ИЗВЕСТИЯ ВЫСШИХ УЧЕБНЫХ ЗАВЕДЕНИЙ

2001 МАТЕМАТИКА № 7 (470)

УДК 512.573

*М.Н. КУБЕНСКИЙ*

# АРИФМЕТИЧЕСКИЕ ВЛОЖЕНИЯ ПРОСТЫХ ЦЕНТРАЛЬНЫХ АЛГЕБР В АЛГЕБРУ МАТРИЦ

В данной работе обобщаются результаты из [1] на вложения простых центральных алгебр в алгебру матриц. Б.А. Венков в своих работах по арифметике кватернионов ввел (по аналогии с комплексными числами) понятия поворотов кватернионов. Развивая теорию поворотов, Ю.В. Линник применил ее к исследованию представлений чисел тернарными квадратичными формами. В дальнейшем другие авторы развивали теорию поворотов, обобщая ее на порядки в алгебрах обобщенных кватернионов. Подробную библиографию по этой теме можно найти в [2]. В этой же работе авторы предложили вместо поворотов кватернионов рассматривать "повороты" вложений с некоторым "арифметическим" условием. Это позволило обобщить теорию поворотов на простые центральные алгебры над алгебраическими числовыми полями.

Пусть $\mathfrak{A}$ — простая центральная алгебра над полем рациональных чисел $\mathbb{Q}$ размерности $n$. Как обычно, буквой $A$ внизу будут обозначаться адельные объекты, соответствующие глобальным: $\mathfrak{A}_A$ — кольцо аделей алгебры $\mathfrak{A}$, $\mathbb{Q}_A$ — кольцо аделей поля $\mathbb{Q}$ и т. д. Через $\mathfrak{A}^*_A$, $\mathbb{Q}^*_A$, $\mathfrak{O}^*_A$ и т. д. будут обозначаться идели (т. е. обратимые адели) соответствующих колец аделей. Если $\lambda_A \in \mathfrak{A}^*_A$, то $\lambda_A = (\dots, \lambda_p, \dots)$, где $\lambda_p$ означает $p$-компоненту и $\|\lambda_p\|_p = 1$ для почти всех $p$, пробегающих простые числа в $\mathbb{Z}$ и $\infty$. Более подробное описание и обозначение адельных объектов можно найти в ([3], с. 271).

Пусть $M_n(\mathbb{Q})$ — алгебра матриц размера $n \times n$ над полем $\mathbb{Q}$ рациональных чисел. Все вложения алгебры $\mathfrak{A}$ в $M_n(\mathbb{Q})$ по теореме Сколема–Нётер сопряжены и, следовательно, с алгебраической точки зрения неразличимы. Рассмотрим теперь эти вложения с арифметической точки зрения. Пусть $\mathfrak{O}$ — порядок в алгебре $\mathfrak{A}$. Рассмотрим множество вложений $\tau$ алгебры $\mathfrak{A}$ в $M_n(\mathbb{Q})$ с арифметическим условием

$$\tau(\mathfrak{O}) = \tau(\mathfrak{A}) \cap M_n(\mathbb{Z}). \tag{1}$$

Если $V$ — произвольная матрица из $GL_n(\mathbb{Q})$, то для $V^{-1}\tau V$ необязательно должно выполняться условие (1). В то же время, если $V \in GL_n(\mathbb{Z})$ (т. е. $V$ целая и $\det V = \pm 1$), то условие (1) должно выполняться для $\tau$ и $V^{-1}\tau V$ одновременно.

**Определение 1.** Два вложения $\tau_1$ и $\tau_2$ алгебры $\mathfrak{A}$ в $M_n(\mathbb{Q})$ называются эквивалентными, если существует такая матрица $V$ из $GL_n(\mathbb{Z})$, что $\tau_2 = V^{-1}\tau_1 V$.

Пусть теперь $I$ — некоторый идеал в алгебре $\mathfrak{A}$, $\mathfrak{O}_I$ — его левый порядок. Зафиксируем в $I$ базис $\omega_1, \dots, \omega_n$ и построим следующее вложение $\tau_I$ алгебры $\mathfrak{A}$ в $M_n(\mathbb{Q})$:

$$\tau_i(\alpha) \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix} = \alpha \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix}.$$

Легко проверить, что

$$\tau_I(\mathfrak{O}_I) = \tau_I(\mathfrak{A}) \cap M_n(\mathbb{Z}).$$

Будем говорить, что вложение $\tau_I$ связано с идеалом $I$.

**Лемма 1.** *Любое вложение $\tau$ алгебры $\mathfrak{A}$ в $M_N(\mathbb{Q})$ получается описанным выше образом для некоторого идеала $J$.*

**Доказательство.** Пусть дано произвольное вложение алгебры $\mathfrak{A}$ в $M_n(\mathbb{Q})$. Построим для некоторого идеала $I$ в алгебре $\mathfrak{A}$ и его базиса $\omega_1, \ldots, \omega_n$ соответствующее вложение $\tau_I$. По теореме Сколема–Нётер $\tau$ и $\tau_I$ сопряжены. Следовательно, существует такая матрица $A \in GL_n(\mathbb{Q})$, что $\tau = A^{-1}\tau_I A$. Для любого $\alpha$ из $\mathfrak{A}$ имеют место следующие равенства:

$$\tau_I(\alpha) = \begin{pmatrix}\omega_1\\ \vdots\\ \omega_n\end{pmatrix} = \alpha \begin{pmatrix}\omega_1\\ \vdots\\ \omega_n\end{pmatrix}, \quad \tau(\alpha)A^{-1}\begin{pmatrix}\omega_1\\ \vdots\\ \omega_n\end{pmatrix} = A^{-1}\tau_I(\alpha)AA^{-1}\begin{pmatrix}\omega_1\\ \vdots\\ \omega_n\end{pmatrix} = \alpha A^{-1}\begin{pmatrix}\omega_1\\ \vdots\\ \omega_n\end{pmatrix}.$$

Пусть $\begin{pmatrix}\eta_1\\ \vdots\\ \eta_n\end{pmatrix} = A^{-1}\begin{pmatrix}\omega_1\\ \vdots\\ \omega_n\end{pmatrix}$. Тогда $\tau(\alpha)\begin{pmatrix}\eta_1\\ \vdots\\ \eta_n\end{pmatrix} = \alpha\begin{pmatrix}\eta_1\\ \vdots\\ \eta_n\end{pmatrix}$. Если $J$ — идеал с базисом $\eta_1, \ldots, \eta_n$, то $\tau = \tau_J$ — вложение, связанное с идеалом $J$. $\square$

Введем более широкое понятие эквивалентности, чем в определении 1. Пусть $\mathbb{Z}_p$ — кольцо целых $p$-адических чисел.

**Определение 2** (ср. [4], [5]). Два вложения $\tau_1$ и $\tau_2$ алгебры $\mathfrak{A}$ в $M_n(\mathbb{Q})$ называются поворотно эквивалентными, если для любого простого числа $p$ существует такая матрица $V_p \in GL_n(\mathbb{Z}_p)$, что $\tau_2 = V_p^{-1}\tau_1 V_p$.

**Лемма 2.** *Пусть $k$ — некоторое поле, $\mathfrak{A}$ — простая центральная алгебра над $k$ размерности $n$ и $\tau$ — вложение $\mathfrak{A}$ в $M_n(k)$, порождаемое базисами алгебры $\mathfrak{A}$ : $\omega_1, \ldots, \omega_n$ и $\eta_1, \ldots, \eta_n$, т. е. для любого $\alpha \in \mathfrak{A}$*

$$\begin{aligned}\tau(\alpha)\begin{pmatrix}\omega_1\\ \vdots\\ \omega_n\end{pmatrix} &= \alpha\begin{pmatrix}\omega_1\\ \vdots\\ \omega_n\end{pmatrix},\\ \tau(\alpha)\begin{pmatrix}\eta_1\\ \vdots\\ \eta_n\end{pmatrix} &= \alpha\begin{pmatrix}\eta_1\\ \vdots\\ \eta_n\end{pmatrix}.\end{aligned} \tag{2}$$

*Тогда существует такой элемент $\lambda \in \mathfrak{A}^*$, что*

$$\begin{pmatrix}\omega_1\\ \vdots\\ \omega_n\end{pmatrix} = \begin{pmatrix}\eta_1\\ \vdots\\ \eta_n\end{pmatrix}\lambda.$$

**Доказательство.** Так как $\omega_1, \ldots, \omega_n$ и $\eta_1, \ldots, \eta_n$ — базисы алгебры $\mathfrak{A}$, то существует такая матрица $U \in GL_n(k)$, что

$$U\begin{pmatrix}\omega_1\\ \vdots\\ \omega_n\end{pmatrix} = \begin{pmatrix}\eta_1\\ \vdots\\ \eta_n\end{pmatrix}.$$

Из равенства (2) получаем

$$U\tau(\alpha)\begin{pmatrix}\omega_1\\ \vdots\\ \omega_n\end{pmatrix} = \alpha U\begin{pmatrix}\omega_1\\ \vdots\\ \omega_n\end{pmatrix}, \quad \tau(\alpha)U\begin{pmatrix}\omega_1\\ \vdots\\ \omega_n\end{pmatrix} = \alpha U\begin{pmatrix}\omega_1\\ \vdots\\ \omega_n\end{pmatrix}.$$

Отсюда (т. к. $\omega_1, \ldots, \omega_n$ — базис) $U\tau(\alpha) = \tau(\alpha)U$ для любого $\alpha$. По теореме из ([6], с. 128) существует такое $\lambda$ из $\mathfrak{A}^*$, что

$$\begin{pmatrix} \eta_1 \\ \vdots \\ \eta_n \end{pmatrix} = U \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix} = \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix} \lambda. \quad \square$$

**Теорема.** *Пусть вложение $\tau_I$ связано с идеалом $I$, а вложение $\tau_J$ — с идеалом $J$. Вложения $\tau_I$ и $\tau_J$ поворотно эквивалентны тогда и только тогда, когда*

1) $\mathfrak{O}_I = \mathfrak{O}_J$;
2) *существует такой идель $\lambda_A = (\ldots, \lambda_p, \ldots)$ из $\mathfrak{A}_A^*$, что $I = J\lambda_A$*

*(левые порядки идеалов $I$ и $J$ совпадают, а правые родственны, т. е. локально сопряжены).*

**Доказательство. Необходимость.** Пусть $\tau_I$ и $\tau_J$ поворотно эквивалентны. Тогда для любого простого $p$ существует такая матрица $E_p \in GL_n(\mathbb{Z}_p)$, что $\tau_J = E_p^{-1}\tau_I E_p$. Пусть базисы идеалов $I$ и $J$, связанных с вложениями $\tau_I$ и $\tau_J$, будут соответственно $\omega_1, \ldots, \omega_n$ и $\eta_1, \ldots, \eta_n$. Тогда для любого $\alpha$ из $\mathfrak{A} \otimes_{\mathbb{Q}} \mathbb{Q}_p$ будем иметь

$$\begin{aligned} \tau_I(\alpha) \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix} &= \alpha \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix}, \\ E_p^{-1}\tau_I(\alpha)E_p \begin{pmatrix} \eta_1 \\ \vdots \\ \eta_n \end{pmatrix} &= \alpha \begin{pmatrix} \eta_1 \\ \vdots \\ \eta_n \end{pmatrix} \end{aligned} \tag{3}$$

или

$$\tau_I(\alpha) \left( E_p \begin{pmatrix} \eta_1 \\ \vdots \\ \eta_n \end{pmatrix} \right) = \alpha E_p \begin{pmatrix} \eta_1 \\ \vdots \\ \eta_n \end{pmatrix}. \tag{4}$$

Из (3) и (4) по лемме 2 следует, что существует такой элемент $\lambda_A = (\ldots, \lambda_p, \ldots)$ из $\mathfrak{A}_A^*$, что для любого $p$

$$\begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix} = E_p \begin{pmatrix} \eta_1 \\ \vdots \\ \eta_n \end{pmatrix} \lambda_p. \tag{5}$$

Далее

$$\tau_J(\mathfrak{O}_I) = \bigcap_p (E_p^{-1}\tau(\mathfrak{O}_I)E_p) = \bigcap_p (E_p^{-1}(\tau_I(\mathfrak{A}) \cap M_n(\mathbb{Z}))E_p) =$$
$$= \bigcap_p E_p^{-1}\tau_I(\mathfrak{A})E_p \cap M_n(\mathbb{Z}) = \tau_J(\mathfrak{A}) \cap M_n(\mathbb{Z}) = \tau_J(\mathfrak{O}_J).$$

Отсюда следует

$$\mathfrak{O}_I = \mathfrak{O}_J. \tag{6}$$

Из равенств (5) и (6) вытекает необходимость условий теоремы.

**Достаточность.** Пусть $\mathfrak{O}_I = \mathfrak{O}_J$ и для некоторого иделя $\lambda_A = (\ldots, \lambda_p, \ldots)$ из $\mathfrak{A}_A^*$ имеет место $I = J\lambda_A$. Пусть $\omega_1, \ldots, \omega_n$ и $\eta_1, \ldots, \eta_n$ — базисы идеалов $I$ и $J$, задающих вложения $\tau_I$ и

$\tau_J$ соответственно. Для любого простого $p$ имеем $I_p = J_p\lambda_p$. Следовательно, существует такая матрица $E_p \in GL_n(\mathbb{Z}_p)$, что

$$\begin{pmatrix}\omega_1\\ \vdots\\ \omega_n\end{pmatrix} = E_p \begin{pmatrix}\eta_1\\ \vdots\\ \eta_n\end{pmatrix} \lambda_p.$$

Отсюда следует, что для любого $\alpha$ из $\mathfrak{A}$

$$E_p\tau_J(\alpha)E_p^{-1}\begin{pmatrix}\omega_1\\ \vdots\\ \omega_n\end{pmatrix} = E_p\tau_J(\alpha)\begin{pmatrix}\eta_1\\ \vdots\\ \eta_n\end{pmatrix}\lambda_p = E_p\alpha\begin{pmatrix}\eta_1\\ \vdots\\ \eta_n\end{pmatrix}\lambda_p = \alpha\begin{pmatrix}\omega_1\\ \vdots\\ \omega_n\end{pmatrix}.$$

Следовательно, для любого $\alpha$ и любого простого $p$

$$\tau_I(\alpha) = E_p\tau_J(\alpha)E_p^{-1}, \quad E_p \in GL_n(\mathbb{Z}_p),$$

что означает поворотную эквивалентность $\tau_I$ и $\tau_J$. $\square$

Если определить действие локально-главных идеалов на вложениях (см. [1], [7]), то можно на основании этой теоремы заключить, что все вложения с условием (1), для которых $\mathfrak{O}$ — максимальный порядок, образуют одну орбиту (ср. [2], п. 5).

## Литература


1. Кубенский М.Н., Малышев А.В. *К теории целых поворотов в алгебре матриц порядка n над полем рациональных чисел* // Вестн. С.-Петерб. ун-та. Сер. 1. – 1993. – Вып. 2. – С. 38–60.
2. Кубенский М.Н., Малышев А.В. *Теория поворотов в простых центральных алгебрах* // Acta Arithmetica. – 1990. – V. 53. – P. 477–498.
3. Платонов В.П., Рапинчук А.С. *Алгебраические группы и теория чисел.* – М.: Наука, 1991. – 654 с.
4. Венков Б.А. *Об арифметике кватернионов* // Изв. АН СССР. Отд. физ.-матем. наук. – 1929. – СС. 489–504, 535–562, 607–622.
5. Линник Ю.В. *О представлении больших чисел положительными тернарными квадратичными формами* // Изв. АН СССР. Сер. матем. – 1940. – № 4. – С. 363–402.
6. Вейль Г. *Классические группы, их инварианты и представления.* – М.: Ин. лит., 1947.
7. Кубенский М.Н., Малышев А.В. *Погружение алгебр в простые центральные алгебры* // Аналитич. теория чисел. – Петрозаводск, 1992. – С. 101–105.



*Высшее инженерное морское училище* (*Санкт-Петербург*)



*Поступили*
*первый вариант* 27.02.1997
*окончательный вариант* 20.11.2000