ПРЕПРИНТЫ ПОМИ РАН

Учредитель: Санкт-Петербургское отделение Математического института им. В. А. Стеклова Российской академии наук

Свидетельство о регистрации средства массовой информации: ЭЛ №ФС 77-33560 от 16 октября 2008 г. Выдано Федеральной службой по надзору в сфере связи и массовых коммуникаций

Контактные данные: 191023, г. Санкт-Петербург, наб. реки Фонтанки, дом 27

телефоны:(812)312-40-58; (812) 571-57-54

e-mail: admin@pdmi.ras.ru

http://www. pdmi.ras.ru /preprint/

Заведующая информационно-издательским сектором Симонова В.Н

Санкт-Петербургское отделение Математического института

им. В. А. Стеклова Российской академии наук

ПРЕПРИНТ ПОМИ – 01/2008

Элементарные подгруппы в изотропных редуктивных группах

В. А. Петров[1]

Department of Mathematical and Statistical Sciences

University of Alberta

Edmonton, AB T6G 2G1, Canada

victorapetrov@googlemail.com

А. К. Ставрова

Математико – механический факультет

Санкт-Петербургский Государственный Университет

198504, Санкт-Петербург, Петродворец, Россия

a_stavrova@mail.ru

Пусть G — не обязательно расщепимая редуктивная алгебраическая группа над коммутативным кольцом R с 1. Для любой параболической подгруппы P в G определим элементарную подгруппу $\mathrm{E}_P(R)$ как подгруппу в $G(R)$, порожденную унипотентными радикалами $U_P(R)$ и $U_{P^-}(R)$ подгруппы P и противоположной к ней параболической подгруппы P^-. Мы доказываем, что если локально в топологии Зариского G содержит расщепимый тор ранга ≥ 2, то подгруппа $E_P(R)$ не зависит от выбора P и, в частности, нормальна в G.

[1]Работа выполнена при содействии PIMS Postdoctoral Fellowship и INTAS 03-51-3251.

1 Введение

На протяжении данной статьи G — редуктивная алгебраическая группа над коммутативным кольцом R с единицей.

Понятие *элементарной подгруппы* $\mathrm{E}_n(R)$ полной линейной групы $\mathrm{GL}_n(R)$ было введено Бассом [12] (до этого в неявном виде оно использовалось Уайтхедом при изучении гомотопических типов CW-комплексов) и легло в основу построения алгебраической K-теории. В частности, нестабильный K_1-функтор определяется как фактор-группа $\mathrm{GL}_n(R)/\,\mathrm{E}_n(R)$, а K_2 — как ядро некоторого центрального расширения $\mathrm{E}_n(R)$. В определении элементарной подгруппы участвует фиксированный базис модуля R^n, но, согласно теореме Суслина [5], в случае, когда R коммутативно, а $n \geq 3$, $\mathrm{E}_n(R)$ не зависит от выбора базиса, иначе говоря, нормальна в $\mathrm{GL}_n(R)$. Обсуждение различных методов доказательства этого результата можно найти в работах Вавилова и Степанова [23, 31].

Сходным образом, элементарная подгруппа была определена для произвольных расщепимых полупростых групп над R как подгруппа, порожденная всеми элементарными корневыми унипотентами $x_\alpha(\xi)$ или, что то же самое, R-точками унипотентного радикала некоторой борелевской подгруппы B в G и унипотентного радикала противоположной борелевской подгруппы B^- (см., например, [7, 21]). Аналогично описанному выше случаю $G = \mathrm{GL}_n$ оказывается, что если ранг неприводимых компонент системы корней G хотя бы 2, элементарная подгруппа не зависит от выбора борелевской подгруппы, то есть нормальна в $G(R)$. Для ортогональной и симплектической группы это было доказано Суслиным и Копейко [6, 2] и Фу-ан Ли [20], а для произвольной группы Шевалле — Абе [7] в случае локального кольца и Таддеи [25] в общем случае (см. также [8]). Упрощенное доказательство содержится в работе Хазрата и Вавилова [17]. Нормальность элементарной подгруппы в скрученных группах Шевалле была доказана Судзуки [24] и Баком и Вавиловым [10].

Для классических групп имеются также варианты определения элементарной подгруппы с использованием инволюции и "форменного параметра" (унитарные группы Бака), в этом случае нормальность доказана Васерштейном и Хон Ю [30] и Баком и Вавиловым [11]; см. также статью первого автора для случая "нечетных" унитарных групп [3]. Разумеется, не все классические группы Бака являются группами точек редуктивных групповых схем, однако с точки зрения методов эти работы являются прямым обобщением упомянутых выше.

Для нерасщепимых почти простых групп над полем k часто рассматривается следующий аналог элементарной подгруппы, который был введен Титсом [26]. Именно, он определил группу $G^+(k)$ (в оригинале G_k^0) как подгруппу, порожденную k-точками унипотентных радикалов *всех* параболических подгрупп в G, определенных над k. При таком определении ее нормальность очевидна. Оказывается, группа $G^+(k)$ почти всегда (см. [26]) проективно проста, и описание нормальных подгрупп в $G(k)$ сводится к вычислению фактора $G(k)/G^+(k)$ (который является аналогом K_1-функтора). Известная проблема Кнезера–Титса заключается в том, чтобы выяснить, является ли этот фактор тривиальным для односвязной группы G. Для числовых полей это доказано для групп всех типов, кроме ${}^2E_{6,1}^{35}$, но в общем случае ответ отрицательный даже для групп типа A_l (контрпример Платонова), см. [4].

Сходным образом, в случае нерасщепимых классических групп над кольцами Васерштейн ([28, 29]) определил элементарную подгруппу как подгруппу, порожденную *всеми* трансвекциями Эйхлера–Зигеля–Диксона. Нормальность при этом также очевидна, однако Васерштейн доказывает, что элементарная подгруппа порождается трансвекциями специального вида. По существу, он фиксирует параболическую подгруппу типа P_1 и рассматривает точки ее унипотентного радикала и унипотентного радикала противоположной подгруппы.

Это естественным образом приводит нас к следующему определению элементарной подгруппы, обобщающему все вышеупомянутые.

Пусть P — параболическая подгруппа редуктивной группы G над R, U_P — ее унипотентный радикал. Так как G является редуктивной группой над аффинной схемой $\operatorname{Spec} R$, группа P обладает некоторой подгруппой Леви L_P ([16], Exp. XXVI Cor. 2.3 [2]). При этом существует единственная параболическая подгруппа P^- группы G, противоположная P относительно L_P (то есть такая, что $P^- \cap P = \mathrm{L}_P$, см. Exp. XXVI Th. 4.3.2).

Определим *элементарную подгруппу* $\mathrm{E}_P(R)$, соответствующую P, как подгруппу в $G(R)$, порожденную (в абстрактном смысле) $\mathrm{U}_P(R)$ и $\mathrm{U}_{P^-}(R)$.

Заметим, что если L'_P — другая подгруппа Леви параболической подгруппы P, то L'_P и L_P сопряжены посредством некоторого элемента $u \in \mathrm{U}_P(R)$ (Exp. XXVI Cor. 1.8), поэтому группа $\mathrm{E}_P(R)$ не зависит от выбора подгруппы Леви или, соответственно, противоположной подгруппы P^-. Мы покажем, что при некоторых естественных ограничениях $\mathrm{E}_P(R)$ не зависит и от выбора самой параболической подгруппы P и, в частности, является нормальной подгруппой $G(R)$.

Напомним, что основным инвариантом расщепимой редуктивной группы G над алгебраически замкнутым полем (или кольцом, Exp. XXII) является ее система корней Φ относительно произвольного расщепимого максимального тора T. Каждая параболическая подгруппа P расщепимой группы с точностью до сопряженности характеризуется своим типом $J \subseteq \Pi$, где Π — произвольная система простых корней в Φ. Классическое обобщение этих понятий на случай нерасщепимой редуктивной группы над алгебраически незамкнутым полем k (или локальным кольцом, Exp. XXVI §7) состоит в замене системы корней Φ на относительную систему корней ${}_k\Phi$ в смысле Бореля–Титса [1, 27], и соответствующей адаптации понятия типа параболической подгруппы (см. также параграф 2).

В случае произвольной редуктивной группы G над кольцом R, обозначим через G^{ad} соответствующую присоединенную алгебраическую группу. Мы называем параболическую подгруппу P в G *строго собственной*, если для любого максимального идеала M в R проекция параболической подгрупы P_{R_M} на каждый сомножитель G_i, участвующий в разложении $G^{ad}_{R_M} = \prod_i G_i$ полупростой группы $G^{ad}_{R_M}$ в произведение простых алгебраических групп, является собственной подгруппой G_i. В терминологии Бореля–Титса (Exp. XXVI §7) это условие эквивалентно следующему: тип параболической подгруппы P_{R_M} группы G_{R_M} имеет нетривиальное пересечение с каждой неприводимой компонентой относительной системы корней G_{R_M}.

Основным результатом настоящей работы является следующая теорема.

Теорема 1. *Предположим, что для любого максимального идеала M кольца R все неприводимые компоненты относительной системы корней группы G_{R_M} имеют ранг хотя бы 2. Тогда $\mathrm{E}_P(R)$ не зависит от выбора строго собственной параболической подгруппы P. В частности, $\mathrm{E}(R) = \mathrm{E}_P(R)$ нормальна в $G(R)$.*

Замечание 1. Условие, что все неприводимые компоненты относительной системы корней группы G_{R_M} имеют ранг хотя бы 2, эквивалентно существованию расщепимых торов ранга 2 в простых сомножителях присоединенной группы $G^{ad}_{R_M}$.
Замечание 2. По существу, Теорема утверждает, что если P и P' — строго собственные параболические подгруппы в G, то в следующих двух случаях $E_{P'}(R) = E_P(R)$:
- когда P и P' — (локально) сопряженные параболические подгруппы;
- когда $P \leq P'$ — вложенные параболические подгруппы.

Во втором случае условие на ранги неприводимых компонент относительных систем корней можно опустить (Лемма 12).

Ключевым моментом в доказательстве Теоремы 1 является применение аналога леммы Квиллена–Суслина (Лемма 17), которая, по существу, сводит задачу к случаю

[2]В дальнейшем все ссылки, начинающиеся с Exp., являются ссылками на SGA 3 [16].

локального кольца R. K_0-аналог этой леммы возник в решении Квиллена [22] проблемы Серра, а K_1-версия, которой пользуемся мы, предложена Суслиным [5]. Над локальным кольцом утверждение теоремы справедливо даже без ограничения на ранг относительной системы корней и проверяется сравнительно несложно благодаря теореме о локальной сопряженности минимальных параболических подгрупп (Exp. XXVI § 5).

Основным техническим приемом является использование относительных корневых подгрупп группы G. Именно, в параграфах 3–4 мы определяем *систему относительных корней* Φ_P группы G по отношению к произвольной параболической подгруппе P, обобщая классическое определение относительных корней Бореля и Титса [1], упомянутое выше. В отличие от классического случая, Φ_P не обязательно является системой корней. Далее, с помощью строго плоского спуска для каждого относительного корня $A \in \Phi_P$ мы строим (параграф 4, Теорема 2) некоторый проективный R-модуль V_A и замкнутое вложение групповых схем

$$X_A\colon\ \mathrm{W}(V_A) \to G,$$

где $\mathrm{W}(V_A)$ — аффинная групповая схема, соответствующая V_A. Элементы $X_A(v)$, $A \in \Phi_P$, $v \in V_A$, группы $G(R)$ являются аналогами элементарных корневых унипотентов в расщепимых группах. В частности, они порождают элементарную подгруппу $\mathrm{E}_P(R)$ и удовлетворяют коммутационным соотношениям, обобщающим коммутационную формулу Шевалле (Леммы 9, 10):

$$[X_A(v), X_B(u)] = \prod_{i,j>0} X_{iA+jB}(N_{ABij}(v,u)),$$

где $N_{ABij} : V_A \times V_B \to V_{iA+jB}$ — некоторые полиномиальные отображения, однородные степени i по первому аргументу и степени j по второму. При определенных условиях получающиеся “коэффициентные отображения” N_{ABij} сюръективны, что соответствует обратимости коэффициентов в расщепимом случае.

Авторы выражают благодарность Николаю Александровичу Вавилову за неизменное внимание и всестороннюю поддержку.

2 Локальные оснащения и параболические подгруппы

Пусть G — редуктивная алгебраическая группа над R. Напомним, что *оснащением* (épinglage, Exp. XXIII Déf 1.1) группы G называется набор $\mathcal{E}$, состоящий из корневых данных $\mathcal{R} = (\mathrm{X}, \mathrm{X}^\vee, \Phi, \Phi^\vee, \Pi)$ с фиксированным базисом простых корней Π, расщепимого максимального тора T в G, изоморфизма $\mathrm{X}^*(T) \simeq \mathrm{X}$, где $\mathrm{X}^*(T)$ — решетка характеров T, и выбора для каждого *простого* корня $\alpha \in \Pi$ изоморфизма $x_\alpha\colon\ \mathbf{G}_{\mathrm{a}} \to X_\alpha$ на соответствующую корневую подгруппу. Оснащение однозначно продолжается до *системы Шевалле*, т.е. набора изоморфизмов x_α для всех корней $\alpha \in \Phi$, для которого выполняются коммутационные формулы Шевалле. Группа G, для которой можно выбрать оснащение, называется *расщепимой*.

Если в расщепимой группе G выбраны два оснащения $\mathcal{E}$ и $\mathcal{E}'$, то существует единственный внутренний автоморфизм ι этой группы, который локально в fpqc-топологии он переводит одно оснащение в другое. Точнее, ι переводит T в T', и существуют fpqc-покрытие $\coprod \operatorname{Spec} S_\mu \to \operatorname{Spec} R$, элементы $g_\mu \in G(S_\mu)$ и изоморфизмы $\gamma_\mu\colon\ \mathcal{R} \to \mathcal{R}'$ (при этом предполагается, что $\gamma_\mu(\Pi) = \Pi'$) такие, что над S_μ морфизм ι представляется в виде сопряжения при помощи g_μ, а изоморфизм

$$\mathrm{X}'_{S_\mu} \simeq \mathrm{X}^*(T'_\mu) \simeq \mathrm{X}^*(T_\mu) \simeq \mathrm{X}_{S_\mu},$$

индуцированный ι, совпадает с γ_μ^{-1}, и $\iota \circ x_\alpha = x'_{\gamma_\mu(\alpha)}$ для всех $\alpha \in \Phi$ (см. Exp. XXIV, Lemme 1.5). Ясно, что если $\operatorname{Spec} S_\mu$ и $\operatorname{Spec} S_\nu$ пересекаются (т.е. $S_\mu \otimes_R S_\nu \neq 0$), то $\gamma_\mu = \gamma_\nu$. Таким образом, множество изоморфизмов $\{\gamma_\mu\}$ не зависит от выбора покрытия; будем называть их *склеивающими симметриями* между $\mathcal{E}$ и $\mathcal{E}'$.

Пусть P — параболическая подгруппа (Exp. XXVI Déf. 1.1) в расщепимой группе G. Оснащение $\mathcal{E}$ называется *совместимым с* P, если существует такое параболическое множество корней Ψ, $\Pi \subseteq \Psi \subseteq \Phi$, что P порождена (в алгебраическом смысле) тором T и корневыми подгруппами X_γ, $\gamma \in \Psi$. При этом, в частности, унипотентный радикал U_P группы P порожден X_α, $\alpha \in \Psi \setminus -\Psi$. Если в P выбрана некоторая подгруппа Леви L_P, то оснащение называется *совместимым с парой* P *и* L_P, если группа L_P порождена T и X_α, $\alpha \in \Psi \cap -\Psi$, то есть является единственной подгруппой Леви в P, содержащей тор T (Exp. XXVI Prop. 1.12).

Если в G выбраны два оснащения $\mathcal{E}$ и $\mathcal{E}'$, совместимые с P, то элементы g_μ, осуществляющие переход от одного к другому, лежат в $P(S_\mu)$ (Exp. XXVI Prop. 1.15). Если эти оснащения, сверх того, совместимы с некоторой подгруппой Леви L_P, то элементы g_μ лежат в $\mathrm{L}_P(S_\mu)$ (Exp. XXVI Cor. 1.8).

Предположим теперь, что G — произвольная (т.е. не обязательно расщепимая) редуктивная алгебраическая группа. Тогда G расщепима локально в этальной, а значит, и в fpqc-топологии (Exp. XXII Cor. 2.3).

Пусть P — параболическая подгруппа в G. Тогда локально в fpqc-топологии можно выбрать оснащение G, совместимое с P (Exp. XXVI Lemme 1.14). Так как G является редуктивной группой над аффинной схемой $\operatorname{Spec} R$, группа P обладает некоторой подгруппой Леви L_P (Exp. XXVI Cor. 2.3). Из того, что локально в этальной топологии L_P содержит максимальный тор группы G, следует, что локально в fpqc-топологии можно выбрать оснащение G, совместимое с P и L_P.

Локальным оснащением будем называть набор данных τ, состоящий из аффинного открытого подмножества $U_\tau \subseteq \operatorname{Spec} R$, его строго плоского аффинного расширения $\operatorname{Spec} S_\tau \to U_\tau$, над которым G расщепляется, и оснащения $\mathcal{E}_\tau$ группы G_{S_τ}.

Рассмотрим категорию, объектами которой являются локальные оснащения, а морфизмами между двумя объектами — графовые изоморфизмы соответствующих диаграмм Дынкина D_τ. Таким образом, рассматриваемая категория является *симметрическим группоидом* $\operatorname{Sym}(\{D_\tau\})$, определенным семейством всех диаграмм Дынкина локальных расщеплений.

Два объекта τ и σ задают два оснащения группы $G_{S_\tau \otimes S_\sigma}$; соответственно, определены склеивающие симметрии из $\mathcal{R}_\tau$ в $\mathcal{R}_\sigma$, которые индуцируют графовые изоморфизмы диаграмм Дынкина D_τ и D_σ. Определим *склеивающий группоид* Γ как подгруппоид в $\operatorname{Sym}(\{D_\tau\})$, порожденный всеми склеивающими изоморфизмами. Группу автоморфизмов объекта D_τ в группоиде Γ будем обозначать через Γ_τ; таким образом, Γ_τ — некоторая подгруппа в $\operatorname{Aut}(D_\tau)$. Например, в случае, когда $R = k$ — поле, а $S_\tau = K$, где K/k — расширение Галуа, Γ_τ совпадает с образом группы Галуа $\operatorname{Gal}(K/k)$ относительно $*$-действия [27].

Рассмотрим какой-нибудь класс изоморфности ξ локальных оснащений, и определим открытое подмножество U_ξ как объединение всех U_τ по $\tau \in \xi$. Несложно видеть, что U_ξ образуют разбиение $\operatorname{Spec} R$; в частности, они являются открыто-замкнутыми аффинными подсхемами. Поскольку $\operatorname{Spec} R$ квазикомпактен, количество классов изоморфности конечно. Так что можно записать $U_\xi = \operatorname{Spec} R_\xi$, причем $R \simeq \prod\limits_\xi R_\xi$.

Нетрудно видеть, что $\mathrm{E}_P(R) \simeq \prod\limits_\xi \mathrm{E}_{P_{R_\xi}}(R_\xi)$ для любой параболической подгруппы P, поэтому большинство вопросов про элементарную подгруппу сводится к случаю, когда группоид состоит из одного класса изоморфности.

Дадим теперь соответствующее определение типа параболической подгруппы P. Рассмотрим локальные оснащения τ, совместимые с P. Каждая группа P_{S_τ} является стандартной параболической подгруппой, соответствующей некоторому подмножеству $J_\tau \subseteq \Pi_\tau$ такому, что P_{S_τ} порождена соответствующим тором T_τ и корневыми подгруппами, отвечающими корням, в разложение которых простые корни из J_τ входят с неотрицательными коэффициентами. Набор всех J_τ инвариантен относительно действия Γ (в частности, каждое множество J_τ инвариантно относительно Γ_τ). Очевидно, его можно единственным образом доопределить для любого локального оснащения τ (не обязательно совместимого с P) с сохранением свойства инвариантности. Полученный набор $\{J_\tau\}$ будем называть *типом* P.

Постоянные схемы D_τ над S_τ можно склеить вдоль склеивающих изоморфизмов и получить скрученную постоянную схему над R, которая называется *схемой Дынкина* (см. Exp XXIV § 3). Аналогично, открыто-замкнутые подсхемы J_τ над S_τ можно склеить и получить открыто-замкнутую подсхему в схеме Дынкина, которая в SGA 3 и называется типом параболической подгруппы. Нам, однако, будут более удобны изложенные выше теоретико-множественные понятия.

В случае, когда R локальное кольцо, среди типов параболических подгрупп существует наибольший по включению, отвечающий *минимальной* параболической подгруппе (Exp. XXVI Cor. 5.7).

3 Относительные корни

На протяжении данного параграфа Φ — приведенная система корней в l-мерном евклидовом пространстве со скалярным произведением $(\ ,\ )$ и фиксированной системой простых корней $\Pi = \{\alpha_1, \dots, \alpha_l\}$ (в случае, когда Φ неприводима, нумерация следует [14]). Мы отождествляем элементы Π с вершинами соответствующей диаграммы Дынкина D.

Зафиксируем некоторое подмножество $J \subseteq \Pi$. Пусть Δ — подсистема Φ, порожденная $\Pi \setminus J$. Каждый корень $\alpha \in \Phi$ единственным образом представляется в виде

$$\alpha = \sum_{1 \le r \le l} m_r(\alpha)\alpha_r.$$

Для $\alpha \in \Phi \setminus \Delta$ мы полагаем

$$\alpha_J = \sum_{\substack{1 \le r \le l, \\ \alpha_r \in J}} m_r(\alpha)\alpha_r.$$

Мы будем называть линейную комбинацию a простых корней из J *шаблоном* (“shape” в [9]), если существует корень $\alpha \in \Phi \setminus \Delta$ такой, что $\alpha_J = a$. Таким образом, α — корень шаблона α_J.

Лемма 1. *Пусть $\alpha, \beta, \gamma \in \Phi$ таковы, что $\alpha + \beta + \gamma$ является корнем, и среди α, β, γ нет противоположных. Тогда по крайней мере две из сумм $\alpha+\beta, \alpha+\gamma, \beta+\gamma$ являются корнями.*

Proof. Можно считать, что система Φ неприводима. Положим $\delta = \alpha + \beta + \gamma$. Так как $(\delta, \alpha+\beta+\gamma) = (\delta, \delta) > 0$, одно из произведений (δ, α), (δ, β), (δ, γ) является положительным, пусть это (δ, α). Тогда $\delta - \alpha = \beta + \gamma$ является корнем. Далее, если $(\alpha, \beta + \gamma) < 0$, то одно из произведений (α, β), (α, γ) тоже отрицательно, а значит, $\alpha + \beta$ или $\alpha + \gamma$ является корнем. Если же $(\alpha, \beta + \gamma) \ge 0$, то $(\delta, \beta + \gamma) = (\alpha, \beta + \gamma) + (\beta + \gamma, \beta + \gamma) > 0$, откуда одно из произведений (δ, β), (δ, γ) положительно, то есть $\delta - \beta$ или $\delta - \gamma$ — корень.

□

Лемма 2. *Пусть a, b, c — такие шаблоны, что $a + b = c$. Тогда для любого корня γ шаблона c существуют такой корень α шаблона a и такой корень β шаблона b, что $\alpha + \beta = \gamma$.*

Proof. Из равенства $a+b=c$ следует, что шаблоны a,b,c являются линейными комбинациями простых корней из одной неприводимой компоненты Φ, поэтому можно считать, что система Φ неприводима. Мы можем представить γ в виде суммы $\gamma = \alpha_0+\beta_0+\lambda_1+\ldots+\lambda_n$, где α_0 — корень шаблона a, β_0 — корень шаблона b, $\lambda_i\in\Delta$. Проведем индукцию по n. База $n=0$ очевидна. Если $(\gamma,\alpha_0)>0$ или $(\gamma,\beta_0)>0$, то $\gamma-\alpha_0$ или, соответственно, $\gamma-\beta_0$ является корнем, следовательно, мы можем взять $\alpha=\alpha_0$, $\beta=\gamma-\alpha_0$ или $\beta=\beta_0$, $\alpha=\gamma-\beta_0$. В противном случае из $(\gamma,\gamma)>0$ следует, что существует такое λ_i, что $(\gamma,\lambda_i)>0$, то есть $\gamma'=\gamma-\lambda_i$ является корнем. По предположению индукции $\gamma'=\alpha'+\beta'$, где α' — некоторый корень шаблона a, а β' — некоторый корень шаблона b. Остается заметить, что по Лемме 1 одна из сумм $\alpha'+\lambda_i,\beta'+\lambda_i$ является корнем. □

Пусть Γ — подгруппа $\mathrm{Aut}\,(D)$, J — подмножество Π, инвариантное относительно действия Γ. Будем считать, что Γ тривиально действует на $\mathbb{Z}$. Тогда абелева группа $\mathrm{Map}_{\Gamma}(J,\mathbb{Z})$ всех Γ-эквивариантных отображений из J в $\mathbb{Z}$ является свободной абелевой группой, ранг которой совпадает с числом орбит, на которые распадается J. Определим на решетке корней $\mathbb{Z}\,\Phi$ линейное отображение

$$\pi=\pi_{J,\Gamma}\colon\ \mathbb{Z}\,\Phi\to\mathrm{Map}_{\Gamma}(J,\mathbb{Z})$$

следующим образом: вектор v переводится в отображение, которое отправляет $\alpha_i\in J$ в сумму коэффициентов v при простых корнях α_j, образующих орбиту α_i относительно Γ.

Множество $\pi(\Phi)\setminus\{0\}$ будем называть *множеством* (или *системой*) *относительных корней* и обозначать через $\Phi_{J,\Gamma}$. *Рангом* $\mathrm{rank}\,\Phi_{J,\Gamma}$ множества относительных корней будем называть ранг группы $\mathrm{Map}_{\Gamma}(J,\mathbb{Z})$.

Заметим сразу, что в случае, когда R — локальное кольцо, Φ — система корней редуктивной алгебраической группы G, J — тип минимальной параболической подгруппы, а Γ — группа автоморфизмов объекта склеивающего группоида, то $\Phi_{J,\Gamma}$ образует в действительности систему корней (возможно, неприведенную, т.е. типа BC_l). Если группа G полупроста, ранг этой системы корней равен рангу максимального расщепимого тора в G. Подробности см. в Exp. XXVI § 7 или (в случае поля) [1, § 5]. В общем случае, однако, $\Phi_{J,\Gamma}$ системой корней не является, и нам придется переопределить некоторые стандартные понятия, относящиеся к системам корней.

Ясно, что любой относительный корень $A\in\Phi_{J,\Gamma}$ единственным образом представляется в виде линейной комбинации относительных корней, входящих в $\pi(\Pi)$. *Уровнем* $\mathrm{lev}(A)$ относительного корня A будем называть сумму коэффициентов в его разложении.

Относительный корень $A\in\Phi_{J,\Gamma}$ будем называть *положительным* (соответственно, *отрицательным*), если он представляется в виде линейной комбинации элементов $\pi(\Pi)$ с неотрицательными (соответственно, неположительными) коэффициентами. Множества положительных и отрицательных относительных корней будут обозначаться $\Phi^+_{J,\Gamma}$ и $\Phi^-_{J,\Gamma}$ соответственно. Очевидно, $A\in\Phi^\pm_{J,\Gamma}$ тогда и только тогда, когда $\pi^{-1}(A)\subseteq\Phi^\pm$, и, в частности, $\Phi_{J,\Gamma}=\Phi^+_{J,\Gamma}\cup\Phi^-_{J,\Gamma}$.

Заметим, что группа автоморфизмов Γ действует перестановками на множестве неприводимых компонент системы Φ. Если это действие является транзитивным, систему относительных корней $\Phi_{J,\Gamma}$ будем называть *неприводимой*. Нетрудно видеть, что любая система относительных корней является дизъюнктным объединением неприводимых систем относительных корней — своих *неприводимых компонент*.

Ясно, что если $\alpha_i,\alpha_j\in J$, то $\pi(\alpha_i)=\pi(\alpha_j)$ тогда и только тогда, когда α_i и α_j переводятся друг в друга элементом Γ. Кроме того, $\pi|_\Delta=0$, то есть значение π на корне $\alpha\in\Phi$ совпадает со значением π на соответствующем шаблоне, $\pi(\alpha)=\pi(\alpha_J)$. Если Γ — тривиальная группа, то относительные корни находятся в очевидном взаимнооднозначном соответствии с шаблонами относительно J.

Лемма 3. *Пусть $\alpha, \beta \in \Phi$. Тогда $\pi(\alpha) = \pi(\beta)$ тогда и только тогда, когда существует элемент Γ, переводящий α_J в β_J.*

Proof. Случай, когда Γ — тривиальная группа, очевиден. Далее, нетрудно видеть, что систему корней Φ можно считать неприводимой. Кроме того, для доказательства мы можем заменить подмножество J на любое подмножество $J' \subseteq \Pi$, отличающееся от него на объединение нескольких одноэлементных Γ-орбит в Π. Тогда в случае $\Phi = D_l$, $l \geq 4$, можно считать, что множество J состоит ровно из одной орбиты, и утверждение непосредственно очевидно. Рассмотрим оставшиеся случаи $\Phi = A_l$, $l \geq 1$, и $\Phi = E_6$.

Нетрудно видеть, что в случае $\Phi = A_l$ множество шаблонов относительно Γ-инвариантного множества J находится во взаимнооднозначном соответствии с корнями некоторой системы корней $\Phi' = A_m$, $m \leq l$, причем действие Γ на этом множестве отождествляется с действием $\mathrm{Aut}\,(D')$, где D' — диаграмма Дынкина этой системы. Поэтому можно считать, что $J = \Pi$. Тогда $\Phi_{J,\Gamma}$ можно отождествить с относительной системой корней в смысле Бореля–Титса некоторой квазирасщепимой алгебраической группы типа A_m над полем, поэтому наше утверждение следует из общей теории [1, 27].

Аналогично, если $\Phi = E_6$ и $J \supseteq \{\alpha_1, \alpha_6\} \cup \{\alpha_3, \alpha_5\}$ содержит две нетривиальные Γ-орбиты, то мы можем считать, что $J = \Pi$, и снова $\Phi_{J,\Gamma}$ можно отождествить с относительной системой корней квазирасщепимой группы в смысле Бореля–Титса. Если же J состоит из единственной нетривиальной Γ-орбиты, то есть $J = \{\alpha_1, \alpha_6\}$ или $J = \{\alpha_3, \alpha_5\}$, утверждение очевидно — достаточно заметить, что в E_6 нет корня с коэффициентами 0 и 2 при простых корнях α_3 и α_5. $\square$

Лемма 4. *Пусть $A, B, C \in \Phi_{J,\Gamma}$ и $A + B = C$. Тогда для любого корня $\gamma \in \pi^{-1}(C)$ существуют такие корни $\alpha \in \pi^{-1}(A)$, $\beta \in \pi^{-1}(B)$, что $\alpha + \beta = \gamma$.*

Proof. Если группа автоморфизмов Γ тривиальна, то относительные корни совпадают с шаблонами, и утверждение прямо следует из Леммы 2. В противном случае, очевидно, достаточно найти такие шаблоны a, b, c, что $\pi(a) = A$, $\pi(b) = B$, $\pi(c) = C$ и $a + b = c$. Далее, перенеся, если необходимо, некоторые из корней A, B, C в другую часть равенства $A + B = C$, можно считать, что $A, B, C \in \Phi^+_{J,\Gamma}$. Как и в доказательстве Леммы 3, мы можем считать, что система корней Φ неприводима, и исключить из множества J одноэлементные Γ-орбиты. Поэтому случай $\Phi = D_l$, $l \geq 4$, снова очевиден. Для доказательства остальных случаев обозначим через σ нетривиальный элемент Γ.

В случае $\Phi = A_l$, снова аналогично доказательству Леммы 3, можно считать, что $J = \Pi$, то есть шаблоны совпадают с корнями, и система относительных корней является относительной системой корней в смысле Бореля–Титса некоторой квазирасщепимой алгебраической группы над полем, Γ является образом соответствующей группы Галуа относительно $*$-действия [1, 27]. Так как мы можем пренебречь одноэлементной орбитой, достаточно рассмотреть случай, когда $l = 2n$ четно. Тогда $\Phi_{J,\Gamma} = BC_n$. Известно [1], что в этом случае любой элемент группы Вейля $\Phi_{J,\Gamma}$ может быть поднят до элемента группы Вейля Φ, поэтому мы можем считать, что один из корней A, B, скажем, A, является простым корнем системы $\Phi_{J,\Gamma}$, то есть $A = \pi(\alpha_i)$, или удвоенным коротким простым корнем, то есть $A = \pi(\alpha_n + \alpha_{n+1})$. Пусть $\alpha \in \pi^{-1}(B)$, $\gamma \in \pi^{-1}(C)$, $J' = \Pi \setminus \pi^{-1}(A)$. Тогда $\alpha_{J'} = \gamma_{J'}$, поэтому по Лемме 3 можно считать, что $\alpha_{J'} = \gamma_{J'}$. Нетрудно видеть, что тогда $\pi(\alpha) + A = \pi(\gamma)$ влечет $\alpha + \alpha_i = \gamma$ или $\alpha + \sigma(\alpha_i) = \gamma$ в первом случае, и $\alpha + \alpha_n + \alpha_{n+1} = \gamma$ во втором.

Пусть теперь $\Phi = E_6$, и $\alpha, \beta, \gamma \in \Phi^+$ — такие корни, что $\pi(\alpha) = A$, $\pi(\beta) = B$ и $\pi(\gamma) = C$. Если шаблоны α_J, β_J, γ_J не содержат в разложении по простым корням коэффициентов, больших 1, то задача сводится к случаю $\Phi = A_5$, разобранному выше. В противном случае $\alpha_3, \alpha_5 \in J$ и, не умаляя общности, $m_3(\gamma) = 2$. Тогда $m_5(\gamma) = 2$ или $m_5(\gamma) = 1$. Если $J = \{\alpha_3, \alpha_5\}$, то, как нетрудно видеть, доказательство завершается применением σ к одному из шаблонов α_J, β_J, поэтому предположим, что $J = \{\alpha_1, \alpha_3, \alpha_5, \alpha_6\}$.

По случаю $J = \{\alpha_3, \alpha_5\}$ можно считать, что $\alpha_{J'} + \beta_{J'} = \gamma_{J'}$, где $J' = \{\alpha_3, \alpha_5\}$. Если $m_5(\gamma) = 2$, то $m_1(\gamma) = m_6(\gamma) = 1$. Если в разложении одного из корней α, β

присутствует коэффициент ≥ 2, то, не умаляя общности, $m_3(\alpha) = 2$, $m_5(\alpha) = 1$, откуда $m_1(\alpha) = 1$ и $m_3(\beta) = 0$, $m_5(\beta) = 1$. Тогда $m_1(\beta) = 0$ и $m_6(\alpha) + m_6(\beta) = m_6(\gamma)$, так что $\alpha_J + \beta_J = \gamma_J$. При $m_3(\alpha) = m_5(\alpha) = m_3(\beta) = m_5(\beta) = 1$ следует воспользоваться случаем $J = \{\alpha_1, \alpha_6\}$. Оставшийся случай $m_3(\gamma) = 2$, $m_5(\gamma) = 1$ разбирается аналогично. □

Лемма 5. *Если относительный корень $A \in \Phi_{J,\Gamma}$ содержится в неприводимой компоненте ранга ≥ 2, то существуют такие неколлинеарные $B, C \in \Phi_{J,\Gamma}$, что $A = B + C$. Если $\Phi = G_2$, то B, C можно выбрать так, что $B - C \notin \Phi_{J,\Gamma}$.*

Proof. Мы можем предполагать, что система корней Φ неприводима. Рассмотрим сначала случай, когда $\Phi = G_2$. Так как $\operatorname{rank} \Phi_{J,\Gamma} \geq 2$, в этом случае $\Phi = \Phi_{J,\Gamma}$ и относительные корни совпадают с обычными. Так как любой корень переводится элементом группы Вейля в простой, можно считать, что A — простой корень в G_2. Тогда следует положить $B = \alpha_1 + \alpha_2$, $C = -\alpha_2$ в случае, когда $A = \alpha_1$ — короткий простой корень, и $B = 3\alpha_1 + 2\alpha_2$, $C = -(3\alpha_1 + \alpha_2)$ в случае, когда $A = \alpha_2$ — длинный простой корень. Перейдем к случаю $\Phi \neq G_2$. Можно считать, что A — положительный относительный корень, то есть $\pi^{-1}(A) \subseteq \Phi^+$.

Предположим сначала, что $A = k\pi(\alpha_r)$, где $\alpha_r \in \Pi$ — простой корень, $k > 0$. Пусть $\alpha_s \in \Pi$ — ближайший к α_r на диаграмме Дынкина корень из другой Γ-орбиты, содержащейся в J. Легко видеть, что для любого корня $\alpha \in \pi^{-1}(A)$ существует корень $\beta \in \pi^{-1}(\alpha_s)$ такой, что $(\alpha, \beta) < 0$ и, следовательно, $\alpha + \beta \in \Phi$. Действительно, для любого $\alpha \in \pi^{-1}(A)$ мы имеем $m_s(\alpha) = 0$ по определению π, поэтому в качестве β можно взять сумму простых корней, образующих на диаграмме Дынкина цепочку, соединяющую α_s и ближайший к нему простой корень, входящий в разложение α с ненулевым коэффициентом. Теперь можно рассмотреть относительные корни $B = \pi(\alpha + \beta)$ и $C = \pi(-\beta)$. Так как $\pi(\alpha) = k\pi(\alpha_r)$, а $\pi(-\beta)$ содержит в разложении $\pi(\alpha_s)$, выбранные относительные корни неколлинеарны.

Рассмотрим теперь случай, когда $A \neq k\pi(\alpha_r)$. Для любого корня $\alpha \in \pi^{-1}(A)$ существует такой набор простых корней $\beta_1, \ldots, \beta_n \in \Pi$, что $\alpha = \beta_1 + \ldots + \beta_n$, и для любого $1 \leq i \leq n$ сумма $\beta_1 + \ldots + \beta_i$ является корнем. Пусть i — наименьшее возможное значение индекса, для которого $\beta_{i+1}, \ldots, \beta_n \in \Delta$. Тогда $\beta_i \in J$ и $\pi(\beta_1 + \ldots + \beta_{i-1} + \beta_i) = A$. Положим $B = \pi(\beta_1 + \ldots + \beta_{i-1})$ и $C = \pi(\beta_i)$. Относительные корни B и C неколлинеарны, поскольку в противном случае мы имели бы $A = k\pi(\beta_i)$ для некоторого $k > 0$. □

4 Относительные корневые подгруппы

В этом параграфе мы предполагаем, что склеивающий группоид состоит из одного класса изоморфности; P — фиксированная параболическая подгруппа G типа $\{J_\tau\}$. Тогда отображения $\pi_\tau \colon \mathrm{X}^*(T_\tau) \to \mathrm{Map}_\Gamma(J_\tau, \mathbb{Z})$ согласованы друг с другом, что позволяет отождествить множества относительных корней $\Phi_{J_\tau, \Gamma_\tau}$ между собой. Полученное множество будет обозначаться через Φ_P.

Пусть Ψ — *унипотентное замкнутое* подмножество относительных корней, т.е. подмножество, содержащее вместе с любыми двумя относительными корнями их сумму (если она тоже является относительным корнем) и не содержащее двух коллинеарных противонаправленных относительных корней. Тогда прообраз $\pi^{-1}(\Psi)$ — унипотентное замкнутое подмножество в Φ.

Зафиксируем в P некоторую подгруппу Леви L_P. Ясно, что локальные оснащения τ, совместимые с P и L_P, образуют покрытие $\operatorname{Spec} R$. Для любого такого τ определим $\mathrm{U}_{\Psi,\tau}$ как подгруппу в G_{S_τ}, порожденную всеми корневыми подгруппами $X_{\alpha,\tau}$ по $\alpha \in \pi^{-1}(\Psi)$. Поскольку для любых двух оснащений τ, σ, совместимых с L_P, переход от одного к другому осуществляется локально посредством сопряжения элементом L_P, $\mathrm{U}_{\Psi,\tau}$ переходит в $\mathrm{U}_{\Psi,\sigma}$. Поэтому $\mathrm{U}_{\Psi,\tau}$ склеиваются в некоторую глобальную подгруппу U_Ψ группы G.

В частности, определены подгруппы $\mathrm{U}_{(A)}$, где (A) означает подмножество, состоящее из всех положительных кратных A относительных корней. Легко видеть, что $\mathrm{U}_{(iA)}$ нормальна в $\mathrm{U}_{(A)}$ для любого $i \geq 1$.

Для конечнопорожденного проективного R-модуля V функтор $S \mapsto V \otimes_R S$ представим аффинной групповой схемой $\mathrm{W}(V) = \operatorname{Spec} \operatorname{Sym}^*(V^*)$, где V^* — двойственный модуль, Sym^* — симметрическая алгебра. Таким образом, морфизм *схем* $\mathrm{W}(V_1) \to \mathrm{W}(V_2)$ задается элементом $\operatorname{Sym}^*(V_1^*) \otimes_R V_2$. Если этот элемент лежит в $\operatorname{Sym}^d(V_1^*) \otimes_R V_2$, будем называть морфизм *однородным* степени d. В частности, морфизмы степени 1 линейны.

Теорема 2. *Для всех относительных корней $A \in \Phi_P$ существуют проективные модули V_A над R и замкнутые вложения* схем

$$X_A \colon \mathrm{W}(V_A) \to G$$

такие, что при переходе на каждое локальное оснащение τ, совместимое с P и L_P, модули $V_A \otimes_R S_\tau$ становятся свободными, а отображения X_A принимает вид (после некоторого выбора базиса $e_1, \ldots, e_{k_A}$ в $V_A \otimes_R S_\tau$)

$$X_A(e_1 a_1 + \ldots + e_{k_A} a_{k_A}) = \prod_{j=1}^{k_A} x_{\gamma_j}(a_j) \cdot \prod_{i \geq 2} \prod_{\pi(\beta) = iA} x_\beta(p^i_{\beta,\tau}(a_1, \ldots, a_{k_A})), \qquad (1)$$

где γ_j — все корни из $\pi^{-1}(A)$, а каждый $p^i_{\beta,\tau}$ является однородным многочленом степени i (произведение берется в любом фиксированном порядке, совместимом с уровнем).

Кроме того, построенные отображения обладают следующими свойствами:

1. *$X_A(0) = 1$;*
2. *Для каждого элемента $g \in \mathrm{L}_P$ выполнено тождество*
$$g X_A(v) g^{-1} = \prod_{i \geq 1} X_{iA}(\varphi^i_{g,A}(v)),$$
где $\varphi^i_{g,A} \colon \mathrm{W}(V_A) \to \mathrm{W}(V_{iA})$ однородно степени i;
3. *Выполнено тождество*
$$X_A(v) X_A(w) = X_A(v + w) \prod_{i > 1} X_A(q^i_A(v, w))$$
где $q^i_A \colon \mathrm{W}(V_A) \times_{\operatorname{Spec} R} \mathrm{W}(V_A) = \mathrm{W}(V_A \oplus V_A) \to \mathrm{W}(V_{iA})$ однородно степени i.

Proof. Над локальным оснащением τ определим $V_{A,\tau}$ как $S_\tau^{k_A}$, где k_A — число корней из $\pi^{-1}(A)$, и рассмотрим морфизмы схем

$$Y_{A,\tau} \colon \mathrm{W}(V_{A,\tau}) \to U_{A,\tau},$$

заданные по формуле

$$Y_{A,\tau}(e_1 a_1 + \ldots + e_{k_A} a_{k_A}) = \prod_j x_{\gamma_j}(a_j),$$

где γ_j — все корни из $\pi^{-1}(A)$ в некотором порядке. Коммутационная формула Шевалле показывает, что над $\operatorname{Spec} S_\tau$ для $Y_{A,\tau}$ выполнены аналоги утверждений 1 и 3 теоремы, а также утверждения 2 для элементов $(\mathrm{L}_P)_\tau$, лежащих в торе T_τ или корневых подгруппах. Поскольку над S_τ большая клетка Ω_{L_P} плотна в L_P и порождается в абстрактном смысле тором и корневыми подгруппами, утверждение 2 выполнено для всех элементов $(\mathrm{L}_P)_\tau$.

Далее, для любых двух элементов покрытия имеет место равенство

$$\iota_{\sigma\tau}(Y_{A,\tau}(v)) = Y_{A,\sigma}(\varphi_{A,\sigma,\tau}(v)) \mod \mathrm{U}_{(2A)},$$

где $\varphi_{A,\sigma,\tau}\colon V_{A,\tau}\otimes_R S_\sigma \to V_{A,\sigma}\otimes_R S_\tau$ — линейные отображения; очевидно, они удовлетворяют соотношению 1-коцикла, так что при помощи них модули $V_{A,\tau}$ склеиваются в проективный R-модуль V_A. Это означает, что существуют линейные изоморфизмы $\theta_{A,\tau}\colon V_A\otimes_R S_\tau \to V_{A,\tau}$ такие, что $\varphi_{A,\sigma,\tau} = \theta_{A,\sigma}\circ(\theta_{A,\tau})^{-1}$.

Теперь индукцией по j будем находить такие сечения $X^j_{A,\tau}\colon V_{A,\tau}\to \mathrm{U}_{A,\tau}$, что выполнено соотношение

$$\iota_{\sigma\tau}(X^j_{A,\tau}(v)) = X^j_{A,\sigma}(\varphi_{A,\sigma,\tau}(v)) \mod \mathrm{U}_{((j+1)A)},$$

причем $X^j_{A,\tau}$ задаются формулой (1). После этого отображения $X^j_{A,\tau}$ с достаточно большим j, будучи аффинными, склеиваются в глобально определенное отображение $X_A\colon \mathrm{W}(V_A)\to \mathrm{U}_{(A)}$, и все его свойства, перечисленные в теореме, легко получаются спуском из коммутационных формул Шевалле.

Итак, положим $X^1_{A,\tau} = Y_{A,\tau}$. Пусть мы уже определили $X^j_{A,\tau}$ и хотим определить $X^{j+1}_{A,\tau}$. Будем искать его в виде

$$X^{j+1}_{A,\tau}(v) = X^j_{A,\tau}(v)Y_{(j+1)A,\tau}(\chi_\tau(v)),$$

где $\chi_\tau\colon V_{A,\tau}\to V_{(j+1)A,\tau}$ является полиномиальным однородным отображением. Мы хотим, чтобы выполнялось соотношение

$$\iota_{\sigma\tau}(X^j_{A,\tau}(v)Y_{(j+1)A,\tau}(\chi_\tau(v))) = X^j_{A,\sigma}(\varphi_{A,\sigma,\tau}(v))Y_{(j+1)A,\sigma}(\chi_\sigma(\varphi_{A,\sigma,\tau}(v))) \mod \mathrm{U}_{((j+2)A)},$$

иначе говоря,

$$\iota_{\sigma\tau}(X^j_{A,\tau}(v))^{-1}X^j_{A,\sigma}(\varphi_{A,\sigma,\tau}(v)) = Y_{(j+1)A,\sigma}(\varphi_{(j+1)A,\sigma,\tau}(\chi_\tau(v)) - \chi_\sigma(\varphi_{A,\sigma,\tau}(v))) \mod \mathrm{U}_{((j+2)A)}.$$

Обозначим через $\psi_{\sigma\tau}(v)$ единственный элемент $V_{(j+1)A,\sigma}\otimes_R S_\tau$ такой, что

$$\iota_{\sigma\tau}(X^j_{A,\tau}(v))^{-1}X^j_{A,\sigma}(\varphi_{A,\sigma,\tau}(v)) = Y_{(j+1)A,\sigma}(\psi_{\sigma\tau}(v)) \mod \mathrm{U}_{((j+2)A)};$$

тогда прямая проверка показывает, что

$$\psi_{\rho\tau} = \varphi_{(j+1)A,\rho,\sigma}\circ\psi_{\sigma\tau} + \psi_{\rho\sigma}\circ\varphi_{A,\sigma,\tau}.$$

Полагая $a_{\sigma\tau} = \theta^{-1}_{(j+1)A,\sigma}\circ\psi_{\sigma\tau}\circ\theta_{A,\tau}$, переписываем это равенство в виде

$$a_{\rho\tau} = a_{\rho\sigma} + a_{\sigma\tau}.$$

Поскольку любое аффинное покрытие ациклично с коэффициентами в $\mathrm{W}(V_{(j+1)A})$, и $\mathrm{H}^1(\operatorname{Spec}R, \mathrm{W}(V_{(j+1)A})) = 0$, найдутся функции b_τ со свойством

$$a_{\sigma\tau} = b_\tau - b_\sigma.$$

Теперь достаточно положить $\chi_\tau = \theta_{(j+1)A,\tau}\circ b_\tau\circ\theta^{-1}_{A,\tau}$, и тогда

$$\psi_{\sigma\tau} = \varphi_{(j+1)A,\sigma,\tau}\circ\chi_\tau - \chi_\sigma\circ\varphi_{A,\sigma,\tau}, \tag{2}$$

что и требуется.

Осталось показать, что отображения χ_τ можно выбрать полиномиальными однородными степени $j+1$. Из коммутационных формул Шевалле следует, что $\psi_{\sigma\tau}$ являются полиномиальными однородными степени $j+1$. Расширим базу до кольца многочленов $R[Z_1,\ldots,Z_{k_A}]$ и положим $v_Z = e_1Z_1+\ldots+e_{k_A}Z_{k_A}\in S_\tau[Z_1,\ldots,Z_{k_A}]^{k_A}$. Найдем $\chi_\tau(v_Z)$ как элемент $S_\tau[Z_1,\ldots,Z_{k_A}]^{k_{(j+1)A}}$ и оставим в каждом коэффициенте только однородную компоненту степени $j+1$; получившийся элемент обозначим через $\chi'_\tau(v_Z)$. Теперь для произвольного $v = e_1 a_1 + \ldots + e_{k_A} a_{k_A}$ полагаем $\chi'_\tau(v)$ равным образу $\chi'_\tau(v_Z)$ при гомоморфизме специализации

$$S_\tau[Z_1, \ldots, Z_{k_A}] \to S_\tau$$
$$Z_1 \mapsto a_1, \ldots, Z_{k_A} \mapsto a_{k_A}.$$

Легко видеть, что при таком определении нужное соотношение (2) все еще выполняется. Теорема доказана. □

Лемма 6. *Отображение*

$$X_\Psi \colon\ \mathrm{W}(\bigoplus_{A\in\Psi} V_A) \to \mathrm{U}_\Psi$$
$$(v_A)_A \mapsto \prod_A X_A(v_A),$$

где произведение берется в любом фиксированном порядке, совместимом с уровнем, является изоморфизмом схем.

Proof. Утверждение легко проверяется на каждом члене покрытия с использованием формулы (1), после чего нужный результат получается спуском. □

Лемма 7. *Предположим, что для любого $A \in \Psi$ в V_A выбрана конечная порождающая система $f_1^A, \ldots, f_{n_A}^A$, $n_A \geq 1$. Тогда для любого расширения колец $R \to S$ группа точек $U_\Psi(S)$ как абстрактная группа порождена всеми элементами вида $X_A(\xi f_i^A)$, $\xi \in S$, $A \in \Psi$, $1 \leq i \leq n_A$.*

Proof. Следует из пункта 3 Теоремы 2 и Леммы 6. □

Начиная с настоящего момента, зафиксируем на множестве относительных корней некоторый порядок, совместимый с уровнем. Тогда для любого унипотентного замкнутого множества $\Psi \subseteq \Phi_P$ мы можем определить некоторые гомоморфизмы

$$p_{\Psi,A} \colon\ \mathrm{U}_\Psi \to \mathrm{W}(V_A)$$

("коэффициент" при относительном корне A).

Лемма 8. *Для любого элемента $g \in \mathrm{U}_\Psi(R)$ существует $g(X) \in \mathrm{U}_\Psi(R[X])$ со свойствами $g(0) = 1$ и $g(1) = g$.*

Proof. Если $g = \prod_A X_A(v_A)$, положим $g(X) = \prod_A X_A(v_A X)$. □

5 Коммутационные формулы Шевалле

Мы продолжаем считать, что склеивающий группоид состоит из одного класса изоморфности и что в параболической подгруппе P зафиксирована некоторая подгруппа Леви L_P.

Для любых относительных корней $A, B \in \Phi_P$ мы обозначаем через (A, B) унипотентное замкнутое множество относительных корней, образованное всеми комбинациями $iA + jB$, $i, j > 0$, принадлежащими Φ_P.

Лемма 9. *Пусть A, B — относительные корни, причем $mA \neq -kB$ для любых $m, k \geq 1$. Тогда коммутант $[X_A(V_A), X_B(V_B)]$ содержится в $U_{(A,B)} = \prod\limits_{i,j>0} X_{iA+jB}(V_{iA+jB})$, и каждое отображение*

$$N_{ABij}\ :\ V_A \times V_B \to V_{iA+jB}$$
$$(v_A, v_B) \mapsto p_{(A,B),iA+jB}([X_A(v_A), X_B(v_B)])$$

однородно степени i по первому аргументу и степени j по второму.

Proof. Получается из коммутационной формулы Шевалле в расщепимой ситуации спуском при помощи Теоремы 2. □

Лемма 10. *Пусть $A, B, A+B \in \Phi_P$, и A, B не коллинеарны. Тогда*

1) *если $A - B \notin \Phi_P$, то*
$$\mathrm{Im}\ N_{AB11} = V_{A+B}.$$

2) *если $A - B \in \Phi_P$ и $\Phi \neq G_2$, то*
$$\mathrm{Im}\ N_{AB11} + \mathrm{Im}\ N_{A-B,2B,1,1} + \sum_{v \in V_B} \mathrm{Im}\,(N_{A-B,B,1,2}(-, v)) = V_{A+B},$$

где если $2B \notin \Phi_P$, считаем $\mathrm{Im}\ N_{A-B,2B,1,1} = 0$.

Proof. 1) По Лемме 4 условие означает, что любой корень $\gamma \in \pi^{-1}(A+B)$ имеет представление $\gamma = \alpha + \beta$, $\alpha \in \pi^{-1}(A)$, $\beta \in \pi^{-1}(B)$, где $\alpha - \beta$ — не корень. Тогда коммутатор $[X_A(e_\alpha), X_B(e_\beta)]$, взятый по модулю U_Ψ, где $\Psi = (A, B) \setminus \{A+B\}$, на каждом элементе покрытия S_τ имеет вид $x_{\alpha+\beta}(\pm 1)$, откуда $\mathrm{Im}\,(N_{AB11})_\tau = V_{A+B} \otimes S_\tau$; поскольку $\mathrm{Im}\ N_{AB11}$ является подмодулем V_{A+B}, определенным над базовым кольцом, имеем $\mathrm{Im}\ N_{AB11} = V_{A+B}$.

2) Действуя, как в пункте 1), мы можем получить, что на каждом элементе покрытия S_τ модуль $\mathrm{Im}\,(N_{AB11})_\tau$ содержит $\pm e_\gamma$, где γ — короткий корень из $\pi^{-1}(A+B)$. Если же γ — длинный корень из $\pi^{-1}(A+B)$, из наших предположений и Леммы 4 следует существование $\alpha \in \pi^{-1}(A-B)$, $\beta \in \pi^{-1}(B)$ таких, что $\gamma = \alpha + 2\beta$. Пользуясь пунктом 3 Теоремы 2, получаем, что коммутатор $[X_{A-B}(e_\alpha), X_B(e_\beta)]$ по модулю U_Ψ, где $\Psi = (A-B, B) \setminus \{A+B\}$, на каждом элементе покрытия S_τ имеет вид
$$x_{\alpha+2\beta}(\pm 1) \cdot \prod_{\beta' \in 2B} [x_\alpha(1), x_{\beta'}(u_{\beta'})], \qquad u_{\beta'} \in S_\tau.$$

Следовательно, $e_\gamma \in \mathrm{Im}\,(N_{A-B,B,1,2})_\tau(-, e_\beta) + \mathrm{Im}\,(N_{A-B,2B,1,1})_\tau$. Далее, существует представление e_β в виде
$$e_\beta = a_1 f_1 + \ldots + a_m f_m, \quad a_i \in S_\tau, \quad f_i \in V_B.$$

Легко видеть, что для любого $\delta \in \pi^{-1}(A-B)$
$$\begin{aligned}
[X_{A-B}(e_\delta), X_B(e_\beta)] &= [X_{A-B}(e_\delta), \prod_i X_B(a_i f_i) \cdot X_{2B}(w)] = \\
&= [X_{A-B}(e_\delta), \prod_i X_B(a_i f_i)] \cdot [X_{A-B}(e_\delta), X_{2B}(w)] = \\
&= \prod_i [X_{A-B}(e_\delta), X_B(a_i f_i)] \prod_{i<j} [X_B(a_i f_i), [X_{A-B}(e_\delta), X_B(a_j f_j)]] \cdot \\
&\qquad \cdot [X_{A-B}(e_\delta), X_{2B}(w)] \mod U_\Psi
\end{aligned}$$

для некоторого $w \in (V_{2B})_\tau$ (Теорема 2, пункт 3). Раскрывая коммутаторы далее, получаем, что $(N_{A-B,B,1,2})_\tau(e_\delta, e_\beta)$ содержится в
$$\begin{aligned}
&\sum_i (N_{A-B,B,1,2})_\tau(e_\delta, a_i f_i) + \mathrm{Im}\,(N_{AB11})_\tau + \mathrm{Im}\,(N_{A-B,2B,1,1})_\tau = \\
&\qquad \sum_i (N_{A-B,B,1,2})_\tau(a_i^2 e_\delta, f_i) + \mathrm{Im}\,(N_{AB11})_\tau + \mathrm{Im}\,(N_{A-B,2B,1,1})_\tau.
\end{aligned}$$

Суммируя все вышесказанное, видим, что e_γ принадлежит
$$\sum_i \mathrm{Im}\,(N_{A-B,B,1,2})_\tau(-, f_i) + \mathrm{Im}\,(N_{AB11})_\tau + \mathrm{Im}\,(N_{A-B,2B,1,1})_\tau,$$

что и завершает доказательство. □

Лемма 11. *Предположим, что относительный корень $A \in \Phi_P$ содержится в неприводимой компоненте ранга ≥ 2. Тогда для любого $v \in V_A$ существуют относительные корни $B_i, C_i \in \Phi_P$, не коллинеарные A, элементы $v_i \in V_{B_i}$, $u_i \in V_{C_i}$, и числа $k_i, l_i > 0$, $n_i \geq 0$ ($1 \leq i \leq m$), такие что для любых $\xi, \eta \in R$ выполнено*[3]

$$X_A(\xi\eta^2 v) = \prod_{i=1}^{m} X_{B_i}(\xi^{k_i}\eta^{n_i}v_i)^{X_{C_i}(\eta^{l_i}u_i)}.$$

Proof. Мы можем считать, что ξ, η являются свободными переменными, порождающими кольцо многочленов $R[\xi,\eta]$, и рассматривать $R[\xi,\eta]$-точки функторов X_A, $A \in \Phi_P$, вместо R-точек. Утверждение леммы тогда получается соответствующей специализацией ξ и η.

По Лемме 5 найдутся такие неколлинеарные относительные корни $B, C \in \Phi_P$, что $A = B + C$, причем если $\Phi = G_2$, то $B - C$ не является относительным корнем. Тогда по Леммам 9 и 10 (заметим, что коммутационные формулы остаются верными над расширением $R[\xi,\eta]$ кольца R) элемент $X_A(\xi\eta^2 v)$ содержится в группе, порожденной элементами

$$[X_B(\xi \cdot V_B), X_C(\eta^2 \cdot V_C)] \qquad \text{и} \qquad \prod_{\substack{i,j>0,\\(i,j)\neq(1,1)}} X_{iB+jC}(\xi^i\eta^{2j} \cdot V_{iB+jC}),$$

а также, если $B - C$ является относительным корнем, элементами

$$[X_{B-C}(\xi \cdot V_{B-C}), X_{2C}(\eta^2 \cdot V_{2C})], \qquad \prod_{\substack{i,j>0,\\(i,j)\neq(1,1)}} X_{i(B-C)+2jC}(\xi^i\eta^{2j} \cdot V_{i(B-C)+2jC}),$$

$$[X_{B-C}(\xi \cdot V_{B-C}), X_C(\eta \cdot V_C)], \qquad \prod_{\substack{i,j>0,\\(i,j)\neq(1,2)}} X_{i(B-C)+jC}(\xi^i\eta^{j} \cdot V_{i(B-C)+jC})$$

и, с учетом пункта 3 Теоремы 2,

$$\prod_{i>1} X_{iA}(\xi^i\eta^{2i} \cdot V_{iA}).$$

Поскольку B и C не коллинеарны, все возникающие относительные корни либо не коллинеарны A, либо имеют вид iA, $i > 1$. Следовательно, достаточно применить индукцию по убыванию $k = \operatorname{lev}(A)$. □

Пусть $P \leq P'$ — две параболические подгруппы в G. Заметим, что если $\mathrm{L}_{P'}$ — подгруппа Леви P', то P обладает подгруппой Леви L_P такой, что $\mathrm{L}_P \subseteq \mathrm{L}_{P'}$ (Exp. XXVI Prop. 1.20). Пусть τ — некоторое локальное оснащение, совместимое с P и L_P, и подгруппа P имеет тип $J = J_\tau \subseteq \Pi_\tau = \Pi$. Так как $P \subseteq P'$, локальное оснащение τ автоматически совместимо с P' и $\mathrm{L}_{P'}$ (ср. Exp. XXVI Prop. 1.4), и параболическая подгруппа P' имеет тип $J' \subseteq J$.

Лемма 12. *Пусть $P \leq P'$ — строго собственные параболические подгруппы в G. Тогда найдется такое число $k > 0$, зависящее только от ранга Φ_P, что для любого относительного корня $A \in \Phi_P$ и любого $v \in V_A$ существуют относительные корни*

[3] Мы используем экспоненциальную запись для обозначения сопряжения в группе, т.е. x^y означает $y^{-1}xy$.

$B_i, C_{ij} \in \Phi_{P'}$, элементы $v_i \in V_{B_i}$, $u_{ij} \in V_{C_{ij}}$, и числа $k_i, n_i, l_{ij} > 0$, такие что для любых $\xi, \eta \in R$ выполнено

$$X_A(\xi\eta^k v) = \prod_{i=1}^{m} X_{B_i}(\xi^{k_i}\eta^{n_i} v_i)^{\prod_{j=1}^{m_i} X_{C_{ij}}(\eta^{l_{ij}} u_{ij})}.$$

В частности, $\mathrm{E}_P(R) = \mathrm{E}_{P'}(R)$.

Proof. Пусть $\Theta \subseteq \Phi^+$ — множество положительных корней, соответствующее унипотентному радикалу $\mathrm{U}_{P'}$. Ясно, что унипотентному радикалу $\mathrm{U}_{(P')^-}$ соответствует множество корней $-\Theta$. Тогда в обозначениях предыдущего параграфа $\mathrm{U}_{P'} = \mathrm{U}_\Psi$, $\mathrm{U}_{(P')^-} = U_{-\Psi}$, где $\Psi = \pi(\Theta) \subseteq \Phi_P^+$ — соответствующее множество относительных корней.

Зафиксируем на множестве положительных корней Φ^+ некоторый порядок, индуцирующий на $\Phi_{P'}^+$ порядок, согласованный с уровнем. Не умаляя общности, можно считать, что $A \in \Phi_P^+$.

Если $A \in \Psi$, то по Лемме 6 определены некоторые отображения схем

$$\lambda_B = p_{\Phi_{P'}^+, B} \circ X_A : \mathrm{W}(V_A) \to \mathrm{W}(V_B), \qquad B \in \Phi_{P'}^+,$$

такие что $X_A(u) = \prod_{B \in \Phi_{P'}^+} X_B(\lambda_B(u))$ для любого $u \in V_A$, где произведение берется в выбранном порядке. Из коммутационных формул Шевалле при помощи спуска следует, что λ_B, $B \in \Phi_{P'}^+$, — однородные полиномиальные отображения. Следовательно, для всех $A \in \Psi$ (и, аналогично, для всех $A \in (-\Psi)$) утверждение леммы выполнено с $u_{ij} = 0$, $1 \le i, j \le m$.

Рассмотрим случай, когда $A \notin \Psi$. Множества простых корней J и J' инвариантны относительно группы автоморфизмов диаграммы Дынкина $\Gamma_\tau = \Gamma$, то есть представляют собой объединения некоторых Γ-орбит простых корней. Предположим сначала, что разность $J \setminus J'$ состоит из единственной Γ-орбиты, содержащей простой корень $\alpha_r \in \Pi$. Тогда $\Psi = \Phi_P^+ \setminus \mathbb{N}\pi(\alpha_r)$, следовательно, можно считать, что $A \in \Phi_P^+$ имеет вид $A = n\pi(\alpha_r)$, $n \in \mathbb{Z}$. Так как P' — строго собственная параболическая подгруппа, то ранг неприводимой компоненты Φ_P, содержащей A, не меньше 2. Тогда наше утверждение при $k \ge 3$ прямо следует из Леммы 11 (с заменой ξ на $\xi\eta$) и предыдущего случая, так как любой корень $B \in \Phi_P$, не коллинеарный A, автоматически содержится в $\Psi \cup (-\Psi) = \Phi_P \setminus \mathbb{Z}\pi(\alpha_r)$.

Теперь если $J \setminus J'$ состоит из более чем одной Γ-орбиты, то доказательство легко завершается по индукции, учитывая, что для любого Γ-инвариантного множества $J'' \subseteq \Pi$ такого, что $J' \subseteq J'' \subseteq J$, существует строго собственная параболическая подгруппа P'' группы G, содержащая P и имеющая тип J'' (Exp. XXVI Lemme 3.8). ☐

6 Лемма Квиллена-Суслина и доказательство основной теоремы

Введем некоторые дополнительные обозначения. Для идеала I кольца R мы обозначим через $G(R, I)$ ядро гомоморфизма редукции $G(R) \to G(R/I)$, через $\mathrm{U}_\Psi(R, I)$ — пересечение $\mathrm{U}_\Psi(R) \cap G(R, I)$, через $\mathrm{E}_P(I)$ — подгруппу, порожденную $\mathrm{U}_P(R, I)$ и $\mathrm{U}_{P^-}(R, I)$, а через $\mathrm{E}_P(R, I)$ — нормальное замыкание $\mathrm{E}_P(I)$ в $\mathrm{E}_P(R)$. Кроме того, для максимального идеала M кольца R обозначим через F_M гомоморфизм локализации $G(R) \to G(R_M)$.

Лемма 13. *Имеет место равенство* $\mathrm{E}_P(R[X]) \simeq \mathrm{E}_P(R[X], XR[X]) \rtimes \mathrm{E}_P(R)$.

Proof. Группа $\mathrm{E}_P(R[X], XR[X])$ по определению нормальна в $\mathrm{E}_P(R[X])$ и пересекается с $\mathrm{E}_P(R)$ только по единице. Так что осталось доказать, что $\mathrm{U}_P(R)$ и $\mathrm{U}_P(R[X], XR[X])$

порождают $\mathrm{U}_P(R[X])$. Можно считать, что склеивающий группоид состоит из одного класса изоморфности. Тогда утверждение прямо следует из Леммы 7. $\square$

Следствие. $\mathrm{E}_P(R[X]) \cap G(R[X], XR[X]) = \mathrm{E}_P(R[X], XR[X])$.

Proof. Пусть $g(X)$ лежит в $\mathrm{E}_P(R[X]) \cap G(R[X], XR[X])$; представим его в виде $g_1(X)g_2$, где $g_1(X) \in \mathrm{E}_P(R[X], XR[X])$, $g_2 \in \mathrm{E}_P(R)$. Тогда $g_2 = g_1(0)g_2 = g(0) = 1$. $\square$

Лемма 14. *Пусть $g(Z)$, $h(Z) \in G(R[Z])$ таковы, что $F_M(g(Z)) = F_M(h(Z))$ и $g(0) = h(0)$. Тогда существует $s \in R \setminus M$ такой, что $g(sZ) = h(sZ)$.*

Proof. Действительно, для $\mathbb{A}^n$ аналогичное утверждение очевидно, а G является замкнутой подсхемой $\mathbb{A}^n$ для некоторого n. $\square$

Начиная с настоящего момента мы предполагаем, что выполнено условие Теоремы 1.

Лемма 15. *Для любого $g(Z) \in \mathrm{E}_P(R_M[Z], ZR_M[Z])$ существуют элементы $h(Z) \in \mathrm{E}_P(R[Z], ZR[Z])$ и $s \in R \setminus M$ такие, что $F_M(h(Z)) = g(sZ)$.*

Proof. Можно считать, что склеивающий группоид G (над R) состоит из одного класса изоморфности. В самом деле, если замкнутая точка $\operatorname{Spec} R$, соответствующая M, лежит в компоненте $U_\xi = \operatorname{Spec} R_\xi$, и мы нашли элемент $h'(Z) \in \mathrm{E}_P(R_\xi[Z], ZR_\xi[Z])$, отображающийся в $g(sZ)$, можно в качестве $h(Z)$ взять элемент, равный $h'(Z)$ над U_ξ и 1 над $\coprod\limits_{\eta \neq \xi} U_\eta$.

Доказательство Леммы 13 показывает, что $\mathrm{E}_P(R_M[Z])$ порождается $\mathrm{E}_P(ZR_M[Z])$ и $\mathrm{E}_P(R_M)$. Следовательно, достаточно рассмотреть элементы $g(Z)$ вида $g_1 g_2(Z) g_1^{-1}$, где $g_1 \in \mathrm{E}_P(R_M)$ и $g_2(Z) \in \mathrm{E}_P(ZR_M[Z])$. Положим $S = R \setminus M$. Нетрудно видеть, что для любого $s' \in S$ можно найти такой элемент $s \in S$, что $g_2(sZ)$ лежит в $F_M(\mathrm{E}_P(s'ZR[Z]))$. Остается доказать, что существует элемент $s' \in S$, удовлетворяющий

$$g_1 F_M(\mathrm{E}_P(s'ZR[Z])) g_1^{-1} \subseteq F_M(\mathrm{E}_P(R[Z], ZR[Z])).$$

В действительности мы будем доказывать, что для любого $s'' \in S$ существует $s' \in S$ такой, что

$$g_1 F_M(\mathrm{E}_P(s'ZR[Z]))^{F_M(\mathrm{E}_P(s'R[Z]))} g_1^{-1} \subseteq F_M(\mathrm{E}_P(s''ZR[Z]))^{F_M(\mathrm{E}_P(s''R[Z]))}. \qquad (3)$$

Тогда можно считать, что g_1 является произвольной образующей $\mathrm{E}_P(R_M)$.

Пусть $P_{\min}$ — минимальная параболическая подгруппа группы G_{R_M}, содержащаяся в P_{R_M}, $\Phi_{P_{\min}}$ — соответствующая система относительных корней. Из Леммы 12 следует, что группа $\mathrm{E}_P(R_M) = \mathrm{E}_{P_{R_M}}(R_M)$ совпадает с $\mathrm{E}_{P_{\min}}(R_M)$, поэтому возьмем $g_1 = X_A(v)$ для некоторых $A \in \Phi_{P_{\min}}$, $v \in V_A$. Из Леммы 12 также следует, что $X_A(tv) \in F_M(\mathrm{E}_P(R))$ для некоторого $t = t(g_1) \in S$.

По Лемме 7 группа $F_M(\mathrm{E}_P(s'R[Z]))$ соотв. $F_M(\mathrm{E}_P(s'ZR[Z]))$ порождается элементами h_0 вида $X_C(\xi s' F_M(e_{C,i}))$ соотв. $X_C(\xi s' Z F_M(e_{C,i}))$, где $C \in \Phi_P$, $\xi \in R[Z]$ и элементы $e_{C,i}$ образуют порождающую систему модуля $V_C \otimes R[Z]$ над $R[Z]$. Чтобы доказать формулу (3), достаточно доказать, что $g_1 h_0 g_1^{-1} \in F_M(\mathrm{E}_P(s''R[Z]))$ соотв. $g_1 h_0 g_1^{-1} \in F_M(\mathrm{E}_P(s''ZR[Z]))^{F_M(\mathrm{E}_P(s''R[Z]))}$ для всех образующих h_0 с $\xi = 1$, так как утверждение для произвольной образующей получается подстановкой $Z \mapsto \xi Z$.

Положив в Лемме 12 $\xi = 1$, $\eta = s'$ соотв. $\xi = Z$, $\eta = s'$, а также $s' = (s''')^k$ для некоторого $s''' \in S$, мы можем представить h_0 в виде (конечного) произведения элементов h вида $X_B(s'''u)$ соотв. $X_B(s'''Zu)^{\prod_i D_i(s'''w_i)}$, где $B \in \Phi_{P_{\min}}$, $u \in V_B \otimes R_M[Z]$, $D_i \in \Phi_{P_{\min}}$, $w_i \in V_{D_i} \otimes R_M[Z]$. Ясно, что достаточно рассматривать только элементы h вида $X_B(s'''u)$ соотв. $X_B(s'''Zu)$. Как и выше, по Лемме 12 $h \in F_M(\mathrm{E}_P(R[Z]))$ соотв. $F_M(\mathrm{E}_P(ZR[Z]))$, если s''' делится на некоторое $r = r(h) \in S$.

Далее, в случае, когда $mB \neq -kA$ для любых $m, k \geq 1$, Лемма 9, очевидно, влечет $g_1 h g_1^{-1} \in F_M(\mathrm{E}_P(s''R[Z]))$ соотв. $g_1 h g_1^{-1} \in F_M(\mathrm{E}_P(s''ZR[Z]))$, если s''' делится на s'' и достаточно большую степень t и r. Разберем случай, когда A и B коллинеарны.

По предположению Теоремы 1 ранг каждой неприводимой компоненты $\Phi_{P_{\min}}$ не менее 2. Тогда по Лемме 11 для любого $u \in V_B \otimes R_M[Z]$ существуют относительные корни $B_1, \ldots, B_m, C_1, \ldots, C_m \in \Phi_{P_{\min}}$, не коллинеарные B (а значит, и A), элементы $v_i \in V_{B_i} \otimes R_M[Z]$, $u_i \in V_{C_i} \otimes R_M[Z]$, и числа $k_i, l_i > 0$, $n_i \geq 0$ ($1 \leq i \leq m$), такие что

$$X_B(\xi\eta^2 u) = \prod_{i=1}^{m} X_{B_i}(\xi^{k_i}\eta^{n_i}v_i)^{X_{C_i}(\eta^{l_i}u_i)}$$

для любых $\xi, \eta \in R_M[Z]$. Положим $\xi = s_1$ соотв. Zs_1, $\eta = s_2$, где оба элемента $s_1, s_2 \in S$ делятся на достаточно большие степени t и s'', а также на такое число $p \in S$, что $pu_i, pv_i \in R[Z]$ для любого $1 \leq i \leq m$. Тогда если $s''' \in S$ делится на $s_1 s_2^2$, по Леммам 9 и 12 мы как раз получим $g_1 h g_1^{-1} \in F_M(\mathrm{E}_P(s''R[Z]))^{F_M(\mathrm{E}_P(s''R[Z]))} = F_M(\mathrm{E}_P(s''R[Z]))$ соотв. $g_1 h g_1^{-1} \in F_M(\mathrm{E}_P(s''ZR[Z]))^{F_M(\mathrm{E}_P(s''R[Z]))}$.

□

Лемма 16. *Для любого $g(X) \in G(R[X])$ такого, что $F_M(g(X))$ лежит в $\mathrm{E}_P(R_M[X])$, существует $s \in R \setminus M$ такой, что $g(aX)g(bX)^{-1} \in \mathrm{E}_P(R[X])$ для всех $a, b \in R$ таких, что $a \equiv b \mod s$.*

Proof. Рассмотрим элемент $f(Z) = g(X(Y+Z))g(XY)^{-1} \in G(R[X,Y,Z])$. Заметим, что $F_M(f(Z)) \in \mathrm{E}_P(R_M[X,Y,Z])$ и $f(0) = 1$. По Следствию из Леммы 13 $F_M(f(Z))$ лежит в $\mathrm{E}_P(R_M[X,Y,Z], ZR_M[X,Y,Z])$. Теперь по Лемме 15 существуют элемент $h(Z)$ из $\mathrm{E}_P(R[X,Y,Z], ZR[X,Y,Z])$ и $s_1 \notin M$ такие, что $F_M(h(Z)) = F_M(f(s_1 Z))$. По Лемме 14 существует $s_2 \notin M$ такой, что $h(s_2 Z) = f(s_1 s_2 Z)$. Положим $s = s_1 s_2$; тогда $g(X(Y+sZ))g(XY)^{-1}$ лежит в $\mathrm{E}_P(R[X,Y,Z])$, откуда специализацией переменных Y и Z и получается нужное утверждение. □

Лемма 17. *Пусть $g(X) \in G(R[X])$ обладает тем свойством, что $g(0) \in \mathrm{E}_P(R)$ и $F_M(g(X)) \in \mathrm{E}_P(R_M[X])$ для всех максимальных идеалов M. Тогда $g(X) \in \mathrm{E}_P(R[X])$.*

Proof. Для любого максимального идеала M выберем $s_M \notin M$ как в Лемме 16. Поскольку идеал, порожденный всеми s_M, не содержится ни в каком максимальном идеале, найдется разбиение единицы $1 = \sum_{i=1}^{N} s_{M_i} t_i$. Применим трюк Абеля: обозначим через a_j частичную сумму $\sum_{i=1}^{N-j} s_{M_i} t_i$. Тогда $a_{j+1} \equiv a_j \mod s_{M_{N-j}}$, и мы имеем разложение

$$g(X) = \Big(\prod_{j=0}^{N-1} g(a_j X) g(a_{j+1}X)^{-1}\Big) g(0),$$

где все сомножители лежат в $\mathrm{E}_P(R[X])$ по выбору s_M. □

Доказательство Теоремы 1. Пусть Q — параболическая подгруппа G, отличная от P. Пусть $g \in \mathrm{E}_Q(R)$; надо доказать, что $g \in \mathrm{E}_P(R)$. Можно считать, что $g \in \mathrm{U}_Q(R)$. Найдем $g(X) \in \mathrm{U}_Q(R[X])$ как в Лемме 8. Пусть теперь M — какой-то максимальный идеал. Из SGA 3, Exp. XXVI, Cor. 5.2 и Cor. 5.7 следует, что P содержит над R_M некоторую минимальную параболическую $P_{\min}$, Q содержит минимальную параболическую $Q_{\min}$, причем они сопряжены некоторым элементом $h \in \mathrm{E}_{P_{\min}}(R_M)$. Теперь $F_M(g(X))$ лежит в $\mathrm{U}_Q(R_M[X])$ и a fortiori в $\mathrm{U}_{Q_{\min}}(R_M[X])$. Значит, $hF_M(g(X))h^{-1}$, а тем самым и $F_M(g(X))$, лежит в группе $\mathrm{E}_{P_{\min}}(R_M[X])$, которая по Лемме 12 совпадает с $\mathrm{E}_P(R_M[X])$. Поскольку $g(0) = 1$, можно применить Лемму 17 и получить, что $g(X)$ лежит в $\mathrm{E}_P(R[X])$. Теперь $g = g(1)$, так что g лежит в $\mathrm{E}_P(R)$, и теорема доказана. □

7 Примеры

1. Пусть D — алгебра Адзумайи над R степени d. Тогда группа $G = \mathrm{GL}_{r+1}(D)$ является редуктивной группой типа $A_{(r+1)d-1}$ (точнее, функтор $S \mapsto \mathrm{GL}_{r+1}(D \otimes S)$

представим редуктивной групповой схемой G). Подгруппа P, состоящая из верхнетреугольных матриц, является параболической подгруппой типа $\{d, 2d, \dots, (r+1)d\}$; относительные корни образуют систему корней A_r. Модуль V_A, соответствующий относительному корню A, можно отождествить с D. При этом отображение $N_{\varepsilon_i-\varepsilon_j,\varepsilon_j-\varepsilon_k,11}: D\times D\to D$ совпадает с умножением в D. Элементарная подгруппа $\mathrm{E}_P(R)$ совпадает с подгруппой $\mathrm{E}_{r+1}(D)$, порожденной элементарными матрицами.

2. Пусть V — проективный модуль ранга $2n$, снабженный неособой квадратичной формой Q. Тогда на группе $\mathrm{O}(V,Q)$, состоящей из всех автоморфизмов V, сохраняющих Q, определено отображение Диксона со значением в постоянной схеме $(\mathbb{Z}/2\mathbb{Z})_R$, которое в случае $2\in R^*$ оно совпадает с определителем при отождествлении $(\mathbb{Z}/2\mathbb{Z})_R$ с $(\mu_2)_R$ (см., например, [18]). Его ядро $\mathrm{O}^+(V,Q)$ является редуктивной группой типа D_n. Предположим, что V содержит набор из $r<n$ попарно ортогональных гиперболических пар (e_1,f_1),…,(e_r,f_r) (это значит, что $Q(e_i)=Q(f_i)=0$ и $Q(e_i+f_j)=\delta_{ij}$). Тогда подгруппа P, состоящая из преобразований, сохраняющих флаг

$$\langle e_1\rangle \le \langle e_1,\, e_2\rangle \ldots \le \langle e_1,\dots,e_r\rangle,$$

является параболической подгруппой типа $\{1,\dots,r\}$; относительные корни образуют систему корней типа B_r. Модуль V_A, соответствующий относительному корню A, можно отождествить с R, если A длинный, и с ортогональным дополнением к подмодулю $\langle e_1,\dots,e_r,\, f_1,\dots,f_r\rangle$, если A короткий. Если A, B и $A+B$ — относительные корни, то отображение N_{AB11} выглядит так:

- $(u,v)\mapsto \pm(Q(u+v)-Q(u)-Q(v))$, если A и B короткие;
- $(a,b)\mapsto \pm ab$, если A и B длинные;
- $(a,v)\mapsto \pm av$, если A длинный, а B короткий.

Наконец, если A длинный, а B короткий, и $A+2B$ является относительным корнем, то N_{AB12} переводит (a,v) в $\pm aQ(v)$. Элементарная подгруппа совпадает с подгруппой, порожденной трансвекциями Эйхлера–Зигеля–Диксона.

3. Пусть S — квадратичное этальное расширение R, т.е. скрученная форма алгебры $R\times R$. Тогда на S определена инволюция $x\mapsto\bar{x}$, получающаяся скручиванием инволюции $(a,b)\mapsto(b,a)$; множество ее неподвижных элементов совпадает с R. Отображение $\mathrm{tr}\colon S\to R$, $x\mapsto x+\bar{x}$, называется *отображением следа*.

Пусть V — проективный S-модуль ранга $n+1$, снабженный неособой эрмитовой формой H. Тогда группа $\mathrm{U}(V,H)$, состоящая из всех автоморфизмов V, сохраняющих H, является редуктивной группой (над R) типа ${}^2A_n$ (индекс 2 означает, что группы автоморфизмов объектов склеивающего группоида состоят из двух элементов). Предположим, что V содержит набор из $r\le\frac{n}{2}$ попарно ортогональных гиперболических пар (e_1,f_1), …, (e_r,f_r) (это значит, что $H(e_i,e_i)=H(f_i,f_i)=0$ и $H(e_i,f_j)=\delta_{ij}$). Тогда подгрупа P, состоящая из преобразований, сохраняющих флаг

$$\langle e_1\rangle \le \langle e_1,\, e_2\rangle \ldots \le \langle e_1,\dots,e_r\rangle,$$

является параболической подгруппой типа $\{1,\dots,r,\, n-r+1,\dots,n\}$; относительные корни образуют систему корней типа BC_r. Модуль V_A, соответствующий относительному корню A, можно отождествить с S, если A короткий, с ортогональным дополнением к $\langle e_1,\dots,e_r,\, f_1,\dots,f_r\rangle$, если A экстракороткий, и с ядром отображения следа, если A длиный. Если A, B и $A+B$ — относительные корни, то отображение N_{AB11} выглядит так:

- $(u,v)\mapsto \pm H(u,v)$, если A и B экстракороткие;
- $(a,b)\mapsto \pm ab$, если A, B и $A+B$ короткие;

- $(a, v) \mapsto \pm av$, если A короткий, а B экстракороткий;
- $(a, b) \mapsto \pm(ab - \bar{b}\bar{a})$, если A и B короткие, а $A + B$ длинный;
- $(a, b) \mapsto \pm ab$, если A длинный, а B короткий;
- $(u, v) \mapsto \pm(H(u, v) - H(v, u))$, если $A = B$ экстракороткий.

Если $A+2B$ является относительным корнем, то отображение N_{AB12} выглядит так:

- $(a, b) \mapsto \pm\bar{b}ab$, если A длинный, а B короткий;
- $(a, v) \mapsto \pm a\sigma(H(v, v))$, где σ — некоторое фиксированное сечение к отображению следа, если A короткий, а B экстракороткий.

4. Напомним, что алгебра называется *альтернативной*, если любые ее два элемента порождают ассоциативную подалгебру. *Алгеброй Кэли* над кольцом R называется альтернативная алгебра C с 1, снабженна инволюцией $x \mapsto \bar{x}$, причем требуется, чтобы C являлась проективным R-модулем постоянного ранга 8, а отображение *нормы* $n(x) = \bar{x}x = x\bar{x}$ принимало значения в R и являлось неособой квадратичной формой на C. На C тогда определено также отображение *следа* $t(x) = x + \bar{x}$ со значениями в R (действительно, $t(x) = n(x + 1) - n(x) - 1$).

По алгебре Кэли C и обратимым скалярам γ_1, γ_2 и γ_3 можно построить кубическую йорданову алгебру $J = \mathcal{H}_3(C, \gamma_1, \gamma_2, \gamma_3)$, состоящую из элементов вида

$$\begin{pmatrix} \xi_1 & c_3 & \gamma_1^{-1}\gamma_3\bar{c}_2 \\ \gamma_2^{-1}\gamma_1\bar{c}_3 & \xi_2 & c_1 \\ c_2 & \gamma_3^{-1}\gamma_2\bar{c}_1 & \xi_3 \end{pmatrix} \tag{4}$$

где c_1, c_2, c_3 — элементы C, а ξ_1, ξ_2, ξ_3 — скаляры. В частности, на J определена *норма* — кубическое отображение $N\colon J \to R$; норма матрицы (4) записывается как

$$\xi_1\xi_2\xi_3 - \gamma_3^{-1}\gamma_2\xi_1 n(c_1) - \gamma_1^{-1}\gamma_3\xi_2 n(c_2) - \gamma_2^{-1}\gamma_1\xi_1 n(c_3) + t(c_1c_2c_3)$$

(последнее слагаемое не зависит от способа расстановки скобок). Подробности см., например, в [19] или [13].

Положим

$$e_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad e_2 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix} \quad \text{и} \quad e_3 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Заметим, что e_1, e_2, e_3 — попарно ортогональные идемпотенты в J, дающие в сумме 1. Через $c[ij]$, где $c \in C$ и $1 \le i \ne j \le 3$, будем обозначать матрицу вида (4) с элементом $\gamma_j c$ в позиции $(i,\, j)$ и нулями в позициях, отличных от $(i,\, j)$ и $(j,\, i)$.

Функтор

$$S \mapsto \{g \in \mathrm{GL}(J \otimes S) \mid N(gx) = N(x) \text{ для всех } x \in J \otimes S',\ S \subseteq S'\}$$

представим полупростой групповой схемой G типа E_6. Подгруппа P, состоящая из всех преобразований, сохраняющих флаг

$$\mathbf{0} \le \begin{pmatrix} * & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \le \begin{pmatrix} * & * & 0 \\ * & * & 0 \\ 0 & 0 & 0 \end{pmatrix} \le J,$$

является параболической подгруппой типа $\{\alpha_1, \alpha_6\}$ (ср. [15, Table 1]). Заметим, что первое нетривиальное пространство флага натянуто на идемпотент e_1, а второе совпадает со слагаемым $J_0(e_3)$ разложения Пирса, полученного по идемпотенту e_3 (т.е. с множеством элементов J, аннулируемых умножением на e_3).

Относительные корни образуют систему корней типа A_2, в обозначениях [14] $\Phi_P = \{\pm(\varepsilon_1-\varepsilon_2), \pm(\varepsilon_2-\varepsilon_3), \pm(\varepsilon_1-\varepsilon_3)\}$. Модуль V_A, соответствующий относительному корню A, можно отождествить с C. При этом элемент $X_{\varepsilon_i-\varepsilon_j}(c)$ является "алгебраической трансвекцией" $T_{\gamma_j^{-1}c[ij],e_j}$, а отображение $N_{\varepsilon_i-\varepsilon_j,\varepsilon_j-\varepsilon_k,11}: C\times C\to C$ совпадает с умножением в C (например, [13, (v)]). Элементарная подгруппа $\mathrm{E}_P(R)$ совпадает с подгруппой, порожденной всеми алгебраическими трансвекциями.

Литература

[1] А. Борель, Ж. Титс, *Редуктивные группы*, Сб. Математика, **11** (1967), 1, 43–111; 2, 3–31.

[2] В.И. Копейко, *Стабилизация симплектических групп над кольцом многочленов*, Мат. Сборник **106** (1978), 94–107.

[3] В.А. Петров, *Нечетные унитарные группы*, Зап. Научн. Сем. ПОМИ **305** (2003), 195–225.

[4] В.П. Платонов, А.С. Рапинчук, *Алгебраические группы и теория чисел*, Наука, Гл. ред. физ.-мат. лит., М., 1991.

[5] А.А. Суслин, *О структуре специальной линейной группы над кольцами многочленов*, Изв. АН СССР. Сер. мат. **41** (1977), 235–252.

[6] А.А. Суслин, В.И. Копейко, *Квадратичные модули и ортогональные группы над кольцами многочленов*, Зап. Научн. Сем. ЛОМИ **71** (1977), 216–250.

[7] E. Abe, *Chevalley groups over local rings*, Tôhoku Math. J. **21** (1969), 474–494.

[8] E. Abe, *Normal subgroups of Chevalley groups over commutative rings*, Algebraic K-theory and algebraic number theory (Honolulu, HI, 1987), Contemp. Math **83**, Amer. Math. Soc., Providence RI, 1989, 1–17.

[9] H. Azad, M. Barry, G. Seitz, *On the structure of parabolic subgroups*, Comm. in Algebra **18** (1990), 551–562.

[10] A. Bak, N. Vavilov, *Normality for elementary subgroup functors*, Math. Proc. Cambridge Phil. Soc. **118** (1995), 35–47.

[11] A. Bak, N. Vavilov, *Structure of hyperbolic unitary groups* I. *Elementary subgroups*, Algebra Colloquium **7** (2000), 159–196.

[12] H. Bass, *K-theory and stable algebra*, Publ. Math. I.H.É.S. **22** (1964), 5–60.

[13] R. Bix, *Octonion planes over local rings*, Trans. of Amer. Math. Soc. **261** (1980), 417–438.

[14] N. Bourbaki, *Groupes et algèbres de Lie. Chapitres 4–6*, Hermann, Paris, 1968.

[15] S. Garibaldi, M. Carr, *Geometries, the principle of duality, and algebraic groups*, Exp. Math. **24** (2006), 195–234.

[16] M. Demazure, A. Grothendieck, *Schémas en groupes*, Lecture Notes in Mathematics, Vol. 151–153, Springer-Verlag, Berlin-Heidelberg-New York, 1970.

[17] R. Hazrat, N. Vavilov, *K_1 of Chevalley groups are nilpotent*, J. Pure Appl. Algebra **179** (2003), 99–116.

[18] M.-A. Knus, *Quadratic and Hermitian forms over rings*, Springer-Verlag, Berlin, 1991.

[19] M.-A. Knus, A. Merkurjev, M. Rost, J.-P. Tignol. *The book of involutions*, Amer. Math. Soc., Providence, RI, 1998.

[20] Fu-An Li, *The structure of orthogonal groups over arbitrary commutative rings*, Chinese Ann. Math. Ser. B **10** (1989), 341–350.

[21] H. Matsumoto, *Subgroups of finite index in certain arithmetic groups*, Algebraic groups and discontinuous subgroups, Proc. Sympos. Pure Math. **9**, Amer. Math. Soc., Providence RI, 1966, 99–103.

[22] D. Quillen, *Projective modules over polynomial rings*, Invent. Math. **36** (1976), 167–171.

[23] A. Stepanov, N. Vavilov, *Decomposition of transvections: a theme with variations*, K-theory **19** (2000), 109–153.

[24] K. Suzuki, *Normality of the elementary subgroups of twisted Chevalley groups over commutative rings*, J. Algebra **175** (1995), 526–536.

[25] G. Taddei, *Normalité des groupes élémentaires dans les groupes de Chevalley sur un anneau*, Contemp. Math **55** (1986), 693–710.

[26] J. Tits, *Algebraic and abstract simple groups*, Ann. of Math. **80** (1964), 313–329.

[27] J. Tits, *Classification of algebraic semisimple groups*, Algebraic groups and discontinuous subgroups, Proc. Sympos. Pure Math. **9**, Amer. Math. Soc., Providence RI, 1966, 33–62.

[28] L.N. Vaserstein, *Normal subgroups of orthogonal groups over commutative rings*, Amer. J. Math. **110** (1988), 955–973.

[29] L.N. Vaserstein, *Normal subgroups of symplectic groups over rings*, K-Theory **2** (1989), 647–673.

[30] L.N. Vaserstein, Hong You, *Normal subgroups of classical groups over rings*, J. Pure Appl. Algebra **105** (1995), 93–106.

[31] N.A. Vavilov, *Structure of Chevalley groups over commutative rings*, Nonassociative algebras and related topics (Hiroshima, 1990), World Sci. Publ., River Edge, NJ, 1991, 219–335.