Е. И. Бунина, П. П. Семёнов, Автоморфизмы полугруппы обратимых матриц с неотрицательными элементами над коммутативными частично упорядоченными кольцами, *Фундамент. и прикл. матем.*, 2008, том 14, выпуск 2, 69–100

Автоморфизмы полугруппы обратимых матриц с неотрицательными элементами над коммутативными частично упорядоченными кольцами

Е. И. БУНИНА, П. П. СЕМЁНОВ
Московский государственный университет им. М. В. Ломоносова

УДК 512.643+512.552.2

Ключевые слова: частично упорядоченные кольца, полугруппа неотрицательных матриц, стандартные автоморфизмы.

Аннотация

В данной работе описываются автоморфизмы полугруппы $G_n(R)$ неотрицательных обратимых матриц с неотрицательными коэффициентами в случае, когда R является коммутативным частично упорядоченным кольцом, содержащим $\mathbb{Q}$, $n \geqslant 3$.

Abstract

E. I. Bunina, P. P. Semenov, Automorphisms of the semigroup of invertible matrices with nonnegative elements over commutative partially ordered rings, Fundamentalnaya i prikladnaya matematika, vol. 14 (2008), no. 2, pp. 69—100.

We describe automorphisms of the semigroup $G_n(R)$ of invertible matrices with nonnegative coefficients in the case where R is a commutative partially ordered ring containing $\mathbb{Q}$ and $n \geqslant 3$.

Пусть R — упорядоченное кольцо, $G_n(R)$ — подполугруппа группы $\mathrm{GL}_n(R)$, состоящая из матриц с неотрицательными элементами. В [3] А. В. Михалёв и М. А. Шаталова описали все автоморфизмы полугруппы $G_n(R)$ в случае, когда R является линейно упорядоченным телом и $n \geqslant 2$. В [1] Е. И. Бунина и А. В. Михалёв описали все автоморфизмы полугруппы $G_n(R)$, если R — произвольное линейно упорядоченное ассоциативное кольцо с $1/2$, $n \geqslant 3$. В данной работе мы описываем автоморфизмы полугруппы $G_n(R)$ в случае, когда R является коммутативным частично упорядоченным кольцом, содержащим $\mathbb{Q}$, $n \geqslant 3$.

Естественным примером коммутативных частично упорядоченных колец, не являющихся линейно упорядоченными и при этом содержащих $\mathbb{Q}$, являются прямые суммы линейно упорядоченных коммутативных колец (содержащих $\mathbb{Q}$) с покомпонентным сравнением. Также классическим примером являются кольца многочленов (от одной или нескольких коммутирующих переменных) над линейно (частично) упорядоченными коммутативными кольцами, содержащими $\mathbb{Q}$, где

Фундаментальная и прикладная математика, 2008, том 14, № 2, с. 69—100.

неотрицательными являются многочлены, у которых все коэффициенты неотрицательны.

1. Необходимые определения и понятия, формулировка основной теоремы

Пусть R — ассоциативное (коммутативное) кольцо с 1.

Определение 1. Кольцо R называется *частично упорядоченным*, если на нём задано отношение частичного порядка $\leqslant$, удовлетворяющее следующим условиям:

1) $\forall\, x, y, z \in R\ (x \leqslant y \Longrightarrow x + z \leqslant y + z)$;
2) $\forall\, x, y \in R\ (0 \leqslant x \wedge 0 \leqslant y \Longrightarrow 0 \leqslant xy)$.

Мы будем рассматривать такие частично упорядоченные кольца, в которых $1/m \geqslant 0$ для всех $m \in \mathbb{N}$.

Элементы r кольца R, для которых $0 \leqslant r$, называются *неотрицательными*.

Определение 2. Пусть R — частично упорядоченное кольцо. Через $G_n(R)$ обозначается подполугруппа группы $\mathrm{GL}_n(R)$, состоящая из всех матриц с неотрицательными элементами.

Множество всех обратимых элементов кольца R обозначается через R^*. Если $1/2 \in R$, то множество R^* бесконечно, так как оно содержит все $1/2^n$ для $n \in \mathbb{N}$. Множество $R_+ \cap R^*$ обозначается через R_+^*. Если $1/2 \in R$, то оно также бесконечно.

Определение 3. Пусть $I = I_n$, $\Gamma_n(R)$ — группа, состоящая из всех обратимых матриц из $G_n(R)$, Σ_n — симметрическая группа порядка n, S_σ — матрица перестановки $\sigma \in \Sigma_n$ (т. е. матрица $\bigl(\delta_{i\sigma(j)}\bigr)$, где $\delta_{i\sigma(j)}$ — символ Кронекера), $S_n = \{S_\sigma \mid \sigma \in \Sigma_n\}$, $\mathrm{diag}[d_1, \ldots, d_n]$ — диагональная матрица с элементами $d_1, \ldots, d_n$ на диагонали, $d_1, \ldots, d_n \in R_+^*$. Через $D_n(R)$ обозначим группу всех обратимых диагональных матриц из $G_n(R)$.

Определение 4. Если $\mathcal{A}$, $\mathcal{B}$ — подмножества в $G_n(R)$, то положим

$$C_{\mathcal{A}}(\mathcal{B}) = \{a \in \mathcal{A} \mid \forall\, b \in \mathcal{B}\ (ab = ba)\}.$$

Пусть E_{ij} — матричная единица.

Определение 5. Через $B_{ij}(x)$ обозначим матрицу $I + xE_{ij}$. Пусть $\mathbf{P}$ обозначает подполугруппу в $G_n(R)$, порождённую всеми матрицами S_σ $(\sigma \in \Sigma_n)$, $B_{ij}(x)$ $(x \in R_+,\ i \neq j)$ и $\mathrm{diag}[\alpha_1, \ldots, \alpha_n] \in D_n(R)$.

Определение 6. Две матрицы $A, B \in G_n(R)$ называются *$\mathcal{P}$-эквивалентными* [3], если существуют матрицы $A_j \in G_n(R)$, $j = 0, \ldots, k$, $A = A_0$, $B = A_k$, и матрицы $P_i, \tilde{P}_i, Q_i, \tilde{Q}_i \in \mathbf{P}$, $i = 0, \ldots, k-1$ такие, что $P_i A_i \tilde{P}_i = Q_i A_{i+1} \tilde{Q}_i$.

Определение 7. Через $\mathrm{GE}_n^+(R)$ обозначим подполугруппу в $G_n(R)$, порождённую всеми матрицами, $\mathcal{P}$-эквивалентными матрицам из $\mathbf{P}$.

Заметим, что если, например, R — линейно упорядоченное поле, то $\mathrm{GE}_n^+(R) = G_n(R)$.

Определение 8. Если G — некоторая полугруппа (например, $G = R_+^*$, $G_n(R), \mathrm{GE}_n^+(R)$), то гомоморфизм $\lambda(\cdot)\colon G \to G$ называется *центральным гомоморфизмом* G, если $\lambda(G) \subset Z(G)$. Отображение $\Omega(\cdot)\colon G \to G$, такое что $\Omega(X) = \lambda(X) \cdot X$ для всех $X \in G$, где $\lambda(\cdot)$ — центральный гомоморфизм, называется *центральной гомотетией*.

Например, если $R = \mathbb{R}$ (поле действительных чисел), то гомоморфизм $\lambda(\cdot)\colon G_n(\mathbb{R}) \to G_n(\mathbb{R})$, такой что $\lambda(A) = |\det A| \cdot I$ для всех $A \in G_n(\mathbb{R})$, является центральным гомоморфизмом, а отображение $\Omega(\cdot)\colon G_n(\mathbb{R}) \to G_n(\mathbb{R})$, такое что $\Omega(A) = |\det A| \cdot A$ для всех $A \in G_n(\mathbb{R})$, является центральной гомотетией. Заметим, что центральная гомотетия $\Omega(\cdot)$ всегда является эндоморфизмом полугруппы G: для всех $X, Y \in G$

$$\Omega(X)\Omega(Y) = \lambda(X)X \cdot \lambda(Y)Y = \lambda(X)\lambda(Y)X \cdot Y = \lambda(XY)XY = \Omega(XY).$$

Для каждой матрицы $M \in \Gamma_n(R)$ пусть Φ_M обозначает такой автоморфизм полугруппы $G_n(R)$, что $\Phi_M(X) = MXM^{-1}$ для всех $X \in G_n(R)$.

Для каждого автоморфизма $y(\cdot) \in \mathrm{Aut}(R_+)$ через Φ^y обозначим такой автоморфизм полугруппы $G_n(R)$, что $\Phi^y(X) = \Phi^y\big((x_{ij})\big) = \big(y(x_{ij})\big)$ для всех $X = (x_{ij}) \in G_n(R)$.

Основным результатом этой работы является следующая теорема.

Теорема. *Пусть Φ — автоморфизм полугруппы $G_n(R)$, $n \geqslant 3$, $\mathbb{Q} \subset R$. Тогда на полугруппе $\mathrm{GE}_n^+(R)$ $\Phi = \Phi_M\Phi^b\Omega$, где $M \in \Gamma_n(R)$, $b(\cdot) \in \mathrm{Aut}(R_+)$, $\Omega(\cdot)$ — центральная гомотетия полугруппы $\mathrm{GE}_n^+(R)$.*

2. Построение автоморфизма Φ'

В этом разделе мы предполагаем, что фиксирован некоторый автоморфизм $\Phi \in \mathrm{Aut}\big(G_n(R)\big)$, где $n \geqslant 3$, $\mathbb{Q} \subset R$, и с помощью его мы строим новый автоморфизм $\Phi' \in \mathrm{Aut}\big(G_n(R)\big)$, такой что $\Phi' = \Phi_{M'}\Phi$ для некоторой матрицы $M' \in \Gamma_n(R)$ и для всех $\sigma \in \Sigma_n$ выполнено условие $\Phi'(S_\sigma) = \alpha^{\mathrm{sgn}\,\sigma} S_\sigma$, $\alpha^2 = 1$ (элемент α единый для всех подстановок).

Лемма 1. *Для всех $x, y \in R_+$, если $x + y = 0$, то $x = 0$ и $y = 0$.*

Доказательство. По определению частично упорядоченного кольца получаем, что если $0 \leqslant y$, то $x \leqslant x + y$. Тогда $x \leqslant 0$, а значит, $x = 0$. Аналогично $y = 0$. □

Лемма 2. *Если Φ — автоморфизм полугруппы $G_n(R)$, где $n \geqslant 3$, $\mathbb{Q} \subset R$, то*

1) $\Phi\big(\Gamma_n(R)\big) = \Gamma_n(R)$;
2) $\Phi\big(D_n(R)\big) = D_n(R)$.

Доказательство. Так как $\Gamma_n(R)$ является подгруппой всех обратимых матриц полугруппы $G_n(R)$, то $\Phi\big(\Gamma_n(R)\big) = \Gamma_n(R)$. Утверждение 1) доказано.

Докажем второе утверждение. Рассмотрим множество $\mathcal{F}$ всех матриц $A \in \Gamma_n(R)$, коммутирующих со всеми матрицами, сопряжёнными к A.

Рассмотрим
$$B = \operatorname{diag}[\alpha_1, \dots, \alpha_n] \in D_n(R).$$
Пусть
$$A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix} \in \Gamma_n(R), \quad A^{-1} = \begin{pmatrix} a'_{11} & \dots & a'_{1n} \\ \vdots & \ddots & \vdots \\ a'_{n1} & \dots & a'_{nn} \end{pmatrix}.$$
Имеем
$$\sum_{k=1}^{n} a'_{ik} \cdot a_{kj} = 0 \quad \text{для всех} \quad i \neq j.$$
Значит, $a'_{ik} \cdot a_{kj} = 0$ для всех $i \neq j$ (по лемме 1). Тогда $A^{-1}BA$ — диагональная матрица, поэтому $D_n(R) \subset \mathcal{F}$.

Пусть существует матрица $C \in \mathcal{F} \setminus D_n(R)$,
$$C = \begin{pmatrix} c_{11} & \dots & c_{1i} & \dots & c_{1j} & \dots & c_{1n} \\ \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots \\ c_{i1} & \dots & c_{ii} & \dots & c_{ij} & \dots & c_{in} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ c_{j1} & \dots & c_{ji} & \dots & c_{jj} & \dots & c_{jn} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ c_{n1} & \dots & c_{in} & \dots & c_{jn} & \dots & c_{nn} \end{pmatrix}.$$
Сопряжём C с помощью матрицы $\operatorname{diag}[d, 1, \dots, 1] \cdot S_{i,j}$ $(i, j \neq 1)$. Сопряжённая матрица имеет вид
$$C' = \begin{pmatrix} c_{11} & \dots & c_{1j}d^{-1} & \dots & c_{1i}d^{-1} & \dots & c_{1n}d^{-1} \\ \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots \\ c_{j1}d & \dots & c_{jj} & \dots & c_{ji} & \dots & c_{jn} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ c_{i1}d & \dots & c_{ij} & \dots & c_{ii} & \dots & c_{in} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ c_{n1}d & \dots & c_{nj} & \dots & c_{nj} & \dots & c_{nn} \end{pmatrix}.$$

Использовав соотношение $CC' = C'C$, получаем (беря первый столбец и первую строку)
$$\begin{aligned} &c_{11}^2 + c_{12}c_{21}d + \dots + c_{1i}c_{j1}d + \dots + c_{1j}c_{i1}d + \dots + c_{1n}c_{n1}d = \\ &\qquad = c_{11}^2 + c_{21}c_{12}d^{-1} + \dots + c_{i1}c_{1j}d^{-1} + \dots + c_{j1}c_{1i}d^{-1} + \dots + c_{n1}c_{1n}. \end{aligned}$$

Если взять $d = 2$, то получим

$$3 \cdot (c_{12}c_{21} + \ldots + c_{1i}c_{j1} + \ldots + c_{1j}c_{i1} + \ldots + c_{1n}c_{n1}) = 0.$$

Значит (по лемме 1),

$$c_{1i}c_{j1} = 0 \quad \text{для всех} \quad i, j \neq 1.$$

Аналогично

$$c_{ki}c_{jk} = 0 \quad \text{для всех} \quad i, j \neq k.$$

Пусть

$$C^{-1} = \begin{pmatrix} \gamma_{11} & \ldots & \gamma_{1n} \\ \vdots & \ddots & \vdots \\ \gamma_{n1} & \ldots & \gamma_{nn} \end{pmatrix}.$$

Беря 1-ю строку и k-й столбец в соотношении $CC^{-1} = E$, получаем

$$0 = \gamma_{11}c_{1k} + \gamma_{12}c_{2k} + \ldots + \gamma_{1n}c_{nk},$$

откуда

$$\gamma_{11}c_{1k} = 0, \quad k \neq 1.$$

Кроме того,

$$1 = \gamma_{11}c_{11} + \gamma_{12}c_{21} + \ldots + \gamma_{1n}c_{n1}.$$

Домножим это равенство на c_{1k}, получим $c_{1k} = 0$. Аналогично $c_{ij} = 0$ при $i \neq j$. Таким образом, $\mathcal{F} = D_n(R)$, и значит, $\varphi\big(D_n(R)\big) = D_n(R)$ (так как множество $\mathcal{F}$ определяется формулой). □

Лемма 3. *Пусть* $\tau = (12)(34)\cdots(2[n/2]-1, 2[n/2]) \in S_n$. *Если* Φ *является автоморфизмом полугруппы* $G_n(R)$, $n \geqslant 3$, *то существует матрица* $M \in \Gamma_n(R)$, *такая что* $\Phi_M\Phi(S_\tau) = bS_\tau$, $b \in R_+^*$, $b^2 = 1$.

Доказательство. Рассмотрим произвольную матрицу

$$A = \begin{pmatrix} a_{11} & \ldots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \ldots & a_{nn} \end{pmatrix} \in G_n(R),$$

такую что $A^2 = 1$. Для неё выполнены соотношения $a_{ik}a_{kj} = 0$ для всех $i \neq j$. Кроме того,

$$1 = a_{11}^2 + a_{12}a_{21} + \ldots + a_{1n}a_{n1}.$$

Пусть $a_{1i}a_{i1} = e_i$, $i = 1, \ldots, n$. Тогда сразу видно, что $\{e_i\}$ — это система попарно ортогональных идемпотентов (возможно, среди них есть нулевые) кольца R, дающих в сумме 1, т. е.

$$R = e_1R \oplus e_2R \oplus \ldots \oplus e_nR.$$

Разложим матрицу A в сумму $e_1A + \ldots + e_nA$. Явно выпишем $A_i = e_iA$:

$$A_1 = \begin{pmatrix} a_{11} & 0 & \ldots & 0 \\ 0 & e_1a_{22} & \ldots & e_1a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & e_1a_{n2} & \ldots & e_1a_{nn} \end{pmatrix},$$

$$A_i = \begin{pmatrix} 0 & 0 & 0 & a_{1i} & 0 & 0 \\ 0 & e_ia_{22} & \ldots & 0 & \ldots & e_ia_{2n} \\ 0 & \vdots & * & 0 & * & \vdots \\ a_{i1} & 0 & 0 & 0 & 0 & 0 \\ 0 & \vdots & * & 0 & * & \vdots \\ 0 & e_ia_{n2} & \ldots & 0 & \ldots & e_ia_{nn} \end{pmatrix}, \quad i > 1.$$

Сопряжем матрицу A матрицей $B = e_1B + \ldots + e_nB = B_1 + \ldots + B_n$, где $B_1 = e_1 \cdot I$, $B_i = e_i \cdot S_{(2i)}$. Тогда

$$A' = B^{-1}AB = e_1A' + \ldots e_nA' = A'_1 + \ldots + A'_n,$$

где $A'_1 = A_1$,

$$A'_i = \begin{pmatrix} 0 & a_{1i} & 0 & \ldots & 0 \\ a_{i1} & 0 & 0 & \ldots & 0 \\ 0 & 0 & \alpha_{11} & \ldots & \alpha_{1,n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \alpha_{n-2,1} & \ldots & \alpha_{n-2,n-2} \end{pmatrix}, \quad i > 1.$$

Обозначим матрицу

$$\begin{pmatrix} \alpha_{11} & \ldots & \alpha_{1,n-2} \\ \vdots & \ddots & \vdots \\ \alpha_{n-2,1} & \ldots & \alpha_{n-2,n-2} \end{pmatrix},$$

а в случае $i = 1$ матрицу

$$\begin{pmatrix} e_1a_{22} & \ldots & e_1a_{2n} \\ \vdots & \ddots & \vdots \\ e_1a_{n2} & \ldots & e_1a_{nn} \end{pmatrix},$$

через $\Lambda_i^{(1)}$. Получается, что исходная матрица A сопряжена к матрице

$$\sum_{i=1}^{n} \begin{pmatrix} D_i^{(1)} & 0 \\ 0 & \Lambda_i^{(1)} \end{pmatrix},$$

все матрицы $D_i^{(1)}$ имеют размер 1×1 или 2×2, все слагаемые в сумме взаимно ортогональны.

Заметим, что каждая $\Lambda_i^{(1)}$ — это матрица над кольцом e_iR размера меньше n, такая что ${\Lambda_i^{(1)}}^2 = I$. Значит, можно повторить предыдущие рассуждения для матрицы $\Lambda_i^{(1)}$ и соответствующей системы $\{e_{ij} \mid j = 1, \ldots, n\}$ ортогональных идемпотентов кольца e_iR. В результате мы получим, что исходная матрица сопряжена сумме матриц

$$\sum_{i,j=1}^{n} \begin{pmatrix} D_{ij}^{(1)} & 0 & 0 \\ 0 & D_{ij}^{(2)} & 0 \\ 0 & 0 & \Lambda_{ij}^{(2)} \end{pmatrix},$$

где каждая из матриц в сумме лежит в соответствующем матричном кольце над $e_{ij}R$, матрицы $D_{ij}^{(1)}$ и $D_{ij}^{(2)}$ имеют размер 1×1 или 2×2.

Продолжая этот процесс дальше, мы получим, что матрица A сопряжена сумме матриц из взаимно ортогональных матричных колец (соответствующих системе ортогональных идемпотентов $\{e'_1, \ldots, e'_N\}$ кольца R), каждая из которых блочно-диагональна, блоки имеют размер 1×1 и 2×2. Произведя ещё одну замену базиса с помощью матрицы

$$\sum_{k=1}^{N} e'_k C_k,$$

где каждая C_k есть матрица перестановки, переставляющей в соответствующей матрице суммы все блоки размера 2×2 в начало, а блоки размера 1×1 в конец, мы придём к матрице $\tilde{A}$, сопряжённой исходной матрице A и состоящей из диагональных блоков размера 2×2 и 1×1.

Таким образом, каждый элемент порядка два в группе $\Gamma_n(R)$ сопряжён к матрице, состоящей из диагональный блоков размера 2×2 и 1×1.

Рассмотрим множество

$$\mathcal{F} = \Big\{ D \in D_n(R) \mid \\ \forall\, N \in \Gamma_n(R)\ \Big(N^2 = I \Longrightarrow \exists\, C \in \Gamma_n(R)\ \big(D(CNC^{-1}) = (CNC^{-1}D)\big)\Big)\Big\}.$$

Это множество состоит из всех таких диагональных матриц D, что для любого элемента N нашей полугруппы, имеющего порядок два, существует матрица, сопряжённая к N и коммутирующая с D. Тогда D в некотором базисе имеет вид

$$\begin{aligned} &\operatorname{diag}[\alpha_1, \alpha_1, \alpha_2, \alpha_2, \ldots, \alpha_k, \alpha_k, \alpha], && \text{если } n = 2k+1, \\ &\operatorname{diag}[\alpha_1, \alpha_1, \ldots, \alpha_k, \alpha_k], && \text{если } n = 2k, \end{aligned} \tag{$*$}$$

так как в качестве N можно взять матрицу S_τ.

Далее рассмотрим множество

$$\Lambda = \big\{ D \in \mathcal{F} \mid \forall\, D' \in \mathcal{F}\ C_{\Gamma_n(R)}(D) \not\supset C_{\Gamma_n(R)}(D') \big\},$$

состоящее из матриц из $\mathcal{F}$ с минимальными централизаторами.

Любая матрица из $\mathcal{F}$ коммутирует (в том базисе, в котором она имеет вид $(*)$) со всеми матрицами, которые в этом базисе разбиты на диагональные блоки размера 2×2 (и, возможно, блок 1×1 в самом конце). Значит, Λ содержит матрицы, централизатор которых состоит только из таких матриц. С другой стороны, в любом базисе такие матрицы существуют, например, это матрицы вида $\operatorname{diag}[1, 1, 2, 2, \ldots, k, k, \ldots]$ (здесь используется обратимость натуральных чисел).

Рассмотрим элемент J порядка 2, который коммутирует с некоторой матрицей $C \in \Lambda$ и, если J коммутирует с некоторой диагональной матрицей C', $C_{\Gamma_n(R)}(C) \subset C_{\Gamma_n(R)}(C')$. Так как $J \in C_{\Gamma_n(R)}(C)$ и $C \in \Lambda$, то J состоит из диагональных блоков 2×2 (и, возможно, одного блока 1×1 в конце). Рассмотрим один из этих блоков

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

Так как $J_i^2 = I$, то $e_1 = a^2$ и $e_2 = bc$ — это ортогональные идемпотенты, в сумме дающие 1. Мы знаем, что $J_i \cdot \operatorname{diag}[\alpha, \beta] \neq \operatorname{diag}[\alpha, \beta] \cdot J_i$ ни для каких обратимых $\alpha \neq \beta$ (по выбору матрицы J). Возьмём $\alpha = 1 = a^2 + bc$ и $\beta = a^2/2 + bc$. Тогда α и β обратимы и $J_i \cdot \operatorname{diag}[\alpha, \beta] = \operatorname{diag}[\alpha, \beta] \cdot J_i$. Значит, $\alpha = \beta$, т. е. $a^2 = 0$. Следовательно, $bc = 1$. Так как $abc = 0$, то $a = 0$. Аналогично $d = 0$. Таким образом,

$$J = \begin{pmatrix} 0 & b_1 & \ldots & 0 & 0 \\ b_1^{-1} & 0 & \ldots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 0 & b_k \\ 0 & 0 & \ldots & b_k^{-1} & 0 \end{pmatrix} \quad \text{или} \quad J = \begin{pmatrix} 0 & b_1 & \ldots & 0 & 0 & 0 \\ b_1^{-1} & 0 & \ldots & 0 & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & \ldots & 0 & b_k & 0 \\ 0 & 0 & \ldots & b_k^{-1} & 0 & 0 \\ 0 & 0 & \ldots & 0 & 0 & b \end{pmatrix}.$$

После сопряжения матрицы J с помощью диагональной матрицы $\operatorname{diag}[b_1, 1, b_2, 1, \ldots, b_k, 1]$ или $\operatorname{diag}[b_1, b, b_2, b, \ldots, b_k, b, 1]$ мы получим матрицу $J' = S_\tau$ или соответственно bS_τ. Таким образом, мы нашли такую матрицу $M \in \Gamma_n(R)$, что $M\Phi(S_\tau)M^{-1} = bS_\tau$, $b^2 = 1$. □

Лемма 4. *Пусть $n = 3$, Φ — такой автоморфизм полугруппы $G_n(R)$, что $\Phi(S_\tau) = bS_\tau$, $b^2 = 1$, где τ — подстановка из предыдущей леммы (в нашем случае это просто (12)). Тогда существует такая матрица $M \in \Gamma_{n(R)}$, что $\Phi'(S_\rho) = \Phi_M \circ \Phi(S_\rho) = b^{\operatorname{sgn}\rho} S_\rho$ для всех $\rho \in \Sigma_n$.*

Доказательство. Из леммы 2 следует, что для любых $\alpha, \beta \in R_+^*$

$$\Phi(\operatorname{diag}[\alpha, \alpha, \beta]) = \operatorname{diag}[\alpha', \alpha', \beta'],$$

так как $\Phi\big(S_{(12)}\big) = bS_{(12)}$ и первая из матриц коммутирует с $S_{(12)}$. Если $\alpha \neq \beta$, то $\alpha' \neq \beta'$, так как $\operatorname{diag}[\alpha, \alpha, \beta]$ не может переходить в скалярную матрицу (центр полугруппы матриц). Пусть

$$\Phi\bigl(S_{(23)}\bigr) = A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}.$$

Так как $A^2 = I$, то, как и ранее, получаем

$$a_{ik}a_{kj} = 0, \quad a_{1i}a_{i1} + a_{2i}a_{i2} + a_{3i}a_{i3} = 1. \tag{1}$$

Заметим, что A не коммутирует с $\mathrm{diag}[\alpha', \alpha', \beta']$. Отсюда получаем, что должно выполняться хотя бы одно из следующих условий:

$$\alpha a_{13} \neq \beta a_{13}, \quad \alpha a_{23} \neq \beta a_{23}, \quad \alpha a_{31} \neq \beta a_{31}, \quad \alpha a_{32} \neq \beta a_{32}.$$

Так как $A^2 = I$, то, как и в предыдущей лемме, $\xi = a_{12}a_{21}$ — идемпотент. Предположим, что он ненулевой. Тогда возьмём $\alpha' = 1 + \xi$, $\beta' = 1$ (α' обратим, обратным к нему является элемент $1 - \xi/2$). Тогда не выполняется ни одно из выписанных выше условий. Получаем противоречие, значит, $a_{12}a_{21} = 0$. Так как $A^2 = I$, то $a_{11}^2 + a_{13}a_{31} = 1$. Умножив это равенство на a_{12}, получаем $a_{12} = 0$. Аналогично $a_{21} = 0$. Теперь воспользуемся тем, что матрица $S_{(12)}S_{(23)} = S_{(123)}$ имеет порядок 3, а значит, $\bigl(bS_{(12)}A\bigr)^3 = I$. Отсюда, пользуясь (1), получаем условия

$$a_{11}a_{23}a_{32} + a_{22}a_{13}a_{31} = b, \quad a_{11}^2 a_{22} = 0, \quad a_{11}a_{22}^2 = 0. \tag{2}$$

Согласно (1) имеем, что $a_{11}^3 = a_{11}$, $a_{22}^3 = a_{22}$, $a_{11}a_{23}a_{32} = a_{11}$, $a_{22}a_{13}a_{31} = a_{22}$, следовательно, $a_{11} + a_{22} = b$. С другой стороны, $a_{11}a_{23}a_{32} + a_{22}a_{13}a_{31} + a_{33}^3 = b$, а значит, $a_{33}^3 = 0 = a_{33}$. Таким образом, мы можем переписать (1) в виде

$$a_{13}a_{31} + a_{23}a_{32} = 1, \quad a_{11}^2 + a_{31}a_{13} = 1, \quad a_{22}^2 + a_{32}a_{23} = 1.$$

Обозначим $e_1 = a_{23}a_{32}$, $e_2 = a_{13}a_{31}$. Это ортогональные идемпотенты, в сумме дающие 1. Таким образом, мы знаем, что $a_{11}e_1 + a_{22}e_2 = b$ (это одно из равенств (2)). Значит, $a_{11}e_1 = be_1$, но так как a_{11} ортогонален e_2, то он лежит в кольце e_1R, поэтому $a_{11} = ba_{11}e_1 = be_1$. Аналогично получаем $a_{22} = be_2$, и матрица A имеет вид

$$A = \begin{pmatrix} be_1 & 0 & a_{13} \\ 0 & be_2 & a_{23} \\ a_{31} & a_{32} & 0 \end{pmatrix}.$$

Возьмём теперь матрицу

$$C = \begin{pmatrix} e_1 & e_2 & 0 \\ e_2 & e_1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Она обратима (обратна сама себе) и коммутирует с $S_{(12)}$, следовательно, при автоморфизме Φ_C матрица $S_{(12)}$ перейдёт в $bS_{(12)}$. При этом матрица A перейдёт в матрицу

$$A' = \begin{pmatrix} b & 0 & 0 \\ 0 & 0 & b(a_{13} + a_{23}) \\ 0 & b(a_{31} + a_{32}) & 0 \end{pmatrix}.$$

Заметим, что $(a_{13}+a_{23})(a_{31}+a_{32}) = e_1+e_2 = 1$. Теперь возьмём матрицу $C' = \operatorname{diag}[1,1,a_{13}+a_{23}]$ (она также коммутирует с $S_{(12)}$) и сопряжем A' с помощью неё. Получим $bS_{(23)}$. Так как группа подстановок порождается подстановками (12) и (23), то автоморфизм $\Phi' = \Phi_M \circ \Phi$ является искомым. Лемма доказана. □

Лемма 5. *Пусть* $n = 4$, Φ — *такой автоморфизм полугруппы* $G_n(R)$, *что* $\Phi(S_\tau) = S_\tau$, *где* τ — *подстановка из леммы* 3 (*в нашем случае это просто* (12)(34)). *Пусть* $\rho = (13)(24)$. *Тогда существует такая матрица* $M \in \Gamma_{n(R)}$, *что* $\Phi_M \circ \Phi(S_\rho) = S_\rho$ *и* $\Phi_M \circ \Phi(S_\tau) = S_\tau$.

Доказательство. Пусть $X = \Phi(S_\rho)$. Так как S_τ коммутирует с S_ρ, то

$$X = \begin{pmatrix} a_1 & a_2 & b_1 & b_2 \\ a_2 & a_1 & b_2 & b_1 \\ c_1 & c_2 & d_1 & d_2 \\ c_2 & c_1 & d_2 & d_1 \end{pmatrix}.$$

Будем рассматривать X как матрицу размера 2×2 над матрицами 2×2:

$$X = \begin{pmatrix} A & B \\ C & D \end{pmatrix}, \quad A,B,C,D \in \mathrm{M}_2(R).$$

Так как $X^2 = I$, то $A^2 + BC = I_2$, причём, так как

$$A = \begin{pmatrix} a_1 & a_2 \\ a_2 & a_1 \end{pmatrix},$$

имеем

$$A^2 = \begin{pmatrix} a_1^2+a_2^2 & 2a_1a_2 \\ 2a_1a_2 & a_1^2+a_2^2 \end{pmatrix}.$$

Значит, у матриц A^2 и (аналогично) BC на диагонали стоят равные элементы. Так как сумма матриц A^2 и BC имеет нули вне главной диагонали, то и сами матрицы A^2 и BC диагональны (и даже скалярны). Значит, они являются центральными идемпотентами кольца матриц 2×2. Заметим, далее, что матрица $\operatorname{diag}[d_1,d_1,d_2,d_2]$, где $d_1 \neq d_2$, $d_1,d_2 \in R_+^*$, перейдёт при автоморфизме в матрицу такого же вида, т. е. $\operatorname{diag}[d_1',d_1',d_2',d_2']$, $d_1' \neq d_2'$, потому что данная матрица диагональна, коммутирует с S_τ и нескалярна. Будем рассматривать матрицу

$$\begin{pmatrix} A^2/2+BC & 0 \\ 0 & I_2 \end{pmatrix}.$$

Она имеет описанный выше вид и коммутирует с X (для проверки надо воспользоваться коммутированием B и C и равенствами $B^2C = B$ и $BC^2 = C$, получающимися из $A^2+BC = I_2$ умножением на B и C). Значит, $A^2/2+BC = I_2 = A^2+BC$, $A^2 = 0$, $BC = I_2$, а так как $ABC = 0$, то $A = 0$, аналогично $D = 0$. Теперь нетрудно убедиться, что

$$M = \begin{pmatrix} C & 0 \\ 0 & I_2 \end{pmatrix}$$

(заметим, что M коммутирует с матрицей S_τ). Таким образом, лемма доказана. $\square$

Лемма 6. *Пусть $n = 4$, Φ — автоморфизм, построенный в предыдущей лемме. Тогда найдутся матрица $M \in \Gamma_n(R)$ и инволюция $a \in R_+^*$, такие что $\Phi_M \circ \Phi(S_\sigma) = a^{\operatorname{sgn}\sigma} S_\sigma$ для любой подстановки σ.*

Доказательство. Пусть $Y = \Phi\big(S_{(4321)}\big)$, где Φ — автоморфизм из предыдущей леммы. Так как $S_{(4321)}$ коммутирует с матрицей $S_{(13)(24)}$, Y имеет вид

$$Y = \begin{pmatrix} y_1 & z_1 & y_2 & z_2 \\ x_1 & w_1 & x_2 & w_2 \\ y_2 & z_2 & y_1 & z_1 \\ x_2 & w_2 & x_1 & w_1 \end{pmatrix}.$$

Теперь воспользуемся тождеством

$$S_{(4321)} S_{(12)(34)} = S_{(14)(23)} S_{(4321)},$$

из которого получим равенства $x_1 = z_2$, $z_1 = x_2$, $y_1 = w_2$, $w_1 = y_2$. Таким образом,

$$Y = \begin{pmatrix} y_1 & z_1 & y_2 & z_2 \\ z_2 & y_2 & z_1 & y_1 \\ y_2 & z_2 & y_1 & z_1 \\ z_1 & y_1 & z_2 & y_2 \end{pmatrix}.$$

Наконец, воспользуемся тем, что $Y^2 = S_{(13)(24)}$. Отсюда имеем условия

$$y_1^2 + 2z_1z_2 + y_2^2 = 0, \quad y_1z_2 + y_1z_1 + y_2z_1 + y_2z_2 = 0, \quad z_1^2 + 2y_1y_2 + z_2^2 = 1.$$

Умножив последнее равенство на y_1, получим

$$z_1^2 y_1 + 2y_1^2 y_2 + z_2^2 y_1 = y_1,$$

но из первых равенств следует, что $y_1^2 = 0$, $y_1z_1 = 0$, $y_1z_2 = 0$ (см. лемму 1). Значит, $y_1 = 0$, аналогично $y_2 = 0$. Таким образом,

$$Y = \begin{pmatrix} 0 & z_1 & 0 & z_2 \\ z_2 & 0 & z_1 & 0 \\ 0 & z_2 & 0 & z_1 \\ z_1 & 0 & z_2 & 0 \end{pmatrix} = \begin{pmatrix} 0 & z_1 & 0 & 0 \\ 0 & 0 & z_1 & 0 \\ 0 & 0 & 0 & z_1 \\ z_1 & 0 & 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 0 & z_2 \\ z_2 & 0 & 0 & 0 \\ 0 & z_2 & 0 & 0 \\ 0 & 0 & z_2 & 0 \end{pmatrix}.$$

Имеем $z_1^2 + z_2^2 = 1$ и $z_1z_2 = 0$. Положим $M_1 = z_2^2 S_{(14)(23)} + z_1^2 I_4$ (матрица M обратима — обратна самой себе). Пусть $\Phi_1 = \Phi_{M_1} \circ \Phi$, тогда (так как M_1 коммутирует с S_τ и S_ρ)

$$\Phi_1\big(S_{(4321)}\big) = (z_1 + z_2) S_{(4321)}, \quad \Phi_1(S_\tau) = S_\tau, \quad \Phi_1(S_\rho) = S_\rho.$$

Далее будем рассматривать матрицу $A = \Phi_1(S_{12})$. Тогда из условий коммутирования S_{12} с $S_{(12)(34)}$ и с $\operatorname{diag}[\alpha, \alpha, \beta, \beta]$ (а последняя при автоморфизме переходит в подобную ей, если $\alpha, \beta \in R_+^*$, см. предыдущую лемму) получаем, что

$$A = \begin{pmatrix} a_1 & a_2 & 0 & 0 \\ a_2 & a_1 & 0 & 0 \\ 0 & 0 & b_1 & b_2 \\ 0 & 0 & b_2 & b_1 \end{pmatrix}.$$

Из тождества

$$S_{(13)(24)} S_{(12)} S_{(13)(24)} S_{(12)} = S_{(12)(34)}$$

следуют условия на элементы матрицы:

$$a_1 b_1 + a_2 b_2 = 0, \quad a_1 b_2 + a_2 b_1 = 1.$$

Из первого равенства получим $a_1 b_1 = a_2 b_2 = 0$. Домножим второе равенство на a_1, получим $a_1^2 b_2 + a_1 a_2 b_1 = a_1$. Так как $X^2 = I_4$ ($a_1 a_2 = 0$, $a_1^2 = 1 - a_2^2$), имеем $a_1 = b_2(1 - a_2^2) = b_2$. Аналогично $a_2 = b_1$. Таким образом,

$$A = \begin{pmatrix} a_1 & a_2 & 0 & 0 \\ a_2 & a_1 & 0 & 0 \\ 0 & 0 & a_2 & a_1 \\ 0 & 0 & a_1 & a_2 \end{pmatrix} = \begin{pmatrix} 0 & a_2 & 0 & 0 \\ a_2 & 0 & 0 & 0 \\ 0 & 0 & a_2 & 0 \\ 0 & 0 & 0 & a_2 \end{pmatrix} + \begin{pmatrix} a_1 & 0 & 0 & 0 \\ 0 & a_1 & 0 & 0 \\ 0 & 0 & 0 & a_1 \\ 0 & 0 & a_1 & 0 \end{pmatrix}.$$

Положим $M' = a_1^2 S_{(13)(24)} + a_2^2 I_4$ (эта матрица обратима — обратна самой себе). Пусть $\Phi_2 = \Phi_{M'} \circ \Phi_1$, тогда (так как M' коммутирует с $S_{(4321)}$, S_τ и S_ρ)

$$\Phi_2\big(S_{(12)}\big) = (a_1 + a_2) S_{(12)}, \quad \Phi_2\big(S_{(4321)}\big) = (z_1 + z_2) S_{(4321)},$$
$$\Phi_2(S_\tau) = S_\tau, \quad \Phi_2(S_\rho) = S_\rho.$$

Осталось доказать, что инволюции $a_1 + a_2$ и $z_1 + z_2$ совпадают. Пусть

$$X = \Phi_2\big(S_{(432)}\big) = (a_1 + a_2)(z_1 + z_2) S_{(432)}.$$

Так как $(432) = (4321)(12)$, то $X^3 = I_4$, следовательно, $(a_1 + a_2)^3 (z_1 + z_2)^3 = 1$. Таким образом, $(a_1 + a_2)(z_1 + z_2) = 1$, значит, $z_1 + z_2 = (a_1 + a_2)^{-1} = a_1 + a_2$. $\square$

Определение 9. Пусть число n разложено в сумму степеней двойки:

$$n = 2^{k_1} + 2^{k_2} + \ldots + 2^{k_l}, \quad k_1 > k_2 > \ldots > k_l \geqslant 0.$$

Диагональный блок размера $2^{k_i} \times 2^{k_i}$, $i = 1, \ldots, l$, матрицы размера $n \times n$, соответствующий векторам базиса с номерами

$$2^{k_1} + 2^{k_2} + \ldots + 2^{k_{i-1}} + 1, \ldots, \ 2^{k_1} + 2^{k_2} + \ldots + 2^{k_i},$$

будем обозначать через $\mathbf{D}_i$.

Определение 10. Через $\sigma_i^{(j)}$, $j = 1, \ldots, l$, $i = 1, \ldots, k_i$, обозначим подстановку, которая тождественно действует во всех блоках $\mathbf{D}_m$, кроме блока $\mathbf{D}_j$, а в блоке $\mathbf{D}_j$ является произведением $2^{k_j - 1}$ транспозиций, каждая из которых имеет вид $(p, p + 2^{i-1})$.

Через σ_i обозначим подстановку $\sigma_{i_1}^{(1)} \cdot \ldots \cdot \sigma_{i_l}^{(l)}$, где $i_q = \min(i, k_q)$.

Например, для $n = 7$

$$\sigma_1 = (1,2)(3,4)(5,6), \quad \sigma_2 = (1,3)(2,4)(5,6),$$

для $n = 10$

$$\sigma_1 = (1,2)(3,4)(5,6)(7,8)(9,10), \quad \sigma_2 = (1,3)(2,4)(5,7)(6,8)(9,10),$$
$$\sigma_3 = (1,5)(2,6)(3,7)(4,8)(9,10).$$

Лемма 7. *Пусть Φ — произвольный автоморфизм полугруппы $G_n(R)$. Тогда найдётся матрица $M \in \Gamma_n(R)$, такая что $\Phi_M \circ \Phi(S_{\sigma_i}) = a_i S_{\sigma_i}$, $a_i^2 = 1$, для всех $i = 1, 2, \ldots$.*

Доказательство. По лемме 3 мы можем выбрать такую матрицу M_1, что

$$\Phi_1(S_{\sigma_1}) = \Phi_{M_1} \circ \Phi(S_{\sigma_1}) = S_{\sigma_1}.$$

Теперь рассмотрим матрицу $A_2 = \Phi_1(S_{\sigma_2})$. Пусть n нечётно. Так как A_2 коммутирует с матрицей S_{σ_1}, то она имеет вид

$$A_2 = \begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} & \ldots & a_{1,n-2} & a_{1,n-1} & a_{1,n} \\ a_{12} & a_{11} & a_{14} & a_{13} & \ldots & a_{1,n-1} & a_{1,n-2} & a_{1,n} \\ a_{31} & a_{32} & a_{33} & a_{34} & \ldots & a_{3,n-2} & a_{3,n-1} & a_{3,n} \\ a_{32} & a_{31} & a_{34} & a_{33} & \ldots & a_{3,n-1} & a_{3,n-2} & a_{3,n} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \\ a_{n-2,1} & a_{n-2,2} & a_{n-2,3} & a_{n-2,4} & \ldots & a_{n-2,n-2} & a_{n-2,n-1} & a_{n-2,n} \\ a_{n-2,2} & a_{n-2,1} & a_{n-2,4} & a_{n-2,3} & \ldots & a_{n-2,n-1} & a_{n-2,n-2} & a_{n-2,n} \\ a_{n,1} & a_{n,1} & a_{n,3} & a_{n,3} & \ldots & a_{n,n-2} & a_{n,n-2} & a_{n,n} \end{pmatrix}.$$

Тогда из того, что $A_2^2 = I$, следует, что (если рассмотреть первый столбец, умноженный на вторую строчку, третий столбец, умноженный на четвёртую строчку, и т. д.) $a_{n,i} a_{i,n} = 0$ для всех $i = 1, \ldots, n-1$. Теперь рассмотрим последний столбец, умноженный на последнюю строчку. Из найденных равенств получим $a_{n,n}^2 = 1$, т. е. $a_{n,n}$ — обратимый элемент кольца R. Отсюда следует, что $a_{i,n} = a_{n,i} = 0$ для всех $i = 1, \ldots, n-1$. Таким образом, можно рассматривать ограничение данной матрицы на размер $(n-1) \times (n-1)$. Поэтому можем пока считать, что размерность группы чётна. В этом случае матрица имеет вид

$$A_2 = \begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} & \ldots & a_{1,n-1} & a_{1,n} \\ a_{12} & a_{11} & a_{14} & a_{13} & \ldots & a_{1,n} & a_{1,n-1} \\ a_{31} & a_{32} & a_{33} & a_{34} & \ldots & a_{3,n-1} & a_{3,n} \\ a_{32} & a_{31} & a_{34} & a_{33} & \ldots & a_{3,n} & a_{3,n-1} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{n-1,1} & a_{n-1,2} & a_{n-1,3} & a_{n-1,4} & \ldots & a_{n-1,n-1} & a_{n-1,n} \\ a_{n-1,2} & a_{n-1,1} & a_{n-1,4} & a_{n-1,3} & \ldots & a_{n-1,n} & a_{n-1,n-1} \end{pmatrix}.$$

Будем рассматривать A_2 как матрицу размера $n/2\times n/2$ над матрицами 2×2:

$$A_2 = \begin{pmatrix} A_2^{(1,1)} & \dots & A_2^{1,n/2} \\ \vdots & \ddots & \vdots \\ A_2^{(n/2,1)} & \dots & A_2^{(n/2,n/2)} \end{pmatrix}, \quad A_2^{(1,1)}, \dots, A_2^{(n/2,n/2)} \in \mathrm{M}_2(R).$$

Так как $A_2^2 = 1$, то

$$A_2^{(1,1)^2} + A_2^{(1,2)} A_2^{(2,1)} + \dots + A_2^{(1,n/2)} A_2^{(n/2,1)} = I_2,$$

причём, так как

$$A_2^{(i,j)} = \begin{pmatrix} a & b \\ b & a \end{pmatrix},$$

имеем, что

$$A_2^{(1,i)} A_2^{(i,1)} = \begin{pmatrix} a_1a_2 + b_1b_2 & a_1b_2 + a_2b_1 \\ a_1b_2 + a_2b_1 & a_1a_2 + b_1b_2 \end{pmatrix}.$$

Значит, у матриц $A_2^{(1,i)} A_2^{(i,1)}$ на диагонали стоят равные элементы. Так как сумма всех матриц $A_2^{(1,i)} A_2^{(i,1)}$ имеет нули вне главной диагонали, то и сами матрицы $E_i = A_2^{(1,i)} A_2^{(i,1)}$ диагональны, а следовательно, и скалярны. Значит, они являются центральными идемпотентами кольца матриц размера 2×2. Таким образом, $\{E_i\}$ — это система попарно ортогональных идемпотентов, дающих в сумме 1, т. е.

$$\mathrm{M}_2(R) = E_1\mathrm{M}_2(R) \oplus E_2\mathrm{M}_2(R) \oplus \dots \oplus E_{n/2}\mathrm{M}_2(R).$$

Разложим матрицу A_2 в сумму $E_1A_2 + \dots + E_{n/2}A_2$.

Сопряжём матрицу A_2 матрицей $B = E_1B + \dots + E_nB = B_1 + \dots + B_n$, где $B_1 = E_1 \cdot I$, $B_i = E_i \cdot S_{(3,2i-1)(4,2i)}$. Тогда

$$A_2' = B^{-1}A_2B = E_1A_2' + \dots + E_nA_2' = A_2^{(1)'} + \dots + A_2^{(n)'},$$

где

$$A_2^{(1)'} = \begin{pmatrix} A_2^{(1,1)} & 0 & \dots & 0 \\ 0 & \alpha_{11}^{(1)} & \dots & \alpha_{1,n-1}^{(1)} \\ 0 & \vdots & \ddots & \vdots \\ 0 & \alpha_{n-1,1}^{(1)} & \dots & \alpha_{n-1,n-1}^{(1)} \end{pmatrix},$$

$$A_2^{(i)'} = \begin{pmatrix} 0 & A_{1i} & 0 & \dots & 0 \\ A_{i1} & 0 & 0 & \dots & 0 \\ 0 & 0 & \alpha_{11}^{(i)} & \dots & \alpha_{1,n-2}^{(i)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \alpha_{n-2,1}^{(i)} & \dots & \alpha_{n-2,n-2}^{(i)} \end{pmatrix}, \quad i > 1.$$

Обозначим матрицу

$$\begin{pmatrix} \alpha_{11} & \dots & \alpha_{1,n-2} \\ \vdots & \ddots & \vdots \\ \alpha_{n-2,1} & \dots & \alpha_{n-2,n-2} \end{pmatrix},$$

а в случае $i = 1$ матрицу

$$\begin{pmatrix} \alpha_{11} & \dots & \alpha_{1,n-1} \\ \vdots & \ddots & \vdots \\ \alpha_{n-1,1} & \dots & \alpha_{n-1,n-1} \end{pmatrix},$$

через Λ_i. Заметим, что Λ_i — матрица над кольцом $E_i\mathrm{M}_2(R)$ размера меньше $n/2$, такая что $\Lambda_i^2 = I$. Значит, можно повторить предыдущие рассуждения для матрицы Λ_i и соответствующей системы ортогональных идемпотентов кольца $E_i\mathrm{M}_2(R)$. В результате мы получим матрицу $\tilde{A}_2$, сопряжённую исходной матрице A_2 и состоящую из диагональных блоков размера 4×4 и 2×2. Таким образом, каждый элемент порядка два в группе $\Gamma_n(R)$, коммутирующий с S_{σ_1}, в некотором базисе, в котором S_{σ_1} не меняется, состоит из диагональных блоков размера 4×4 и 2×2 (понятно, что если вернуться к случаю матрицы нечётного размера, то может ещё возникнуть один блок размера 1×1).

Рассмотрим теперь множество

$$\begin{aligned} \mathcal{F}_1 = \bigl\{ & D \in D_n(R) \mid DS_{\sigma_1} = S_{\sigma_1}D \ \wedge \ \forall\, J \in \Gamma_n(R) \\ & \bigl(J^2 = I \wedge JS_{\sigma_1} = S_{\sigma_1}J \Longrightarrow \exists\, C \in \Gamma_n(R)\ (D(CJC^{-1}) = CJC^{-1}D)\bigr)\bigr\}. \end{aligned}$$

Это множество должно состоять из диагональных матриц, у которых на диагонали стоят попарно равные элементы и которые в некотором базисе коммутируют со всеми матрицами порядка 2, представимыми в виде блоков размера 4×4 и 2×2. Значит, любой элемент D этого множества в некотором базисе имеет вид

$$\begin{array}{ll} \mathrm{diag}[\alpha_1 I_2, \alpha_1 I_2, \alpha_2 I_2, \alpha_2 I_2, \dots, \alpha_k I_2, \alpha_k I_2, I_2], & \text{если } n/2 = 2k+1, \\ \mathrm{diag}[\alpha_1 I_2, \alpha_1 I_2, \dots, \alpha_k I_2, \alpha_k I_2], & \text{если } n/2 = 2k \end{array} \qquad (*)$$

(если размерность полугруппы нечётна, то добавляется ещё один диагональный элемент в конце), причём соответствующая замена базиса не меняет S_{σ_1}, D коммутирует с S_{σ_1} и в некотором базисе — с матрицей S_{σ_2}.

Далее рассмотрим множество

$$\Lambda_1 = \bigl\{ D \in \mathcal{F}_1 \mid \forall\, D' \in \mathcal{F}_1 \ \bigl(C_{\Gamma_n(R)}(D) \not\supset C_{\Gamma_n(R)}(D')\bigr)\bigr\}.$$

Любая матрица из $\mathcal{F}_1$ коммутирует (в том базисе, в котором она имеет вид $(*)$) со всеми матрицами, которые в этом базисе разбиты на диагональные блоки размера 4×4 (и, возможно, 2×2 в конце, и ещё, возможно, 1×1

в самом конце). Значит, Λ_1 содержит матрицы, централизатор которых состоит только из таких матриц. С другой стороны, в любом базисе такие матрицы существуют, например, это матрицы вида $\mathrm{diag}[1,1,1,1,2,2,2,2,\dots,k,k,k,k,\dots]$.

Рассмотрим инволюцию K — образ матрицы S_{σ_2}. Это матрица, коммутирующая с S_{σ_1} и с некоторой матрицей $C\in\Lambda_1$. Кроме того, если она коммутирует с некоторой диагональной матрицей C', то $C_{\Gamma_n(R)}(C)\subset C_{\Gamma_n(R)}(C')$. Так как $K\in C_{\Gamma_n(R)}(C)$ и $C\in\Lambda_1$, то J состоит из диагональных блоков 4×4 (и, возможно, одного блока 2×2, и ещё, возможно, одного блока 1×1).

Рассмотрим один из этих блоков (размера 4×4)

$$\tilde{K}_i=\begin{pmatrix} A & B\\ C & D\end{pmatrix},\quad A,B,C,D\in\mathrm{M}_2(R).$$

Так как $\tilde{K}_i$ — инволюция, коммутирующая с ограничением S_{σ_1} на данную часть базиса, то $E_1=A^2$ и $E_2=BC$ — это центральные ортогональные идемпотенты кольца $\mathrm{M}_2(R)$, в сумме дающие I_2. Мы знаем, что

$$\tilde{K}_i\cdot\mathrm{diag}[\alpha,\alpha,\beta,\beta]\neq\mathrm{diag}[\alpha,\alpha,\beta,\beta]\cdot\tilde{K}_i$$

ни для каких обратимых $\alpha\neq\beta$ (по выбору матрицы K). Возьмём $\alpha I_2=A^2+BC$ и $\beta I_2=A^2/2+BC$. Тогда α и β обратимы и

$$\tilde{K}_i\cdot\mathrm{diag}[\alpha,\alpha,\beta,\beta]=\mathrm{diag}[\alpha,\alpha,\beta,\beta]\cdot\tilde{K}_i.$$

Значит, $\alpha=\beta$, т. е. $A^2=0$. Следовательно, $BC=1$. Так как $ABC=0$, то $A=0$. Аналогично $D=0$. Таким образом, K (в зависимости от размерности) может иметь один из четырёх видов:

$$\begin{pmatrix} 0 & B_1 & \dots & 0 & 0\\ B_1^{-1} & 0 & \dots & 0 & 0\\ \vdots & \vdots & \ddots & \vdots & \vdots\\ 0 & 0 & \dots & 0 & B_k\\ 0 & 0 & \dots & B_k^{-1} & 0\end{pmatrix},\qquad \begin{pmatrix} 0 & B_1 & \dots & 0 & 0 & 0\\ B_1^{-1} & 0 & \dots & 0 & 0 & 0\\ \vdots & \vdots & \ddots & \vdots & \vdots & 0\\ 0 & 0 & \dots & 0 & B_k & 0\\ 0 & 0 & \dots & B_k^{-1} & 0 & 0\\ 0 & 0 & \dots & 0 & 0 & b_{k+1}\end{pmatrix},$$

$$\begin{pmatrix} 0 & B_1 & \dots & 0 & 0 & 0 & 0\\ B_1^{-1} & 0 & \dots & 0 & 0 & 0 & 0\\ \vdots & \vdots & \ddots & \vdots & \vdots & 0 & 0\\ 0 & 0 & \dots & 0 & B_k & 0 & 0\\ 0 & 0 & \dots & B_k^{-1} & 0 & 0 & 0\\ 0 & 0 & \dots & 0 & 0 & 0 & b_{k+1}\\ 0 & 0 & \dots & 0 & 0 & b_{k+1}^{-1} & 0\end{pmatrix},$$

$$\begin{pmatrix}
0 & B_1 & \dots & 0 & 0 & 0 & 0 & 0\\
B_1^{-1} & 0 & \dots & 0 & 0 & 0 & 0 & 0\\
\vdots & \vdots & \ddots & \vdots & \vdots & 0 & 0 & 0\\
0 & 0 & \dots & 0 & B_k & 0 & 0 & 0\\
0 & 0 & \dots & B_k^{-1} & 0 & 0 & 0 & 0\\
0 & 0 & \dots & 0 & 0 & 0 & b_{k+1} & 0\\
0 & 0 & \dots & 0 & 0 & b_{k+1}^{-1} & 0 & 0\\
0 & 0 & \dots & 0 & 0 & 0 & 0 & b_{k+2}
\end{pmatrix}.$$

После сопряжения матрицы K с помощью блочно-диагональной матрицы, которая имеет вид

$$\operatorname{diag}[B_1, I_2, B_2, I_2, \dots, B_k, I_2]$$

в первом случае,

$$\operatorname{diag}[B_1, b_{k+1}I_2, B_2, b_{k+1}I_2, \dots, B_k, b_{k+1}I_2, 1]$$

во втором случае,

$$\operatorname{diag}[B_1, I_2, B_2, I_2, \dots, B_k, I_2, b_{k+1}, 1]$$

в третьем случае,

$$\operatorname{diag}[B_1, b_{k+2}I_2, B_2, b_{k+2}I_2, \dots, B_k, b_{k+2}I_2, b_{k+1}, b_{k+2}, 1]$$

в четвёртом случае, мы получим матрицу $K' = S_{\sigma_2}$ или $b_{k+1}S_{\sigma_2}$, $b_{k+2}S_{\sigma_2}$, при этом матрица S_{σ_1} не изменится. Таким образом, мы нашли матрицу $M_2 \in \Gamma_n(R)$, такую что $M\Phi(S_{\sigma_i})M_2^{-1} = b_iS_{\sigma_i}$, $i = 1, 2$. Продолжая данную процедуру далее (а именно рассматривая матрицы размера $n \times n$ как матрицы $n/4 \times n/4$ над кольцом матриц 4×4 и подстановку σ_3 и т. д.), дойдём до искомой замены базиса. □

Определение 11. Назовём диагональную матрицу $D \in \Gamma_n(R)$ *блочно-скалярной инволюцией*, если $D^2 = I$ и матрица D является скалярной в каждом блоке $\mathbf{D}_i$, $i = 1, \dots, l$. Множество (группу) всех блочно-скалярных инволюций будем обозначать через $\mathcal{Q}$.

Лемма 8. *Пусть автоморфизм Φ полугруппы $G_n(R)$ таков, что $\Phi(S_{\sigma_i}) = a_iS_{\sigma_i}$, $a_i^2 = 1$, $i = 1, \dots, k_1$. Тогда каждая матрица $S_{\sigma_i^{(j)}}$ под действием Φ переходит в $D \cdot S_{\sigma_i^{(j)}}$, где $D \in \mathcal{Q}$.*

Доказательство. Будем доказывать это утверждение по индукции по размеру блока с номером j.

База индукции. Для блока $\mathbf{D}_l$ размера 1×1 доказывать нечего, поэтому начнём с блока размера 2×2 (если он существует).

Пусть блок размера 2×2 находится на месте $(p, p+1)$. Рассмотрим матрицу $S_{\sigma_1^{(l)}} = S_{(p,p+1)}$. Она удовлетворяет следующим свойствам:

1) $S_{(p,p+1)}$ коммутирует со всеми σ_i, $i = 1, \dots, k_1$;

2) $S^2_{(p,p+1)} = I$;
3) если некоторая диагональная матрица D коммутирует с какой-то матрицей S_{σ_i}, то D коммутирует и с $S_{(p,p+1)}$;
4) если диагональная матрица коммутирует с $S_{(p,p+1)}$, то она коммутирует и с любой другой матрицей, удовлетворяющей свойствам 1)—3).

Так как любая матрица, которая скалярна в каждом блоке $\mathbf{D}_i$, коммутирует с S_{σ_i}, $i = 1, \ldots, k_1$, то образ $A_{(p,p+1)} = \Phi\big(S_{(p,p+1)}\big)$ должен коммутировать, например, с матрицей $\mathrm{diag}[I_{2^{k_1}}, 2 \cdot I_{2^{k_2}}, \ldots, l \cdot I_{2^{k_l}}]$, поэтому матрица $A_{(p,p+1)}$ также разбивается на блоки $\mathbf{D}_1, \ldots, \mathbf{D}_l$. Рассмотрим у матрицы $A_{(p,p+1)}$ блок $\mathbf{D}_i$ размера, большего 2×2. В этом блоке есть ровно k_i различных $S_{\sigma^{(i)}_m}$. Рассмотрим набор диагональных матриц $H_1, \ldots, H_{k_i}$, единичных во всех блоках, кроме $\mathbf{D}_i$, а в блоке $\mathbf{D}_i$

$$\begin{aligned}
H_1 &= \mathrm{diag}[1, 1, 2, 2, 3, 3, \ldots, 2^{k_i-1}, 2^{k_i-1}],\\
H_2 &= \mathrm{diag}[1, 2, 1, 2, 3, 4, 3, 4, \ldots, 2^{k_i-1} - 1, 2^{k_i-1}, 2^{k_i-1} - 1, 2^{k_i-1}],\\
H_3 &= \mathrm{diag}[1, 2, 3, 4, 1, 2, 3, 4, \ldots],\\
&\ldots\\
H_{k_i} &= \mathrm{diag}[1, 2, \ldots, 2^{k_i-1}, 1, 2, 3, \ldots, 2^{k_i-1}].
\end{aligned}$$

Каждая матрица H_j коммутирует с соответствующей матрицей S_{σ_j}, поэтому по условию 3) матрица $A_{(p,p+1)}$ должна коммутировать со всеми H_j, $j = 1, \ldots, k_i$. Значит, $A_{(p,p+1)}$ в блоке $\mathbf{D}_i$ диагональна. Из условия 1) следует, что матрица $A_{(p,p+1)}$ в блоке $\mathbf{D}_i$ скалярна (так как она имеет порядок 2, то соответствующий скаляр является инволюцией). Теперь посмотрим на последний блок (имеющий размер 2×2). Пусть в этом блоке матрица $A_{(p,p+1)}$ имеет вид

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

Так как $A_{(p,p+1)}$ коммутирует с S_{σ_1}, то $a = d$, $b = c$. Так как $A_{(p,p+1)}$ имеет порядок 2, то $a^2 + b^2 = 1$, $ab = 0$.

Воспользуемся теперь условием 4). Рассмотрим диагональную матрицу H, единичную во всех блоках $\mathbf{D}_i$, кроме рассматриваемого, а в рассматриваемом блоке размера 2×2 имеющую вид $\mathrm{diag}[1, a^2/2 + b^2]$. Тогда

$$\begin{pmatrix} 1 \cdot a & 1 \cdot b\\ (a^2/2 + b^2) \cdot b & (a^2/2 + b^2) \cdot a \end{pmatrix} = \begin{pmatrix} 1 \cdot a & (a^2/2 + b^2) \cdot b\\ 1 \cdot b & (a^2/2 + b^2) \cdot a \end{pmatrix},$$

так как $ab = 0$, т. е. H и $A_{(p,p+1)}$ коммутируют. Значит, матрица H должна коммутировать с любой другой матрицей, удовлетворяющей условиям 1)—3), в том числе с $S_{(p,p+1)}$. А это означает, что $a^2/2 + b^2 = 1$, т. е. $a^2 = 0$. Следовательно, $a = 0$ (так как из $a^2 + b^2 = 1$ и $ab = 0$ следует $a^3 = a$). Таким образом, обязательно $A_{(p,p+1)} = DS_{(p,p+1)}$, где $D \in \mathcal{Q}$.

Шаг индукции. Теперь мы можем сделать предположение индукции о том, что матрица каждой подстановки $\sigma^{(j)}_m$, $j > i$, $m = 1, \ldots, k_{i+1}$, переходит при автоморфизме в себя, умноженную на некоторую матрицу из $\mathcal{Q}$. Принимая это предположение, рассмотрим теперь матрицы подстановок $\sigma_m^{(i)}$, $m = 1, \ldots, k_i$. Образы всех таких матриц коммутируют со всеми диагональными матрицами, одновременно коммутирующими со всеми матрицами $S_{\sigma_1}, \ldots, S_{\sigma_{k_1}}$, а значит, и с матрицей $\mathrm{diag}[I_{2^{k_1}}, 2 \cdot I_{2^{k_2}}, \ldots, l \cdot I_{2^{k_l}}]$, поэтому все эти образы также разбиваются на блоки $\mathbf{D}_1, \ldots, \mathbf{D}_l$.

Пусть $A_{\sigma_1^{(i)}} = \Phi\big(S_{\sigma_1^{(i)}}\big)$. Из того, что $A_{\sigma_1^{(i)}}$ коммутирует со всеми диагональными матрицами, коммутирующими с S_{σ_1}, следует, что A_σ разбивается на диагональные блоки размера 2×2. Теперь мы можем сказать, что матрица A_σ коммутирует с любой диагональной матрицей, коммутирующей с матрицей подстановки $\sigma_1^{(1)} \cdot \ldots \cdot \sigma_1^{(i)} = \sigma_1 \cdot \sigma_1^{(i+1)} \cdots \sigma_1^{(l)}$. Такие диагональные матрицы могут иметь любые произвольные элементы на диагонали начиная с блока $\mathbf{D}_{i+1}$, поэтому матрица $A_{\sigma_1^{(i)}}$ на блоках $\mathbf{D}_{i+1}, \ldots, \mathbf{D}_l$ диагональна. Благодаря тому что она коммутирует со всеми матрицами $S_{\sigma_m^{(j)}}$, $j > i$, получаем, что в каждом блоке $\mathbf{D}_j$, $j > i$, матрица $A_{\sigma_1^{(i)}}$ скалярна.

Матрица $A_{\sigma_1^{(i)}}$ коммутирует со всеми $S_{\sigma_1}, \ldots, S_{\sigma_{k_1}}$, поэтому внутри каждого $\mathbf{D}_j$ все блоки 2×2 одинаковые.

Теперь рассмотрим блок $\mathbf{D}_j$, $j < i$. Матрицы $S_{\sigma_i}, S_{\sigma_{i+1}}, \ldots, S_{\sigma_{k_1}}$ совпадают на блоке $\mathbf{D}_i$, поэтому все их попарные произведения тождественны на $\mathbf{D}_i$. Значит, матрица $A_{\sigma_1^{(i)}}$ коммутирует со всеми диагональными матрицами, коммутирующими с одной из матриц $S_{\sigma_1}S_{\sigma_i}S_{\sigma_{i+1}}, S_{\sigma_1}S_{\sigma_i}S_{\sigma_{i+2}}, \ldots, S_{\sigma_1}S_{\sigma_i}S_{\sigma_{k_1}}$. Например, мы можем взять матрицу $\mathrm{diag}[1, 2, 1, 2, \ldots, 2, 1, 2, 1]$ на $\mathbf{D}_j$, она должна будет коммутировать с матрицей $A_{\sigma_1^{(i)}}$, откуда получаем, что на блоке $\mathbf{D}_j$ наша $A_{\sigma_1^{(i)}}$ диагональна, а следовательно, скалярна.

Осталось рассмотреть матрицу $A_{\sigma_1^{(i)}}$ на блоке $\mathbf{D}_i$. Благодаря тому что $A_{\sigma_1^{(i)}}$ коммутирует со всеми S_{σ_i}, $i = 1, \ldots, k_1$, мы знаем, что $A_{\sigma_1^{(i)}}$ на $\mathbf{D}_i$ состоит из одинаковых диагональных блоков размера 2×2 вида

$$\begin{pmatrix} a & b \\ b & a \end{pmatrix}$$

и, кроме того (так как $A_{\sigma_1^{(i)}}$ имеет порядок 2), $a^2 + b^2 = 1$, $ab = 0$. Теперь заметим, что матрица $S_{\sigma_1^{(i)}}$ такова, что если диагональная матрица с ней коммутирует, то она коммутирует и с любой другой матрицей, удовлетворяющей всем перечисленным выше свойствам. Значит, такова же и матрица $A_{\sigma_1^{(i)}}$. Следовательно, как и выше (в базе индукции), заключаем, что в каждом блоке $a = 0$. Следовательно, на блоке $\mathbf{D}_i$ имеем $A_{\sigma_1^{(i)}} = bS_{\sigma_1^{(i)}}$, $b^2 = 1$, что и требовалось.

Доказательство для $S_{\sigma_m^{(i)}}$, $m = 2, 3, \ldots$, совершенно аналогично, надо лишь использовать дополнительно доказанное условие $A_{\sigma_1^{(i)}} = DS_{\sigma_1^{(i)}}$. $\square$

Определение 12. Через $\tau(i, p, m)$, $i = 1, \ldots, l$, $p = 1, \ldots, k_i$, $m = p, \ldots, k_i$, обозначим подстановку, которая на всех блоках, кроме $\mathbf{D}_i$, тождественна, а на блоке $\mathbf{D}_i$ на первых 2^m элементах базиса совпадает с σ_p, а на остальных элементах базисах тождественна. Таким образом, $\tau(i,1,1)$ — это просто транспозиция, $\tau(i,p,k_i)=\sigma_p^{(i)}$.

Лемма 9. *Пусть автоморфизм Φ полугруппы $G_n(R)$ таков, что $\Phi(S_{\sigma_i}) = a_i S_{\sigma_i}$, $a_i^2=1$, $i=1,\dots,k_1$. Тогда существует такая матрица $M\in\Gamma_n(R)$, что каждая матрица $S_{\tau(i,1,m)}$, $i=1,\dots,l$, $m=1,\dots,k_i$, под действием $\Phi_M\circ\Phi$ переходит в $D\cdot S_{\tau(i,1,m)}$, где $D\in\mathcal{Q}$. При этом если подстановка $\tau(i,1,m)$ чётна, то $D=E$.*

Доказательство. Фиксируем какой-то конкретный блок $\mathbf{D}_i$ и будем доказывать утверждение для всех $\tau(i,1,m)$, $m=1,\dots,k_i$, по индукции от k_i до 1. Заметим, что для k_i всё уже доказано. Произведём переход от k_i к k_i-1.

Сразу заметим, что любая из матриц $S_{\tau(i,p,m)}$ коммутирует с каждой диагональной матрицей, с которой коммутирует $S_{\tau(i,p,k_i)}$. Это сразу даёт нам, что для каждого $m=p,\dots,k_i$ образ $A_{\tau(i,p,m)}=\Phi\bigl(S_{\tau(i,p,m)}\bigr)$ диагонален во всех блоках, кроме $\mathbf{D}_i$, а так как все $S_{\tau(i,p,m)}$ коммутируют со всеми $S_{\sigma_q^{(p)}}$, $q\neq i$, сразу получаем, что этот образ во всех блоках скалярен. Значит, нам осталось рассмотреть только блок $\mathbf{D}_i$. В этом блоке будем использовать индукцию.

Матрица $A_{\tau(i,1,k_i-1)}$ коммутирует со всеми S_{σ_q}, $q=1,\dots,k_i-1$, откуда сразу следует, что на $\mathbf{D}_i$ матрица $A_{\tau(i,1,k_i-1)}$ состоит из диагональных блоков размера 2×2, при этом первая половина блоков совпадает друг с другом и вторая половина тоже. Пусть каждый блок в первой половине равен

$$\begin{pmatrix} a & b\\ b & a\end{pmatrix},$$

каждый блок во второй половине равен

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

Теперь воспользуемся соотношением

$$S_{\tau(i,1,k_i-1)}S_{\sigma_{k_i}}S_{\tau(i,1,k_i-1)}S_{\sigma_{k_i}}=S_{\tau(i,1,k_i)}.$$

Оно даёт

$$\begin{pmatrix} a & b\\ b & a\end{pmatrix}\begin{pmatrix} c & d\\ d & c\end{pmatrix}=\begin{pmatrix} 0 & \alpha\\ \alpha & 0\end{pmatrix},$$

откуда $ac=bd=0$, $ad+bc=\alpha$. Заменим базис с помощью матрицы $b^2E+a^2S_{\tau(i,k_i,k_i)}$ (такая замена базиса коммутирует со всеми введёнными нами матрицами), придём к матрице $A_{\tau(i,1,k_i-1)}$, у которой в первой половине блока $\mathbf{D}_i$ стоят матрицы

$$\begin{pmatrix} 0 & \alpha\\ \alpha & 0\end{pmatrix},\quad \alpha^2=1,$$

а во второй половине — матрицы βI_2, $\beta^2=1$. Произведём замену базиса (только в блоке $\mathbf{D}_i$) с помощью диагональной матрицы $\mathrm{diag}[\alpha/\beta,1,\alpha/\beta,1\dots,\alpha/\beta,1]$.

Такая замена не изменит $A_{\sigma_q^{(i)}}$, $q > 1$, при этом рассматриваемая матрица $A_{\tau(i,1,k_i-1)}$ примет искомый вид.

Снова из соотношения

$$A_{\tau(i,1,k_i-1)}A_{\sigma_{k_i}^{(i)}}A_{\tau(i,1,k_i-1)}A_{\sigma_{k_i}^{(i)}} = A_{\tau(i,1,k_i)}$$

получаем, что $A_{\tau(i,1,k_i)} = S_{\tau(i,1,k_i)}$.

Если $k_i - 1 = 1$, то дальше рассматривать нечего. Поэтому пусть k_i было больше двух. Проведём ещё один шаг индукции (остальные шаги проводятся совершенно аналогично).

Для начала покажем, что если в блоке $\mathbf{D}_i$ $A_{\tau(i,1,k_i-1)} = \alpha S_{\tau(i,1,k_i-1)}$, то обязательно $\alpha = 1$.

Заметим, что существуют матрица B (на самом деле это, например, матрица транспозиции $(1,3)$), которая коммутирует со всеми диагональными матрицами, коммутирующими с S_{σ_2}, и матрица C (например, $S_{(1,4)}$), которая коммутирует со всеми диагональными матрицами, коммутирующими с $S_{\sigma_1}S_{\sigma_2}$, такие что

$$B \cdot S_{\tau(i,1,k_i-1)} \cdot B^{-1} \cdot S_{\tau(i,1,k_i-1)} = C \cdot S_{\tau(i,1,k_i-1)} \cdot C^{-1}.$$

Естественно, это условие должно сохраниться при автоморфизме. Так как матрица $\Phi(B)$ коммутирует со всеми диагональными матрицами, коммутирующими с S_{σ_2}, то она независимо действует в первой и второй половинах блока $\mathbf{D}_i$. То же самое можно сказать и о матрице $\Phi(C)$. Так как на второй половине блока $\mathbf{D}_i$ матрица $A_{\tau(i,1,k_i-1)}$ скалярна (имеет вид αI), то при сопряжении она не изменит вид. Значит, $\alpha^2 = \alpha$, откуда $\alpha = 1$. Таким образом, $A_{\tau(i,1,k_i-1)} = S_{\tau(i,1,k_i-1)}$.

Теперь рассмотрим матрицу $A_{\tau(i,1,k_i-2)} = \Phi\big(S_{\tau(i,1,k_i-2)}\big)$. Мы уже знаем, что эта матрица скалярна в блоках $\mathbf{D}_j$, $j \neq i$. Так как она коммутирует со всеми диагональными матрицами, с которыми коммутирует $A_{\tau(i,1,k_i-1)}$, то она диагональна и на второй половине блока $\mathbf{D}_i$. Будем обозначать первую половину блока $\mathbf{D}_i$ через $\mathbf{D}_i'$, вторую — через $\mathbf{D}_i''$.

Матрица $A_{\tau(i,1,k_i-2)}$ коммутирует со всеми S_{σ_q}, $q = 1, \ldots, k_i - 2$, поэтому

1) на $\mathbf{D}_i'$ она состоит из диагональных блоков размера 2×2, из которых первая половина блоков совпадает друг другом и вторая половина блоков совпадает друг с другом;
2) на $\mathbf{D}_i''$ она имеет вид $\mathrm{diag}[aI_{2^{k_i-2}}, bI_{2^{k_i-2}}]$, $a^2 = b^2 = 1$.

Пусть на $\mathbf{D}_i$ $A_{\tau(i,1,k_i-1)} = \alpha S_{\tau(i,1,k_i-1)}$.

Рассмотрим соотношение

$$A_{\tau(i,1,k_i-2)}A_{\sigma_{k_i-1}^{(i)}}A_{\tau(i,1,k_i-2)}A_{\sigma_{k_i-1}^{(i)}} = S_{\tau(i,1,k_i-1)}.$$

Проведём рассуждения, аналогичные предыдущему шагу, и проведём замену базиса с помощью подходящей матрицы $b'^2E + a'^2S_{\tau(i,k_i-1,k_i-1)}$. Такая замена не изменит $A_{\sigma_q^{(i)}}$, $q > 1$, при этом рассматриваемая матрица $A_{\tau(i,1,k_i-2)}$ примет искомый вид.

Продолжая эту процедуру для $k_i - 3, \ldots, 1$, мы придём к базису, в котором все $A_{\tau(i,1,q)}$, $q > 1$, совпадают с $S_{\tau(i,1,q)}$, а $A_{\tau(i,1,1)}$ отличается от $S_{\tau(i,1,1)}$ на множитель из $\mathcal{Q}$.

Заметим, что мы доказали и последнее утверждение леммы, так как нечётными являются ровно подстановки $S_{\tau(i,1,1)}$. □

Лемма 10. *Пусть автоморфизм Φ полугруппы $G_n(R)$ таков, что каждая матрица $S_{\tau(i,1,m)}$, $i = 1, \ldots, l$, $m = 1, \ldots, k_i$, под действием Φ переходит в $D \cdot S_{\tau(i,1,m)}$, где $D \in \mathcal{Q}$ и если подстановка $\tau(i,p,m)$ чётна, то $D = I$. Тогда найдётся такая матрица $M \in \Gamma_n(R)$, что любая матрица подстановки τ, действующей независимо в блоках $\mathbf{D}_1, \ldots, \mathbf{D}_l$, переходит под действием автоморфизма $\Phi_M \circ \Phi$ в матрицу DS_τ, причём если подстановка τ чётна, то $D = I$.*

Доказательство. Будем рассматривать матрицы подстановок, тождественно действующих во всех блоках, кроме некоторого фиксированного блока $\mathbf{D}_i$. Их образы коммутируют со всеми диагональными матрицами, коммутирующими одновременно с образами $S_{\sigma_1^{(i)}}, \ldots, S_{\sigma_{k_i}^{(i)}}$, а также с образами всех $S_{\sigma_j^{(p)}}$, $p \neq i$. Следовательно, во всех блоках $\mathbf{D}_p$, $p \neq i$, образы таких матриц скалярны. Сосредоточимся на блоке $\mathbf{D}_i$.

Заметим, что если размер блока $\mathbf{D}_i$ не превосходит двух, то всё уже доказано. Поэтому мы можем считать, что этот размер не меньше 4×4. Для удобства будем считать, что элементы базиса в блоке $\mathbf{D}_i$ нумеруются с единицы (т. е. это самый первый блок).

По условию всё уже доказано для матрицы транспозиции $(1,2)$, т. е. $\Phi\big(S_{(1,2)}\big) = \alpha S_{(1,2)}$, $\alpha^2 = 1$. Так как транспозиции $(3,4), (5,6), \ldots, (2^{k_i} - 1, 2^{k_i})$ сопряжены к транспозиции $(1,2)$ с помощью подстановок $\sigma_2, \sigma_3, \ldots, \sigma_{k_i}$ и различных их произведений, то $\Phi\big(S_{(2p-1,2p)}\big) = \alpha S_{(2p-1,22)}$ для всех $p = 2, \ldots, 2^{k_i - 1}$.

Рассмотрим матрицу $A_{(1,3)}$ — образ матрицы транспозиции $(1,3)$. Из того что она коммутирует со всеми диагональными матрицами, с которыми коммутирует S_{σ_2}, а также с самой S_{σ_2}, следует, что она разбивается на диагональные блоки размера 4×4 вида

$$\begin{pmatrix} a & 0 & b & 0 \\ 0 & c & 0 & d \\ b & 0 & a & 0 \\ 0 & d & 0 & c \end{pmatrix}, \quad a^2 + b^2 = c^2 + d^2 = 1, \quad ab = cd = 0.$$

Из того что матрица $A_{(1,2)}A_{(1,3)}$ имеет порядок три, сразу следует, что все блоки, кроме самого первого, — это скалярные матрицы с коэффициентом α. Рассмотрим первый блок. Из того же самого условия получаем $ac = bd = 0$, $a = d$, $b = c$. Сделаем новую замену базиса с помощью матрицы $b^2 I + a^2 S_{\sigma_1^{(i)}}$. Такая замена не изменит ни одну из рассмотренных ранее матриц, а нашу матрицу приведёт к виду $\alpha S_{(1,3)}$. Понятно, что все остальные матрицы порождающих транспозиций можно получить сопряжением с помощью уже полученных выше матриц. □

Лемма 11. *Пусть $n > 4$, Φ — автоморфизм полугруппы $G_n(R)$. Тогда существуют матрица $M \in \Gamma_n(R)$ и инволюция $a \in R_+^*$, такие что*

$$\Phi_1(S_\sigma) = \Phi_M \circ \Phi(S_\sigma) = S_\sigma$$

для любой чётной подстановки σ и

$$\Phi_1(S_\sigma) = \Phi_M \circ \Phi(S_\sigma) = aS_\sigma$$

для любой нечётной подстановки σ.

Доказательство. Благодаря предыдущим леммам мы можем считать, что $\Phi\bigl(S_{(p,p+1)}\bigr) = D_p S_{(p,p+1)}$, $D_p \in \mathcal{Q}$, для всех транспозиций $(p, p+1)$, меняющих элементы внутри одного блока $\mathbf{D}_i$, $i = 1, \ldots, l$. Так как произведение любых двух транспозиций чётно, а матрица чётной подстановки переходит сама в себя, то все матрицы D_p совпадают. Так как все транспозиции сопряжены, то соответствующие матрицы должны иметь одинаковый след. Если $D_p = D = \mathrm{diag}[\alpha_1 I_{2^{k_1}}, \ldots, \alpha_l I_{2^{k_l}}]$, рассмотрим два различных блока $\mathbf{D}_i$ и $\mathbf{D}_j$ неединичных размеров. Рассмотрим транспозиции τ_i и τ_j, произвольные в соответствующих блоках. След матрицы A_{τ_i} равен $\alpha_1 2^{k_1} + \ldots + \alpha_l 2^{k_l} - 2\alpha_i$, а след матрицы A_{τ_j} — $\alpha_1 2^{k_1} + \ldots + \alpha_l 2^{k_l} - 2\alpha_j$. Таким образом, $\alpha_i = \alpha_j$ всегда, кроме, может быть, блока 1×1.

Пусть n нечётно (тогда в разложении есть блок 1×1). Рассмотрим $A_{(n-1,n)} = \Phi\bigl(S_{(n-1,n)}\bigr)$. Здесь следует рассмотреть два случая: когда есть блок размера 2×2 и когда его нет.

1. Пусть имеется блок размера 2×2. Тогда он расположен прямо перед блоком размера 1×1.

Матрица $A_{(n-1,n)}$ коммутирует со всеми транспозициями из блоков $\mathbf{D}_1, \ldots, \mathbf{D}_{l-2}$ и при этом имеет порядок 2. Посмотрим, например, что это означает для транспозиции $S_{(1,2)}$ (по нашему предположению $n > 4$, т. е. для нашего случая $n > 6$, поэтому транспозиция $(1,2)$ не пересекается с транспозицией $(n-2, n-1)$).

Если

$$A_{(n-1,n)} = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \ldots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \ldots & a_{2n} \\ a_{31} & a_{32} & a_{33} & \ldots & a_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & a_{n3} & \ldots & a_{nn} \end{pmatrix},$$

то из того что $A_{(n-1,n)}$ коммутирует с $S_{(1,2)}$, следует, что $a_{2i} = a_{1i}$, $a_{i2} = a_{i1}$, $i = 3, \ldots, n$, $a_{22} = a_{11}$, $a_{12} = a_{21}$. С другой стороны, матрица $A_{(n-1,n)}$ имеет порядок 2, поэтому

$$a_{11}^2 + a_{12}^2 + a_{13}a_{31} + \ldots + a_{1n}a_{n1} = 1$$

(умножение первого столбца на первую строку),

$$a_{11}a_{12} = a_{13}a_{31} = \ldots = a_{1n}a_{n1} = 0$$

(умножение второго столбца на первую строку). Кроме того, как обычно, для матриц второго порядка $a_{ik}a_{kj} = 0$ при $i \neq j$. Следовательно, $a_{11}^2 + a_{12}^2 = 1$, а так как

$$a_{1i}a_{11} = a_{i1}a_{11} = a_{1i}a_{12} = a_{i1}a_{12} = 0, \quad i = 3, \ldots, n,$$

то $a_{1i} = a_{i1} = 0$ для всех $i = 3, \ldots, n$.

Аналогичными рассуждениями для других транспозиций, коммутирующих с $A_{(n-1,n)}$, приходим к тому, что $A_{(n-1,n)}$ в каждом блоке $\mathbf{D}_i$, $i = 1, \ldots, l-2$, скалярна, а в конце её стоит блок размера 3×3. Понятно, что можно его рассматривать отдельно. Но тогда мы приходим ровно к ситуации леммы 4 и с помощью замены базиса (вида $\mathrm{diag}[1, 1, \ldots, 1, \gamma]\bigl(aE + bS_{(n-2,n-1)}\bigr)$, т. е. коммутирующей со всеми рассмотренными выше матрицами) можем прийти к ситуации $A_{(n-1,n)} = DS_{(n-1,n)}$, $D \in \mathcal{Q}$, D скалярна на объединении последних двух блоков. Из того что матрица $A_{(n-2,n-1)}A_{(n-1,n)}$ имеет порядок 3, получаем сразу, что $D = \alpha E$. Это нам и требовалось.

2. Пусть блока 2×2 нет. Этот случай даже проще предыдущего. Начальные рассуждения аналогичны предыдущим, благодаря им мы получаем, что $A_{(n-1,n)}$ в каждом блоке $\mathbf{D}_i$, $i = 1, \ldots, l-2$, скалярна. Теперь рассмотрим предпоследний блок, имеющий размер по крайней мере 4×4. Так как $A_{(n,n-1)}$ коммутирует со всеми матрицами транспозиций вида $(p, p+1)$ в этом блоке, кроме последней, мы получаем, что матрица $A_{(n-1,n)}$ скалярна на всех элементах блока, кроме последнего, т. е. матрица $A_{(n-1,n)}$ диагональна везде, кроме последнего блока размера 2×2. Далее легко заключаем, что она имеет вид $DS_{(n-1,n)}$ для некоторой диагональной матрицы D, а после замены базиса с помощью $\mathrm{diag}[1, 1, \ldots, 1, \gamma]$ приходим к $A_{(n-1,n)} = \alpha S_{(n-1,n)}$.

Совершенно аналогично мы можем получить транспозиции, стоящие на «стыках» других блоков. На каждом шаге (стыке между блоками $\mathbf{D}_i$ и $\mathbf{D}_{i+1}$) будет достаточно применять диагональные замены, единичные в блоках $\mathbf{D}_1, \ldots, \mathbf{D}_i$ и домножающие на некоторый скаляр γ в остальных блоках. Понятно, что такие замены коммутируют со всеми рассмотренными на предыдущих шагах транспозициями, что нам и требуется.

В результате мы получаем, что $A_{(p,p+1)} = \alpha S_{(p,p+1)}$ для всех $p = 1, \ldots, n-1$, что и требовалось. $\square$

3. Действие автоморфизма Φ' на диагональных матрицах

В предыдущем разделе по нашему автоморфизму Φ мы построили новый автоморфизм $\Phi' = \Phi_M\Phi$, такой что $\Phi'(S_\sigma) = \alpha^{\mathrm{sgn}\,\sigma}S_\sigma$, $\alpha^2 = 1$, для всех $\sigma \in \Sigma_n$. Мы предположим, что такой автоморфизм Φ' фиксирован.

Лемма 12. *Если $n \geqslant 3$, $1/2 \in R$, автоморфизм $\Phi' \in \mathrm{Aut}\big(G_n(R)\big)$ таков, что $\Phi'(S_\sigma) = \alpha^{\operatorname{sgn}\sigma} S_\sigma$, $\alpha^2 = 1$, для всех $\sigma \in \Sigma_n$, то для всех $\alpha, \beta \in R_+^*$ мы имеем*

$$\Phi'(\mathrm{diag}[\alpha, \beta, \ldots, \beta]) = \mathrm{diag}[\gamma, \delta, \ldots, \delta], \quad \gamma, \delta \in R_+^*.$$

Если $\alpha \neq \beta$, то $\gamma \neq \delta$.

Доказательство. По лемме 2

$$\Phi'(\mathrm{diag}[\alpha, \beta, \ldots, \beta]) = \mathrm{diag}[\gamma_1, \ldots, \gamma_n].$$

Рассмотрим подстановку $\sigma = (2, 3, \ldots, n)$. Так как $\Phi'(S_\sigma) = \alpha S_\sigma$, то $\Phi'\big(C_{D_n(R)}(S_\sigma)\big) = C_{D_n(R)}(S_\sigma)$. Таким образом, $\mathrm{diag}[\gamma_1, \ldots, \gamma_n]$ коммутирует с S_σ, а значит, $\gamma_2 = \gamma_3 = \ldots = \gamma_n$. Остаётся доказать, что $\gamma_1 \neq \gamma_2$. Это сразу же следует из того, что матрица $\mathrm{diag}[\alpha, \beta, \ldots, \beta]$ не коммутирует с $S_{(12)}$. $\square$

Лемма 13. *Если $n \geqslant 3$, $1/2 \in R$, автоморфизм $\Phi' \in \mathrm{Aut}\big(G_n(R)\big)$ таков, что $\Phi'(S_\sigma) = \alpha^{\operatorname{sgn}\sigma} S_\sigma$, $\alpha^2 = 1$, для всех $\sigma \in \Sigma_n$, то для всех $X \in G_2(R)$ имеет место равенство*

$$\Phi' \begin{pmatrix} X & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 \\ \ldots\ldots & & \ddots & \ldots \\ 0 & \ldots\ldots & & 1 \end{pmatrix} = \begin{pmatrix} Y & 0 & \ldots & 0 \\ 0 & a & \ldots & 0 \\ \ldots\ldots & & \ddots & \ldots \\ 0 & \ldots\ldots & & a \end{pmatrix}, \quad \text{где} \;\; Y \in G_2(R), \quad a \in R_+^*.$$

Доказательство. Обозначим

$$C = \begin{pmatrix} X & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 \\ \ldots\ldots & & \ddots & \ldots \\ 0 & \ldots\ldots & & 1 \end{pmatrix}.$$

Аналогично доказательству леммы 12 можно доказать, что для любой матрицы

$$A = \mathrm{diag}[\alpha, \alpha, \beta, \ldots, \beta] \in D_n(R), \quad \alpha \neq \beta,$$

имеет место равенство

$$\Phi'(A) = \mathrm{diag}[\gamma, \gamma, \delta, \ldots, \delta] \in D_n(R), \quad \gamma \neq \delta.$$

Заметим, что матрица C коммутирует с A и $S_{(3,4,\ldots,n)}$, а значит, $\Phi'(C)$ имеет искомый вид. $\square$

Лемма 14. *Если $n \geqslant 3$, $1/2 \in R$, автоморфизм $\Phi' \in \mathrm{Aut}\big(G_n(R)\big)$ таков, что $\Phi'(S_\sigma) = \alpha^{\operatorname{sgn}\sigma} S_\sigma$, $\alpha^2 = 1$, для всех $\sigma \in \Sigma_n$, то для любых $x_1, x_2 \in R_+^*$, таких что $x_1 \neq x_2$,*

$$\Phi'(A_1) = \Phi'(\mathrm{diag}[x_1, 1, \ldots, 1]) = \mathrm{diag}[\xi_1, \eta_1, \ldots, \eta_1],$$
$$\Phi'(A_2) = \Phi'(\mathrm{diag}[x_2, 1, \ldots, 1]) = \mathrm{diag}[\xi_2, \eta_2, \ldots, \eta_2],$$

имеем $\xi_1 \eta_1^{-1} \neq \xi_2 \eta_2^{-1}$.

Доказательство. Предположим, что для некоторых различных $x_1, x_2 \in R_+^*$ имеет место равенство $\xi_1\eta_1^{-1} = \xi_2\eta_2^{-1}$, т. е.

$$\Phi'(A_1) = \Phi'(\mathrm{diag}[x_1, 1, \ldots, 1]) = \mathrm{diag}[\xi, \eta, \ldots, \eta] = A_1',$$
$$\Phi'(A_2) = \Phi'(\mathrm{diag}[x_2, 1, \ldots, 1]) = \alpha \cdot \mathrm{diag}[\xi, \eta, \ldots, \eta] = A_2'.$$

Значит,

$$\Phi'^{-1}(\alpha I) = \Phi'^{-1}\big(A_1' A_2'^{-1}\big) = \mathrm{diag}[x_1 x_2^{-1}, 1, \ldots, 1] = \mathrm{diag}[\beta, 1, \ldots, 1],$$

где $1 \neq \beta \in R_+^*$, что невозможно. Таким образом, $\xi_1\eta_1^{-1} \neq \xi_2\eta_2^{-1}$. □

4. Основная теорема

В этом разделе мы докажем основную теорему.

Лемма 15. *Если $n \geqslant 3$, $1/2 \in R$, автоморфизм $\Phi' \in \mathrm{Aut}\big(G_n(R)\big)$ таков, что $\Phi'(S_\sigma) = \alpha^{\mathrm{sgn}\,\sigma} S_\sigma$, $\alpha^2 = 1$, для всех $\sigma \in \Sigma_n$, то существует некоторое отображение $c(\cdot)\colon R_+ \to R_+$, такое что $\Phi'\big(B_{12}(x)\big) = B_{12}\big(b(x)\big)$ для всех $x \in R_+$.*

Доказательство. По лемме 13 имеем

$$\Phi'\big(B_{12}(1)\big) = \begin{pmatrix} \alpha & \beta & & & \\ \gamma & \delta & & & \\ & & a & & \\ & & & \ddots & \\ & & & & a \end{pmatrix}, \quad a \in R_+^*, \quad \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in G_2(R).$$

Пусть для каждого $x \in R_+^*$

$$\Phi'(\mathrm{diag}[x, 1, \ldots, 1]) = \mathrm{diag}[\xi(x), \gamma(x), \ldots, \gamma(x)], \quad \xi(x), \eta(x) \in R_+^*$$

(см. лемма 12). Тогда для любого $x \in R_+^*$

$$\Phi'\big(B_{12}(x)\big) = \Phi'(\mathrm{diag}[x, 1, \ldots, 1] B_{12}(1)\, \mathrm{diag}[x^{-1}, 1, \ldots, 1]) =$$
$$= \mathrm{diag}[\xi(x), \eta(x), \ldots, \eta(x)] \begin{pmatrix} \alpha & \beta & & & \\ \gamma & \delta & & & \\ & & a & & \\ & & & \ddots & \\ & & & & a \end{pmatrix} \mathrm{diag}[\xi(x)^{-1}, \eta(x)^{-1}, \ldots, \eta(x)^{-1}] =$$
$$= \begin{pmatrix} \alpha & \nu(x)\beta & & & \\ \nu(x)^{-1}\gamma & \delta & & & \\ & & a & & \\ & & & \ddots & \\ & & & & a \end{pmatrix}$$

для $\nu(x) = \xi(x)\eta(x)^{-1}$.

По лемме 14 для $x_1 \neq x_2$ имеем $\nu(x_1) \neq \nu(x_2)$.

Для каждого $x \in R_+$ матрицы $\Phi'\big(B_{12}(1)\big)$ и $\Phi'\big(B_{12}(x)\big)$ коммутируют. Напишем это условие в матричной форме для $x \in R_+^*$:

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} \alpha & \nu(x)\beta \\ \nu(x)^{-1}\gamma & \delta \end{pmatrix} = \begin{pmatrix} \alpha & \nu(x)\beta \\ \nu(x)^{-1}\gamma & \delta \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}.$$

Следовательно,

$$\begin{pmatrix} \alpha^2 + \nu(x)^{-1}\beta\gamma & \nu(x)\alpha\beta + \beta\delta \\ \gamma\alpha + \nu(x)^{-1}\delta\gamma & \nu(x)\gamma\beta + \delta^2 \end{pmatrix} = \begin{pmatrix} \alpha^2 + \nu(x)\beta\gamma & \alpha\beta + \nu(x)\beta\delta \\ \nu(x)^{-1}\gamma\alpha + \delta\gamma & \nu(x)^{-1}\gamma\beta + \delta^2 \end{pmatrix}.$$

Таким образом, $\nu(x)^{-1}\beta\gamma = \nu(x)\beta\gamma$ для различных $x \in R_+^*$. Значит (так как $\nu(x) - \nu(x)^{-1}$ для некоторых x принимает обратимые значения), $\beta\gamma = 0$.

Используем условие

$$\big(B_{12}(1)\big)^2 = \operatorname{diag}[2, 1, \ldots, 1] B_{12}(1) \operatorname{diag}[1/2, 1, \ldots, 1].$$

Имеем

$$\begin{pmatrix} \alpha^2 & \beta(\alpha+\delta) & & & \\ \gamma(\alpha+\delta) & \delta^2 & & & \\ & & a^2 & & \\ & & & \ddots & \\ & & & & a^2 \end{pmatrix} = \begin{pmatrix} \alpha & \nu(2)\beta & & & \\ \nu(2)^{-1}\gamma & \delta & & & \\ & & a & & \\ & & & \ddots & \\ & & & & a \end{pmatrix},$$

откуда получаем, что $\alpha^2 = \alpha$, $\delta^2 = \delta$, $a = 1$ (так как a обратим).

Воспользуемся соотношением

$$B_{12}(1)B_{13}(1) = B_{13}(1)B_{12}(1),$$

из которого следует, что

$$\begin{pmatrix} \alpha^2 & \beta & \alpha\beta \\ \alpha\gamma & \delta & \gamma\beta \\ \gamma & 0 & \delta \end{pmatrix} = \begin{pmatrix} \alpha^2 & \beta\alpha & \beta \\ \gamma & \delta & 0 \\ \alpha\gamma & 0 & \delta \end{pmatrix},$$

откуда получаем $\alpha\gamma = \gamma$.

Далее воспользуемся соотношением

$$B_{12}(1)B_{13}(1) = B_{13}(1)B_{23}(1)B_{12}(1),$$

которое даёт

$$\begin{pmatrix} \alpha & \alpha\beta & \beta^2 \\ \gamma & \alpha\delta & \beta\delta \\ 0 & \gamma & \delta \end{pmatrix} = \begin{pmatrix} \alpha^2 & \alpha\beta & \beta\delta \\ \gamma & \alpha\delta & \beta \\ \alpha\gamma + \gamma^2\delta & \gamma\delta^2 & \delta^2 \end{pmatrix}.$$

Значит, $\alpha\gamma + \gamma^2\delta = 0$, откуда $\alpha\gamma = \gamma = 0$. Так как $\gamma = 0$, то элементы α и δ обратимы, а так как α и δ — идемпотенты, то $\alpha = \delta = 1$. Таким образом, $\Phi'\big(B_{12}(1)\big) = B_{12}(\beta)$.

Теперь рассмотрим $B_{12}(x)$, $x \in R_+$. Из соотношения

$$B_{12}(1)B_{23}(x) = B_{13}(x)B_{23}(x)B_{12}(1)$$

получаем

$$\begin{pmatrix} 1 & a\beta & b\beta \\ 0 & a & b \\ 0 & c & d \end{pmatrix} = \begin{pmatrix} a & a\beta + bc & bd \\ 0 & a & b \\ c & c\beta + cd & d^2 \end{pmatrix}.$$

Значит, $c = 0$, поэтому a и d обратимы. Из соотношения

$$B_{12}(x)^2 = \operatorname{diag}[2, 1, \ldots, 1]^{-1} B_{12}(x) \operatorname{diag}[2, 1, \ldots, 1]$$

получаем, что $a^2 = a$, $d^2 = d$. Значит, $a = d = 1$. Таким образом, $\Phi'\bigl(B_{12}(x)\bigr) = B_{12}\bigl(b(x)\bigr)$. □

Напомним (см. определение 8), что если G — полугруппа, то гомоморфизм $\lambda(\cdot)\colon G \to G$ называется *центральным гомоморфизмом* полугруппы G, если $\lambda(G) \subset Z(G)$. Отображение $\Omega(\cdot)\colon G \to G$, такое что для всех $X \in G$

$$\Omega(X) = \lambda(X) \cdot X,$$

где $\lambda(\cdot)$ — центральный гомоморфизм, называется *центральной гомотетией*.

Напомним, что для любого автоморфизма $y(\cdot) \in \operatorname{Aut}(R_+)$ через Φ^y мы обозначаем такой автоморфизм полугруппы $G_n(R)$, что

$$\Phi^y(X) = \Phi^y\bigl((x_{ij})\bigr) = \bigl(y(x_{ij})\bigr)$$

для всех $X = (x_{ij}) \in G_n(R)$.

Теорема. *Пусть Φ — любой автоморфизм полугруппы $G_n(R)$, $n \geqslant 3$, $1/2 \in R$. Тогда на полугруппе $\mathrm{GE}_n^+(R)$ (см. определение 7) $\Phi = \Phi_M \Phi^c \Omega$, где $M \in \Gamma_n(R)$, $c(\cdot) \in \operatorname{Aut}(R_+)$, $\Omega(\cdot)$ — центральная гомотетия полугруппы $\mathrm{GE}_n^+(R)$.*

Доказательство. По леммам 4, 6, 11 существует такая матрица $M' \in \Gamma_n(R)$, что для любой перестановки $\sigma \in \Sigma_n$

$$\Phi'(S_\sigma) = \Phi_{M'}\Phi(S_\sigma) = \alpha^{\operatorname{sgn}\sigma} S_\sigma, \quad \alpha^2 = 1.$$

Теперь рассмотрим автоморфизм Φ'. По лемме 15 существует отображение $b(\cdot)\colon R_+ \to R_+$, такое что для любого элемента $x \in R_+$

$$\Phi'\bigl(B_{12}(x)\bigr) = B_{12}\bigl(b(x)\bigr).$$

Рассмотрим это отображение. Так как Φ' — автоморфизм полугруппы $G_n(R)$, то отображение $b(\cdot)\colon R_+ \to R_+$ биективно.

Так как для всех $x_1, x_2 \in R_+$

$$B_{12}(x_1 + x_2) = B_{12}(x_1)B_{12}(x_2),$$

то

$$\begin{aligned} B_{12}\bigl(b(x_1 + x_2)\bigr) &= \Phi'\bigl(B_{12}(x_1 + x_2)\bigr) = \Phi'\bigl(B_{12}(x_1)B_{12}(x_2)\bigr) = \\ &= \Phi'\bigl(B_{12}(x_1)\bigr)\Phi'\bigl(B_{12}(x_2)\bigr) = B_{12}\bigl(b(x_1)\bigr) \cdot B_{12}\bigl(b(x_2)\bigr) = B_{12}\bigl(b(x_1) + b(x_2)\bigr), \end{aligned}$$

откуда следует, что $b(x_1+x_2)=b(x_1)+b(x_2)$ для всех $x_1,x_2\in R_+$, поэтому $b(\cdot)$ аддитивно.

Для того чтобы доказать мультипликативность отображения $b(\cdot)$, используем следующие условия:

1) $\Phi'\bigl(B_{13}(x)\bigr)=\Phi'\bigl(S_{(2,3)}B_{12}(x)S_{(2,3)}\bigr)=\alpha S_{(2,3)}B_{12}\bigl(b(x)\bigr)\alpha S_{(2,3)}=$
$=\alpha^2B_{13}\bigl(b(x)\bigr)=B_{13}\bigl(b(x)\bigr);$

2) аналогично $\Phi'\bigl(B_{32}(x)\bigr)=B_{32}\bigl(b(x)\bigr);$

3) (сравните с доказательством леммы 15)

$$\begin{aligned}
&B_{13}(x_1)B_{32}(x_2)=B_{32}(x_2)B_{13}(x_1)B_{12}(x_1x_2)\Longrightarrow\\
&\quad\Longrightarrow\Phi'\bigl(B_{13}(x_1)\bigr)\Phi'\bigl(B_{32}(x_2)\bigr)=\Phi'\bigl(B_{32}(x_2)\bigr)\Phi'\bigl(B_{13}(x_1)\bigr)\Phi'\bigl(B_{12}(x_1x_2)\bigr)\Longrightarrow\\
&\quad\Longrightarrow B_{13}\bigl(b(x_1)\bigr)B_{32}\bigl(b(x_2)\bigr)=B_{32}\bigl(b(x_2)\bigr)B_{13}\bigl(b(x_1)\bigr)B_{12}\bigl(b(x_1x_2)\bigr)\Longrightarrow\\
&\quad\Longrightarrow\forall\,x_1,x_2\in R_+\ \begin{pmatrix}1&b(x_1)b(x_2)&b(x_1)\\0&1&0\\0&b(x_2)&1\end{pmatrix}=\begin{pmatrix}1&b(x_1x_2)&b(x_1)\\0&1&0\\0&b(x_2)&1\end{pmatrix}\Longrightarrow\\
&\quad\Longrightarrow\forall\,x_1,x_2\in R_+\ b(x_1x_2)=b(x_1)b(x_2).
\end{aligned}$$

Значит, $b(\cdot)$ является мультипликативным отображением.

Так как $b(\cdot)$ биективно, аддитивно и мультипликативно, то $b(\cdot)$ является автоморфизмом полукольца R_+.

Рассмотрим теперь отображение $\Phi^{b^{-1}}$, которое переводит каждую матрицу $A=(a_{ij})$ в матрицу $\Phi^{b^{-1}}(A)=\bigl(b^{-1}(a_{ij})\bigr)$. Это отображение является автоморфизмом полукольца $G_n(R)$. Тогда

$$\Phi''=\Phi^{b^{-1}}\circ\Phi'=\Phi^{b^{-1}}\circ\Phi_{M'}\circ\Phi$$

является автоморфизмом полугруппы $G_n(R)$, оставляющим на месте все матрицы $B_{ij}(x)$ ($x\in R_+$, $i,j=1,\dots,n$, $i\ne j$) и таким, что $\Phi''(S_\sigma)=\alpha^{\operatorname{sgn}\sigma}S_\sigma$ ($\sigma\in\Sigma_n$). Именно,

$$\Phi''(S_\sigma)=\Phi^{b^{-1}}\bigl(\Phi'(S_\sigma)\bigr)=\Phi^{b^{-1}}(\alpha S_\sigma)=b^{-1}(\alpha)S_\sigma,$$

так как матрица S_σ содержит только 0 и 1. Для $i=3,\dots,n$

$$\begin{aligned}
\Phi''\bigl(B_{i2}(x)\bigr)&=\Phi''\bigl(S_{(1,i)}B_{12}(x)S_{(1,i)}\bigr)=S_{(1,i)}\Phi''\bigl(B_{12}(x)\bigr)S_{(1,i)}=\\
&=S_{(1,i)}\Phi^{b^{-1}}\bigl(B_{12}(b(x)\bigr)S_{(1,i)}=S_{(1,i)}B_{12}(x)S_{(1,i)}=B_{i,2}(x);
\end{aligned}$$

для $j=3,\dots,n$

$$\Phi''\bigl(B_{1j}(x)\bigr)=\Phi''\bigl(S_{(2,j)}B_{12}(x)S_{(2,j)}\bigr)=S_{(2,j)}B_{12}(x)S_{(2,j)}=B_{1j}(x);$$

для $i,j=3,\dots,n$

$$\Phi''\bigl(B_{ij}(x)\bigr)=\Phi''\bigl(S_{(i,1)}B_{1j}(x)S_{(1,i)}\bigr)=S_{(1,i)}B_{1j}(x)S_{(1,i)}=B_{ij}(x).$$

Как мы знаем (см. лемму 12), для всех $\alpha\in R_+^*$

$$\Phi''(\operatorname{diag}[a,1,\dots,1])=\operatorname{diag}[\beta(a),\gamma(a),\dots,\gamma(a)],\quad \beta(a),\gamma(a)\in R_+^*.$$

Имеем

$$
\begin{aligned}
&\operatorname{diag}[a,1,\dots,1]B_{12}(1)\operatorname{diag}[a^{-1},1,\dots,1]=B_{12}(a)\Longrightarrow\\
&\quad\Longrightarrow\Phi''(\operatorname{diag}[a,1,\dots,1])\Phi''\big(B_{12}(1)\big)\Phi''(\operatorname{diag}[a^{-1},1,\dots,1])=\Phi''\big(B_{12}(a)\big)\Longrightarrow\\
&\quad\Longrightarrow\operatorname{diag}[\beta(a),\gamma(a),\dots,\gamma(a)]B_{12}(1)\operatorname{diag}[\beta(a)^{-1},\gamma(a)^{-1},\dots,\gamma(a)^{-1}]=B_{12}(a)\Longrightarrow\\
&\quad\Longrightarrow\beta(a)\gamma(a)^{-1}=a\Longrightarrow\beta(a)=a\gamma(a)\Longrightarrow\\
&\quad\Longrightarrow\forall\, a\in R_+^*\ \Phi''(\operatorname{diag}[a,1,\dots,1])=\operatorname{diag}[a\gamma(a),\gamma(a),\dots,\gamma(a)].
\end{aligned}
$$

Поскольку для всех $a_1,a_2\in R_+^*$

$$
\begin{aligned}
\operatorname{diag}[a_1a_2\gamma(a_1a_2),\gamma(a_1a_2),\dots,\gamma(a_1a_2)]&=\Phi''(\operatorname{diag}[a_1a_2,1,\dots,1])=\\
&=\Phi''(\operatorname{diag}[a_1,1,\dots,1])\Phi''(\operatorname{diag}[a_2,1,\dots,1])=\\
&=\operatorname{diag}[a_1\gamma(a_1),\gamma(a_1),\dots,\gamma(a_1)]\operatorname{diag}[a_2\gamma(a_2),\gamma(a_2),\dots,\gamma(a_2)]=\\
&=\operatorname{diag}[a_1a_2\gamma(a_1)\gamma(a_2),\gamma(a_1)\gamma(a_2),\dots,\gamma(a_1)\gamma(a_2)],
\end{aligned}
$$

то для всех $a_1,a_2\in R_+^*$

$$\gamma(a_1a_2)=\gamma(a_1)\gamma(a_2).$$

Следовательно, отображение $\gamma(\cdot)$ — центральный гомоморфизм $\gamma(\cdot)\colon R_+^*\to R_+^*$.

Если $A=\operatorname{diag}[a_1,\dots,a_n]\in D_n(R)$, то

$$
\begin{aligned}
&\Phi''(A)=\\
&\quad=\Phi''\big(\operatorname{diag}[a_1,1,\dots,1]S_{1,2}\operatorname{diag}[a_2,1,\dots,1]S_{(1,2)}\times\\
&\quad\times S_{(1,3)}\operatorname{diag}[a_3,1,\dots,1]S_{(1,3)}\cdots S_{(1,n)}\operatorname{diag}[a_n,1,\dots,1]S_{(1,n)}\big)=\\
&\quad=\alpha^{2(n-1)}\gamma(a_1)\operatorname{diag}[a_1,1,\dots,1]S_{(1,2)}\times\\
&\quad\times\gamma(a_2)\operatorname{diag}[a_2,1,\dots,1]S_{(1,2)}\cdots S_{(1,n)}\gamma(a_n)\operatorname{diag}[a_n,1,\dots,1]\gamma(a_n)=\\
&\quad=\gamma(a_1)\cdots\gamma(a_n)A=\gamma(a_1\cdots a_n)A.
\end{aligned}
$$

Напомним (см. определение 5), что $\mathbf{P}$ является подполугруппой в $G_n(R)$, порождённой матрицами S_σ ($\sigma\in\Sigma_n$), $B_{ij}(x)$ ($x\in R_+$, $i,j=1,\dots,n$, $i\neq j$) и $\operatorname{diag}[\alpha_1,\dots,\alpha_n]$ ($\alpha_1,\dots,\alpha_n\in R_+^*$).

Заметим, что определитель любой матрицы из полугруппы $\mathrm{GE}_n^+(R)$ есть обратимое число, сравнимое с нулём (либо большее нуля, либо меньшее). Это следует из того, что все диагональные матрицы имеют определитель, больший нуля, матрицы подстановок имеют определитель ±1, матрицы $B_{ij}(x)$ и их обратные имеют определитель 1.

Пусть $\Phi''\big(S_{(1,2)}\big)=\alpha S_{(1,2)}$, $\alpha^2=1$, $\alpha\geqslant 0$. Рассмотрим отображение $\mu\colon R_+^*\cup R_-^*\to R_+^*$, ставящее в соответствие каждому $a\in R_+^*$ этот же элемент, а каждому $a\in R_-^*$ — элемент $-\alpha a$. Очевидно, что μ — гомоморфизм.

Тогда отображение, ставящее в соответствие каждой матрице A матрицу $\mu(\det A)A$, является центральной гомотетией группы $\mathrm{GE}_n^+(R)$. Обозначим эту гомотетию через Ω' и рассмотрим композицию $\Phi'''=\Omega'\circ\Phi''$. Это автоморфизм полугруппы $\mathrm{GE}_n^+(R)$, оставляющий на месте все S_σ, $\sigma\in\Sigma_n$, и все $B_{ij}(x)$, $i\neq j$, $x\in R_+$.

Ясно, что любая матрица $A \in \mathbf{P}$ может быть представлена в виде

$$A = \operatorname{diag}[\alpha_1, \ldots, \alpha_n] A_1 \cdots A_k,$$

где

$$\alpha_1, \ldots, \alpha_n \in R_+^*,$$
$$A_1, \ldots, A_k \in \{S_\sigma,\ B_{ij}(x) \mid \sigma \in \Sigma_n,\ x \in R_+,\ i,j = 1, \ldots, n,\ i \neq j\}.$$

Тогда

$$\Phi'''(A) = \Phi'''(\operatorname{diag}[\alpha_1, \ldots, \alpha_n] A_1 \cdots A_k) = \\ = \gamma(\alpha_1 \cdots \alpha_n) \operatorname{diag}[\alpha_1, \ldots, \alpha_n] A_1 \cdots A_k = \gamma(\alpha_1 \cdots \alpha_n) A.$$

Теперь введём отображение $\bar{\gamma}(\cdot)\colon \mathbf{P} \to R_+^*$ с помощью следующего правила: если $A \in \mathbf{P}$ и $A = \operatorname{diag}[\alpha_1, \ldots, \alpha_n] A_1 \cdots A_k$, где

$$A_1, \ldots, A_k \in \{S_\sigma,\ B_{ij}(x) \mid \sigma \in \Sigma_n,\ x \in R_+,\ i,j = 1, \ldots, n,\ i \neq j\},$$

то $\bar{\gamma}(A) = \gamma(\alpha_1, \ldots, \alpha_n)$.

Отображение $\bar{\gamma}(\cdot)$ определено однозначно, так как если

$$A = \operatorname{diag}[\alpha_1, \ldots, \alpha_n] A_1 \cdots A_k = \operatorname{diag}[\alpha_1', \ldots, \alpha_n'] A_1' \cdots A_m',$$

то

$$\Phi'''(A) = \gamma(\alpha_1 \cdots \alpha_n) A, \quad \Phi'''(A) = \gamma(\alpha_1' \cdots \alpha_n') A$$

и поэтому

$$\gamma(\alpha_1 \cdots \alpha_n) = \gamma(\alpha_1' \cdots \alpha_n').$$

Так как

$$\bar{\gamma}(AA')AA' = \Phi'''(AA') = \Phi'''(A)\Phi'''(A') = \bar{\gamma}(A)A \cdot \bar{\gamma}(A')A' = \bar{\gamma}(A)\bar{\gamma}(A')AA',$$

то $\bar{\gamma}$ является гомоморфизмом $\mathbf{P} \to R_+^*$.

Теперь мы видим, что на полугруппе $\mathbf{P}$ автоморфизм Φ''' совпадает с центральной гомотетией $\Omega(\cdot)\colon \mathbf{P} \to \mathbf{P}$, где $\Omega(A) = \bar{\gamma}(A) \cdot A$ для всех $A \in \mathbf{P}$.

Пусть $B \in \mathrm{GE}_n^+(R)$. Тогда (см. определения 6, 7) матрица B $\mathcal{P}$-эквивалентна некоторой матрице $A \in \mathbf{P}$, т. е. существуют матрицы $A_0, \ldots, A_k \in G_n(R)$, $A_0 = A \in \mathbf{P}$, $A_k = B$, и матрицы $P_i, \tilde{P}_i, Q_i, \tilde{Q}_i \in \mathbf{P}$, $i = 0, \ldots, k-1$, такие что $P_i A_i \tilde{P}_i = Q_i A_{i+1} \tilde{Q}_i$ для всех $i = 0, \ldots, k-1$. Тогда

$$\begin{aligned}
&\Phi'''(P_0 A_0 \tilde{P}_0) = \Phi'''(Q_0 A_1 \tilde{Q}_0) \Longrightarrow \\
&\quad \Longrightarrow \bar{\gamma}(P_0) P_0 \bar{\gamma}(A_0) A_0 \bar{\gamma}(\tilde{P}_0) \tilde{P}_0 = \bar{\gamma}(Q_0) Q_0 \Phi''(A_1) \bar{\gamma}(\tilde{Q}_0) \tilde{Q}_0 \Longrightarrow \\
&\quad \Longrightarrow \bar{\gamma}(P_0 A_0 \tilde{P}_0) P_0 A_0 \tilde{P}_0 = \bar{\gamma}(Q_0 \tilde{Q}_0) Q_0 \Phi'''(A_1) \tilde{Q}_0 \Longrightarrow \\
&\quad \Longrightarrow \bar{\gamma}(P_0 A_0 \tilde{P}_0) \bar{\gamma}(Q_0 \tilde{Q}_0)^{-1} Q_0 A_1 \tilde{Q}_0 = Q_0 \Phi'''(A_1) \tilde{Q}_0 \Longrightarrow \\
&\quad \Longrightarrow \Phi'''(A_1) = \bar{\gamma}(P_0 A_0 \tilde{P}_0) \bar{\gamma}(Q_0 \tilde{Q}_0)^{-1} A_1, \ldots, \\
&\qquad \Phi'''(B) = \Phi''(A_n) = \bar{\gamma}(P_{n-1}) \bar{\gamma}(A_{n-1}) \bar{\gamma}(\tilde{P}_{n-1}) \bar{\gamma}(Q_{n-1})^{-1} \bar{\gamma}(\tilde{Q}_{n-1}).
\end{aligned}$$

Значит, мы можем продолжить отображение $\bar{\gamma}(\cdot)\colon \mathbf{P} \to R_+^*$ до некоторого отображения $\lambda(\cdot)\colon \mathrm{GE}_n^+(R) \to R_+^*$, такого что для каждого $B \in \mathrm{GE}_n^+(R)$

$$\Phi'''(B) = \lambda(B) \cdot B.$$

Так как Φ''' является автоморфизмом полугруппы $\mathrm{GE}_n^+(R)$, то $\lambda(\cdot)$ является центральным гомоморфизмом $\lambda(\cdot)\colon \mathrm{GE}_n^+(R) \to R_+^*$, и значит, автоморфизм $\Phi'''\colon \mathrm{GE}_n^+(R) \to \mathrm{GE}_n^+(R)$ является центральной гомотетией $\Omega''(\cdot)\colon \mathrm{GE}_n^+(R) \to \mathrm{GE}_n^+(R)$, где $\Omega''(X) = \lambda(X) \cdot X$ для всех $X \in \mathrm{GE}_n^+(R)$.

Так как $\Phi''' = \Omega''$ на $\mathrm{GE}_n^+(R)$ и $\Phi''' = \Omega' \circ \Phi^{b^{-1}} \circ \Phi_{M'} \circ \Phi$ на $G_n(R)$, то $\Phi = \Phi_M \circ \Phi^b \circ \Omega$ на $\mathrm{GE}_n^+(R)$, где $M = {M'}^{-1}$, $\Omega = \Omega'\Omega''$.

Теорема доказана. $\square$

Литература

[1] Бунина Е. И., Михалёв А. В. Автоморфизмы полугруппы обратимых матриц с неотрицательными элементами // Фундамент. и прикл. мат. — 2005. — Т. 11, вып. 2. — С. 3—23.

[2] Ильин С. Н. Обратимые матрицы над (неассоциативными) антикольцами // Универсальная алгебра и её приложения. — Волгоград: Перемена, 2000. — С. 81—89.

[3] Михалёв А. В., Шаталова М. А. Автоморфизмы и антиавтоморфизмы полугруппы обратимых матриц с неотрицательными элементами // Мат. сб. — 1970. — Т. 81, № 4. — С. 600—609.