В. Г. Бардаков

О РАЗЛОЖЕНИИ АВТОМОРФИЗМОВ СВОБОДНЫХ МОДУЛЕЙ НА ПРОСТЫЕ МНОЖИТЕЛИ

Изучаются разложения автоморфизмов некоторых свободных модулей в произведение трансвекций и дилатаций. В частности, для свободного $\mathbb{Z}$-модуля $M = \mathbb{Z}^n$ доказано, что при $n \geq 3$ всякий автоморфизм $\sigma \in \mathrm{GL}_n(M)$ представим в виде произведения не более $2n + 5$ трансвекций и одного простого преобразования, которое является трансвекцией, если $\sigma \in \mathrm{SL}_n(M)$, и дилатацией – в противном случае. В качестве следствия получается, что при $n \geq 3$ ширина группы $\mathrm{SL}_n(\mathbb{Z})$ относительно множества коммутаторов не превосходит 10.

Библиография: 24 названия.

Введение

Хорошо известно (см., например, [1, с. 25]), что всякая матрица из общей линейной группы $\mathrm{GL}_n(F)$ над полем F представима в виде произведения элементарных трансвекций и диагональной матрицы, причем из самого доказательства легко вывести оценку числа элементарных трансвекций, требующихся для такого разложения. Это число зависит только от n и не зависит от самой матрицы. В связи с рассмотренным примером возникает следующая проблема: для группы G с порождающим множеством S найти наименьшее $m \in \mathbb{N} \cup \{+\infty\}$ такое, что всякий элемент из G представим в виде произведения $\leq m$ элементов из S. Следуя Ю. И. Мерзлякову [2], будем называть такое m *шириной* группы G относительно множества S и обозначать $\mathrm{wid}(G, S)$. В предлагаемой работе исследуется ширина некоторых линейных групп относительно различных порождающих множеств.

Из уже известных результатов отметим работу [3], в которой доказано, что ширина группы $\mathrm{SL}_n(\acute{O})$, где $\acute{O}$ – кольцо целых чисел алгебраического числового поля, относительно множества элементарных трансвекций, конечна, и работу [4] в которой доказано конечность ширины симплектической группы $\mathrm{Sp}_{2n}(\acute{O})$, $n \geq 3$, относительно множества элементарных матриц. Аналогичные результаты для некоторых групп Шевалле над тем же кольцом $\acute{O}$ получены О. Н. Тавгенем [5]. С другой стороны, ван дер Каллен [6] доказал, что если F — поле бесконечной степени трансцендентности над своим простым подполем, то группа $\mathrm{SL}_n(F[x])$ при $n \geq 2$ имеет бесконечную ширину относительно множества элементарных трансвекций.

Так как группа матриц $\mathrm{GL}_n(R)$ над кольцом R изоморфна группе $\mathrm{GL}_n(M)$ автоморфизмов свободного n-мерного модуля $M = R^n$, то по аналогии с предыдущими результатами можно изучать разложения автоморфизмов из $\mathrm{GL}_n(M)$ в произведение простых автоморфизмов. Отметим, что в случае коммутативного кольца R простые автоморфизмы исчерпываются множеством трансвекций и дилатаций. Из теоремы Дьедонне следует, что если V – n-мерное векторное пространство над полем F, то всякое преобразование $\sigma \in \mathrm{GL}_n(V)$, не являющееся большой дилатацией, представимо в виде произведения $\leq n - 1$ трансвекций и одного простого преобразования; если же σ является большой дилатацией, то она представима в виде произведения $\leq n$ трансвекций и одного простого преобразования. Эллерс и Лауш [8] получили аналогичные утверждения для группы автоморфизмов $\mathrm{GL}_n(M)$, $n \geq 3$, свободного модуля $M = R^n$ над локальным ассоциативным кольцом R с единицей. В этой же работе ими получены аналогичные результаты для некоторых других классических групп.

Дьекович [9] изучал разложимость простого преобразования модуля $M = R^n$, $n \geq 3$, над телом R в произведение трансвекций и отражений и получил критерий разложимости простого преобразования в произведение трех трансвекций, а также критерий разложимости простого преобразования в произведение трех отражений. А. А. Коробов [10] обобщил эти результаты, найдя критерий разложимости простого преобразования в произведение трех простых преобразований с заданными параметрами.

Отметим связь описанной проблематики с задачей вычисления ширины $\mathrm{wid}(G, V)$ вербальной подгруппы $V(G)$ линейной группы G относительно множества теоретико-групповых слов V, т. е. относительно множества S значений слов из V на группе G. Наиболее общий результат здесь принадлежит Ю. И. Мерзлякову [2] (см. также [11, § 12]), установившему, что всякая вербальная подгруппа алгебраической группы $G \leq \mathrm{GL}_n(\Omega)$, где Ω – алгебраически замкнутое поле бесконечной степени трансцендентности над простым подполем, имеет конечную ширину относительно любого слова v.

Ряд работ посвящен исследованию ширины коммутанта некоторых классических групп относительно коммутатора $v = x^{-1}y^{-1}xy$. Так, например, Томпсон [12] доказал, что для всякого поля F ширина $\mathrm{wid}(\mathrm{GL}_n(F), v) = 1$, а $\mathrm{wid}(\mathrm{SL}_n(F), v) \leq 2$ при любом $n \geq 2$. Гоу [13] доказал, что ширина $\mathrm{wid}(\mathrm{Sp}_{2n}(F), v)$ коммутанта симплектической группы не превосходит 2 при любом $n \geq 1$. С другой стороны, известно, что ширина всякой собственной вербальной подгруппы $\mathrm{SL}_2(\mathbb{Z})$ относительно любого нетривиального слова бесконечна. При $n \geq 3$ Ньюмэн [14] доказал, что $\mathrm{wid}(\mathrm{SL}_n(\mathbb{Z}), v) < \infty$. Но для кольца $R = F[x]$ многочленов над полем F бесконечной степени трансцендентности над простым подполем и любого $n \geq 2$ ширина $\mathrm{wid}(\mathrm{SL}_n(R), v)$ бесконечна. Этот результат, а также ряд близких к этой тематике результатов были получены в работе [15]. В связи с двумя последними результатами интересно было бы найти ширину коммутанта группы $\mathrm{SL}_n(\mathbb{Q}[x])$, а также, по-видимому, тесно связанную с ней ширину группы $\mathrm{SL}_n(\mathbb{Q}[x])$, $n \geq 3$, относительно элементарных трансвекций (последний вопрос отмечается в [3]).

В предлагаемой работе исследуются автоморфизмы некоторых свободных R-модулей, где R – ассоциативное кольцом с единицей, являющееся областью целостности. Так в § 2 для свободного R-модуля $M = R^n$, при некоторых дополнительных ограничений на M, доказывается, что если ранг стабильности кольца R равен m, то всякое преобразование σ из $\mathrm{GL}_n(M)$, $n > m$, не являющееся большой дилатацией, представимо в виде произведения $\leq 2(n-m)$ трансвекций и одного преобразования с вычетом $\leq m$. Если же σ – большая дилатация, то она представима в виде произведения $\leq n$ трансвекций и одного простого преобразования.

В § 3 исследуются автоморфизмы свободного $\mathbb{Z}$-модуля $M = \mathbb{Z}^n$ при $n \geq 3$ и доказывается, что всякий такой автоморфизм представим в виде произведения $\leq 2n + 6$ простых автоморфизмов. В качестве следствия будет доказано, что ширина коммутанта группы $\mathrm{SL}_n(\mathbb{Z})$ при всех $n \geq 3$ не превосходит 10, что улучшает оценку Ньюмэна [14] из которой следовало, что эта ширина $\leq c\ln(n) + 40$, где $c = 2\ln(3/2)$. Отметим, с другой стороны, что для достаточно больших n эта ширина ≤ 4 (см. [24]). Возможно, что эта оценка справедлива и для всех $n \geq 3$.

Автор благодарит профессора Ю. И. Мерзлякова за постоянную помощь и поддержку в работе.

§ 1. Предварительные замечания

Пусть R — ассоциативное кольцо с единицей, являющееся областью целостности; R^* — его мультипликативная группа, F — поле частных кольца R; $M = R^n$ — свободный R–модуль размерности n. Через $\mathrm{GL}_n(M)$ будем обозначать группу автоморфизмов свободного модуля M, которая, очевидно, изоморфна кольцу матриц $\mathrm{GL}_n(R)$ размера $n \times n$ с элементами из R, $\mathrm{SL}_n(R)$ — подгруппа группы $\mathrm{GL}_n(R)$, состоящая из матриц с определителем 1. *Элементарной трансвекцией* $t_{i,j}(\lambda)$, $1 \le i,j \le n$, $i \ne j$, $\lambda \in R$, называется матрица из $\mathrm{GL}_n(R)$ которая отличается от единичной матрицы лишь тем, что у нее на месте (i,j) находится элемент λ.

Напомним определение ранга стабильности кольца R (см., например, [16], где используется термин "стабильный ранг", который кажется менее удачным). Элемент $\alpha = (a_1, a_2, \dots, a_n) \in R^n$ называется *унимодулярным* в R^n, если найдутся элементы $b_1, b_2, \dots, b_n$ из R такие, что $\sum_{i=1}^n a_i b_i = 1$. *Рангом стабильности* или, короче, s–*рангом* кольца R называется наименьшее натуральное число m для которого выполняется следующее условие: для любого вектора $\alpha = (a_1, a_2, \dots, a_{m+1})$ унимодулярного в R^{m+1}, существуют $c_1, c_2, \dots, c_m$ из R такие, что вектор $(a_1 + c_1 a_{m+1}, a_2 + c_2 a_{m+1}, \dots, a_m + c_m a_{m+1})$ унимодулярен в R^m. Известно [16], что для всякого подполя k поля вещественных чисел s-ранг кольца многочленов $k[x_1, \dots, x_n]$ равен $n+1$. Интересно было бы найти s-ранг кольца $\mathbb{Z}[x_1, \dots, x_n]$ при $n \ge 1$ (s-ранг кольца $\mathbb{Z}$, как легко заметить, равен 2). Интерес к этому вопросу объясняется его связью с вопросом ван дер Каллена [17, вопрос 10.38]: "Имеет ли группа $E_{n+3}(\mathbb{Z}[x_1, \dots, x_n])$, $n \ge 1$, конечную ширину относительно множества трансвекций?" Отметим, что речь здесь идет о множестве элементарных трансвекций (см. [6]), а при $n = 0$ вопрос имеет положительное решение [18].

Пусть V – n–мерное векторное пространство над полем F, $\mathrm{GL}_n(V)$ — группа автоморфизмов пространства V. Следующие определения можно найти в лекциях О'Миры [7]. Для автоморфизма σ из $\mathrm{GL}_n(V)$ определим *вычетное пространство* R_σ, *неподвижное пространство* P_σ и *вычет* $\mathrm{res}\,\sigma$ следующими равенствами:

$$R_\sigma = V(\sigma - 1_V), \quad P_\sigma = \ker(\sigma - 1_V) = \{x \in X \mid x\sigma = x\}, \quad \mathrm{res}\,\sigma = \mathrm{dim} R_\sigma.$$

Автоморфизм σ называется *трансвекцией,* если $\sigma = 1_V$ или

$$\mathrm{res}\,\sigma = 1, \quad \det\sigma = 1;$$

σ называется *дилатацией,* если

$$\mathrm{res}\,\sigma = 1, \quad \det\sigma \ne 1.$$

Трансвекции и дилатации будем называть *простыми преобразованиями* векторного пространства V. Легко заметить, что сопрягая простое преобразование автоморфизмом из $\mathrm{GL}_n(V)$, опять получим простое преобразование. Автоморфизм $\sigma \in \mathrm{GL}_n(V)$ называется *большой дилатацией,* если существует такое разложение $V = U \oplus W$, что $W \ne 0$ и $\sigma = (1_U) \oplus (\alpha 1_W)$, $\alpha \in F$. В этом случае $R_\sigma = W$, $P_\sigma = U$.

Нам потребуются следующие два предложения из работы О'Миры.

Лемма 1 ([7, предложение 1.4.8]). *Если σ_1 и σ_2 – нетривиальные трансвекции из $\mathrm{GL}_n(V)$, то $\sigma_1\sigma_2$ тогда и только тогда является трансвекцией, когда $R_1 = R_2$ или $P_1 = P_2$, где R_i и P_i соответственно вычетное и неподвижное пространство преобразования σ_i.*

Лемма 2 ([7, предложение 2.1.4]). *Пусть σ — большая дилатация, а τ – нетривиальная трансвекция с вычетной прямой L и неподвижной гиперплоскостью H. Если $H \supseteq P_\sigma$ и $L \subseteq P_\sigma$, то $\sigma\tau$ не является большой дилатацией.*

Пусть теперь R — ассоциативное кольцо с единицей, являющееся областью целостности, F — его поле частных. Мы будем рассматривать свободный R–модуль $M = R^n$, как подмодуль векторного пространства $V = F^n$. Поэтому мы можем рассматривать линейную группу на M, полагая

$$\mathrm{GL}_n(M) = \{\sigma \in \mathrm{GL}_n(V) \ \mid \ M\sigma = M\}\,.$$

Изучая автоморфизмы модуля M, мы будем предполагать, что M удовлетворяет следующему *условию дополняемости*: неподвижный подмодуль P_σ всякого преобразования σ из $\mathrm{GL}_n(M)$ выделяется в M прямым слагаемым. Я не знаю, насколько богат класс модулей, обладающих этим свойством, но кажется очевидным, что свободные модули над евклидовыми кольцами удовлетворяют условию дополняемости.

Отметим связь между элементарными матрицами из $\mathrm{GL}_n(R)$ и простыми преобразованиями из $\mathrm{GL}_n(M)$. В случае если R — некоторое поле, то это соответствие взаимно однозначно, т. е. для каждой трансвекции (соответственно, для каждой дилатации) τ из $\mathrm{GL}_n(V)$ можно так подобрать базис пространства V, что матрицей преобразования $[\tau]$ является некоторая элементарная трансвекция $t_{i,j}$ (соответственно некоторая диагональная матрица $\mathrm{diag}(1, \ldots, 1, \lambda)$). И обратно, если t – некоторая элементарная матрица из $\mathrm{GL}_n(R)$, то ей соответствует некоторое простое преобразование векторного пространства V. Для произвольного кольца R эта связь уже не столь очевидна. Чтобы как–то описать эту связь, отметим некоторые свойства сопряжения в группе $\mathrm{GL}_n(R)$.

Если опять R — поле, то в группе $\mathrm{GL}_n(R)$ мы можем эффективно проверить, сопряжены ли в ней две матрицы. Каждая матрица сопряжена с некоторой матрицей, имеющей нормальную форму [19, с. 175] (в случае, когда поле алгебраически замкнуто, эта форма называется *жордановой*) и две матрицы сопряжены в $\mathrm{GL}_n(R)$ тогда и только тогда, когда они имеют одну и ту же нормальную форму. Но уже для кольца целых алгебраических чисел R, некоторого числового поля неизвестно эффективного алгоритма, позволяющего проверить сопряженность заданных матриц, хотя проблема сопряженности в группе $\mathrm{GL}_n(R)$ над этими кольцами разрешима [20], [21]. В связи с этим интересно было бы найти в каждом классе сопряженных элементов группы $\mathrm{GL}_n(R)$ представители (подобные уже упоминавшимся нормальным формам матриц для поля), позволяющие эффективно решать проблему сопряженности в группе $\mathrm{GL}_n(R)$ хотя бы для кольца целых алгебраических чисел.

Мы же заметим, как меняются матрицы из $\mathrm{GL}_n(R)$ при сопряжении элементарными трансвекциями. Пусть a — матрица из $\mathrm{GL}_n(R)$, $n \geq 3$, с элементами $a_{i,j} \in R$, $1 \leq i,j \leq n$. Тогда при умножении a справа на трансвекцию $t_{i,j}(\lambda)$ в матрице a i–й столбец умножается на λ и прибавляется к j–му столбцу, а при умножении a слева на $t_{i,j}(\lambda)$ в матрице a j–ая строка умножается на λ и прибавляется к i–ой. Следовательно, при сопряжении матрицы a элементарной трансвекцией $t_{i,j}(\lambda)$ получится матрица, у которой на месте (i,j) стоит элемент

$$a_{i,j} - \lambda^2 a_{j,i} + \lambda(a_{i,i} - a_{j,j}),$$

на остальных местах i–ой строки находятся те же элементы, что и в i–ой строке матрицы $t_{i,j}(-\lambda)a$, на остальных местах j–го столбца те же элементы, что и в j–м столбце матрицы $at_{i,j}(\lambda)$, а на оставшихся местах — соответствующие элементы матрицы a. Поэтому, используя сопряжения элементарными трансвекциями, мы можем произвольный недиагональный элемент матрицы a умножить на некоторое число λ и прибавить к любому другому элементу, находящемуся в той же строке или в том же столбце.

Пусть $v = (v_1, v_2, \ldots, v_{n-1})$ — некоторый вектор из R^{n-1}. Символом $t_i(v)$, $i = 1, 2, \ldots, n$, будем обозначать матрицу из $\mathrm{GL}_n(R)$, у которой i–ая строка имеет вид

$$(v_1, v_2, \ldots, v_{i-1}, 1, v_i, \ldots, v_{n-1}),$$

а остальные строки — те же, что и у единичной матрицы. Через $t^i(v)$ обозначим матрицу, полученную транспонированием матрицы $t_i(v)$. Очевидно, если у вектора v только одна компонента отлична от 0, то $t_i(v)$ (равно как и $t^i(v)$) является элементарной трансвекцией. Поэтому матрицы вида $t_i(v)$ и $t^i(v)$ будем называть *обобщенно элементарными трансвекциями.* Свойства этих матриц во многом напоминают свойства элементарных трансвекций. В частности справедлива

Лемма 3. *Пусть $\alpha_1, \alpha_2, \ldots, \alpha_{n-1}$ — элементы некоторого ассоциативного кольца R; u, v — векторы из R^{n-1}. Тогда в группе $\mathrm{GL}_n(R)$ для всякого i, $i = 1, \ldots, n$ справедливы следующие утверждения*:

а) $t_i(v)t_i(u) = t_i(u)t_i(v) = t_i(v+u)$;

б) $(t_i(v))^{-1} = t_i(-v)$;

в) $(t_j(v))^{t_{j+1,j-1}(\alpha)} = t_j(w)$, $j = 2, \ldots, n-1$, *где w — некоторый вектор из R^{n-1}*;

г) $t_{i,1}(\alpha_1)t_{i,2}(\alpha_2)\ldots t_{i,n}(\alpha_{n-1}) = t_i(w)$, *где $w = (\alpha_1, \ldots, \alpha_{n-1})$*;

д) *если матрица $D = D_1 t_i(v) D_2 t_i(u) D_3$ представлена в виде произведения некоторых матриц, то их число можно уменьшить, положив $D = D_1 D_2^{t_i(-v)}\ t_i(u+v) D_3$ или $D = D_1 t_i(u+v) D_2^{t_i(u)} D_3$.*

Доказательство. Утверждения а), б), г) и д) очевидны. Утверждение в) вытекает из описания сопряжения матрицы элементарной трансвекцией. Действительно, умножить матрицу $t_j(v)$ слева на $t_{j+1,j-1}(-\alpha)$ это все равно, что к $(j+1)$-й строке матрицы $t_j(v)$ прибавить $(j-1)$–ю строку умноженную на $-\alpha$. В результате, на месте $(j+1, j-1)$ появится элемент $-\alpha$. При умножении полученной матрицы справа на $t_{j+1,j-1}(\alpha)$ ее $(j+1)$-й столбец умножится на α и прибавится к $(j-1)$-у столбцу, и на месте $(j+1, j-1)$ опять появится 0. Лемма доказана.

Пусть теперь $M = R^n$ — свободный n–мерный модуль с условием дополняемости и σ — некоторая трансвекция из $\mathrm{GL}_n(M)$. Выбрав базу неподвижного модуля P_σ и дополнив ее до базы всего модуля M, получим базу в которой матрица $[\sigma]$ преобразования σ является обобщенно элементарной трансвекцией, а если кольцо R евклидово, то $[\sigma]$ сопряжена с некоторой элементарной трансвекцией. Аналогично, если σ – дилатация из $\mathrm{GL}_n(M)$, то в подходящей базе она имеет вид $[\sigma] = d_i(\lambda_1, \ldots, \lambda_n) \in \mathrm{GL}_n(M)$ при некотором i, $i = 1, \ldots, n$; $\lambda_j \in R$, а i–я строка имеет вид $(\lambda_1, \ldots, \lambda_n)$, остальные же строки те же, что и у единичной матрицы. Множество обобщенно элементарных трансвекций и матриц $d_i(\lambda_1, \ldots, \lambda_n)$, $\lambda_i \in R^*$, а также транспонированные к ним будем называть *обобщенно элементарными матрицами.* По аналогии с простыми преобразованиями, будем называть матрицу из $\mathrm{GL}_n(R)$ *простой,* если она сопряжена с некоторой обобщенно элементарной матрицей. Таким образом, множеству простых автоморфизмов свободного n–мерного модуля $M = R^n$ с условием дополняемости соответствует множество простых матриц из $\mathrm{GL}_n(R)$.

Отметим также, что если σ — большая дилатация из $\mathrm{GL}_n(M)$, то в подходящей базе она имеет матрицу

$$[\sigma] = \left(\begin{array}{c|c} \mathbf{1}_k & \mathbf{0} \\ \hline * & \alpha \mathbf{1}_{n-k} \end{array}\right)$$

где $\alpha \in R^*$, а k — размерность неподвижного модуля P_σ.

§ 2. Разложение автоморфизмов свободного модуля

В работе [15] сформулировано следующее утверждение

Лемма 4. *Пусть R — ассоциативное кольцо с единицей, s-ранг которого $\leq m$. Тогда для всякого $n \geq m$*

$$\mathrm{GL}_n(R) = ULUL \begin{pmatrix} \mathrm{GL}_m(R) & \mathbf{0} \\ \mathbf{0} & \mathbf{1}_{n-m} \end{pmatrix} = UL \begin{pmatrix} \mathrm{GL}_m(R) & \mathbf{0} \\ \mathbf{0} & \mathbf{1}_{n-m} \end{pmatrix} UL,$$

где U (соответственно L) – группа всех верхне (соответственно нижне) унитреугольных матриц в $E_n(R)$.

Так как всякая унитреугольная матрица представима в виде произведения $\leq n(n-1)/2$ элементарных трансвекций, то из этой леммы следует, что всякая матрица из $\mathrm{GL}_n(R)$ представима в виде произведения не более чем $2n(n-1)$ элементарных трансвекций и матрицы вида

$$\begin{pmatrix} a & \mathbf{0} \\ \mathbf{0} & \mathbf{1}_{n-m} \end{pmatrix} \in \mathrm{GL}_n(R), \quad a \in \mathrm{GL}_m(R).$$

Для автоморфизмов свободного модуля справедливо аналогичное утверждение.

Теорема 1. *Пусть R — ассоциативное кольцо с единицей являющееся областью целостности и s–ранга $\leq m$. Пусть также $M = R^n$ — свободный R–модуль с условием дополняемости. Тогда всякое преобразование σ из $\mathrm{GL}_n(M)$, $n > m$, не являющееся большой дилатацией представимо в виде произведения $\leq 2(n-m)$ трансвекций и некоторого преобразования с вычетом $\leq m$.*

Доказательство. Можно считать, что $l = \mathrm{res}\ \sigma > m$, так как в противном случае доказывать нечего. Выберем базу $p_1, \ldots, p_k$ неподвижного модуля P_σ и дополним ее векторами $p_{k+1}, \ldots, p_n$ до базы всего модуля M. В этой базе преобразование σ будет иметь матрицу

$$[\sigma] = \left(\begin{array}{c|c} \mathbf{1}_k & \mathbf{0} \\ \hline b & a \end{array}\right), \quad a \in \mathrm{GL}_l(R), b \in \mathrm{M}_{l,k}(R) \tag{1}$$

где $l = \mathrm{res}\ \sigma = \dim(M/P_\sigma) = n-k > m$. Очевидно, что вектор $\alpha_1 = (a_1, \ldots, a_l)$, являющийся первой строкой матрицы a, унимодулярен в R^l. Следовательно, найдутся элементы $b_1, \ldots, b_{l-1}$ кольца R такие, что вектор $\alpha_2 = (a_1 + b_1 a_l, a_2 + b_2 a_l, \ldots, a_{l-1} + b_{l-1} a_l)$ унимодулярен в R^{l-1} (учесть, что s-ранг кольца R меньше l).

Сопряжем матрицу $[\sigma]$ матрицей $t^{k+1}(0, \ldots, 0, b_1, b_2, \ldots, b_{l-1})$. Полученная матрица $[\sigma]_1$ будет иметь ту же блочную структуру, что и матрица (1), но в правом нижнем углу у нее будет стоять матрица a_1 с первой строкой вида $\alpha_3 = (\alpha_2, a_l)$. Так как вектор α_2 унимодулярен в R^{l-1}, то найдутся элементы $c_1, \ldots, c_{l-1}$ из R такие, что $\sum_{i=1}^{l-1} c_i a'_i = 1 - a_l$, где $a'_i = a_i + b_i a_l$. Умножим матрицу $[\sigma]_1$ справа на трансвекцию $t_{k+1,n}(c_1)$ и сопряжем получившуюся матрицу обобщенной трансвекцией $t^n(0, \ldots, 0, c_2, c_3, \ldots, c_{l-1})$. В результате опять получится матрица вида (1), у которой на месте $(k+1, n)$ стоит 1, а на месте $(k+1, k+1)$ — некоторый элемент $\eta \in R$. Сопрягая ее трансвекцией $t_{n,k+1}(1-\eta)$, получим 1 на месте $(k+1, k+1)$. Так как сопряжение матрицы означает переход к новому базису, а при сопряжении трансвекции опять получается трансвекция, то на самом деле мы показали, что для преобразования σ найдется трансвекция $\tau_1 \in \mathrm{GL}_n(M)$ такая, что преобразование $\sigma\tau_1$ в некоторой базе имеет матрицу вида

$$[\sigma\tau_1] = \left(\begin{array}{c|c} \mathbf{1}_k & \mathbf{0} \\ \hline \lambda_1, \ldots, \lambda_k & 1, \mu_2, \ldots, \mu_l \\ \hline * & * \end{array}\right) \in \mathrm{GL}_n(R), \quad \lambda_i, \mu_j \in R. \tag{2}$$

Выберем далее трансвекцию $\tau_2 \in \mathrm{GL}_n(M)$, которая в той же базе имеет матрицу $[\tau_2] = t_{k+1}(-\lambda_1, \ldots, -\lambda_k, -\mu_2, \ldots, -\mu_l)$. Тогда

$$[\sigma\tau_1\tau_2] = \left(\begin{array}{c|c} \mathbf{1}_{k+1} & \mathbf{0} \\ \hline * & * \end{array}\right) \in \mathrm{GL}_n(R).$$

Таким образом, преобразование $\sigma\tau_1\tau_2$ имеет неподвижный модуль размерности $k+1$ и его вычет равен $l-1$.

Предположим, что $\sigma_1 = \sigma\tau_1\tau_2$ — большая дилатация. Построим трансвекцию τ_3 такую, что произведение $\tau_2\tau_3$ является трансвекцией, а преобразование $\sigma_1\tau_3$ уже не является большой дилатацией. Пусть $e_1, \ldots, e_k$ — базис неподвижного модуля $P_{\sigma\tau_1}$, а $e_1, \ldots, e_{k+1}$ — базис неподвижного модуля P_{σ_1}. Вычетный модуль трансвекции τ_2, очевидно, порождается вектором $e_{k+1}\tau_2 - e_{k+1}$, который, вообще говоря, не является унимодулярным в R^n, но для которой найдется некоторое $\lambda \in F$ такое, что вектор $f_1 = \lambda(e_{k+1}\tau_2 - e_{k+1})$ унимодулярен в R^n. Так как M удовлетворяет условию дополняемости, то мы можем подобрать векторы $e_{k+3}, \ldots, e_n$ так, чтобы множество векторов $\{e_1, \ldots, e_{k+1}, f_1, e_{k+3}, \ldots, e_n\}$ образовывало базу M. Удалим из этого множества вектор e_{k+3}. Тогда оставшиеся векторы будут порождать некоторый подмодуль H. В качестве искомой трансвекции τ_3 выберем трансвекцию с неподвижным модулем H и вычетным модулем $P_{\tau_3} = R(e_{k+1}\tau_2 - e_{k+1})$. Так как вычетные модули трансвекций τ_2 и τ_3 совпадают, то по лемме 1 произведение $\tau_2\tau_3$ является трансвекцией. На векторах базы τ_3 действует следующим образом:

$$f_1\tau_3 = f_1,$$

$$e_{k+3}\tau_3 = e_{k+3} + (e_{k+1}\tau_2 - e_{k+1}),$$

$$e_i\tau_3 = e_i, \quad i = 1, \ldots, k+1, k+4, \ldots, n.$$

Так как $P_{\sigma\tau_1} \subseteq P_{\tau_2\tau_3}$, а $R_{\tau_2\tau_3} \not\subseteq P_{\sigma\tau_1}$, то ввиду леммы 2 преобразование $\sigma_1\tau_3 = \sigma\tau_1 \cdot \tau_2\tau_3$ не является большой дилатацией. Таким образом, полученное преобразование $\sigma_1\tau_3$ не является большой дилатацией и имеет вычет $l-1$. Ввиду индуктивного предположения, получаем требуемое разложение. Теорема доказана.

Как было замечено в конце предыдущего параграфа, всякая большая дилатация σ из $\mathrm{GL}_n(M)$ в некоторой базе имеет матрицу

$$[\sigma] = \left(\begin{array}{c|c} \mathbf{1}_k & \mathbf{0} \\ \hline a & u\mathbf{1}_l \end{array}\right) \in \mathrm{GL}_n(R), \quad l = \mathrm{res}\ \sigma, \quad u \in R^*. \tag{3}$$

Очевидно, что она является произведением $\leq l$ простых преобразований. Мы же докажем следующее утверждение, являющееся обобщением теоремы Дьедонне для больших дилатаций.

Теорема 2. *Пусть R — ассоциативное кольцо с единицей, являющееся областью целостности, и свободный модуль $M = R^n$ удовлетворяет условию дополняемости. Тогда всякая большая дилатация σ из $\mathrm{GL}_n(M)$ с вычетом $l = \mathrm{res}\ \sigma > 1$ представима в виде произведения l трансвекций и одного простого преобразования, которое является трансвекцией, если $\sigma \in \mathrm{SL}_n(M)$, и является дилатацией в противном случае, причем меньшего числа трансвекций недостаточно.*

Доказательство. Будем считать, что в некоторой базе $e_1, \ldots, e_n$ преобразование σ имеет матрицу (3). Подберем трансвекцию τ_1 так, чтобы в этой же базе она имела матрицу

$$t^n(\underbrace{0, \ldots, 0}_{k}, \underbrace{u^{-1}, \ldots, u^{-1}}_{l-1}).$$

Тогда матрица $[\sigma\tau_1]$ будет содержать в последнем столбце на местах с $(k+1)$–го до $(n-1)$–го единицы. Пусть, далее, трансвекция τ_2 имеет матрицу $t_{n,k+1}(1-u)$. Тогда матрица преобразования $\tau_2^{-1}\sigma\tau_1\tau_2$ имеет вид

$$[\tau_2^{-1}\sigma\tau_1\tau_2] = \left(\begin{array}{c|c} \mathbf{1}_k & \mathbf{0} \\ \hline a_1 & b \end{array}\right), \quad \text{где} \quad b = \left(\begin{array}{c|c|c} 1 & 0\ldots 0 & 1 \\ \hline 1-u & & 1 \\ \vdots & u\mathbf{1}_{l-2} & \vdots \\ 1-u & & 1 \\ \hline -(1-u)^2 & 0\ldots 0 & 2u-1 \end{array}\right) \in \mathrm{GL}_l(R).$$

Выберем, наконец, трансвекцию τ_3, имеющую в нашем базисе матрицу $t_{k+1}(-a_{11}, \ldots, -a_{1k}, \underbrace{0, \ldots, 0}_{l-2}, -1)$, где $a_{i,j}$ — соответствующие элементы матрицы a_1. Тогда

$$[\sigma_1] = [\tau_2^{-1}\sigma\tau_1\tau_2\tau_3] = \left(\begin{array}{c|c|c} & & 0 \\ \mathbf{1}_{k+1} & \mathbf{0} & \vdots \\ & & 0 \\ \hline & & u \\ & u\mathbf{1}_{l-2} & \vdots \\ a_2 & & u \\ & 0\ldots 0 & u^2 \end{array}\right)$$

и преобразование σ_1 имеет вычет $l-1$. Если $l=2$, то мы тем самым представили исходное преобразование σ в виде произведения двух трансвекций и одного простого преобразования, которое является трансвекцией при $u^2=1$ и является дилатацией в противном случае.

Допустим, что $l>2$. Выберем преобразование ρ, имеющее матрицу

$$t_{k+2,n}(u^{-1})t_{n,k+2}(1-u),$$

и сопряжем им преобразование σ_1, получим

$$[\rho^{-1}\sigma_1\rho] = \left(\begin{array}{c|c} \mathbf{1}_{k+1} & \mathbf{0} \\ \hline a_3 & b_1 \end{array}\right), \quad \text{где} \quad b_1 = \left(\begin{array}{c|c|c} 1 & 0\ldots 0 & 1 \\ \hline u-u^2 & & u \\ \vdots & u\mathbf{1}_{l-3} & \vdots \\ u-u^2 & & u \\ \hline v & 0\ldots 0 & v+u^3 \end{array}\right) \in \mathrm{GL}_{l-1}(R),$$

$$v = -u^3+u^2+u-1.$$

Далее, подбираем трансвекцию τ_4 с матрицей

$$[\tau_4] = t_{k+2}(-a'_{11}, \ldots, -a'_{1,k+1}, \underbrace{0, \ldots, 0}_{l-3}, -1),$$

где $a'_{i,j}$ — соответствующие элементы матрицы a_3. Тогда преобразование $\sigma_2 = \rho^{-1}\sigma_1\rho\tau_4$ имеет матрицу

$$[\sigma_2] = \left(\begin{array}{c|c|c} \mathbf{1}_{k+2} & \mathbf{0} & 0 \\ \hline & & u^2 \\ & u\mathbf{1}_{l-3} & \vdots \\ * & & u^2 \\ & 0\dots 0 & u^3 \end{array}\right).$$

Если $l-3=0$, то мы получим разложение преобразования σ в произведение трех трансвекций и одного простого преобразования, которое является трансвекцией, если $u^3 = 1$, и является дилатацией в противном случае. Если же $l-3>0$, то, проводя преобразования, аналогичные описанным выше, в конце концов получим требуемое разложение.

Заключительное утверждение теоремы следует из того, что группа $\mathrm{GL}_n(M)$ вложена в группу $\mathrm{GL}_n(V)$, где V — n–мерное векторное пространство над полем частных кольца R, а в группе $\mathrm{GL}_n(V)$ никакая большая дилатация σ не разложима в произведение $<\operatorname{res}\sigma$ трансвекций и одного простого преобразования [7, предложение 2.1.6]. Теорема доказана.

§ 3. Случай $R = \mathbb{Z}$

В настоящем параграфе мы рассмотрим автоморфизмы свободного $\mathbb{Z}$–модуля $M = \mathbb{Z}^n$, $n \geq 3$. Пусть σ — некоторое преобразование из $\mathrm{GL}_n(M)$. Если σ является большой дилатацией, то σ представима в виде произведения простых преобразований по теореме 2. Поэтому далее будем считать, что σ не является большой дилатацией. Так как ранг стабильности кольца $\mathbb{Z}$ равен 2, то по теореме 1, существует разложение $\sigma = \sigma_0\tau_1\tau_2\dots\tau_{2(n-2)}$, где τ_i — трансвекция, а σ_0 — преобразование с вычетом $\operatorname{res}\sigma_0 \leq 2$. Если $\operatorname{res}\sigma_0 \leq 1$, то σ_0 является либо трансвекцией, либо дилатацией и поэтому мы имеем разложение σ в произведение простых преобразований. Поэтому будем считать, что $\operatorname{res}\sigma_0 = 2$, и мы хотим разложить σ_0 в произведение простых преобразований. Так как $\mathbb{Z}$ удовлетворяет условию дополняемости, то в некоторой базе преобразование σ_0 имеет матрицу следующего вида

$$A = \left(\begin{array}{c|cc} \mathbf{1}_{n-2} & \multicolumn{2}{c}{\mathbf{0}} \\ \hline & a & b \\ * & & \\ & c & d \end{array}\right), \quad a,b,c,d \in \mathbb{Z}; \quad ad-bc = \pm 1. \tag{1}$$

Учитывая связь между простыми преобразованиями и простыми матрицами, достаточно разложить матрицу A в произведение простых матриц (которые мы также будем называть трансвекциями и дилатациями) в случае $n=3$.

Для всякой матрицы $X \in \mathrm{GL}_n(\mathbb{Z})$ через $\nu_n(X)$ будем обозначать наименьшее $m \in \mathbb{N}$ такое, что X — произведение m простых матриц.

В работе [18] доказано, что если в матрице A вместо клетки, отмеченной звездочкой, стоит нулевая клетка, и $A \in \mathrm{SL}_3(\mathbb{Z})$, то $\nu_3(A) \leq 43$, правда, авторы [18] разлагали матрицу A в произведение элементарных трансвекций. Подправив соответствующим образом их доказательство, мы покажем, что $\nu_3(A) \leq 10$. Для доказательства этого факта нам потребуется следующая лемма.

Лемма 5. *Пусть e — неотрицательное целое число и*

$$P = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \alpha & \beta \\ 0 & \gamma & \delta \end{pmatrix}, \qquad Q = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \alpha^e & \beta \\ 0 & x & y \end{pmatrix}$$

– матрицы из $\mathrm{SL}_3(\mathbb{Z})$*. Тогда найдутся целые числа* κ_1 *и* κ_2 *и векторы* $v_1, \ldots, v_8$ *из* $\mathbb{Z}^2$*такие, что*

$$P^e = (Qt_{32}(\kappa_1))^{t_3(v_1)}(t_1(v_2))^{t^1(v_3)}(t^2(v_4))^{t^1(v_5)}t^1(v_6)(t_2(v_7))^{t_{3,1}(\kappa_2)}t_1(v_8).$$

Доказательство. В случае если один из элементов α, β, γ или δ равен нулю, утверждение тривиально. Поэтому мы будем считать, что все эти коэффициенты отличны от нуля.

Положим

$$L = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

По теореме Гамильтона–Кэли, матрица L удовлетворяет уравнению $L^2 = -I + \mathrm{tr}(L) \cdot L$, где I — единичная матрица из $\mathrm{SL}_2(\mathbb{Z})$. Легко заметить, что и для всякого целого положительного $m \geq 2$ найдутся целые числа f_m и g_m, для которых

$$L^m = f_m I + g_m L. \tag{2}$$

Действительно, если f_{m-1} и g_{m-1} уже найдены, то

$$L^m = L^{m-1}L = (f_{m-1}I + g_{m-1}L)L =$$

$$= f_{m-1}L + g_{m-1}L^2 = f_{m-1}L + g_{m-1}(-I + \mathrm{tr}(L) \cdot L) = -g_{m-1}I + (f_{m-1} + g_{m-1}\mathrm{tr}(L))L,$$

и достаточно положить $f_m = -g_{m-1}$, $g_m = f_{m-1} + g_{m-1}\mathrm{tr}(L)$.

Обозначим $f = f_e$, $g = g_e$. Так как $1 = \det(L^e) \equiv \det(gL) \equiv g^2(\mathrm{mod} f)$, то f делит $g^2 - 1 = (g+1)(g-1)$. Положим

$$\begin{aligned} &f = f^+ f^-, \qquad f^+, f^- \in \mathbb{Z}, \\ &g + 1 = jf^+, \quad g - 1 = kf^-, \quad k, j \in \mathbb{Z}. \end{aligned}$$

Непосредственные вычисления приводят к равенству

$$R = (t_1(-1, k))^{t_{31}(-f^-)}t^1(1 - f^+, f^-)t^2(j, -f^-) = \begin{pmatrix} * & 1 & * \\ * & * & 0 \\ f & 0 & g \end{pmatrix}.$$

Используя элементарные преобразования матрицы R, легко проверяется равенство

$$S = t_{21}(\lambda)Rt_{31}(\alpha)t_{23}(\mu)t_{21}(\eta) = \begin{pmatrix} * & * & * \\ -\beta & 1 & 0 \\ f + g\alpha & 0 & g \end{pmatrix},$$

где $\lambda = -j(1 - f^+)$, $\mu = kj(1 - f^+)$, $\eta = (1 - f^+)(g + j\alpha k) - \beta$.

Используя свойства обобщенно элементарных трансвекций (лемма 3), представим S в виде произведения четырех простых матриц:

$$S = (t_1(w_1))^{t^1(w_1)}(t^2(j, -f^-))^{t^1(w_2)}t^1(w_3)t_2(\eta, \mu),$$

где $w_1 = (-\lambda, -f^-)$, $w_2 = (f^+ - 1 - \lambda, -f^-)$, $w_3 = (1 - f^+ + \lambda, \alpha + f^-)$.

Заметим далее, что при кольцевом гомоморфизме $\mathbb{Z} \longrightarrow \mathbb{Z}/\beta\mathbb{Z}$ матрицы P и P^e перейдут в треугольные матрицы и, следовательно, ввиду соотношения (2) справедливо сравнение $f + g\alpha \equiv \alpha^e (\mathrm{mod}\ \beta)$. Поэтому существует некоторое целое число k для которого

$$C = Qt_{32}(k) = \begin{pmatrix} 1 & 1 & 0 \\ 0 & f+g\alpha & \beta \\ 0 & s & y \end{pmatrix}.$$

Матрицу

$$U = CS = \begin{pmatrix} * & * & * \\ 0 & f+g\alpha & \beta \\ 1 & * & * \end{pmatrix}$$

сопряжем элементарной трансвекцией $t_{31}(\lambda_1)$, где λ_1 подберем так, чтобы получившаяся матрица U_1 имела следующий вид:

$$U_1 = U^{t_{31}(\lambda_1)} = \begin{pmatrix} 1 & \mu_1 & \eta_1 \\ 0 & f+g\alpha & \beta \\ 1 & * & * \end{pmatrix}$$

для некоторых целых μ_1 и η_1. Умножим ее слева на $t_{31}(-1)$, а справа на $t_1(-\mu_1, -\eta_1)$, получим матрицу

$$U_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & f+g\alpha & \beta \\ 0 & * & * \end{pmatrix}.$$

Легко заметить, что если матрицы M и N из $\mathrm{SL}_2(\mathbb{Z})$ имеют одинаковые первые строки, т. е.

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad N = \begin{pmatrix} a & b \\ c_1 & d_1 \end{pmatrix},$$

то найдется некоторое целое число l такое, что $(c, d) = (c_1 + la, d_1 + lb)$. Поэтому мы можем найти целое число k_1 такое, что произведение $t_{3,2}(k_1)U_2$ равно матрице P^e. Таким образом,

$$P^e = t_{31}(-1)t_{32}(k_1)(CS)^{t_{31}(\lambda_1)}t_1(-\mu_1, \eta_1).$$

Вспоминая представление матрицы CS в виде произведения простых матриц и учитывая, что матрицы $t^1(v)$ и $t_{31}(\lambda_1)$ перестановочны, получим

$$P^e = t_{3,1}(-1)t_{3,2}(k_1)(Qt_{3,2}(k))^{t_{3,1}(\lambda_1)}(t_1(w_1)^{t^1((w_1')}(t^2(j,-f^-))^{t^1(w_2')}t^1(w_3)(t_2(\eta,\mu))^{t_{3,1}(\lambda_1)}t_1(-\mu_1,\eta_1),$$

где $w_i' = w + (0, \lambda_1)$, $i = 1, 2$. Запишем это разложение в таком виде:

$$P^e = t_{31}(-1)P_1 t^1(w_3)P_2,$$

где

$$P_1 = t_{32}(k_1)(Qt_{32}(k))^{t_{31}(\lambda_1)}(t_1(w_1))^{t^1(w_1')}(t^2(j,-f^-))^{t^1(w')},$$
$$P_2 = (t_2(\eta,\mu))^{t_{31}(\lambda_1)}t_1(-\mu_1,\eta_1).$$

По лемме 3, д)

$$P^e = P_1^{t_{31}(1)} t^1(w_3') P_2,$$

где $w_3' = w_3 - (0,1)$. Обозначим

$$P_3 = \left((t_1(w_1))^{t^1(w_1')} (t^2(j, -f^-))^{t^1(w_2')} \right)^{t_{31}(1)} t^1(w_3') P_2.$$

Тогда

$$P^e = t_{32}(k_1)(Qt_{32}(k))^{t_{31}(\lambda_1+1)} P_3.$$

Учитывая, что трансвекции $t_{32}(x)$ и $t_{31}(y)$ перестановочны, ввиду леммы 3, д), можем уменьшить число простых матриц в разложении P^e:

$$P^e = (Qt_{32}(\lambda_2))^{t_3(w_4)} P_3,$$

где $\lambda_2 = k + k_1$, $w_4 = (\lambda_1 + 1, -k_1)$. Подставив в выражение для P_3, окончательно получим:

$$P^e = (Qt_{32}(\lambda_2))^{t_3(w_4)} (t_1(w_1))^{t^1(w_2)} (t^2(j, -f^-))^{t^1(w_5)} t^1(w_3') (t_2(\eta, \mu))^{t_{3,1}(\lambda_1)} t_1(-\mu_1, \eta_1).$$

Лемма доказана.

Используя эту лемму, докажем следующее утверждение

Лемма 6. *Всякая матрица*

$$A = \begin{pmatrix} 1 & 0 & 0 \\ * & a & b \\ * & c & d \end{pmatrix} \in \mathrm{GL}_3(\mathbb{Z})$$

представима в виде произведения ≤ 10 *простых матриц. Если же* $\det A = 1$, *то эти матрицы можно подобрать так, чтобы они являлись трансвекциями.*

Доказательство. Будем считать, что A не является ни большой дилатацией ни трансвекцией, так как в этом случае утверждение тривиально. Используя, если надо, попеременное сопряжение матрицы A элементарными трансвекциями $t_{23}(\lambda_i)$ и $t_{32}(\mu_i)$ при подходящих целых числах λ_i и μ_i, можно считать, что матрица A имеет такой вид

$$A = \begin{pmatrix} 1 & 0 & 0 \\ h & a & b \\ 0 & c & d \end{pmatrix}.$$

Очевидно, что если хотя бы один из коэффициентов a, b, c или d равен 0, то $\nu_3(A) \leq 2$. Поэтому мы будем считать, что все эти коэффициенты отличны от нуля. Если A не лежит в группе $\mathrm{SL}_3(\mathbb{Z})$, то домножим ее слева на дилатацию $d_1 = \mathrm{diag}(1, -1, 1)$. Тогда полученная матрица $A_1 = d_1 A$ имеет определитель, равный 1. Далее, чтобы избавиться от коэффициента стоящего на месте $(2,1)$, умножим нашу матрицу слева на трансвекцию $t_{2,1}(\pm h)$. Получим матрицу вида

$$A_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & * & * \\ 0 & * & * \end{pmatrix} \in \mathrm{SL}_3(\mathbb{Z}).$$

Теперь мы хотим добиться того, чтобы в нашей матрице на месте $(2,3)$ стоял нечетный коэффициент. Если это не так, то коэффициент стоящий на месте $(3,3)$ в матрице A_2 нечетен.

Умножим A_2 слева на $t_{23}(1)$, получим матрицу $A_3 = t_{23}(1)A_2 = t_{23}(1)t_{21}(h)d_1A$ у которой коэффициент $(2,3)$ нечетен. Более того, переходя, если надо, к обратной матрице, мы будем считать, что этот коэффициент сравним с 3 по модулю 4.

В работе [18] доказано, что для такой матрицы A_3 можно так подобрать целые числа m_1 и m_2, что матрица

$$H = t_{32}(m_1)t_{23}(m_2)A_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & u & p \\ 0 & q & v \end{pmatrix}$$

обладает следующими свойствами: коэффициенты p и q – положительные простые числа, $\frac{1}{2}(p-1)$ не делится нацело на 2 и числа $\frac{1}{2}(p-1)$, $q-1$ взаимно просты. Следовательно, найдутся такие целые положительные числа ρ и σ, что $\frac{1}{2}(p-1)\rho - (q-1)\sigma = 1$. Поэтому матрицу H можно представить в виде произведения

$$H = H^{\frac{1}{2}(p-1)\rho}H^{-(q-1)\sigma}.$$

Далее, пользуясь леммой 5, мы представим матрицу H в виде произведения простых матриц и уже из этого представления найдем требуемое разложение для матрицы A.

Представим вначале матрицу $H^{\frac{1}{2}(p-1)\rho}$ в виде произведения простых матриц. Ввиду теоремы Ферма (см., например, [23, с. 44]) справедливо сравнение

$$u^{(p-1)\rho} \equiv 1(\mathrm{mod}\ p).$$

Следовательно, $u^{\frac{1}{2}(p-1)\rho} \equiv \pm 1(\mathrm{mod}\ p)$. Если $u^{\frac{1}{2}(p-1)\rho}$ сравнимо с 1, то для некоторого целого α имеет место равенство $u^{\frac{1}{2}(p-1)\rho} - 1 = \alpha p$. Положим

$$B_1 = t_{2,3}(p)t_{3,2}(\alpha) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1+\alpha p & p \\ 0 & \alpha & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & u^{\frac{1}{2}(p-1)\rho} & p \\ 0 & \alpha & 1 \end{pmatrix}.$$

По лемме 5

$$H^{\frac{1}{2}(p-1)\rho} = (t_{23}(p)t_{32}(\alpha+\zeta_1))^{t_3(u_1)}(t_1(u_2))^{t^1(u_3)}(t^2(u_4))^{t^1(u_5)}t^1(u_6)(t_2(u_7))^{t_{31}(\zeta_2)}t_1(u_8)$$

для некоторых целых ζ_1 и ζ_2 и векторов u_i из $\mathbb{Z}^2$. Покажем, что на самом деле, $\nu_3(H^{\frac{1}{2}(p-1)\rho}) \leq 5$. Ввиду леммы 3, в)

$$(t_2(u_7))^{t_{31}(\zeta_2)} = t_2(u_7')$$

для некоторого вектора u_7' из $\mathbb{Z}^2$, кроме того, заметим, что произведение $t^1(u_6)t_2(u_7')$ равно произведению $t_2(u_6')t_{31}(\zeta_3)$ для некоторого ζ_3 и вектора u_6'. Следовательно,

$$H^{\frac{1}{2}(p-1)\rho} = (t_{23}(p))^{t_3(u_1)}t_{32}(\alpha+\zeta_1)(t_1(u_2))^{t^1(u_3)}(t^2(u_4))^{t^1(u_5)}t_2(u_6')t_{31}(\zeta_3)t_1(u_8).$$

Положим, далее, $u_9 = (\zeta_3, \alpha+\zeta_1)$, $u_3' = u_3 + (\zeta_3, 0)$, $w_5' = w_5 + (\zeta_3, 0)$ и, перенося соответствующие матрицы (по лемме 3, д)), получим разложение на 6 простых матриц:

$$H^{\frac{1}{2}(p-1)\rho} = (t_{23}(p))^{t_3(u_1)}t_3(u_9)(t_1(u_2))^{t^1(u_3')}(t^2(u_4))^{t^1(u_5')}(t_2(u_6'))^{t_{31}(\zeta_3)}t_1(u_8).$$

Найдем вектор u_6'' из равенства $(t_2(u_6'))^{t_{31}(\zeta_3)} = t_2(u_6'')$. Сравнивая векторы u_3' и u_5', замечаем, что их вторые компоненты совпадают, а первые — отличаются на некоторое число ζ_4. Следовательно, $t^1(u_5') = t^1(u_3')t_{12}(\zeta_4)$, и ввиду перестановочности $t^2(u_4)$ и $t_{12}(\zeta_4)$ имеем

$$(t_1(u_2))^{t^1(u_3')}(t^2(u_4))^{t^1(u_5')} = (t_1(u_2)t^2(u_4))^{t^1(u_5')}.$$

Преобразуем правую часть этого равенства, используя соотношения

$$t_1(u_2)t^2(u_4) = t_1(u_2')t_{32}(\zeta_5), \quad (t_{32}(\zeta_5))^{t^1(u_5')} = t_3(u_5''),$$

справедливые при некотором целом ζ_5 и целочисленных векторах u_2' и u_5'', получим

$$(t_1(u_2))^{t^1(u_3')}(t^2(u_4))^{t^1(u_5')} = (t_1(u_2'))^{t^1(u_5')}t_3(u_5'').$$

Отсюда

$$H^{\frac{1}{2}(p-1)\rho} = (t_{23}(p))^{t_3(u_1)}t_3(u_9)(t_1(u_2'))^{t^1(u_5')}t_3(u_5'')t_2(u_6'')t_1(u_8).$$

Объединяя трансвекции $t_3(u_9)$ и $t_3(u_5'')$, по лемме 3, д), получим искомое разложение

$$H^{\frac{1}{2}(p-1)\rho} = (t_{23}(p))^{t_3(u_1)}t_3(u_9')(t_1(u_2'))^{t^1(u_5')t_3(u_5'')},$$

где $u_9' = u_9 + u_5''$.

Если же $u^{\frac{1}{2}(p-1)\rho} \equiv -1 (\mathrm{mod}\ p)$, то для некоторого α выполнено равенство

$$u^{\frac{1}{2}(p-1)\rho} + 1 = \alpha p.$$

В этом случае полагаем

$$B_1 = (t_{32}(-1))^{t_{23}(-2)}t_{2,3}(4-p)t_{32}(\alpha) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & u^{\frac{1}{2}(p-1)\rho} & p \\ 0 & 0 & p-1 \end{pmatrix}$$

и, проводя те же рассуждения, что и выше, найдем разложение

$$H^{\frac{1}{2}(p-1)\rho} = (t_{32}(-1))^{t_{23}(-2)t_3(u_1)}(t_{23}(4-p))^{t_3(u_1)}t_3(u_2)(t_1(u_3))^{t^1(u_4)t_3(u_5)}t_2(u_6)t_1(u_7)$$

для некоторых векторов $u_1, \ldots, u_7$ из $\mathbb{Z}^2$.

Найдем теперь разложение матрицы $H^{-(q-1)\sigma}$ в произведение простых матриц. Опять по теореме Ферма найдем целое число β, для которого $v^{(q-1)\sigma} - 1 = \beta q$, и положим

$$B_2 = t_{23}(-q)t_{32}(-\beta) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & v^{(q-1)\sigma} & -q \\ 0 & -\beta & 1 \end{pmatrix}.$$

Далее, по лемме 5 найдем разложение матрицы

$$B_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & v & -q \\ 0 & -p & u \end{pmatrix}^{(q-1)\sigma}$$

в произведение простых матриц. Проводя те же рассуждения, что и выше, заметим, что $\nu_3(B_3) \le 5$, и, наконец, воспользовавшись тем, что $H^{-(q-1)\sigma} = B_3^T$, получим искомое разложение

$$H^{-(q-1)\sigma} = t^1(w_1)t^2(w_2)(t^1(w_3))^{t^3(w_4)t_1(w_5)}t^3(w_6)(t_{32}(\xi))^{t^3(w_7)},$$

где w_i — некоторые векторы из $\mathbb{Z}^2$, а $\xi \in \mathbb{Z}$.

Вспоминаем, что

$$H = t_{32}(m_1)t_{23}(m_2)A_3 = t_{32}(m_1)t_{23}(m_2+1)A_2 = t_{32}(m_1)t_2(v)d_1A,$$

где $v = (h, m_2+1)$, а для конкретной матрицы A некоторые простые матрицы могут отсутствовать. Отсюда

$$A = d_1t_2(-v)t_{32}(-m_1)H^{\frac{1}{2}(p-1)\rho}H^{-(q-1)\sigma}.$$

Подставим разложения $H^{\frac{1}{2}(p-1)\rho}$ и $H^{-(q-1)\sigma}$ в произведение простых матриц, причем для первой из них возьмем разложение из второго случая, так как он является более общим. Получим

$$A = d_1t_2(-v)t_{32}(-m_1)(t_{32}(-1))^{t_{23}(-2)t_3(u)}\times$$
$$\times(t_{23}(4-p))^{t_3(u_1)}t_3(u_2)(t_1(u_3))^{t^1(u_4)t_3(u_5)}t_2(u_6)t_1(u_7)\times$$
$$\times t^1(w_1)t^2(w_2)(t^1(w_3))^{t^3(w_4)t_1(w_5)}t^3(w_6)(t_{32}(\xi))^{t^3(w_7)}.$$

Покажем, что на самом деле $\nu_3(A) \leq 10$.

По лемме 3, д) перенесем $t_{32}(-m_1)$ вправо так, чтобы она оказалась рядом с $t_3(u_2)$. Их произведение $t_{32}(-m_1)t_3(u_2) = t_3(u_2')$ для некоторого вектора u_2'. Кроме того, произведение $t_3(u_1)t_{32}(m_1)$ объединим в одну матрицу $t_3(u_1')$. Заметим далее, что произведение $t_2(u_6)t_1(u_7)t^1(w_1)$ равно произведению

$$t_2(u_6')(t_1(u_7'))^{t_{21}(\xi_1)}t_{31}(\xi_2)$$

для некоторых векторов u_6' и u_7' из $\mathbb{Z}^2$ и некоторых чисел ξ_1, $\xi_2 \in \mathbb{Z}$. Следовательно,

$$A = d_1t_2(-v)(t_{32}(-1))^{t_{23}(-2)t_3(u_1')}(t_{23}(4-p))^{t_3(u_1')}t_3(u_2')\times$$
$$\times(t_1(u_3))^{t^1(u_4)t_3(u_5)}t_2(u_6')(t_1(u_7'))^{t_{21}(\xi_1)}t_{31}(\xi_2)t^2(w_2)\times$$
$$\times(t^1(w_3))^{t^3(w_4)t_1(w_5)}t^3(w_6)(t_{32}(\xi))^{t^3(w_7)}.$$

В этом разложении по лемме 3, д) перенесем матрицу $t_{31}(\xi_2)$ влево и положим $t_3(u_2'') = t_3(u_2')t_{31}(\xi_2)$. Тогда

$$A = C_1t_3(u_2'')(t_1(u_3))^{t^1(u_4)t_3(u_5')}t_2(u_6'')(t_1(u_7'))^{t^1(u_8)}t^2(w_2)C_2,$$

где через C_i обозначены соответствующие произведения простых матриц, а векторы u_5', u_6'', u_8 найдем из равенств

$$t_3(u_5') = t_3(u_5)t_{31}(\xi_2), \quad t_2(u_6'') = (t_2(u_6'))^{t_{31}(\xi_2)}, \quad t^1(u_8) = t_{21}(\xi_1)t_{31}(\xi_2).$$

Аналогично, перенося трансекцию $t_2(u_6'')$ влево и замечая, что матрица $d = d_1t_2(-v)t_2(u_6'') = d_1t_2(u_6''-v)$ является дилатацией, получим искомое разложение матрицы A. Таким образом, лемма 6 доказана.

Из этой леммы, ввиду теорем 1 и 2 легко выводится

Теорема 3. *Пусть $n \geq 3$. Всякий автоморфизм σ свободного $\mathbb{Z}$–модуля $M = \mathbb{Z}^n$ представим в виде произведения не более $2n+5$ трансвекций и одного простого преобразования, которое является трансвекцией, если $\sigma \in \mathrm{SL}_n(M)$, и дилатацией в противном случае.*

Рассмотрим теперь ширину группы $\mathrm{SL}_n(\mathbb{Z})$ при $n \geq 3$ относительно множества коммутаторов. Ввиду того, что всякая трансвекция модуля $\mathbb{Z}^n$ при $n \geq 3$ является коммутатором, из теоремы 3 непосредственно следует, что эта ширина не превосходит $2n+6$. Мы же сейчас дадим более точную оценку, которая не зависит от n.

Следствие. *Всякая матрица из* $\mathrm{SL}_n(\mathbb{Z})$, $n \geq 3$, *представима в виде произведения не более 10 коммутаторов из* $\mathrm{SL}_n(\mathbb{Z})$.

Доказательство. Пусть X — произвольная матрица из $\mathrm{SL}_n(\mathbb{Z})$, $n \geq 3$. Ввиду леммы 4

$$X = u_1 l_1 \begin{pmatrix} \mathbf{1}_{n-3} & 0 \\ 0 & A_2 \end{pmatrix} u_2 l_2,$$

где u_i, l_i — унитреугольные матрицы из $\mathrm{SL}_n(\mathbb{Z})$, а $A_2 \in \mathrm{SL}_3(\mathbb{Z})$ и имеет тот же вид, что и в доказательстве последней леммы. Следовательно, для нее мы имеем следующее разложение:

$$A_2 = t_{23}(\lambda_1) t_{32}(\mu_1) C (t_{23}(\lambda_2))^{t_3(\alpha_1)} t_3(\alpha_2) \times$$
$$\times (t_1(\beta_1))^{t^1(\alpha_3) t_3(\alpha_4)} t_2(\gamma_1) t_1(\beta_2) t^1(\alpha_5) t^2(\gamma_2) \times$$
$$\times (t^1(\alpha_6))^{t^3(\alpha_7) t_1(\beta_3)} t^3(\alpha_8) (t_{32}(\mu_2))^{t^3(\alpha_9)},$$

где λ_i, μ_i — целые числа, α_j, β_k, γ_l — некоторые векторы из $\mathbb{Z}^2$, а

$$C = (t_{32}(\mu_3))^{t_{23}(\lambda_3) t_3(\alpha_{10})}$$

– матрица, сопряженная с элементарной трансвекцией. В силу того, что всякая элементарная трансвекция является коммутатором, матрица C также представима в виде коммутатора. Перепишем это разложение в таком виде:

$$A_2 = C_1 t_{23}(\lambda_1) t_{32}(\mu_1) (t_{23}(\lambda_2))^{t_3(\alpha_1)} t_3(\alpha_2) \times$$
$$\times (t_1(\beta_1))^{t^1(\alpha_3) t_3(\alpha_4)} t_2(\gamma_1) t_1(\beta_2) t^1(\alpha_5) t^2(\gamma_2) \times$$
$$\times (t^1(\alpha_6))^{t^3(\alpha_7) t_1(\beta_3)} t^3(\alpha_8) (t_{32}(\mu_2))^{t^3(\alpha_9)},$$

где $C_1 = C^{t_{32}(-\mu_1) t_{23}(-\mu_1)}$. Далее мы хотим представить произведение трансвекций, стоящих после C_1, в виде произведения унитреугольных матриц. Для этого разложим трансвекции $t_2(\gamma_1)$ и $t^2(\gamma_2)$ в произведение элементарных трансвекций:

$$t_2(\gamma_1) = t_{21}(\xi_1) t_{23}(\xi_2), \quad t^2(\gamma_2) = t_{32}(\xi_4) t_{12}(\xi_3),$$

$\gamma_1 = (\xi_1, \xi_2)$, $\gamma_2 = (\xi_3, \xi_4)$, а также обозначим:

$$u_3 = t_{23}(\lambda_1), \qquad l_3 = t_{32}(\mu_1) t_3(-\alpha_1),$$

$$u_4 = t_{23}(\lambda_2), \qquad l_4 = t_3(\alpha_1) t_3(\alpha_2) t_3(-\alpha_4) t^1(-\alpha_3),$$

$$u_5 = t_1(\beta_1), \qquad l_5 = t^1(\alpha_3) t_3(\alpha_4) t_{21}(\xi_1),$$

$$u_6 = t_{23}(\xi_2) t_1(\beta_2), \qquad l_6 = t^1(\alpha_5) t_{32}(\xi_4),$$

$$u_7 = t_{12}(\xi_3) t_1(-\beta_3) t^3(-\alpha_7), \qquad l_7 = t^1(\alpha_6),$$

$$u_8 = t^3(\alpha_7) t_1(\beta_3) t^3(\alpha_8) t^3(-\alpha_9), \quad l_8 = t_{32}(\mu_2),$$

$$u_9 = t^3(\alpha_9).$$

Следовательно,

$$A_2 = C_1 \left(\prod_{i=3}^{8} (u_i l_i) \right) u_9,$$

где, как легко заметить, все матрицы u_i являются верхнеунитреугольными, а l_i — нижнеунитреугольными. Из этого разложения легко получить разложение матрицы X в виде произведения коммутатора и 16 унитреугольных матриц. Так как всякая матрица представленная в виде произведения m унитреугольных матриц может быть представлена в виде произведения $\leq [m/2]+1$ коммутаторов [24, следствие 14], то матрица X представима в виде произведения ≤ 10 коммутаторов. Следствие доказано.

Отметим в заключение, что оценка, полученная в теореме 3, является, по-видимому, довольно грубой. Интересно было бы получить точное значение ширины. Обобщить теорему 3 на все кольца s-ранга 2 и даже на все евклидовы кольца уже нельзя, так как ширина коммутанта группы группы $\mathrm{SL}_n(\mathbb{C}[x])$, $n \geq 2$, бесконечна [15]. Но можно попробовать обобщить теорему 3 на случай произвольного кольца целых чисел некоторого алгебраического числового поля, подобно тому, как это сделано для элементарных трансвекций в работе [3]

Список литературы

[1] Каргаполов М. И., Мерзляков Ю. И. Основы теории групп, 3–е изд., М., Наука, 1982.

[2] Мерзляков Ю. И. Алгебраические линейные группы как полные группы автоморфизмов и замкнутость их вербальных подгрупп, Алгебра и логика, 6, № 1 (1967), 83–94.

[3] Carter D., Keller G. Bounded elementary generation of $\mathrm{SL}_n(\acute{O})$, Amer. J. Math., 103, № 3 (1983), 673–687.

[4] Закирьянов К. Х. Конечность ширины симплектической группы над кольцами алгебраических чисел относительно элементарных матриц, Алгебра и логика, 24, № 6 (1985), 667–673.

[5] Тавгень О. Н. Ограниченная порождаемость групп Шевалле над кольцами S–целых алгебраических чисел, Известия АН СССР, Сер. математическая, 54, № 1 (1990), 97–122.

[6] Van der Kallen W. $\mathrm{SL}_3(\mathbb{C}[x])$ does not have bounded word length, Lect. Notes in Math. Berlin-New York: Springer-Verlag, 366, 1982, 357–361.

[7] О'Мира О. Лекции о линейных группах. В сб. статей: Автоморфизмы классических групп. М.:Мир, 1976, 57–167.

[8] Ellers E., Lausch H. Generators for classical groups of moduls over local rings, J. Geometry, 39, № 1–2 (1990), 60–79.

[9] Djokovic D. Z. Characterization of dilatations which are expressible as a product of three transvections or three reflections, Proc. Amer. Math. Soc., 92, № 3 (1984), 315–319.

[10] Коробов А. А. О разложении простого преобразования в произведение простых преобразований с заданными параметрами. В сб. статей: Некоторые проблемы дифференциальных уравнений и дискретной математики. Новосибирск, 1986, 28–33.

[11] Мерзляков Ю. И. Рациональные группы, М.: Наука, 1980.

[12] Thompson R. C. Commutators in the special linear and general linear groups, Trans. Amer. Math. Soc., 101, № 1 (1961), 16–33.

[13] Gow R. Commutators in the symplectic groups, Arch. Math., 50, № 3 (1988), 204–209.

[14] Newman M. Unimodular commutators, Proc. Amer. Math. Soc., 101, № 4 (1987), 605–609.

[15] Dennis R. K., Vaserstein L. N. On a question of M. Newman on the number of commutators, J. Algebra, 118, № 1 (1988), 150–161.

[16] Васерштейн Л. Н. Стабильный ранг колец и размерность топологических пространств, Функц. анализ и его прилож., 5, № 2 (1971), 17–27.

[17] Коуровская тетрадь. Нерешенные вопросы теории групп, 11-е изд., Новосибирск, Ин–т матем. СО РАН, 1990.

[18] Carter D., Keller G. Elementary expressions for unimodular matrices, Commun. Algebra, 12, № 3-4 (1984), 379–389.

[19] Мальцев А. И. Основы линейной алгебры. М.: Наука, 1970.

[20] Саркисян Р. А. Проблема сопряженности для целочисленных матриц, Матем. заметки, 25, № 6 (1979), 811–824.

[21] Grunewald F. Solution of the Conjugacy Problem in Certain Arithmetic Groups, Amsterdam: North Holland, 1979.

[22] Vaserstein L. N., Wheland E. Factorization of invertible matrices over rings of stable rank one, J. Austral Math. Soc., Ser. A 48, № 3 (1990), 455–460.

[23] Виноградов И. М. Основы теории чисел. М.: Наука, 1972.

[24] Vaserstein L., Wheland E. Commutators and companion matrices over rings of stable rank 1, Linear Algebra Appl., 142, № 1 (1990), 263–277.