L. A. Bokut', Unsolvability of certain algorithmic problems in a class of associative rings,
Algebra Logika, 1970, Volume 9, Number 2, 137–144

Алгебра и логика, 9, № 2 (1970), 137-144.

УДК 519.48

НЕРАЗРЕШИМОСТЬ НЕКОТОРЫХ АЛГОРИТМИЧЕСКИХ ПРОБЛЕМ В КЛАССЕ АССОЦИАТИВНЫХ КОЛЕЦ

Л.А.БОКУТЬ

1. Абстрактное свойство α конечно определенных (к.о.) полугрупп (групп) называется марковским свойством, если существует хотя бы одна к.о. полугруппа (группа), обладающая свойством α, и хотя бы одна к.о. полугруппа (группа), не вложимая ни в какую к.о. полугруппу (группу) со свойством α. В работах [1]-[3] доказано, что марковские свойства к.о. полугрупп и групп алгоритмически нераспознаваемы. Цель настоящей заметки состоит в том, чтобы доказать аналогичный факт для к.о. ассоциативных колец и алгебр.

2. Пусть Ω – коммутативное кольцо с единицей. Слово "алгебра" будет означать ассоциативную унитарную Ω-алгебру. Через $\Omega[X]$, X – некоторое множество, будем обозначать свободную Ω-алгебру (без единицы) с множеством X свободных порождающих, то есть алгебру многочленов (без свободных членов) от X над Ω. Пусть $\Phi \subseteq \Omega[X]$. Говорят, что алгебра R задается множеством порождающих X и множеством определяющих соотношений Φ:

$$R = \langle X; \Phi \rangle, \qquad (1)$$

если $R \cong \Omega[X]/(\Phi)$, где (Φ)-идеал, порожденный Φ. Алгебру (1) называем конечно определенной, если множества X и Φ конечны.

В дальнейшем мы будем употреблять понятие свободного произведения Ω-алгебр. Так как это понятие в случае, когда кольцо Ω не является полем, встречается довольно редко, приведем соответствующее определение. Пусть R_α, $\alpha \in \mathcal{I}$,-некоторое семейство Ω-алгебр. Как и в случае алгебр над полем, следующие три определения равносильны.

ОПРЕДЕЛЕНИЕ 1. Свободным произведением $R = \prod^*_{\alpha\in J} R_\alpha$ алгебр называется алгебра, содержащая алгебры R_α, порождаемая этими алгебрами и такая, что любые гомоморфизмы

$$\varphi_\alpha : R_\alpha \to S, \alpha\in J, \tag{2}$$

где S - некоторая алгебра, можно продолжить до гомоморфизма $\varphi : R \to S$.

Легко показать, что алгебра R, удовлетворяющая этому определению, единственна.

ОПРЕДЕЛЕНИЕ 2. Зададим алгебры R_α образующими и определяющими соотношениями:

$$R_\alpha = <\Sigma_\alpha ; \Phi_\alpha>, \alpha\in J,$$

где мы считаем, что $\Sigma_\alpha \cap \Sigma_\beta = \varnothing$, если $\alpha \neq \beta$. Назовем свободным произведением алгебр R_α следующую алгебру:

$$R = <\bigcup_{\alpha\in J} \Sigma_\alpha ; \bigcup_{\alpha\in J} \Phi_\alpha>.$$

ОПРЕДЕЛЕНИЕ 3. Рассмотрим абелевы группы

$$R_{i_1 \dots i_k} = R_{i_1} \otimes R_{i_2} \otimes \dots \otimes R_{i_k}, \tag{3}$$

где $k \geqslant 1$, $i_1,\dots,i_k \in J$ и любые два соседних индекса не совпадают (тензорное произведение берется над Ω). Так как Ω - коммутативное кольцо, то группы $R_{i_1\dots i_k}$ можно естественным образом рассматривать как левые (и правые) Ω -модули. Возьмем прямую сумму этих модулей

$$R = \sum_{k\geqslant 1} \oplus R_{i_1 \dots i_k},$$

где сумма берется по всем последовательностям $i_1,\dots,i_k$, удовлетворяющим высказанному после (3) условию. Определим в модуле R произведение обычным образом:

$$r_{i_1}\dots r_{i_k} \cdot r_{j_1} \dots r_{j_s} = \begin{cases} r_{i_1}\dots r_{i_k} r_{j_1} \dots r_{j_s}, & \text{если } i_k \neq j_1, \\ \\ r_{i_1}\dots r_{i_{k-1}} (r_{i_k} r_{j_1}) r_{j_2} \dots r_{j_s}, & \text{если } i_k = j_1, \end{cases}$$

где $r_{i_e} \in R_{i_e}, r_{j_e} \in R_{j_e}$. Этим модуль R превращается в ассоциативную алгебру над R. Назовем алгебру R свободным произведением алгебр R_α.

Отметим следующее свойство свободного произведения алгебр. Пусть алгебры $R_\alpha, \alpha \in \mathcal{J}$, являются свободными Ω -модулями. Тогда алгебра $R = \prod^*_{\alpha \in \mathcal{J}} R_\alpha$ -также свободный Ω -модуль. Именно, если $\{a_{\beta\alpha}, \beta \in \mathcal{J}_\alpha\}$ - базы модулей R_α, то множество

$$\{a_{\beta_1\alpha_1} \ldots a_{\beta_k\alpha_k}, \ \alpha_i \neq \alpha_{i+1}, \ 1 \leqslant i \leqslant k-1, \ k \geqslant 1\}$$

является базой модуля R. Это следует из определения 3 и справедливости соответствующего утверждения для тензорного произведения модулей (см., например, [4]).

3. Пусть R - Ω-алгебра, которая является свободным Ω -модулем. Элемент $a \in R$ будем называть примитивным элементом, если его можно включить в некоторую базу модуля R.

ЛЕММА. Пусть R - к.о. алгебра, являющаяся свободным модулем над Ω, a - её произвольный примитивный элемент или нуль. Тогда можно эффективно построить к.о. алгебру $R(a)$, удовлетворяющую следующим условиям: если $a = 0$, то $R(a) = 0$; если $a \neq 0$, то алгебра R является подалгеброй алгебры $R(a)$.

ДОКАЗАТЕЛЬСТВО. Пусть

$$R = \langle \Sigma ; \Phi \rangle,$$

где $\Sigma = \{a_1, \ldots, a_n\}$, $n \geqslant 2$, Φ - конечное подмножество з $\Omega[\Sigma]$. Рассмотрим свободную алгебру

$$F = \Omega[x_1, x_n, y_1, \ldots, y_n]$$

и образуем свободное произведение $R' = F * R$. Далее, рассмотрим идеал N алгебры R', порожденный элементами:

$$x_i a y_i - a_i, \ x_{i+1} x_i a y_{i+1} - x_i, \ x_{i+2} x_i a y_{i+1} - y_i,$$

где $1 \leqslant i \leqslant n$, $x_{n+e} = x_e$, $e = 1, 2, y_{n+1} = y_1$. Положим

$$R(a) = F * R / N.$$

Если $a=0$, то понятно, что $R(a)=0$. Пусть $a\neq 0$. Рассмотрим в алгебре R некоторую базу $\{b_\alpha, \alpha\in J\}$, содержащую элемент a. Ввиду свойства, высказанного в предыдущем пункте, следующее множество элементов образует базу алгебры $F*R$:

$$\mathfrak{M}=\{z_{i_1}\ldots z_{i_k},\ k\geqslant 1\},$$

где $z_i=b_\alpha$, или $z_i=x_j$, или $z_i=y_j$; при этом в выражении $z_{i_1}\ldots z_{i_k}$ рядом не стоят элементы алгебры R. Элементы множества $\mathfrak{M}$ будем называть **базисными словами** алгебры $F*R$. Определим понятие длины базисных слов следующим образом:

$$\ell(z_{i_1}\ldots z_{i_k})=k.$$

Предположим теперь, что естественный гомоморфизм $R\to R(a)$ не является мономорфизмом. Тогда существует элемент $b\in R$, $b\neq 0$, такой, что $b\in N$ в алгебре $F*R$. Это означает, что справедливо равенство

$$b=\Sigma\alpha_{ij}c_{ij}(x_i a y_i-a_i)d_{ij}+\Sigma\beta_{ij}e_{ij}(x_{i+1}x_i a y_{i+1}-x_i)f_{ij}+$$
$$+\Sigma\gamma_{ij}g_{ij}(x_{i+2}x_i a y_{i+1}-y_i)h_{ij}, \tag{4}$$

где $\alpha_{ij},\beta_{ij},\gamma_{ij}\in\Omega$, и без ограничения общности можно считать, что элементы $c_{ij},\ldots,h_{ij}$ - базисные слова (некоторые из них, возможно, пустые). Кроме того, будем считать, что слова c_{ij}, e_{ij}, g_{ij} не содержат подслов:

$$x_k a y_k,\ x_{k+1}x_k a y_{k+1},\ x_{k+2}x_k a y_{k+1},\ 1\leqslant k\leqslant n. \tag{5}$$

Пусть, например, слово c_{ij} содержит некоторое подслово вида (5). Выделим в c_{ij} первое вхождение такого слова. Пусть это будет вхождение слова $x_{k+1}x_k a y_{k+1}$:

$$c_{ij}\equiv c'x_{k+1}x_k a y_{k+1}c'',$$

где c' не содержит подслов вида (5). Преобразуем элемент $c_{ij}(x_i a y_i-a_i)d_{ij}$ следующим образом:

$$c_{ij}(x_i a y_i-a_i)d_{ij}=c'(x_{k+1}x_k a y_{k+1}-x_k)c'''+$$
$$+c'x_k c''(x_i a y_i-a_i)d_{ij}, \tag{6}$$

где $c''' = c''(x_i a y_i - a_i) d_{ij}$. Понятно, что длина слова $c' x_k c''$ меньше длины слова c_{ij}. Отсюда следует, что с помощью преобразований вида (6) правую часть равенства (4) можно привести к виду, удовлетворяющему высказанному выше условию.

Далее, будем считать, что в правой части равенства (4) все подобные члены приведены в том смысле, что, например, $(c_{ij}, d_{ij}) \neq$ $\neq (c_{ik}, d_{ik})$ при $j \neq k$.

Покажем теперь, что в правой части равенства (4) все суммы пустые (то есть правая часть (4) есть нуль). Предположим противное. Рассмотрим в правой части (4) некоторое базисное слово u наибольшей длины. Таким словом может быть одно из слов вида

$$c_{ij} x_i a y_i d_{ij}, e_{ij} x_{i+1} x_i a y_{i+1} f_{ij}, g_{ij} x_{i+2} x_i a y_{i+1} h_{ij}. \tag{7}$$

Слово u должно иметь себе подобное в правой части равенства (4), так как $\ell(u) > 1$ (длина слов в левой части равенства (4) равна единице). Пусть, например, выделенное слово u есть слово $c_{ij} x_i a y_i d_{ij}$. Если

$$u = c_{k\ell} x_k a y_k d_{k\ell},$$

то либо $c_{ij} \equiv c_{k\ell}$, $d_{ij} \equiv d_{k\ell}$, либо одно из слов $c_{ij}, c_{k\ell}$ содержит подслово $x_m a y_m$. Оба эти случая по условию невозможны. Если

$$u = e_{k\ell} x_{k+1} x_k a y_{k+1} f_{k\ell},$$

то так как $y_{k+1} \neq y_k$ (ввиду условий $n \geqslant 2$) из предыдущего равенства получаем, что либо слово c_{ij} содержит подслово $x_{k+1} x_k a y_{k+1}$, либо слово $e_{k\ell}$ содержит подслово $x_i \quad y_i$, что невозможно. Случай

$$u = g_{k\ell} x_{k+2} x_k a y_{k+1} h_{k\ell}$$

рассматривается так же, как и предыдущий.

Наконец, если u – другое слово из числа слов (7), то все рассуждения вполне аналогичны.

Полученные противоречия показывают, что если $a \neq 0$, то $\ell \subseteq R(a)$.

Нам остается заметить, что построенная алгебра $R(a)$ является конечно определенной. Лемма доказана.

4. Пусть α - некоторое абстрактное свойство к.о. Ω -алгебр. Мы будем рассматривать вопрос об алгоритмической распознаваемости свойства α. Как всегда в таких случаях, этот вопрос требует уточнения на языке теории алгоритмов. С этой целью будем считать, что Ω - счетное кольцо с фиксированной системой порождающих $\omega_1, \omega_2, \ldots, \omega_n, \ldots$. После этого можно определить эффективную нумерацию всех к.о. Ω -алгебр (считая, что порождающие элементы всех к.о. Ω -алгебр берутся из некоторого счетного множества $a_1, a_2, \ldots, a_n, \ldots$), и вопрос о распознаваемости свойства α уточняется как вопрос о рекурсивности множества номеров к.о. Ω -алгебр, обладающих свойством α.

ТЕОРЕМА. *Пусть α - абстрактное свойство к.о. алгебр, удовлетворяющее условиям: существует хотя бы одна к.о. алгебра R_1 со свойством α и существует хотя бы одна к.о. алгебра R_2, являющаяся свободным Ω-модулем и не вложимая ни в какую к.о. алгебру со свойством α. Тогда свойство α алгоритмически нераспознаваемо.*

ДОКАЗАТЕЛЬСТВО. Пусть

$$\Pi_0 = \langle\langle \Sigma_0 ; A_i = B_i , \ 1 \leq i \leq k \rangle\rangle \quad -$$

к.о. полугруппа с неразрешимой проблемой тождества, $R_0 = \Omega(\Pi_0)$- полугрупповая алгебра полугруппы Π_0 над кольцом Ω. Алгебра R_0 является к.о. алгеброй, свободным Ω -модулем, и в этой алгебре выполняется равенство $A - B = 0$, где A, B - слова от Σ_0, тогда и только тогда, когда $A = B$ в Π_0. Далее, элемент $a = A - B$ является примитивным элементом алгебры R_0 или нулем. Рассмотрим алгебру $R_2 * R_0$ и произвольный элемент этой алгебры вида $a = A - B, A, B$ - слова от Σ_0. Из предыдущего следует, что алгебра $R_2 * R_0$ и элемент a удовлетворяют условиям леммы из п.3. Образуем согласно этой лемме алгебру $(R_2 * R_0)(a)$. Тогда ясно, что к.о. алгебра

$$R_1 * (R_2 * R_0)(a)$$

обладает свойством α тогда и только тогда, когда $a=A-B=0$ в R_0, то есть $A=B$ в Π_0. Последний вопрос, как мы предположили, алгоритмически нераспознаваем. Это доказывает теорему.

СЛЕДСТВИЕ. Любое марковское свойство к.о. алгебр над полем алгоритмически нераспознаваемо.

Приведем примеры свойств, удовлетворяющих условиям теоремы: коммутативность, нильпотентность, свойство быть ниль-алгеброй, свойство быть PJ-алгеброй (с тождественным соотношением), свойство быть конечномерной алгеброй (если Ω – поле), свойство быть алгеброй без делителей нуля (если Ω – без делителей нуля), свойство быть вложимой в тело (если Ω – без делителей нуля) и т.д.

Отметим, что аналогичным способом могут быть доказаны следующие утверждения: если над кольцом Ω существует хотя бы одна к.о. простая алгебра, то свойство быть простой алгеброй алгоритмически нераспознаваемо (в частности, нераспознаваемо свойство быть простым кольцом (Ω – целые числа) и свойство быть простой алгеброй над полем); если над кольцом Ω существует хотя бы одна к.о. полупростая в смысле Джекобсона) алгебра, то свойство быть полупростой алгеброй алгоритмически нераспознаваемо (случай колец и алгебр над полем здесь содержится).

В заключение отметим, что в классе всех (неассоциативных) алгебр и в классе всех коммутативных (неассоциативных) алгебр утверждение, аналогичное доказанной выше теореме, уже не выполняется: это следует из того, что свойство быть нулевой алгеброй (н[illegible] полем) является марковским, но тем не менее в указанных классах алгебр оно распознаваемо (следует из разрешимости в этих классах алгебр проблемы тождества – см. [5], [6]).

Литература

1. А.А.МАРКОВ, Невозможность алгорифмов распознавания некоторых свойств ассоциативных систем, Доклады АН СССР, 77 № 6 (1951), 953-956.

2. С.И.АДЯН, Неразрешимость некоторых алгоритмических проблем в теории групп, Труды Москов.матем.об-ва, 6(1957), 231-298.

3. M.RABIN, Recursive unsolvability of group theoretic problems, Ann. of Math., 67(1958), 172-194.

4. Н.ДЖЕКОБСОН, Строение колец, М., Мир, 1961.

5. А.И.ЖУКОВ, Приведенные системы определяющих соотношений в неассоциативных алгебрах, Матем.сб., 27 (1950), 267-280.

6. А.И.ШИРШОВ, Некоторые алгоритмические проблемы для ε - алгебр, Сиб.матем.журнал, 3, № 1 (1962), 132-137.

Поступило 25 ноября 1969 г.