СИБИРСКИЙ МАТЕМАТИЧЕСКИЙ ЖУРНАЛ
Т. 32, № 6 НОЯБРЬ — ДЕКАБРЬ 1991

УДК 519.48

Памяти А. И. Ширшова посвящается

И. И. ДУБРОВИН

О РАЦИОНАЛЬНОМ ЗАМЫКАНИИ ГРУППОВОЙ АЛГЕБРЫ ЛИНЕЙНО УПОРЯДОЧЕННОЙ ГРУППЫ В ТЕЛЕ РЯДОВ МАЛЬЦЕВА

Рассмотрим скрещенное групповое кольцо $S = KG$ тела K с линейной упорядоченной группой G [1]. Обозначим через $K\{G\}$ множество формальных степенных рядов вида

$$a = \sum_{g \in G} k_g g \tag{1}$$

с вполне упорядоченным по возрастанию носителем $\operatorname{supp} a$. Известно, что естественным образом введенные операции сложения и умножения на множестве $K \setminus \{G\}$ превращают последнее в тело, содержащее $K \setminus G$ как подкольцо [1, 2]. Для любого элемента a вида (1), не равного нулю, существует наименьший элемент h его носителя. Обозначим $v(a) = h$ и назовем этот элемент *нормой ряда* a. По определению полагаем $v(0) = \infty$. Заметим, что отображение $v\colon K \setminus \{G\} \to (G, \infty)$ будет нормированием [3, гл. VI].

Перейдем к определению конструктивной алгебраической системы U сигнатуры σ. За основными определениями теории алгебраических систем отсылаем к книгам [4, 5]. Операции из σ предполагаются, вообще говоря, частичными. В дальнейшем в качестве «универсального» конструктивного множества выбираем множество слов в некотором достаточно большом алфавите, содержащем и редакционные буквы — скобки, запятые и т. п., а в качестве математической реализации идеи конструктивной процедуры — нормальные алгорифмы Маркова (см. [6]). Символ λ означает пустое слово.

Определение 1. Алгебраическую систему $\langle U, \sigma\rangle$ назовем *конструктивной*, если найдутся рекурсивное словарное множество W и наложение $\psi\colon W \to U$ такие, что а) существует алгоритм распознавания равенства $\psi(a) = \psi(b)$ для элементов $a, b \in W$; б) для каждой n-арной операции $f \in \sigma$ существует алгорифм $\mathscr{F}$, применяемый к любой строке $(a_1, \ldots, a_n)$, где $a_i \in W$, причем

$$\mathscr{F}(a_1, \ldots, a_n) = \begin{cases} \lambda, & \text{если } f(\psi(a_1), \ldots, \psi(a_n)) \text{ не определено,} \\ b, & \text{где } b \in W \text{ и } \psi(b) = f(\psi(a_1), \ldots, \psi(a_n)); \end{cases}$$

в) для каждого n-арного отношения $r \in \sigma$ существует алгорифм $\mathscr{R}$, применяемый к любой строке $(a_1, \ldots, a_n)$ и выясняющий, находятся или нет элементы $\psi(a_1), \ldots, \psi(a_n)$ в отношении r.

Заметим, что определение 1 лишь формой отличается от определения Мальцева [7] конструктивной алгебраической системы. Эквивалентную формулировку можно найти также в дополнении к книге [8], написанном Ю. Л. Ершовым.

Если D — S-тело, то через $\Sigma(D)$ обозначим множество квадратных, не вырожденных над D матриц с элементами из кольца S. Дополнение

множества $\Sigma(D)$ до множества всех квадратных матриц над S обозначим через $m(D)$. В связи с этими обозначениями, а также понятиями тела частных, локализующего множества матриц и т. п., отсылаем к книге [9].

Следующие обозначения сохраняются на протяжении всей работы: R — подкольцо в S, состоящее из элементов $k_1g_1+\ldots+k_ng_n$ таких, что $g_i \geqslant 1$ для любого i (здесь $k_i \in K$, $g_i \in G$, 1 — единица группы G); J — идеал в R, состоящий из элементов r, норма которых больше 1; π: $R \mapsto R$ — проекция на тело K, соответствующая разложению в полупрямую сумму $R = K \oplus J$; $\operatorname{Div} S$ — рациональное замыкание кольца S в теле $K\{G\}$ (см. [9, гл. 7]); $\Sigma = \Sigma(\operatorname{Div} S)$; Σ_0 — множество квадратных матриц A над R таких, что $\pi(A)$ не вырождена над телом K; e, f — элементы стандартного базиса S-модуля строк и столбцов соответственно. Заметим, что $\Sigma_0 \subseteq \Sigma$.

Основным результатом работы является

Теорема 1. *Пусть тело* $K(+, \cdot, {}^{-1}, 0, 1)$, *линейно упорядоченная группа* $G(\cdot, {}^{-1}, 1, \leqslant)$, *а также система факторов и автоморфизмов, задающих кольцо* S, *конструктивны. Тогда существует алгорифм, применяемый к любой записи вида* $pA^{-1}q$ (p — строка, q — столбец, A — матрица над S), *который выясняет принадлежность* A *множеству* Σ *и в случае* $A \in \Sigma$ *перерабатывает эту запись в* 0, *если* $pA^{-1}q = 0$ *в теле* $\operatorname{Div} S$, *или в запись*

$$geC^{-1}f, \tag{2}$$

где $g \in G$, $C \in \Sigma_0$, $e\pi(C)^{-1}f \neq 0$ *и элементы тела* $\operatorname{Div} S$, *соответствующие записям* (2) *и* $pA^{-1}q$, *равны.*

Следствиями этой теоремы являются утверждения: а) тело $\operatorname{Div} S$ конструктивно; б) нормирование v: $\operatorname{Div} S \to (G, \infty)$ конструктивно; в) отображение $\operatorname{Div} S \to (K, \infty)$, задающее точку тела $\operatorname{Div} S$, соответствующую нормированию v, конструктивно.

Из известных результатов в этом направлении следует отметить прежде всего работы по конструктивным полям (см. дополнение Ю. Л. Ершова к [8]), а также работу [10], основной результат которой представляет частный случай теоремы 1 (рассматривается случай, когда G — свободная группа, а S — групповое кольцо).

Запись вида (2) с условием $e\pi(C)^{-1}f \neq 0$, а также символ 0 будем называть *каноническими.*

§ 1. Предварительные результаты

Элементы $s_1, \ldots, s_k$ архимедовой линейно упорядоченной группы G называются *независимыми*, если из равенства $s_1^{z_1} \ldots s_k^{z_k} = 1$ ($z_i \in \mathbf{Z}$) следует, что все числа z_i равны нулю.

Лемма 1. *Пусть* $1 < g_1 < g_2 < \ldots < g_m$ — *элементы линейно упорядоченной архимедовой группы* G. *Существуют независимые элементы* $s_1, \ldots, s_k$ *группы* G *такие, что* а) $k \leqslant m$; б) *каждый* g_j *выражается через* $s_i, \ldots, s_k$ *в виде произведения степеней с неотрицательными показателями;* в) $1 < s_1 < s_i < s_1^2$ *для всех* i, $2 \leqslant i \leqslant k$.

Доказательство. Если элементы g_i независимы, то достаточно сделать замену $s_i = g_1^{-n_i}g_i$, $2 \leqslant i \leqslant m$, $s_1 = g_1$, где неотрицательные числа n_i выбираются так, что $g_1 < s_i < g_1^2$. Существование таких чисел обеспечивается архимедовостью группы G. Пусть

$$g_1^{z_1}g_2^{z_2} \ldots g_m^{z_m} = 1 \tag{3}$$

— нетривиальная зависимость. Доказательство утверждения леммы проведем индукцией по вполне упорядоченному лексикографически множеству $\mathbf{N} \times \mathbf{N}$. Элементам g_i с зависимостью (3) сопоставим пару (m, ξ), где $\xi = |z_1| + |z_2| + \ldots + |z_m|$ назовем *характеристикой зависимости* (3).

Можно считать, что все z_i отличны от нуля и $z_1 > 0$. Наша ближайшая цель — выбрать индексы $1 \leqslant i_1 < i_2 \ldots i_t \leqslant m$ так, чтобы замена g_i на $h_i = g_{i_1}^{-1} g_i$, если $i = i_\nu$ и $\nu \neq 1$, и на $h_i = g_i$ в противном случае привела к зависимости над h_i с меньшей характеристикой. Легко понять, что h_i удовлетворяют п. б) и зависимость (3) переходит в зависимость над h_i с характеристикой, отличающейся от ξ на величину

$$\varepsilon = |z_{i_1} + z_{i_2} + \ldots + z_{i_t}| - |z_{i_1}|. \tag{4}$$

Пусть $(z_1 z_2 \ldots z_m) = \alpha_1 * \alpha_2 * \ldots * \alpha_p$ — разбиение такое, что в строке α_j все числа имеют тот же знак, что и $(-1)^{j+1}$; $*$ обозначает операцию катенации. Пусть $|\alpha_j|$ — сумма чисел в строке α_j; a_j — первое из чисел строки a_j; $g(\alpha_j)$ — произведение $g_i^{z_i}$, соответствующих строке α_j.

Предположим ,что для любого набора индексов $\{i_\nu\}$ величина ε неотрицательна. Тогда $|\alpha_j| < |a_{j+1}|$ для любого j, $1 \leqslant j \leqslant p-1$. В этом случае из линейной упорядоченности элементов g_i вытекает, что модуль элемента $g(\alpha_j)$ меньше модуля первого сомножителя в $g(\alpha_{j+1})$ и тем более меньше модуля $g(\alpha_{j+1})$. Предположим, что $p = 2q$. Тогда $g(\alpha_{2j-1}) g(\alpha_{2j}) < 1$ $(1 \leqslant j \leqslant q)$, и поэтому $1 = (g(\alpha_1) g(\alpha_2)) \ldots (g(\alpha_{p-1}) g(\alpha_p)) < 1$. Полученное противоречие показывает, что p может быть лишь нечетным числом. Но тогда $g(\alpha_1) > 1$, $g(\alpha_{2j}) g(\alpha_{2j+1}) > 1$ и, следовательно, $1 = g(\alpha_1)(g(\alpha_2) \times \times g(\alpha_3)) \ldots (g(\alpha_{p-1}) g(\alpha_p)) > 1$, что снова приводит к противоречию. Итак, требуемый набор индексов $i_1, i_2, \ldots, i_t$ с $\varepsilon < 0$ существует. Остается применить индукционное предположение к элементам h_i.

Лемма 2 [10]. *Пусть A — квадратная матрица порядка n над телом K с центром Z; p — строка, q — столбец длины n. Предположим, что $pA^\nu q = 0$ для $\nu = 0, 1, \ldots, n-1$. Тогда $pBq = 0$ для любой матрицы B из рационального замыкания Z $[A]$ в кольце матриц K_n.*

Пусть A_i $(0 \leqslant i \leqslant m)$ — $(n \times n)$-матрицы над телом K, причем A_0 не вырождена, а $1 < h_1 < \ldots < h_m$ — элементы группы G. Тогда матрица $C = A_0 - A_1 h_1 - \ldots - A_m h_m$ принадлежит множеству Σ_0. Рассмотрим элемент $a = eC^{-1}f$ тела $\mathrm{Div}\, S$.

Лемма 3. *Если $a \neq 0$, то $v(a) < h_m^{2mn}$.*

Доказательство. Обозначим $G_0 = \mathrm{gr}\{h_1, h_2, \ldots, h_m\}$; N — наибольшая собственная выпуклая подгруппа в G_0; $H = G_0/N$; $K_N = K\{N\}$ — тело рядов Мальцева, где система автоморфизмов и факторов индуцирована группой G. Заметим, что отмеченная выше группа N всегда существует, причем N содержит коммутант G_0'. Порядок на группе H, индуцированный группой G_0, превращает H в архимедову линейно упорядоченную группу [11]. Тело $K\{G_0\}$ можно рассматривать как тело скрещенных формальных рядов группы H над телом K_N. Обозначим через V: $K_N\{H\} \to (H, \infty)$ соответствующее нормирование, а образ элемента из G_0 в H — чертой сверху. Среди элементов $\bar{1}, \bar{h}_1, \ldots, \bar{h}_m$ могут быть совпадающие. Однако ясно, что $\bar{1} \neq \bar{h}_m$. Обозначим через $\bar{g}_1, \ldots, \bar{g}_\mu$ элементы группы G_0 такие, что $\bar{1} < \bar{g}_1 < \ldots < \bar{g}_\mu$ и $\{\bar{1}, \bar{g}_1, \ldots, \bar{g}_\mu\} = \{\bar{1}, \bar{h}_1, \ldots, \bar{h}_m\}$. Элемент a можно записать в виде

$$a = e(\bar{A}_0 - \bar{A}_1 g_1 - \ldots - \bar{A}_\mu g_\mu)^{-1} f, \tag{5}$$

где $\bar{A}_i$ — $(n \times n)$-матрицы над кольцом KN. Согласно лемме 1 в группе H найдутся линейно независимые элементы $\bar{s}_1, \ldots, s_k$ $(s_i \in G_0)$ такие, что $k \leqslant \mu \leqslant m$, $\bar{1} < \bar{s}_1 < \bar{s}_i < \bar{s}_1^2$ $(2 \leqslant i \leqslant k)$ и $\bar{g}_i = \bar{s}_1^{n_{i1}} \ldots \bar{s}_k^{n_{ik}}$ для $i = 1, \ldots$ $\ldots, \mu$. Пользуясь формулой

$$P(C + AB)^{-1} Q = (P, 0) \begin{pmatrix} C & -A \\ B & E \end{pmatrix}^{-1} \begin{pmatrix} Q \\ 0 \end{pmatrix}, \tag{6}$$

приведем запись элемента a к виду

$$a = e(C_0 - C_1 s_1 - \ldots - C_k s_k)^{-1} f, \tag{7}$$

где C_i — $(n_1 \times n_1)$-матрицы над кольцом KN и $C_0 \in \Sigma_0$. Оценим число n_1. Пусть $t = \max\limits_i \sum\limits_j n_{ij}$ достигается при $i = i_0$. Расщепляя $\bar{g}_i$ на сомножители $\bar{s}_1, \ldots, \bar{s}_k$, мы совершим не более чем $t-1$ расщеплений. Так как количество g_i не превосходит m, то всего потребуется не более чем $m(t-1)$ расщеплений. При каждом расщеплении мы преобразуем клетку размеров $n \times n$; поэтому при применении формулы (6) порядок добавляемой единичной матрицы E все время один и тот же, именно n. Итак, от (5) к (7) можно перейти не более чем за $m(t-1)$ расщеплений, и при каждом расщеплении размер матрицы увеличивается на n. Следовательно, $n_1 \leqslant (t(m-1)+1)n \leqslant tmn$. Обозначим $B = C_1 s_1 + \ldots + C_k s_k$. Имеет место разложение $a = \sum\limits_{\nu=0}^{\infty} e\left(C_0^{-1}B\right)^{\nu} C_0^{-1} f$ в теле $K\lambda\{G_0\}$. Предположим, что $a \neq 0$. Из леммы 2 вытекает, что в этом случае $e\left(C_0^{-1}B\right)^{\nu} C_0^{-1} f \neq 0$ для некоторого $\nu \leqslant n-1$. Тогда в силу независимости элементов $\bar{s}_1, \ldots, \bar{s}_k$ будет $V(a) \leqslant V\left(e\left(C_0^{-1}B\right)^{\nu} C_0^{-1} f\right)$. Далее,

$$V\left(e\left(C_0^{-1}B\right)^{\nu} C_0^{-1} f\right) \leqslant \bar{s}_k^{n_1 - 1} \leqslant \bar{s}_1^{2(n_1-1)} < \bar{s}_1^{2tmn}. \tag{8}$$

Так как $\bar{g}_{i_0} \geqslant \bar{s}_1^t$, то из (8) следует, что $V(a) < \bar{g}_{i_0}^{2mn} \leqslant \bar{h}_m^{2mn}$. Отсюда окончательно получаем, что $v(a) < h_m^{2mn}$.

Следствие. *Пусть $a = geC^{-1}f$, где $g \in G$, a e, C, f, $h_1, \ldots, h_m$, n имеют тот же смысл, что и раньше; $\bar{a}$ — какой-либо формальный ряд тела $K\{G\}$, у которого однородные слагаемые со значениями нормирования, меньшими чем gh_m^{2mn}, совпадают с соответствующими слагаемыми элемента a. Тогда $a = 0$ в том и только том случае, когда $va \geqslant gh_m^{2mn}$.*

Доказательство легко сводится к случаю $g = 1$, когда следствие непосредственно вытекает из леммы 3.

§ 2. Минимальность первичного матричного идеала $m(\mathrm{Div}\, S)$

Основная цель этого параграфа — доказательство следующей теоремы.

Теорема 2. *Всякое нетривиальное S-тело D такое, что $\Sigma(D) \supseteq \Sigma_0$, S-изоморфно телу $\mathrm{Div}\, S$. В частности, Σ — максимальное локализующее множество, а $m(\mathrm{Div}\, S)$ — минимальный первичный матричный идеал S-тела $\mathrm{Div}\, S$.*

Доказательство разобьем на этапы.

1°. Обозначим через $S\Sigma_0^{-1}$ универсальное Σ_0-обращающее S-кольцо; $\mu\colon S \to D$, $\nu\colon S\Sigma_0^{-1} \to D$, $r\colon S\Sigma_0^{-1} \to \mathrm{Div}\, S$ — естественные S-гомоморфизмы. Пусть

$$a = \sum_{i=1}^{i=M} p_i C_{i1}^{-1} B_{i1} \ldots C_{ik_i}^{-1} q_i \tag{9}$$

— элемент кольца $S\Sigma_0^{-1}$, где $C_{ij} \in \Sigma_0$, B_{ij} — матрицы, p_i — строки, q_i — столбцы с элементами из кольца S. Естественный гомоморфизм $S \to S\Sigma_0^{-1}$ будет инъективным, и поэтому можно не отличать элементы из S от образов при этом вложении.

2°. Опишем процедуру, которая преобразует запись (9) элемента a к специальному виду. Пусть Z — непустое подмножество в G. Обозначим через Z^* моноид, порожденный элементами из Z. Если $Z_1, Z_2 \subseteq G$, то полагаем по определению $Z_1 * Z_2 = \{z_1 z_2 | z_1 \in Z_1,\ z_2 \in Z_2\}$. В случае, когда $Z_1 = \varnothing$ или $Z_2 = \varnothing$, считаем $Z_1 * Z_2 = \varnothing$. Если $B = (b_{ij})$ — матрица с эле-

ментами из S, то определим носитель supp B как объединение носителей всех элементов b_{ij}.

Записи вида (9) элемента a поставим в соответствие подмножество $\omega(a)$ группы G:

$$\omega(a) = \bigcup_{i=1}^{i=M} \operatorname{supp} p_i * (\operatorname{supp} C_{i1})^* * \operatorname{supp} B_{i1} * \ldots * (\operatorname{supp} C_{ik_i})^* * \operatorname{supp} q_i. \quad (10)$$

Допуская вольность речи, будем говорить об a то как об элементе кольца $S\Sigma_0^{-1}$, то как о записи, т. е. как о слове в некотором алфавите. Знак $=$ будет использоваться как знак равенства элементов кольца. Множество $\omega(a)$ определено именно по записи (9).

Лемма 4 [2]. *Множество $\omega(a)$ вполне упорядочено.*

Лемма 5. *Пусть $B_{ij} = B'_{ij} + B''_{ij}$ — разложение по разным однородным компонентам. Тогда подстановка в (9) суммы $B'_{ij} + B''_{ij}$ вместо B_{ij} и раскрытие скобок в i-м слагаемом не меняют множества $\omega(a)$. Это свойство верно и для строк p_i, и для столбцов q_i.*

Пусть $B_{ij} = gB^0_{ij}$, где $g \in G$, а B^0_{ij} — матрица над S. Тогда вынесение элемента g вперед в i-м слагаемом с соответствующими изменениями впереди стоящих матриц C_{ik}, B_{ik} и p_i не меняет множества $\omega(a)$.

Доказательство. Второе утверждение очевидно: соответствующая i-я компонента в объединении (10) при таком преобразовании не меняется. Первое утверждение следует из такого факта: если Z_1, Z', Z'', Z_2 — подмножества в G, то $Z_1 * (Z' \cup Z'') * Z_2 = Z_1 * Z' * Z_2 \cup Z_1 * Z'' * Z_2$.

Следствие. *От разложения вида (9) можно перейти, не меняя множества $\omega(a)$, к разложению элемента a такого же вида, но с дополнительными условиями:*

а) *B_{ij}, q_i — матрицы с элементами из тела K;*

б) *$p_i = g_a g_i p^0_i$, где g_i, $g_a \in G$, $g_i \geqslant 1$, p^0_i — строка с элементами из тела K;*

в) *$1 = g_1 \leqslant g_2 \leqslant \ldots \leqslant g_M$.*

Запись вида (9) с дополнительными условиями а) — в) из следствия леммы 5 назовем *специальной*.

3°. Опишем процедуру (т. е. алгоритм), которая по специальной записи вида (9) позволяет получить запись элемента a вида $g_a e C^{-1} f$, где $C \in \Sigma_0$ — матрица, быть может, большего размера, который эффективно вычисляется по записи (9). Соотношения

$$\begin{aligned} (p_1 C_1^{-1} q_1)(p_2 C_2^{-1} q_2) &= (p_1 0) \begin{pmatrix} C_1 & -q_1 p_2 \\ 0 & C_2 \end{pmatrix}^{-1} \begin{pmatrix} 0 \\ q_2 \end{pmatrix}, \\ p_1 C_1^{-1} q_1 + p_2 C_2^{-1} q_2 &= (p_1 p_2) \begin{pmatrix} C_1 & 0 \\ 0 & C_2 \end{pmatrix}^{-1} \begin{pmatrix} q_1 \\ q_2 \end{pmatrix}, \end{aligned} \quad (11)$$

примененные многократно, позволяют перейти от специальной записи вида (9) к записи вида $pC^{-1}q$, где $C \in \Sigma_0$, p — строка с элементами из S, q — столбец с элементами из тела K. Из формул (11) и определения специального вида следует, что $p = g_a p_0$, где p_0 — строка с элементами из R. Пусть P_0 — квадратная матрица, i-я строка которой равна p_0, а на остальных местах стоят нули; F — невырожденная матрица над K такая, что $Ff = q$. Тогда в кольце $S\Sigma_0^{-1}$ выполняется равенство

$$g_a p_0 C^{-1} q = g_a (e, 0) \begin{pmatrix} E & -p_0 \\ 0 & F^{-1} C \end{pmatrix}^{-1} \begin{pmatrix} 0 \\ f \end{pmatrix},$$

правая часть которого имеет требуемый вид. Описанную процедуру обозначим через $\mathscr{P}$.

4°. Пусть g, h — элементы группы G. Будем писать $g \sim h$, если существуют такие натуральные числа n и m, что $|g|^n \geqslant |h|$ и $|h|^m \geqslant |g|$.

Здесь $|g| = g$, если $g \geqslant 1$, и $|g| = g^{-1}$ в противном случае. Отношение эквивалентности обозначим $\sim$. Если $g \sim h$, то будем говорить, что *элементы g и h одного порядка*. Если же $1 \leqslant h < g^n$ для любого натурального n, то пишем $h \ll g$ и называем элемент h *бесконечно малым по сравнению с g*. Для специальной записи вида (9) обозначим

$$SC(a) = \bigcup_{i,j} \operatorname{supp} C_{ij}; \quad S(a) = SC(a) \cup \{g_1, g_2, \ldots, g_M\};$$

$$h(a) = \max S(a); \quad d(a) = g_M.$$

Наибольший элемент множества $SC(a)$ назовем *начальным шагом разложения* и обозначим его $hc(a)$. *Шагом специального разложения* (9) назовем элемент $h \in SC(a)$ такой, что элементы из $SC(a)$, большие, чем h, имеют один порядок с h. Очевидно, что начальный шаг разложения является шагом разложения.

Пусть h — шаг специального разложения (9) и в $SC(a)$ существуют элементы, меньшие, чем h, но эквивалентные h. Такую ситуацию будем называть *ситуацией пересчета* и заменять здесь шаг разложения на меньший (см. § 3).

Введем еще одну характеристику для специального разложения (9): $H(a) = g_n h(a)^{2tn}$, где n — порядок матрицы C, а t — число элементов носителя матрицы C, которая получается в результате применения процедуры $\mathscr{P}$ к записи (9).

5°. Опишем процедуру разложения (обозначим ее $\mathscr{R}$), применяемую к любой специальной записи вида (9), при условии, что задан шаг разложения h.

Случай 1. Разбиение суммы (9) на слагаемые $a_1 + \ldots + a_z$ с условиями: а) $g_{a_1} < g_{a_2} < \ldots < g_{a_z}$ и б) неверно $d(a_i) \gg h$ $(2 \leqslant i \leqslant z-1)$ — назовем *разложением по случаю 1*. Заметим, что такое разложение определено неоднозначно, и поэтому всякий раз, когда речь будет идти о разложении по случаю 1, будем уточнять, как именно оно проводится. Определим теперь два частных, в некотором смысле крайних, способа разложения по случаю 1.

Начальным разложением по случаю 1 назовем такое разбиение $a_1 + a_2 + \ldots + a_z$ суммы (9), что кроме а) и б) выполняются свойства в) $d(a_i) \leqslant h$ для $i = 1, \ldots, z$ и г) $g_{a_{i-1}}^{-1} g_{a_i} > h$ $(i = 2, \ldots, z)$. Заметим, что начальное разложение определено однозначно и представляет собой эффективную процедуру в случае конструктивности K, G и S.

Идеальным разложением по случаю 1 назовем такое разложение $a_1 + a_2 + \ldots + a_z$ по случаю 1, что $g_{a_{i-1}}^{-1} g_{a_i} \gg h$ для любого $i = 2, \ldots, z$. Заметим, что идеальное разложение определено также однозначно, но эффективной процедурой, вообще говоря, не является.

Кроме начального шага разложения однозначно, но, вообще говоря, не эффективно определяется минимальный шаг разложения. Это наименьший из шагов разложения, взятый из конечного множества $SC(a)$.

Лемма 6. *Если $a = a_1 + \ldots + a_z$ — идеальное разложение по случаю 1 относительно минимального шага разложения элемента a, то для $i \leqslant z-1$ имеют место строгие неравенства* $\operatorname{ord} \omega(a_1 + \ldots + a_i) < \operatorname{ord} \omega(a)$.

Здесь и далее $\operatorname{ord} W$ — ординал, соответствующий вполне упорядоченному множеству W.

Доказательство. Действительно, при $i \leqslant z-1$ любой элемент из $\omega(a_i)$ меньше, чем $g_{a_{i+1}}$, причем $g_{a_{i+1}} \in \omega(a)$. Следовательно, $\omega(a_1 + \ldots + a_i)$ вкладывается в собственный начальный отрезок множества $\omega(a)$. Отсюда и вытекает доказываемое неравенство.

Случай 2. Разложение по случаю 2 с шагом h определяем лишь тогда, когда $h \sim d(a)$ либо $d(a) \leqslant h$.

Для каждой пары (i, j) разложим матрицу C_{ij}:

$$C_{ij} = C_{ij}^0 - B_{ij}^1 h^{(1)} - \ldots - B_{ij}^{\alpha} h^{(\alpha)}, \tag{12}$$

где C_{ij}^0 — сумма однородных слагаемых матрицы C_{ij} с нормой меньше, чем h, $h \leqslant h^{(1)} < \ldots < h^{(\alpha)}$, и $B_{ij}^1, \ldots, B_{ij}^{(\alpha)}$ — ненулевые матрицы над телом K. Случай $\alpha = 0$ не исключается, но согласно определению шага разложения существует пара (i, j), для которой $\alpha > 0$. Обозначим $B(i, j) = B_{ij}^1 h^{(1)} + \ldots + B_{ij}^{\alpha} h^{(\alpha)}$. Для каждого натурального l имеет место равенство

$$C_{ij}^{-1} = \sum_{j=0}^{l} [(C_{ij}^0)^{-1} B(i, j)]^j (C_{ij}^0)^{-1} + [(C_{ij}^0)^{-1} B(i, j)]^{l+1} C_{ij}^{-1}. \tag{13}$$

Для каждой пары (i, j) выберем какое-либо число l так, что $h_1^{l+1} \geqslant h(a)^{2ln}$. Это возможно сделать, ибо $h_1 \sim h(a) \sim h$. Далее, для каждой пары (i, j) подставим (13) в (9), раскроем все скобки, приведем к специальному виду и в полученной сумме выберем слагаемые, перед которыми стоит элемент из G вида $g_s g$, где $g < h(a)^{2ln}$ (т. е. выберем слагаемые s такие, что $g_s < H(a)$). Эту сумму обозначим через a^*, а оставшиеся слагаемые составят сумму r.

Итак, результатом разложения по случаю 2 будет слово $a^* + r$, представляющее в $S\Sigma_0^{-1}$ тот же элемент, что и a. Отметим, что $\omega(a^*) \subseteq \omega(a)$ и $H(a) \leqslant g_r$. Предположим, что мы к полученному слову a^* в случае 2 применили разложение по случаю 1 с шагом $hc(a^*)$. Тогда $a^* = a_1 + \ldots + a_z$, где $g_{a_1} < \ldots < g_{a_z} < H(a)$ и $\omega(a_i) \subseteq \omega(a^*) \subseteq \omega(a)$. Отметим, что случаи 1 и 2 не взаимоисключающие.

Лемма 7. *Если $a = a^* + r$ — разложение по случаю 2 относительно минимального шага, то* $\operatorname{ord} \omega(a^*) < \operatorname{ord} \omega(a)$.

Доказательство. Действительно, существует элемент вида $g_s g_i h^m$, принадлежащий множеству $\omega(a)$ и больший, чем $H(a)h$. Но $H(a)h$ больше, чем любой элемент из $\omega(a^*)$. Отсюда снова, как и в лемме 6, получаем искомое неравенство.

Лемма 8. *Пусть в условиях леммы 7 $a^* = a_1 + a_2 + \ldots + a_z$ — идеальное разложение по случаю 1 относительно $hc(a^*)$. Тогда $\tau(a) = 0$ в том и только том случае, когда $\tau(a_i) = 0$ для всех i, для которых $g_{a_i}^{-1} H(a) \sim h$.*

Доказательство. Так как $g_{a_1} < \ldots < g_{a_z}$, то существует натуральное число k, $k \leqslant z$, такое, что элемент $g_{a_i}^{-1} H(a)$ эквивалентен h в том и только том случае, когда $i \leqslant k$. Пусть $\bar{a} = a_1 + a_2 + \ldots + a_k$. Из следствия леммы 3 (см. § 1) вытекает, что $\tau(a) = 0$ тогда и только тогда, когда $v(\tau(\bar{a})) \geqslant H(a)$. С другой стороны, в силу выбора слагаемых в сумме $\bar{a}$ имеем $v(\tau(\bar{a})) \geqslant H(a)$, если и только если $\tau(\bar{a}) = 0$, что эквивалентно равенствам $\tau(a_i) = 0$ для всех i, $i \leqslant k$. Это завершает доказательство леммы.

6°. Несложно доказать следующие две леммы.

Лемма 9. *Специальная запись $g_1 e_1 C_1^{-1} f_1 + g_2 e_2 C_2^{-1} f_2$, где $g_1 < g_2$ и $e_1 \pi (C_1)^{-1} f_1 \neq 0$, эффективно приводится к каноническому виду.*

Лемма 10. *Пусть $C \in \Sigma_0$ и $e\pi(C)^{-1} f \neq 0$. Тогда элемент $eC^{-1}f$ обратим в кольце $S\Sigma_0^{-1}$.*

7°. **Лемма 11.** *Если $\tau(a) = 0$, то $\nu(a) = 0$, а если $\tau(a) \neq 0$, то в кольце $S\Sigma_0^{-1}$ найдется элемент b, имеющий каноническую запись и такой, что $\tau(a) = \tau(b)$.*

Доказательство проводим трансфинитной индукцией по ординалу $\operatorname{ord} \omega(a)$, где запись (9) предполагается уже приведенной к специальному виду. Основание индукции — тривиальность. Пусть утверждение доказано для $\operatorname{ord} \omega(a) < \gamma$. Докажем утверждение в случае, когда $\operatorname{ord} \omega(a) = \gamma$. Применим к записи (9) процедуру $\mathcal{R}$ относительно мини-

мального шага разложения h. Предположим сначала, что имеет место случай 2 разложения $\mathscr{R}$ (см. обозначения лемм 7 и 8). Пусть $\tau(a)=0$. Тогда $\tau(a_i)=0$, и отсюда $\nu(a_i)=0$ для любого i, $1\leqslant i\leqslant k$, в силу предположения индукции и леммы 7. Применим теперь к специальной записи (9) преобразование $\mathscr{P}$. Пусть $C=A_0-A_1h_1-\ldots-A_mh_m$, где $1<h_1<\ldots<h_m$ и A_i — матрицы над телом K, причем $h_1\sim h_m\sim h$ и любой элемент из $\operatorname{supp}A_0$ бесконечно мал по сравнению с h. Найдем элементы $s_1,\ldots,s_k$ такие же, как в доказательстве леммы 3, и проделаем с записью $eC^{-1}f$ те же преобразования, что и в доказательстве этой леммы, за исключением разложения в ряд, которое заменим разложением

$$a=\sum_{j=0}^{j=n_1-1}e\left(C_0^{-1}B\right)^jC_0^{-1}f+e\left(C_0^{-1}B\right)^{n_1}C^{-1}f$$

(обозначения, как и в лемме 3).

Докажем, что $\nu\left(e\left(C_0^{-1}B\right)^jC_0^{-1}f\right)=0$ для всех j от 0 до n_1-1. Действительно, элемент $e\left(C_0^{-1}B\right)^jC_0^{-1}f$ кольца $S\Sigma_0^{-1}$ после раскрытия всех скобок и преобразований, обратных к (6), совпадает с суммой некоторых a_i. Тогда из равенств $\nu(a_i)=0$ для всех i, $1\leqslant i\leqslant k$, вытекает требуемое утверждение.

Далее, из равенств $\nu\left(e\left(C_0^{-1}B\right)^jC_0^{-1}f\right)=0$ $(0\leqslant j\leqslant n_1-1)$ следует согласно лемме 2, что $(0=\nu\left(e\left(E-C_0^{-1}B\right)^{-1}C_0^{-1}f\right)=\nu\left(e\left(C_0-B\right)^{-1}f\right)=\nu\left(eC^{-1}f\right)$. Отсюда $\nu(a)=\nu(g_aeC^{-1}f)=0$, что и требовалось доказать.

Разберем случай $\tau(a)\neq 0$. Имеем $\tau(a^*)\neq 0$ и по лемме 7, а также по предположению индукции существует канонический вид $g_1eC_1^{-1}f$ такой, что $\tau(a^*)=\tau\left(g_1eC_1^{-1}f\right)$. В силу леммы 3 $g_1<H(a)$. Но, с другой стороны, $g_r\geqslant H(a)$, и поэтому элемент $g_1eC_1^{-1}f+r$, а значит, и элемент $\tau(a)$ имеет каноническую запись (см. лемма 9).

Предположим, что случай 2 разложения $\mathscr{R}$ не применяется к a, т. е. минимальный шаг разложения h записи (9) бесконечно мал по сравнению с $d(a)$. Применим к a идеальное разложение по случаю 1: $a=a_1+\ldots+a_z$. Заметим, что обязательно $z>1$. Если $\tau(a_1+\ldots+a_{z-1})=0$, то $\nu(a_1+\ldots+a_{z-1})=0$ по лемме 6 и предположению индукции. Это равенство позволяет от элемента a перейти к элементу a_z, причем здесь либо множество $SC(a)$ уменьшилось, либо к a_z уже применяется случай 2. Значит, такого рода редукций $(a\mapsto a_z)$ может быть лишь конечное число. Следовательно, можно считать, что $\tau(a_1+\ldots+a_{z-1})\neq 0$. Тогда по предположению индукции у этого элемента существует соответствующая каноническая запись $ge_1C^{-1}f_1$. Так как $g<g_{a_z}$, то, применяя к слову $ge_1C^{-1}f_1+a_z$ лемму 9, получим каноническую запись элемента $\tau\left(ge_1C^{-1}f_1+a_z\right)=\tau(a)$. Лемма доказана.

8°. **Теорема 3.** *В теле* $\operatorname{Div}S$ *любой элемент имеет каноническую запись.*

Доказательство. Из леммы 11 вытекает, что множество элементов из $\operatorname{Div}S$, имеющих каноническую запись, образует подкольцо (очевидно, содержащее S). Это подкольцо в силу леммы 10 будет подтелом в $\operatorname{Div}S$. Так как $\operatorname{Div}S$ — наименьшее тело в $K\{G\}$, содержащее S, то теорема доказана.

9°. Теперь теорема 2 немедленно следует из критерия $\tau(a)=0\Leftrightarrow$ $\Leftrightarrow\nu(a)=0$ и эпиморфности τ (см. теорему 3). Ввиду леммы 11 осталось доказать лишь импликацию $\Leftarrow$. Если $\tau(a)\neq 0$, то пусть $geC^{-1}f$ — канонический вид элемента $\tau(a)$. Из леммы 10 вытекает, что элемент $\nu(eC^{-1}f)$, а значит, и элемент $\nu(a)=\nu(g)\nu(eC^{-1}f)$ обратим в теле D. Равенство $\nu(a)=0$ в этом случае может иметь место лишь тогда, когда тело D тривиально.

§ 3. Доказательство основного результата

3.1. Докажем конструктивный аналог леммы 11, а именно: предполагая K, G, S конструктивно заданными, построим алгорифм $\mathcal{U}$, который применяется к любой записи вида (9) и результат применения которого будет символом 0, если $\tau(a)=0$ либо каноническая запись вида $geC^{-1}f$ такова, что $\tau(a)=\tau(geC^{-1}f)$.

Пусть U — множество слов вида (a, h), где a — специальное разложение вида (9), а h — шаг разложения для a. Рассмотрим вполне упорядоченное множество $\beta=\sigma\times\sigma\times\mathbf{N}$, где σ — достаточно большой ординал (больше, чем $\operatorname{ord}\omega(a)$ для любой записи вида (9)). Тройки $(\gamma_1, \gamma_2, n)\in\beta$ упорядочим лексикографически. Обозначим через φ: $U\to\beta$ отображение такое, что $\varphi(a, h)=(\operatorname{ord}\omega(a), \operatorname{ord}\{g\in\omega(a)\mid g\leqslant H(a)\}, N(a, h))$, где $N(a, h)$ определяется следующим образом. Пусть $SC(a)=\{h_1, h_2, \ldots, h_l\}$, где $h_1<h_2<\ldots<h_l$. Тогда $N(a, h)=i$, для которого $h=h_i$.

Сначала построим методом спуска по вполне упорядоченному множеству β алгорифм $\mathscr{W}$, применяемый к любой паре $(a, h)\in U$ и вырабатывающий каноническую запись элемента a. Обозначим для $\gamma\in\beta$ через U_γ множество элементов $(a, h)\in U$ таких, что $\varphi(a, h)<\gamma$. Пусть дана пара $(a, h)\in U$ такая, что $\varphi(a, h)=\gamma$, и построен алгорифм $\mathscr{M}$, применяемый к любому элементу из U_γ.

А. Если $d(a)>hc(a)$, то применим к a начальное разложение по случаю 1 с шагом h. В результате получим слово $a_1+a_2+\ldots+a_z$, где $z>1$, $\omega(a_i)\leqslant\omega(a)$, $H(a_1+\ldots+a_{z-1})<H(a)$. По индукционному предположению элемент $b=a_1+\ldots+a_{z-1}$ приводится к каноническому виду. Если b приводится к 0, то, учитывая, что $H(a_z)<H(a)$, и снова пользуясь индукционным предположением, приведем a_z к каноническому виду. В противном случае b приводится к виду $g_1eC_1^{-1}f$. Если $g_1<g_{a_z}$, то приведение a к каноническому виду заканчивается по лемме 9. Иначе, если $g_1\geqslant g_{a_z}$, то в силу $g_1\in\omega(b)$ неверно, что $d(a_{z-1}+a_z)\gg h$. Тогда вместо разложения $a_1+\ldots+a_z$ рассмотрим разложение $a_1+\ldots+a_{z-2}+\bar{a}_{z-1}$ элемента a по случаю 1 относительно шага h, где $\bar{a}_{z-1}=a_{z-1}+a_z$. Применим к этому разложению описанную выше процедуру. Мы либо дойдем до возможности использования индукционного предположения, либо получим, что вся сумма (9) представляет собой разложение a по случаю 1 с шагом h. Но тогда неверно $d(a)\gg hc(a)$, и мы вправе применить к a разложение по случаю 2, что и делаем в п. Б.

Б. Пусть либо $d(a)\leqslant hc(a)$, либо уже установлено, что $d(a)\sim h$. Применяя к a разложение $\mathscr{R}$ по случаю 2 с шагом h, получим, что $a=a^*+r$, где $\omega(a^*)\subseteq\omega(a)$ (см. § 2, п. 5°). Теперь применим к a^* начальное разложение по случаю 1 с начальным шагом $hc(a^*)$. Обозначим через $a_1+a_2+\ldots+a_z$ результат этого разложения. Если $H(a_1)\geqslant H(a)$, то $hc(a^*)\sim h$, и поэтому возникает ситуация пересчета. Заменяя h меньшим шагом и пользуясь индукционным предположением, получим искомый канонический вид. В случае $H(a_1)<H(a)$ к a_1 можно применить индукционное предположение и привести его к каноническому виду. Если этот вид будет 0, то переходим к a_2 и рассуждаем так же и т. д. Если все a_i привелись к 0, то каноническим видом для a будет 0, и процесс заканчивается. Итак, считаем, что a_1 приводится к каноническому виду $g_1eC_1^{-1}f$. Если $g_1<g_{a_2}$, то приведение a к каноническому виду заканчивается по лемме 9. В противном случае $\bar{a}_1+a_3+\ldots+a_z$, где $\bar{a}_1=a_1+a_2$, будет разложением a^* по случаю 1. К нему применим описанную выше процедуру. Либо мы придем к возможности применения леммы 9, либо к случаю, когда $d(a_1)\geqslant h$. Но тогда $hc(a_1)\sim h$, и возникает ситуация пересчета. Мы возвращаемся к паре (a, h_1), где $h_1<h$, $h_1\in SC(a)$, $h_1\sim h$, и применяем индукционное предположение.

Алгорифм $\mathcal{M}$ построен. Для того чтобы построить алгорифм $\mathcal{U}$, достаточно заметить, что $\mathcal{U} = \mathcal{M} \circ \mathcal{D} \circ \mathcal{C}$, где $\mathcal{C}$ — алгорифм приведения слова a к специальному виду, а $\mathcal{D}$ — алгорифм, сопоставляющий специальной записи a пару $(a, hc(a))$.

3.2. Сделаем замечание общего характера. Пусть D — произвольное тело. Рассмотрим $\mathrm{GL}(D)$, а также линейную группу тела D как прямой предел системы групп $\mathrm{GL}(n, D)$.

Следующая лемма — стандартный результат из линейной алгебры.

Лемма 12. *Пусть C — невырожденная матрица над телом D, а матрица B, получающаяся из C вычеркиванием i-й строки и j-го столбца, вырождена. Тогда $e_j C^{-1} e_i^{\top} = 0$* ($^{\top}$ — операция транспонирования).

Предложение. *Если тело D рационально над своим подкольцом S, то группа $\mathrm{GL}(D)$ порождается множеством $\Sigma(D)$.*

Доказательство. Обозначим через $A \oplus B$ диагональную сумму матриц A и B (см. [9, гл. 7]). Достаточно доказать индукцией по n, что если $C \in \mathrm{GL}(n, D)$, то для некоторой единичной матрицы E $C \oplus E$ будет представлена в виде произведения матриц из $\Sigma(D)$ и им обратных.

Рассмотрим случай $n = 1$. Пусть $c \in D$, $c \neq 0$. Тогда из условия вытекает, что $c = eA^{-1}f$, где $A \in \Sigma(D)$. Можно считать, что у e и f первая координата — единица, а все остальные — нули. Обозначим через B матрицу, получающуюся из A вычеркиванием первой строки и первого столбца. Согласно лемме 12 и предположению $c \neq 0$ матрица B не вырождена. Пусть

$$A = \begin{pmatrix} a & p \\ q & B \end{pmatrix}.$$

Нетрудно проверить, что

$$\begin{pmatrix} c & & & 0 \\ & 1 & & \\ & & \ddots & \\ 0 & & & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \dots 0 \\ & \\ q & B \end{pmatrix} A^{-1} \begin{pmatrix} 1 & p \\ & \\ 0 & B \end{pmatrix} \begin{pmatrix} 1 & 0 \\ & \\ 0 & B \end{pmatrix}^{-1}, \qquad (14)$$

причем все матрицы в правой части этого равенства принадлежат $\Sigma(D)$. Отсюда следует утверждение при $n = 1$.

Пусть для $(n \times n)$-матриц утверждение доказано и C — невырожденная матрица размеров $(n+1) \times (n+1)$ с элементами из тела D. Из леммы 12 вытекает, что существует невырожденная $(n \times n)$-подматрица B матрицы C. Можно считать, что

$$C = \begin{pmatrix} b & y \\ x & B \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & B \end{pmatrix} \begin{pmatrix} 1 & y \\ 0 & E \end{pmatrix} \begin{pmatrix} b - yB^{-1}x & 0 \\ 0 & E \end{pmatrix} \begin{pmatrix} 1 & 0 \\ B^{-1}x & E \end{pmatrix}, \qquad (15)$$

где второе равенство проверяется непосредственно. В разложении (15) первая матрица принадлежит $\mathrm{gr}\,\Sigma(D)$ по предположению индукции, а третья — по доказанному выше утверждению для случая $n = 1$. Остается доказать, что элементарные матрицы $E_{ij}(d)$, где $i \neq j$ и $d \in D$, также лежат в $\mathrm{gr}\,\Sigma(D)$. Заметим, что вторую и четвертую матрицы в правой части (15) можно представить в виде произведения таких элементарных матриц. Но $E_{ij}(d) = QE_{ij}(1)Q^{-1}$, где Q — диагональная матрица, и утверждение следует из вышедоказанного для случая $n = 1$.

3.3. Возвратимся к нашей конкретной ситуации. Имеем

$$G \subseteq \Sigma \subseteq \mathrm{GL}(\mathrm{Div}\, S) \subseteq \mathrm{GL}(K\{G\}).$$

Обозначим через $\mathrm{UG}(S)$ подгруппу в $\mathrm{GL}(\mathrm{Div}\, S)$, состоящую из всех матриц вида $\mathrm{diag}(s_1, \dots, s_n)$, где s_i — обратимые элементы кольца S. Нетрудно видеть, что s_i имеет вид kg, где $k \in K$, $k \neq 0$, $g \in G$.

Теорема 4. *Группа* $\mathrm{GL}(\mathrm{Div}\,S)$ *порождается множеством* Σ_0 *и подгруппой* $\mathrm{UG}(S)$. *Более того, если кольцо* S, *тело* K *и группа* G *вместе с порядком на ней заданы конструктивно, то существует алгорифм* $\mathscr{K}$, *распознающий вырожденность матрицы* A *над* $\mathrm{Div}\,S$ *и в случае ее невырожденности вырабатывающий запись вида*

$$A \oplus E = B_1 C_1^{\varepsilon_1} B_2 C_2^{\varepsilon_2} \dots B_k C_k^{\varepsilon_k}, \tag{16}$$

где $B_i \in \mathrm{UG}(S)$, $C_i \in \Sigma_0$, $\varepsilon_i \in \{-1, 1\}$, E — *единичная матрица, размер которой эффективно вычисляется.*

Доказательство. Достаточно установить справедливость конструктивного варианта теоремы. Сначала индукцией по размеру матриц докажем, что существует алгорифм $\mathscr{K}_0$, применяемый к любой матрице над S и в остальном работающий так же, как и $\mathscr{K}$. Для (1×1)-матриц этот алгорифм очевиден. Предположим, что алгорифм $\mathscr{K}_0$ построен для $(n\times n)$-матриц над S, и теперь A — $(n+1)\times(n+1)$-матрица с элементами из кольца.

Пользуясь предположением индукции, проверим все $(n\times n)$-подматрицы матрицы A на невырожденность. Если все они вырождены, то и матрица A вырождена. В противном случае, переставляя строки и столбцы матрицы A, запишем A в виде

$$A = \begin{pmatrix} a & p \\ q & C \end{pmatrix},$$

где C — невырожденная $(n\times n)$-матрица, q — столбец, p — строка, $a \in S$. Имеет место равенство

$$A = \begin{pmatrix} 1 & 0 \\ 0 & C \end{pmatrix}\begin{pmatrix} 1 & p \\ 0 & E \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & C^{-1} \end{pmatrix}\begin{pmatrix} a - pC^{-1}q & 0 \\ 0 & E \end{pmatrix}\begin{pmatrix} 1 & 0 \\ q & E \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & C \end{pmatrix}. \tag{17}$$

Тогда матрица A вырождена в том и только том случае, если $a = pC^{-1}q$, что можно проверить эффективно на основании предположения индукции и алгорифма $\mathscr{U}$, построенного в п. 3.1. Пусть проверка показала, что $a - pC^{-1}q = geC_0^{-1}f$, где $geC_0^{-1}f$ — каноническая запись. Докажем, что каждый сомножитель в (17) имеет представление вида (16). Первая, третья и последняя матрицы в правой части (17) приводятся к виду (16) по предположению индукции. Вторая и предпоследняя матрицы сопряжены с матрицами из Σ_0 посредством диагональной матрицы из $\mathrm{UG}(S)$. Пусть E_0 — единичная матрица того же размера, что и C_0. Тогда

$$\begin{pmatrix} a - pC^{-1}q & 0 \\ 0 & E_0 \end{pmatrix} = \begin{pmatrix} -g & 0 \\ 0 & E_0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & C_0 \end{pmatrix}\begin{pmatrix} 1 & -e \\ 0 & E_0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & C_0 \end{pmatrix}^{-1} \times$$
$$\times \begin{pmatrix} 0 & e \\ f & C_0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & C_0 \end{pmatrix}^{-1}\begin{pmatrix} 1 & 0 \\ -f & E_0 \end{pmatrix} \tag{18}$$

— разложение вида (16). Пятая матрица в правой части (18) принадлежит Σ_0 в силу того, что $e\pi(C_0)^{-1}f \neq 0$.

Индукционный переход завершен, алгорифм $\mathscr{K}_0$ построен.

Переходим к построению алгорифма $\mathscr{K}$. Снова воспользуемся индукцией по размерам $n\times n$ матрицы C с элементами из тела $\mathrm{Div}\,S$. Если $n = 1$, то применяем (14) и алгорифм $\mathscr{K}_0$. Предположим, что алгорифм $\mathscr{K}$ для $(k\times k)$-матриц, где $k \leqslant n$, над $\mathrm{Div}\,S$ построен, и теперь C — $(n+1)\times(n+1)$-матрица с элементами из тела $\mathrm{Div}\,S$. Пользуясь предположением индукции, проверим на невырожденность все $(n\times n)$-подматрицы матрицы C. Если все они вырождены, то и матрица C вырождена. В противном случае можно считать, что матрица C имеет вид, как и в (15), где B — невырожденная $(n\times n)$-матрица над $\mathrm{Div}\,S$. Из формулы

(15) и предположения индукции следует, что достаточно получить разложение вида (16) для элемента $b - yB^{-1}x$. Снова по предположению индукции матрицу B можно записать в виде (16), а каждый элемент строки y, столбца x и элемент b — в каноническом виде, пользуясь алгорифмами $\mathscr{K}_0$ и $\mathscr{U}$. Тогда с помощью алгорифма $\mathscr{U}$ можно проверить равенство $b - yB^{-1}x = 0$ и тем самым проверить, вырождена или нет матрица C. В случае $b - yB^{-1}x \neq 0$ запишем этот элемент в каноническом виде. После этого остается к каноническому виду применить алгорифм $\mathscr{K}_0$.

3.4. Доказательство теоремы 1 теперь немедленно следует из построенных алгорифмов $\mathscr{U}$ и $\mathscr{K}_0$. Действительно, для любого выражения вида $pC^{-1}q$, где C — матрица, p — строка, q — столбец с элементами из кольца S, можно прежде всего проверить невырожденность матрицы C, пользуясь алгорифмом $\mathscr{K}_0$, а затем записать C^{-1} как (16). Тогда элемент $pC^{-1}q$ будет вида (9), поэтому применим алгорифм $\mathscr{U}$, который выработает канонический вид элемента $pC^{-1}q$.

ЛИТЕРАТУРА

1. *Бовди А. А.* О скрещенных произведениях полугруппы и кольца // Докл. АН СССР. 1961. Т. 137, № 6. С. 307—313.
2. *Мальцев А. И.* О включении групповых алгебр в алгебры с делением // Докл. АН СССР. 1948. Т. 60, № 9. С. 1499—1501.
3. *Бурбаки Н.* Коммутативная алгебра. М.: Мир, 1971.
4. *Мальцев А. И.* Алгоритмы и рекурсивные функции. М.: Наука, 1986.
5. *Ершов Ю. Л., Палютин Е. А.* Математическая логика. М.: Наука, 1987.
6. *Марков А. А., Нагорный Н. М.* Теория алгорифмов. М.: Наука, 1984.
7. *Мальцев А. И.* Конструктивные алгебры. I // Успехи мат. наук. 1961. Т. 16, № 3. С. 3—60.
8. *Справочная* книга по математической логике. Ч. III: Теория рекурсии. М.: Наука, 1982.
9. *Кон П.* Свободные кольца и их связи. М.: Мир, 1975.
10. *Cohn P. M.* The word problem for free fields // J. Symbol. Log. 1973. V. 38, N 2. P. 309—314.
11. *Кокорин А. И., Копытов В. М.* Линейно упорядоченные группы. М.: Наука, 1972.

г. Владимир

Статья поступила
18 января 1989 г.