Автоморфизмы элементарных присоединенных групп Шевалле

типов A_l, D_l, E_l над локальными кольцами с $1/2$[1]

Е. И. Бунина

Аннотация.

В данной работе мы доказываем, что каждый автоморфизм элементарной присоединенной группы Шевалле типа A_l, D_l или E_l над коммутативным локальным кольцом с обратимой двойкой есть композиция кольцевого автоморфизма и сопряжения с помощью некоторой матрицы из нормализатора этой группы в $\mathrm{GL}\,(V)$ (V — пространство присоединенного представления).

Введение

Пусть $G_{\,\mathrm{ad}}$ — это схема Шевалле–Демазюра, ассоциированная с неприводимой системой корней Φ типа A_l ($l \geq 2$), D_l ($l \geq 4$), E_l ($l = 6, 7, 8$); $G_{\,\mathrm{ad}}\,(\Phi, R)$ — множество точек $G_{\,\mathrm{ad}}$ со значениями в коммутативном кольце R; $E_{\,\mathrm{ad}}\,(\Phi, R)$ — элементарная присоединенная подгруппа в $G_{\,\mathrm{ad}}\,(\Phi, R)$, где R — коммутативное кольцо с единицей. В данной работе мы описываем автоморфизмы группы $E_{\,\mathrm{ad}}\,(\Phi, R)$ над локальными коммутативными кольцами с $1/2$.

Подобные результаты для групп Шевалле над полями были доказаны Р. Стейнбергом [55] для конечного случая и Дж. Хамфри [44] для бесконечного. Описанию автоморфизмов групп Шевалле над различными коммутативными кольцами были посвящены работы многих авторов, среди которых следует отметить работы Бореля–Титса [25], Картера–Чен Ю [28], самого Чен Ю [29]–[33]. Э. Абе [1] доказал стандартность автоморфизмов для нетеровых колец, что полностью могло бы закрыть вопрос об автоморфизмах групп Шевалле над произвольными коммутативными кольцами (для случая системы корней ранга ≥ 2 и колец с обратимой двойкой), однако в рассмотрении случая присоединенных элементарных групп в работе [1] содержится ошибка, которую не удается устранить методами этой статьи. Именно, в доказательстве леммы 11 используется то, что $\mathrm{ad}\,(x_\alpha)^2 = 0$ для всех длинных корней, что неверно в присоединенном представлении. Главной проблемой здесь является случай групп типа E_8, так как во всех остальных случаях группы Шевалле допускают представление, обладающие свойством $\mathrm{ad}\,(x_\alpha)^2 = 0$ для всех длинных корней, а в случае E_8 таких представлений нет.

В данной работе удалось преодолеть трудности, возникающие в этом случае, что может помочь закрыть вопрос об автоморфизмах групп Шевалле над коммутативными кольцами с $1/2$.

[1]Работа поддержана грантом Президента РФ МК-2530.2008.1 и грантом РФФИ 08-01-00693.

Для доказательства основной теоремы обобщаются некоторые методы из работы В. М. Петечука [14].

Заметим, что хотя мы рассматриваем одновременно случаи систем корней A_l, D_l, E_l, но случай A_l был полностью закрыт работами В. Уотерхауза [63], В.М. Петечука [13], Ли Фуаня и Ли-Дзун-сяна [47], причем даже без условия обратимости двойки в кольце. Статья И.З. Голубчика и А.В. Михалева [8] охватывает случай системы корней C_l, который в этой работе не рассматривается.

Автор выражает благодарность Н.А. Вавилову, А.Ю. Голубкову, А.А. Клячко, А.В. Михалеву, и особенно рецензенту данной статьи за ценные советы, замечания и консультации.

1. Определения и формулировка основной теоремы.

Мы фиксируем систему корней Φ, имеющую один из типов A_l ($l \geq 2$), D_l ($l \geq 4$), или E_l ($l = 6, 7, 8$), с системой простых корней Δ, множеством положительных (отрицательных) корней Φ^+ (Φ^-), группой Вейля W. Напомним, что в нашем случае любые два корня сопряжены под действием группы Вейля. Пусть $|\Phi^+| = m$. Более подробные сведения о системах корней и их свойствах можно найти в книгах [45], [26].

Предположим теперь,что у нас имеется полупростая комплексная алгебра Ли $\mathcal{L}$ с картановской подалгеброй $\mathcal{H}$ (подробную информацию о полупростых алгебрах Ли можно найти в книге [45]).

Алгебра Ли $\mathcal{L}$ допускает разложение $\mathcal{L} = \mathcal{H} \oplus \sum\limits_{\alpha \neq 0} \mathcal{L}_\alpha$,

$$\mathcal{L}_\alpha := \{x \in \mathcal{L} \mid [h, x] = \alpha(h)x \text{ для каждого } h \in \mathcal{H}\},$$

и если $\mathcal{L}_\alpha \neq 0$, то $\dim \mathcal{L}_\alpha = 1$, все ненулевые $\alpha \in \mathcal{H}$ такие, что $\mathcal{L}_\alpha \neq 0$, образуют некоторую систему корней Φ. Система корней Φ и полупростая алгебра Ли $\mathcal{L}$ над $\mathbb{C}$ однозначно (с точностью до автоморфизма) определяют друг друга.

На алгебре Ли $\mathcal{L}$ можно ввести билинейную *форму Киллинга* $\varkappa(x, y) = \operatorname{tr}(\operatorname{ad} x \operatorname{ad} y)$, невырожденную на $\mathcal{H}$. Таким образом, пространства $\mathcal{H}$ и $\mathcal{H}^*$ можно отождествить.

Можно выбрать базис $\{h_1, \dots, h_l\}$ в $\mathcal{H}$ и для каждого $\alpha \in \Phi$ элементы $x_\alpha \in \mathcal{L}_\alpha$ так, что $\{h_i; x_\alpha\}$ образуют базис в $\mathcal{L}$ и для любых двух элементов этого базиса их коммутатор является целочисленной линейной комбинацией элементов того же базиса. Этот базис называется *базисом Шевалле.*

Введем теперь элементарные группы Шевалле (см., например, [54]).

Пусть $\mathcal{L}$ — полупростая алгебра Ли (над $\mathbb{C}$) с системой корней Φ, $\pi : \mathcal{L} \to \mathfrak{gl}(V)$ — ее конечномерное точное представление (размерности n). Если $\mathcal{H}$ — картановская подалгебра алгебры $\mathcal{L}$, то функционал $\lambda \in \mathcal{H}^*$ называется *весом* данного представления, если существует ненулевой вектор $v \in V$ (который называется *весовым вектором*) такой, что для любых $h \in \mathcal{H}$ $\pi(h)v = \lambda(h)v$.

В пространстве V в базисе Шевалле все операторы $\pi(x_\alpha)^k/k!$ для $k \in \mathbb{N}$ записываются целочисленными (нильпотентными) матрицами. Целочисленная матрица также может рассматриваться как матрица над произвольным коммутативным кольцом с единицей. Пусть R — такое кольцо. Рассмотрим матрицы размера $n \times n$ над R, матрицы $\pi(x_\alpha)^k/k!$ при $\alpha \in \Phi$, $k \in \mathbb{N}$ вложим в $M_n(R)$.

Теперь рассмотрим автоморфизмы свободного модуля R^n вида

$$\exp(tx_\alpha) = x_\alpha(t) = 1 + t\pi(x_\alpha) + t^2\pi(x_\alpha)^2/2 + \dots + t^k\pi(x_\alpha)^k/k! + \dots$$

Так как все матрицы $\pi(x_\alpha)$ нильпотентны, этот ряд конечен. Автоморфизмы $x_\alpha(t)$ называются *элементарными корневыми элементами*. Подгруппа в $\operatorname{Aut}(R^n)$, порожденная всеми автоморфизмами $x_\alpha(t)$, $\alpha \in \Phi$, $t \in R$, называется *элементарной группой Шевалле* (обозначение: $E_\pi(\Phi, R)$).

В элементарной группе Шевалле можно ввести следующие важные элементы и подгруппы:

— $w_\alpha(t) = x_\alpha(t)x_{-\alpha}(-t^{-1})x_\alpha(t)$, $\alpha \in \Phi$, $t \in R^*$;

— $h_\alpha(t) = w_\alpha(t)w_\alpha(1)^{-1}$;

— подгруппа N порождена всеми $w_\alpha(t)$, $\alpha \in \Phi$, $t \in R^*$;

— подгруппа H порождена всеми $h_\alpha(t)$, $\alpha \in \Phi$, $t \in R^*$;

Действие элементов $x_\alpha(t)$ на базисе Шевалле описано в работах [27], [62].

Известно, что группа N является нормализатором группы H в элементарной группе Шевалле, факторгруппа N/H изоморфна группе Вейля $W(\Phi)$.

Все веса данного представления (по сложению) порождают решетку (свободную абелеву группу, в которой любой $\mathbb{Z}$-базис также является $\mathbb{C}$-базисом в $\mathcal{H}^*$), называемую *решеткой весов* Λ_π.

Элементарные группы Шевалле определяются даже не представлением соответствующей алгебры Ли, а просто ее *решеткой весов*. Именно, с точностью до абстрактного изоморфизма элементарная группа Шевалле полностью определяется системой корней Φ, коммутативным кольцом R с единицей и решеткой весов Λ_π.

Среди всех решеток выделим две: решетку, соответствующую присоединенному представлению, она порождается всеми корнями (*решетка корней* Λ_{ad}) и решетку, порожденную всеми весами всех представлений (*решетка весов* Λ_{sc}). Для любого точного представления π имеет место включение $\Lambda_{\mathrm{ad}} \subseteq \Lambda_\pi \subseteq \Lambda_{\mathrm{sc}}$. Соответственно, мы можем говорить о *присоединенной* и *односвязной* элементарных группах Шевалле. Нас в этой работе будут интересовать именно присоединенные элементарные группы Шевалле.

В группе Шевалле выполняются следующие соотношения:

(R1) $\forall \alpha \in \Phi\ \forall t, u \in R \quad x_\alpha(t)x_\alpha(u) = x_\alpha(t+u)$;

(R2) $\forall \alpha, \beta \in \Phi\ \forall t, u \in R \quad \alpha + \beta \neq 0 \Rightarrow$

$$[x_\alpha(t), x_\beta(u)] = x_\alpha(t)x_\beta(u)x_\alpha(-t)x_\beta(-u) = \prod x_{i\alpha+j\beta}(c_{ij}t^iu^j),$$

где i, j — целые числа, произведение берется по всем корням $i\alpha + j\beta$, расположенным в некотором фиксированном порядке; c_{ij} — целые числа, не зависящие от t и u, но зависящие от α и β и от порядка корней в произведении. В случае рассматриваемых нами систем корней всегда

$$[x_\alpha(t), x_\beta(u)] = x_{\alpha+\beta}(\pm tu).$$

(R3) $\forall \alpha \in \Phi\ w_\alpha = w_\alpha(1)$;

(R4) $\forall \alpha, \beta \in \Phi\ \forall t \in R^*\ w_\alpha h_\beta(t) w_\alpha^{-1} = h_{w_\alpha(\beta)}(t)$;

(R5) $\forall \alpha, \beta \in \Phi\ \forall t \in R^*\ w_\alpha x_\beta(t) w_\alpha^{-1} = x_{w_\alpha(\beta)}(ct)$, где $c = c(\alpha, \beta) = \pm 1$;

(R6) $\forall \alpha, \beta \in \Phi\ \forall t \in R^*\ \forall u \in R\ h_\alpha(t)x_\beta(u)h_\alpha(t)^{-1} = x_\beta(t^{\langle \beta, \alpha\rangle}u)$.

Через X_α обозначим подгруппу, состоящую из всех $x_\alpha(t)$ для $t \in R$.

Нам понадобятся два типа автоморфизмов элементарной группы Шевалле $E_{\mathrm{ad}}(\Phi, R)$.

Кольцевые автоморфизмы. Пусть $\rho : R \to R$ — автоморфизм кольца R. Отображение $x \mapsto \rho(x)$ из $E_{\mathrm{ad}}(\Phi, R)$ на себя является автоморфизмом группы $E_{\mathrm{ad}}(\Phi, R)$, который обозначается той же буквой ρ и называется *кольцевым автоморфизмом* группы $E_\pi(\Phi, R)$. Заметим, что для всех $\alpha \in \Phi$ и $t \in R$ элемент $x_\alpha(t)$ отображается в $x_\alpha(\rho(t))$.

Автоморфизмы-сопряжения. Пусть V — пространство представления группы $E_{\mathrm{ad}}(\Phi, R)$, $C \in \mathrm{GL}(V)$ — матрица, оставляющая группу Шевалле на месте:

$$CE_{\mathrm{ad}}(\Phi, R)C^{-1} = E_{\mathrm{ad}}(Phi, R).$$

Тогда отображение $x \mapsto CxC^{-1}$ из $E_\pi(\Phi, R)$ на себя является автоморфизмом группы Шевалле, который обозначается i и называется *автоморфизмом-сопряжением* группы $E(R)$, *индуцированным элементом* C группы $\mathrm{GL}(V)$.

Теорема 1. *Пусть $E_{\mathrm{ad}}(\Phi, R)$ — элементарная группа Шевалле с неприводимой системой корней одного из типов A_l $(l \geq 2)$, D_l $(l \geq 4)$, E_l $(l = 6, 7, 8)$, R — коммутативное локальное кольцо с $1/2$. Тогда любой автоморфизм группы $E_{\mathrm{ad}}(\Phi, R)$ есть композиция кольцевого автоморфизма и автоморфизма-сопряжения.*

Следующие параграфы посвящены доказательству теоремы 1.

2. Замена изначального автоморфизма на специальный изоморфизм.

Начиная с этого параграфа, кольцо R будет предполагаться локальным кольцом с $1/2$, группа Шевалле присоединенной, в этом параграфе система корней произвольная. В этом параграфе мы используем некоторые соображения из работы [14].

Пусть J — максимальный идеал (радикал) кольца R, k — поле вычетов R/J. Тогда $E_J = E_{\mathrm{ad}}(\Phi, R, J)$ — наибольшая нормальная собственная подгруппа в $E_{\mathrm{ad}}(\Phi, R)$ (см. [18]). Таким образом, подгруппа E_J инвариантна относительно действия автоморфизма φ.

Значит, автоморфизм

$$\varphi : E_{\mathrm{ad}}(\Phi, R) \to E_{\mathrm{ad}}(\Phi, R)$$

индуцирует автоморфизм

$$\overline{\varphi} : E_{\mathrm{ad}}(\Phi, R)/E_J = E_{\mathrm{ad}}(\Phi, k) \to E_{\mathrm{ad}}(\Phi, k).$$

Группа $E_{\mathrm{ad}}(\Phi, k)$ является присоединенной группой Шевалле над полем, значит, автоморфизм $\overline{\varphi}$ стандартен (см. [54]), т. е. имеет вид

$$\overline{\varphi} = i_{\overline{g}}\overline{\rho}, \quad \overline{g} \in N(E_{\mathrm{ad}}(\Phi, k)),$$

где $\overline{\rho}$ — кольцевой автоморфизм, индуцированный некоторым автоморфизмом поля k.

Ясно, что существует матрица $g \in \mathrm{GL}_n(R)$ такая, что ее образ при факторизации R по J совпадает с $\overline{g}$. Мы не можем быть уверены, что $g \in N(E_{\mathrm{ad}}(\Phi, R))$.

Рассмотрим отображение $\varphi' = i_{g^{-1}}\varphi$. Это изоморфизм группы $E_{\mathrm{ad}}(\Phi, R) \subset \mathrm{GL}_n(R)$ на некоторую подгруппу $\mathrm{GL}_n(R)$, с тем свойством, что ее образ при факторизации R по J совпадает с автоморфизмом $\overline{\rho}$.

Проведенные рассуждения доказывают

Предложение 1. *Любая матрица $A \in E_{\mathrm{ad}}(\Phi, R)$ с элементами из подкольца R' в R, порожденного единицей, отображается при изоморфизме φ' в матрицу из множества*

$$A \cdot \mathrm{GL}_n(R, J) = \{B \in \mathrm{GL}_n(R) \mid A - B \in M_n(J)\}.$$

Пусть $a \in E_{\mathrm{ad}}(\Phi, R)$, $a^2 = 1$. Тогда элемент $e = \frac{1}{2}(1+a)$ является идемпотентом в кольце $M_n(R)$. Этот идемпотент e определяет разложение свободного R-модуля $V \cong R^n$:

$$V = eV \oplus (1-e)V = V_0 \oplus V_1$$

(модули V_0, V_1 свободны, так как любой проективный модуль над локальным кольцом свободен [49]). Пусть $\overline{V} = \overline{V}_0 \oplus \overline{V}_1$ — разложение k-модуля (линейного пространства) $\overline{V} \cong k^n$ по отношению к $\overline{a}$, и $\overline{e} = \frac{1}{2}(1+\overline{a})$.

Тогда имеем

Предложение 2. *Модули (подпространства) $\overline{V}_0$, $\overline{V}_1$ являются образами модулей V_0, V_1 при факторизации по J.*

Доказательство. Обозначим образы модулей V_0, V_1 при факторизации по J через $\widetilde{V}_0$, $\widetilde{V}_1$, соответственно. Так как $V_0 = \{x \in V | ex = x\}$, $V_1 = \{x \in V | ex = 0\}$, то $\overline{e}(\overline{x}) = \frac{1}{2}(1+\overline{a})(\overline{x}) = \frac{1}{2}(1+\overline{a}(\overline{x})) = \frac{1}{2}(1+\overline{a(x)}) = \overline{e(x)}$. Тогда $\widetilde{V}_0 \subseteq \overline{V}_0$, $\widetilde{V}_1 \subseteq \overline{V}_1$.

Пусть $x = x_0 + x_1$, $x_0 \in V_0$, $x_1 \in V_1$. Тогда $\overline{e}(\overline{x}) = \overline{e}(\overline{x}_0) + \overline{e}(\overline{x}_1) = \overline{x}_0$. Если $\overline{x} \in \widetilde{V}_0$, то $\overline{x} = \overline{x}_0$. □

Пусть $b = \varphi'(a)$. Тогда $b^2 = 1$ и b сравнимо с a по модулю J.

Предложение 3. *Предположим, что $a, b \in E_\pi(\Phi, R)$, $a^2 = b^2 = 1$, a — матрица с элементами из подкольца $R' \subset R$, порожденного единицей, b и a сравнимы по модулю J, $V = V_0 \oplus V_1$ — разложение V по отношению к a, $V = V_0' \oplus V_1'$ — разложение V по отношению к b. Тогда $\dim V_0' = \dim V_0$, $\dim V_1' = \dim V_1$.*

Доказательство. Мы имеем R-базис модуля V $\{e_1, \ldots, e_n\}$ такой, что $\{e_1, \ldots, e_k\} \subset V_0$, $\{e_{k+1}, \ldots, e_n\} \subset V_1$. Ясно, что

$$\overline{a}\overline{e}_i = \overline{ae_i} = \overline{(\sum_{j=1}^{n} a_{ij}e_j)} = \sum_{j=1}^{n} \overline{a}_{ij}\overline{e}_j.$$

Пусть $\overline{V} = \overline{V}_0 \oplus \overline{V}_1$, $\overline{V} = \overline{V}'_0 \oplus \overline{V}'_1$ — разложения k-модуля (пространства) $\overline{V}$ по отношению к $\overline{a}$ и $\overline{b}$. Ясно, что $\overline{V}_0 = \overline{V}'_0$, $\overline{V}_1 = \overline{V}'_1$. Таким образом, по предложению 2 образы модулей V_0 и V_0', V_1 и V_1' при факторизации J совпадают. Возьмем такие $\{f_1, \ldots, f_k\} \subset V_0'$, $\{f_{k+1}, \ldots, f_n\} \subset V_1'$, что $\overline{f}_i = \overline{e}_i$, $i = 1, \ldots, n$. Так как матрица перехода от $\{e_1, \ldots, e_n\}$ к $\{f_1, \ldots, f_n\}$ обратима (сравнима с единичной матрицей по модулю J), то $\{f_1, \ldots, f_n\}$ — это R-базис в V. Ясно, что $\{f_1, \ldots, f_k\}$ является R-базисом в V_0', $\{v_{k+1}, \ldots, v_n\}$ — R-базисом в V_1'. □

3. Образы w_{α_i}

Рассмотрим некоторую фиксированную присоединенную группу Шевалле $E = E_{\mathrm{ad}}(\Phi, R)$ с системой корней A_l ($l \geq 2$), D_l ($l \geq 4$), E_6, E_7 или E_8, ее присоединенное представление в группе $\mathrm{GL}_n(R)$ ($n = l + 2m$, где m — число положительных корней системы Φ), с базисом из весовых векторов $v_1 = x_{\alpha_1}, v_{-1} = x_{-\alpha_1}, \dots, v_n = x_{\alpha_n}, v_{-n} = x_{-\alpha_n}, V_1 = h_1, \dots, V_l = h_l$, соответствующему базису Шевалле системы Φ.

У нас также есть изоморфизм φ', описанный в параграфе 2.

Рассмотрим матрицы $h_{\alpha_1}(-1), \dots, h_{\alpha_l}(-1)$ в нашем базисе. Они имеют вид

$$h_{\alpha_i}(-1) = \mathrm{diag}\,[\pm 1, \dots, \pm 1, \underbrace{1, \dots, 1}_{l}],$$

на $(2j-1)$-м и $(2j)$-м местах стоят -1 тогда и только тогда, когда $\langle \alpha_i, \alpha_j \rangle = -1$. Как мы видим, для всех i $h_{\alpha_i}(-1)^2 = 1$.

В соответствии с предложением 3 мы знаем, что любая матрица $h_i = \varphi'(h_{\alpha_i}(-1))$ в некотором базисе диагональна с ± 1 на диагонали, и число 1 и -1 совпадает с их числом для матрицы $h_{\alpha_i}(-1)$. Так как все матрицы h_i коммутируют, то существует базис, в котором все h_i имеют тот же вид, что и $h_{\alpha_i}(-1)$ в изначальном базисе из весовых векторов. Предположим, что мы перешли к этому базису с помощью матрицы g_1. Ясно, что $g_1 \in \mathrm{GL}_n(R, J)$. Рассмотрим отображение $\varphi_1 = i_{g_1}^{-1}\varphi'$. Оно также является изоморфизмом группы E на некоторую подгруппу $\mathrm{GL}_n(R)$ таким, что его образ при факторизации R по J есть $\overline{\rho}$, и $\varphi_1(h_{\alpha_i}(-1)) = h_{\alpha_i}(-1)$ для всех $i = 1, \dots, l$.

Вместо изоморфизма φ' будем теперь рассматривать изоморфизм φ_1.

Матрицы $h_{\alpha_k}(a) = \mathrm{diag}\,[a_1, 1/a_1, a_2, 1/a_2, \dots, a_m, 1/a_m, 1, \dots, 1]$ коммутируют со всеми $h_{\alpha_i}(-1)$, таким образом, их образы под действием изоморфизма φ_1 также коммутируют со всеми $h_{\alpha_i}(-1)$. Значит, эти образы имеют вид

$$\begin{pmatrix} C_1 & 0 & \dots & 0 & 0 \\ 0 & C_2 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & C_n & 0 \\ 0 & 0 & \dots & 0 & C \end{pmatrix}, \quad C_i \equiv \begin{pmatrix} \overline{\rho}(a_i) & 0 \\ 0 & \overline{\rho}(1/a_i) \end{pmatrix} \mod J, \quad C \in \mathrm{GL}_l(R, J).$$

Каждый элемент $w_i = w_{\alpha_i}(1)$ переводит (сопряжением) диагональные матрицы в диагональные, поэтому его образ имеет блочно-мономиальный вид.

Из $\varphi_1(w_i) \equiv w_i \mod J$ следует, что блоки у $\varphi_1(w_i)$ стоят на тех же местах, что и блоки у w_i.

Рассмотрим первый вектор нового, замененного, базиса, обозначим его через e. Группа Вейля W транзитивно действует на всех корнях, поэтому для любого корня α_i существует такой $w^{(\alpha_i)} \in W$, что $w^{(\alpha_i)}\alpha_1 = \alpha_i$. Рассмотрим теперь базис $e_1, \dots, e_{2m}, e_{2m+1}, \dots, e_{2m+l}$, где $e_1 = e$, $e_i = \varphi_1(w^{(\alpha_i)})e$; при $2m < i \leq 2m+1$ e_i не меняются. Ясно, что матрица такой замены базиса сравнима с 1 по модулю J. Значит, полученное множество векторов является базисом.

Ясно, что матрица $\varphi_1(w_i)$ $(i = 1, \dots, l)$ на части базиса $\{e_1, \dots, e_{2m}\}$ совпадает с матрицей w_i в изначальном базисе из весовых векторов. Так как $h_i(-1)$ являются квадратами элементов w_i, то их образы также не меняются в новом базисе.

Кроме того, мы знаем, что $\varphi_1(w_i)$ блочно-диагональна по отношению к первым $2m$ и последним l элементам. Значит, последнюю часть базиса, состоящую из l элементов, можно менять независимо.

Обозначим матрицы w_i и $\varphi_1(w_i)$ на этой части базиса через $\widetilde{w}_i$ и $\widetilde{\varphi_1(w_i)}$, соответственно. Все эти матрицы являются инволюциями, при этом у них ровно одна -1 в диагональной форме. Пусть $\widetilde{V} = \widetilde{V}_0^i \oplus \widetilde{V}_1^i$ — разложение матрицы $\widetilde{\varphi_1(w_i)}$.

Лемма 1. *Матрицы $\widetilde{\varphi_1(w_i)}$ и $\widetilde{\varphi_1(w_j)}$, при $i \neq j$, коммутируют тогда и только тогда, когда $\widetilde{V}_1^i \subseteq \widetilde{V}_0^j$ и $\widetilde{V}_1^j \subseteq \widetilde{V}_0^i$.*

Доказательство. Если $\widetilde{\varphi_1(w_i)}$ и $\widetilde{\varphi_1(w_j)}$ коммутируют, то (свободный одномерный) подмодуль $\widetilde{V}_1^i$ является собственным для $\widetilde{\varphi_1(w_j)}$ и (свободный одномерный) подмодуль $\widetilde{V}_1^j$ является собственным для $\widetilde{\varphi_1(w_i)}$. Таким образом, либо $\widetilde{V}_1^i \subset \widetilde{V}_1^j$, либо $\widetilde{V}_1^i \subset \widetilde{V}_0^j$. Если $\widetilde{V}_1^i \subset \widetilde{V}_1^j$, то $\widetilde{V}_1^i = \widetilde{V}_1^j$. Так как модуль V_0^i инвариантен для $\widetilde{\varphi}_1(w_j)$, то $\widetilde{V}_0^i \subset \widetilde{V}_0^j$, следовательно, $\widetilde{V}_0^i = \widetilde{V}_0^j$, и, значит, $\widetilde{\varphi}_1(w_i) = \widetilde{\varphi}_1(w_j)$ и мы приходим к противоречию. Следовательно, $\widetilde{V}_1^i \subset \widetilde{V}_0^j$, и, аналогично, $\widetilde{V}_1^j \subset \widetilde{V}_0^i$. $\square$

Лемма 2. *Для любой рассматриваемой системы корней Φ существует такой базис в $\widetilde{V}$, что матрица $\widetilde{\varphi}_1(w_1)$ в этом базисе имеет тот же вид, что и w_1, т.е. равна*

$$\begin{pmatrix} -1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & E_{l-2} \end{pmatrix}.$$

Доказательство. Так как $\widetilde{w}_1$ — инволюция, а $\widetilde{V}_1^1$ имеет размерность 1, то существует базис $\{e_1, e_2, \dots, e_l\}$, в котором $\widetilde{\varphi}_1(w_1)$ имеет вид $\operatorname{diag}[-1, 1, \dots, 1]$. В базисе $\{e_1, e_2 - 1/2e_1, e_3, \dots, e_l\}$ матрица $\widetilde{\varphi}_1(w_1)$ имеет искомую форму. $\square$

Лемма 3. *Для системы корней A_2 существует такой базис, что $\widetilde{\varphi}_1(w_1)$ и $\widetilde{\varphi}_1(w_2)$ в этом базисе имеют тот же вид, что w_1 и w_2, т.е. равны*

$$\begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix} \text{ и } \begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix},$$

соответственно.

Доказательство. По лемме 2 можно найти базис в $\widetilde{V}$ такой, что матрица $\widetilde{\varphi}_1(w_1)$ в этом базисе имеет тот же вид, что и w_1. Пусть матрица $\widetilde{\varphi}_1(w_2)$ в этом базисе — это

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Произведем замену базису с помощью матрицы

$$\begin{pmatrix} c & (1-c)/2 \\ 0 & 1 \end{pmatrix}$$

(эта замена корректна, так как $c \equiv 1 \mod J$). При этой замене базиса матрица $\widetilde{\varphi}_1(w_1)$ не меняет вид, а матрица $\widetilde{\varphi}_1(w_2)$ становится

$$\begin{pmatrix} a' & b' \\ 1 & d' \end{pmatrix}.$$

Так как эта матрица имеет порядок два, то $a' + d' = 0$, ${a'}^2 + b' = 1$. Значит, $d' = -a'$. Теперь используем условие

$$\left(\begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a' & b' \\ 1 & -a' \end{pmatrix}\right)^2 = \begin{pmatrix} a' & b' \\ 1 & -a' \end{pmatrix}\begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Это условие дает (вторая строка, первый столбец) $1 - 2a' = -1$, следовательно, $a' = 1$. Из ${a'}^2 + b' = 1$ следует $b' = 0$. $\square$

Лемма 4. *Для любой системы корней $\Phi \neq A_2$ можно выбрать базис в $\widetilde{V}$ такой, что матрицы $\widetilde{\varphi}_1(w_1)$ и $\widetilde{\varphi}_1(w_2)$ в этом базисе имеют тот же вид, что и $\widetilde{w}_1$ и $\widetilde{w}_2$, соответственно.*

Доказательство. Пересечение модулей $\widetilde{V}_0^1$ и $\widetilde{V}_0^2$ — это свободный модуль размерности $\geq l-3$. Таким образом, мы можем считать, что $\widetilde{\varphi}_1(w_1)$ и $\widetilde{\varphi}_1(w_2)$ имеют вид $\begin{pmatrix} * & 0 \\ 0 & E_{l-3} \end{pmatrix}$. Кроме того, по лемме 2 мы можем считать, что $\widetilde{\varphi}_1(w_1)$ имеет тот же вид, что и $\widetilde{w}_1$. Мы теперь можем рассматривать не весь модуль $\widetilde{V}$, а его ограничение на первые три базисных вектора. Пусть

$$\widetilde{\varphi}_1(w_1) = \begin{pmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{pmatrix}.$$

Проведем замену базису с помощью матрицы

$$\begin{pmatrix} b_1 & (1-b_1)/2 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

при этом не поменяется $\widetilde{\varphi}_1(w_1)$, но $\widetilde{\varphi}_1(w_2)$ перейдет в

$$\widetilde{\varphi}_1(w_1) = \begin{pmatrix} a'_1 & a'_2 & a'_3 \\ 1 & b'_2 & b'_3 \\ c'_1 & c'_2 & c'_3 \end{pmatrix}.$$

Теперь используем те же условия, что и в предыдущей лемме. Первое — это $\widetilde{\varphi}_1(w_2)^2 - 1 = 0$ (соотн. 1), второе — $(\widetilde{\varphi}_1(w_1)\widetilde{\varphi}_1(w_2))^2 - \widetilde{\varphi}_1(w_2)\widetilde{\varphi}_1(w_1) = 0$ (соотн. 2). Если вычесть соотношение 1 из соотношения 2, мы получим (строка 2, столбец 1) $a'_1 = 1$, (строка 2, столбец 2) $a'_2 = 0$, то из соотн. 1, строка 1, столбец 3, мы получим $a'_3(1 + c'_3) = 0$. Так как $c'_3 \equiv 1 \mod J$, то $a'_3 = 0$. То же соотношение (строка 2, столбец 3) дает $b'_3(b'_2 + c'_3) = 0$, а так как $b'_3 \in R^*$, то $c'_3 = -b'_2$.

Снова взяв замену базиса, но с помощью матрицы

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -c_1' & 1 \end{pmatrix},$$

мы не меняем $\widetilde{\varphi}_1(w_1)$, а $\widetilde{\varphi}_1(w_2)$ переходит в

$$\widetilde{\varphi}_1(w_1) = \begin{pmatrix} 1 & 0 & 0 \\ 1 & b_2'' & b_3'' \\ 0 & c_2'' & -b_2'' \end{pmatrix}.$$

Тогда прямо из соотношения 1 получаем $b_2'' = -1$, $c_2'' = 0$, и последняя замена базиса с помощью матрицы $\operatorname{diag}[1, 1, b_3'']$ дает нам требуемую форму для $\widetilde{\varphi}_1(w_1)$ и $\widetilde{\varphi}_1(w_2)$. $\square$

Лемма 5. *Для системы корней D_4 существует такой базис, что $\widetilde{\varphi}_1(w_1)$, $\widetilde{\varphi}_1(w_2)$, $\widetilde{\varphi}_1(w_3)$ и $\widetilde{\varphi}_1(w_4)$ в этом базисе имеют тот же вид, что и $\widetilde{w}_1$, $\widetilde{w}_2$, $\widetilde{w}_3$, и $\widetilde{w}_4$, т.е. равны*

$$\begin{pmatrix} -1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & -1 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & -1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \text{ и } \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & -1 \end{pmatrix},$$

соответственно.

Доказательство. Сначала возьмем такой базис, что $\widetilde{\varphi}_1(w_1)$, $\widetilde{\varphi}_1(w_3)$, $\widetilde{\varphi}_1(w_4)$ имеют тот же вид, что и изначальные $\widetilde{w}_1$, $\widetilde{w}_3$, $\widetilde{w}_4$. Мы это можем сделать, так как w_1, w_3, w_4 являются коммутирующими инволюциями, существует базис, в котором $\widetilde{\varphi}_1(w_1)$, $\widetilde{\varphi}_1(w_3)$, $\widetilde{\varphi}_1(w_4)$ имеют вид $\operatorname{diag}[-1, 1, 1, 1]$, $\operatorname{diag}[1, 1, -1, 1]$, $\operatorname{diag}[1, 1, 1, -1]$, соответственно. Далее, сопрягая их матрицей

$$\begin{pmatrix} 1 & -1/2 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & -1/2 & 1 & 0 \\ 0 & -1/2 & 0 & 1 \end{pmatrix},$$

мы переходим к требуемому базису. Теперь посмотрим на $\widetilde{\varphi}_1(w_2)$. Имеем следующие соотношения: $\widetilde{w}_2^2 = 1$ (соотн. 1), $(\widetilde{w}_1\widetilde{w}_2)^2 = \widetilde{w}_2\widetilde{w}_1$ (соотн. 2), $(\widetilde{w}_3\widetilde{w}_2)^2 = \widetilde{w}_2\widetilde{w}_3$ (соотн. 3), $(\widetilde{w}_4\widetilde{w}_2)^2 = \widetilde{w}_2\widetilde{w}_4$ (соотн. 4). Пусть

$$\widetilde{\varphi}_1(w_2) = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ b_1 & b_2 & b_3 & b_4 \\ c_1 & c_2 & c_3 & c_4 \\ d_1 & d_2 & d_3 & d_4 \end{pmatrix}.$$

Рассмотрим теперь замену базиса с помощью матрицы

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & \frac{d_1}{2d_1 - b_1} & 0 & \frac{b_1}{b_1 - 2d_1} \end{pmatrix},$$

мы тогда не поменяем $\widetilde{\varphi}_1(w_1)$, $\widetilde{\varphi}_1(w_3)$, $\widetilde{\varphi}_1(w_4)$, а $\widetilde{\varphi}_1(w_2)$ становится

$$\begin{pmatrix} a_1 & a_2 & a_3 & a_4\\ b_1 & b_2 & b_3 & b_4\\ c_1 & c_2 & c_3 & c_4\\ 0 & d_2 & d_3 & d_4 \end{pmatrix}$$

(для краткости мы не ставим штрихи).

Теперь из 4-ой строки разности соотношений 1 и 2 следует $d_2 = d_3 = 0$, $d_4 = 1$.

Строка 2, столбец 4 разности соотношений 1 и 4 дает $b_4(b_4 - 1) = 0$. Так как $b_4 \in R^*$, получаем $b_4 = 1$.

Теперь, взяв замену базиса с помощью матрицы

$$\begin{pmatrix} \frac{b_3}{b_3-2a_3} & \frac{a_3}{2a_3-b_3} & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 1 \end{pmatrix},$$

мы не меняем $\widetilde{\varphi}_1(w_1)$, $\widetilde{\varphi}_1(w_3)$, $\widetilde{\varphi}_1(w_4)$, а $\widetilde{\varphi}_1(w_2)$ становится

$$\begin{pmatrix} a_1 & a_2 & 0 & a_4\\ b_1 & b_2 & b_3 & 1\\ c_1 & c_2 & c_3 & c_4\\ 0 & 0 & 0 & 1 \end{pmatrix}$$

(мы снова не ставим штрихи для краткости).

Теперь строка 1, столбец 3 соотношения 1 дает $a_2 b_3 = 0 \Rightarrow a_2 = 0$, строка 1, столбец 1 соотношения 1 дает $a_1^2 = 1 \Rightarrow a_1 = 1$, строка 1, столбец 4 дает $2a_4 = 0 \Rightarrow a_4 = 0$. Строка 2, столбец 4 разности соотношений 1 и 2 дает $b_1 = 1$, строка 3, столбец 4 дает $c_4 = c_1$. Строка 2, столбец 3 соотношения 1 дает $c_3 = -b_2$.

Наконец, взяв замену базиса с помощью матрицы

$$\begin{pmatrix} 1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & \frac{1-b_3}{2} & b_3 & 0\\ 0 & 0 & 0 & 1 \end{pmatrix},$$

мы не поменяем $\widetilde{\varphi}_1(w_1)$, $\widetilde{\varphi}_1(w_3)$, $\widetilde{\varphi}_1(w_4)$, а $\widetilde{\varphi}_1(w_2)$ станет равной

$$\begin{pmatrix} 1 & 0 & 0 & a_4'\\ 1 & b_2' & 1 & 1\\ c_1' & c_2' & -b_2' & c_1'\\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

После этого строка 2, столбец 3 соотношения 3 дает $b_2' = -1$, и тогда соотн. 1 дает $c_1' = c_2' = 0$. $\square$

Лемма 6. *Предположим, что у нас есть некоторая система корней Φ и элементы $\widetilde{\varphi}_1(w_{i_1}) = \widetilde{w}_{i_1}, \ldots, \widetilde{\varphi}_1(w_{i_k}) = \widetilde{w}_{i_k}$, и также $\widetilde{\varphi}_1(w_{i_{k+1}})$, где выполнен один и следующих случаев:*

а) $\Phi = A_l$, $l \geq 3$, $i_1 = 1$, $i_2 = 2,\dots$, $i_k = k$, $i_{k+1} = k+1$, $k+1 < l$;
б) $\Phi = D_l$, $l > 4$, $i_1 = l$, $i_2 = l-1$, $i_3 = l-2$, $\dots$, $i_k = l-k+1$, $i_{k+1} = l-k$, $4 < k < l$;
в) $\Phi = E_6, E_7$ *или* E_8, $i_1 = 1$, $i_2 = 2,\dots$, $i_k = k$, $i_{k+1} = k+1$, $4 \leq k < l-1$.
Тогда можно выбрать такой базис в $\widetilde{V}$, *что* $\widetilde{\varphi}_1(w_{i_1}) = \widetilde{w}_{i_1},\dots$, $\widetilde{\varphi}_1(w_{i_{k+1}}) = \widetilde{w}_{i_{k+1}}$.

Доказательство. Во всех случаях $\widetilde{\varphi}_1(w_{i_{k+1}})$ коммутирует со всеми $\widetilde{\varphi}_1(w_{i_1}) = \widetilde{w}_{i_1},\dots,\widetilde{\varphi}_1(w_{i_{k-1}}) = \widetilde{w}_{i_{k-1}}$, следовательно (см. лемму 1), для всех $j = i_1, \dots, i_{k-1}$ $V_1^j \subset V_0^{i_{k+1}}$. Так как $V_1^{i_1} \oplus \dots \oplus V_1^{i_{k-1}} = \langle e_{i_1}, \dots, e_{i_{k-1}} \rangle$, мы получаем, что $\widetilde{\varphi}_1(w_{i_{k+1}})$ тождественна на первых $k-1$ базисных векторах. Как и в лемме 4, мы получаем, что $\widetilde{\varphi}_1(w_{i_{k+1}})$ тождественна на последних $l-k-2$ базисных векторах. Таким образом, мы можем ограничить $\widetilde{\varphi}_1(w_{i_{k+1}})$ на часть базиса $\{e_k, e_{k+1}, e_{k+2}\}$ (без потери общности). Теперь доказательство становится полностью аналогичным доказательству леммы 4. $\square$

Предложение 4. *Для любой из систем корней* $\Phi = A_l, D_l, E_l$ *мы можем выбрать базис в* $\widetilde{V}$ *такой, что матрицы* $\widetilde{\varphi}_1(w_1),\dots$, $\widetilde{\varphi}_1(w_l)$ *в этом базисе имеют вид* $\widetilde{w}_1,\dots$, $\widetilde{w}_l$, *соответственно.*

Доказательство. В случае системы корней A_2 мы можем использовать лемму 3. Если $\Phi = A_l$, $l \geq 3$, то применим лемму 4, после этого лемму 6 $l-3$ раз, и, наконец, те же рассуждения, что и в лемме 3, для элемента $\widetilde{\varphi}_1(w_l)$.

Если $\Phi = D_l$, то применим лемму 5 для корней $\alpha_{l-3}, \dots, \alpha_l$, затем лемму 6 $l-5$ раз к корням $\alpha_{l-4}, \dots, \alpha_2$, и, наконец, те же аргументы, что и в лемме 3, для элемента $\widetilde{\varphi}_1(w_1)$.

Если $\Phi = E_l$, то применим лемму 5 к корням $\alpha_2, \dots, \alpha_5$, затем лемму 6 к корням $\alpha_6, \dots, \alpha_{l-1}$, и, наконец, те же рассуждения, что и в лемме 3, к элементам $\widetilde{\varphi}_1(w_1)$ и $\widetilde{\varphi}_1(w_l)$. $\square$

Таким образом, мы теперь можем рассмотреть изоморфизм φ_2 со всеми свойствами φ_1, и еще такой, что $\varphi_2(w_i) = w_i$ для всех $i = 1, \dots, l$.

Будем далее предполагать, что мы рассматриваем изоморфизм φ_2 с этими свойствами.

4. Образы элементов $x_{\alpha_i}(1)$ и диагональных матриц.

Теперь нас будут интересовать образы $x_{\alpha_i}(t)$. Пусть $\varphi_2(x_{\alpha_1}(1)) = x_1$. Так как x_1 коммутирует со всеми $h_{\alpha_i}(-1)$, $i = 1, 3, \dots, l$, то получаем, что x_1 можно разделить на блоки следующего вида: блоки 2×2 соответствуют части базиса $\{v_i, v_{-i}\}$, где $i > 1$ и $\langle \alpha_i, \alpha_1 \rangle \neq 0$; блоки 4×4 соответствуют частям базиса $\{v_i, v_{-i}, v_j, v_{-j}\}$, где $i > 1$, $\alpha_i = \alpha_j \pm \alpha_1$; кроме того, у нас есть часть $\{v_1, v_{-1}, V_1, \dots, V_l\}$.

Для $h_{\alpha_2}(-1)$ мы знаем, что $h_{\alpha_2}(-1) x_1 h_{\alpha_2}(-1) = x_1^{-1}$. Тогда на блоках 2×2, описанных выше, если x_1 имеет вид
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix},$$
то эта матрица в квадрате есть 1, поэтому $a^2 + bc = d^2 + bc = 1$, $b(a+d) = c(a+d) = 0$. Так как $a + d \equiv 2 \mod J$, имеем $a + d \in R^*$, т.е. $b = c = 0$. Так как $a^2 = d^2 = 1$ и $a, d \equiv 1 \mod J$, то $a = d = 1$. Значит, на блоках 2×2 матрица x_1 всегда единична (т.е. совпадает с $x_{\alpha_1}(1)$ на этих блоках), значит, мы можем даже не рассматривать базисные элементы такого вида.

Теперь используем соотношения $w_i x_1 w_i^{-1} = x_1$ для $i \geq 3$.

Для начала, все блоки 4×4 имеют одинаковый вид, так как любые два таких блока сопряжены относительно действия w_i, $i \geq 3$.

Соотношения $w_i x_1 w_i^{-1} = x_1$ для $i \geq 3$ для остальных элементов базиса вместе с соотношением $h_2 x_1 h_2^{-1} = x_1^{-1}$ утверждают, что наша матрица на подмножестве базиса

$$\{v_1, v_{-1}, V_1, V_2, V_3, \ldots, V_l\}$$

имеет вид

$$\begin{pmatrix} * & * & * & * & 0 & \ldots & 0 \\ * & * & * & * & 0 & \ldots & 0 \\ * & * & * & * & 0 & \ldots & 0 \\ * & * & * & * & 0 & \ldots & 0 \\ * & * & * & * & 1 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ * & * & * & * & 0 & \ldots & 1 \end{pmatrix},$$

а все строки $5, \ldots, l$ выражаются через четвертую строку. Благодаря углу нулей для данной матрицы мы можем ограничить соотношения на ее левую верхнюю подматрицу размера 4×4.

Предположим, что на этой части базиса матрица x_1 имеет вид

$$\begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ b_1 & b_2 & b_3 & b_4 \\ c_1 & c_2 & c_3 & c_4 \\ d_1 & d_2 & d_3 & d_4 \end{pmatrix},$$

а на части базиса $v_2, v_{-2}, v_{1+2}, v_{-1-2}$ — вид

$$\begin{pmatrix} e_1 & e_2 & e_3 & e_4 \\ f_1 & f_2 & f_3 & f_4 \\ g_1 & g_2 & g_3 & g_4 \\ h_1 & h_2 & h_3 & h_4 \end{pmatrix}.$$

Мы будем рассматривать часть базиса $\{v_1, v_{-1}, v_2, v_{-2}, v_{1+2}, v_{-1-2}, V_1, V_2\}$.

Возьмем замену базиса с помощью блочно-диагональной матрицы, которая имеет вид

$$\begin{pmatrix} 1 & -\frac{b_4}{a_4} \\ -\frac{b_4}{a_4} & 1 \end{pmatrix}$$

на каждом блоке $\{v_i, v_{-i}\}$ (это возможно, так как $b_4 \in J$), и тождественна на блоке $\{V_1, \ldots, V_l\}$. Тогда элементы w_i, h_i не изменятся, а у x_1 теперь будет $b_4 = 0$. Значит, мы можем считать, что изоморфизм φ_2 таков, что $\varphi_2(x_{\alpha_1}(1))$ имеет $b_4 = 0$.

Теперь проделаем еще одну замену базиса с помощью диагональной матрицы, имеющей вид $\frac{1}{a_4} \cdot E$ на части $\{v_1, v_{-1}, \ldots, v_m, v_{-m}\}$, и единичной на части $\{V_1, \ldots, V_l\}$. Аналогично, элементы w_i, h_i не меняются, а a_4 становится равным 1.

Значит, мы можем считать, что $\varphi_2(x_{\alpha_1}(1))$ имеет $b_4 = 0$ и $a_4 = 1$.

На рассматриваемой части базиса

$$w_1=\begin{pmatrix}0&-1&0&0&0&0&0&0\\-1&0&0&0&0&0&0&0\\0&0&0&0&1&0&0&0\\0&0&0&0&0&1&0&0\\0&0&-1&0&0&0&0&0\\0&0&0&-1&0&0&0&0\\0&0&0&0&0&0&-1&1\\0&0&0&0&0&0&0&1\end{pmatrix},\quad w_2=\begin{pmatrix}0&0&0&0&-1&0&0&0\\0&0&0&0&0&-1&0&0\\0&0&0&-1&0&0&0&0\\0&0&-1&0&0&0&0&0\\1&0&0&0&0&0&0&0\\0&1&0&0&0&0&0&0\\0&0&0&0&0&0&1&0\\0&0&0&0&0&0&1&-1\end{pmatrix}.$$

Так как

$$x_{\alpha_1}(1)=\begin{pmatrix}1&-1&0&0&0&0&-2&1\\0&1&0&0&0&0&0&0\\0&0&1&0&0&0&0&0\\0&0&0&1&0&1&0&0\\0&0&-1&0&1&0&0&0\\0&0&0&0&0&1&0&0\\0&1&0&0&0&0&1&0\\0&0&0&0&0&0&0&1\end{pmatrix},$$

получаем

$$x_1=\varphi_2(x_1(1))=\begin{pmatrix}a_1&a_2&0&0&0&0&a_3&1\\b_1&b_2&0&0&0&0&b_3&0\\0&0&e_1&e_2&e_3&e_4&0&0\\0&0&f_1&f_2&f_3&f_4&0&0\\0&0&g_1&g_2&g_3&g_4&0&0\\0&0&h_1&h_2&h_3&h_4&0&0\\c_1&c_2&0&0&0&0&c_3&c_4\\d_1&d_2&0&0&0&0&d_3&d_4\end{pmatrix},$$

где $a_1,b_2,e_1,f_2,f_4,g_3,h_4,c_2,c_3,d_4\equiv 1 \mod J$, $a_2,g_1\equiv -1 \mod J$, $a_3\equiv -2 \mod J$, остальные коэффициенты лежат в J.

Тогда

$$x_{1+2}=\varphi_2(x_{\alpha_1+\alpha_2}(1))=w_2x_1w_2^{-1}=\begin{pmatrix}g_3&g_4&g_2&g_1&0&0&0&0\\h_3&h_4&h_2&h_1&0&0&0&0\\f_3&f_4&f_2&f_1&0&0&0&0\\e_3&e_4&e_2&e_1&0&0&0&0\\0&0&0&0&a_1&a_2&1+a_3&-1\\0&0&0&0&b_1&b_2&b_3&0\\0&0&0&0&c_1&c_2&c_3+c_4&-c_4\\0&0&0&0&c_1-d_1&c_2-d_2&c_3-d_3+c_4-d_4&-c_4+d_4\end{pmatrix}$$

и

$$x_2 = \varphi_2(x_{\alpha_2}(1)) = w_1 x_{1+2} w_1^{-1} = \begin{pmatrix} h_4 & h_3 & 0 & 0 & h_2 & h_1 & 0 & 0 \\ g_4 & g_3 & 0 & 0 & g_2 & g_1 & 0 & 0 \\ 0 & 0 & a_1 & a_2 & 0 & 0 & -1-a_3 & a_3 \\ 0 & 0 & b_1 & b_2 & 0 & 0 & -b_3 & b_3 \\ f_4 & f_3 & 0 & 0 & f_2 & f_1 & 0 & 0 \\ e_4 & e_3 & 0 & 0 & e_2 & e_1 & 0 & 0 \\ 0 & 0 & -d_1 & -d_2 & 0 & 0 & d_3+d_4 & -d_3 \\ 0 & 0 & c_1-d_1 & c_2-d_2 & 0 & 0 & -c_3+d_3-c_4+d_4 & c_3-d_3 \end{pmatrix}.$$

Будем использовать следующие соотношения:

$$\mathrm{Con1} := (x_1 x_{1+2} - x_{1+2} x_1 = 0), \quad \mathrm{Con2} := (h_2 x_1 h_2 x_1 - 1 = 0).$$

Позиция (3,8) соотн. Con1 дает $f_3 = -e_3$, позиция (2,8) соотн. Con1 дает $h_3 = -b_3 c_4$, позиция (2,8) соотн. Con2 дает $b_1 = b_3 c_4$, таким образом, $h_3 = -b_1$. Из позиции (1,1) соотн. Con1 получаем $b_1(a_2 + g_4) = 0$, откуда $b_1 = 0$, так как $a_2 + g_4 \in R^*$.

Введем еще два соотношения:

$$\mathrm{Con3} := (x_1 w_1 x_1 w1^{-1} - w_1 h_2 x_1 h_2 = 0), \quad \mathrm{Con4} := (x_2 x_1 - x_{1+2} x_1 x_2 = 0).$$

Обозначим $y_1 = a_1 - 1, y_2 = a_2 + 1, y_3 = a_3 + 2, y_4 = b_2 - 1, y_5 = b_3, y_6 = c_1, y_7 = c_2 - 1, y_8 = c_3 - 1, y_9 = c_4, y_{10} = d_1, y_{11} = d_2, y_{12} = d_3, y_{13} = d_4 - 1, y_{14} = e_1 - 1, y_{15} = e_2, y_{16} = e_3, y_{17} = e_4, y_{18} = f_1, y_{19} = f_2 - 1, y_{20} = f_4 - 1, y_{21} = g_1 + 1, y_{22} = g_2, y_{23} = g_3 - 1, y_{24} = g_4, y_{25} = h_1, y_{26} = h_2, y_{27} = h_4 - 1$. Все эти элементы y_i лежат в J. Из соотношений 1–4 получаем следующие 27 уравнений (линейных относительно y_i):

$y_{23}(-a_2)+y_{24}(a_1-b_2)+y_{27}a_2=0,$ Con1, поз. (1,2),
$y_{18}(-g_1)+y_{22}(a_1-e_1)+y_{26}(a_2)=0,$ Con1, поз. (1,3),
$y_1g_1+y_{15}(-g_2)+y_{19}(-g_1)+y_{25}a_2=0,$ Con1, поз. (1,4),
$y_6(a_3+1)+y_{10}(-1)+y_{16}(g_1+g_2)=0,$ Con1, поз. (1,5),
$y_3(c_2)+y_7(-1)+y_{11}(-1)+y_{20}+y_{21}(-f_4)+y_{22}(-e_4)=0,$ Con1, поз. (1,6),
$y_3(c_3+c_4-g_3)+y_8(-1)+y_9(-1)+y_{13}(-1)+y_{14}(-1)+y_{23}2+$
$+y_{24}(-b_3)=0,$ Con1, поз. (1,7),
$y_9(-a_3-1)+y_{13}+y_{23}(-1)=0,$ Con1, поз. (1,8),
$y_5c_2+y_{25}(-f_4)+y_{26}(-e_4)=0,$ Con1, поз. (2,6),
$y_{16}a_2+y_{17}(b_2-f_2)+y_{18}(-f_4)=0,$ Con1, поз. (3,6),
$y_5(e_4-f_4)+y_{16}(1+2a_3)=0,$ Con1, поз. (3,7),
$y_{15}(-f_1f_4-f_2e_3)+y_{16}(a_1-a_2+a_1h_2+f_1f_2-f_2^2)+y_{22}(e_3a_2-f_4b_2)=0,$ Con4, поз. (3,5),
$y_{10}(-d_3-d_4)+y_{11}(a_1+1)+y_{12}c_1=0,$ Con3, поз. (8,2),
$y_1(-1)+y_2(a_1+b_2)+y_3(-c_2)+y_4(-1)+y_72+y_{11}(-1)=0,$ Con2, поз. (1,2),
$y_5(-c_2g_3)+y_{16}(b_2-b_2h_4)+y_{17}a_2=0,$ Con4, поз. (6,2),
$y_{14}g_3+y_{16}(e_4-e_3)+y_{21}+y_{23}=0,$ Con3, поз. (3,3),
$y_4(b_2+1)+y_5(-c_2)=0,$ Con2, поз. (2,2),
$y_{14}(e_1+1)+y_{15}f_1+y_{16}(-g_1)+y_{17}(-h_1)=0,$ Con2, поз. (3,3),
$y_{15}(e_1+f_2)+y_{16}(-g_2)+y_{17}(-h_2)=0,$ Con2, поз. (3,4),
$y_6(-g_1a_1)+y_9(c_3+c_4-d_4)(c_1-d_1)+y_{10}(c_3^2+c_3c_4-d_3c_4-e_1)+$
$+y_{11}(-f_1)+y_{25}c_2a_1=0,$ Con4, поз. (7,3),
$y_{16}g_4+y_{18}e_4+y_{19}+y_{20}(f_2-h_4)+y_{27}(-1)=0,$ Con2, поз. (4,6),
$y_{14}+y_{21}(g_3-e_1)+y_{22}f_1+y_{23}(-1)+y_{24}h_1=0,$ Con2, поз. (5,3),
$y_{17}(-g_1)+y_{22}(-f_4)+y_{24}(g_3+h_4)=0,$ Con2, поз. (5,6),
$y_4(-c_2)+y_6(-a_2)+y_8c_2+y_9d_2=0,$ Con2, поз. (7,2),
$y_6(-1)+y_9(c_3+d_4)=0,$ Con2, поз. (7,8),
$y_1a_2+y_2+y_4+y_6a_3+y_{10}(-1-a_3)=0,$ Con3, поз. (1,2),
$y_{19}h_4+y_{20}(-1)+y_{25}(-g_2)+y_{26}(-h_2)+y_{27}=0,$ Con3, поз. (6,6),
$y_6(-g_3f_2)+y_{15}(-c_1g_4-c_2h_4)+y_{16}(d_2-d_1)+$
$+y_{22}(c_4d_2-c_3c_2-c_2c_4)+y_{26}(c_4d_1-c_3c_1-c_4c_1)=0,$ Con4, поз. (7,5).

Матрица полученной системы линейных уравнений по модулю радикала J имеет вид

$$\begin{pmatrix}
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&-1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&-1&0\\
-1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&-1&0&0\\
0&0&0&0&0&-1&0&0&0&-1&0&0&0&0&0&-1&0&0&0&0&0&0&0&0&0&0&0\\
0&0&1&0&0&0&-1&0&0&0&-1&0&0&0&0&0&0&0&0&1&-1&0&0&0&0&0&0\\
0&0&0&0&0&0&0&1&1&0&0&1&1&0&0&0&0&0&0&0&0&0&-2&0&0&0&0\\
0&0&0&0&0&0&0&0&1&0&0&0&1&0&0&0&0&0&0&0&0&0&-1&0&0&0&0\\
0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&-1&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&1&0&0&0&0&0&0&0&0&0\\
0&0&0&0&-1&0&0&0&0&0&0&0&0&0&0&-3&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&-1&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&-1&2&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
-1&2&-1&-1&0&0&2&0&0&0&-1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&1&0&1&0&0&0&0\\
0&0&0&2&-1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&2&0&1&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&2&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&-1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&-1&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&-1&0&2&0&0&0\\
0&0&0&-1&0&1&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&-1&0&0&2&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
-1&1&0&1&0&-2&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&-1&0&0&0&0&0&0&1\\
0&0&0&0&0&1&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&1&0&0&0&0&0
\end{pmatrix}.$$

Определитель этой матрицы есть 2^8, то есть это элемент, обратимый в R. Таким образом, данная система имеет единственное решение $y_1 = \dots = y_{27} = 0$. Следовательно, $x_1 = x_{\alpha_1}(1)$ на рассматриваемой части базиса. Так как все корни сопряжены друг другу относительно действия группы W, получаем $x_1 = x_{\alpha_1}(1)$ на всем базисе. Ясно, что $x_2 = x_{\alpha_2}(1)$.

Теперь рассмотрим матрицу $d_t = \varphi_2(h_{\alpha_1}(t))$. Матрица $h_{\alpha_1}(t)$ — это $\mathrm{diag}\,[t^2, 1/t^2, 1/t, t, t, 1/t, 1, 1]$ на рассматриваемой части базиса.

Лемма 7. *Матрица d_t — это $h_{\alpha_1}(s)$ для некоторого $s \in R^*$.*

Доказательство. Для матрицы d_t имеем соотношения $d_t w_3 = w_3 d_t$, …, $d_t w_l = w_l d_t$.

Пусть $l > 2$ и

$$d_t = \begin{pmatrix} \gamma_{11} & \gamma_{12} & \cdots & \gamma_{1l} \\ \gamma_{21} & \gamma_{22} & \cdots & \gamma_{2l} \\ \vdots & \vdots & \ddots & \vdots \\ \gamma_{l1} & \gamma_{l2} & \cdots & \gamma_{ll} \end{pmatrix}$$

на $\widetilde{V}$.

Каждое из соотношений $d_t w_i = w_i d_t$, $i > 2$, дает $\gamma_{1i} = \dots = \gamma_{i-1,i} = \gamma_{i+1,i} = \dots = \gamma_{li} = 0$. Из соотношения $d_t w_1 d_t w_1^{-1} = 1$ теперь сразу следует $\gamma_{33}^2 = \dots = \gamma_{ll}^2 = 1 \Rightarrow \gamma_{33} = \dots = \gamma_{ll} = 1$. Условие $d_t w_l = w_l d_t$ показывает, что $\gamma_{l-1,j}$ линейно выражается через $\gamma_{l,j}$, $j = 1, 2, \dots$, условие $d_t w_3 = w_3 d_t$ показывает, что $\gamma_{2,j}$ линейно выражается через $\gamma_{l,j}$, $j = 1, 2$.

Благодаря углу нулей мы можем рассматривать соотношения для d_t на части базиса $v_1, v_{-1}, v_2, v_{-2}, v_{1+2}$, v_{-1-2}, V_1, V_2, как мы это делали для x_1.

Так как d_t коммутирует со всеми h_i, мы получаем, что на рассматриваемой части базиса

$$d_t = \begin{pmatrix} k_1 & k_2 & 0 & 0 & 0 & 0 & 0 & 0 \\ k_3 & k_4 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & l_1 & l_2 & 0 & 0 & 0 & 0 \\ 0 & 0 & l_3 & l_4 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & m_1 & m_2 & 0 & 0 \\ 0 & 0 & 0 & 0 & m_3 & m_4 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & n_1 & n_2 \\ 0 & 0 & 0 & 0 & 0 & 0 & n_3 & n_4 \end{pmatrix}.$$

Мы знаем, что $x_2 = x_{\alpha_2}(1)$ и $x_2^t = \varphi_2(x_{\alpha_2}(t)) = d_t x_2 d_t^{-1} = d_t x_2 w_1 d_t w_1^{-1}$. Используя эти условия, получаем выражение x_2^t через коэффициенты d_t. Теперь мы можем использовать условие $\mathrm{Con5} := (x_2^t x_2 - x_2 x_2^t = 0)$. Его позиция (1,6) дает $k_1(k_2 + k_3) = 0 \Rightarrow k_2 = -k_3$, позиция (2,1) дает $k_4(l_3 - m_3) = 0 \Rightarrow m_3 = l_3$, поз. (2,5) дает $l_3(l_1 + m_4) = 0 \Rightarrow l_3 = 0$, поз. (5,6) дает $k_2(l_4 + m_1) = 0 \Rightarrow k_2 = 0$. Из $\mathrm{Con6} := (d_t w_1 d_t w_1^{-1} - 1 = 0)$ следует $k_1k_4 = l_1m_1 = l_4m_4 = 1$. Используя соотношение $\mathrm{Con7} := (w_2 d_t w_2^{-1} - d_t w_1 w_2 d_t w_2^{-1} w_1^{-1} = 0)$, получаем $m_2 = l_2 = 0$ (позиции (1,2) и (4,3)) и $l_4 = l_1k_1$ (поз. (1,1)). Позиция (7,7) соотношения Con6 дает $n_1^2 - (n_1 + n_2)n_3 = 1$, позиция (3,7) соотношения Con5 дает $n_1^2 - (3n_1 + n_2 - 2n_3 - n_4)n_3 = 1$. Таким образом, $n_3 = 0$, $n_1^2 = 1$. После этого мы очевидно получаем $n_1 = n_4 = 1$, $n_2 = 0$. Наконец, позиция (3,4) соотношения Con5 дает $k_1 = 1/l_1^2$. Обозначим $1/l_1$ через s.

Очевидно, что с помощью w_i, $i = 3, \dots l$, мы можем однозначно определить все остальные диагональные элементы. Именно, если $\langle \alpha_1, \alpha_k \rangle = p$, то $\varphi(h_{\alpha_1}(t))v_k = s^p \cdot v_k$, $\varphi(h_{\alpha_1}(t))v_{-k} = s^{-p} \cdot v_{-k}$. Поэтому $\varphi(h_{\alpha_1}(t)) = h_{\alpha_1}(s)$. □

5. Образы матриц $x_{\alpha_i}(t)$, доказательство основной теоремы.

Ясно, что $\varphi_2(h_{\alpha_k}(t)) = h_{\alpha_k}(s)$, $k = 1, \dots, n$. Обозначим отображение $t \mapsto s$ через $\rho : R^* \to R^*$. Заметим, что для $t \in R^*$ $\varphi_2(x_1(t)) = \varphi_2(h_{\alpha_2}(t^{-1})x_1(1)h_{\alpha_2}(t)) = h_{\alpha_2}(s^{-1})x_1(1)h_{\alpha_2}(s) = x_1(s)$. Если $t \notin R^*$, то $t \in J$, т. е. $t = 1 + t_1$, где $t_1 \in R^*$. Тогда $\varphi_2(x_1(t)) = \varphi_2(x_1(1)x_1(t_1)) = x_1(1)x_1(\rho(t_1)) = x_1(1 + \rho(t_1))$. Таким образом, если мы продолжим отображение ρ на все кольцо R (по формуле $\rho(t) := 1 + \rho(t-1)$, $t \in R$), то получим $\varphi_2(x_1(t)) = x_1(\rho(t))$ для всех $t \in R$. Ясно, что ρ инъективно, аддитивно, а также мультипликативно на всех обратимых элементах. Так как каждый элемент кольца R есть сумма двух обратимых, то получаем, что ρ — это изоморфизм из кольца R на некоторое его подкольцо R'. Заметим, что в данной ситуации $CE(\Phi, R)C^{-1} = E(\Phi, R')$ для некоторой матрицы $C \in \mathrm{GL}\,(V)$. Покажем, что $R' = R$.

Обозначим матричные единицы через E_{ij}.

Лемма 8. *Элементарная группа Шевалле $E(\Phi, R)$ порождает кольцо $M_n(R)$.*

Доказательство. Матрица $(x_{\alpha_1}(1) - 1)^2$ имеет единственный ненулевой элемент $-2 \cdot E_{12}$. Умножая его на подходящие диагональные матрицы, мы можем получить произвольную матрицу вида $\lambda \cdot E_{12}$ (так как $-2 \in R^*$ и R^* порождает R). Так как группа Вейля транзитивно действует на системе корней Φ, т.е. для любого корня α_k существует такой элемент $w \in W$, что $w(\alpha_1) = \alpha_k$, то матрица $\lambda E_{12} \cdot w$ имеет вид $\lambda E_{1,2k}$, а матрица $w^{-1} \cdot \lambda E_{12}$ — вид

$\lambda E_{2k-1,2}$. Кроме того, благодаря элементу группы Вейля, переводящему первый корень в противоположный, мы имеем элемент $E_{2,1}$. Беря различные комбинации полученных элементов, мы можем получить произвольный элемент λE_{ij}, $1 \leq i,j \leq 2m$. Таким образом, мы уже породили подкольцо $M_{2m}(R)$. Теперь вычтем из матрицы $x_{\alpha_1}(1)-1$ подходящие матричные единицы, получим матрицу $E_{2m+1,2}-2E_{1,2m+1}+E_{1,2m+2}$. Умножая ее (справа) на $E_{2,i}$, $1 \leq i \leq 2m$, получаем все $E_{2m+1,i}$, $1 \leq i \leq 2m$. С помощью элементов группы Вейля получим все $E_{i,j}$, $2m < i \leq 2m+l$, $1 \leq j \leq 2n$. Теперь мы имеем матрицу $-2E_{1,2m+1}+E_{1,2m+2}$. Умножая ее (слева) на $E_{2m+1,1}$, получим $E_{2m+1,2m+1}$. С помощью последних двух полученных матриц имеем $E_{1,2m+1}$, и, таким образом, все $E_{i,j}$, $1 \leq i \leq 2m$, $2m < j \leq 2m+l$. Ясно, что теперь мы породили все матричные единицы, т.е. все матричное кольцо $M_n(R)$.

Продемонстрируем это подробнее на простейшем случае системы корней A_2. Имеем $(x_{\alpha_1}(1)-1)^2 = -2E_{12}$, $h_{\alpha_2}(t)(-2E_{12}) = -2tE_{12}$, т. е. мы можем получить любой λE_{12}. Тогда $w_{\alpha_1}\lambda E_{12} w_{\alpha_1}(1)^{-1} = \lambda E_{21}$, $\lambda E_{12}E_{21} = \lambda E_{11}$, $\lambda E_{21}E_{12} = \lambda E_{22}$, $w_{\alpha_2}(1)\lambda E_{12} = \lambda E_{52}$, $w_{\alpha_2}(1)\lambda E_{21} = \lambda E_{61}$, $\lambda E_{52}E_{21} = \lambda E_{51}$, $\lambda E_{61}E_{12} = \lambda E_{62}$, $\lambda E_{12} w_{\alpha_2}(1) = \lambda E_{16}$, $\lambda E_{21} w_{\alpha_2}(1) = \lambda E_{25}$, $\lambda E_{21}E_{16} = \lambda E_{26}$, $\lambda E_{12}E_{25} = \lambda E_{15}$, $\lambda E_{51}E_{15} = \lambda E_{55}$, $\lambda E_{61}E_{16} = \lambda E_{66}$, $\lambda E_{51}E_{16} = E_{56}$, $\lambda E_{61}E_{15} = E_{65}$, $\lambda E_{i5} w_{\alpha_1}(1) = \lambda E_{i3}$, $i = 1,2,5,6$, $\lambda E_{i6} w_{\alpha_1}(1) = \lambda E_{i4}$, $i = 1,2,5,6$, $\lambda w_{\alpha_1}(1)E_{5i} = \lambda E_{3i}$, $i = 1,2,5,6$, $\lambda w_{\alpha_1}(1)E_{6i} = \lambda E_{4i}$, $i = 1,2,5,6$, $\lambda E_{41}E_{13} = \lambda E_{43}$, $\lambda E_{41}E_{14} = \lambda E_{44}$, $\lambda E_{31}E_{13} = \lambda E_{33}$, $\lambda E_{31}E_{14} = \lambda E_{34}$, таким образом, мы получили все матричные единицы подкольца $M_6(R)$.

Далее $y = x_{\alpha_1}(1)-1 = -E_{12}-2E_{17}+E_{18}+E_{46}-E_{53}+E_{73}$, $y' = y+E_{12}-E_{46}+E_{53} = E_{18}-2E_{17}+E_{72}$, $(E_{18}-2E_{17}+E_{72})\cdot\lambda E_{2i} = \lambda E_{7i}$, $i = 1,\ldots,6$, $(w_{\alpha_2}(1)-1)\lambda E_{7i} = \lambda E_{8i}$, $i = 1,\ldots,6$, $y'' = y'-E_{72} = E_{18}-2E_{17}$, $\lambda E_{81}y'' = \lambda E_{88}$, $\lambda E_{71}y'' = -2\lambda E_{77}$, $y''\lambda E_{88} = \lambda E_{18}$, $y''\lambda E_{77} = -2\lambda E_{17}$, $\lambda E_{i1}E_{17} = \lambda E_{i7}$, $\lambda E_{i1}E_{18} = \lambda E_{i8}$, и мы породили все кольцо $M_8(R)$. $\square$

Лемма 9. *Если для некоторого* $C \in \mathrm{GL}(V)$ *имеет место* $CE(\Phi,R)C^{-1} = E(\Phi,R')$, *где* R' *— это подкольцо в* R, *то* $R' = R$.

Доказательство. Предположим, что R' — это собственное подкольцо в R.

Тогда $CM_n(R)C^{-1} = M_n(R')$, так как группа $E(\Phi,R)$ порождает кольцо $M_n(R)$, а группа $E(\Phi,R') = CE(\Phi,R)C^{-1}$ порождает кольцо $M_n(R')$. Это невозможно, так как $C \in \mathrm{GL}_n(R)$. $\square$

Таким образом, мы доказали, что ρ — это автоморфизм кольца R. Следовательно, композиция изначального автоморфизма φ и некоторой замены базиса с помощью матрицы $C \in \mathrm{GL}_n(R)$, (переводящей $E(\Phi,R)$ в себя) — это кольцевой автоморфизм ρ. Это доказывает теорему 1. $\square$

Список литературы

[1] Абе Э. Автоморфизмы групп Шевалле над коммутативными кольцами. Алгебра и анализ, 1993, 5(2), 74–90.

[2] Блошицын В.Я. Автоморфизмы общей линейной группы над коммутативным кольцом, не порождаемым делителями нуля. Алгебра и логика, 1978, 17(6), 639–642.

[3] Борель А. Свойства и линейные представления групп Шевалле. Семинар по алгебраическим группам, М., 1973, 9–59.

[4] Вавилов Н.А. Параболические подгруппы групп Шевалле над коммутативным кольцом. Записки научных семинаров ЛОМИ, 1982, 116, 20–43.

[5] Вавилов Н.А., Гаврилович М.Р. A_2-доказательство структурных теорем для групп Шевалле типов E_6 и E_7. Алгебра и Анализ, 2004, 116(4), 54–87.

[6] Вавилов Н.А, Гаврилович М.Р., Николенко С.И. Строение групп Шевалле: доказательство из книги. Записки научных семинаров ЛОМИ, 2006, 330, 36–76.

[7] Вавилов Н.А., Петров В.А. О надгруппах $Ep(2l, R)$. Алгебра и Анализ, 2003, 15(3), 72–114.

[8] Голубчик И.З., Михалев А.В. Изоморфизмы унитарных групп над ассоциативными кольцами. Записки научных семинаров ЛОМИ, 1983, 132, 97–109.

[9] Голубчик И.З., Михалев А.В. Изоморфизмы общей линейной группы над ассоциативным кольцом. Вестник МГУ, серия математика, 1983, 3, 61–72.

[10] Дьедонне Ж. Геометрия классических групп. Мир, М., 1974.

[11] Залесский А.Е. Линейные группы. Итоги науки. Фундаментальные направления, М., 1989, 114–228.

[12] Зельманов Е.И. Изоморфизмы полных линейных групп над ассоциативными кольцами. Сибирский математический журнал, 1985, 26(4), 49–67.

[13] Петечук В.М. Автоморфизмы матричных групп над коммутативными кольцами. Математический сборник, 1983, 45, 527–542.

[14] Петечук В.М. Автоморфизмы групп SL_n, GL_n над некоторыми локальными кольцами. Математические заметки, 28(2), 1980, 187–206.

[15] Петечук В.М. Автоморфизмы групп $\mathrm{SL}_3(K)$, $\mathrm{GL}_3(K)$. Математические заметки, 31(5), 1982, 657–668.

[16] Суслин А.А. Об одной теореме Кона. Записки научных семинаров ЛОМИ, 1976, 64, 127–130.

[17] Шевалле К. О некоторых простых группах. Математика. Период. сб. перев. иностр. статей, 1958, 2(1), 3–58.

[18] Abe E. Chevalley groups over local rings. Tohoku Math. J., 1969, 21(3), 474–494.

[19] Abe E. Chevalley groups over commutative rings. Proc. Conf. Radical Theory, Sendai — 1988, 1–23.

[20] Abe E. Normal subgroups of Chevalley groups over commutative rings. Contemp. Math., 1989, 83, 1–17.

[21] Abe E., Hurley J. Centers of Chevalley groups over commutative rings. Comm. Algebra, 1988, 16(1), 57–74.

[22] Abe E., Suzuki K. On normal subgroups of Chevalley groups over commutative rings. Tohoku Math. J., 1976, 28(1), 185-198.

[23] Bak A. Nonabelian K-theory: The nilpotent class of K_1 and general stability. K-Theory, 1991, 4, 363–397.

[24] Bak A., Vavilov Normality of the elementary subgroup functors. Math. Proc. Cambridge Philos. Soc., 1995, 118(1), 35–47.

[25] Borel A., Tits J. Homomorphismes “abstraits” de groupes algébriques simples. Ann. Math., 1973, 73, 499–571.

[26] Bourbaki N. Groupes et Algébres de Lie. Hermann, 1968.

[27] Carter R.W. Simple groups of Lie type, 2nd ed., Wiley, London et al., 1989.

[28] Carter R.W., Chen Yu. Automorphisms of affine Kac–Moody groups and related Chevalley groups over rings. J. Algebra, 1993, 155, 44–94.

[29] Chen Yu. Isomorphic Chevalley groups over integral domains. Rend. Sem. Mat. univ. Padova, 1994, 92, 231–237.

[30] Chen Yu. On representations of elementary subgroups of Chevalley groups over algebras. proc. Amer. Math. Soc., 1995, 123(8), 2357–2361.

[31] Chen Yu. Automorphisms of simple Chevalley groups over $\mathbb{Q}$-algebras. Tohoku Math. J., 1995, 348, 81–97.

[32] Chen Yu. Isomorphisms of adjoint Chevalley groups over integral domains. Trans. Amer. Math. Soc., 1996, 348(2), 1–19.

[33] Chen Yu. Isomorphisms of Chevalley groups over algebras. J. Algebra, 2000, 226, 719–741.

[34] Chevalley C. Certain schemas des groupes semi-simples. Sem. Bourbaki, 1960–1961, 219, 1–16.

[35] Cohn P., On the structure of the GL_2 of a ring, Publ. Math. Inst. Hautes Et. Sci., 1966, 30, 365–413.

[36] Demazure M., Gabriel P. Groupes algébriques. I. North Holland, Amsterdam et al., 1970, 1–770.

[37] Demazure M., Grothendieck A. Schémas en groupes. I, II, III, Lecture Notes Math., 1971, 151, 1-564; 152, 1–654; 153, 1–529.

[38] Diedonne J., On the automorphisms of classical groups, Mem. Amer. Math. Soc., 1951, 2.
[39] Golubchik I.Z. Isomorphisms of the linear general group $\mathrm{GL}_n(R)$, $n \geq 4$, over an associative ring. Contemp. Math., 1992, 131(1), 123–136.
[40] Grothendieck A. Eléments de géoméntie algébrique (rédigés avec la collaboration de Jean Dieudonné). IV. Etude locale des schémas et des morphisms de schémas, 1967, 32, Publ. Math. IHES, 5–361.
[41] Hahn A.J., O'Meara O.T. The classical groups ans K-theory. Springer, Berlin et al., 1989.
[42] Hazrat R., Vavilov N.A. K_1 of Chevalley groups are nilpotent. J. Pure Appl. Algebra, 2003, 179, 99–116.
[43] Hua L.K., Reiner I., Automorphisms of unimodular groups, Trans. Amer. Math. Soc., 71, 1951, 331–348.
[44] Humphreys J. F., On the automorphisms of infinite Chevalley groups, Canad. J. Math., 21, 1969, 908-911.
[45] Humphreys J.E. Introduction to Lie algebras and representation theory. Springer–Verlag New York, 1978.
[46] Jantzen J.C. Representations of algebraic groups. Academic Press, N.Y., 1987.
[47] Fuan Li, Zunxian Li. Automorphisms of $\mathrm{SL}_3(R)$, $\mathrm{GL}_3(R)$. Contemp. Math., 1984, 82, 47–52.
[48] Matsumoto H. Sur les sous-groupes arithmétiques des groupes semi-simples deployés. Ann. Sci. Ecole Norm. Sup. 4$^{\text{éme}}$ sér., 1969, 2, 1–62.
[49] McDonald B.R., Automorphisms of $\mathrm{GL}_n(R)$., Trans. Amer. Math. Soc., 215, 1976, 145–159.
[50] O'Meara O.T., The automorphisms of linear groups over any integral domain, J. reine angew. Math., 223, 1966, 56–100.
[51] Stein M.R. Generators, relations and coverings of Chevalley groups over commutative rings. Amer. J. Math., 1971, 93(4), 965–1004.
[52] Stein M.R. Surjective stability in dimension 0 for K_2 and related functors, Trans. Amer. Soc., 1973, 178(1), 165–191.
[53] Stein M.R. Stability theorems for K_1, K_2 and related functors modeled on Chevalley groups. Japan J. Math., 1978, 4(1), 77–108.
[54] Steinberg R. Lectures on Chevalley groups, Yale University, 1967.
[55] Steinberg R., Automorphisms of finite linear groups, Canad. J. Math., 121, 1960, 606–615.
[56] Suzuki K., On the automorphisms of Chevalley groups over p-adic integer rings, Kumamoto J. Sci. (Math.), 16(1), 1984, 39–47.
[57] Swan R., *Generators and relations for certain special linear groups*, Adv. Math. 6 (1971), 1–77.
[58] Taddei G. Normalité des groupes élémentaire dans les groupes de Chevalley sur un anneau. Contemp. Math., Part II, 1986, 55, 693–710.
[59] Vaserstein L.N. On normal subgroups of Chevalley groups over commutative rings. Tohoku Math. J., 1986, 36(5), 219–230.
[60] Vavilov N.A. Structure of Chevalley groups over commutative rings. Proc. Conf. Non-associative algebras and related topics (Hiroshima – 1990). World Sci. Publ., London et al., 1991, 219–335.
[61] Vavilov N.A. An A_3-proof of structure theorems for Chevalley groups of types E_6 and E_7. J. Pure Appl. Algebra, 2007, 1-16.
[62] Vavilov N.A., Plotkin E.B. Chevalley groups over commutative rings. I. Elementary calculations. Acta Applicandae Math., 1996, 45, 73–115.
[63] Waterhouse W.C. Introduction to affine group schemes. Springer-Verlag, N.Y. et al., 1979.
[64] Waterhouse W.C. Automorphisms of $GL_n(R)$. Proc. Amer. Math. Soc., 1980, 79, 347–351.
[65] Waterhouse W.C. Automorphisms of quotients of $\prod GL(n_i)$. Pacif. J. Math., 1982, 79, 221–233.
[66] Waterhouse W.C. Automorphisms of $det(X_{ij})$: the group scheme approach. Adv. Math., 1987, 65(2), 171–203.