотношения $(a_2, -a_1)$, ставится в соответствие S-многочлен

$$\lambda_\alpha^{(i)} W_j M f_i + \lambda_\alpha^{(j)} f_j M W_i, \quad \{i, j\} = \{1, 2\}.$$

Напомним, что коммутативное кольцо R называется *арифметическим*, если для всякого максимального идеала P в R локализация R_P является кольцом Безу. В [1] было показано, что кольцо R является арифметическим, если и только если для любого семейства элементов $a_1, \ldots, a_k \in R$ модуль соотношений $\{(\lambda_1, \ldots, \lambda_k) \in R^k \colon \lambda_1 a_1 + \ldots + \lambda_k a_k = 0\}$ порождается двучленными соотношениями, т. е. такими, что среди коэффициентов $\lambda_1, \ldots, \lambda_k$ не более двух отличны от нуля. Нам потребуется также следующее утверждение из [2].

Пусть $\{f_i\}_{i \in I}$ — система порождающих идеала J в T, $\omega(f_i) = a_i W_i$ — их старшие члены и

$$z_\beta = \sum_q M_{\beta,q} u_{i_q} N_{\beta,q} -$$

такое множество 1-циклов комплекса Шафаревича $\mathrm{Sh}(\{\omega(f_i)\}_{i \in I}, T)$ (т. е. $\sum\limits_q M_{\beta,q} \omega(f_{i_q}) N_{\beta,q} = 0$), что их образы порождают как T-бимодуль первую группу гомологий этого комплекса. Тогда $\{f_i\}$ является базисом Грёбнера идеала J в том (и только том) случае, если элементы $g_\beta = \sum\limits_q M_{\beta,q} f_{i_q} N_{\beta,q} \in T$ редуцируемы к нулю относительно $\{f_i\}$.

Теорема. *Следующие условия эквивалентны*:

1) R *— арифметическое кольцо*;
2) *для всякого идеала* J *в свободной ассоциативной алгебре*

$$T = R\langle X_1, \ldots, X_n \rangle$$

и допустимого порядка на множестве (*некоммутативных*) *мономов от* $X_1, \ldots, X_n$ *некоторый базис* $\{f_i\}_{i \in I}$ *идеала* J *является его базисом Грёбнера, если* (*и только если*) *все* S*-многочлены для всех пар элементов* $\{f_i, f_j\}$, $i, j \in I$, *редуцируемы к нулю относительно этого базиса.*

Импликация 1) $\Longrightarrow$ 2) непосредственно вытекает из следующей леммы, которая обобщает на случай свободной ассоциативной алгебры над арифметическим кольцом известное, когда R — поле, описание системы порождающих бимодуля 1-гомологий комплекса Шафаревича для семейства мономов.

Лемма. *Пусть R — арифметическое кольцо, $T = R\langle X_1, \ldots, X_n\rangle$ — свободная ассоциативная алгебра, W_i, $i \in I$, — некоммутативные мономы от $X_1, \ldots, X_n$ и $a_i \in R$. Для каждой пары $i, j \in I$ рассмотрим всевозможные представления мономов W_i, W_j в виде* (1) *и* (2) *и некоторое множество порождающих $\{(\lambda_\alpha^{(i)}, \lambda_\alpha^{(j)})\}$ модуля соотношений между a_i и a_j. Поставим в соответствие каждому представлению вида* (1) (*вида* (2)) *и соотношению $(\lambda_\alpha^{(i)}, \lambda_\alpha^{(j)})$ цикл $\lambda_\alpha^{(i)} u_i N + \lambda_\alpha^{(j)} M u_j$* (*соответственно $\lambda_\alpha^{(i)} u_i + \lambda_\alpha^{(j)} M' u_j N'$*). Кроме того, всякому моному M и всякому соотношению $(\lambda_\alpha^{(i)}, \lambda_\alpha^{(j)})$, не являющемуся кратным тривиального соотношения $(a_j, -a_i)$, поставим в соответствие цикл $\lambda_\alpha^{(i)} W_j M u_i + \lambda_\alpha^{(j)} u_j M W_i$. Множество классов гомологий получаемых таким образом циклов порождает T-бимодуль 1-гомологий комплекса Шафаревича*

$$\mathrm{Sh}(\{a_i W_i\}_{i\in I}, T).$$

Доказательство. Рассмотрим некоторый 1-цикл

$$z = \sum_{q=1}^{m} \lambda_q M_q u_{i_q} N_q,$$

где M_q, N_q — мономы, $\lambda_q \in R$. Этот цикл можно считать однородным в том смысле, что $M_q W_{i_q} N_q$ — один и тот же моном для всех q; этот моном мы называем *степенью однородного цикла z*. Покажем сначала, что R-модуль однородных циклов фиксированной степени порождается двучленными циклами, т. е. с $m \leqslant 2$. То, что z является циклом, означает, что $\sum\limits_{q=1}^{m} \lambda_q a_{i_q} = 0$. Так как кольцо R арифметическое, это соотношение между элементами a_{i_q} является суммой двучленных соотношений, и тем самым цикл z является суммой двучленных циклов. Пусть теперь цикл z двучленный:

$$z = \lambda_i M_i u_i N_i + \lambda_j M_j u_j N_j.$$

Соотношение (λ_i, λ_j) является линейной комбинацией выбранных порождающих соотношений между a_i, a_j, и можно считать, что оно одно из них. С точностью до умножения слева и справа на моном можно считать, что M_i или M_j и N_i или N_j являются пустыми мономами. Но тогда цикл z совпадает с одним из циклов, указанных в формулировке леммы, или является границей, если в мономе $M_i W_i N_i = M_j W_j N_j$ подмономы W_i и W_j не пересекаются и соотношение (λ_i, λ_j) кратно тривиальному. Тем самым лемма доказана. □

Импликация 1) $\Longrightarrow$ 2) следует из того, что для порождающих циклов, указанных в лемме, соответствующие элементы g в точности совпадают с S-многочленами.

Импликация 2) $\Longrightarrow$ 1) доказана в [1], так как, если кольцо R не является арифметическим, там указан идеал в кольце многочленов от одной переменной над R, не удовлетворяющий условию 2).

Отметим одно существенное отличие ситуации с некоммутативными базисами Грёбнера, когда коэффициенты берутся из коммутативного кольца, не являющегося полем, как от аналогичной коммутативной ситуации, так и от некоммутативной ситуации в случае коэффициентов из поля. В двух последних ситуациях, если задан некоторый конечный базис идеала, то имеется лишь конечный запас S-многочленов и тем самым эффективно проверяется, является ли данный базис базисом Грёбнера (в коммутативной ситуации здесь предполагается, что кольцо коэффициентов нётерово и над ним конечные системы порождающих модулей соотношений эффективно вычислимы). В некоммутативном случае даже над кольцом целых чисел (или кольцом дискретного нормирования) нужно рассматривать бесконечное множество S-многочленов. Остаётся открытым вопрос, можно ли и в этой ситуации эффективно указать некоторый конечный набор S-многочленов, для которых достаточно проверять редуцируемость к нулю. То, что недостаточно рассматривать лишь «классические» S-многочлены, показывают простейшие примеры.

Пример 1. В свободной ассоциативной алгебре $\mathbb{Z}\langle X, Y, Z\rangle$ рассмотрим идеал, порождённый элементами $2YZ + X$, $2XZ$, и лексикографически-степенной порядок на мономах, при котором $X > Y > Z$. В $\mathbb{Q}\langle X, Y, Z\rangle$ указанные элементы образуют базис Грёбнера порождаемого ими идеала. В то же время в $\mathbb{Z}\langle X, Y, Z\rangle$ они порождают идеал, не имеющий конечного базиса Грёбнера.

Сформулированный выше вопрос имеет некоторый аналог в классической ситуации базисов Грёбнера для идеалов в кольце (коммутативных) многочленов $R = K[X_1, \ldots, X_n]$ над полем K. Пусть идеал $J \subset R$ порождается многочленами $f_1, \ldots, f_k$ и a_iM_i — их старшие члены, где $a_i \in K$ и M_i — мономы. Хорошо известно так называемое *правило треугольника*: если наименьшее общее кратное $M_1N_{13} = M_3N_{31}$ мономов M_1, M_3 делится на наименьшие общие кратные $M_1N_{12} = M_2N_{21}$ и $M_2N_{23} = M_3N_{32}$ соответственно мономов M_1, M_2 и M_2, M_3, то можно не проверять редуцируемость к нулю S-многочлена, соответствующего паре f_1, f_3. Это немедленно следует из того, что класс гомологий цикла

$$z_{13} = a_3N_{13}e_1 - a_1N_{31}e_3$$

в модуле гомологий $H_1(\{a_iM_i\}, R)$ комплекса Козюля $K(\{a_iM_i\}, R)$ содержится в подмодуле, порождённом классами гомологий циклов

$$z_{12} = a_2N_{12}e_1 - a_1N_{21}e_2 \quad \text{и} \quad z_{23} = a_3N_{23}e_2 - a_2N_{32}e_3.$$

Действительно,

$$z_{13} = \frac{a_3}{a_2}\frac{N_{13}}{N_{12}}z_{12} + \frac{a_1}{a_2}\frac{N_{31}}{N_{32}}z_{23},$$

так как $N_{13}N_{21}N_{32} = N_{12}N_{23}N_{31}$. Вопрос состоит в следующем. Пусть задан конечный набор мономов $\{M_i\}$ в R. Может ли существовать такое множество J

пар $\{i,j\}$, что классы гомологий соответствующих им циклов порождают собственный R-подмодуль в $H_1(\{M_i\},R)$, но тем не менее для любого набора многочленов $\{f_i\}$ со старшими членами M_i из редуцируемости к нулю S-многочленов, соответствующих парам $\{i,j\}\in J$, следует редуцируемость к нулю всех остальных S-многочленов, т. е. следует, что многочлены $\{f_i\}$ образуют базис Грёбнера порождаемого ими идеала. Имеются два варианта этого вопроса: можно требовать, чтобы J обладало указанным свойством для любого допустимого порядка на мономах или только при некотором фиксированном порядке. Следующий простой пример показывает, что по крайней мере в последнем варианте ответ на этот вопрос может быть положительным.

Пример 2. В кольце $R=K[X_1,X_2,X_3]$ рассмотрим мономы $M_1=X_3^2$, $M_2=X_1X_3$, $M_3=X_2X_3$ и множество $J=\{\{1,2\},\{2,3\}\}$. Классы гомологий циклов $z_{12}=X_1e_1-X_3e_2$ и $z_{23}=X_2e_2-X_1e_3$ порождают собственный подмодуль в $H_1(M_1,M_2,M_3;R)$. Рассмотрим лексикографически-степенной порядок на мономах, при котором $X_1>X_2>X_3$. Тогда для любых f_1, f_2, f_3 из редуцируемости к нулю S-многочленов, соответствующих z_{12} и z_{23}, следует, что S-многочлен, соответствующий z_{13}, тоже редуцируем к нулю. Более того, из выполнения априори более слабого условия поднимаемости (в смысле [2]) циклов z_{12} и z_{23} следует поднимаемость цикла z_{13}, а потому и редуцируемость к нулю соответствующего S-многочлена.

В заключение, в связи с изложенным выше, сформулируем ещё один вопрос, относящийся к случаю свободной ассоциативной алгебры $T=K\langle X_1,\ldots,X_n\rangle$ над полем K. Пусть задан некоторый мономиальный идеал в T (не обязательно конечно порождённый); при каких условиях он является идеалом старших членов (относительно произвольного или некоторого допустимого порядка на мономах) некоторого конечно порождённого идеала в T? Если мономиальный идеал задан эффективно, то можно поставить вопрос о существовании алгоритма, выясняющего, существует ли такой конечно порождённый идеал. Ниже обсуждаются некоторые простейшие примеры.

Пример 3. Мономиальный идеал в $K\langle X,Y\rangle$, порождённый множеством $\{XYX^nY^2\mid n\geqslant 0\}$, и мономиальный идеал в $K\langle X,Y,Z\rangle$, порождённый множеством $\{XY^nZ\mid n\geqslant 0\}$, не являются идеалами старших членов никакого конечно порождённого идеала при любом допустимом порядке на мономах. Действительно, если бы такой конечно порождённый идеал существовал, то из системы его порождающих с указанными старшими членами можно было бы выбрать конечную систему порождающих и эта конечная система уже была бы базисом Грёбнера этого идеала.

Пример 4. Если мономиальный идеал имеет минимальную систему порождающих $\{M_1,M_2,\ldots\}$, такую что $\deg M_k=d_k$ и $d_{k+1}>2d_k-1$, то он не является идеалом старших членов никакого конечно порождённого идеала относительно любого допустимого порядка на мономах, учитывающего степень (т. е. для двух мономов $M>N$, если $\deg M>\deg N$). Действительно, такой идеал порождался бы некоторой конечной системой элементов $f_1,\ldots,f_k$ со

старшими членами $M_1, \dots, M_k$ и любой S-многочлен, имея степень $\leqslant 2d_k - 1$, редуцировался бы к нулю относительно $f_1, \dots, f_k$.

Пример 5. Мономиальный идеал в $K\langle X, Y\rangle$, порождённый множеством $\{XY^nX \mid n \geqslant 0\}$, является идеалом старших членов конечно порождённого идеала при любом допустимом порядке на мономах. Если $X > Y$, то можно взять идеал, порождённый элементом $X^2 - YX$, а если $Y > X$, то идеал, порождённый элементами $X^2 - X$ и $XYX - YX$. Более общо, базис Грёбнера идеала, порождённого элементами $XY^kX - Y^mX$ и $XY^lX - Y^nX$, где $m - k = n - l$, имеющими в качестве старших членов соответственно XY^kX и XY^lX (в случае $m > k$ это равносильно тому, что $X > Y^{m-k}$), состоит из всех элементов вида

$$XY^{k+sm+(t+1)n}X - Y^{(s+1)m+(t+1)n}X,$$
$$XY^{k+sm}X - Y^{(s+1)m}X, \quad XY^{l+tn}X - Y^{(t+1)n}X,$$

где s, t — любые неотрицательные целые числа.

Литература

[1] Голод Е. С. Арифметические кольца, биэндоморфизмы и базисы Грёбнера // Успехи мат. наук. — 2005. — Т. 60, № 1.

[2] Golod E. S. Standard bases and homology // Lect. Notes Math. Vol. 1352. — 1988. — P. 105—110.