l = Länge von g. Nach dem Gesagten ist jetzt klar, daß

$$\left|\frac{D(L)}{8x}\right|\frac{2\chi i}{t}\sum_{(1/t)|\omega-x|<1\leqslant(1/t)|\omega+x|}\frac{t}{\omega}$$

eine Riemannsche Summe ist, die für $t\to\infty$ gegen das Integral

$$\int_{-1}^{1}\frac{d(i\chi y)}{\chi(\sqrt{1-y^2}+iy)}=i\int_{-1}^{1}\frac{dy}{\sqrt{1-y^2}+iy}=2i\int_{0}^{1}\sqrt{1-y^2}\,dy=\frac{\pi i}{2}$$

konvergiert. Damit ist alles bewiesen.

Abschließend ist noch zu bemerken, daß der Satz von van der Corput nur zum Beweis von Satz 1 im Falle $k=1$ benötigt wird, nicht jedoch im Falle $k=2$, wo ein völlig elementares Argument zum Ziel führt.

Literatur

[1] E. Hecke, *Mathematische Werke*, Vandenhoeck & Ruprecht, Göttingen 1970.
[2] E. Landau, *Vorlesungen über Zahlentheorie*, Bd. II, Leipzig 1927.
[3] R. Sczech, *Zur Summation von L-Reihen*, Bonner Mathematische Schriften Nr. 141, Bonn 1982.
[4] A. Weil, *Elliptic functions according to Eisenstein and Kronecker*, Springer, Berlin–Heidelberg–New York 1976.

MAX-PLANCK-INSTITUT
FÜR MATHEMATIK
Gottfried-Claren-Straße 26
D-5300 Bonn 3
Federal Republic of Germany
DEPARTMENT OF MATHEMATICS
RUTGERS UNIVERSITY
Newark, NJ 07102
USA

Eingegangen am 28.10.1988
und in revidierter Form am 20.2.1989 (1881)

ACTA ARITHMETICA
LIII (1990)

Теория поворотов в простых центральных алгебрах

М. Н. Кубенский, А. В. Малышев (Ленинград)

Памяти Владимира Геннадиевича
Спринджука посвящается

1. Введение. Цель предлагаемой работы — обобщение на простые центральные алгебры теории поворотов целых векторов, построенной Б. А. Венковым [1] для гурвицева порядка алгебры кватернионов Гамильтона над полем рациональных чисел. В этой статье мы пользуемся общепринятыми определениями и известными результатами теории колец и алгебр — см. [14], [23], [27], [11]. Теория поворотов Б. А. Венкова обобщалась на другие кватернионные алгебры и алгебры матриц второго порядка Ю. В. Линником [4], [5], А. В. Малышевым [7], А. В. Малышевым и У. М. Пачевым [8], Ю. Г. Тетериным [9] (см. также Райс [24], Рем [22] и Шеманске [25]). Наиболее интересные и общие результаты здесь принадлежат Ю. Г. Тетерину [9], который построил теорию поворотов целых векторов порядков в произвольных кватернионных алгебрах над полем рациональных чисел (по-видимому, только технические трудности возникают при обобщении методики и результатов работы [9] на кватернионные алгебры над алгебраическими числовыми полями).

В нашей работе обобщение этих результатов на простые центральные алгебры над алгебраическими числовыми полями достигается существенным изменением методики исследования: предлагается иная конструкция поворотов, мы рассматриваем не повороты целых векторов, а „повороты" соответсвующих вложений расширений основного поля в рассматриваемую алгебру. Такая конструкция в частном случае кватернионной алгебры была предложена в статье [2] (для произвольных простых центральных алгебр она намечена в заметке [3]).

В §2 нашей работы детально описывается и обосновывается конструкция целого поворота в простой центральной алгебре над полем алгебраических чисел. Построенным поворотам (точнее, их „связкам") взаимно однозначно сопоставляются классы идеалов соответствующего конечного расширения базисного алгебраического числового поля (см. теорему 1). В теореме 2 получена формула для числа орбит связок при действии группы классов. В §3 рассматривается и изучается понятие поворотной эквивалентности, рассматривается задача, обратная задаче §2 конструирования поворотов, — нахождение условий, при которых существует поворот, переводящий данное вложение в другое заданное вложение (см. теорему 3).

Далее общие исследования §§2–3, являющиеся основными в работе, применяются в частных случаях алгебры кватернионов (§4) — ср. [9], [2]; алгебры квадратных матриц n-го порядка (§5). Исследования §4 являются новым изложением работ [9], [2] и обобщением их на алгебраические числовые поля. В частном случае $n = 2$ и поля $\boldsymbol{Q}$ исследования §§2, 3, 5 приводят к результатам [8].

Помимо самостоятельного интереса исследования теории поворотов для простых центральных алгебр, в частности, алгебры матриц n-го порядка, по-видимому, найдут применения при осуществлении плана Ю. В. Линника [6], [19] перенесения дискретного эргодического метода на матрицы n-го порядка и на исследования эргодических свойств алгебраических числовых полей.

Предлагаемая статья не исчерпывает всех задач, естественно возникающих в теории целых поворотов. Этим задачам, которые явно или неявно содержатся в §2–5, мы имеем в виду посвятить дальнейшие исследования. Особенно это касается специального рассмотрения частного случая алгебры матриц n-го порядка над алгебраическим числовым полем, ибо §5 содержит лишь простейшие результаты по теории поворотов для такой алгебры.

2. Вложения алгебраических расширений и конструирование их поворотов. Пусть $\mathfrak{A} = \mathfrak{A}/k$ — простая центральная алгебра над алгебраическим числовым полем k (конечным расширением поля рациональных чисел $\boldsymbol{Q}$); ω — кольцо всех целых элементов поля k. Известно ([14], [27]), что ранг $\operatorname{rang}\mathfrak{A} = [\mathfrak{A}:k] = n^2$, где n — целое число. Пусть $\mathfrak{O}$ — порядок (не обязательно максимальный) в алгебре $\mathfrak{A}$. Порядком мы называем кольцо $\mathfrak{O}$ с единицей, являющееся полной k-решеткой в $\mathfrak{A}$; под полной k-решеткой (ср. [27]) мы понимаем конечно порожденный ω-модуль, содержащий базис алгебры $\mathfrak{A}/k$.

Пусть K — расширение поля k степени n, $[K:k] = n$, Ω — кольцо целых элементов (не обязательно всех) алгебраического числового поля K. Рассмотрим вложение (мономорфизм) τ поля K в алгебру $\mathfrak{A}$

$$\tau: K \to \mathfrak{A}. \tag{2.1}$$

Тогда (см. [14], [27]) $\tau(K) = \mathfrak{B}$ — максимальное подполе алгебры $\mathfrak{A}$. Будем рассматривать только оптимальные (ср. [15]) вложения τ, т.е. вложения (1) с условием

$$\tau(\Omega) = \tau(K) \cap \mathfrak{O} \tag{2.2}$$

(мы предполагаем, что такие вложения имеются).

Введем следующие обозначения. Пусть v — какое-либо нормирование поля k; k_v и ω_v — пополнения по этому нормированию; $H \subset \mathfrak{A}$ или $H \subset K$, обозначим через H_v ω_v-модуль, порожденный над ω_v множеством H. В частности, $\mathfrak{O}_v = \{\alpha\}_v$, где множество $\{\alpha\}$ порождает над ω порядок $\mathfrak{O}$. Конечные нормирования v мы отождествляем с простыми идеалами $\mathfrak{p}$ кольца ω. Пусть $V_\infty = S$ — множество $\{v\}$ бесконечных нормирований v. Тогда [27]

$$\mathfrak{O} = \bigcap_{v \notin V_\infty} (\mathfrak{O}_v \cap \mathfrak{A}) = \bigcap_{\mathfrak{p}} (\mathfrak{O}_\mathfrak{p} \cap \mathfrak{A}), \tag{2.3}$$

где $\mathfrak{p}$ пробегает все простые идеалы (конечные нормирования) поля k (кольца ω);

$$\Omega = \bigcap_{\mathfrak{P}} (\Omega_\mathfrak{P} \cap K), \tag{2.4}$$

где $\mathfrak{P}$ пробегает все простые идеалы (конечные нормирования) поля K; $K_\mathfrak{P}$, $\Omega_\mathfrak{P}$ — пополнения K, Ω по $\mathfrak{P}$. Пусть, соответственно,

$\mathfrak{A}_A$, K_A, k_A — кольца аделей алгебры $\mathfrak{A}$ и полей K и k;

$\mathfrak{O}_A$, Ω_A, ω_A — кольца целых аделей алгебры $\mathfrak{A}$ и полей K и k (кольца аделей порядков $\mathfrak{O}$, Ω и ω), так что ([27], гл. V, §2)

$$\mathfrak{O}_A = \prod_{v \in S} \mathfrak{A}_v \times \prod_{v \notin S} \mathfrak{O}_v; \tag{2.5}$$

$\mathfrak{A}_A^*$, K_A^*, k_A^* — группы аделей алгебры $\mathfrak{A}$, полей K и k;

$\mathfrak{O}_A^*$, Ω_A^*, ω_A^* — группы адельных единиц порядков $\mathfrak{O}$, Ω и ω; понятия кольца аделей, кольца целых аделей, группы аделей см., например, в [27], [11].

Пусть L — k-решетка в $\mathfrak{A}$, $x_A \in \mathfrak{A}_A$. Определяем (ср. [11], гл. X, §3, п. 3) умножение

$$x_A \cdot L = \bigcap_{v \notin S} (x_v L_v \cap \mathfrak{A}) \tag{2.6}$$

(аналогично определяется $L \cdot x_A$). Пусть $\mathfrak{O}$ — порядок в $\mathfrak{A}$; k-решетка L в $\mathfrak{A}$ называется *правым идеалом*, если

$$L \cdot \mathfrak{O} = L$$

(аналогично определяется и левый идеал $L' : \mathfrak{O} \cdot L' = L'$). В дальнейшем рассматриваются лишь локально главные правые (и левые) идеалы, т.е. идеалы вида $x_A \cdot \mathfrak{O}$ (соответственно: $\mathfrak{O} \cdot x_A$). В максимальном порядке $\mathfrak{O}$ все идеалы — локально главные (см. [27], [23]). Число классов локально главных правых идеалов конечно; оно равно числу двойных классов

$$\mathfrak{A}^* \backslash \mathfrak{A}_A^* / \mathfrak{O}_A^*.$$

То же верно для числа классов локально главных левых идеалов; оно равно $\#\ (\mathfrak{O}_A^* \backslash \mathfrak{A}_A^* / \mathfrak{A}^*)$.

Вложение τ поля K в алгебру $\mathfrak{A}$ можно однозначно продолжить до вложения

$$\tau\colon\ K_{\mathfrak{P}} \to \mathfrak{A}_{\mathfrak{p}}, \tag{2.7}$$

где $\mathfrak{P}$ — простой идеал поля K; $\mathfrak{p}$ — простой идеал поля k (кольца ω), однозначно определяемый условием $\mathfrak{P}\,|\,\mathfrak{p}$. А именно, в силу

$$\bigoplus_{\mathfrak{P}|\mathfrak{p}} K_{\mathfrak{P}} \cong k_{\mathfrak{p}} \otimes_k K$$

определяем:

$$\tau\colon\ K_{\mathfrak{P}} \to \bigoplus_{\mathfrak{P}|\mathfrak{p}} K_{\mathfrak{P}} \to k_{\mathfrak{p}} \otimes_k \tau(K). \tag{2.8}$$

Точно так же в силу

$$K_A \cong k_A \otimes_k K$$

вложение τ однозначно продолжается до вложения

$$\tau\colon\ K_A \to \mathfrak{A}_A, \tag{2.9}$$

а именно

$$\tau\colon\ K_A \to k_A \otimes_k \tau(K). \tag{2.10}$$

Прежде, чем приступить к описанию конструкции поворотов, приведем эквивалент условия (2.2) оптимальности вложения τ.

Лемма 1. *Условие* (2.2) *вложения τ поля K в алгебру $\mathfrak{A}$ равносильно следующему условию: для любого простого идеала $\mathfrak{P}$ поля K (кольца $\tilde{\Omega}$ всех целых чисел поля K)*

$$\tau(\Omega_{\mathfrak{P}}) = \tau(K_{\mathfrak{P}}) \cap \mathfrak{O}_{\mathfrak{p}}, \tag{2.11}$$

где $\mathfrak{p}$ — простой идеал поля k (кольца ω), однозначно определенный условием $\mathfrak{P}\,|\,\mathfrak{p}$. Здесь $\tau(K_{\mathfrak{P}})$ определено (2.8).

Доказательство. 1) Пусть для всех $\mathfrak{P}$ имеет место (2.11). Тогда в силу (2.4) и (2.11), учитывая, что $\tau(K) \subset \tau(K_{\mathfrak{P}})$, $\tau(K) \subset \mathfrak{A}$ последовательно получаем:

$$\begin{aligned}\tau(\Omega) &= \bigcap_{\mathfrak{P}} \big(\tau(K) \cap \tau(\Omega_{\mathfrak{P}})\big) = \bigcap_{\mathfrak{P}} \big(\tau(K) \cap \tau(K_{\mathfrak{P}}) \cap \mathfrak{O}_{\mathfrak{p}}\big) \\ &= \bigcap_{\mathfrak{P}} \big(\tau(K) \cap \mathfrak{O}_{\mathfrak{p}}\big) = \bigcap_{\mathfrak{P}} \big(\mathfrak{A} \cap \tau(K) \cap \mathfrak{O}_{\mathfrak{p}}\big) \\ &= \tau(K) \cap \bigcap_{\mathfrak{p}} (\mathfrak{O}_{\mathfrak{p}} \cap \mathfrak{A}) = \tau(K) \cap \mathfrak{O},\end{aligned}$$

и мы доказали (2.2).

2) Пусть имеет место (2.2). Обозначим через $\tilde{\Omega}$ кольцо всех целых элементов поля K, так что $\Omega \subset \tilde{\Omega}$. Пусть $\mathfrak{P}$ — фиксированный простой идеал кольца $\tilde{\Omega}$. Докажем, что для него имеет место (2.11).

а) Сначала докажем, что

$$\tau(\Omega_{\mathfrak{P}}) \subset \tau(K_{\mathfrak{P}}) \cap \mathfrak{O}_{\mathfrak{p}}. \tag{2.12}$$

Действительно, пусть $x_{\mathfrak{P}} \in \Omega_{\mathfrak{P}}$. Тогда найдется $x \in \Omega$, для которого для любого заданного целого числа $\nu \geqslant 0$

$$x \equiv x_{\mathfrak{P}} (\operatorname{mod} \mathfrak{p}^{\nu}), \quad x_{\mathfrak{P}} = x + \mathfrak{p}^{\nu} u, \quad u \in \tilde{\Omega}_{\mathfrak{P}}.$$

Подберем ν столь большим, что

$$\mathfrak{p}^{\nu} \tau(\tilde{\Omega}_{\mathfrak{P}}) \subset \mathfrak{O}_{\mathfrak{p}}.$$

Тогда

$$\tau(x_{\mathfrak{P}}) = \tau(x) + \mathfrak{p}^{\nu} \tau(u) \in \big(\tau(K) \cap \mathfrak{O}\big) + \mathfrak{O}_{\mathfrak{p}} \subset \mathfrak{O}_{\mathfrak{p}},$$

что и доказывает (2.12).

б) Теперь докажем. что

$$\tau(K_{\mathfrak{P}}) \cap \mathfrak{O}_{\mathfrak{p}} \subset \tau(\Omega_{\mathfrak{P}}). \tag{2.13}$$

Действительно, пусть

$$\tau(x_{\mathfrak{P}}) \in \tau(K_{\mathfrak{P}}) \cap \mathfrak{O}_{\mathfrak{p}}, \quad x_{\mathfrak{P}} \in K_{\mathfrak{P}}.$$

По теореме о сильной апроксимации для любого $\nu \geqslant 0$ найдется ([11], гл. II, §15; [27], гл. V, §2) $x \in K$, для которого

$$x \equiv x_{\mathfrak{P}} (\operatorname{mod} \mathfrak{p}^{\nu}), \quad x = x_{\mathfrak{P}} + \mathfrak{p}^{\nu} u, \quad u \in \tilde{\Omega}_{\mathfrak{P}},$$

$x \in \Omega_{\mathfrak{P}'}$ для всех $\mathfrak{P}' \neq \mathfrak{P}$, таких что $\Omega_{\mathfrak{P}'} \neq \tilde{\Omega}_{\mathfrak{P}'}$; $x \in \tilde{\Omega}_{\mathfrak{P}'}$ для остальных конечных нормирований. Подбираем ν столь большим, что

$$\mathfrak{p}^{\nu} \tau(\tilde{\Omega}_{\mathfrak{P}}) \subset \mathfrak{O}_{\mathfrak{p}}, \quad \mathfrak{p}^{\nu} \tilde{\Omega}_{\mathfrak{P}} \subset \Omega_{\mathfrak{P}}.$$

Тогда

$$\tau(x) = \tau(x_{\mathfrak{P}}) + \mathfrak{p}^{\nu} \tau(u) \in \big(\tau(K_{\mathfrak{P}}) \cap \mathfrak{O}_{\mathfrak{p}}\big) + \mathfrak{p}^{\nu} \tau(\Omega_{\mathfrak{P}}) \subset \mathfrak{O}_{\mathfrak{p}},$$

причем для любого $\mathfrak{P}' \neq \mathfrak{P}$ в силу (2.12)

$$\tau(x) \in \tau(\Omega_{\mathfrak{P}'}) \subset \tau(K_{\mathfrak{P}'}) \cap \mathfrak{O}_{\mathfrak{p}'} \subset \mathfrak{O}_{\mathfrak{p}'}, \quad \mathfrak{P}'\,|\,\mathfrak{p}.$$

Поэтому в силу (2.12) и (2.2)

$$\tau(x) = \bigcap_{\mathfrak{p}} \big(\mathfrak{O}_{\mathfrak{p}} \cap \tau(K)\big) = \tau(K) \cap \Big(\bigcap_{\mathfrak{p}} (\mathfrak{O}_{\mathfrak{p}} \cap \mathfrak{A})\Big) = \tau(K) \cap \mathfrak{O} = \tau(\Omega).$$

Отсюда следует, что

$$x_{\mathfrak{P}} = x - \mathfrak{p}^{\nu} u \in \Omega + \mathfrak{p}^{\nu} \tilde{\Omega}_{\mathfrak{P}} \subset \Omega + \Omega_{\mathfrak{P}} = \Omega_{\mathfrak{P}},$$

$$\tau(x_{\mathfrak{P}}) \in \tau(\Omega_{\mathfrak{P}}),$$

и мы доказали (2.13).

(2.12) и (2.13) приводят к (2.11). Итак, (2.3) и (2.11) равносильны. Лемма 1 доказана.

Следствие. *Пусть* $\tau(\Omega) = \tau(K) \cap \mathfrak{O}$. *Тогда* $\tau(\Omega_A^*) = \tau(K_A^*) \cap \mathfrak{O}_A^*$.

Обозначим через $\mathfrak{M}(\Omega, \mathfrak{O})$ множество всех оптимальных вложений τ кольца целых чисел Ω (не обязательно максимального) поля K в порядок $\mathfrak{O}$ (не обязательно максимальный) алгебры $\mathfrak{A}$. Пусть

(2.14) $$\psi_1\mathfrak{O}, \ldots, \psi_q\mathfrak{O}, \quad \psi_i \in \mathfrak{A}_A^* \quad (i = 1, \ldots, q)$$

— полный набор представителей классов локально главных идеалов порядка $\mathfrak{O}$ и пусть

(2.15) $$\mathfrak{O}_1 = \psi_1\mathfrak{O}\psi_1^{-1}, \quad \ldots, \quad \mathfrak{O}_q = \psi_q\mathfrak{O}\psi_q^{-1}$$

— соответствующие им левые порядки. Говорят, что порядки $\mathfrak{O}_i$ и $\mathfrak{O}_j$ $(i, j = 1, \ldots, q)$ связаны идеалом $\psi_i\psi_j^{-1}\mathfrak{O}_j$:

(2.16) $$\mathfrak{O}_i = \psi_i\psi_j^{-1}\mathfrak{O}_j(\psi_i\psi_j^{-1})^{-1}.$$

Наша конструкция поворотов вложений $\tau \in \mathfrak{M}(\Omega, \mathfrak{O}_i)$ $(i = 1, \ldots, q)$ предполагает рассмотрение сразу всех порядков (2.15) — ср. [9]. Пусть

$$\mathfrak{N} = \mathfrak{N}(\Omega, \mathfrak{O}) = \bigcup_{i=1}^{q} \mathfrak{M}(\Omega, \mathfrak{O}_i).$$

Для данного вложения $\tau \in \mathfrak{N}(\Omega, \mathfrak{O})$ и данного иделя $l_A \in K_A^*$ мы (не вполне однозначно) строим вложение $\tau_1 \in \mathfrak{N}(\Omega, \mathfrak{O})$, управляемое иделем l_A,

$$\tau_1 = l_A[\tau].$$

Конструкция опирается на следующее разложение (его частный случай для алгебры кватернионов см. Винера [26]).

Лемма 2. *Для любого индекса* $i = 1, \ldots, q$ *имеет место разложение*:

(2.17) $$\mathfrak{A}_A^* = \bigcup_{r=1}^{q} \mathfrak{A}^*\psi_r\psi_i^{-1}(\mathfrak{O}_i)_A^*$$

на попарно не пересекающиеся множества:

(2.18) $$\mathfrak{A}^*\psi_{r_1}\psi_i^{-1}(\mathfrak{O}_i)_A^* \cap \mathfrak{A}^*\psi_{r_2}\psi_i^{-1}(\mathfrak{O}_i)_A^* = \varnothing, \quad r_1 \neq r_2.$$

Доказательство. 1) Докажем (2.18). В противном случае найдутся $a \in \mathfrak{A}^*$, $(e_i)_A \in (\mathfrak{O}_i)_A^*$ с условием

$$\psi_{r_1}\psi_i^{-1} = a\psi_{r_2}\psi_i^{-1}(e_i)_A, \quad \psi_{r_1} = a\psi_{r_2}(\psi_i^{-1}(e_i)_A\psi_i) \in \mathfrak{A}^*\psi_{r_2}\mathfrak{O}_A^*$$

так что идеалы $\psi_{r_1}\mathfrak{O}$ и $\psi_{r_2}\mathfrak{O}$ принадлежат одному классу, что противоречит выбору (2.14).

2) Докажем (2.17). Пусть $x \in \mathfrak{A}_A^*$. Рассмотрим идеал $x\psi_i\mathfrak{O}$. Он принадлежит одному из классов идеалов (2.14), скажем $\psi_r\mathfrak{O}$. Тогда

$$x\psi_i = a\psi_r e_A, \quad a \in \mathfrak{A}^*, \quad e_A \in \mathfrak{O}_A^*.$$

Поэтому

$$x = a\psi_r\psi_i^{-1}(\psi_i e_A \psi_i^{-1}) \in \mathfrak{A}^*\psi_r\psi_i^{-1}(\mathfrak{O}_i)_A^*.$$

Лемма 2 доказана.

Следствие. *Для любого иделя* $l_A \in K_A^*$ *и любого вложения* $\tau \in \mathfrak{M}(\Omega, \mathfrak{O}_i)$ *найдется единственный индекс* r, *для которого*

(2.19) $$\tau(l_A) = h\psi_r\psi_i^{-1}(e_i)_A, \quad h = h(l_A) \in \mathfrak{A}^*, \quad (e_i)_A \in (\mathfrak{O}_i)_A^*.$$

При этом, если помимо (2.19), *имеет место равенство*

(2.20) $$\tau(l_A) = h'\psi_r\psi_i^{-1}(e_i')_A, \quad h' \in \mathfrak{A}^*, \quad (e_i')_A \in (\mathfrak{O}_i)_A^*,$$

то

(2.21) $$h' = h'(l_A) = he_r, \quad e_r \in \mathfrak{O}_r^*,$$

причем $(e_i')_A$ *однозначно определяется по* τ, l_A, h'.

Доказательство. $\tau(l_A) \in \mathfrak{A}_A^*$. Поэтому по лемме 2 найдется единственный индекс r, для которого

$$\tau(l_A) \in \mathfrak{A}^*\psi_r\psi_i^{-1}(\mathfrak{O}_i)_A^*,$$

так что имеет место (2.19). Если имеет место и (2.20), то

$$h' = h\psi_r\psi_i^{-1}(e_i)_A(e_i')_A^{-1}\psi_i\psi_r^{-1} = h \cdot (e_r)_A, \quad (e_r)_A \in (\mathfrak{O}_r)_A^*.$$

Так как h, $h' \in \mathfrak{A}^*$, то и $(e_r)_A \in \mathfrak{A}^*$, откуда:

$$(e_r)_A \in \mathfrak{A}^* \cap (\mathfrak{O}_r)_A^* \subset \mathfrak{O}_r^*, \quad (e_r)_A = e_r \in \mathfrak{O}_r^*.$$

Следствие доказано.

Приступим непосредственно к конструированию поворота данного вложения $\tau \in \mathfrak{M}(\Omega, \mathfrak{O}_i)$ поля K в алгебру $\mathfrak{A}$, управляемого заданным иделем $l_A \in K_A^*$. Пусть имеет место равенство (2.19) с фиксированными $h \in \mathfrak{A}^*$ и $(e_i)_A \in (\mathfrak{O}_i)_A^*$ (в нем r однозначно определено τ и l_A; степень произвола $h = h(l_A)$ описывается формулой (2.21); $(e_i)_A$ однозначно определено τ, l_A, h). Определяем отображение $\tau_1 = l_A[\tau] = l_A[\tau, h]$,

(2.22) $$\tau_1 \colon K \to \mathfrak{A},$$

формулой

(2.23) $$\tau_1 = h^{-1}\tau h,$$

где (2.23) означает, что для любого $x \in K$

(2.24) $$\tau_1(x) = h^{-1}\tau(x)h.$$

Лемма 3. *Отображение* $\tau_1 = l_A[\tau, h]$, *определенное равенствами* (2.19), (2.23)–(2.24), *есть вложение (мономорфизм)* K *в* $\mathfrak{A}$. *При этом*

$$\tau_1 = l_A[\tau] = l_A[\tau, h] \in \mathfrak{M}(\Omega, \mathfrak{O}_r).$$

Доказательство. То, что τ_1 — вложение K в $\mathfrak{A}$, следует из определения (2.19), (2.23)–(2.24). Докажем оптимальность вложения,

$$\tau_1(\Omega) = \tau_1(K) \cap \mathfrak{O}_r.$$

Действительно, учитывая (2.23)–(2.24) и (2.19), последовательно получаем:

$$\begin{aligned}
\tau_1(K)\cap\mathfrak{O}_r &= h^{-1}\tau(K)h\cap\mathfrak{O}_r = h^{-1}\tau(l_A)\tau(K)(\tau(l_A))^{-1}\cdot h\cap\mathfrak{O}_r \\
&= \psi_r\psi_i^{-1}(e_i)_A\tau(K)(e_i)_A^{-1}\psi_i\psi_r^{-1}\cap\mathfrak{O}_r \\
&= \psi_r\psi_i^{-1}(e_i)_A\{\tau(K)\cap(e_i)_A^{-1}\psi_i\psi_r^{-1}\mathfrak{O}_r\psi_r\psi_i^{-1}(e_i)_A\}(e_i)_A^{-1}\psi_i\psi_r^{-1} \\
&= \psi_r\psi_i^{-1}(e_i)_A\{\tau(K)\cap\mathfrak{O}_i\}(e_i)_A^{-1}\psi_i\psi_r^{-1} = \psi_r\psi_i^{-1}(e_i)_A\tau(\Omega)(e_i)_A^{-1}\psi_i\psi_r^{-1} \\
&= \psi_r\psi_i^{-1}(e_i)_A\cdot\tau(l_A)^{-1}\tau(\Omega)\tau(l_A)(e_i)_A^{-1}\psi_i\psi_r^{-1} = h^{-1}\tau(\Omega)h = \tau_1(\Omega).
\end{aligned}$$

Лемма 3 доказана.

Итак, на множестве оптимальных вложений

$$\mathfrak{N}(\Omega, \mathfrak{O}) = \bigcup_{i=1}^{q} \mathfrak{M}(\Omega, \mathfrak{O}_i)$$

поля K в алгебру $\mathfrak{A}$ мы определили операцию

$$l_A[\tau] = l_A[\tau, h], \quad \tau\in\mathfrak{N}(\Omega, \mathfrak{O}),$$

поворота вложения τ во вложение

$$\tau_1 = l_A[\tau] = l_A[\tau, h] \in \mathfrak{N}(\Omega, \mathfrak{O}),$$

управляемую заданным иделем $l_A\in K_A^*$. К сожалению, эта операция не однозначно определяется l_A и τ: она зависит также от h из равенства (2.19); степень произвола выбора h при данных l_A и τ описывается равенством (2.21). Чтобы избежать этой неоднозначности, будем рассматривать операцию поворота не на отдельных вложениях τ, а на их „связках" $\bar{\tau}$ — классах эквивалентных вложений.

Два оптимальных вложения $\tau, \tau'\in\mathfrak{M}(\Omega, \mathfrak{O}_i)$ поля K в алгебру $\mathfrak{A}$ называем эквивалентными, если найдется $e\in\mathfrak{O}_i^*$ для которого

$$e\tau e^{-1} = \tau'.$$

Отношение эквивалентности разбивает вложения $\tau\in\mathfrak{M}(\Omega, \mathfrak{O}_i)$ на классы, которые мы будем называть связками. Связку, определяемую вложением $\tau\in\mathfrak{M}(\Omega, \mathfrak{O}_i)$ обозначаем через

$$\bar{\tau} = \{e\tau e^{-1} \mid e\in\mathfrak{O}_i^*\}. \tag{2.25}$$

Ясно, что если $\tau\in\mathfrak{M}(\Omega, \mathfrak{O}_i)$ то

$$\bar{\tau} \subset \mathfrak{M}(\Omega, \mathfrak{O}_i), \tag{2.26}$$

так что множества $\mathfrak{M}(\Omega, \mathfrak{O}_i)$ $(i = 1, \ldots, q)$ разбиваются на попарно не пересекающиеся связки вложений $\bar{\tau}$. Обозначим через $\bar{\mathfrak{M}}(\Omega, \mathfrak{O}_i)$, множество связок входящих в $\mathfrak{M}(\Omega, \mathfrak{O}_i)$ $(i = 1, \ldots, q)$, а через

$$\bar{\mathfrak{N}} = \bar{\mathfrak{N}}(\Omega, \mathfrak{O}) = \bigcup_{i=1}^{q} \bar{\mathfrak{M}}(\Omega, \mathfrak{O}_i) \tag{2.27}$$

множество связок, входящих в $\mathfrak{N} = \mathfrak{N}(\Omega, \mathfrak{O})$.

На множестве $\bar{\mathfrak{N}} = \bar{\mathfrak{N}}(\Omega, \mathfrak{O})$ следующим образом определим однозначную операцию поворота данным иделем $l_A\in K_A^*$ связки $\bar{\tau}\in\bar{\mathfrak{N}}$ в связку $\bar{\tau}_1 = l_A[\bar{\tau}]\in\bar{\mathfrak{N}}$. Пусть $\bar{\tau}\in\bar{\mathfrak{N}}$, т.е. $\bar{\tau}\in\bar{\mathfrak{M}}(\Omega, \mathfrak{O}_i)$ для некоторого i, $1\leqslant i\leqslant q$; пусть τ — какое-либо фиксированное вложение из связки $\bar{\tau}$, $\tau\in\bar{\tau}$. По l_A и τ строим равенство (2.19), где r определено однозначно, а h — с точностью до равенства (2.21). По формуле (2.23) строим вложение $\tau_1 = l_A[\tau, h]\in\mathfrak{M}(\Omega, \mathfrak{O}_r)$. Определяем:

$$\bar{\tau}_1 = l_A[\bar{\tau}] = \overline{l_A[\tau, h]}. \tag{2.28}$$

Докажем корректность этого определения, т.е. докажем, что а) при данных l_A и τ равенство (2.28) не зависит от выбора h в равенстве (2.19); б) при данных l_A и $\bar{\tau}$ равенство (2.28) не зависит от выбора $\tau\in\bar{\tau}$.

Докажем а). Пусть $\tau\in\mathfrak{M}(\Omega, \mathfrak{O}_i)$ и выполнены (2.19) и (2.20), так что имеет место (2.21). Тогда по определению (2.23)–(2.24), учитывая лемму 3,

$$\tau_1'(x) = l_A[\tau, h'](x) = (h')^{-1}\tau(x)h' = e_r^{-1}h^{-1}\tau(x)he_r = e_r^{-1}\{l_A[\tau, h](x)\}e_r,$$

$$\tau_1'\in\mathfrak{M}(\Omega, \mathfrak{O}_r), \quad \bar{\tau}_1' = \bar{\tau}_1\in\bar{\mathfrak{M}}(\Omega, \mathfrak{O}_r).$$

Докажем б). Пусть $\tau, \tau'\in\bar{\tau}\in\bar{\mathfrak{M}}(\Omega, \mathfrak{O}_i)$, так что

$$\tau' = e\tau e^{-1}.$$

Отсюда, используя (2.19),

$$\tau'(l_A) = e\tau(l_A)e^{-1} = eh\psi_r\psi_i^{-1}(e_i)_A e^{-1}.$$

Поэтому

$$\begin{aligned}
\tau_1'(x) &= l_A[\tau', eh](x) = (eh)^{-1}\tau'(x)(eh) = h^{-1}\{e^{-1}\tau'(x)e\}h \\
&= h^{-1}\tau(x)h = \tau_1(x),
\end{aligned}$$

$$\bar{\tau}_1' = \bar{\tau}_1\in\bar{\mathfrak{M}}(\Omega, \mathfrak{O}_r).$$

Итак, на множестве $\bar{\mathfrak{N}}$ мы определили однозначную операцию $l_A[\bar\tau]$, задаваемую („управляемую") иделем $l_A \in K_A^*$, поворота любой связки $\bar\tau \in \bar{\mathfrak{N}}$ в некоторую связку $\bar\tau_1 = l_A[\bar\tau] \in \bar{\mathfrak{N}}$:

$$l_A\colon \bar{\mathfrak{N}} \to \bar{\mathfrak{N}}. \tag{2.29}$$

Докажем, что множество таких операций, „управляемых" группой иделей $\{l_A\} = K_A^*$, ассоциативно.

Лемма 4. *Пусть l_A, l'_A, $l''_A \in K_A^*$, причем $l_A = l'_A l''_A$. Тогда для любой связки $\bar\tau \in \bar{\mathfrak{N}}$*

$$l_A[\bar\tau] = l'_A[l''_A[\bar\tau]]. \tag{2.30}$$

Доказательство. Обозначим:

$$\bar\tau \in \bar{\mathfrak{M}}(\Omega, \mathfrak{D}_i), \quad \bar\tau_1 = l_A[\bar\tau] \in \bar{\mathfrak{M}}(\Omega, \mathfrak{D}_r),$$

$$\bar\tau_2 = l''_A[\bar\tau] \in \bar{\mathfrak{M}}(\Omega, \mathfrak{D}_t), \quad \bar\tau_{21} = l'_A[\bar\tau_2] = l'_A[l''_A[\bar\tau]].$$

Нам надо доказать, что

$$\bar\tau_{21} = \bar\tau_1. \tag{2.31}$$

Фиксировав $\tau \in \bar\tau$, строим равенство вида (2.19)

$$\tau(l''_A) = h''\psi_t\psi_i^{-1}(e''_i)_A, \quad h'' \in \mathfrak{A}^*, \quad (e''_i)_A \in (\mathfrak{D}_i)_A^*,$$

и по нему поворот:

$$\tau_2 = (h'')^{-1}\tau h'' \in \bar\tau_2. \tag{2.32}$$

Далее строим равенство вида (2.19)

$$\tau_2(l'_A) = h'\psi_r\psi_t^{-1}(e'_t)_A, \quad h' \in \mathfrak{A}^*, \quad (e'_t)_A \in (\mathfrak{D}_t)_A^*, \tag{2.33}$$

и по нему поворот

$$\tau_{21} = (h')^{-1}\tau_2 h' = (h''h')^{-1}\tau h''h', \quad h''h' \in \mathfrak{A}^*. \tag{2.34}$$

С другой стороны по (2.32) и (2.33)

$$\tau(l'_A) = (h''\tau_2(h'')^{-1})(l'_A) = h''\tau_2(l'_A)(h'')^{-1} = h''h'\psi_r\psi_t^{-1}(e'_t)(h'')^{-1},$$

$$\tau(l_A) = \tau(l'_A)\tau(l''_A) = h''h'\psi_r\psi_i^{-1}\{\psi_i\psi_t^{-1}(e'_t)_A\psi_t\psi_i^{-1}\}(e''_i)_A = h''h'\psi_r\psi_i^{-1}(e'''_i)_A,$$

$$(e'''_i)_A \in (\mathfrak{D}_i)_A^*,$$

так что

$$\tau_1 = l_A[\tau, h''h'] = (h''h')^{-1}\tau h''h', \quad h''h' \in \mathfrak{A}^*. \tag{2.35}$$

Теперь равенство (2.31) следует из (2.34) и (2.35).

Лемма доказана.

Группа операций (2.29) поворотов, управляемых группой иделей $\{l_A\} = K_A^*$, заданная на множестве связок $\bar{\mathfrak{N}} = \bar{\mathfrak{N}}(\Omega, \mathfrak{D})$ индуцирует группу

операций тех же поворотов на $\bar{\mathfrak{N}}$, управляемых группой $J(\Omega)$ собственных локально главных идеалов порядка Ω. Идеал I кольца Ω мы называем собственным, если Ω является кольцом множителей для I, т.е. если

$$\Omega = \{\alpha \in K \mid \alpha I \subset I\}. \tag{2.36}$$

Тогда (см. [27], гл. V, §3)

$$J(\Omega) \cong K_A^*/\Omega_A^*. \tag{2.37}$$

Это в свою очередь индуцирует управление поворотами на $\mathfrak{N}$ группой $\mathrm{cl}(\Omega)$ классов собственных локально главных идеалов порядка Ω;

$$\mathrm{cl}(\Omega) \cong J(\Omega)/K^* \cong K_A^*/\Omega_A^* K^*. \tag{2.38}$$

Для обоснования этих утверждений мы доказываем (см. ниже теорему 1), что стабилизатор операции $l_A[\bar\tau]$ для любой связки $\bar\tau \in \bar{\mathfrak{N}}$ равен $\Omega_A^* K^*$.

Теорема 1. *Описанная выше группа поворотов на $\bar{\mathfrak{N}}$, управляемая группой иделей K_A^*, индуцирует на $\bar{\mathfrak{N}}$ те же повороты, управляемые группой $\mathrm{cl}(\Omega)$ классов собственных локально главных идеалов порядка Ω. При этом неподвижные элементы имеет только единица группы $\mathrm{cl}(\Omega)$.*

Доказательство. В силу (2.38) нам достаточно доказать, что стабилизатор действия группы иделей K_A^* на данной связке $\bar\tau \in \bar{\mathfrak{N}}$ равен $\Omega_A^* \cdot K^*$.

Итак, пусть задана связка $\bar\tau \in \bar{\mathfrak{N}}$, $\bar\tau \in \bar{\mathfrak{M}}(\Omega, \mathfrak{D}_i)$, причем

$$l_A[\bar\tau] = \bar\tau, \quad l_A \in K_A^*. \tag{2.39}$$

Докажем, что

$$l_A \in \Omega_A^* K^*. \tag{2.40}$$

Фиксируем $\tau \in \bar\tau$. В силу (2.39) найдется h:

$$\tau(l_A) = h \cdot (e_i)_A, \quad h \in \mathfrak{A}^*, \quad (e_i)_A \in (\mathfrak{D}_i)_A^*,$$

и

$$h^{-1}\tau h = e\tau e^{-1}, \quad e \in \mathfrak{D}_i^* \subset \mathfrak{A},$$

так что для любого $x \in K$

$$\tau(x)(he) = (he)\tau(x).$$

Поэтому, так как $\tau(K)$ — максимальное поле в $\mathfrak{A}$, то

$$he \in \tau(K), \quad he = \tau(g), \quad g \in K^*.$$

Отсюда:

$$\tau(l_A) = \tau(g)e^{-1}(e_i)_A, \quad e^{-1}(e_i)_A = \tau(l_A g^{-1}),$$
$$e^{-1}(e_i)_A \in \tau(K_A) \cap (\mathfrak{D}_i)^*_A = \tau(\Omega^*_A),$$
$$\tau(l_A) \in \tau(\Omega^*_A)\tau(K^*), \quad l_A \in \Omega^*_A K^*,$$

и мы доказали (2.40).

Обратно, пусть имеет место (2.40), так что $l_A \in K^*_A$. Докажем (2.39). Имеем:

$$l_A = ge_A, \quad g \in K^*, \quad e_A \in \Omega^*_A,$$

откуда

$$\tau(l_A) = \tau(g)\tau(e_A), \quad \tau(g) \in \mathfrak{A}^*, \quad \tau(e_A) \in (\mathfrak{D}_i)^*_A,$$

так что по коммутативности

$$l_A[\tau, \tau(g)] = \tau(g)^{-1}\tau\tau(g) = \tau,$$

и мы доказали (2.39).

Теорема 1 доказана.

Под действием операции поворотов, управляемых $\mathrm{cl}(\Omega)$ (или $J(\Omega)$, или K^*_A), множество связок $\bar{\mathfrak{N}}$ распадается на орбиты, каждая из которых содержит $h(\Omega) = \#\,\mathrm{cl}(\Omega)$ элементов; $h(\Omega)$ — число классов собственных локально-главных идеалов кольца Ω. Таким образом, число орбит $s(\Omega, \mathfrak{D})$ поворотов связок $\bar{\mathfrak{N}}$ группой $\mathrm{cl}(\Omega)$ равно

$$s(\Omega, \mathfrak{D}) = \frac{\#\,\mathfrak{N}}{h(\Omega)}, \tag{2.41}$$

где $h(\Omega) = \#\,\mathrm{cl}(\Omega)$; здесь и далее $\#\,M = \mathrm{card}\, M$ — число элементов множества M.

Получим формулу для числа орбит $s(\Omega, \mathfrak{D})$. Пусть $\tau \in \mathfrak{M}(\Omega, \mathfrak{D})$. Определим множество $T_A \subset \mathfrak{A}^*_A$ следующим образом

$$T_A = T_A(\tau, \Omega) = \{t_A \in \mathfrak{A}^*_A \mid t_A^{-1}\tau(\Omega_A)t_A = \mathfrak{D}_A \cap t_A^{-1}\tau(K_A)t_A\}.$$

Заметим, что

$$\tau(K^*) \subset \tau(K^*_A) \subset T_A, \tag{2.42}$$

$$\mathfrak{D}^*_A \subset T_A \tag{2.43}$$

(это прямо следует из определения и коммутативности $\tau(K^*)$), и рассмотрим множества двойных классов

$$\tau(K^*_A)\backslash T_A/\mathfrak{D}^*_A, \quad \tau(K^*)\backslash T_A/\mathfrak{D}^*_A.$$

Следующее предложение в частном случае алгебры кватернионов и в других терминах содержится в монографии Винера [26] (теорема III.5.II).

Теорема 2. *Имеет место формула*

$$s(\Omega, \mathfrak{D}) = \#\,\{\tau(K^*_A)\backslash T_A/\mathfrak{D}^*_A\}. \tag{2.44}$$

Доказательство. В силу определения (2.41) нам достаточно доказать, что

$$\#\,\bar{\mathfrak{N}}(\Omega, \mathfrak{D}) = \#\,\{\tau(K^*)\backslash T_A/\mathfrak{D}^*_A\}, \tag{2.45}$$

$$\#\,\{\tau(K^*)\backslash T_A/\mathfrak{D}^*_A\} = h(\Omega)\,\#\,\{\tau(K^*_A)\backslash T_A/\mathfrak{D}^*_A\}. \tag{2.46}$$

Докажем (2.45). В силу (2.17) и (2.18)

$$\mathfrak{A}^*_A = \bigcup_{r=1}^{q} \mathfrak{A}^*\psi_r\mathfrak{D}^*_A, \quad \mathfrak{A}^*\psi_{r_1}\mathfrak{D}^*_A \cap \mathfrak{A}^*\psi_{r_2}\mathfrak{D}^*_A = \varnothing, \quad r_1 \neq r_2,$$

так что для $T_A \subset \mathfrak{A}^*_A$ имеет место дизъюнктное разложение

$$\begin{gathered} T_A = \bigcup_{r=1}^{q} T_r\psi_r\mathfrak{D}^*_A, \quad T_r \subset \mathfrak{A}^*, \\ T_{r_1}\psi_{r_1}\mathfrak{D}^*_A \cap T_{r_2}\psi_{r_2}\mathfrak{D}^*_A = \varnothing, \quad r_1 \neq r_2. \end{gathered} \tag{2.47}$$

Сначала докажем, что

$$\#\,\{\tau(K^*)\backslash T_r/\mathfrak{D}^*_r\} = \#\,\bar{\mathfrak{M}}(\Omega, \mathfrak{D}_r) \quad (r = 1, \ldots, q). \tag{2.48}$$

Действительно, пусть

$$t_A = t_r\psi_r e_A \in T_r\psi_r\mathfrak{D}^*_A \subset T_A.$$

Тогда

$$t_A^{-1}\tau(\Omega_A)t_A = \mathfrak{D}_A \cap t_A^{-1}\tau(K_A)t_A,$$
$$e_A^{-1}\psi_r^{-1}t_r^{-1}\tau(\Omega_A)t_r\psi_r e_A = \mathfrak{D}_A \cap e_A^{-1}\psi_r^{-1}t_r^{-1}\tau(K_A)t_r\psi_r e_A,$$
$$t_r^{-1}\tau(\Omega_A)t_r = \psi_r e_A\mathfrak{D}_A e_A^{-1}\psi_r^{-1} \cap t_r^{-1}\tau(K_A)t_r = (\mathfrak{D}_r)_A \cap t_r^{-1}\tau(K_A)t_r.$$

Поэтому, используя лемму 1, получаем

$$t_r^{-1}\tau t_r \in \mathfrak{M}(\Omega, \mathfrak{D}_r). \tag{2.49}$$

Обращая эти рассуждения, из (2.49) выведем:

$$t_r \in T_r.$$

Отсюда следует формула (2.48), если учесть, что равенство

$$t_r^{-1}\tau t_r = (t'_r)^{-1}\tau t'_r, \quad t_r,\ t'_r \in T_r,$$

равносильно включению $t'_r \in \tau(K^*)t_r$ (в силу коммутативности $\tau(K)$) и что

$$T_r\mathfrak{O}_r\psi_r\mathfrak{O}_A^* = T_r\psi_r\mathfrak{O}^*\mathfrak{O}_A^* = T_r\psi_r\mathfrak{O}_A^*.$$

Формула (2.45) следует из (2.47) и (2.48):

$$\# \{\tau(K^*)\backslash T_A/\mathfrak{O}_A^*\} = \sum_{r=1}^{q} \# \{\tau(K^*)\backslash T_r/\mathfrak{O}_r^*\}$$
$$= \sum_{r=1}^{q} \# \{\bar{\mathfrak{M}}(\Omega, \mathfrak{O}_r)\} = \# \bar{\mathfrak{N}}.$$

Докажем теперь формулу (2.46). Рассмотрим дизъюнктное разложение по двойным классам $\tau(K_A^*)\backslash T_A/\mathfrak{O}_A^*$:

$$T_A = \bigcup_{\nu=1}^{n} \tau(K_A^*)\lambda_\nu\mathfrak{O}_A^*, \quad \lambda_\nu \in T_A. \tag{2.50}$$

Разобьем (2.50) на более мелкое дизъюнктное разложение:

$$T_A = \bigcup_{\nu=1}^{n} \{ \bigcup_{\mu=1}^{m} \tau(K^*)\tau(\sigma_\mu)\} \lambda_\nu\mathfrak{O}_A^*, \tag{2.51}$$

где $\sigma_\mu \in K_A^*$ выбраны так, чтобы при данном ν множества

$$\tau(K^*)\tau(\sigma_\mu)\lambda_\nu\mathfrak{O}_A^*$$

попарно не пересекались. Заметим, что если

$$\tau(K^*)\tau(\sigma)\lambda_\nu\mathfrak{O}_A^* \cap \tau(K^*)\tau(\sigma')\lambda_\nu\mathfrak{O}_A^* \neq \varnothing; \quad \sigma, \sigma' \in K_A^*,$$

то

$$\tau(\sigma')\lambda_\nu = \tau(\delta)\tau(\sigma)\lambda_\nu e_A, \quad \delta \in K^*, \quad e_A \in \mathfrak{O}_A^*,$$
$$\lambda_\nu e_A \lambda_\nu^{-1} = \tau(\sigma)^{-1}\tau(\delta)^{-1}\tau(\sigma') \in \tau(K_A) \cap \lambda_\nu\mathfrak{O}_A^*\lambda_\nu^{-1}$$
$$= \lambda_\nu\{\lambda_\nu^{-1}\tau(K_A)\lambda_\nu \cap \mathfrak{O}_A^*\}\lambda_\nu^{-1}$$
$$= \lambda_\nu\lambda_\nu^{-1}\tau(\Omega_A^*)\lambda_\nu\lambda_\nu^{-1} = \tau(\Omega_A^*).$$

Поэтому $\tau(\sigma_\mu)$ определены с точностью до множителя из $\tau(K^*)\tau(\Omega_A^*)$ так что

$$m = \# (K_A^*/K^*\Omega_A^*) = h(\Omega). \tag{2.52}$$

Из (2.51) и (2.52) следует формула (2.46).

Теорема 2 доказана.

3. Поворотная эквивалентность связок. Пусть $\bar{\tau}_1, \bar{\tau}_2 \in \bar{\mathfrak{N}}$, $\bar{\tau}_1 \in \bar{\mathfrak{M}}(\Omega, \mathfrak{O}_i)$, $\bar{\tau}_2 \in \bar{\mathfrak{M}}(\Omega, \mathfrak{O}_j)$. Говорим, что связки $\bar{\tau}_1$ и $\bar{\tau}_2$ поворотно эквивалентны, если найдется идель $l_A \in K_A^*$ с условием

$$l_A[\bar{\tau}_1] = \bar{\tau}_2. \tag{3.1}$$

Можно говорить и о существовании класса идеалов $[l_A]$, определяемого иделем l_A, который управляет поворотом $\bar{\tau}_1$ в $\bar{\tau}_2$:

$$[l_A][\bar{\tau}_1] = \bar{\tau}_2. \tag{3.2}$$

Иначе говоря, $\bar{\tau}_1$ и $\bar{\tau}_2$ поворотно эквивалентны, если $\bar{\tau}_2$ лежит в орбите действия группы $\mathrm{cl}(\Omega)$ на связку $\bar{\tau}_1$:

$$\{[l_A][\bar{\tau}_1] \mid [l_A] \in \mathrm{cl}(\Omega)\}. \tag{3.3}$$

Теорема 3. *Для того, чтобы связки* $\bar{\tau}_1$, $\bar{\tau}_2 \in \bar{\mathfrak{N}}$, $\bar{\tau}_1 \in \bar{\mathfrak{M}}(\Omega, \mathfrak{O}_i)$, $\bar{\tau}_2 \in \bar{\mathfrak{M}}(\Omega, \mathfrak{O}_j)$, *были поворотно эквивалентны, необходимо и достаточно, чтобы для любого идеала* $\mathfrak{m}$ *кольца* ω *всех целых чисел поля* k *для любых* $\tau_1 \in \bar{\tau}_1$, $\tau_2 \in \bar{\tau}_2$ *нашелся элемент* $w \in \psi_i\psi_j^{-1}\mathfrak{O}_j$, *для которого*

$$\tau_2 = w^{-1}\tau_1 w, \quad \text{н.о.д.} \left(n(w\psi_j\psi_i^{-1}), \mathfrak{m}\right) = (1); \tag{3.4}$$

здесь $n(\ldots)$ — *норма элемента* (см. [27], гл. IX, §2).

Доказательство. 1) Необходимость. Пусть имеет место (3.2). Тогда найдется такой идель $l_A \in [l_A]$, что из теоремы о сильной аппроксимации (см. [11], гл. II, §15) следует, что

$$l_A \in \Omega_A, \quad \text{н.о.д.} \left(n(l_A), \mathfrak{m}\right) = (1), \tag{3.5}$$

и имеет место (3.1). Фиксируем $\tau_1 \in \bar{\tau}_1$, $\tau_2 \in \bar{\tau}_2$. Тогда

$$\tau_1(l_A) = h\psi_j\psi_i^{-1}(e_i)_A, \quad h \in \mathfrak{A}^*, \quad (e_i)_A \in (\mathfrak{O}_i)_A^*;$$
$$\tau_2 = e_j^{-1}h^{-1}\tau_1 h e_j, \quad e_j \in \mathfrak{O}_j^*.$$

С другой стороны

$$h\psi_j\psi_i^{-1}(e_i)_A \in (\mathfrak{O}_i)_A, \quad h \in (\mathfrak{O}_i)_A\psi_i\psi_j^{-1} = \psi_i\psi_j^{-1}(\mathfrak{O}_j)_A, \quad he_j \in \psi_i\psi_j^{-1}(\mathfrak{O}_j)_A.$$

Полагая

$$w = he_j,$$

приходим к (3.4), ибо

$$\tau_2 = w^{-1}\tau_1 w,$$

$$n(w) = n(h)n(e_j) = n(e_j)n(\tau(l_A))\frac{1}{n(\psi_j\psi_i^{-1})n((e_i)_A)}$$
$$= n(l_A)\cdot\{n(\psi_j\psi_i^{-1})\}^{-1}\cdot\{n(e_j)\cdot n((e_i)_A)\}^{-1},$$
$$n(e_j) \in \omega^*, \quad n((e_i)_A) \in \omega_A^*,$$

так что в силу (3.5)

$$\text{н.о.д.}\left(n(w\psi_j\psi_i^{-1}), \mathfrak{m}\right) = \text{н.о.д.}\left(n(l_A), \mathfrak{m}\right) = (1).$$

2) Достаточность. Пусть

$$\tau_1 \in \bar{\tau}_1 \in \bar{\mathfrak{M}}(\Omega, \mathfrak{O}_i), \quad \tau_2 \in \bar{\tau}_2 \in \bar{\mathfrak{M}}(\Omega, \mathfrak{O}_j).$$

По предположению для любого простого идеала $\mathfrak{p}$ кольца ω (конечного нормирования v) можно подобрать

$$w = w(\mathfrak{p}) \in \psi_i \psi_j^{-1} \mathfrak{O}_j$$

с условиями

$$\tau_2 = w(\mathfrak{p})^{-1} \tau_1 w(\mathfrak{p}), \tag{3.6}$$

$$\text{н.о.д.}\big(n(w(\mathfrak{p})\psi_j \psi_i^{-1}), \mathfrak{p}\big) = (1). \tag{3.7}$$

Для каждого бесконечного нормирования $v \in V_\infty$ по теореме Сколема–Нетер (см. [27], стр. 228) подбираем $w = w(v) \in \mathfrak{A}^*$ с условием

$$\tau_2 = w(v)^{-1} \tau_1 w(v). \tag{3.8}$$

Мы имеем:

$$w(\mathfrak{p})\psi_j \psi_i^{-1} \in \psi_i \{\psi_j^{-1} (\mathfrak{O}_j)_A \psi_j\} \psi_i^{-1} = \psi_i \mathfrak{O}_A \psi_i^{-1} = (\mathfrak{O}_i)_A.$$

В силу (3.7) и (3.8)

$$\text{н.о.д.}\big(n(w(\mathfrak{p})(\psi_j \psi_i^{-1})_\mathfrak{p}), \mathfrak{p}\big) = (1), \tag{3.9}$$

где $(\psi_j \psi_i^{-1})_\mathfrak{p}$ — $\mathfrak{p}$-компонента аделя $\psi_j \psi_i^{-1}$, так что

$$w(\mathfrak{p})(\psi_j \psi_i^{-1})_\mathfrak{p} \in \mathfrak{O}_\mathfrak{p}^*. \tag{3.10}$$

Определим теперь адель $(e_i)_A \in (\mathfrak{O}_i)_A^*$ условием: для любой v-компоненты (как конечной $\mathfrak{p}$-компоненты, так и для бесконечной $v \in V_\infty$)

$$\{(e_i)_A^{-1}\}_v = w(v)(\psi_j \psi_i^{-1})_v. \tag{3.11}$$

Тогда из (3.6) и (3.8) выводим:

$$\tau_2 = \psi_j \psi_i^{-1} (e_i)_A \tau_1 (e_i)_A^{-1} \psi_i \psi_j^{-1}. \tag{3.12}$$

По теореме Сколема–Нетер найдется $h \in \mathfrak{A}^*$ с условием

$$\tau_2 = h^{-1} \tau_1 h. \tag{3.13}$$

Тогда в силу (3.12) и (3.13)

$$\tau_1 \{h\psi_j \psi_i^{-1} (e_i)_A\} = \{h\psi_j \psi_i^{-1} (e_i)_A\} \tau_1,$$

и так как $\tau_1(K)$ — максимальное подполе алгебры $\mathfrak{A}$, то найдется такой идель $l_A \in K_A^*$, что

$$h\psi_j \psi_i^{-1} (e_i)_A = \tau_1(l_A). \tag{3.14}$$

В силу (3.13) и (3.14), по определениям §2

$$\tau_2 = l_A[\tau_1, h], \quad \bar{\tau}_2 = l_A[\bar{\tau}_1], \quad \bar{\tau}_2 = [l_A][\bar{\tau}_1].$$

Теорема 3 доказана.

4. Теория поворотов в кватернионных алгебрах. Рассмотрим частный случай — алгебру кватернионов $\mathfrak{A}$ над алгебраическим числовым полем k, т.е. простую центральную алгебру ранга 4. Приложенная к этому случаю общая теория поворотов, построенная в §§2–3, по существу, обобщает теорию Ю. Г. Тетерина [9] поворотов целых векторов в порядках кватернионной алгебры $\mathfrak{A}$ над полем рациональных чисел $k = Q$ (в свою очередь, обобщающую исследования [1], [4], [5], [7], [8], [24], [22], [25]). Набросок теории поворотов в кватернионных алгебрах над алгебраическим числовым полем содержится в заметке [2].

Не вдаваясь в детали, рассмотрим лишь специфику, которую привносит в общую теорию то обстоятельство, что алгебра кватернионов — четырехмерное квадратичное пространство над k, задаваемое приведенной нормой $n(a) = n_\mathfrak{A}(a) = a \cdot \bar{a}$, $a \in \mathfrak{A}$ (определение нормы см., например [27]). Это позволяет несколько уточнить действие группы классов собственных идеалов $\mathrm{cl}(\Omega) = \{[l_A] \mid l_A \in K_A^*\}$ на $\bar{\mathfrak{N}}$.

Сохраняем обозначения §2. Пусть

$$\bar{\mathfrak{N}} = \bigcup_{i=1}^{q} \bar{\mathfrak{M}}(\Omega, \mathfrak{O}_i)$$

— множество всех связок. По построению (2.15) порядки $\mathfrak{O}_1, \ldots, \mathfrak{O}_q$ принадлежат одному роду (как решетки четырехмерного квадратичного пространства), ибо имеет место равенство (2.16). Род порядков (решеток) $\mathfrak{O}_1, \ldots, \mathfrak{O}_q$ разбивается на спинорные роды $\mathfrak{Q}_j$ $(j = 1, \ldots, r)$ $\mathfrak{O}_1 \cup \ldots \cup \mathfrak{O}_q = \mathfrak{Q}_1 \cup \ldots \cup \mathfrak{Q}_r$; $\mathfrak{Q}_j = \mathfrak{O}_1^{(j)} \cup \ldots \cup \mathfrak{O}_{t_j}^{(j)} = \mathrm{spn}\, \mathfrak{O}_1^{(j)}$ $(j = 1, \ldots, r)$. Соответственно, связки $\bar{\mathfrak{M}}(\Omega, \mathfrak{O}_i)$ $(i = 1, \ldots, q)$ объединяются в спинорные роды связок $\mathfrak{S}(\Omega, \mathfrak{Q}_j)$ $(j = 1, \ldots, r)$

$$\bar{\mathfrak{N}} = \bigcup_{j=1}^{r} \mathfrak{S}(\Omega, \mathfrak{Q}_j), \quad \mathfrak{S}(\Omega, \mathfrak{Q}_j) = \bigcup_{v=1}^{t_j} \bar{\mathfrak{M}}(\Omega, \mathfrak{O}_v^{(j)}). \tag{4.1}$$

Оказывается, что описанная в §2 операция поворота связок $\bar{\mathfrak{N}}$, управляемая иделем $l_A \in K_A^*$ (или идеалом $J(\Omega)$, или классом идеалов $[l_A] \in \mathrm{cl}(\Omega)$), переводит спинорный род связок $\mathfrak{S}(\Omega, \mathfrak{Q})$ в некоторый полный спинорный род связок $\mathfrak{S}(\Omega, \mathfrak{Q}')$, где $\mathfrak{Q}$ и $\mathfrak{Q}'$ — спинорные роды решеток $\{\mathfrak{O}_i\}$.

Теорема 4. *Пусть $\mathfrak{S}(\Omega, \mathfrak{Q})$ — спинорный род связок, $l_A \in K_A^*$. Тогда*

$$l_A[\mathfrak{S}(\Omega, \mathfrak{Q})] = \mathfrak{S}(\Omega, \mathfrak{Q}') \tag{4.2}$$

где $\mathfrak{O}'$ — некоторый спинорный род порядков (решеток) $\mathfrak{O}_i$, определяемый $\mathfrak{O}$, l_A и Ω. Иначе говоря,

$$[l_A][\mathfrak{S}(\Omega, \mathfrak{O})] = \mathfrak{S}(\Omega, \mathfrak{O}'); \quad [l_A] \in \mathrm{cl}(\Omega). \tag{4.3}$$

Доказательство. Пусть $\bar\tau_1, \bar\tau_2 \in \mathfrak{S}(\Omega, \mathfrak{O})$, т.е.

$$\bar\tau_1 \in \bar{\mathfrak{M}}(\Omega, \mathfrak{O}_i), \quad \bar\tau_2 \in \bar{\mathfrak{M}}(\Omega, \mathfrak{O}_k), \quad \mathfrak{O}_k \in \mathrm{spn}\, \mathfrak{O}_i, \tag{4.4}$$

и пусть для некоторого $l_A \in K_A^*$

$$\bar\tau_1' = l_A[\bar\tau_1] \in \bar{\mathfrak{M}}(\Omega, \mathfrak{O}_j), \quad \bar\tau_2' \in l_A[\bar\tau_2] \in \bar{\mathfrak{M}}(\Omega, \mathfrak{O}_l).$$

Докажем, что тогда $\mathfrak{O}_l \in \mathrm{spn}\, \mathfrak{O}_j = \mathfrak{O}'$, так что

$$\bar\tau_1, \bar\tau_2 \in \mathfrak{S}(\Omega, \mathfrak{O}'). \tag{4.5}$$

Действительно, по построениям §2 можно подобрать

$$\tau_1 \in \bar\tau_1 \in \bar{\mathfrak{M}}(\Omega, \mathfrak{O}_i), \quad \tau_2 \in \bar\tau_2 \in \bar{\mathfrak{M}}(\Omega, \mathfrak{O}_k),$$

$$\tau_1' \in \bar\tau_1' \in \bar{\mathfrak{M}}(\Omega, \mathfrak{O}_j), \quad \tau_2' \in \bar\tau_2' \in \bar{\mathfrak{M}}(\Omega, \mathfrak{O}_l),$$

так, чтобы

$$\begin{aligned} l_A[\tau_1] &= \tau_1', \quad \tau_1' = h_1^{-1}\tau_1 h_1, \quad \tau_1(l_A) = h_1\psi_j\psi_i^{-1}(e_i)_A, \\ l_A[\tau_2] &= \tau_2', \quad \tau_2' = h_2^{-1}\tau_2 h_2, \quad \tau_2(l_A) = h_2\psi_l\psi_k^{-1}(e_k)_A, \end{aligned} \tag{4.6}$$

где $h_1, h_2 \in \mathfrak{A}^*$, $(e_i)_A \in (\mathfrak{O}_i)_A^*$, $(e_k)_A \in (\mathfrak{O}_k)_A^*$. Так как $\mathfrak{O}_i$ и $\mathfrak{O}_k$ принадлежат одному спинорному роду, то [20] найдется $(e_i')_A \in (\mathfrak{O}_i)_A^*$, так что

$$\psi_j\psi_i^{-1}(e_i')_A \in \mathfrak{A}^*\mathfrak{A}_A^1, \tag{4.7}$$

где

$$\mathfrak{A}_A^1 = \{a \in \mathfrak{A}_A \mid n(a) = 1\}.$$

Так как

$$\psi_l\psi_j^{-1} = h_2^{-1}h_1h_1^{-1}\{(h_2\psi_l\psi_k^{-1}(e_k)_A)(e_k)_A^{-1}(\psi_k\psi_i^{-1}(e_i')_A)(e_i')_A^{-1}(e_i)_A \times ((e_i)_A^{-1}\psi_i\psi_j^{-1}h_1^{-1})\}h_1,$$

$$n(\psi_l\psi_j^{-1}) \in n((e_k)_A^{-1})n((e_i')_A(e_i)_A)k^*$$

то

$$n(\psi_l\psi_j^{-1}((\psi_j\psi_k^{-1})(e_k)_A\psi_k\psi_j^{-1})\psi_j\psi_i^{-1}(e_i')_A(e_i)_A\psi_i\psi_j^{-1}) = n(\psi_l\psi_j^{-1})n((e_k)_A)n((e_i')_A(e_i^{-1})_A) \in k^*.$$

Это включение можно переписать так

$$n(\psi_l\psi_j^{-1}(e_j)_A) \in k^*, \tag{4.8}$$

где обозначено

$$(e_j)_A = \psi_j\psi_k^{-1}(e_k)_A\psi_k\psi_j^{-1}\psi_j\psi_i^{-1}(e_i')_A(e_i)_A^{-1}\psi_i\psi_j^{-1} \in (\mathfrak{O}_j)_A^*.$$

Но по принципу Хассе (ср. [26]) (4.8) означает, что

$$\psi_l\psi_j^{-1}(e_j)_A \in \mathfrak{A}^*\mathfrak{A}_A^1. \tag{4.9}$$

Так как при этом

$$\psi_l\psi_j^{-1}(e_j)_A\mathfrak{O}_j(e_j)_A^{-1}\psi_j\psi_l^{-1} = \mathfrak{O}_l$$

то из равенства (4.9) выводим, что порядки (решетки) $\mathfrak{O}_j$ и $\mathfrak{O}_l$ спинорно родственны, и мы имеем (4.5).

Теорема 4 доказана.

5. Теория поворотов в алгебрах матриц n-го порядка. Пусть k — алгебраическое числовое поле, $\mathfrak{A} = \mathscr{M}_n(k)$ — алгебра матриц n-го порядка ($n \geqslant 2$) над k, т.е. совокупность матриц размера $n \times n$ над k с их сложением и умножением. Это — простая центральная алгебра над k (см. [14], [27]). Общая теория поворотов (§2) естественно приложима и в этом случае. Было бы полезно для приложений конкретизировать ее, приблизив изложение к работам [1], [8]. Но в этой работе мы остановимся лишь на вопросе поворотной эквивалентности вектор-матриц (связок вложений).

К сожалению, мы вынуждены ограничиться лишь случаем, когда Ω — максимальный порядок(¹) поля K, изоморфного максимальному подполю алгебры $\mathfrak{A}$, $\mathfrak{O} = \mathscr{M}_n(\omega)$, где ω — кольцо всех целых чисел поля k. В этом случае оказывается, что все связки из $\bar{\mathfrak{N}}(\Omega, \mathfrak{O})$ поворотно эквивалентны; т.е. группа иделей $\{l_A\}$ (равно как группа идеалов, группа классов идеалов $\mathrm{cl}(\Omega)$) на $\bar{\mathfrak{N}}(\Omega, \mathfrak{O})$ имеет одну орбиту. Мы покажем, что это — простое следствие общего замечательного предложения Шевалле (см. [13], см. также [16], [21], [18]).

Предложение. *Пусть $\mathfrak{O}$ — максимальный порядок в простой центральной алгебре $\mathfrak{A}$ над алгебраическим числовым полем k; K — расширение k, изоморфное максимальному подполю алгебры $\mathfrak{A}$; Ω — максимальный порядок (множество всех целых элементов) поля K. Пусть J — правый идеал порядка $\mathfrak{O}$, причем $\mathfrak{O}'$ — его левый порядок, и пусть J взаимно прост с дифферентной порядка $\mathfrak{O}$. Тогда если*

$$\tau \in \mathfrak{M}(\Omega, \mathfrak{O}), \quad \tau \in \mathfrak{M}(\Omega, \mathfrak{O}'), \tag{5.1}$$

то найдется такой идеал I порядка Ω, что

$$J = \tau(I) \cdot \mathfrak{O}. \tag{5.2}$$

В терминах иделей это предложение может быть переформулировано следующим образом.

(¹) Для максимального порядка Ω все идеалы собственные и локально главные (см. [27]).

Лемма 5. *В обозначениях предложения Шевалле, пусть* $\mathfrak{O}$ — *максимальный порядок в* $\mathfrak{A}$, Ω — *максимальный порядок в* K. *Пусть*

$$J = c_A \cdot \mathfrak{O}, \quad c_A \in \mathfrak{A}_A^*. \tag{5.3}$$

Тогда если J *взаимно прост с дифферентной порядка* $\mathfrak{O}$, *то найдутся такие* $l_A \in K_A^*$ *и* $e_A \in \mathfrak{O}_A^*$, *что*

$$c_A e_A = \tau(l_A). \tag{5.4}$$

Теорема 5. *Пусть* $\mathfrak{A} = \mathcal{M}_n(k)$ — *алгебра матриц порядка* $n \geqslant 2$ *над алгебраическим числовым полем* k *с кольцом всех целых элементов* ω; K — *расширение поля* k *степени* n, Ω — *максимальный порядок в* K. *Пусть* $\mathcal{M}_n(\omega) = \mathfrak{O}$ *и пусть*

$$\mathfrak{O}_1, \ldots, \mathfrak{O}_q \tag{5.5}$$

— *польный набор*(²) *правых порядков, соответствующих порядку* $\mathfrak{O}$ (см. §2, (2.15)). *Тогда все связки вложений*

$$\bar{\mathfrak{N}}(\Omega, \mathfrak{O}) = \bigcup_{i=1}^{q} \bar{\mathfrak{M}}(\Omega, \mathfrak{O}_i) \tag{5.6}$$

поворотно эквивалентны, т.е. лежат в одной орбите действия группы $\mathrm{cl}(\Omega)$.

Доказательство. 1. Пусть

$$\tau \in \bar{\tau} \in \bar{\mathfrak{M}}(\Omega, \mathfrak{O}_i), \quad \tau' \in \bar{\tau}' \in \bar{\mathfrak{M}}(\Omega, \mathfrak{O}_j). \tag{5.7}$$

По теореме Сколема–Нетер (см. [27]) найдется такой элемент $h \in \mathfrak{A}^*$, что

$$\tau' = h^{-1} \tau h. \tag{5.8}$$

В силу (5.7) и (5.8) последовательно получаем:

$$\begin{aligned} \tau(\Omega) &= \tau(K) \cap \mathfrak{O}_i, \\ h^{-1}\tau(\Omega)h &= h^{-1}\tau(K)h \cap \mathfrak{O}_j, \\ h^{-1}\tau(\Omega)h &= h^{-1}\tau(K)h \cap \psi_j\psi_i^{-1}\mathfrak{O}_i\psi_i\psi_j^{-1}, \\ \tau(\Omega) &= \tau(K) \cap h\psi_j\psi_i^{-1}\mathfrak{O}_i\psi_i\psi_j^{-1}h^{-1}. \end{aligned} \tag{5.9}$$

2. Покажем, что в алгебре матриц $\mathfrak{A} = \mathcal{M}_n(k)$ дифферента любого максимального порядка $\mathfrak{O}$ равна $(1) = \mathfrak{O}$. Действительно, можно подобрать такое $c_A \in \mathfrak{A}_A^*$, что

$$\mathfrak{O} = c_A \mathcal{M}_n(\omega) c_A^{-1} \tag{5.10}$$

(²) Все максимальные порядки в $\mathfrak{A}$ подобны, $q = \# \mathrm{cl}(\omega)$ число классов идеалов в ω (все они собственные и локально главные).

Дифферента порядка $\mathfrak{O}$ по определению [23] равна

$$D(\mathfrak{O}) = \{a \in \mathfrak{A} \mid \Phi(\mathfrak{O})a \subset \mathfrak{O}\}, \tag{5.11}$$

где

$$\Phi(\mathfrak{O}) = \{a \in \mathfrak{A} \mid \mathrm{sp}(a \cdot \mathfrak{O}) \subset \omega\}.$$

Имеем в силу (5.10) и определения

$$\begin{aligned} \Phi(\mathfrak{O}) &= \{a \in \mathfrak{A} \mid \mathrm{sp}(ac_A\mathcal{M}_n(\omega)c_A^{-1}) \subset \omega\} \\ &= \{a \in \mathfrak{A} \mid \mathrm{sp}(c_A^{-1}ac_A\mathcal{M}_n(\omega)) \subset \omega\} \\ &= c_A\mathcal{M}_n(\omega)c_A^{-1} = \mathfrak{O}, \end{aligned}$$

так что по (5.11)

$$D(\mathfrak{O}) = \{a \in \mathfrak{A} \mid \mathfrak{O} \cdot a \subset \mathfrak{O}\} = \mathfrak{O} = (1). \tag{5.12}$$

3. В силу (5.12) лемма 5 применима к любому идеалу I. Применяя ее к идеалу

$$J = h\psi_j\psi_i^{-1}\mathfrak{O}_i,$$

подберем такую единицу $(e_i)_A \in (\mathfrak{O}_i)_A^*$ и такой идель $l_A \in K_A^*$, что

$$\tau(l_A) = h\psi_j\psi_i^{-1}(e_i)_A. \tag{5.13}$$

По построениям §2 это означает, что

$$\bar{\tau}' = l_A[\bar{\tau}] = h^{-1}\bar{\tau}h, \tag{5.14}$$

т.е. $\bar{\tau}'$ и $\bar{\tau}$ поворотно эквивалентны.

Теорема 5 доказана.

Ясно, что в теореме 5 вместо порядка $\mathcal{M}_n(\omega)$ можно взять любой другой максимальный порядок $\mathfrak{O}$ алгебры $\mathcal{M}_n(k)$.

Литература

[1] Б. А. Венков, *Об арифметике кватернионов*. I–V, Изв. Росс. АН, 1922, 205–220, 221–246; Изв. АН СССР. Отд. физ.-мат. н., 1929, 489–504, 535–562, 607–622.

[2] М. Н. Кубенский, *Теория поворотов*, В сб.: *Автоморфные функции и теория чисел*, Ижевск 1987, 47–55.

[3] — *О поворотах в простых центральных алгебрах*, В сб.: *Аналитическая теория чисел*. 2, Петрозаводск 1988, 43–46.

[4] Ю. В. Линник, *On certain results relating to positive ternary quadratic forms*, Матем. сб. 5 (47) (1939), 453–471.

[5] — *О представлении больших чисел положительными тернарными квадратичными формами*, Изв. АН СССР, сер. матем. 4 (1940), 363–402.

[6] — *Эргодические свойства алгебраических полей*, Ленинград 1967, 208 с. [English transl. Yu. V. Linnik, *Ergodic properties of algebraic fields*, New York 1968, ix, 194 p.]

[7] А. В. Малышев, *О представлении целых чисел положительными квадратичными формами*, Труды МИАН, т. 65, Москва–Ленинград, 1962, 212 с.

[8] А. В. Малышев и У. М. Пачев, *Об арифметике матриц второго порядка*, В сб.: *Исследования по теории чисел*. 6, Зап. научн. семинаров ЛОМИ, т. 93, 1980, 41–86.
[9] Ю. Г. Тетерин, *Действие группы классов на представлениях чисел тернарной квадратичной формой. Формулы Зигеля и Кнезера-Сии-Петерса*, В. сб.: *Исследования по теории чисел*. 9, Зап. научн. семинаров ЛОМИ, т. 151, 1986, 141–158.
[10] Н. Г. Чеботарев, *Основы теории Галуа*, ч. 2, Ленинград–Москва 1937, 159 с.
[11] *Algebraic Number Theory* (ed. by J. W. S. Cassels and A. Fröhlich), London–New York 1967 [русск. пер. *Алгебраическая теория чисел* (под ред. Дж. Касселса и А. Фрелиха), Москва 1969, 483 с.]
[12] J. W. S. Cassels, *Rational quadratic forms*, London 1978, xvi, 413 p. [русск. пер.: Дж. Касселс, *Рациональные квадратичные формы* , Москва 1982, 436 с.]
[13] Cl. Chevalley, *Sur certains idéaux d'un algèbre simple*, Abh. Math. Seminar Hamburg. Univ. 10 (1934), 83–105.
[14] M. Deuring, *Algebren*, Berlin 1935 (1968), viii, 143 p.
[15] M. Eichler, *The basis problem for modular form and the traces of the Hecke operators*, in: *Modular functions of one variable*, I, Lect. Notes in Math., 320, Berlin 1973, 75–151.
[16] H. Hasse, *Über gewisse Ideale in einer einfachen Algebra*, Act. Sci. Ind. 109, Paris 1934, 16 p.
[17] H. Hijikata, *Explicit formula of the traces of Hecke operators for $\Gamma_0(N)$*, J. Math. Soc. Japan 26 (1974), 56–82.
[18] W. Kořínek, *Maximale kommutative Körper in einfachen Systemen hyperkomplexer Zahlen*, Mém. Soc. Sci. Bohême 1932, 1 (1933), 1–24.
[19] A. V. Malyshev, *Yu. V. Linnik's ergodic method in number theory*, Acta Arith. 27 (1975), 555–598.
[20] O. T. O'Meara, *Introduction to quadratic forms*, Berlin 1963 (1971, 1973), xi, 342 p.
[21] E. Noether, *Zerfallende verschränkte Produkte und ihre Maximalordnungen*, Act. Sci. Ind. 111, Paris 1934.
[22] H. P. Rehm, *On a theorem of Gauss concerning the number of integral solutions of the equation $x^2+y^2+z^2=m$*, In: *Ternary quadratic forms and norms*, New York–Basel 1982, 31–38.
[23] I. Reiner, *Maximal orders*, London 1975, xii, 395 p.
[24] B. Rice, *Quaternions and binary quadratic forms*, Proc. Amer. Math. Soc. 27 (1971), 1–7.
[25] T. R. Shemanske, *Representations of ternary quadratic forms and the class number of imaginary quadratic fields*, Pacific J. Math. 122 (1986), 223–250.
[26] M.-F. Vignéras, *Arithmétique des algèbres de quaternions*, Lect. Notes in Math. 800, Berlin 1980, vii, 169 p.
[27] A. Weil, *Basic number theory*, Berlin 1967 [русск. пер.: А. Вейль, *Основы теории чисел*, Москва 1972, 408 с.]

Поступило 22.11.1988 (1883)

ACTA ARITHMETICA
LIII (1990)

On the greatest prime factor of an arithmetical progression (II)

by

T. N. Shorey (Bombay) and R. Tijdeman (Leiden)

To the memory of Professor V. G. Sprindžuk

1. For an integer $v>1$, we denote by $P(v)$ the greatest prime factor of v and we write $\omega(v)$ for the number of distinct prime factors of v. We put $P(1)=1$ and $\omega(1)=0$. Let a, d and k be positive integers satisfying $\gcd(a,d)=1$ and $k\geqslant 3$. We put

$$\chi = a+(k-1)d, \quad \chi_1=\chi/k, \quad \chi_2=\max(\chi_1,3),$$
$$\Delta(a;d)=a(a+d)\ldots(a+(k-1)d)$$

and

$$P=P(\Delta(a;d)), \quad \omega=\omega(\Delta(a;d)).$$

A classical theorem of Sylvester [5] states that

$$P>k \quad \text{if } a\geqslant d+k. \tag{1}$$

Langevin [2] improved (1) to

$$P>k \quad \text{if } a>k.$$

Further, Shorey and Tijdeman [4] showed that

$$P>k \quad \text{if } d\geqslant 2 \quad \text{and} \quad (a,k,d)\neq(2,3,7). \tag{2}$$

Also, Langevin [3] obtained results which imply that, under suitable conditions, there exists some number $r>1$ such that

$$P>C_1 k\log\log a \quad \text{if } a>k^r$$

where $C_1>0$ is an effectively computable number depending only on r. This is an immediate consequence of the following result.

THEOREM 1. *Let $\varepsilon>0$ and*

$$\chi>k^{1+\varepsilon}. \tag{3}$$