Записки научных
семинаров ПОМИ
Том 388, 2011 г.

Н. А. Вавилов, А. В. Смоленский, Б. Сури

УНИТРЕУГОЛЬНЫЕ ФАКТОРИЗАЦИИ ГРУПП ШЕВАЛЛЕ

В настоящей заметке мы показываем, что из сопоставления результатов Хаймана Басса [14] и Олега Тавгеня [10] моментально вытекает следующий результат, являющийся одновременно и более общим и более точным, чем все недавно опубликованные результаты, относящиеся к унитреугольным факторизациям.

Теорема 1. *Пусть Φ – приведенная неприводимая система корней, а R – коммутативное кольцо такое, что $\mathrm{sr}(R) = 1$. Тогда односвязная группа Шевалле $G(\Phi, R)$ допускает унитреугольную факторизацию*

$$G(\Phi, R) = U(\Phi, R)U^-(\Phi, R)U(\Phi, R)U^-(\Phi, R).$$

длины 4.

С другой стороны, так как $U^-(\Phi, R) \cap B(\Phi, R) = 1$, то

$$T(\Phi, R) \cap U(\Phi, R)U^-(\Phi, R)U(\Phi, R) = 1.$$

Ключевые слова: Группы Шевалле, унитреугольные факторизации, унипотентные факторизации, кольца стабильного ранга 1, дедекиндовы кольца арифметического типа, параболические подгруппы, ограниченное порождение, разложение Гаусса, LULU-разложение.

Работа первого автора выполнялась в рамках проектов РФФИ 09-01-00784, “Эффективное порождение в группах типа Ли” (ПОМИ РАН), РФФИ 09-01-00878 “Надгруппы редуктивных групп в алгебраических группах над кольцами” (СПбГУ), РФФИ 10-01-90016 “Исследование структуры форм редуктивных групп и поведения малых унипотентных элементов в представлениях алгебраических групп” (СПбГУ), работа первого и третьего авторов проходила в рамках совместного Российско-Индийского проекта РФФИ 10-01-92651 “Высшие законы композиции, алгебраическая K-теория и исключительные группы” (СПбГУ). Кроме того, первый автор частично пользовался поддержкой грантов РФФИ 09-01-00762 (Сибирский Федеральный Университет), РФФИ 09-01-91333 (ПОМИ РАН) и РФФИ 11-01-00756 (РГПУ). Кроме того, работа первого и второго авторов поддержана НИР 6.38.74.2011 Санкт-Петербургского государственного Университета, “Структурная теория и геометрия алгебраических групп и их приложения в теории представлений и алгебраической K-теории”. Третий автор благодарен Петербургскому Отделению Математического Института и Санкт-Петербургскому Государственному Университету за приглашение посетить Санкт-Петербург в мае–июне 2011 года.

Иными словами, 1 является *единственным* элементом тора $T(\Phi, R)$, допускающим унитреугольную факторизацию длины < 4. Таким образом, если в кольце R есть хотя бы один нетривиальный обратимый элемент, то установленное в теореме разложение действительно является кратчайшим возможным.

Совершенно удивительно здесь то, что обычное *линейное* условие стабильного ранга работает для групп всех типов! При чуть более сильных условиях стабильности аналогичный результат справедлив также для скрученных групп Шевалле. Однако, рассмотрение скрученных групп требует несколько более детального анализа групп рангов 1 и 2, когда нельзя просто сослаться на известные результаты. Этим результатам будет посвящена следующая статья авторов.

Ясно, что для колец размерности ≥ 1 невозможно, вообще говоря, надеяться получить унитреугольные факторизации длины 4. Однако, для некоторых достаточно хороших колец размерности 1 удается получить унитреугольные факторизации длины 5 или 6. Второй основной результат настоящей работы как раз и дает простейший такой пример.

Теорема 2. *Пусть Φ – приведенная неприводимая система корней, а $p \in \mathbb{Z}$ – рациональное простое. В предположении обобщенной гипотезы Римана односвязная группа Шевалле $G\big(\Phi, \mathbb{Z}\big[\frac{1}{p}\big]\big)$ допускает унитреугольную факторизацию*

$$G\Big(\Phi, \mathbb{Z}\Big[\frac{1}{p}\Big]\Big) = \Big(U\Big(\Phi, \mathbb{Z}\Big[\frac{1}{p}\Big]\Big)U^-\Big(\Phi, \mathbb{Z}\Big[\frac{1}{p}\Big]\Big)\Big)^3$$

длины 6.

В настоящее время мы работаем над обобщениями этого результата на другие области Хассе и планируем вернуться к этой теме в отдельной статье.

Первая часть настоящей работы является курсовой работой второго автора, выполненной под руководством первого автора, а вторая часть возникла в процессе работы над арифметическими вопросами нашего совместного Российско–Индийского проекта “Высшие законы композиции, алгебраическая K-теория и исключительные группы” в Санкт-Петербургском университете, Тата Институте (Мумбай) и Индийском Статистическом Институте (Бангалор).

Так как унитреугольным факторизациям посвящено значительное число статей, в которых зачастую нет ссылок на предшествующие работы, содержащие аналогичные – или даже более сильные! – результаты, мы начинаем статью с краткого обзора известных результатов, как мы их понимаем. Этому посвящены §§1–4. После этого в §§5 и 6 вводятся основные обозначения. В §7 доказывается вариант теоремы Тавгеня о редукции ранга, из которого сразу вытекает теорема 1. В §8 обсуждается связь унитреугольных факторизаций с разложениями Брюа и Гаусса. В §9 рассматриваются группы Шевалле над арифметическими кольцами и доказывается теорема 2. Наконец, в §10 мы упоминаем некоторые дальнейшие близкие темы и формулируем несколько нерешенных задач.

§1. Существование унитреугольных факторизаций

Недавно в нескольких различных контекстах снова всплыла следующая задача: найти кратчайшую факторизацию $G = UU^-UU^- \dots U^{\pm}$ группы Шевалле $G = (\Phi, R)$ в терминах унипотентного радикала $U = U(\Phi, R)$ борелевской подгруппы $B = B(\Phi, R)$ и унипотентного радикала $U^- = U^-(\Phi, R)$ противоположной борелевской подгруппы $B^- = B^-(\Phi, R)$.

Упомянем три такие большие кластера разных наук, где возникала эта задача. В следующих параграфах мы увидим, что информация между науками внутри кластера передается хоть и с опозданием, но все же *значительно* быстрее и надежнее, чем между самими кластерами.

• Алгебраическая K-теория, структурная теория алгебраических групп, теория арифметических групп.

• Теория конечных и проконечных групп, асимптотическая теория групп, конечные геометрии.

• Вычислительная линейная алгебра, теория вейвлетов, компьютерная графика, теория управления.

Перечислим некоторые имеющиеся результаты, посвященные факторизациям вида $G = UU^-UU^- \dots U^{\pm}$. Во-первых, нужно установить *существование* таких факторизаций, а, во-вторых, найти их *длину*.

Ясно, что существование какой-то унитреугольной факторизации эквивалентно выполнению следующих двух условий.

• Группа Шевалле $G(\Phi, R)$ совпадает со своей элементарной подгруппой $E(\Phi, R)$, порожденной элементарными образующими.

• Ширина элементарной группы Шевалле $E(\Phi, R)$ в элементарных образующих ограничена.

Ответ на оба эти вопроса, вообще говоря, безнадежно отрицателен, так что существование унитреугольных факторизаций следует ожидать только для некоторых очень специальных колец. Этим вопросам посвящена *огромная* литература, и мы не будем вдаваться в детали, а ограничимся краткой выжимкой из введения к [59], отсылая к [61, 46] по поводу более широкой картины и дальнейших ссылок.

• В случае, когда кольцо R полулокально – например, имеет конечную размерность над полем – для односвязных групп Шевалле имеет место равенство $E(\Phi, R) = G(\Phi, R)$. Конечность ширины в элементарных образующих моментально следует из разложения Гаусса.

• Классически известно, что выражение матрицы в группе $\mathrm{SL}(2, R)$ над эвклидовым кольцом R как произведения элементарных матриц соответствует цепным дробям. Существование сколь угодно длинных `division chains` в $\mathbb{Z}$ показывает, что группа $\mathrm{SL}(2, \mathbb{Z})$ не может иметь ограниченной ширины. Много дальнейших примеров такого рода построено в [22, 23].

• С другой стороны Дэвид Картер и Гордон Келлер [15, 16] и Олег Тавгень [9, 10, 61] показали, что для дедекиндова кольца арифметического типа R группы Шевалле $G(\Phi, R) = E(\Phi, R)$ ранга ≥ 2 имеют ограниченную ширину в элементарных образующих.

• Вильберд ван дер Каллен [30] обнаружил, что вообще говоря, даже группы Шевалле ранга ≥ 2 над эвклидовыми кольцами имеют бесконечную ширину в элементарных образующих. Точнее, он доказал, что уже $\mathrm{SL}(3, \mathbb{C}[t])$ – и, тем самым, так как $\mathrm{sr}(\mathbb{C}[t]) = 2$, то и ни одна из групп $\mathrm{SL}(n, \mathbb{C}[t])$ при $n \geq 4$ – не имеет ограниченной ширины в элементарных образующих.

Таким образом, надеяться на существование унитреугольных факторизаций можно только для групп Шевалле над некоторыми очень специальными кольцами размерности ≤ 1.

В следующих трех параграфах мы перечислим некоторые работы, относящиеся к длине унитреугольных факторизаций. Из этого краткого обзора будет видно, что стандартные результаты одной области как правило не известны специалистам в других областях. Трудно

себе представить, сколько времени можно было бы сэкономить, если бы миллионы программистов и инженеров вместо манипуляций с матрицами выучили бы слова параболическая подгруппа и разложение Леви.

То же замечание относится и к приложению 1.1 из работы [13], где фактически результат, по крайней мере для линейного случая, был уже некоторое время известен, в гораздо большей общности, и с лучшей оценкой, специалистам по другим наукам, как по алгебраической K-теории [24], так и по вычислительной линейной алгебре [60]. Разумеется, после того, как его механизм понят для случая $\mathrm{SL}(n, R)$, обобщение на группы Шевалле не требует серьезных интеллектуальных усилий, а лишь владения соответствующей техникой.

§2. Длина факторизаций: линейные группы

Для линейного случая систематическое рассмотрение этого вопроса начато в работе Кейта Денниса и Леонида Васерштейна [24]. Их интерес к этому вопросу связан со следующим наблюдением.

• Любой элемент группы $U(n, R)$, $n \geq 3$, над произвольным ассоциативным кольцом R есть произведение не более двух коммутаторов в элементарной группе $E(n, R)$, лемма 13. Ранее в работе ван дер Каллена [30] было замечено, что элементы $U(n, R)$ представляются как произведения не более трех коммутаторов.

Сформулируем несколько типичных результатов работы [24], относящихся к длине унитреугольных факторизаций.

• Если для некоторого кольца R группа $E(m, R)$, $m \geq 2$, представляется в виде конечного произведения $UU^-UU^- \dots U^{\pm}$ с L множителями, то и все группы $E(n, R)$, $n > m$, представляются в таком виде, с тем же количеством множителей, лемма 7.

• Если стабильный ранг кольца R равен 1, то, как известно из работы Хаймана Басса [14], группа $E(2, R)$ – а, тем самым, в силу предыдущего утверждания и все группы $E(n, R)$ – допускают унитреугольную факторизацию

$$E(n, R) = U(n, R)U^-(n, R)U(n, R)U^-(n, R)$$

длины 4.

Авторам [24], как и всем специалистам по K-теории, этот факт *настолько* очевиден, что в [24] он даже не формулируется отдельно,

а лишь упоминается внутри доказательства теоремы 6. Тем не менее, поскольку это один из ключевых шагов в доказательстве теоремы 1, причем *единственный*, где используется условие стабильности, мы воспроизведем его доказательство, представляющее собой адаптацию более общего вычисления такого типа, проведенного в [14].

Напомним, что кольцо R имеет **стабильный ранг 1**, если для любых $x, y \in R$, которые порождают R как *правый* идеал, найдется $z \in R$ такое, что $x + yz$ обратим *справа*. В этом случае мы пишем $\mathrm{sr}(R) = 1$.

Простейшим и типичнейшим примером колец стабильного ранга 1 являются полулокальные кольца. Впрочем, имеется много гораздо менее очевидных примеров, скажем, кольцо всех целых алгебраических чисел. Много дальнейших примеров и дальнейшие ссылки можно найти в [64].

Хорошо известно, что в действительности кольца стабильного ранга 1 слабо конечны (теорема Капланского–Ленстры), так что в их определении можно сразу требовать выполнения условия $x + yz \in R^*$. Так как для линейного случая результат хорошо известен, а группы Шевалле других типов существуют только над коммутативными кольцами, в дальнейшем мы ограничимся случаем, когда R коммутативно, когда это доказательство доказывает заодно равенство $\mathrm{SL}(2, R) = E(2, R)$.

В следующем доказательстве и в дальнейшем, имея дело с линейным случаем, мы используем стандартные матричные обозначения. В частности, e обозначает единичную матрицу, e_{ij}, $1 \leq i, j \leq n$, – стандартную матричную единицу, т.е. матрицу, у которой в позиции (i, j) стоит 1, и нули во всех остальных позициях. Далее, для $1 \leq i \neq j \leq n$ и $\xi \in R$ через $t_{ij}(\xi)$ обозначаем матрицу $e + \xi e_{ij}$. Матричный элемент g в позиции (i, j) обозначается через g_{ij}, а матричный элемент обратной матрицы g^{-1} – через g'_{ij}.

Лемма 1. *Пусть R – коммутативное кольцо стабильного ранга 1. Тогда*

$$\mathrm{SL}(2, R) = U(2, R)U^-(2, R)U(2, R)U^-(2, R).$$

Доказательство. Проследим, сколько элементарных преобразований потребуется для приведения матрицы $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2, R)$ к виду e. Мы не будем вводить на каждом шаге новые обозначения, а будем, как это принято у программистов, просто заменять матрицу g на ее текущее значение. При этом следует, конечно, иметь в виду,

что и коэффициентам a, b, c, d нужно на каждом шаге присваивать текущие значения.

Шаг 1. Умножение на одно *нижнее* элементарное преобразование справа позволяет сделать элемент в левом нижнем углу обратимым. В самом деле, так как строки матрицы унимодулярны, то $cR + dR = R$. Так как $\mathrm{sr}(R) = 1$, найдется такое $z \in R$, что $c + dz \in R^*$. Таким образом,

$$gt_{21}(z) = \begin{pmatrix} a + bz & b \\ c + dz & d \end{pmatrix},$$

где $c + dz \in R^*$.

Шаг 2. Итак, пусть $c \in R^*$. Умножение на одно *верхнее* элементарное преобразование справа позволяет сделать элемент в правом нижнем углу равным 1. В самом деле,

$$gt_{12}(c^{-1}(1-d)) = \begin{pmatrix} a & b + ac^{-1}(1-d) \\ c & 1 \end{pmatrix},$$

Шаг 3. Итак, пусть теперь $d = 1$. Умножение на одно *нижнее* элементарное преобразование справа позволяет сделать элемент в левом нижнем углу равным 0. В самом деле,

$$gt_{21}(-c) = \begin{pmatrix} a - bc & b \\ 0 & 1 \end{pmatrix}.$$

Так как $\det(g) = 1$, то матрица справа равна $t_{12}(b)$. Перенося элементарные множители в правую часть, мы видим, что любая матрица g с определителем 1 представима в виде $t_{12}(*)t_{21}(*)t_{12}(*)t_{21}(*)$, как и утверждалось. □

Вернемся теперь к работе Денниса–Васерштейна [24].

• Если кольцо R булево, т.е. $x^2 = x$ для всех $x \in R$, то элементарная группа $E(n, R)$, $n \geq 2$, допускает унитреугольную факторизацию

$$E(n, R) = U(n, R)U^-(n, R)U(n, R)$$

длины 3. Для коммутативных колец верно и обратное: если при некотором $n \geq 2$ группа $E(n, R)$ допускает факторизацию длины 3, то кольцо R булево, замечание 15.

• Пусть $d = \mathrm{diag}(\varepsilon_1, \ldots, \varepsilon_n)$, $\varepsilon_i \in R^*$, – такая диагональная матрица, что $\varepsilon_1 \ldots \varepsilon_n = 1$. Тогда $d \in U(n, R)U^-(n, R)U(n, R)U^-(n, R)$, лемма 18. Доказательство в [24] основано на приведении в общее положение. В §8 мы дадим еще одно доказательство чуть более общего факта,

основанное на индукции по рангу, которое несколько легче перенести на все группы Шевалле.

• Если стабильный ранг кольца R конечен и для какого-то $m \geq 2$ группа $E(m, R)$ имеет конечную ширину по отношению к элементарным образующим, то для всех достаточно больших n имеет место унитреугольная факторизация

$$E(n, R) = (U(n, R)U^-(n, R))^3$$

длины 6.

• Чрезвычайно поучительно сравнить этот результат с *разложением Шарпа*. Напомним, что в работе [54] доказано, что для произвольного ассоциативного кольца предельная элементарная группа $E(R) = \varinjlim E(n, R)$, $g \mapsto g \oplus 1$, допускает разложение

$$\begin{aligned} E(R) &= B(R)N(R)U(R)U^-(R) \\ &= B(R)U^-(R)U(R)U^-(R) = U(R)D(R)U^-(R)U(R)U^-(R), \end{aligned}$$

где через $B(R)$, $N(R)$, $U(R)$, $U^-(R)$, $D(R)$ обозначены индуктивные пределы соответствующих групп конечной степени относительно того же вложения. Так как $D(R) \subseteq U(R)U^-(R)U(R)U^-(R)$, то для произвольного ассоциативного кольца предельная элементарная группа $E(R)$ допускает унитреугольную факторизацию

$$E(R) = (U(R)U^-(R))^3$$

длины 6.

• Недавно в связи с приложениями в задачах факторизации целочисленных матриц Томас Лаффи [31], [32] явно вычислил оценку в теореме Денниса–Васерштейна для кольца $R = \mathbb{Z}$. В частности, унитреугольная факторизация

$$\mathrm{SL}(n, \mathbb{Z}) = (U(n, \mathbb{Z})U^-(n, \mathbb{Z}))^3$$

длины 6 имеет место для любого $n \geq 82$.

§3. Длина факторизаций: группы Шевалле

Доказательство ограниченности ширины групп Шевалле над дедекиндовыми кольцами арифметического типа по отношению к элементарным образующим, данное в работе Олега Тавгеня [10], опиралось на редукцию к группам ранга 2. Основой этой редукции является следующий факт (предложение 1 работы [10]).

• Если все группы Шевалле некоторого ранга l допускают унитреугольную факторизацию $G = (UU^-)^L$ некоторой длины, то и все группы большего ранга допускают факторизацию той же длины. Фактически наша теорема 3 является незначительной обработкой идеи Тавгеня.

• Еще одна обработка той же темы Тавгеня содержится в недавней работе Андрея Рапинчука и Игоря Рапинчука [51]. Там та же идея используется, чтобы доказать, что группа Шевалле над локальным кольцом R представляется в виде

$$G(\Phi, R) = (U(\Phi, R)U^-(\Phi, R))^4.$$

Для полей, в особенности для конечных полей, интерес к явному вычислению длины оживился последнее десятилетие. Пусть $\mathbb{F}_q$, $q = p^m$ – конечное поле характеристики p. В этом случае группа $U(\Phi, q) = U(\Phi, \mathbb{F}_q)$ представляет собой силовскую p-подгруппу группы Шевалле $G(\Phi, q) = G(\Phi, \mathbb{F}_q)$. Таким образом, фактически в этом случае вопрос о длине унитреугольной факторизации превращается в вопрос о длине факторизации простой группы типа Ли в терминах ее силовских p-подгрупп, в определяющей характеристике.

• Мартин Либек и Ласло Пибер [41], теорема D, доказывают, что конечные группы Шевалле допускают унитреугольную факторизацию

$$G(\Phi, q) = (U(\Phi, q)U^-(\Phi, q))^6 U(\Phi, q)$$

длины 13. На самом деле, они, конечно, рассматривают также скрученные группы Шевалле и получают для них такую же оценку длины, кроме старших групп Ри ${}^2\mathrm{F}_4(q)$, для которых они доказывают существование факторизации $G = (UU^-)^{12}U$.

• Ласло Бабаи, Николай Николов и Ласло Пибер [13], приложение 1.1, доказывают, что конечные группы Шевалле допускают унитреугольную факторизацию

$$G(\Phi, q) = U(\Phi, q)U^-(\Phi, q)U(\Phi, q)U^-(\Phi, q)U(\Phi, q)$$

длины 5. Аналогичный результат с той же оценкой получен и для скрученных групп.

В отличие от [41], доказательства в работе [13] носят крайне оккультный характер. В конечном счете, они основаны на оценках роста произведений = `product growth estimates`, наподобие следующей. Пусть $X, Y \subseteq G$ – два непустых подмножества конечной группы G. Тогда

$$|XY| \geq \min\left(\frac{|G|}{2}, \frac{m|X| \cdot |Y|}{2|G|}\right),$$

где через m обозначена наименьшая размерность нетривиального вещественного представления группы G. В частности, в случае, когда группа G простая, а порядки $|X|, |Y|$ достаточно велики, но все еще далеки от $|G|$, произведения быстро растут: порядок $|XY|$ много больше, чем $\max(|X|, |Y|)$.

По этому поводу в работе [13] делается следующее экстравагантное заявление: "For the most part we can argue by the size of certain subsets, ignoring the structure and thus greatly simplifying the proofs and at the same time obtaining considerably better, nearly optimal bounds."

Честно говоря, предложение полностью игнорировать структуру рассматриваемых объектов представляется нам несколько сомнительным. Конечно, применение асимптотических методов вполне на месте при изучении проконечных групп или групп бесконечного ранга. С другой стороны, в приложении к собственно конечным группам и группам типа Ли конечного ранга, асимптотические методы следует рассматривать скорее как *суррогат* структурных алгебраических методов, как метод проверки интересующего нас результата, **идентичный** настоящему доказательству.

Разумеется, во многих ситуациях такого настоящего алгебраического доказательства нет. Более того, для многих интересных задач получить алгебраические решения совсем непросто, так как они либо связаны с *огромным* перебором случаев, либо вообще не могут быть получены существующими методами.

В качестве примера первой ситуации укажем на работу Мартина Либека и Анера Шалева [36], в которой доказано, что – за вычетом трех исключительных серий, групп Судзуки и групп $\mathrm{Sp}(4, 2^m)$ и $\mathrm{Sp}(4, 3^m)$ – почти все конечные простые группы $(2, 3)$-порождены. Для каждой конкретной группы типа Ли, притом не только над конечным полем, но и над конечно порожденными кольцами, в принципе

понятно, как доказывать ее $(2,3)$-порожденность. И для многих конкретных групп, в частности, для всех групп большого лиевского ранга (порядка нескольких десятков для конечных простых групп) такие доказательства действительно получены. Однако полное рассмотрение групп небольших рангов требует такого объема вычислительной работы, что до сих пор не завершено, несмотря на огромные усилия многих авторов.

Совершенно иная ситуация с недавними работами по вербальной ширине конечных групп. Упомянем недавний общий результат Анера Шалева [53], утверждающий, что для *любого* нетривиального слова $w \neq 1$ вербальная ширина почти всех конечных простых групп G равна 3. Иными словами, каждый элемент группы G представляется как произведение не более чем трех значений слова w. См. также [28, 34, 37, 40, 52], где можно найти дальнейшие результаты в таком духе, улучшение оценки вербальной ширины до 2 в некоторых случаях и ссылки на предшествующие работы. В этом случае, насколько нам известно, аналогичных результатов нет не то, что для колец, но даже для бесконечных полей. Притом не то, что для всех слов, а для простейших конкретных слов, типа степеней. Более того, совершенно непонятно, как их можно было бы доказать.

Тем не менее, мы считаем, что *в тех случаях, когда их удается применить*, алгебраические методы, приходящие из структурной теории и теории представлений алгебраических групп, будут *неизменно* давать более сильные и общие результаты. Для тех результатов, которые верны для произвольных полей, они должны давать лучшие оценки и, *хотелось бы надеяться*, иметь более простые доказательства.

§4. Длина факторизаций: вычислительная линейная алгебра

Разумеется, для группы $\mathrm{SL}(n,K)$ унитреугольная факторизация настолько очевидна и естественна, что трудно сомневаться в том, что она должна была быть известна специалистам по линейной алгебре. Вот, однако, самая ранняя ссылка, которую нам удалось обнаружить.

• Гильберт Стрэнг [60] доказал, что все группы $\mathrm{SL}(n,K)$ над полем допускают унитреугольную факторизацию

$$\mathrm{SL}(n,K) = U^-(n,K)U(n,K)U^-(n,K)U(n,K)$$

длины 4. Это то, что специалисты по вычислительной линейной алгебре называют LULU-факторизацией, где мнемонически `L` следует истолковывать как первую букву слова `lower`, а `U` – как первую букву слова `upper`.

Заметим, что этот факт вошел в обиход линейной алгебры через десятилетия после того, как он – в гораздо большей общности – стал стандартным в алгебраической K-теории. Однако, как мы уже знаем, барьеры между разными разделами математики высоки.

Еще забавнее, что, насколько нам известно, этот результат был замечен только в связи с приложениями в компьютерной графике! Поясним, как именно это произошло. Нам трудно уловить *точный* смысл, в котором в компьютерной графике используется термин *сдвиг* = `shear`. В качестве первого приближения можно считать, что это любой унипотентный элемент группы $\mathrm{SL}(n, K)$. Во всяком случае, большинство авторов в этой области использует термин `shear` для *всех* элементов групп $U(n, K)$ и $U^-(n, K)$.

Нет, однако, никаких сомнений относительно значения термина *одномерный сдвиг* = `one-dimensional shear`. Так называются в точности трансвекции, не обязательно элементарные! Совершенно особую роль играют трансвекции, сконцентрированные в одной строке = `beam shears` или в одном столбце = `slice shears`. Дело в том, что им отвечают параллельные переносы рядов пикселей = `string copy with offset`, которые *чрезвычайно* эффективно реализуются на аппаратном уровне.

В работе Алана Пэта [50] предложен следующий метод осуществления 2D поворота:

$$\begin{pmatrix} \cos(\varphi) & \sin(\varphi) \\ -\sin(\varphi) & \cos(\varphi) \end{pmatrix} = \begin{pmatrix} 1 & \mathrm{tg}(\varphi/2) \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -\sin(\varphi) & 1 \end{pmatrix} \begin{pmatrix} 1 & \mathrm{tg}(\varphi/2) \\ 0 & 1 \end{pmatrix}.$$

Так как сдвиги имплементируются на уровне пересылки данных, этот метод оказался значительно быстрее, чем пересчет координат.

В связи с этим естественно возник вопрос аналогичной аппаратной имплементации 3D поворотов. Прежде всего, конечно, были предприняты попытки вначале раскладывать 3D поворот в произведение трех 2D поворотов, а потом каждый из них, в свою очередь, в произведение трех трансвекций. Однако вскоре Томмазо Тоффоли и Джейсон Квик [63] реализовали схему, основанную на разложении 3D поворота в произведение трех унипотентных матриц.

Напомним, что трехмерное вращение g определяется своими углами Эйлера (α, β, γ), например, так

$$g = \begin{pmatrix} c(\alpha)c(\beta)c(\gamma) - s(\alpha)s(\gamma) & -c(\alpha)c(\beta)s(\gamma) - s(\alpha)c(\gamma) & c(\alpha)s(\beta) \\ s(\alpha)c(\beta)c(\gamma) + c(\alpha)s(\gamma) & -s(\alpha)c(\beta)s(\gamma) + c(\alpha)c(\gamma) & s(\alpha)s(\beta) \\ -s(\beta)c(\gamma) & s(\beta)s(\gamma) & c(\beta) \end{pmatrix},$$

где через $c(\varphi)$ и $s(\varphi)$ обозначены $\cos(\varphi)$ и $\sin(\varphi)$. Несложно заметить – именно это и является отправной точкой работы [63] – что g допускает следующую унитреугольную факторизацию длины 3:

$$g = \begin{pmatrix} 1 & -\operatorname{tg}\left(\dfrac{\alpha+\gamma}{2}\right) & \cos(\alpha)\operatorname{tg}\left(\dfrac{\beta}{2}\right) \\ 0 & 1 & \sin(\alpha)\operatorname{tg}\left(\dfrac{\beta}{2}\right) \\ 0 & 0 & 1 \end{pmatrix} \times \begin{pmatrix} 1 & 0 & 0 \\ \sin(\alpha+\gamma) & 1 & 0 \\ -\cos(\gamma)\sin(\beta) & -\dfrac{\sin\left(\dfrac{\alpha-\gamma}{2}\right)}{\cos\left(\dfrac{\alpha+\gamma}{2}\right)}\sin(\beta) & 1 \end{pmatrix} \times \begin{pmatrix} 1 & -\operatorname{tg}\left(\dfrac{\alpha+\gamma}{2}\right) & \dfrac{\cos\left(\dfrac{\alpha-\gamma}{2}\right)}{\cos\left(\dfrac{\alpha+\gamma}{2}\right)}\operatorname{tg}\left(\dfrac{\beta}{2}\right) \\ 0 & 1 & -\sin(\gamma)\operatorname{tg}\left(\dfrac{\beta}{2}\right) \\ 0 & 0 & 1 \end{pmatrix}.$$

Процитированная в начале параграфа работа Стрэнга [60] как раз и возникла из попытки обобщения этой формулы на произвольное n. После этого появилось большое количество статей, в которых обсуждались разные аспекты этого разложения. Чтобы дать представление об этой деятельности, сформулируем пару типичных результатов работы Тоффоли [62].

• Почти все элементы $\mathrm{SL}(n,\mathbb{R})$ допускают унитреугольную факторизацию длины 3 – ULU-факторизацию, как говорят специалисты по линейной алгебре. Разумеется, в отличие от предыдущего параграфа, выражение **почти все** здесь следует понимать в смысле меры Лебега.

• Для любой матрицы $g \in \mathrm{SL}(n,K)$ найдется такая матрица перестановки (π), $\pi \in \mathrm{S}_n$, что хотя бы одна из матриц $(\pi)g$ или $(\pi)^{-1}g$ допускает унитреугольную факторизацию длины 3

Мы не будем даже пытаться систематически отразить появившуюся с тех пор литературу, а ограничимся несколькими типичными ссылками [19, 29, 33, 55], где можно найти дальнейшую библиографию.

§5. Некоторые подгруппы групп Шевалле

Все наши обозначения, относящиеся к группам Шевалле, совершенно стандартны и совпадают с теми, которые использовались в [66, 67], где можно найти также много дальнейших ссылок.

Пусть Φ – приведенная неприводимая система корней ранга l, $W = W(\Phi)$ – ее группа Вейля, а $\mathcal{P}$ – решетка, лежащая между решеткой корней $\mathcal{Q}(\Phi)$ и решеткой весов $\mathcal{P}(\Phi)$. Мы фиксируем на Φ некоторый порядок и обозначаем через $\Pi = \{\alpha_1, \dots, \alpha_l\}$, Φ^+ и Φ^- множества простых, положительных и отрицательных корней, отвечающие этому порядку. Наша нумерация простых корней следует Бурбаки. Пусть, кроме того, R – коммутативное кольцо с единицей и мультипликативной группой R^*.

Как хорошо известно, по этим данным можно построить группу Шевалле $G = G_{\mathcal{P}}(\Phi, R)$, являющуюся группой R-точек некоторой аффинной групповой схемы $G_{\mathcal{P}}(\Phi, -)$, называемой схемой Шевалле–Демазюра. Так как наши результаты не зависят от выбора решетки $\mathcal{P}$, в дальнейшем мы будем считать, что $\mathcal{P} = \mathcal{P}(\Phi)$ и опускать указание на $\mathcal{P}$ в обозначениях. Таким образом, $G(\Phi, R)$ будет обозначать односвязную группу Шевалле типа Φ над R.

В дальнейшем мы фиксируем некоторый расщепимый максимальный тор $T(\Phi, -)$ схемы $G(\Phi, -)$ и полагаем $T = T(\Phi, R)$. Как обычно, X_α, $\alpha \in \Phi$, обозначает унипотентную корневую подгруппу в G, элементарную относительно T. Мы фиксируем изоморфизмы $x_\alpha : R \mapsto X_\alpha$, так что $X_\alpha = \{x_\alpha(\xi) \mid \xi \in R\}$, связанные между собой коммутационной формулой Шевалле, см. [8, 18, 67]. Через $E(\Phi, R)$ обозначается элементарная подгруппа в $G(\Phi, R)$, порожденная всеми корневыми подгруппами X_α, $\alpha \in \Phi$.

В дальнейшем элементы $x_\alpha(\xi)$ называются корневыми унипотентами. Пусть теперь $\alpha \in \Phi$ и $\varepsilon \in R^*$. Как обычно, мы полагаем $h_\alpha(\varepsilon) = w_\alpha(\varepsilon)w_\alpha(1)^{-1}$, где $w_\alpha(\varepsilon) = x_\alpha(\varepsilon)x_{-\alpha}(-\varepsilon^{-1})x_\alpha(\varepsilon)$. Элементы $h_\alpha(\varepsilon)$ называются полупростыми корневыми элементами. Для односвязной группы

$$T = T(\Phi, R) = \langle h_\alpha(\varepsilon),\ \alpha \in \Phi,\ \varepsilon \in R^* \rangle.$$

Пусть теперь $N = N(\Phi, R)$ – алгебраический нормализатор тора $T = T(\Phi, R)$, т.е. подгруппа, порожденная $T = T(\Phi, R)$ и всеми элементами $w_\alpha(1)$, $\alpha \in \Phi$. Фактор-группа N/T канонически изоморфна группе Вейля W, и мы зафиксируем для каждого $w \in W$ *какой-то* его прообраз n_w в N.

Следующий результат очевиден, хорошо известен и часто используется.

Лемма 2. *Элементарная группа Шевалле $E(\Phi, R)$ порождается унипотентными корневыми элементами $x_\alpha(\xi)$, $\alpha \in \pm\Pi$, $\xi \in R$, отвечающими простым и отрицательным простым корням.*

Доказательство. В самом деле, каждый корень сопряжен с простым корнем при помощи элемента группы Вейля, а группа Вейля порождается фундаментальными отражениями w_α, $\alpha \in \Pi$. Таким образом, элементарная группа $E(\Phi, R)$ порождается корневыми унипотентами $x_\alpha(\xi)$, $\alpha \in \Pi$, $\xi \in R$, и элементами $w_\alpha(1)$, $\alpha \in \Pi$. Осталось вспомнить, что $w_\alpha(1) = x_\alpha(1)x_{-\alpha}(-1)x_\alpha(1)$. □

Пусть, далее, $B = B(\Phi, R)$ и $B^- = B^-(\Phi, R)$ – пара противоположных борелевских подгрупп, содержащих $T = T(\Phi, R)$, стандартная относительно фиксированного порядка. Напомним, что B и B^- являются полупрямыми произведениями $B = T \leftthreetimes U$, а $B^- = T \leftthreetimes U^-$, тора T и своих унипотентных радикалов

$$U = U(\Phi, R) = \langle x_\alpha(\xi),\ \alpha \in \Phi^+,\ \xi \in R \rangle,$$

$$U^- = U^-(\Phi, R) = \langle x_\alpha(\xi),\ \alpha \in \Phi^-,\ \xi \in R \rangle.$$

Здесь, как обычно, для подмножества X группы G через $\langle X \rangle$ обозначается порожденная X подгруппа в G. Иными словами, утверждается, что $B = TU = UT$, причем $U \trianglelefteq B$ и $T \cap U = 1$. Аналогичные утверждения верны с заменой B и U на B^- и U^-. Иногда, чтобы одновременно говорить о двух подгруппах U и U^-, мы будем обозначать $U = U(\Phi, R)$ через $U^+ = U^+(\Phi, R)$.

Более общо, каждому замкнутому подмножеству S в Φ можно сопоставить группу $E(S) = E(S, R)$. Напомним, что подмножество S в Φ называется *замкнутым*, если для любых двух корней $\alpha, \beta \in S$ из того, что $\alpha + \beta \in \Phi$, следует, что $\alpha + \beta \in S$. Определим $E(S) = E(S, R)$ как подгруппу, порожденную всеми элементарными корневыми подгруппами X_α, $\alpha \in S$:

$$E(S, R) = \langle x_\alpha(\xi), \quad \alpha \in S, \quad \xi \in R \rangle.$$

В этих обозначениях U и U^- совпадают с $E(\Phi^+, R)$ и $E(\Phi^-, R)$, соответственно. Группы $E(S, R)$ особенно важны в случае, когда множество S является *специальным = унипотентным*, иными словами $S \cap (-S) = \varnothing$. В этом случае $E(S, R)$ является в точности *произведением* корневых подгрупп X_α, $\alpha \in S$, в каком-то/любом фиксированном порядке.

Пусть снова $S \subseteq \Phi$ является любым замкнутым множеством корней. Тогда S представляется как дизъюнктное объединение своей *редуктивной = симметричной* части S^r, состоящей из тех $\alpha \in S$, для которых $-\alpha \in S$ и своей *унипотентной* части S^u, состоящей из тех $\alpha \in S$, для которых $-\alpha \notin S$. Множество S^r является замкнутой подсистемой корней, в то время как множество S^u специально. Кроме того, S^u является *идеалом* в S, иными словами, если $\alpha \in S$, $\beta \in S^u$ и $\alpha + \beta \in \Phi$, то $\alpha + \beta \in S^u$. *Разложение Леви* утверждает, что группа $E(S, R)$ раскладывается в полупрямое произведение $E(S, R) = E(S^r, R) \leftthreetimes E(S^u, R)$ своей *подгруппы Леви* $E(S^r, R)$ и своего *унипотентного радикала* $E(S^u, R)$.

§6. Элементарные параболические подгруппы

Основную роль в доказательстве теоремы 1 играет разложение Леви для элементарных параболических подгрупп. Обозначим через $m_k(\alpha)$ коэффициент при α_k в разложении α по простым корням:

$$\alpha = \sum m_k(\alpha)\alpha_k, \quad 1 \leq k \leq l.$$

Зафиксируем теперь какое-то $r = 1, \ldots, l$ – в действительности в редукции к меньшему рангу достаточно использовать только терминальные параболические подгруппы, отвечающие первому и последнему простым корням, $r = 1, l$. Обозначим через

$$S = S_r = \{\alpha \in \Phi, \ m_r(\alpha) \geq 0\}$$

r-ое стандартное параболическое подмножество в Φ. Как обычно, редуктивная $\Delta = \Delta_r$ и специальная части $\Sigma = \Sigma_r$ множества $S = S_r$ определяются равенствами

$$\Delta = \{\alpha \in \Phi,\ m_r(\alpha) = 0\}, \quad \Sigma = \{\alpha \in \Phi,\ m_r(\alpha) > 0\}.$$

Противоположное параболическое множество и его специальная часть определяются аналогично

$$S^- = S_r^- = \{\alpha \in \Phi,\ m_r(\alpha) \leq 0\}, \quad \Sigma^- = \{\alpha \in \Phi,\ m_r(\alpha) < 0\}.$$

Ясно, что редуктивная часть S_r^- равна Δ.

Обозначим теперь через P_r *элементарную* максимальную параболическую подгруппу элементарной группы $E(\Phi, R)$. По определению

$$P_r = E(S_r, R) = \langle x_\alpha(\xi),\ \alpha \in S_r,\ \xi \in R\rangle.$$

Теперь разложение Леви утверждает, что группа P_r представляется в виде полупрямого произведения

$$P_r = L_r \leftthreetimes U_r = E(\Delta, R) \leftthreetimes E(\Sigma, R)$$

элементарной подгруппы Леви $L_r = E(\Delta, R)$ и унипотентного радикала $U_r = E(\Sigma, R)$. Напомним, что

$$L_r = E(\Delta, R) = \langle x_\alpha(\xi), \quad \alpha \in \Delta, \quad \xi \in R\rangle,$$

в то время как

$$U_r = E(\Sigma, R) = \langle x_\alpha(\xi),\ \alpha \in \Sigma,\ \xi \in R\rangle.$$

Аналогичное разложение имеет место и для противоположной параболической подгруппы P_r^-, при этом подгруппа Леви та же, что и для P_r, но унипотентный радикал заменяется на противоположный $U_r^- = E(-\Sigma, R)$

В действительности мы будем пользоваться разложением Леви в следующей форме. При этом нам будет удобно чуть изменить обозначения и писать $U(\Sigma, R) = E(\Sigma, R)$ и $U^-(\Sigma, R) = E(-\Sigma, R)$.

Лемма 3. *Группа $\langle U^\sigma(\Delta, R), U^\rho(\Sigma, R)\rangle$, где $\sigma, \rho = \pm 1$, является полупрямым произведением своего нормального делителя $U^\rho(\Sigma, R)$ и дополнительной подгруппы $U^\sigma(\Delta, R)$.*

Иными словами, здесь утверждается, что подгруппа $U^\pm(\Delta, R)$ нормализует каждую из групп $U^\pm(\Sigma, R)$, так что, в частности, имеют место следующие четыре равенства для произведений

$$U^\pm(\Delta, R)U^\pm(\Sigma, R) = U^\pm(\Sigma, R)U^\pm(\Delta, R),$$

и, кроме того, очевидно, имеют место следующие четыре равенства для пересечений

$$U^{\pm}(\Delta, R) \cap U^{\pm}(\Sigma, R) = 1.$$

В частности, имеют место разложения

$$U(\Phi, R) = U(\Delta, R) \leftthreetimes U(\Sigma, R), \quad U^-(\Phi, R) = U^-(\Delta, R) \leftthreetimes U^-(\Sigma, R).$$

§7. Редукция к группам меньшего ранга

Следующий результат является незначительной обработкой предложения 1 работы Олега Тавгеня [10]. Тавгень формулирует чуть более слабое, но более общее утверждение, в терминах выполнения факторизации для *всех* неприводимых систем некоторого ранга[1]. При этом он рассматривает также скрученные группы, кроме типа ${}^2\mathrm{A}_{2l}$.

Теорема 3. *Пусть Φ – приведенная неприводимая система корней ранга $l \geq 2$, а R – коммутативное кольцо. Предположим, что для подсистем $\Delta = \Delta_1, \Delta_l$, элементарная группа Шевалле $E(\Delta, R)$ представляется в виде*

$$E(\Delta, R) = (U(\Delta, R)U^-(\Delta, R))^L.$$

Тогда для элементарной группы Шевалле $E(\Phi, R)$ имеет место факторизация

$$E(\Phi, R) = (U(\Phi, R)U^-(\Phi, R))^L.$$

с той же константой L.

Ясно, что теорема 1 сразу следует из леммы 1 и теоремы 3, так что нам остается лишь доказать теорему 3.

Основная идея доказательства Тавгеня настолько общая и красивая, что работает и во многих других аналогичных ситуациях. Она основана на том, что для систем ранга ≥ 2 любой простой корень попадает в систему меньшего ранга, которая получается отбрасыванием либо первого, либо последнего простого корня. В описании нормальных подгрупп Эйичи Абе и Кадзуо Судзуки использовали аналогичное соображение для извлечении корневых унипотентов [11] и [12]. Близкая идея, в сочетании с приведением в общее положение использована Владимиром Черноусовым, Эрихом Эллерсом и Николаем Гордеевым

[1]Заметим, что первое равенство в формулировке предложения 1 работы [10] следует читать как $\mathrm{rk}({}^{\sigma}\Phi_0) = m$.

в упрощенном доказательстве разложения Гаусса с предписанной полупростой частью [21].

Воспроизведем теперь детали. Вообще говоря, по определению

$$Y = (U(\Phi, R)U^-(\Phi, R))^L$$

является *подмножеством* в $E(\Phi, R)$. Обычно самый простой способ доказать, что какое-то подмножество $Y \subseteq G$ совпадает со всей группой G состоит в следующем.

Лемма 4. *Предположим, что $Y \subseteq G$, $Y \neq \varnothing$, а $X \subseteq G$ – симметрическое порождающее множество. Если $XY \subseteq Y$, то $Y = G$.*

Доказательство теоремы 3. По лемме 2 группа G порождается фундаментальными корневыми унипотентами

$$X = \{x_\alpha(\xi) \mid \alpha \in \pm\Pi,\ \xi \in R\}.$$

Таким образом, в силу леммы 4 нам достаточно показать, что $XY \subseteq Y$.

Зафиксируем фундаментальный корневой унипотент $x_\alpha(\xi)$. Так как $\mathrm{rk}(\Phi) \geq 2$, то α принадлежит хотя бы одной из подсистем $\Delta = \Delta_r$, где $r = 1$ или $r = l$, порожденных всеми простыми корнями, кроме первого или последнего, соответственно. Положим $\Sigma = \Sigma_r$ и представим $U^\pm(\Phi, R)$ в виде

$$U(\Phi, R) = U(\Delta, R)U(\Sigma, R), \quad U^-(\Phi, R) = U^-(\Delta, R)U^-(\Sigma, R).$$

Воспользовавшись леммой 3 мы видим, что

$$Y = (U(\Delta, R)U^-(\Delta, R))^L (U(\Sigma, R)U^-(\Sigma, R))^L.$$

Так как $\alpha \in \Delta$, то $x_\alpha(\xi) \in E(\Delta, R)$, так что включение $x_\alpha(\xi)Y \subseteq Y$ сразу следует из условия теоремы. □

§8. Использование разложений Брюа и Гаусса

Заметим, что, в отличие от доказательства в работе [13], доказательство в работе Либека и Пибера [41] естественно и элементарно и основано на разложении Брюа $g = udn_w v$, где $u, v \in U$, $d \in T$, $w \in W$. Неоправданно большое количество множителей связано с тем, что они отдельно раскладывают d и n_w, причем делают и то, и другое неоптимальным образом. Например, для разложения элемента $h_\alpha(\varepsilon)$ вместо вычисления в $\mathrm{SL}(2, R)$ они пользуются непосредственно определением $h_\alpha(\varepsilon) = w_\alpha(\varepsilon)w_\alpha(-1)$, которое, после подстановки сюда выражения

$w_\alpha(\varepsilon)$ через корневые унипотенты, и дает выражение $h_\alpha(\varepsilon)$ как произведения 5 корневых унипотентов:

$$\begin{pmatrix} \varepsilon & 0 \\ 0 & \varepsilon^{-1} \end{pmatrix} = \begin{pmatrix} 1 & \varepsilon \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -\varepsilon^{-1} & 1 \end{pmatrix} \begin{pmatrix} 1 & \varepsilon - 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}.$$

Однако, в действительности, хорошо известно, что $h_\alpha(\varepsilon)$ является произведением 4 корневых унипотентов:

$$\begin{pmatrix} \varepsilon & 0 \\ 0 & \varepsilon^{-1} \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1-\varepsilon & 1 \end{pmatrix} \begin{pmatrix} 1 & \varepsilon^{-1} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ \varepsilon(\varepsilon-1) & 1 \end{pmatrix}.$$

В действительности, та же идея позволяет *сразу* получить для групп Шевалле над полулокальными кольцами унитреугольную факторизацию той же длины 5. Это доказательство основано на разложении Гаусса и игрушечной версии теоремы 1.

Напомним, что в работах Эйичи Абе и Кадзуо Судзуки [11, 12] и Майкла Стайна [58] доказан следующий аналог разложения Гаусса[2].

Лемма 5. *Пусть R – полулокальное кольцо. Тогда для односвязной группы Шевалле имеет место разложение*

$$G(\Phi, R) = U(\Phi, R)T(\Phi, R)U^-(\Phi, R)U(\Phi, R).$$

Как мы уже знаем, разложение Гаусса для группы $\mathrm{SL}(n, R)$ выполняется при более слабом условии $\mathrm{sr}(R) = 1$, см., *например*, [65]. В работе первого автора [2] отмечено, что в действительности для *всех* типов условие $\mathrm{sr}(R) = 1$ *необходимо* для того, чтобы группа Шевалле $G(\Phi, R)$ допускала разложение Гаусса. Для линейного случая это обстоятельство переоткрыто спустя 20+ лет в [47, 20]. С другой стороны, для всех типов, кроме $\Phi = \mathrm{A}_l, \mathrm{C}_l$ требуется какое-то более сильное условие стабильности, скажем, $\mathrm{asr}(R) = 1$, так что между необходимым и достаточным условием остается некоторый зазор.

Следующий результат является обобщением леммы 18 работы [24], где для случая $\Phi = \mathrm{A}_l$ доказан чуть более слабый факт.

[2]В терминах линейной алгебры это ULU-разложение, в то время как разложение Брюа – это UPU-разложение, где `P` следует истолковывать как первую букву слова `permutation`. Впрочем, сам Стайн называл это разложение `Bruhat type decomposition`. В работах Эриха Эллерса и Николая Гордеева разложением Гаусса называется LPU-разложение, которое обычно называется разложением Биркгофа. В то же время, в работах по вычислительной линейной алгебре разложением Гаусса обычно называется PLU-разложение или LUP-разложение.

Теорема 4. *Пусть Φ – приведенная неприводимая система корней, а R – произвольное коммутативное кольцо. Тогда имеет место включение*

$$N(\Phi, R) \subseteq U(\Phi, R)U^-(\Phi, R)U(\Phi, R)U^-(\Phi, R).$$

Следствие. *Пусть Φ – приведенная неприводимая система корней, а R – коммутативное полулокальное кольцо. Тогда односвязная группа Шевалле $G(\Phi, R)$ допускает унитреугольную факторизацию*

$$G(\Phi, R) = U(\Phi, R)U^-(\Phi, R)U(\Phi, R)U^-(\Phi, R)U(\Phi, R)$$

длины 5.

Доказательство. В самом деле,

$$G = UTU^-U \leq U(UU^-UU^-)U^-U = UU^-UU^-U.$$

□

Так как этот результат хуже и по условию на кольцо и по получающейся длине факторизации, чем теорема 1, мы не будем приводить доказательство теоремы 4 во всех случаях. В иллюстративных целях приведем, тем не менее, доказательство в линейном случае. Напомним, что в этом случае $N(\mathrm{A}_{n-1}, R)$ совпадает с группой $N = \mathrm{SN}(n, R)$ мономиальных матриц с определителем 1.

Доказательство теоремы 4 для $\Phi = \mathrm{A}_{n-1}$. Пусть $g = (g_{ij}) \in \mathrm{SN}(n, R)$. Будем вести доказательство индукцией по n. В случае $n = 1$ доказывать нечего, пусть поэтому $n \geq 2$.

Случай 1. Пусть вначале $g_{nn} = 0$. В этом случае найдется единственное $1 \leq r \leq n-1$ такое, что $a = g_{rn} \neq 0$, и единственное $1 \leq s \leq n-1$ такое, что $b = g_{ns} \neq 0$, причем автоматически $a, b \in R^*$, а все остальные элементы в s-м и n-м столбцах равны 0. Матрица $gt_{sn}(b^{-1})$ отличается от g только в позиции (n, n), где теперь вместо 0 стоит 1. Последовательно умножая получившуюся матрицу справа на $t_{ns}(-b)$ и затем снова на $t_{sn}(b^{-1})$, мы получим матрицу h, которая отличается от g только на пересечении r-й и n-й строк с s-м и n-м столбцами, где теперь вместо $\begin{pmatrix} 0 & a \\ b & 0 \end{pmatrix}$ стоит $\begin{pmatrix} -ab & 0 \\ 0 & 1 \end{pmatrix}$. Заметим, что определитель ведущей подматрицы порядка $n-1$ матрицы h равен 1, поэтому мы можем применить к ней индукционное предположение и получить для нее требуемое разложение в группе $\mathrm{SL}(n-1, R)$, не затрагивающее последнюю строку и последний столбец. Таким образом, все множители

разложения h лежат в L_{n-1}. Осталось заметить, что $t_{sn}(b^{-1}) \in U_{n-1}$, а $t_{ns}(-b) \in U^-_{n-1}$ и сослаться на лемму 3.

Случай 2. Пусть теперь $b = g_{nn} \neq 0$. Выберем произвольные $1 \leq r, s \leq n-1$, для которых $a = g_{rs} \neq 0$. Снова автоматически $a, b \in R^*$. Как и в предыдущем случае сконцентрируемся на строках с номерами r и n и столбцах с номерами s и n. Так как никаких других ненулевых элементов в этих строках и столбцах нет, прибавления между ними не затрагивают остальные элементы матрицы, а меняют лишь подматрицу, стоящую на пересечении r-й и n-й строк с s-м и n-м столбцами. Теперь умножая g на $t_{ns}(b^{-1})t_{sn}(1-b)t_{ns}(-1)t_{ns}(-b^{-1}(1-b))$ справа, мы получим матрицу h, в которой эта подматрица, изначально равная $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$, заменится на $\begin{pmatrix} ab & 0 \\ 0 & 1 \end{pmatrix}$. Теперь доказательство завершается точно так же, как в предыдущем случае. □

§9. Дедекиндовы кольца арифметического типа

Пусть K – глобальное поле, т.е. либо конечное алгебраическое расширение поля $\mathbb{Q}$, либо поле алгебраических функций от одной переменной над конечным полем констант $\mathbb{F}_q$ и пусть S – конечное множество неэквивалентных нормирований поля K, непустое в функциональном случае и содержащее все архимедовы нормирования в числовом случае. Для неархимедова нормирования $\mathfrak{p}$ поля K обозначим через $v_\mathfrak{p}$ соответствующий показатель.

Как обычно, $R = \mathcal{O}_S$ обозначает кольцо, состоящее из всех тех $x \in K$, для которых $v_\mathfrak{p}(x) \geq 0$ для всех нормирований $\mathfrak{p}$ поля K, не принадлежащих S. Кольцо $\mathcal{O}_S$ называется дедекиндовым кольцом арифметического типа, определенным множеством нормирований S поля K, или областью Хассе, см., например, [1]. Мы будем интересоваться случаем $|S| \geq 2$, когда по теореме Дирихле о единицах в $\mathcal{O}_S$ есть единица бесконечного порядка.

В качестве еще одного немедленного следствия редукции к меньшему рангу, положительного решения конгруэнц-проблемы [1, 43, 7] и работы Кука–Уайнбергера [23] можно сформулировать следующий результат. Заметим, что вычисления Кука–Уайнбергера зависит от бесконечности множества простых в арифметических прогрессиях, удовлетворяющих дополнительным мультипликативным ограничениям, и таким образом, опираются на GRH = обобщенную гипотезу Римана.

Теорема 5. *Пусть Φ – приведенная неприводимая система корней, а $R = \mathcal{O}_S$ – дедекиндово кольцо арифметического типа с бесконечной мультипликативной группой. Предположим, что выполняется обобщенная гипотеза Римана. Тогда односвязная группа Шевалле $G(\Phi, R)$ допускает унитреугольную факторизацию*

$$G(\Phi, R) = (U(\Phi, R)U^-(\Phi, R))^4 U(\Phi, R)$$

длины 9.

Аналогичные результаты известны и без предположения справедливости обобщенной гипотезы Римана. Однако, в этом случае оценки на количество множителей значительно хуже и зависят от числа классов кольца R или от количества простых делителей дискриминанта. Тем не менее, мы уверены, что в действительности 9 здесь можно заменить на 5 или 6.

Доказательство теоремы 2. Из теоремы 3 вытекает, что нам достаточно доказать существование факторизации длины 6 для группы $\mathrm{SL}\left(2, \mathbb{Z}[\frac{1}{p}]\right)$. В действительности, мы докажем следующий чуть более точный результат, где $U = U\left(2, \mathbb{Z}[\frac{1}{p}]\right)$ и $U^- = U^-\left(2, \mathbb{Z}[\frac{1}{p}]\right)$, соответственно. □

Лемма 6. *Пусть $p \in \mathbb{Z}$ – рациональное простое. Тогда в предположении обобщенной гипотезы Римана имеет место равенство*

$$\mathrm{SL}\left(2, \mathbb{Z}[\frac{1}{p}]\right) = U^-UU^-UU^- \bigcup UU^-UU^-U.$$

Наше доказательство самым существенным образом опирается на недавние результаты по гипотезе Артина, точнее на следующий результат, который сформулирован в работах Питера Мори [44, 45]. Полное доказательство приведено в [35, Следствие 5.4].

Лемма 7. *Пусть $a \in \mathbb{Z}$, $a \neq 0, 1, -1$, бесквадратное целое, а $c, d \in \mathbb{Z}$, $c \perp d$, – взаимно простые целые. Тогда в предположении обобщенной гипотезы Римана плотность множества простых q в классе вычетов $c \pmod d$, для которых q является примитивным корнем $\bmod d$, существует и положительна, за исключением случая, когда дискриминант $\mathbb{Q}(\sqrt{a})$ делит d, а каждое простое в классе вычетов $c \pmod d$ полностью распадается в $\mathbb{Q}(\sqrt{a})$.*

Отметим такое непосредственное следствие этого утверждения.

Следствие. *Пусть $p \in \mathbb{Z}$ – рациональное простое, а $c \perp d$ взаимно просты, причем $p \perp d$. Тогда в предположении справедливости обобщенной гипотезы Римана имеется бесконечно много простых q в классе вычетов $c \pmod d$, для которых p является примитивным корнем по модулю q.*

Теперь у нас все готово, чтобы доказать лемму 6, а вместе с тем и теорему 2.

Доказательство. Пусть $g = \begin{pmatrix} x & y \\ z & w \end{pmatrix} \in \mathrm{SL}\left(2, \mathbb{Z}[\frac{1}{p}]\right)$. Так как случай, когда хотя бы один из матричных коэффициентов x, y, z, w равен 0 уже был фактически нами рассмотрен в приведенном выше доказательстве теоремы 4 для линейного случая, в дальнейшем мы будем считать, что $xyzw \neq 0$. Положим теперь

$$g = \begin{pmatrix} x & y \\ z & w \end{pmatrix} = \begin{pmatrix} p^\alpha a & p^\beta b \\ * & * \end{pmatrix} \in \mathrm{SL}\left(2, \mathbb{Z}[\frac{1}{p}]\right),$$

где $a, b \in \mathbb{Z}$ не делятся на p, а $\alpha, \beta \in \mathbb{Z}$.

Случай 1: $\alpha \geq \beta$. По следствию из леммы 7 существует бесконечно много простых q вида $p^{\alpha-\beta}a + bk$ таких, что p – примитивный корень по модулю q. Тогда,

$$gt_{21}(k) = \begin{pmatrix} p^\beta q & p^\beta b \\ * & * \end{pmatrix}.$$

Так как p – примитивный корень $\bmod q$, то найдется такое $u \geq 1$, что $p^u \equiv b \pmod q$. Пусть, скажем, $p^u = b + lq$. В этом случае

$$gt_{21}(k)t_{12}(l) = \begin{pmatrix} p^\beta q & p^{\beta+u} \\ * & * \end{pmatrix}.$$

Тогда для $\theta = (1 - p^\alpha q)/p^{\beta+u}$, получим

$$gt_{21}(k)t_{12}(l)t_{21}(\theta) = \begin{pmatrix} 1 & p^{\beta+u} \\ * & * \end{pmatrix}$$

и, окончательно,

$$gt_{21}(k)t_{12}(l)t_{21}(\theta)t_{12}(-p^{\beta+u}) = \begin{pmatrix} 1 & 0 \\ * & 1 \end{pmatrix}.$$

Таким образом, в этом случае $g \in U^-UU^-UU^-$.

Случай 2: $\alpha < \beta$**.** В этом случае точно такое же вычисление доказывает, что $g \in UU^-UU^-U$. □

§10. Некоторые дальнейшие задачи

Перечислим несколько дальнейших задач, тесно связанных с унитреугольными факторизациями. В некоторых из них наша теорема 1 позволяет слегка улучшить оценки.

• В качестве еще одной близкой задачи упомянем вычисление ширины группы $E(\Phi, R)$ по отношению ко *всем* унипотентным элементам. Из доказанного Эрихом Эллерсом и Николаем Гордеевым разложением Гаусса с предписанной полупростой частью сразу вытекает, что каждый нецентральный элемент группы Шевалле $G(\Phi, K)$ является произведением двух унипотентных элементов [25].

Из теоремы 1 сразу вытекает следующий результат.

Следствие 1. *Пусть* Φ *– приведенная неприводимая система корней, а* R *– коммутативное кольцо такое, что* $\mathrm{sr}(R) = 1$*. Тогда любой элемент односвязной группы Шевалле* $G(\Phi, R)$ *представляется как произведение трех унипотентных элементов.*

Для колец размерности ≥ 1 ситуация значительно сложнее, см., в частности, работу Фрица Грюневальда, Йенса Меннике и Леонида Васерштейна [27].

• Еще один вопрос, который для полей недавно рассматривался в работе Мартина Либека, Николая Николова и Анера Шалева [38], это ширина группы Шевалле в фундаментальных $\mathrm{SL}(2, R)$. Для групп Шевалле над [конечным] полем там дается оценка $5|\Phi^+|$, вытекающая из [13]. Из нашей теоремы 1 сразу вытекает лучшая оценка в гораздо более широкой ситуации.

Следствие 2. *Пусть* Φ *– приведенная неприводимая система корней, а* R *– коммутативное кольцо такое, что* $\mathrm{sr}(R) = 1$*. Тогда односвязная группа Шевалле* $G(\Phi, R)$ *представляется в виде произведения* $4|\Phi^+|$ *подгрупп* $\mathrm{SL}(2, R)$*.*

В действительности, даже эта оценка все еще очень далека от настоящей. Из разложения Брюа сразу вытекает оценка $3|\Phi^+|$, чуть более детальные вычисления позволяют получить оценку $2|\Phi^+|$, этому будет посвящена работа первого автора и Евдокима Ковача.

• Большое число работ посвящено ширине групп Шевалле в коммутаторах [25, 39, 57, 59]. Для групп Шевалле над кольцом стабильного ранга 1 из нашей теоремы 1 вытекает тривиальная оценка 6, которая далека от оптимальной. Мы уверены, что в действительности для групп Шевалле над кольцом стабильного ранга 1 ширина в коммутаторах не превосходит 2 или 3.

Сформулируем в заключение несколько дальнейших нерешенных задач в этой области.

Проблема 1. *Найти для каждой группы Шевалле ранга* ≥ 2 *минимальное* L *такое, что*

$$G(\Phi, \mathbb{Z}) = (U(\Phi, \mathbb{Z})U^-(\Phi, \mathbb{Z}))^L.$$

В действительности, точная оценка не известна даже в следующем частном случае. С нашей точки зрения, вытекающая из [24] оценка в работах Томаса Лаффи [31, 32] сильно завышена.

Проблема 2. *Найти минимальное* n*, начиная с которого имеет место факторизация*

$$\mathrm{SL}(n, \mathbb{Z}) = (U(n, \mathbb{Z})U^-(n, \mathbb{Z}))^3.$$

В связи с леммой 6 представляет интерес следующий вопрос.

Проблема 3. *Верно ли, что* $U^-UU^-UU^- = UU^-UU^-U$?

Скорее всего, в общем случае это не так, но было бы интересно увидеть явный контр-пример.

Для колец размерности > 1, вообще говоря, никаких треугольных факторизаций не существует и не может существовать. Их роль принимают на себя параболические факторизации, см. [3, 4, 59] и содержащиеся там ссылки, позволяющие эффективно сводить задачи, относящиеся к самой группе, к группам меньших рангов.

Проблема 4. *Оценить ширину групп Шевалле над коммутативными кольцами небольшого стабильного ранга в классических подгруппах/подгруппах типа* A_l.

Даже для случая поля эти оценки должны быть много лучше тех, которые получены в [51, 52].

Следующая задача может быть легко решена методами настоящей работы.

Проблема 5. *Чему равна ширина элементарной группы Шевалле $E(\Phi, R)$ над полулокальным кольцом R в унипотентных радикалах U_P и U_P^-?*

Отметим еще одно направление, в котором было бы естественно обобщить результаты настоящей работы. В работе [6] Виктор Петров и Анастасия Ставрова построили элементарную подгруппу $E(R)$ в изотропной редуктивной группе $G(R)$ и, в случае групп относительного ранга ≥ 2, доказали нормальность $E(R)$ в $G(R)$. См. также работу [5] Александра Лузгарева и Анастасии Ставровой, где доказано, что $E(R)$ совершенна, кроме известных исключений для групп Шевалле ранга 2.

Несмотря на сходство формулировок, следующая задача совсем не так тривиальна, и, насколько нам известно, в общем случае здесь нет вообще никаких оценок.

Проблема 6. *Чему равна ширина элементарной подгруппы $E(R)$ изотропной редуктивной группы $G(R)$ ранга ≥ 1 над полулокальным кольцом R в унипотентных радикалах U_P и U_P^-?*

Тем более не рассмотрена арифметическая ситуация.

Проблема 7. *Доказать, что элементарная подгруппа $E(R)$ изотропной редуктивной группы ранга ≥ 2 имеет ограниченную ширину в унипотентных радикалах U_P и U_P^- в случае, когда $R = \mathcal{O}_S$ – дедекиндово кольцо арифметического типа.*

Единственный известный нам по этому поводу результат для групп, не являющихся квазирасщепимыми, это работа Игоря Еровенко и Андрея Рапинчука [26], где рассмотрен случай ортогональной группы, отвечающей форме индекса Витта ≥ 2.

Авторы благодарят Питера Мори за ссылки по гипотезе Артина и и Дейва Витте Морриса за полезные обсуждения различных подходов к доказательству ограниченного порождения.

Литература

1. Х. Басс, Дж. Милнор, Ж.-П Серр, *Решение конгруэнц-проблемы для* SL_n ($n \geq 3$) *и* Sp_{2n} ($n \geq 2$). — Математика. Период. сб. перев. ин. статей **14**, No. 6 (1970), 64–128; **15**, No. 1 (1971), 44–60.
2. Н. А. Вавилов, *Параболические подгруппы групп Шевалле над коммутативным кольцом.* — Зап. научн. семин. ЛОМИ **116** (1982), 20–43.

3. Н. А. Вавилов, С. С. Синчук, *Разложения типа Денниса–Васерштейна.* — Зап. научн. семин. ПОМИ **375** (2010), 48–60.
4. Н. А. Вавилов, С. С. Синчук, *Параболические факторизации расщепимых классических групп.* — Алгебра и Анализ **23** (2011), No. 4, 1–30.
5. А. Ю. Лузгарев, А. К. Ставрова, *Элементарная подгруппа изотропной редуктивной группы совершенна.* — Алгебра и Анализ **23** (2011) (to appear).
6. В. А. Петров, А. К. Ставрова, *Элементарные подгруппы изотропных редуктивных групп.* — Алгебра и Анализ **20** (2008), No. 4, 160–188.
7. Ж.-П. Серр, *Проблема конгруэнц-подгрупп для* SL_2. — Математика. Период. сб. перев. ин. статей **15** (1971), No. 6. 12–45.
8. Р. Стейнберг, *Лекции о группах Шевалле.* Мир, М., 1975.
9. О. И. Тавгень, *Конечная ширина арифметических групп Шевалле ранга* ≥ 2. — Докл. АН СССР **310** (1990), No. 4, 802–806.
10. О. И. Тавгень, *Ограниченное порождение групп Шевалле над кольцами алгебраических чисел.* — Изв. АН СССР **54** (1990), No. 1, 97–122.
11. E. Abe, *Chevalley groups over local rings.* — Tôhoku Math. J. **21** (1969), No. 3, 474–494.
12. E. Abe, K. Suzuki, *On normal subgroups of Chevalley groups over commutative rings.* — Tôhoku Math. J. **28** (1976), No. 1, 185–198.
13. L. Babai, N. Nikolov, L. Pyber, *Product growth and mixing in finite groups.* — In: 19th Annual ACM–SIAM Symposium on Discrete Algorithms, ACM–SIAM (2008), pp. 248–257.
14. H. Bass, K*-theory and stable algebra.* — Publ. Math. Inst. Hautes Études Sci. No. 22 (1964), 5–60.
15. D. Carter, G. Keller, *Bounded elementary generation of* $\mathrm{SL}_n(\mathcal{O})$. — Amer. J. Math. **105** (1983), 673–687.
16. D. Carter, G. Keller, *Elementary expressions for unimodular matrices.* — Commun. Algebra **12** (1984), 379–389.
17. D. Carter, G. E. Keller, E. Paige, *Bounded expressions in* $\mathrm{SL}(2,\mathcal{O})$. — Preprint Univ. Virginia (1983).
18. R. W. Carter, *Simple groups of Lie type.* Wiley, London et al., 1972.
19. Chen Baoquan, A. Kaufman, 3D *volume rotation using shear transformations.* — Graph. Models **62** (2000), 308–322.
20. Chen Huanyin, Chen Miaosen, *On products of three triangular matrices over associative rings.* — Linear Algebra Applic. **387** (2004), 297–311.
21. V. Chernousov, E. Ellers, N. Gordeev, *Gauss decomposition with prescribed semisimple part: short proof.* — J. Algebra **229** (2000), 314–332.
22. P. M. Cohn, *On the structure of the* GL_2 *of a ring.* — Publ. Math. Inst. Hautes Études Sci. No. 30 (1967), 5–53.
23. G. Cooke, P. J. Weinberger, *On the construction of division chains in algebraic number rings, with applications to* SL_2. — Commun. Algebra **3** (1975), 481–524.
24. R. K. Dennis, L. N. Vaserstein, *On a question of M. Newman on the number of commutators.* — J. Algebra **118** (1988), 150–161.
25. E. Ellers, N. Gordeev, *On the conjectures of J. Thompson and O. Ore.* — Trans. Amer. Math. Soc. **350** (1998), 3657–3671.

26. I. V. Erovenko, A. S. Rapinchuk, *Bounded generation of some S-arithmetic orthogonal groups.* — C. R. Acad. Sci. **333** (2001), No. 5, 395–398.
27. F. J. Grunewald, J. Mennicke, L. N. Vaserstein, *On the groups* $\mathrm{SL}_2(\mathbb{Z}[x])$ *and* $\mathrm{SL}_2(K[x,y])$. — Israel J. Math. **86** (1994), Nos. 1–3, 157–193.
28. R. M. Guralnick, G. Malle, *Products of conjugacy classes and fixed point spaces.* `arXiv: 1005.3756`.
29. Hao Pengwei, *Customizable triangular factorizations of matrices.* — Linear Algebra Applic. **382** (2004), 135–154.
30. W. van der Kallen, $\mathrm{SL}_3(\mathbb{C}[x])$ *does not have bounded word length.* — Springer Lect. Notes Math. **966** (1982), 357–361.
31. T. J. Laffey, *Expressing unipotent matrices over rings as products of involutions.* — Preprint Univ. Dublin (2010).
32. T. J. Laffey, *Lectures on integer matrices.* — Beijing (2010), 1–38.
33. Lei Yang, Hao Pengwei, Wu Dapeng, *Stabilization and optimization of PLUS factorization and its application to image coding.* — J. Visual Communication & Image Representation **22** (2011), No. 1.
34. M. Larsen, A. Shalev, *Word maps and Waring type problems.* — J. Amer. Math. Soc. **22** (2009), 437–466.
35. H. W. Lenstra (jr.), P. Moree, P. Stevenhagen, *Character sums for primitive root densities.* — (2011) (to appear).
36. M. Liebeck, A. Shalev, *Classical groups, probabilistic methods, and the* $(2,3)$*-generation problem.* — Ann. Math. **144** (1996), No. 1, 77-125.
37. M. Liebeck, A. Shalev, *Diameteres of finite simple groups: sharp bounds and applications.* — Ann. Math. **154** (2001), 383–406.
38. M. Liebeck, N. Nikolov, A. Shalev, *Groups of Lie type as products of* SL_2 *subgroups.* — J. Algebra **326** (2011), 201–207.
39. M. Liebeck, E. A. O'Brien, A. Shalev, Pham Huu Tiep, *The Ore conjecture.* — J. Europ. Math. Soc. **12** (2010), 939–1008.
40. M. Liebeck, E. A. O'Brien, A. Shalev, Pham Huu Tiep, *Products of squares in finite simple groups.* — Proc. Amer. Math. Soc. (2011).
41. M. Liebeck, L. Pyber, *Finite linear groups and bounded generation.* — Duke Math. J. **107** (2001), 159–171.
42. B. Liehl, *Beschränkte Wortlänge in* SL_2. — Math. Z. **186** (1984), 509–524.
43. H. Matsumoto, *Sur les sous-groupes arithmétiques des groupes semi-simples déployés.* — Ann. Sci. École Norm. Sup. (4) **2** (1969), 1–62.
44. P. Moree, *On primes in arithmetic progression having a prescribed primitive root.* — J. Number Theory **78** (1999), 85–98.
45. P. Moree, *On primes in arithmetic progression having a prescribed primitive root.* II. — Funct. Approx. Comment. Math. **39** (2008), 133–144.
46. D. W. Morris, *Bounded generation of* $\mathrm{SL}(n,A)$ (*after D. Carter, G. Keller, and E. Paige*) — New York J. Math. **13** (2007), 383–421.
47. K. R. Nagarajan, M. P. Devaasahayam, T. Soundararajan, *Products of three triangular matrices over commutative rings.* — Linear Algebra Applic. **348** (2002), 1–6.
48. N. Nikolov, *A product decomposition for the classical quasisimple groups.* — J. Group Theory **10** (2007), 43–53.

49. N. Nikolov, L. Pyber, *Product decomposition of quasirandom groups and a Jordan type theorem.* arXiv:math/0703343 (2007).
50. A. Paeth, *A fast algorithm for general raster rotation.* — In: Graphics Gems, Acad. Press (1990), pp. 179–195.
51. A. S. Rapinchuk, I. A. Rapinchuk, *Centrality of the congruence kernel for elementary subgroups of Chevalley groups of rank* > 1 *over Noetherian rings.* (2010), pp. 1–12 arXiv:1007.2261v1 [math.GR].
52. A. Shalev, *Commutators, words, conjugacy classes, and character methods.* — Turk. J. Math. **31** (2007), 131–148.
53. A. Shalev, *Word maps, conjugacy classes, and a noncommutative Waring-type theorem.* — Ann. Math. **170**, No. 3 (2009), 1383–1416.
54. R. W. Sharpe *On the structure of the Steinberg group* $\mathrm{St}(\Lambda)$. — J. Algebra **68** (1981), 453–467.
55. She Yiyuan, Hao Pengwei, *On the necessity and sufficiency of PLUS factorizations.* — Linear Algebra Applic. **400** (2005), 193–202.
56. S. Sinchuk, N. Vavilov, *Parabolic factorisations of exceptional Chevalley groups* (to appear).
57. A. Sivatski, A. Stepanov, *On the word length of commutators in* $\mathrm{GL}_n(R)$. — K-theory **17** (1999), 295–302.
58. M. R. Stein, *Surjective stability in dimension* 0 *for* K_2 *and related functors.* — Trans. Amer. Math. Soc. **178** (1973), 176–191.
59. A. Stepanov, N. Vavilov, *On the length of commutators in Chevalley groups.* — Israel Math. J. (2011), 1–20.
60. G. Strang, *Every unit matrix is a LULU.* — Linear Algebra Applic. **265** (1997), 165–172.
61. O. I. Tavgen, *Bounded generation of normal and twisted Chevalley groups over the rings of S-integers.* — Contemp. Math. **131** (1992), No. 1, 409–421.
62. T. Toffoli, *Almost every unit matrix is a ULU.* — Linear Algebra Applic. **259** (1997), 31–38.
63. T. Toffoli, J. Quick, *Three dimensional rotations by three shears.* — Graphical Models & Image Processing **59** (1997), 89–96.
64. L. N. Vaserstein, *Bass's first stable range condition.* — J. Pure Appl. Algebra **34** (1984), Nos. 2–3, 319–330.
65. L. N. Vaserstein, E. Wheland, *Commutators and companion matrices over rings of stable rank* 1. — Linear Algebra Appl. **142** (1990), 263–277.
66. N. Vavilov, *Structure of Chevalley groups over commutative rings.* — In: Proc. Conf. Non-associative algebras and related topics (Hiroshima – 1990) , World Sci. Publ., London et al. (1991), pp. 219–335.
67. N. Vavilov, E. Plotkin, *Chevalley groups over commutative rings.* I. *Elementary calculations.* — Acta Applicandae Math. **45** (1996), 73–115.

Vavilov N. A., Smolensky A. V., Sury B. Unitriangular factorisations of Chevalley groups.

Lately, the following problem attracted a lot of attention in various contexts: find the shortest factorisation $G = UU^-UU^- \dots U^{\pm}$ of a Chevalley group $G = G(\Phi, R)$ in terms of the unipotent radical $U = U(\Phi, R)$ of the standard Borel subgroup $B = B(\Phi, R)$ and the unipotent radical $U^- = U^-(\Phi, R)$ of the opposite Borel subgroup $B^- = B^-(\Phi, R)$. So far, the record over a finite field was established in a 2010 paper by Babai, Nikolov, and Pyber, where they prove that a group of Lie type admits unitriangular factorisation $G = UU^-UU^-U$ of length 5. Their proof invokes deep analytic and combinatorial tools. In the present paper we notice that from the work of Bass and Tavgen one immediately gets a much more general result, asserting that over any ring of stable rank 1 one has unitriangular factorisation $G = UU^-UU^-$ of length 4. Moreover, we give a detailed survey of triangular factorisations, prove some related results, discuss prospects of generalisation to other classes of rings, and state several unsolved problems. Another main result of the present paper asserts that, in the assumption of the Generalised Riemann's Hypothesis, Chevalley groups over the ring $\mathbb{Z}[\frac{1}{p}]$ admit unitriangular factorisation $G = UU^-UU^-UU^-$ of length 6. Otherwise, the best length estimate for Hasse domains with infinite multiplicative groups that follows from the work of Cooke and Weinberger, gives 9 factors.

С.-Петербургский
государственный университет
Университетский пр. 28, Петродворец,
198504 Санкт-Петербург, Россия
Indian Statistics Institute Bangalore
E-mail: nikolai-vavilov@yandex.ru
andrei.smolensky@gmail.com
surybang@gmail.com

Поступило 27 мая 2011 г.