И З В Е С Т И Я В Ы С Ш И Х У Ч Е Б Н Ы Х З А В Е Д Е Н И Й

2003 МАТЕМАТИКА № 10 (497)

УДК 512.552

А.М. ПОПОВА

МУЛЬТИПЛИКАТИВНАЯ СТРУКТУРА КОНЕЧНО-ПОРОЖДЕННЫХ МАТРИЧНЫХ КОЛЕЦ

1. Постановка задачи

Описание групп единиц различных ассоциативных колец с единицей и нахождение условий на группу, при которых она является мультипликативной группой подходящего кольца, — эти две проблемы были сформулированы Л. Фуксом в ([1], гл.XIII, § 77, с. 299; [2], гл. XVIII, § 129, с. 380). В данной работе эти задачи решаются для произвольного конечно-порожденного матричного кольца над полем рациональных чисел.

Полученные результаты позволяют решать задачу описания групп единиц целочисленных групповых колец конечных групп и групп, представимых матрицами ([3]–[5]).

Пусть $O = rg(x_1, \dots, x_r) \subset Q_n$ — такое кольцо. Прежде всего, заметим, что O приводится над Q к клеточно-треугольному виду, в котором диагональные клетки либо абсолютно неприводимы, либо неприводимы над Q. Поэтому естественным подходом к решению поставленных задач является вначале решение их для каждой клетки в отдельности, а потом "склейка" полученных результатов для общего случая.

В работе [6] доказывается эффективность приведения O к клеточно-треугольному виду, т. е. эффективность нахождения по порождающим $x_1, \dots, x_r$ кольца O порождающих каждой клетки, а один из результатов работы [7] позволяет эффективно отвечать на вопрос, содержит ли клетка единичную матрицу.

Пусть O_i — такая клетка. Обозначим через QO_i алгебру кольца O_i над полем рациональных чисел. Могут возникнуть три случая:

1) $QO_i = Q_{n_i}$;

2) $QO_i \cong F_k$, F — поле;

3) $QO_i \cong T_k$, T — тело.

Первый случай относится к абсолютно неприводимым кольцам, второй и третий — к кольцам, неприводимым над Q. Для первых двух случаев задача описания группы единиц $U(O_i)$ кольца O_i на языке порождающих элементов была решена в [8] и [9]. Третий случай рассмотрен в [10]. Таким образом, в данной работе поставленные задачи решаются уже для произвольного конечно-порожденного матричного кольца.

В силу вышеизложенного будем полагать, что O имеет клеточно-треугольный вид и содержит единичную матрицу

$$O = \begin{pmatrix} \boxed{O_1} & & * \\ & \ddots & \\ 0 & & \boxed{O_q} \end{pmatrix}. \tag{1}$$

Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (код проекта № 99-01-00-571).

2. Строение абсолютно неприводимых и неприводимых над Q колец

В силу того, что в случае неприводимости кольца O алгебра QO изоморфна полной матричной алгебре над полем или телом ([11], с. 142), справедлива

Теорема 1. *Если конечно-порожденное кольцо $O \subset Q_n$ абсолютно неприводимо или неприводимо над Q, то эффективно находятся такие элементы $g_1, \ldots, g_t \in O$ и такое множество простых чисел $\pi = \langle p_1, \ldots, p_s \rangle$, что*

$$O = \{g_1, \ldots, g_t\}_{Z_\pi},$$

где $Z_\pi = Z[\frac{1}{p_1 \cdots p_s}]$.

Доказательство теоремы можно найти в [7] для абсолютно неприводимого случая, аналогично она может быть доказана для кольца, неприводимого над Q. Для неприводимого кольца будем считать, что $QO = H_k$, где $H \subset Q_l$ — тело размерности $l = \frac{n}{k}$ ([11], с. 142). Обозначим $H_\pi = H \cap (Z_\pi)_l$. Из теоремы 1 легко следует, что найдется ненулевое натуральное число m такое, что $(m, p_1 \cdots p_s) = 1$ и справедливы следующие включения:

$m(Z_\pi)_n \subset O$ для абсолютно неприводимого случая, $m(H_\pi)_k \subset O$ для неприводимого случая.

В кольцах Z_π и H_π породим соответственно идеалы $I = (m)$ и $I' = (me_l)$ (e_l — единичная матрица из Q_l). Определим гомоморфизмы

абсолютно неприводимый случай	неприводимый случай
$\gamma_m : Z_\pi \longrightarrow Z_\pi/I = \overline{Z_\pi}$,	$\gamma'_m : H_\pi \longrightarrow H_\pi/I' = \overline{H_\pi}$,
$\psi_m : Z_{\pi^n} \longrightarrow \overline{Z_\pi}_n$,	$\psi'_m : H_{\pi^k} \longrightarrow \overline{H_\pi}_k$,
$\varphi_m : GL_n(Z_\pi) \longrightarrow GL_n(\overline{Z_\pi})$,	$\varphi'_m : GL_k(H_\pi) \longrightarrow GL_k(\overline{H_\pi})$,
$U_0(O) = U(O) \cap \ker \varphi_m$;	$U_0(O) = U(O) \cap \ker \varphi'_m$.

3. Группы единиц абсолютно неприводимых и неприводимых над Q колец

Введем некоторые обозначения. Для абсолютно неприводимого случая

$$\gamma_m^* : U(Z_\pi) \longrightarrow U(\overline{Z_\pi}), \quad \ker \gamma_m^* = \text{гр}\,(\rho_1, \ldots, \rho_q); \quad t_{ij}(\lambda) = e + \lambda e_{ij}, \quad d(\rho) = \mathrm{diag}(1, \ldots, 1, \rho),$$
$$U_0(m, \pi) = \text{гр}\,(t_{ij}(\tfrac{m}{p_1 \cdots p_s}),\ d(\rho_\beta),\ i, j = 1, \ldots, n,\ \beta = 1, \ldots, q). \tag{2}$$

Для неприводимого случая $QO = H_k$, где H — поле. Поскольку $O \subset H_k$, то элементы O имеют клеточное строение, при котором матрица размера $n \times n$ разбита на k^2 клеток размера $l \times l$. В связи с этим пусть e_{ij} — матрица из Q_n, в которой в клетке с номером ij $(i, j = 1, \ldots, k)$ стоит единичная матрица из Q_l, $E_k = e_{11} + e_{22} + \cdots + e_{kk}$. Для $\mu \in H$, $g \in Q_n$ обозначим

$$\mu E_k = \mathrm{diag}(\mu, \ldots, \mu), \quad \mu g = \mu E_k g, \quad t_{ij}(\mu) = E_k + \mu e_{ij}, \quad d(\mu) = \mathrm{diag}(e_l, \ldots, e_l, \mu);$$
$$\gamma'^*_m : U(H_\pi) \longrightarrow U(\overline{H_\pi}), \quad \ker \gamma'^*_m = \text{гр}\,(\tau_1, \ldots, \tau_v);$$
$$U_0(m, \pi, H_\pi) = \text{гр}\,(t_{ij}(\tfrac{mh}{p_1 \cdots p_s}),\ d(\tau_\beta),\ i, j = 1, \ldots, k,\ \beta = 1, \ldots, v). \tag{3}$$

Пусть теперь O неприводимо над Q и $QO = H_k$, где H — тело. Известно ([12], с. 266), что в этом случае $[H : Q] = d^2$ и в H существуют два подполя $F = \{1, f, \ldots, f^{d-1}\}_Q$ и $T = \{1, t, \ldots, t^{d-1}\}_Q$ такие, что

1) $H = \{f^i t^j | i, j = 0, \ldots, d-1\}_Q$,
2) $\exists \xi \in H [f = \xi^{-1} t \xi]$.

Отсюда следует, что для любого $h \in H$ справедливо представление $h = ab$, где $a \in F$, $b \in T$. Тогда, как показано в [10], $H_\pi = F_\pi T_\pi$. Поскольку F и T — алгебраические расширения Q, то для максимальных порядков в них существует теория дивизоров ([13], с. 216), с помощью которой можно найти порождающие групп $U(F_\pi)$ и $U(T_\pi)$ и тем самым порождающие группы

$U(H_\pi) = U(F_\pi)U(T_\pi)$. В [10] доказывается, что порождающие группы $\ker \gamma'^*_m$ и в этом случае находятся эффективно. Пусть $\ker \gamma'^*_m = \text{гр}\,(\eta_1, \ldots, \eta_w)$. Обозначим

$$U_0(m, \pi, F_\pi, T_\pi) = \text{гр}\,(t_{ij}(\tfrac{mf}{p_1 \cdots p_s}), t_{ij}(\tfrac{mt}{p_1 \cdots p_s}),\ d(\eta_\beta),\ i, j = 1, \ldots, k,\ \beta = 1, \ldots, w). \tag{4}$$

В работах [8] и [14] доказаны следующие теоремы.

Теорема 2. *Абсолютно неприводимая группа $G < GL_n(Q)$ $(n > 2)$ является группой единиц конечно-порожденного абсолютно неприводимого матричного кольца над полем рациональных чисел Q тогда и только тогда, когда*

1) G есть конечное расширение $U_0(m, \pi)$ для некоторых m и π;

2) если $Z[G]$ — целочисленная линейная оболочка G, то $\overline{U(Z[G])} = \overline{G}$, где черта означает образ при гомоморфизме φ_m.

Теорема 3. *Неприводимая над Q группа $G < GL_n(Q)$ $(n > 2)$ является группой единиц конечно-порожденного неприводимого над Q матричного кольца тогда и только тогда, когда выполняются следующие условия:*

1) существует $t \in GL_n(Q)$ такая, что $G^t \subset H_{\pi^k}$ и G^t есть конечное расширение $U_0(m, \pi, H_\pi)$ для некоторых m, π, H_π или $U_0(m, \pi, F_\pi, T_\pi)$ для некоторых m, π, F_π, T_π;

2) если $Z[G]$ — целочисленная линейная оболочка G, то $\overline{U(Z[G])} = \overline{G}$, где черта означает образ при гомоморфизме φ'_m.

Кроме того, в обоих случаях справедлива

Теорема 4. *Если $O = rg(x_1, \ldots, x_r) \subset Q_n$ — конечно-порожденное абсолютно неприводимое или неприводимое над Q кольцо, то задача нахождения порождающих группы единиц $U(O)$ кольца O алгоритмически разрешима.*

4. Общий случай

Если $O = rg(x_1, \ldots, x_r) \subset Q_n$ вполне приводимо над Q с двумя неприводимыми частями O_1 и O_2 так, что $O = \text{diag}(O_1, O_2)$, то так же, как в [15], можно показать, что либо существует такое ненулевое $m \in N$, что $\text{diag}(mO_1, 0), \text{diag}(0, mO_2) \subset O$, т. е. O_1 и O_2 “расклеиваются”, либо O_1 и O_2 не “расклеиваются”, и тогда они изоморфны.

Так как в виде (1) кольца $O_i (i = 1, \ldots, q)$ определяются с точностью до изоморфизма и порядка следования, то будем считать, что в последовательности $O_1, \ldots, O_q$ не “расклеивающиеся” кольца следуют друг за другом и образуют блоки $R_1, \ldots, R_{s+1}$, т. е.

$$O = \begin{pmatrix} \boxed{R_1} & & * \\ & \ddots & \\ 0 & & \boxed{R_{s+1}} \end{pmatrix}. \tag{5}$$

Нетрудно показать, что $O = O' \oplus I$, где $O' \cong \text{diag}(R_1, \ldots, R_{s+1})$, I — ядро гомоморфизма

$$\chi : \begin{pmatrix} \boxed{R_1} & & * \\ & \ddots & \\ 0 & & \boxed{R_{s+1}} \end{pmatrix} \longrightarrow \begin{pmatrix} \boxed{R_1} & & 0 \\ & \ddots & \\ 0 & & \boxed{R_{s+1}} \end{pmatrix}. \tag{6}$$

Поскольку $U(O) = U(O')(e \oplus I)$, то естественно вначале описать группы типа $U(R_i)$, затем типа $U(R)$, где $R = \text{diag}(R_1, \ldots, R_{s+1})$, и, наконец, $U(O)$. Все это обосновано в [15] и дословно переносится на изученный здесь случай. Поэтому приведем только формулировки необходимых лемм.

Лемма 1. *Пусть $O = rg(x_1, \dots, x_r) \subset Q_n$ — приводимое над Q кольцо, при этом неприводимые части либо аболютно неприводимы, либо неприводимы над Q и в обоих случаях не "расклеиваются". Тогда эффективно находятся аддитивный базис кольца O и конечная система порождающих группы единиц $U(O)$.*

Заметим, что если кольцо O удовлетворяет условиям леммы 1, то $U_0(O) = U(O) \cap \ker \varphi_m = (U(O') \cap \ker \varphi_m)(e \oplus mI)$ (аналогично для φ'_m), поэтому группа

$$U_0(O) = \text{гр}\left(\begin{pmatrix} \boxed{u_{01}^1} & & * \\ & \ddots & \\ 0 & & \boxed{u_{01}^t} \end{pmatrix}, \dots, \begin{pmatrix} \boxed{u_{0s}^1} & & * \\ & \ddots & \\ 0 & & \boxed{u_{0s}^t} \end{pmatrix}, e + ma_1, \dots, e + ma_q \right), \tag{7}$$

где

$$\text{гр}\left(\begin{pmatrix} \boxed{u_{01}^1} & & * \\ & \ddots & \\ 0 & & \boxed{u_{01}^t} \end{pmatrix}, \dots, \begin{pmatrix} \boxed{u_{0s}^1} & & * \\ & \ddots & \\ 0 & & \boxed{u_{0s}^t} \end{pmatrix} \right) = U_{01}$$

изоморфна группе $U_{01}^1 = \text{гр}\,(u_{01}^1, \dots, u_{0s}^1)$, которая имеет вид (2), (3) или (4), а $I = \{a_1, \dots, a_q\}_{Z_\pi}$.

Лемма 2. *Для любого вполне приводимого конечно-порожденного кольца над полем рациональных чисел эффективно находится аддитивный базис.*

Вернемся к общему случаю. Пусть теперь O имеет вид (5). Используя аддитивный базис кольца $R = \text{diag}(R_1, \dots, R_{s+1})$, получим

$$O = O' \oplus I,$$

где $O' \cong R$, I — ядро гомоморфизма $O \longrightarrow O'$. Как следует из замечания к лемме 1, для каждого R_i эффективно находятся порождающие групп $U_0(R_i) = U(R_i) \cap \ker \varphi_{im}$, поэтому легко, применяя рассуждения такие же, как в [8] и [9], эффективно найти порождающие группы $U(R)$ и, следовательно, порождающие группы $U(O')$. Поскольку, как и выше, $U(O) = U(O')(e \oplus I)$, то для нахождения конечной системы порождающих $U(O)$ нужно любую матрицу из $e \oplus I$ представлять словом от какого-то конечного набора матриц из $e \oplus I$ и матриц из $U(O')$. Назовем этот конечный набор системой элементов, задающих подгруппу $e \oplus I$, и обозначим его через B. Алгоритм построения множества $B = \{h_{11}, \dots, h_{1l_1}, \dots, h_{s1}, \dots, h_{sl_s}\}$ описан в [15].

Лемма 3. *Пусть $h \in I$, тогда $e + h = w((e + h_{ij}), u_k)$, где $h_{ij} \in B$, $u_k \in U(O')$.*

5. Основные результаты

Теорема 5. *Пусть кольцо $O = rg(x_1, \dots, x_r) \subset Q_n$ $(n > 2)$ приводимо над полем рациональных чисел, при этом неприводимые части либо абсолютно неприводимы, либо неприводимы над Q. Тогда задача нахождения порождающих группы единиц $U(O)$ алгоритмически разрешима.*

Поскольку $U(O) = U(O')(e \oplus I)$, то утверждение теоремы следует из замеченного выше факта об эффективности нахождения порождающих $U(O')$ и леммы 3. Таким образом, если $U(O') = \text{гр}\,(u_1, \dots, u_t)$, то

$$U(O) = \text{гр}\,(u_1, \dots, u_t, e + h_{11}, \dots, e + h_{1l_1}, \dots, e + h_{s1}, \dots, e + h_{sl_s}).$$

В следующей теореме сформулированы необходимые и достаточные условия для того, чтобы группа G из $GL_n(Q)$ являлась группой единиц конечно-порожденного матричного кольца над полем рациональных чисел.

Теорема 6. *Группа $G < GL_n(Q)$ $(n > 2)$ является группой единиц конечно-порожденного матричного кольца над полем рациональных чисел Q тогда и только тогда, когда она удовлетворяет следующим условиям:*

1) *существует такая матрица $t \in GL_n(Q)$, что $G^t = \mathrm{гр}\,(u_1, \ldots, u_t, e + h_1, \ldots, e + h_q)$, где группа $U_1 = \mathrm{гр}\,(u_1, \ldots, u_t)$ изоморфна конечному расширению группы*

$$U_0 = \mathrm{гр}\left(\begin{pmatrix} \boxed{e_1} & & & & * \\ & \ddots & & & \\ & & \boxed{u_{ij}} & & \\ & & & \ddots & \\ 0 & & & & \boxed{e_k} \end{pmatrix},\ \ i = 1, \ldots, k,\ \ j = 1, \ldots, t_i\right),$$

для которой группы $U_{0i} = \mathrm{гр}\,(u_{i1}, \ldots, u_{it})$ имеют вид (2)–(4) *или* (7);

2) *если χ — гомоморфизм кольца $Z[G^t]$, определенный аналогично* (6), *$I = \ker \chi$, то система $\langle h_1, \ldots, h_q \rangle$ аддитивных порождающих I обладает свойством*

$$\forall h \in I[e + h = w((e + h_i), u_j),\ u_j \in U_1,\ j = 1, \ldots, q];$$

3) *если $Z[G]$ — целочисленная линейная оболочка G, то $\overline{U(Z[G])} = \overline{G}$, где черта означает образ при гомоморфизме φ_m (φ'_m).*

Литература

1. Fuchs L. *Abelian Groups.* – Budapest: Acad. Sci., 1958. – 367p.
2. Фукс Л. *Бесконечные абелевы группы.* Т. 2. – М.: Мир, 1977. – 416 с.
3. Goodaire E.G., Jespers E., Parmenter M.M. *Determining units in some integral group rings* // Canad. Math. Bull. – 1990. – V. 33. – № 2. – P. 242–246.
4. Ritter J., Sehgal S.K. *Construction of units in integral group rings of finite nilpotent groups* // Trans. Amer. Math. Soc. – 1991. – V. 324. – № 2. – P. 603–621.
5. Алеев Р.Ж. *Единицы полей характеров и центральные единицы целочисленных групповых колец конечных групп* // Матем. тр. – Новосибирск, 2000. – Т. 3. – № 1. – С. 3–37.
6. Попова А.М. *Некоторые алгоритмические проблемы для матричных колец.* – М., 1979. – 9 с. – Деп. в ВИНИТИ 27.07.79, № 2852-79.
7. Попова А.М. *Нахождение определяющих соотношений для конечно-порожденного модуля над конечно-порожденным матричным кольцом* – М., 1984. – 15 с. – Деп. в ВИНИТИ 24.08.84, № 6010-84.
8. Попова А.М. *Группы единиц абсолютно неприводимых матричных колец* // Актуальн. пробл. современ. матем. – Новосибирск, 1997. – Т. 3. – С. 155–161.
9. Попова А.М. *Мультипликативные группы конечно-порожденных неприводимых матричных колец* // Фундаментальн. и прикл. матем. – 1999. – Т. 5. – № 3. – С. 743–749.
10. Попова А.М. *Описание групп единиц неприводимых матричных колец* // Алгебра и теория моделей. – Новосибирск, 1997. – С. 152–159.
11. Супруненко Д.А. *Группы матриц.* – М.: Наука, 1972. – 351 с.
12. Джекобсон Н. *Строение колец.* – М.: Ин. лит., 1961. – 392 с.
13. Боревич З.И., Шафаревич И.Р. *Теория чисел.* – М.: Наука, 1985. – 503 с.
14. Попова А.М. *Конечно-порожденные кольца и их мультипликативная структура* // Тр. конф. по математике, посвящ. памяти А.Д. Тайманова. – Алматы, 1998. – С. 114–117.
15. Попова А.М. *Группы обратимых элементов матричных колец* // Сиб. матем. журн. – 1999. – Т. 40. – № 5. – С. 1127–1136.

Новосибирский государственный технический университет

Поступила 02.07.2001