Автоморфизмы силовских p-подгрупп групп Шевалле над p-примарными кольцами вычетов целых чисел*

С. Г. КОЛЕСНИКОВ
Красноярский государственный университет
e-mail: sklsnkv@mail.ru

УДК 519.54

Ключевые слова: группа Шевалле, силовская p-подгруппа, автоморфизм.

Аннотация

Доказывается, что произвольный автоморфизм силовской p-подгруппы группы Шевалле над кольцом вычетов $\mathbb{Z}_{p^m}$ раскладывается в произведение внутреннего, графового, диагонального и гиперцентрального автоморфизмов.

Abstract

S. G. Kolesnikov, Automorphisms of Sylow p-subgroups of Chevalley groups over p-primary residue rings of integers, Fundamentalnaya i prikladnaya matematika, vol. 12 (2006), no. 8, pp. 121—158.

In this paper, we prove that any automorphism of a Sylow p-subgroup of the Chevalley group over the ring $\mathbb{Z}_{p^m}$ (where p is prime and $m \geqslant 1$) is a product of graph, inner, diagonal, and hypercentral automorphisms.

Введение

В «Коуровской тетради» В. М. Левчук поставил следующий вопрос:

> описать автоморфизмы силовской p-подгруппы группы Шевалле нормального типа над кольцом классов вычетов целых чисел по модулю p^m. Здесь p — простое число, $m \geqslant 2$ [7, вопрос 12.42].

Ранее вопрос был решён при ограничении $p > 3$ (см. [5]). Цель статьи — завершить решение вопроса, рассмотрев и исключительные случаи $p = 2, 3$.

Пусть $G\Phi(K)$ — группа Шевалле над ассоциативно-коммутативным кольцом K с единицей, ассоциированная с системой корней Φ. Пусть $J = (p)$ — идеал кольца $K = \mathbb{Z}_{p^m}$ и $\Phi(J)$ — конгруэнц-подгруппа уровня J группы $G\Phi(K)$, т. е.

*Работа выполнена при поддержке гранта Президента РФ (проект № МК-1133.2005.1) и гранта РФФИ (проект № 06-01-00824).

© 2006 *Центр новых информационных технологий МГУ,*
Издательский дом «Открытые системы»

ядро её гомоморфизма, индуцированного естественным кольцевым гомоморфизмом $K \to K/J$. Унипотентная подгруппа $U\Phi(K)$ порождается корневыми элементами $x_r(t)$ ($r \in \Phi^+$, $t \in K$). Согласно [10, теорема 2] силовской p-подгруппой группы $G\Phi(\mathbb{Z}_{p^m})$ является произведение $S\Phi(\mathbb{Z}_{p^m}) = U\Phi(\mathbb{Z}_{p^m}) \cdot \Phi(J)$.

Автоморфизм нильпотентной группы ступени n называют гиперцентральным, если для некоторого $k < n$, называемого высотой, он не является внутренним по модулю $(k-1)$-го гиперцентра, а по модулю k-го гиперцентра действует тождественно. Гиперцентральные автоморфизмы обобщают центральные, т. е. действующие тождественно по модулю центра. Известно [10], что когда все константы $c_{ij,rs}$ из коммутаторной формулы Шевалле обратимы, ступень нильпотентности группы $S\Phi(\mathbb{Z}_{p^m})$ равна $mh-1$, где h — число Кокстера системы корней Φ. Как правило, в других случаях ступень ниже, но всегда не меньше $(m-1)h-1$ [2—4].

Основная теорема. *Всякий автоморфизм группы $S\Phi(\mathbb{Z}_{p^m})$, $m > 1$, лиева ранга больше двух раскладывается в произведение графового, диагонального, внутреннего и гиперцентрального высоты не выше h автоморфизмов.*

Схема статьи и доказательства основной теоремы следующая. В разделе 1 выписаны порождающие элементы и определяющие соотношения групп $S\Phi(\mathbb{Z}_{p^m})$, там же выделены элементарные гиперцентральные автоморфизмы. Предложение 2 в разделе 2 устанавливает характеристичность конгруэнц-подгрупп $\Phi(J^i)$ в группе $S\Phi(\mathbb{Z}_{p^m})$. В [8, 9, 13] были описаны автоморфизмы унипотентных подгрупп $U\Phi(K)$, а следовательно, и группы $S\Phi(\mathbb{Z}_p) = U\Phi(\mathbb{Z}_p)$. Изоморфизм $S\Phi(\mathbb{Z}_{p^m})/\Phi(J^{m-1}) \simeq S\Phi(\mathbb{Z}_{p^{m-1}})$ позволяет проводить доказательство основной теоремы индукцией по показателю m и редуцировать его к исследованию гиперцентральных автоморфизмов. Разложимость последних в произведение элементарных автоморфизмов доказывается в разделах 3—6.

В случаях лиева ранга 1 и 2 также доказан аналог основной теоремы (с другой оценкой высоты). Однако в статье доказательство аналога опускается ввиду громоздкости; аналог предложения 2 и описание гиперцентральных автоморфизмов в этих случаях устанавливаются другими методами. Исключительность групп $S\Phi(\mathbb{Z}_{p^m})$ рангов 1 и 2 проявляется уже в более сложном строении их центральных рядов [3]. Отметим, что автоморфизмы групп $S\Phi(\mathbb{Z}_{p^m})$ ранга 1 полностью описаны в [5, 6], а для ранга 2 они описаны при $p > 3$ в [5].

Автор выражает благодарность В. М. Левчуку за полезные замечания по оформлению полученных результатов и статьи.

1. Порождающие элементы и элементарные автоморфизмы

Всюду далее в статье предполагаем, что ранг Φ больше двух. Используются стандартные (см., например, [12]) обозначения: $(\ ,\ )$ — скалярное произведение в пространстве представления системы корней Φ; $h_s = 2s/(s,s)$ — кокорень, соответствующий корню $s \in \Phi$. Полагаем $p(\Phi) = \max\{(r,r)/(s,s) \mid r,s \in \Phi\}$.

В группе $G\Phi(K)$, как обычно, выделяем корневые элементы $x_r(t)$ ($r \in \Phi$, $t \in K$) и диагональные элементы $h_r(u)$ ($u \in K^{\#}$). В [10] показано, что силовская p-подгруппа $S\Phi(\mathbb{Z}_{p^m})$ порождается диагональными элементами $h_s(v)$ ($s \in \Phi$, $v \in 1+J$) и корневыми элементами $x_r(t)$ с условием $r \in \Phi^+$, $t \in K$ или $r \in \Phi^-$, $t \in J$. Определяющими для неё служат следующие соотношения:

$$x_r(t)x_r(u) = x_r(t+u), \tag{1}$$

$$h_r(w)h_r(v) = h_r(wv), \tag{2}$$

$$[x_r(t), h_s(w)] = x_r(tw^{(h_s,r)} - t), \tag{3}$$

$$[x_s(u), x_r(t)] = \prod_{i,j>0,\ ir+js\in\Phi} x_{ir+js}(c_{ij,rs}(-t)^i u^j), \tag{4}$$

$$[x_r(t), x_{-r}(u)] = x_r(c^{-1}t^2u)h_r(c)x_{-r}(-c^{-1}tu^2), \quad c = 1-tu. \tag{5}$$

Напомним, что все числа $c_{ij,rs}$ из коммутаторной формулы Шевалле выражаются через структурные константы $N_{r,s}$ соответствующей алгебры Ли и вместе с ними являются делителями числа $p(\Phi)!$. Полагаем также

$$U\Phi^{\varepsilon}(J^i) = \langle x_r(t) \mid r \in \Phi^{\varepsilon},\ t \in J^i\rangle, \quad \varepsilon = \pm, \quad U\Phi^+(J^i) = U\Phi(J^i), \quad i = 0,1,\ldots.$$

Как и в [1, табл. I—VIII], зафиксируем представление системы корней Φ ранга n в евклидовом пространстве с ортонормированным базисом $e_1, e_2, \ldots$, фундаментальные корни $r_1, \ldots, r_n$ и корень r_0 максимальной высоты.

Предложение 1. *Если $p > p(\Phi)$, то*

$$U\Phi(\mathbb{Z}_{p^m}) = \langle x_{r_1}(1), \ldots, x_{r_n}(1)\rangle, \quad S\Phi(\mathbb{Z}_{p^m}) = \langle U\Phi(\mathbb{Z}_{p^m}), x_{-r_0}(p)\rangle.$$

В исключительных случаях $1 < p \leqslant p(\Phi)$ выполняются следующие равенства:

а) $UB_n(\mathbb{Z}_{2^m}) = \langle x_{r_1}(1), \ldots, x_{r_n}(1), x_{r_{n-1}+r_n}(1)\rangle$;

б) $UC_n(\mathbb{Z}_{2^m}) = \langle x_{r_1}(1), \ldots, x_{r_n}(1), x_{2r_{n-1}+r_n}(1)\rangle$;

в) $UF_4(\mathbb{Z}_{2^m}) = \langle x_{r_1}(1), \ldots, x_{r_4}(1), x_{r_2+r_3}(1), x_{r_2+2r_3+2r_4}(1)\rangle$;

г) $S\Phi(\mathbb{Z}_{2^m}) = \langle U\Phi(\mathbb{Z}_{2^m}), x_{-r_0}(2)\rangle$, *если $\Phi = B_n$ или $\Phi = F_4$*;

д) $SC_n(\mathbb{Z}_{2^m}) = \langle UC_n(\mathbb{Z}_{2^m}), x_{r_1-r_0}(2), x_{-r_0}(2)\rangle$.

Доказательство. Первое утверждение доказано в [5, лемма 1, следствие 1]. Далее используем известную факторизацию

$$S\Phi(\mathbb{Z}_{p^m}) = U\Phi(\mathbb{Z}_{p^m}) \cdot H(J) \cdot U\Phi^-(J), \quad H(J^i) = \langle h_r(1+u) \mid r \in \Pi(\Phi),\ u \in J^i\rangle. \tag{6}$$

Кроме того, $S\Phi(\mathbb{Z}_{p^m}) = \langle U\Phi(\mathbb{Z}_{p^m}), U\Phi^-(J)\rangle$, поскольку из (5) получаем

$$h_r(1+u) = x_r(u(1+u)^{-1})[x_r(1), x_{-r}(-u)]x_{-r}(u^2(1+u)^{-1}), \quad r \in \Pi(\Phi), \quad u \in J.$$

Докажем а) и б). Пусть $T = \langle x_{r_1}(1), \ldots, x_{r_n}(1), x_r(1)\rangle$, где $r = r_{n-1}+r_n$, если $\Phi = B_n$, и $r = 2r_{n-1}+r_n$, если $\Phi = C_n$. Очевидно, что $T \subseteq U\Phi(\mathbb{Z}_{2^m})$.

Установим обратное включение. Достаточно показать включение $x_s(1) \in T$ для всех $s \in \Phi^+$. Пусть $q = e_{n-1} + e_n$. Имеем

$$x_q(1) \in \langle [X_{r_{n-1}}(J^0), X_{r_n}(J^0)], X_r(J^0) \rangle.$$

Векторы $r_1, \ldots, r_{n-1}$ и q являются базой подсистемы корней типа D_n, образованной векторами $\pm(e_i \pm e_j)$, $1 \leqslant i < j \leqslant n$. Поэтому $x_{e_i \pm e_j}(1) \in T$. Элементы $x_{e_i}(1)$ (соответственно $x_{2e_i}(1)$, если $\Phi = C_n$), $1 \leqslant i < n-1$, содержатся в подгруппах

$$\langle [X_{e_i - e_n}(J^0), X_{r_n}(J^0)], X_{e_i + e_n}(J^0) \rangle,$$

которые по доказанному выше лежат в T. Таким образом, $T = U\Phi(\mathbb{Z}_{2^m})$.

Докажем равенство в). Пусть

$$T = \langle x_{r_1}(1), \ldots, x_{r_4}(1), x_{r_2+r_3}(1), x_{r_2+2r_3+2r_4}(1) \rangle.$$

Заметим, что корни $\pm(e_i \pm e_j)$, $1 \leqslant i < j \leqslant 4$, и $\pm e_k$, $k = 1, 2, 3, 4$, образуют в F_4 подсистему корней типа B_4, причём $B_4^+ \cap F_4^+ = B_4^+$. По условию элементы $x_{e_l - e_{l+1}}(1)$, $l = 1, 2, 3$, и $x_{e_l}(1)$, $l = 3, 4$, содержатся в T. Поэтому из а) следует, что $x_{e_i \pm e_j}(1) \in T$ и $x_{e_k}(1) \in T$. Далее, пусть $\{i, j, k\} = \{2, 3, 4\}$. Тогда если $r = (e_1 + e_i - e_j - e_k)/2$, то $x_r(1) \in \langle [x_{r_4}(1), x_{e_i}(1)] \rangle \in T$, а если $r = (e_1 + e_i + e_j - e_k)/2$, то $x_r(1) \in \langle [x_{r_4}(1), x_{e_i + e_j}(1)] \rangle \in T$.

Докажем равенства г) и д). Пусть сначала $\Phi = B_n$ или C_n. Обозначим через T подгруппу, порождённую $U\Phi(\mathbb{Z}_{2^m})$ и элементом $x_{-r_0}(2)$ (элементами $x_{-r_0}(2)$ и $x_{r_1 - r_0}(2)$, если $\Phi = C_n$). Покажем, что T содержит подгруппу $U\Phi^-(J)$. В используемом представлении вектор $e_1 + e_2$ является корнем максимальной высоты для Φ типа B_n и D_n и совпадает с $r_0 - r_1$, если $\Phi = C_n$. Поэтому из первого утверждения вытекает, что $x_{e_j - e_i}(2) \in T$ при $1 \leqslant i < j \leqslant n$. Далее, если $\Phi = C_n$, то $x_{-2e_1}(2) \in T$ по условию, а если $\Phi = B_n$, то $x_{-e_1}(2) \in \langle [x_{-r_0}(2), x_{e_2}(1)], x_{-r_1}(2) \rangle \subseteq T$. Отсюда следует, что подгруппы $T_i = \langle [x_{\delta e_1}(2), x_{e_1 - e_i}(1)], x_{-e_1 - e_i}(2) \rangle$, $1 < i \leqslant n$ (здесь $\delta = -1$, если $\Phi = B_n$, и $\delta = -2$, если $\Phi = C_n$), тоже лежат в T. Но $x_{\delta e_i}(2) \in T_i$ и, значит, $x_{\delta e_i}(2) \in T$.

Пусть теперь $\Phi = F_4$ и $T = \langle UF_4(\mathbb{Z}_{2^m}), x_{-r_0}(2) \rangle$. Корень $e_1 + e_2$ является максимальным как в F_4, так и в B_4. Поэтому из доказанного выше следует, что $x_{e_j - e_i}(2) \in T$ для $1 \leqslant i < j \leqslant 4$ и $x_{-e_k}(2) \in T$ при $k = 1, 2, 3, 4$. Далее, положим $q = (-e_1 - e_2 - e_3 - e_4)/2$. Имеем $x_q(2) \in \langle [x_{r_4}(1), x_{-e_1}(1)] \rangle \in T$. Пусть $\{i, j, k\} = \{2, 3, 4\}$. Тогда если $r = (-e_1 + e_i - e_j - e_k)/2$, то $x_r(2) \in \langle [x_q(2), x_{e_i}(1)] \rangle \in T$, а если $r = (-e_1 + e_i + e_j - e_k)/2$, то $x_r(2) \in \langle [x_q(2), x_{e_i + e_j}(1)] \rangle \in T$. Предложение доказано. $\square$

Выделим основные автоморфизмы группы $S\Phi(\mathbb{Z}_{p^m})$.

Графовые автоморфизмы

Обозначим через ρ линейное преобразование пространства, порождённого всеми корнями, индуцированное симметрией диаграммы Дынкина системы корней Φ. Известно [8, 9], что отображение Γ_Φ, действие которого на корневых элементах определяется равенством $\Gamma_\Phi(x_r(t)) = x_{\rho(r)}(\gamma_r t)$ ($r \in \Phi^+$, $\gamma_r = \pm 1$), продолжается до автоморфизма группы $U\Phi^+(\mathbb{Z}_{p^m})$, если Φ типа A_n, D_n или E_6. Этот автоморфизм называется графовым, его продолжение на группу $S\Phi(\mathbb{Z}_{p^m})$ получим, положив $\Gamma_\Phi(x_{-r}(t)) = x_{-r}(\gamma_r t)$.

Диагональные автоморфизмы

Пусть χ — гомоморфизм целочисленной решётки системы корней Φ в мультипликативную группу кольца $\mathbb{Z}_{p^m}$. Тогда отображение, действующее тождественно на диагональной подгруппе и переводящее элементы $x_r(t)$ в $x_r(\chi(r)t)$, является автоморфизмом. Его называем диагональным.

Центральные автоморфизмы

Лемма 1. *Элемент $x_{r_0}(p^{m-1})$ лежит в центре группы $S\Phi(\mathbb{Z}_{p^m})$. Кроме того, центр группы $S\Phi(\mathbb{Z}_{2^m})$ содержит следующие элементы:*

а) $h_{r_1}(1+2^{m-1})h_{r_3}(1+2^{m-1})\dots h_{r_{n-1}}(1+2^{m-1})$, *если Φ типа D_n или C_n и n чётно;*

б) $h_{r_1}(1+2^{m-1})h_{r_3}(1+2^{m-1})\dots h_{r_n}(1+2^{m-1})$, *если Φ типа A_n или C_n и n нечётно;*

в) $h_{r_n}(-1)$, $h_{r_n}(1+2^{m-1})$, $x_{r_1+\dots+r_n}(2^{m-1})$, *если $\Phi = B_n$;*

г) $x_{r_0-r_1}(2^{m-1})$, *если $\Phi = C_n$;*

д) $h_{r_{n-1}}(1+2^{m-1})h_{r_n}(1+2^{m-1})$, *если $\Phi = D_n$;*

е) $x_{r_1+2r_2+3r_3+2r_4}(2^{m-1})$, *если $\Phi = F_4$.*

Доказательство. Легко проверяется перестановочность перечисленных элементов с порождающими группы $S\Phi(\mathbb{Z}_{p^m})$ указанными в предложении 1. □

Напомним, что центральным называется автоморфизм, тождественный по модулю центра группы. Общий способ их построения указывает очевидная лемма.

Лемма 2. *Пусть a — любой из центральных элементов, указанных в предыдущей лемме, а x — любой из порождающих группы $S\Phi(\mathbb{Z}_{p^m})$, указанных в предложении 1, соответствующий простому корню или корню $(-r_0)$. Тогда отображение $x \to x \cdot a$ (остальные порождающие остаются на месте) продолжается до центрального автоморфизма группы $S\Phi(\mathbb{Z}_{p^m})$.*

Перечислим элементарные гиперцентральные автоморфизмы группы $S\Phi(\mathbb{Z}_{p^m})$.

Пусть $K = \mathbb{Z}_{p^m}$ и $\lambda \in (p^{m-1})$. В системе корней Φ выберем простой корень q и корень s, для которых $s + q = r_0$. Тогда отображение

$$x_q(t) \to x_q(t)x_s(\lambda t)x_{r_0}(\lambda'(t^2 - t)), \quad t \in K \tag{7}$$

(остальные корневые элементы остаются на месте), определяет автоморфизм группы $S\Phi(K)$, если λ' является корнем уравнения $2x = \lambda N_{s,q}$ в кольце K. Пусть $\Phi = C_n$. Тогда $q - s$ тоже корень, и отображение

$$x_q(t) \to x_q(t)x_{s-q}(\lambda t)x_s(\lambda'(t^2 - t))x_{r_0}(\lambda''(t^3 - t) + \lambda'''(t - t^2)), \quad t \in K, \tag{8}$$

определяет автоморфизм группы $SC_n(K)$ в том случае, если $x = \lambda'$, $y = \lambda''$, $z = \lambda'''$ — решение системы уравнений $2x = \lambda N_{s-q,q}$, $3y = xN_{s,q}$, $2z = xN_{s,q}$.

Пусть $p = 2$, λ и корни q, s те же, что и выше. Выбор корней q, s однозначен, за исключением случая $\Phi = A_n$. Пусть $\Phi \neq C_n$. Тогда существует простой корень r с условиями $q + r, s - r \in \Phi$ и длины корней q, r, $q + r$, $s - r$, s, $s + q$ совпадают. Отображение

$$x_q(t) \to x_q(t)x_{s-r}(\lambda t), \quad x_{q+r}(t) \to x_{q+r}(t)x_s(\lambda t)x_{s+q}(\lambda t), \quad t \in K, \tag{9}$$

определяет автоморфизм группы $S\Phi(K)$. В случаях $\Phi = B_n$, $n > 3$, и $\Phi = D_n$, $n > 4$, имеется в точности две возможности выбора корня r, скажем r и r'. (При $\Phi = D_4$ имеется три возможности выбора корня r, а в оставшихся случаях корень r определён однозначно.) При этом $f = s-r-r'$, $q+r+r', s-q-r-r' \in \Phi$ и отображение

$$\left.\begin{aligned} &x_{q+r+r'}(t) \to x_{q+r+r'}(t)x_{s-r}(\lambda t)x_{s-r'}(\lambda t)x_{s+q}(\lambda t), \quad t \in K, \\ &x_{q+a}(t) \to x_{q+a}(t)x_f(\lambda t)x_{f-a}(\lambda t)), \quad x_a(t) \to x_a(t)x_{f-q}(\lambda t), \quad a \in \{r, r'\}, \end{aligned}\right\} \tag{10}$$

определяет автоморфизм группы $S\Phi(K)$. Пусть $\Phi = C_n$. Тогда существуют и единственны простые корни r и r', для которых $s - q - 2r, s - q - 2r - r' \in \Phi$. Положим $f = s - q - r - r'$ и обозначим через λ' корень уравнения $2x = \lambda$ в кольце K. Каждое из отображений

$$x_r(t) \to x_r(t)x_{s-r}(\lambda t)x_s(\lambda'(t^2 - t)), \quad t \in K; \tag{11}$$

$$\left.\begin{aligned} &x_r(t) \to x_r(t)x_{s-r-r'}(\lambda t), \quad t \in K, \\ &x_{r+r'}(t) \to x_{r+r'}(t)x_{s-r'}(\lambda t))x_s(\lambda t); \end{aligned}\right\} \tag{12}$$

$$\left.\begin{aligned} &x_q(t) \to x_q(t)x_{s-q-2r}(\lambda t)x_{s-q-r}(\lambda t)x_{s-r}(\lambda'(t^2 - t)), \quad t \in K, \\ &x_{q+r}(t) \to x_{q+r}(t)x_{s-q-r}(\lambda t))x_{s-q}(\lambda t)x_{s-r}(\lambda t))x_s(\lambda t + \lambda'(t^2 - t))x_{r_0}(\lambda t); \end{aligned}\right\} \tag{13}$$

$$\left.\begin{aligned} &x_r(t) \to x_r(t)x_s(\lambda t), \quad t \in K, \\ &x_a(t) \to x_a(t)x_{f-r}(\lambda t), \quad x_{r+a}(t) \to x_{r+a}(t)x_f(\lambda t), \quad a \in \{r, r'\}, \\ &x_{q+r+r'}(t) \to x_{q+r+r'}(t)x_{f+q}(\lambda t)x_{f+r'}(\lambda t)x_{s-r}(\lambda t)x_s(\lambda t) \end{aligned}\right\} \tag{14}$$

определяет автоморфизм группы $SC_n(K)$. Пусть $\Phi = B_n$ или $\Phi = F_4$. Выберем в Φ простой корень q и корень s, для которых $s + q$ — (единственный) короткий корень максимальной высоты и $s + 2q \notin \Phi$. Тогда отображение

$$x_q(t) \to x_q(t)x_s(\lambda t)x_{s+q}(\lambda'(t^2 - t)), \quad t \in K, \tag{15}$$

определяет автоморфизм группы $S\Phi(K)$. Если $\Phi = B_n$, то существует простой корень r с условием $q+r, s-r \in \Phi$. Отображение

$$x_q(t) \to x_q(t)x_{s-r}(\lambda t), \quad x_{r+q}(t) \to x_{r+q}(t)x_s(\lambda t))x_{s+q}(\lambda t), \quad t \in K, \tag{16}$$

определяет автоморфизм группы $SB_n(K)$.

Пусть $p = 3$, $\lambda \in (3^{m-1})$ и f — единственный короткий простой корень системы $\Phi = B_3$. Отображение

$$\left.\begin{array}{l} x_q(t) \to x_q(t)x_{s-f}(bt), \quad x_{2f+q}(t) \to x_{2f+q}(t)x_{s-f}(-bt), \\ x_{q+f}(t) \to x_{q+f}(t)x_{q+r}(-bt)x_s(bt)), \quad x_f(t) \to x_f(t)x_r(bt) \end{array}\right\} \tag{17}$$

определяет автоморфизм группы $SB_3(K)$.

В определении последующих автоморфизмов используется представление системы корней из [1].

Пусть $K = \mathbb{Z}_{p^m}$ и $\lambda \in (p^{m-1})$. Отображение

$$x_{r_i}(1) \to x_{r_i}(1) \prod_{j \neq i} h_{r_j}(1 + j\lambda) \tag{18}$$

продолжается до автоморфизма группы $S\Phi(\mathbb{Z}_{p^m})$, если $\Phi = A_n$, либо $p = 3$ и $\Phi = B_n, C_n$, либо $p = 2$ и $\Phi = B_n$.

Пусть $K = \mathbb{Z}_{2^m}$ и $\lambda \in (2^{m-1})$. Обозначим через s короткий корень максимальной высоты системы корней Φ типа B_n или F_4. Кроме того, положим $s_i = r_i + \ldots + r_n$, если $\Phi = B_n$ и $1 < i < n$, и $s_i = r_i + \ldots + r_3$, если $\Phi = F_4$ и $i = 1, 2$. Тогда отображение

$$x_{s_i + jr_n}(t) \to x_{s_i + jr_n}(t)x_{s+s_i}(\lambda t), \quad t \in K, \quad j = 0, 1, \quad 1 < i < n, \tag{19}$$

определяет автоморфизм группы $SB_n(K)$, а отображение

$$x_{s_i + jr_3}(t) \to x_{s_i + jr_3}(t)x_{s+s_i}(\lambda t), \quad t \in K, \quad j = 0, 1, \quad i = 1, 2, \tag{20}$$

определяет автоморфизм группы $SF_4(K)$. Кроме того, автоморфизм группы $SF_4(K)$ определяет также отображение

$$\begin{gathered} x_{jr_1+r_2+2r_3+ir_4}(t) \to x_{jr_1+r_2+2r_3+ir_4}(t)x_{r_0-(1-j)r_1}(\lambda t), \\ t \in K, \quad j = 0, 1, \quad i = 1, 2. \end{gathered} \tag{21}$$

Пусть $\Phi = C_n$. Для i, $1 < i < n$, положим $s_i = 2r_i + \ldots + 2r_{n-1} + r_n$, $q_i = r_1 + \ldots + r_{i-1}$, $f_i = -(r_i + \ldots + r_n)$. Тогда отображение

$$x_{s_i + jf_i}(t) \to x_{s_i + jf_i}(t)x_{q_i + s_i}(\lambda t), \quad t \in K, \quad j = 0, 1, \quad 1 < i < n, \tag{22}$$

определяет автоморфизм группы $SC_n(K)$.

Выделим в Φ следующие корни:

A_n: $r_0 - r_1,\ r_0 - r_n,\ r_2 + \ldots + r_{n-1}$;

B_n: $r_0 - r_2,\ r_0 - r_1 - 2r_2 - r_3,\ r_1$ и если $n = 3$, то r_3;

C_n: $r_0 - r_1,\ r_0 - 2r_1$;

D_n: $r_0 - r_2,\ r_0 - r_1 - 2r_2 - r_3,\ r_1$ и если $n = 4$, то r_3;
E_8: $r_0 - r_8,\ 2r_1 + r_3 + 4r_4 + 3r_5 + 2r_6 + r_7$;
E_7: $r_0 - r_1,\ r_2 + r_3 + 2r_4 + 2r_5 + 2r_6 + r_7$;
E_6: $r_0 - r_2,\ r_1 + r_3 + r_4 + r_5 + r_6$;
F_4: $r_0 - r_1,\ r_2 + 2r_3 + 2r_4$.

Пусть s — любой из перечисленных выше корней и λ — произвольный элемент из идеала J^{m-2} кольца $\mathbb{Z}_{p^m}$. Отображение

$$\left.\begin{aligned} &x_{-r_0}(u) \to x_{-r_0}(u)x_s(\lambda u), \quad u \in J,\\ &x_{kr-r_0}(u) \to x_{kr-r_0}(u)x_{s+kr}(\lambda u c_{k1,rs}/c_{k1,r,-r_0}), \quad s + kr \in \Phi, \quad k > 0, \end{aligned}\right\} \tag{23}$$

определяет автоморфизм группы $S\Phi(\mathbb{Z}_{p^m})$ при любом p. Отметим, что отображение определено корректно, поскольку константа $c_{k1,r,-r_0}$ всегда равна ± 1 и, следовательно, отношение $c_{k1,rs}/c_{k1,r,-r_0}$ является целым числом.

Пусть $\Phi = B_n$ или $\Phi = F_4$. Положим $s = r_0 - r_2 - \ldots - r_n$, если $\Phi = B_n$, и $s = r_0 - r_1 - r_2 - r_3$, если $\Phi = F_4$. Тогда для любого λ из идеала J^{m-1} кольца $K = \mathbb{Z}_{2^m}$ отображение

$$x_r(t) \to x_r(t)x_{s+r}(\lambda t), \quad t \in K, \tag{24}$$

где r пробегает множество корней $r_j + \ldots + r_n$, $j = 2, \ldots, n$, если $\Phi = B_n$, и r_3, $r_2 + r_3$, $r_1 + r_2 + r_3$, если $\Phi = F_4$, определяет автоморфизм группы $S\Phi(K)$.

Пусть, как и выше, $K = \mathbb{Z}_{2^m}$, но $\lambda \in J^{m-2}$. Положим $s = r_0 - 2r_1 - r_2$, если $\Phi = C_n$, и $s = r_2 + 2r_3 + r_4$, если $\Phi = F_4$. Отображение

$$x_{r-r_0}(u) \to x_{r-r_0}(u)x_{s+r}(\lambda u), \quad u \in J, \tag{25}$$

где r пробегает множества 0, r_1, r_1+r_2 и 0, r_1, r_1+r_2, $r_1+r_2+r_3$, $r_1+r_2+r_3+r_4$, когда соответственно $\Phi = C_n$ и $\Phi = F_4$, определяет автоморфизм группы $S\Phi(K)$.

Пусть $K = \mathbb{Z}_{p^m}$ и $\theta \in J^{m-2}$. Отображение

$$\left.\begin{aligned} &x_{-r_0}(u) \to x_{-r_0}(u)\prod_{i=1}^{n} h_{r_i}(1 + (i-1)\theta u),\\ &x_q(u) \to x_q(u)x_{r_0+q}((q, ne_{n+1} + e_1)N_{-r_0,r_0+q}\theta u), \quad q, -q - r_0 \in \Phi^-,\\ &h_{r_i}(1-u) \to h_{r_i}(1-u)x_{r_0}(1 - (q, ne_{n+1} + e_1)\theta u) \end{aligned}\right\} \tag{26}$$

определяет автоморфизм группы $SA_n(\mathbb{Z}_{p^m})$.

Пусть $K = \mathbb{Z}_{2^m}$ и $\theta \in J^{m-2}$. Отображение

$$\left.\begin{aligned} &x_{-r_0}(u) \to x_{-r_0}(u)h_{r_2}(1+\theta u)h_{r_3}(1+\theta u),\\ &x_q(u) \to x_q(u)x_{r_0+q}(N_{r_0,q}\theta u), \quad q, -q - r_0 \in \Phi^-,\\ &h_{r_1}(1-u) \to h_{r_1}(1-u)x_{r_0}(\theta u) \end{aligned}\right\} \tag{27}$$

определяет автоморфизм группы $SE_7(\mathbb{Z}_{2^m})$.

Пусть $K = \mathbb{Z}_{3^m}$ и $\theta \in J^{m-2}$. Отображение

$$\left.\begin{aligned} &x_{-r_0}(u) \to x_{-r_0}(u)h_{r_2}(1-\theta u)h_{r_5}(1+\theta u)h_{r_6}(1-\theta u),\\ &x_q(u) \to x_q(u)x_{r_0+q}(N_{r_0+q,-r_0}\theta u), \quad q, -q-r_0 \in \Phi^-,\\ &h_{r_2}(1-u) \to h_{r_2}(1-u)x_{r_0}(\theta u) \end{aligned}\right\} \tag{28}$$

определяет автоморфизм группы $SE_6(\mathbb{Z}_{3^m})$.

Пусть $\Phi = C_n$, $K = \mathbb{Z}_{2^m}$, $\lambda \in J^{m-2}$. Пусть также $s = r_0 - 2r_1 - 2r_2 - r_3$. Тогда отображение

$$x_{r+r_1-r_0}(u) \to x_{r+r_1-r_0}(u)x_{s+r}(\lambda u), \quad u \in J, \tag{29}$$

где r пробегает множество 0, r_2, $r_1 + r_2$, $r_1 + r_2 + r_3$, $r_1 + 2r_2 + r_3$, определяет автоморфизм группы $SC_n(\mathbb{Z}_{2^m})$. Если $s = r_0 - r_1 - r_2$, то отображение

$$\left.\begin{aligned} &x_{r+r_1-r_0}(u) \to x_{r+r_1-r_0}(u)x_{s+r}(\lambda u), \quad u \in J,\\ &x_{2r+2r_1-r_0}(u) \to x_{2r+2r_1-r_0}(u)x_{s+2r}(\lambda u), \end{aligned}\right\} \tag{30}$$

где $r = 0, r_2$, тоже определяет автоморфизм группы $SC_n(\mathbb{Z}_{2^m})$.

2. Характеристичность конгруэнц-подгрупп

Установим характеристичность некоторых подгрупп группы $S\Phi(\mathbb{Z}_{p^m})$. Характеристическими подгруппами, очевидно, являются члены нижнего центрального ряда. Как показано в [10], при условии $p > p(\Phi)$ i-й централ группы $S\Phi(\mathbb{Z}_{p^m})$ имеет вид

$$\Gamma_i(S\Phi(K)) = \langle x_r(t), h_r(1+u) \mid r \in \Phi,\ t \in J^{f(r,i)},\ u \in J^{f(0,i)} \rangle,$$

где $f(r,k) = -[(ht(r) - k)/h]$.

Предложение 2. *Конгруэнц-подгруппы $\Phi(J^i)$ характеристичны в $S\Phi(\mathbb{Z}_{p^m})$.*

Доказательство. При $p > p(\Phi)$ предложение доказано в [5]. Рассмотрим оставшиеся случаи. Пусть $K = \mathbb{Z}_{2^m}$ и $J^l = (2^l)$, $l = 0, 1, \ldots$.

Лемма 3. *Множество $1 + J^l$ образует в кольце K циклическую подгруппу относительно умножения, если $l \geqslant 2$.*

Доказательство. Множество $1+J^l$, $l \geqslant 1$, очевидно, замкнуто относительно умножения, содержит единичный элемент и ввиду равенства

$$(1 + 2^l t)^{-1} = 1 + (-2^l t) + (-2^l t)^2 + \ldots + (-2^l t)^m$$

замкнуто относительно взятия обратного элемента. Значит, оно является группой.

Покажем, что группа $1 + J^2$ порождается элементом $1 + 2^2 = 5$. Пусть целое положительное число i удовлетворяет неравенству $i \leqslant m-2$. Используя формулу бинома, получаем

$$(1+2^2)^{2^i} = 1 + 2^{i+2} + \sum_{j=2}^{2^i-1} \mathrm{C}_{2^i}^j 2^{2j} + 2^{2\cdot 2^i}.$$

Пусть j удовлетворяет неравенствам $2 \leqslant j \leqslant 2^i - 1$, и пусть $j = 2^s z$, где НОД$(2, z) = 1$. Тогда биномиальный коэффициент $\mathrm{C}_{2^i}^j$ делится на 2^{i-s}. Действительно,

$$\mathrm{C}_{2^i}^j = \frac{2^i \cdot (2^i - 1) \cdot \ldots \cdot (2^i - j + 1)}{1 \cdot 2 \cdot \ldots \cdot j}$$

и для всякого множителя $2^k u$, НОД$(2, u) = 1$, входящего в знаменатель и не превосходящего $j-1$, в числителе есть множитель $2^i - 2^k u = 2^k(2^{i-k} - u)$, который делится на 2^k, а $2^i/j = 2^{i-s}/u$. Кроме того, из неравенства $j = 2^s z \geqslant 2$ следует, что $2j \geqslant s+3$. Поэтому $C_{2^i}^j 2^{2j} \in J^{i-s} J^{s+3} = J^{i+3}$. Наконец, $2^{2\cdot 2^i} \in J^{2\cdot 2^i} \subseteq J^{i+3}$, поскольку $i \geqslant 1$. Таким образом, $5^{2^i} \equiv 1 + 2^{i+2} \pmod{J^{i+3}}$ и, значит, порядок элемента 5 не меньше чем 2^{m-2}. С другой стороны, $|1 + J^2| = |J^2| = 2^{m-2}$. Значит, группа $1 + J^2$ порождается элементом 5.

Цикличность групп $1 + J^l$ при $l > 2$ вытекает из включений $1 + J^l \subseteq 1 + J^2$, они порождаются элементами $1 + 2^l$. Лемма доказана. □

Для произвольной группы G через G^p обозначаем подгруппу, порождённую p-ми степенями всех её элементов.

Лемма 4. $\Phi(J^l)^2 = \Phi(J^{l+1})$, *если* $l \geqslant 1$.

Доказательство. Пусть $g \in \Phi(J^l)$. Согласно [10, теорема 2] группа $\Phi(J^l)$ допускает следующую факторизацию:

$$\Phi(J^l) = U\Phi(J^l) \cdot H(J^l) \cdot U\Phi^-(J^l). \tag{31}$$

Поэтому элемент g разложим в произведение корневых $x_r(t_r)$ ($r \in \Phi$, $t_r \in J^l$) и диагональных $h_s(1 + u_s)$ ($s \in \Pi(\Phi)$, $u_s \in J^l$) элементов. Квадрат элемента g в силу [11, теорема 12.3.1] раскладывается в произведение квадратов элементов $x_r(t_r)$ и $h_s(1 + u_s)$, и коммутаторов от них. Так как $x_r(t_r)^2 = x_r(2t_r)$ и $h_s(1+u_s)^2 = h_s((1+u_s)^2)$, а $(1+u_s)^2 = 1+2u_s+u_s^2 \in J^{l+1}$, то элементы $x_r(t_r)^2$ и $h_s(1 + u_s)^2$ содержатся в $\Phi(J^{l+1})$. Кроме того, из соотношения

$$[\Phi(J^i), \Phi(J^j)] \subseteq \Phi(J^{i+j}), \tag{32}$$

установленного в [10], следует, что коммутаторы от элементов $x_r(t_r)$ и $h_s(1+u_s)$ содержатся в $\Phi(J^{2l}) \subseteq \Phi(J^{l+1})$, поскольку $l \geqslant 1$. Таким образом, $\Phi(J^l)^2 \subseteq$ $\subseteq \Phi(J^{l+1})$.

Докажем обратное включение. Элементы 2^{l+1} и $5^{2^{l-1}}$ порождают идеал J^{l+1} и группу $1 + J^{l+1}$ (см. лемму 3) соответственно. Поэтому группа $\Phi(J^{l+1})$ порождается множеством элементов $x_r(2^{l+1})$ ($r \in \Phi$) и $h_s(5^{2^{l-1}})$. Ввиду того, что $x_r(2^{l+1}) = x_r(2^l)^2 \in \Phi(J^l)^2$ и если $l \geqslant 2$, то $h_s(5^{2^{l-1}}) = h_s(5^{2^{l-2}})^2 \in \Phi(J^l)^2$, включение $\Phi(J^{l+1}) \subseteq \Phi(J^l)^2$ имеет место, когда $l \geqslant 2$. Включение $\Phi(J^2) \subseteq$ $\subseteq \Phi(J)^2$ также справедливо, поскольку

$$h_s(5) =$$
$$= x_s(2-4{\cdot}5^{-1})^2 x_{-s}(-2)^2 (x_{-s}(2)x_s(-2))^2 x_{-s}(-4{\cdot}5^{-1})^2 [x_s(-2),[x_s(-2),x_{-s}(2)]],$$

а из соотношения (32) следует, что последний коммутатор лежит в $\Phi(J^3)$ и по доказанному $\Phi(J^3) \subseteq \Phi(J^2)^2$. Лемма доказана. □

В силу леммы 4 для доказательства предложения 2 достаточно установить, что $\Phi(J)$ — характеристическая подгруппа в $S\Phi(K)$.

Установим это сначала для Φ типа B_n. Пусть $\Phi = B_n$ и $n \geqslant 3$. Произведение подгруппы $U\Phi(J^{m-1})$ на подгруппу

$$\langle h_r(1+2^{m-1}) \mid r \in \Pi(\Phi) \setminus \{r_{n-1}\}\rangle \cdot \langle x_{-r_n}(2^{m-1}) h_{r_{n-1}}(1+2^{m-1})\rangle$$

обозначим через T. Согласно [4, теорема 2] подгруппа T является членом нижнего центрального ряда группы $S\Phi(K)$ и, следовательно, характеристична в ней. Поскольку $T \subseteq \Phi(J^{m-1})$ и по формуле (32) $[\Phi(J^{m-1}),\Phi(J)] = \Phi(J^m) = 1$, $\Phi(J)$ содержится в централизаторе T. Для доказательства обратного включения нам потребуется лемма 5.

Лемма 5. *Для всякого $s \in \Phi^+$, отличного от r_n (и, если $n = 3$, от r_1 и r_0), хотя бы одно из чисел $|(h_{r_1}, s)|, \ldots, |(h_{r_{n-2}}, s)|$ равно единице.*

Доказательство. Векторы, ортогональные ко всем корням $r_1, \ldots, r_{n-2}$, лежат в подпространстве W, порождённом векторами $(1,\ldots,1,0)$ и $(0,\ldots,0,1)$. Нетрудно видеть, что пересечение $\Phi \cap W$ содержит единственный корень r_n, если $n > 3$, и состоит из двух корней r_0 и r_n, когда $n = 3$. По [1, предложение 8] число (h_r, s) принимает одно из значений 0, 1 или -1, если $|s| \leqslant |r|$ и $s \neq r$. Теперь для завершения доказательства остаётся заметить, что все корни $r_1, \ldots, r_{n-2}$ являются длинными и любые два соседние из них не ортогональны между собой. Лемма доказана. □

Пусть теперь $z \in C_G(T)$ и $g = h_r(1+2^{m-1}) \in T$. В силу разложения (6) $z = x_{s_1}(t_1)\ldots x_{s_k}(t_k)w$, где $s_i \in \Phi^+$, $t_i \in K$ и $w \in \Phi(J)$. Используя соотношения (4) и (32), находим

$$z^g = \prod_i x_{s_i}(t_i(1+2^{m-1})^{(h_r,s_i)}) \cdot w = \prod_i x_{s_i}(t_i + t_i 2^{m-1})(h_r,s_i)) \cdot w. \qquad (33)$$

Отсюда следует, что $z^g = z$ тогда и только тогда, когда $t_i 2^{m-1}(h_r, s_i) = 0$ для всех i. По лемме 5 для всякого корня s_i, отличного от r_n (и от r_1, r_0, если $n = 3$), среди корней $r_1, \ldots, r_{n-2}$ найдётся такой корень r_j, что $(h_{r_j}, s_i) = \pm 1$, а значит, $t_i \in J$. Следовательно, мы можем считать, что $z = x_{r_n}(t)w$, если $n > 3$, и $z = x_{r_0}(u)x_{r_1}(v)x_{r_3}(t)w$, когда $n = 3$. Но в T лежит элемент $q = x_{-r_n}(2^{m-1})h_{r_{n-1}}(1+2^{m-1})$, который тоже должен быть перестановочен с z.

Однако $z^q = zh_{r_n}(1-2^{m-1}t)$ при $n>3$ и

$$z^q = x_{r_0}(u-u2^{m-1})x_{r_1}(v-v2^{m-1})x_{r_3}(t)h_{r_3}(1-t2^{m-1})w,$$

если $n=3$. Отсюда следует, что $t,u,v\in J$, и поэтому во всех случаях $z\in\Phi(J)$.

Пусть $\Phi=C_n$ и $n\geqslant 3$. Обозначим через T $(mh-h-1)$-й член нижнего центрального ряда группы $S\Phi(\mathbb{Z}_{2^m})$. Согласно [4, теорема 2] T лежит в $\Phi(J^{m-1})$ и содержит подгруппу

$$\langle x_{r_i}(2^{m-1}), h_{r_i}(1+2^{m-1}) \mid 1\leqslant i\leqslant n-1\rangle.$$

Кроме того, $x_{-r_1}(2^{m-1})x_{2e_2}(2^{m-1})\in T$, если $m=2$, и $x_{-r_1}(2^{m-1})\in T$, когда $m>2$. Так как $T\in\Phi(J^{m-1})$, то $\Phi(J)\subseteq C_G(T)$.

Установим обратное включение. Следующая лемма доказывается так же, как и аналогичная ей лемма 5.

Лемма 6. *Для всякого короткого корня $s\in\Phi^+$ хотя бы одно из чисел $|(h_{r_1},s)|,\dots,|(h_{r_{n-1}},s)|$ равно единице.*

Пусть теперь $z\in C_G(T)$. Формула (33) и лемма 6 позволяют нам считать, что $z=x_{2e_1}(t_1)\dots x_{2e_n}(t_n)w$, где $t_i\in\mathbb{Z}_{2^m}$ и $w\in\Phi(J)$. Далее,

$$z^{x_{r_i}(2^{m-1})} =$$

$$= \Bigl(\prod_{j\geqslant i} x_{2e_j}(t_j)\Bigr)(x_{2e_{i+1}}(t_{i+1})x_{e_i+e_{i+1}}(2^{m-1}t_{i+1}N_{2e_{i+1},r_i}))\Bigl(\prod_{j\geqslant i+2} x_{2e_j}(t_j)\Bigr)w.$$

Так как $N_{2e_{i+1},r_i}=\pm1$, то $t_i\in J$ для $i=2,\dots,n$. Следовательно, можно считать, что $z=x_{2e_1}(t_1)w$. Однако при любом $m\geqslant 2$ имеем

$$z^{x_{-r_1}(2^{m-1})x_{2e_2}(2^{m-1})} =$$

$$= (zx_{e_1+e_2}(2^{m-1}t_1N_{2e_1,-r_1}))^{x_{2e_2}(2^{m-1})} = zx_{e_1+e_2}(2^{m-1}t_1N_{2e_1,-r_1})$$

и $N_{2e_1,-r_1}=\pm1$. Поэтому $t_1\in J$ и, значит, $z\in\Phi(J)$.

Случай $\Phi=F_4$ рассматривается аналогично. Предложение доказано. □

3. Автоморфизмы, тождественные по модулю $\Phi(J^{m-1})$, I

В данном разделе исследуется действие на элементах $x_{r_i}(1)$ автоморфизмов группы $S\Phi(\mathbb{Z}_{p^m})$, единичных по модулю подгруппы $\Phi(J^{m-1})$.

Пусть автоморфизм φ группы $S\Phi(\mathbb{Z}_{p^m})$ единичен по модулю $\Phi(J^{m-1})$ и для всех $r\in\Phi^+$

$$x_r^{\varphi}(1) = x_r(1)\cdot h_r\cdot \prod x_s(\lambda_s^r), \quad \text{где} \quad h\in H(J^{m-1}). \tag{A}$$

Покажем, что домножением φ на подходящие внутренние, диагональные, центральные и элементарные гиперцентральные автоморфизмы можно добиться равенства единице сомножителей $x_s(\lambda_s^{r_i})$ для всех $r_i\in\Pi(\Phi)$ и $s\in\Phi$.

Зафиксируем простой корень q и корень s.

Случай $s - q \notin \Phi_0$. Предположим сначала, что $s \in \Phi^-$. Рассмотрим коммутатор $[x_q^\varphi(1), x_{-s}^\varphi(1)]$. Он должен равняться единице, поскольку $q - s \notin \Phi_0$, однако

$$[x_q^\varphi(1), x_{-s}^\varphi(1)] = h_q(1 - \lambda_{-q}^{-s}) h_s(1 - \lambda_s^q) \cdot \prod x_r(\mu_r).$$

Отсюда следует, что $h_q(1 - \lambda_{-q}^{-s}) h_s(1 - \lambda_s^q) = 1$. Пусть $h_s = k_1 h_{r_1} + \ldots + k_n h_{r_n}$, тогда

$$h_s(1 - \lambda_s^q) = h_{r_1}(1 - k_1 \lambda_s^q) \ldots h_{r_n}(1 - k_n \lambda_s^q),$$

и поэтому $k_i \lambda_s^q = 0$, если $r_i \neq q$. Обращаясь к [1, табл. I—VIII], видим, что среди коэффициентов $k_1, \ldots, k_n$ всегда найдётся такой отличный от нуля и взаимно простой с p коэффициент k_j, что $r_j \neq q$. Значит, $\lambda_s^q = 0$.

Далее нам потребуется несколько вспомогательных утверждений.

Лемма 7. *Пусть $q \in \Pi(\Phi)$, $s \in \Phi$ и $s - q \notin \Phi_0$. Если существует такой положительный корень r, отличный от q, что $s + r \in \Phi$, но $s - r$, $s + r - q$, $r + q \notin \Phi$, то $\lambda_s^q = 0$.*

Доказательство. Из условий $r + q \notin \Phi$, $s + r \in \Phi$ и $s + r - q \notin \Phi$ следует, что

$$1 = [x_q^\varphi(1), x_r^\varphi(1)] = x_{r+s}(N_{s,r} \lambda_s^q) \ldots$$

и, значит, $N_{s,r} \lambda_s^q = 0$. Далее, $s + r \in \Phi$, но $s - r \notin \Phi$, поэтому $N_{s,r} = \pm 1$ и, следовательно, $\lambda_s^q = 0$. Лемма доказана. □

Замечание 1. Если в лемме 7 опустить условие $s - r \notin \Phi$, то константа $N_{r,s}$ может равняться ± 2. В этом случае утверждать, что $\lambda_s^q = 0$, можно только при условии, что $p > 2$.

Лемма 8. *Если $s, r, q, s + r + q \in \Phi$, то*

$$N_{s,r} N_{s+r,q} + N_{r,q} N_{q+r,s} + N_{q,s} N_{q+s,r} = 0.$$

Кроме того, если $s + r$, $s + r + q \in \Phi$ и $s + q \notin \Phi$, то $r + q \in \Phi$.

Доказательство можно найти, например, в [13, с. 206].

Лемма 9. *Пусть $r, q \in \Pi(\Phi)$ и $s \in \Phi^+$. Предположим, что $s+r$, $r+q$, $s+r+q \in \in \Phi$, но $r + 2q$, $s - q \notin \Phi$. Тогда $\lambda_s^q = 0$, если $p > 2$.*

Доказательство. Покажем сначала, что $s + r - q \notin \Phi$. Предположим противное, пусть $s + r - q \in \Phi$. Так как $s + r, s + r - q \in \Phi$ и $s - q \notin \Phi$, то $r - q \in \Phi$ по лемме 8. Но r и q — простые корни, и поэтому $r - q \notin \Phi$, противоречие. Далее, поскольку $r + 2q$, $s + r - q \notin \Phi$ и $r + q$, $s + r$, $s + r + q \in \Phi$, имеем

$$1 = [x_q^\varphi(1), x_r^\varphi(1), x_r^\varphi(1)] = x_{r+s+q}((N_{s,r} N_{s+r,q} + N_{q,r} N_{q+r,s}) \lambda_s^q) \ldots.$$

В силу леммы 8 также имеем

$$\begin{aligned} N_{s,r} N_{s+r,q} + N_{q,r} N_{q+r,s} &= \\ = N_{s,r} N_{s+r,q} + N_{r,q} N_{q+r,s} + N_{q,s} N_{q+s,r} &+ 2 N_{q,r} N_{q+r,s} = 2 N_{q,r} N_{q+r,s}. \end{aligned}$$

Теперь остаётся заметить, что константы $N_{q,r}$ и $N_{q+r,s}$ равны ± 1 или ± 2, а $p > 2$. Лемма доказана. $\square$

Пару корней (q, s), где $q \in \Pi(\Phi)$, $s \in \Phi^+$ и $s - q \notin \Phi$, $s \neq r_0$, назовём *неособенной*, если она удовлетворяет условиям леммы 7, и *особенной* в противном случае. Из определения следует, что $\lambda_s^q = 0$, если пара (q, s) неособенная (далее будем говорить, что элемент λ_s^q соответствует паре (q, s)). Описание особенных пар содержит лемма 10.

Лемма 10. *Пусть Φ — система корней ранга больше двух. Следующие пары и только они являются особенными*:

A_n: $(r_1, r_0 - r_1)$, $(r_1, r_0 - r_1 - r_2)$, $(r_n, r_0 - r_n)$, $(r_n, r_0 - r_n - r_{n-1})$;

E_8: $(r_8, r_0 - r_8)$, $(r_8, r_0 - r_8 - r_7)$;

E_7: $(r_1, r_0 - r_1)$, $(r_1, r_0 - r_1 - r_3)$;

E_6: $(r_2, r_0 - r_2)$, $(r_2, r_0 - r_2 - r_4)$;

B_n: $(r_1, r_0 - r_1 - 2r_2 - r_3)$, $(r_1, r_2 + \ldots + r_n)$, $(r_1, r_3 + \ldots + r_n)$,
$(r_2, r_0 - r_2)$, $(r_2, r_0 - r_2 - r_3)$, $(r_2, r_0 - r_2 - r_1)$, $(r_2, r_1 + \ldots + r_n)$,
$(r_i, r_i + 2r_{i+1} + \ldots + 2r_n)$, $i = 3, \ldots, n-1$,
и если $n = 3$, *то* (r_3, r_1);

C_n: $(r_1, r_0 - 2r_1 - 2r_2 - r_3)$, $(r_1, r_0 - 2r_1 - 2r_2)$,
$(r_1, r_0 - 2r_1 - r_2)$, $(r_1, r_0 - 2r_2)$,
$(r_2, r_0 - r_1 - r_2 - r_3)$, $(r_2, r_0 - r_1 - r_2)$, $(r_i, r_0 - r_1)$, $i = 3, \ldots, n$,
и если $n = 3$, *то* (r_2, r_1);

D_n: $(r_1, r_0 - r_1 - 2r_2 - r_3)$, $(r_2, r_0 - r_2)$, $(r_2, r_0 - r_2 - r_3)$, $(r_2, r_0 - r_2 - r_1)$,
(r_n, r_{n-1}), $(r_i, r_i + 2r_{i+1} + \ldots + r_{n-1} + r_n)$, $i = 3, \ldots, n-1$,
и если $n = 4$, *то* (r_1, r_3), $(r_2, r_1 + r_2 + r_3)$, (r_3, r_1), (r_4, r_1);

F_4: $(r_1, r_0 - r_1)$, $(r_1, r_0 - r_1 - r_2)$, $(r_1, r_0 - r_1 - r_2 - r_3)$,
$(r_3, r_1 + r_2 + r_3 + r_4)$, $(r_3, r_0 - r_1 - r_2 - 2r_3 - r_4)$,
$(r_4, r_0 - r_1 - r_2 - r_3 - r_4)$.

Рассмотрим элементы λ_s^q, соответствующие особым парам (q, s). Домножив φ на подходящие автоморфизмы вида (7), (8), можем считать, что $\lambda_s^q = 0$ для пар вида $(r_i, r_0 - r_i)$, а также пары $(r_1, r_0 - 2r_1)$, если $\Phi = C_n$. Оставшиеся пары удовлетворяют или замечанию 1, или лемме 9. Поэтому соответствующие им элементы λ_s^q равны нулю при $p > 2$. Если $p = 2$, то, домножив φ на подходящие автоморфизмы вида (9), (16), можем считать, что $\lambda_s^q = 0$ для оставшихся пар, кроме следующих: $(r_i, r_i + 2r_{i+1} + \ldots)$, $i = 3, \ldots, n-1$, если $\Phi = B_n$ или D_n; (r_2, r_1), если $\Phi = C_n$; $(r_3, r_0 - r_1 - r_2 - 2r_3 - r_4)$, $(r_3, r_1 + r_2 + r_3 + r_4)$, если $\Phi = F_4$. Нетрудно показать, что соответствующие этим парам элементы λ_s^q в действительности равны нулю.

Случай $s=-q$. Выберем простой корень r так, чтобы $r+q\in\Phi$, но $r+2q\notin\Phi$. Это возможно, если $q\neq r_n$ или $\Phi\neq B_n$. Тогда

$$1=[x^{\varphi}_{r+q}(1),x^{\varphi}_{q}(1)]=x_r(\lambda^q_{-q}N_{r+q,-q})\dots.$$

Так как $N_{r+q,-q}=\pm1$, то $\lambda^q_{-q}=0$.

Пусть $\Phi=B_n$ и $q=r_n$. Положим $r=r_{n-1}$. Тогда

$$1=[x^{\varphi}_{r+q}(1),x^{\varphi}_{q}(1),x^{\varphi}_{q}(1)]=x_r(\lambda^q_{-q}(N_{r,q}N_{r+q,-q}+N_{r+q,q}N_{2r+q,-q}))\dots.$$

Используя соотношения (i) и (ii) из [12, теорема 4.1.2], находим, что

$$N_{r,q}N_{r+q,-q}+N_{r+q,q}N_{2r+q,-q}=2N^2_{r,q}+N^2_{q,r+q}/2=4.$$

Поэтому $\lambda^q_{-q}=0$, если $p>2$. Это равенство верно и при $p=2$, но доказывается немного сложнее.

Случай $s-q\in\Phi$. Положим $s'=s-q$. Предположим сначала, что q — единственный простой корень, который в сумме с s' лежит в Φ. Если $p>2$ или пара (q,s') отлична от пары (r_n,e_1) при $\Phi=B_n$, пары (r_1,e_1+e_2) при $\Phi=C_n$ и от пары (r_3,e_1) при $\Phi=F_4$, то константа $N_{q,s'}$ обратима в кольце $\mathbb{Z}_{p^m}$. Домножив φ слева на внутренний автоморфизм i_g, индуцированный элементом $x_{s'}(-N^{-1}_{q,s'}\lambda^q_s)$, получим $x^{i_g\varphi}_{r_i}(1)=x^{\varphi}_{r_i}(1)$ для всех $r_i\neq q$ и

$$x^{i_g\varphi}_{q}(1)=x^{\varphi}_{q}(1)x_s(-\lambda^q_s)\cdot\{x_{s'+2q}(c_{12,s',q}N^{-1}_{q,s'}\lambda^q_s)\}.$$

Таким образом, множитель $x_s(\lambda^q_s)$ в разложении (A) элемента $x^{i_g\varphi}(1)$ сокращается. Произведение в фигурных скобках равно единице, если $s'+2q\notin\Phi$, в противном случае существует ещё один простой корень, отличный от q, который в сумме с $s'+q$ лежит в Φ. Этот случай рассматривается ниже. Если $p=2$ и пара (q,s') совпадает с одной из пар, перечисленных выше, то равенства нулю элемента λ^q_s можно добиться, домножив φ на центральный автоморфизм и автоморфизм (17).

Пусть существует ещё один (больше быть не может) простой корень, например r, такой что $s'+r\in\Phi$. С точностью до перестановки r и q может осуществиться один и только один из следующих случаев:

1) $\langle r,s',q\rangle\simeq A_3$ и $r+q\notin\Phi$;
2) $\langle r,q\rangle\simeq A_2$ или B_2 и $s'=-r-q$;
3) $\langle s',r,q\rangle\simeq C_3$ и $s'-r,r+q\in\Phi$;
4) $\langle s',q,r\rangle\simeq B_3$ и $s'+2q,s+q+r\notin\Phi$.

В силу выбора r и q имеем $N_{q,s'}=\pm1$, а в случае 4) ещё и $N_{r,s'+q}=\pm1$. Домножим φ слева на внутренний автоморфизм i_g, индуцированный элементом $g=x_{s'}(-N^{-1}_{q,s'}\lambda^q_s)$ в случаях 1)—3), а в случае 4) — элементом

$$g=x_{s'}(-N^{-1}_{q,s'}\lambda^q_s)x_s(-N^{-1}_{r,s}\lambda^r_{r+s}).$$

В результате получим, что $x^{i_g\varphi}_{r_i}(1)=x^{\varphi}_{r_i}(1)$ для всех $r_i\neq q,r$ и

$$x^{i_g\varphi}_{q}(1)=x^{\varphi}_{q}(1)x_s(-\lambda^q_s)\cdot\{x_{s+q}(\bar\lambda^q_{s+q})\},$$
$$x^{i_g\varphi}_{r}(1)=x^{\varphi}_{r}(1)x_{s'+r}(\bar\lambda^r_{s'+r})\cdot\{x_{s+r}(-\lambda^r_{s+r})\},$$

где

$$\bar\lambda^q_{s+q} = -c_{12,s'q}N^{-1}_{q,s'}\lambda^q_s - N_{q,s}N^{-1}_{r,s}\lambda^r_{s+r}, \quad \bar\lambda^r_{s'+r} = -N_{q,s'}N^{-1}_{r,s}\lambda^r_{s+r},$$

и, кроме случая 4), выражения в фигурных скобках равны единице. Из полученных равенств видно, что после домножения φ на указанный автоморфизм i_g сомножители $x_s(\lambda^q_s)$ и $x_{s+r}(\lambda^r_{s+r})$ в разложениях элементов $x_q^{i_g\varphi}(1)$ и соответственно $x_r^{i_g\varphi}(1)$ сокращаются. Покажем, что элемент $\mu^r_{s'+r} = \lambda^r_{s'+r} + \bar\lambda^r_{s'+r}$, а в случае 4) ещё и элемент $\mu^q_{s+q} = \lambda^q_{s+q} + \bar\lambda^q_{s+q}$, равен нулю. Если выполняются условия 1) или 4), то $r+q \notin \Phi$ и требуемые равенства легко следуют из инвариантности соотношения $1 = [x_r(1), x_q(1)]$. Так, в случае 1) имеем

$$[x_r^{i_g\varphi}(1), x_q^{i_g\varphi}(1)] = x_{s+r}(N_{s'+r,q}\mu^r_{s'+r})\ldots$$

и $N_{s'+r,q} = \pm 1$, а в случае 4)

$$[x_r^{i_g\varphi}(1), x_q^{i_g\varphi}(1)] = x_{s+r}(N_{s'+r,q}\mu^r_{s'+r})x_{s+r+q}(N_{r,s+q}\mu^q_{s+q} + c_{21,q,s'+r}\mu^r_{s'+r})\ldots$$

и каждая из констант $N_{s'+r,q}$, $N_{r,s+q}$, $c_{21,q,s'+r}$ равна ± 1.

Пусть выполняется условие 3). Тогда существует простой корень r' с условием $q+r, q+r+r' \in \Phi$. Используя инвариантность соотношения $[x_q(1), x_r(1), x_{r'}(1), x_q(1)] = 1$, получаем требуемое.

Пусть выполняется 2). Тогда $s' = -r-q$, и нам нужно показать, что $\bar\lambda^r_{-q} = 0$. Так как

$$1 = [x_a^{i_g\varphi}(1), x_{r+q}^{i_g\varphi}(1)] = h_a(1 - \bar\lambda^{r+q}_{-a})h_{r+q}(1 + \lambda^a_{-r-q})\prod_{b\in\Phi} x_b(\mu_b),$$

где $a \in \{r, q\}$ и $h_{r+q} = h_r + h_q$, то $\lambda^r_{-r-q} = \lambda^q_{-r-q} = 0$. Отсюда следует, что

$$x_{r+q}^{i_g\varphi}(N_{r,q}) = [x_r^{i_g\varphi}(1), x_q^{i_g\varphi}(1)] = x_{r+q}(N_{r,q})h_q(1 + \bar\lambda^r_{-q})\prod_{b\in\Phi} x_b(\mu_b^{r+q}).$$

Выберем положительный корень a так, чтобы $|(h_q, a)| = 1$ и $r+q \pm a \notin \Phi$. Тогда из равенства

$$1 = [x_{r+q}^{i_g\varphi}(N_{r,q}), x_a^{i_g\varphi}(1)] = x_a((h_q, a)\bar\lambda^r_{-q})\ldots$$

следует, что $\bar\lambda^r_{-q} = 0$. Таким образом, доказано следующее предложение.

Предложение 3. *Пусть φ — тождественный по модулю подгруппы $\Phi(J^{m-1})$ автоморфизм группы $S\Phi(\mathbb{Z}_{p^m})$. Тогда с точностью до умножения φ на диагональный, внутренний, центральный и элементарные гиперцентральные автоморфизмы* (7)—(17) *можно считать, что $x_r^{\varphi}(1) = x_r(1)\cdot h$, где $h \in H(J^{m-1})$, для всех $r \in \Pi(\Phi)$.*

4. Автоморфизмы, тождественные по модулю $\Phi(J^{m-1})$, II

Пусть автоморфизм φ группы $S\Phi(\mathbb{Z}_{p^m})$ единичен по модулю подгруппы $\Phi(J^{m-1})$ и удовлетворяет условию

$$\text{для всех } r_i \in \Pi(\Phi) \quad x_{r_i}^{\varphi}(1) = x_{r_i}(1) \cdot h_{r_1}(1+\theta_1^i) \dots h_{r_n}(1+\theta_n^i). \tag{Б}$$

Найдём условия, которым должны удовлетворять элементы θ_j^i. Следующая лемма доказана в [5].

Лемма 11. *Пусть автоморфизм φ удовлетворяет условию* (Б). *Положим* $d_{r_i} = h_{r_1}(1+\theta_1^i) \dots h_{r_n}(1+\theta_n^i)$. *Тогда*

а) $[x_s, d_r] = 1$, *если* $r+s,\ r-s \notin \Phi_0$;

б) $[x_s, d_r, x_r][x_{r+s}(N_{sr}), d_r] = 1$, *если* $r, s \in \Pi(\Phi)$ *и* $r+s \in \Phi$, $2r+s,\ r+2s \notin \Phi$;

в) $[x_{r+2s}(c_{21sr}), d_r] = 1$, *если* $r, s \in \Pi(\Phi)$ *и* $r+s,\ r+2s \in \Phi$;

г) $[x_s, d_r, x_r, x_r][x_{r+s}(N_{sr}), d_r, x_r][x_{2r+s}(2c_{21,rs}), d_r] = 1$, *если* $r, s \in \Pi(\Phi)$ *и* $r+s,\ 2r+s \in \Phi$.

Домножив φ на внутренний и диагональный автоморфизмы, можем считать, что $\theta_i^i = 0$ для всех $i = 1, \dots, n$. Используя теперь соотношения из леммы 11, составим системы уравнений на θ_j^i и исследуем их.

Тип A_n, $n > 2$

Случай $i = 1$. Система состоит из уравнений

$$3\theta_2^1 - 2\theta_3^1 = 0, \quad 2\theta_n^1 - \theta_{n-1}^1 = 0$$

и, если $n > 3$, уравнений

$$2\theta_j^1 - \theta_{j-1}^1 - \theta_{j+1}^1 = 0, \quad j = 3, \dots, n-1. \tag{34}$$

Выразим из уравнения $2\theta_n^1 - \theta_{n-1}^1 = 0$ элемент θ_{n-1}^1, а затем последовательно найдём из уравнений (34) выражения $\theta_{n-2}^1, \dots, \theta_2^1$ через θ_n^1. В результате получим

$$\theta_j^1 = (n+1-j)\theta_n^1, \quad j = 2, \dots, n-1. \tag{35}$$

Так как

$$0 = 3\theta_2^1 - 2\theta_3^1 = 3(n+1-2)\theta_n^1 - 2(n+1-3)\theta_n^1 = (n+1)\theta_n^1,$$

то $\theta_n^1 = 0$, значит, система имеет тривиальное решение тогда и только тогда, когда НОД$(p, n+1) = 0$. Если НОД$(p, n+1) = p$, то элемент θ_n^1 может быть любым элементом из идеала J^{m-1}, а все остальные элементы выражаются через θ_n^1 по формулам (35), причём $\theta_j^1 = -j\theta_n^1$, поскольку $(n+1)\theta_n^1 = 0$.

Случай $i = 2$. Если $n = 3$, то система состоит из двух уравнений

$$3\theta_1^2 - \theta_3^2 = 0, \quad 3\theta_3^2 - \theta_1^2 = 0.$$

Её определитель равен 8, поэтому при $p > 2$ она имеет тривиальное решение. Если $p = 2$, то $\theta_3^2 = \theta_1^2$.

Пусть $n > 3$. Тогда система состоит из уравнений

$$3\theta_1^2 - \theta_3^2 = 3\theta_3^2 - 2\theta_4^2 - \theta_1^2 = 2\theta_n^2 - 2\theta_{n-1}^2 = 0$$

и, если $n > 4$, уравнений

$$2\theta_j^2 - \theta_{j-1}^2 - \theta_{j+1}^2 = 0, \quad j = 4, \ldots, n-1. \tag{36}$$

Выразим θ_{n-1}^2 из уравнения $2\theta_n^2 - \theta_{n-1}^2 = 0$, а затем последовательно из уравнений (36) найдём выражения $\theta_{n-2}^2, \ldots, \theta_3^2$ через θ_n^2. В результате получим

$$\theta_j^2 = (n+1-j)\theta_n^2, \quad j = 3, \ldots, n-1. \tag{37}$$

Тогда

$$\theta_1^2 = 3\theta_3^2 - 2\theta_4^2 = 3(n+1-3)\theta_n^2 - 2(n+1-4)\theta_n^2 = n\theta_n^2.$$

Подставляя выражения θ_1^2 и θ_3^2 в уравнение $3\theta_1^2 - \theta_3^2 = 0$, получим

$$0 = 3n\theta_n^2 - (n-2)\theta_n^2 = 2(n+1)\theta_n^2.$$

Таким образом, система имеет тривиальное решение тогда и только тогда, когда НОД$(p, 2n+2) = 0$. Если НОД$(p, 2n+2) = p$, то элемент θ_n^2 может быть любым элементом из идеала J^{m-1}, а все остальные элементы выражаются через θ_n^2 по формулам (37).

В силу известной симметрии диаграммы Дынкина типа A_n далее можно считать, что $n > 4$, и осталось рассмотреть случаи $2 < i < n-2$.

Случаи $2 < i < n-2$. Система состоит из уравнений

$$2\theta_1^i - \theta_2^i = 3\theta_{i-1}^i - 2\theta_{i-2}^i - \theta_{i+1}^i = 3\theta_{i+1}^i - 2\theta_{i+2}^i - \theta_{i-1}^i = 2\theta_n^i - \theta_{n-1}^i = 0$$

и, если $i > 3$ или $i < n-3$, уравнений

$$2\theta_j^i - \theta_{j-1}^i - \theta_{j+1}^i = 0, \quad j = 2, \ldots, i-2, i+2, \ldots, n-1. \tag{38}$$

Из уравнения $2\theta_1^i - \theta_2^i = 0$ выразим θ_2^i, а из уравнения $2\theta_n^i - \theta_{n-1}^i = 0$ выразим θ_{n-1}^i. Затем, используя равенства (38), выразим $\theta_3^i, \ldots, \theta_{i-1}^i$ через θ_1^i, если $i > 3$, а также выразим $\theta_{n-1}^i, \ldots, \theta_{i+1}^i$ через θ_n^i, если $i < n-3$. В результате получим

$$\theta_j^i = j\theta_1^i, \quad j = 2, \ldots, i-1, \tag{39}$$

и

$$\theta_j^i = (n+1-j)\theta_n^i, \quad j = i+1, \ldots, n-1. \tag{40}$$

Теперь подставим выражения θ_{i-2}^i, θ_{i-1}^i и θ_{i+1}^i, θ_{i+2}^i из (39), (40) в уравнения

$$3\theta_{i-1}^i - 2\theta_{i-2}^i - \theta_{i+1}^i = 3\theta_{i+1}^i - 2\theta_{i+2}^i - \theta_{i-1}^i = 0.$$

В результате получим следующую систему уравнений на θ_1^i и θ_n^i:

$$\begin{cases} (1-i)\theta_1^i + (n+2-i)\theta_n^i = 0, \\ (1+i)\theta_1^i + (i-n)\theta_n^i = 0. \end{cases} \tag{41}$$

Определитель системы (41) равен $-2n-2$, поэтому $\theta_1^i = \theta_n^i = 0$, а значит, $\theta_j^i = 0$ для всех $j = 2, \ldots, i-1, i+1, \ldots, n-1$ тогда и только тогда, когда НОД$(p, 2n+2) = 1$.

Исследуем случаи, когда НОД$(p, 2n+2) = p$. Пусть $p = 2$. Тогда если n нечётно, то

$$\theta_1^i = \theta_3^i = \ldots = \theta_n^i, \quad \theta_2^i = \theta_4^i = \ldots = \theta_{n-1}^i = 0.$$

Если же число n чётно, то

$$\theta_1^i = \theta_3^i = \ldots = \theta_{i-2}^i, \quad \theta_2^i = \theta_4^i = \ldots = \theta_{i-1}^i = \theta_{i+1}^i = \theta_{i+2}^i = \ldots = \theta_n^i = 0$$

при нечётном i, а при чётном i

$$\theta_{i+2}^i = \theta_{i+4}^i = \ldots = \theta_n^i, \quad \theta_1^i = \theta_2^i = \ldots = \theta_{i-1}^i = \theta_{i+1}^i = \theta_{i+3}^i = \ldots = \theta_{n-1}^i = 0.$$

Пусть $p > 2$. Тогда хотя бы одно из чисел $1-i$, $1+i$ не делится на p и поэтому система (41) эквивалентна одному уравнению $\theta_1^i + \theta_n^i = 0$. Отсюда и из формул (39), (40) следует, что решение исходной системы имеет вид

$$\theta_j^i = j\theta_1^i, \quad j = 2, \ldots, i-1, i+1, \ldots, n,$$

где θ_1^i может быть любым элементом из идеала J^{m-1}.

Тип B_n, $n > 2$

Случаи $i = 1, \ldots, n-2$. Пусть $n = 3$. Тогда $i = 1$ и система на θ_2^1 и θ_3^1 состоит из уравнений

$$3\theta_2^1 - 4\theta_3^1 = 0, \quad 2\theta_3^1 - \theta_2^1 = 0.$$

Решая её, находим, что $\theta_2^1 = 0$, и $\theta_3^1 = 0$, если $p > 2$.

Пусть, далее, $n > 3$. Тогда при фиксированном i система состоит из уравнения

$$2\theta_n^i - \theta_{n-1}^i = 0$$

и в зависимости от i из следующих уравнений:

$$2\theta_j^i - \theta_{j-1}^i - \theta_{j+1}^i = 0, \quad j = 2, \ldots, i-2, i+2, \ldots, n-1, \tag{42}$$

если $i > 3$ или $i < n-3$, уравнения

$$3\theta_{i+1}^i - 2\theta_{i+2}^i - \theta_{i-1}^i = 0, \tag{43}$$

если $1 < i < n-2$, уравнений

$$\text{а) } 3\theta_2^1 - 2\theta_3^1 = 0, \quad \text{б) } 3\theta_1^2 - \theta_3^2 = 0, \quad \text{в) } 3\theta_{n-1}^{n-2} - 4\theta_n^{n-2} - \theta_{n-3}^{n-2} = 0, \tag{44}$$

если $i = 1$, $i = 2$ и $i = n-2$ соответственно, а также уравнений

$$\text{а) } 3\theta_{i-1}^i - 2\theta_{i-2}^i - \theta_{i+1}^i = 0, \quad \text{б) } 2\theta_1^i - \theta_2^i = 0, \tag{45}$$

если $i > 2$, и, если $i < n-2$, уравнения

$$2\theta_{n-1}^i - 2\theta_n^i - \theta_{n-2}^i = 0. \tag{46}$$

Покажем, что

$$\theta_j^i = 2\theta_n^i, \quad j = i+1, \ldots, n-1. \tag{47}$$

Действительно, $\theta^i_{n-1} = 2\theta^i_n$. Отсюда при $i < n-2$ из (46) следует равенство $\theta^i_{n-2} = 2\theta^i_n$, а из уравнений (42), если $i < n-3$, последовательно находим, что $\theta^i_j = 2\theta^i_n$ для $j = i+1, \dots, n-3$.

Пусть $i = 1$. Подставляя выражения из (47) в (44) а), получим

$$0 = 3\theta^1_2 - 2\theta^1_3 = 6\theta^1_n - 4\theta^1_n = 2\theta^1_n.$$

Следовательно, $\theta^1_2 = \ldots = \theta^1_{n-1} = 0$, а $\theta^1_n = 0$, только если $p > 2$.

Пусть $i = 2$. Тогда из (43) при $i = 2$ следует, что $\theta^2_1 = \theta^2_n$. Отсюда и из (47), (44) б) получаем

$$0 = 3\theta^2_1 - \theta^2_3 = 6\theta^2_n - 2\theta^2_n = 4\theta^2_n.$$

Следовательно, $\theta^2_1 = \theta^2_3 = \ldots = \theta^2_{n-1} = 0$, а $\theta^2_n = 0$, только если $p > 2$.

Пусть теперь $i > 2$. Из уравнения (45) б) и уравнений (42) при $i > 4$ следует, что

$$\theta^i_j = j\theta^i_1, \quad j = 2, \ldots, i-1. \tag{48}$$

Подставим выражения из (47) и (48) в равенства (45) а) и (43) при $i \neq n-2$, а при $i = n-2$ в равенства (45) а) и (44) в). В обоих случаях получим следующую систему уравнений:

$$\begin{cases} (1-i)\theta^i_1 + 2\theta^i_n = 0, \\ (1+i)\theta^i_1 - 2\theta^i_n = 0. \end{cases} \tag{49}$$

Определитель системы (49) равен -4, поэтому $\theta^i_1 = \ldots = \theta^i_n = 0$, когда $p > 2$. Если $p = 2$, то при чётном i получаем, что $\theta^i_1 = \ldots = \theta^i_{n-1} = 0$, а при нечётном i, что

$$\theta^i_1 = \theta^i_3 = \ldots = \theta^i_{i-2}, \quad \theta^i_2 = \theta^i_4 = \ldots = \theta^i_{n-1} = 0.$$

Случай $i = n-1$. Пусть $n = 3$. Тогда система состоит из уравнений

$$3\theta^2_1 - 2\theta^2_3 = 0, \quad 2\theta^2_3 - 2\theta^2_1 = 0.$$

Решая её, находим, что $\theta^2_1 = 0$ при любом p, а $\theta^2_3 = 0$, когда $p > 2$.

Пусть теперь $n > 3$. Тогда система состоит из уравнений

$$3\theta^{n-1}_1 - \theta^{n-1}_2 = 0, \quad 2\theta^{n-1}_n - \theta^{n-1}_{n-2} = 0$$

и, если $n > 4$, уравнений

$$2\theta^{n-1}_j - \theta^{n-1}_{j-1} - \theta^{n-1}_{j+1} = 0, \quad j = 2, \ldots, n-3. \tag{50}$$

Выразим сначала θ^{n-1}_{n-2} через θ^{n-1}_n, а затем последовательно из уравнений (50) найдём выражения $\theta^{n-1}_{n-3}, \ldots, \theta^{n-1}_1$ через θ^{n-1}_n. В результате получим, что $\theta^{n-1}_j = 2\theta^{n-1}_n$ для $j = 1, \ldots, n-2$. Но тогда

$$0 = 3\theta^{n-1}_1 - \theta^{n-1}_2 = 4\theta^{n-1}_n - 2\theta^{n-1}_n = 2\theta^{n-1}_n.$$

Значит, $\theta^{n-1}_1 = \ldots = \theta^{n-1}_{n-2} = 0$ при любом p, а $\theta^{n-1}_n = 0$ при $p > 2$.

Случай $i = n$. Система состоит из уравнения

$$2\theta^n_1 - \theta^n_2 = 0,$$

уравнений
$$2\theta_j^n - \theta_{j-1}^n - \theta_{j+1}^n = 0, \quad j = 2, \ldots, n-2, \tag{51}$$
если $n > 3$, и уравнения
$$6\theta_{n-1}^n - 6\theta_{n-2}^n = 0 \tag{52}$$
при $p > 3$. Из равенства $2\theta_1^n - \theta_2^n = 0$ и (51) находим, что $\theta_j^n = j\theta_1^n$ для $j = 2, \ldots, n-1$. Подставив выражения θ_{n-2}^n и θ_{n-1}^n в (52), получим
$$0 = 6(n-1)\theta_1^n - 6(n-2)\theta_1^n = 6\theta_1^n.$$
Следовательно, $\theta_1^n = \ldots = \theta_{n-1}^n = 0$ при $p > 3$. Если же $p = 2$ или $p = 3$, то θ_1^n может быть любым элементом из идеала J^{m-1}, а $\theta_j^n = j\theta_1^n$ для $j = 2, \ldots, n-1$.

Тип C_n, $n > 2$

Случаи $i = 1, \ldots, n-2$. Пусть $n = 3$. Тогда $i = 1$ и система на θ_2^1 и θ_3^1 состоит из уравнений
$$3\theta_2^1 - 2\theta_3^1 = 0, \quad 2\theta_3^1 - 2\theta_2^1 = 0.$$
Определитель этой системы равен 2. Поэтому $\theta_2^1 = \theta_3^1 = 0$ при $p > 2$. Если $p = 2$, то $\theta_2^1 = 0$, а $\theta_3^1 = 0$ может быть любым элементом из J^{m-1}.

Пусть теперь $n > 3$. Тогда при фиксированном i система состоит из уравнения
$$2\theta_n^i - 2\theta_{n-1}^i = 0 \tag{53}$$
и в зависимости от i из следующих уравнений:
$$2\theta_j^i - \theta_{j-1}^i - \theta_{j+1}^i = 0, \quad j = 2, \ldots, i-2, i+2, \ldots, n-1, \tag{54}$$
если $i > 3$ или $i < n-3$, уравнения
$$3\theta_{i+1}^i - 2\theta_{i+2}^i - \theta_{i-1}^i = 0, \tag{55}$$
если $1 < i < n-2$, уравнений
$$\text{а) } 3\theta_2^1 - 2\theta_3^1 = 0, \quad \text{б) } 3\theta_1^2 - \theta_3^2 = 0, \tag{56}$$
если $i = 1$ и $i = 2$ соответственно, а также уравнений
$$\text{а) } 3\theta_{i-1}^i - 2\theta_{i-2}^i - \theta_{i+1}^i = 0, \quad \text{б) } 2\theta_1^i - \theta_2^i = 0, \tag{57}$$
если $i > 2$.

Из равенств (54) при $i < n-2$ последовательно находим, что $\theta_{n-2}^i, \ldots, \theta_{i+1}^i$ выражаются через θ_{n-1}^i и θ_n^i следующим образом:
$$\theta_j^i = (n-j)\theta_{n-1}^i + (1+j-n)\theta_n^i, \quad j = i+1, \ldots, n-2. \tag{58}$$
Аналогично при $i > 2$ из (57) б) и равенств (54) получаем, что
$$\theta_j^i = j\theta_1^i, \quad j = 2, \ldots, i-1. \tag{59}$$

Предположим, что $i > 2$ и $n > 4$. Подставим в уравнения (53), (55) и (57) а) вместо θ^i_{i-2}, θ^i_{i-1} их выражения из (59), а вместо θ^i_{i+1} при $i < n-2$ и θ^i_{i+2} при $i < n-3$ их выражения из (58). В результате получим следующую систему уравнений:

$$\begin{cases} -2\theta^i_{n-1} + 2\theta^i_n = 0, \\ (1-i)\theta^i_1 + (n-i+1)\theta^i_{n-1} + (i-n)\theta^i_n = 0, \\ (1+i)\theta^i_1 + (i+1-n)\theta^i_{n-1} + (n-i-2)\theta^i_n = 0. \end{cases} \tag{60}$$

Определитель системы (60) равен -4, поэтому $\theta^i_1 = \ldots = \theta^i_n = 0$, когда $p > 2$. Если $p = 2$, то в зависимости от чётности n и i из (60) и (58), (59) вытекают следующие равенства:

$$\theta^i_2 = \theta^i_4 = \ldots = \theta^i_{n-1} = 0, \quad \theta^i_1 = \theta^i_3 = \ldots = \theta^i_{i-2}, \quad \theta^i_{i+2} = \theta^i_{i+4} = \ldots = \theta^i_n,$$

если n и i нечётны;

$$\theta^i_2 = \theta^i_4 = \ldots = \theta^i_{i-2} = 0, \quad \theta^i_1 = \theta^i_3 = \ldots = \theta^i_n, \quad \theta^i_{i+2} = \theta^i_{i+4} = \ldots = \theta^i_{n-1},$$

если n нечётно, а i чётно;

$$\theta^i_2 = \theta^i_4 = \ldots = \theta^i_n = 0, \quad \theta^i_1 = \theta^i_3 = \ldots = \theta^i_{i-2}, \quad \theta^i_{i+2} = \theta^i_{i+4} = \ldots = \theta^i_{n-1},$$

если n чётно, а i нечётно;

$$\theta^i_2 = \theta^i_4 = \ldots = \theta^i_{i-2} = 0, \quad \theta^i_1 = \theta^i_3 = \ldots = \theta^i_{n-1}, \quad \theta^i_{i+2} = \theta^i_{i+4} = \ldots = \theta^i_n,$$

если n и i чётны.

Исследуем случай $i = 1$. Из (58) и (55) а) следует, что $n\theta^1_{n-1} + (1-n)\theta^1_n = 0$. Система уравнений

$$\begin{cases} n\theta^1_{n-1} + (1-n)\theta^1_n = 0, \\ -2\theta^1_{n-1} + 2\theta^1_n = 0 \end{cases}$$

имеет определитель, равный 2, поэтому

$$\theta^1_2 = \theta^1_3 = \ldots = \theta^i_n = 0$$

при $p > 2$. Если же $p = 2$, то

$$0 = \theta^1_2 = \theta^1_4 = \ldots, \quad \theta^1_3 = \theta^1_5 = \ldots.$$

Пусть, наконец, $i = 2$. Составим систему уравнений из (53), (56) б) и (55), заменив θ^2_3 при $n > 4$ и θ^2_4 при $n > 5$ их выражениями из (58):

$$\begin{cases} 3\theta^2_1 + (3-n)\theta^2_{n-1} + (n-4)\theta^2_n = 0, \\ -\theta^2_1 + (n-1)\theta^2_{n-1} + (2-n)\theta^2_n = 0, \\ -2\theta^2_{n-1} + 2\theta^2_n = 0. \end{cases}$$

Её определитель равен 4, поэтому

$$\theta^2_1 = \theta^2_3 = \theta^2_4 = \ldots = \theta^2_n = 0$$

при $p > 2$. Если $p = 2$, то

$$\theta_1^2 = \theta_3^2 = \dots, \quad \theta_4^2 = \theta_6^2 = \dots.$$

Случаи $i = n-1, n$. Если $n = 3$, то θ_1^2, θ_3^2 и θ_1^3, θ_2^3 связаны соотношениями

$$\begin{cases} 3\theta_1^2 - \theta_3^2 = 0, \\ 6\theta_3^2 - 6\theta_1^2 = 0; \end{cases} \qquad \begin{cases} 2\theta_1^3 - \theta_2^3 = 0, \\ -2\theta_1^3 + 2\theta_2^3 = 0. \end{cases}$$

Решая первую систему, находим, что $\theta_1^2 = 0$ при $p > 3$, $\theta_3^2 = 0$ при $p > 2$ и если $p = 2$, то $\theta_1^2 = \theta_3^2$. Решая вторую систему, получаем, что $\theta_2^3 = 0$ при любом p, а $\theta_1^3 = 0$ при $p > 2$.

Пусть теперь $n > 3$. Тогда система на θ_j^i, $i = n-1, n$, состоит из уравнения

$$2\theta_1^i - \theta_2^i = 0, \tag{61}$$

уравнений

$$2\theta_j^i - \theta_{j-1}^i - \theta_{j+1}^i = 0, \quad j = 2, \dots, i-2, \tag{62}$$

если $n > 4$, и уравнений

$$\text{а) } 3\theta_{n-2}^{n-1} - 2\theta_{n-3}^{n-1} - \theta_n^{n-1} = 0, \quad \text{б) } 6\theta_n^{n-1} - 6\theta_{n-2}^{n-1} = 0, \quad \text{в) } 2\theta_{n-1}^n - 2\theta_{n-2}^n = 0. \tag{63}$$

Из (61) и, если $n > 4$, из (62) находим, что

$$\theta_j^i = j\theta_1^i, \quad j = 2, \dots, i-1. \tag{64}$$

Подставив выражения θ_{n-3}^{n-1} и θ_{n-2}^{n-1} из (64) в (63) а) и (63) б), получим следующую систему на θ_1^{n-1} и θ_n^{n-1}:

$$\begin{cases} n\theta_1^{n-1} - \theta_n^{n-1} = 0, \\ 6\theta_n^{n-1} - 6(n-2)\theta_1^{n-1} = 0. \end{cases}$$

Её определитель равен 12, поэтому

$$\theta_j^{n-1} = 0$$

для $j = 1, \dots, n$ при $p > 3$. Если $p = 2$, то

$$0 = \theta_2^{n-1} = \theta_4^{n-1} = \dots, \quad \theta_1^{n-1} = \theta_3^{n-1} = \dots.$$

Если же $p = 3$, то

$$\theta_j^{n-1} = j\theta_1^{n-1}$$

для $j = 1, \dots, n-2, n$.

Подставим теперь выражения для θ_{n-2}^n и θ_{n-1}^n из (64) в уравнение (63) в). Тогда получим, что $2\theta_1^n = 0$. Следовательно,

$$\theta_1^n = \dots = \theta_{n-1}^n = 0$$

при $p > 2$. Если же $p = 2$, то

$$0 = \theta_2^n = \theta_4^n = \dots, \quad \theta_1^n = \theta_3^n = \dots.$$

Тип D_n, $n > 3$

Пусть $n = 4$. В силу известной симметрии порядка три диаграммы Дынкина типа D_4 достаточно найти условия, которым удовлетворяют θ_2^1, θ_3^1, θ_4^1 и θ_1^2, θ_3^2, θ_4^2. Системы уравнений, связывающие эти элементы, следующие:

$$\begin{cases} 3\theta_2^1 - 2\theta_3^1 - 2\theta_4^1 = 0, \\ 2\theta_3^1 - \theta_2^1 = 0, \\ 2\theta_4^1 - \theta_2^1 = 0; \end{cases} \qquad \begin{cases} 3\theta_1^2 - \theta_3^2 - \theta_4^2 = 0, \\ 3\theta_3^2 - \theta_1^2 - \theta_4^2 = 0, \\ 3\theta_4^2 - \theta_1^2 - \theta_3^2 = 0. \end{cases}$$

Определители этих систем равны 4 и 16 соответственно. Поэтому

$$\theta_j^i = 0$$

для всех i, j при $p > 2$. Если же $p = 2$, то

$$\theta_2^1 = \theta_2^3 = \theta_2^4 = 0, \quad \theta_1^2 = \theta_3^2 + \theta_4^2.$$

Далее считаем, что $n > 4$.

Случаи $i = 1, \ldots, n-4$. При фиксированном i система на θ_j^i состоит из уравнений

$$\text{а) } 2\theta_n^i - \theta_{n-1}^i = 0, \quad \text{б) } 2\theta_{n-1}^i - \theta_{n-2}^i = 0, \quad \text{в) } 2\theta_{n-2}^i - \theta_n^i - \theta_{n-1}^i - \theta_{n-3}^i = 0 \quad (65)$$

и в зависимости от i из следующих уравнений:

$$2\theta_j^i - \theta_{j-1}^i - \theta_{j+1}^i = 0, \quad j = 2, \ldots, i-2, i+2, \ldots, n-3, \quad (66)$$

если $i > 3$ или $i < n-4$, уравнения

$$3\theta_{i+1}^i - 2\theta_{i+2}^i - \theta_{i-1}^i = 0, \quad (67)$$

если $i > 1$, уравнений

$$\text{а) } 3\theta_{i+1}^i - 2\theta_{i+2}^i - \theta_{i-1}^i = 0, \quad \text{б) } 2\theta_1^i - \theta_2^i = 0, \quad (68)$$

если $i > 2$, а также уравнений

$$\text{а) } 3\theta_2^1 - 2\theta_3^1 = 0, \quad \text{б) } 3\theta_1^2 - \theta_3^2 = 0, \quad (69)$$

когда $i = 1$ и $i = 2$ соответственно.

Из равенств (65) а) и (65) в) следует, что $\theta_{n-2}^i = 2\theta_n^i$ и $\theta_{n-3}^i = 3\theta_n^i - \theta_{n-1}^i$. Выражения $\theta_{n-4}^i, \ldots, \theta_{i+1}^i$ при $i < n-4$ последовательно находим из равенств (66). В итоге получаем, что

$$\theta_j^i = (n-j)\theta_n^i + (2+j-n)\theta_{n-1}^i, \quad j = i+1, \ldots, n-2. \quad (70)$$

Пусть $i = 1$. Подставляя выражения θ_2^1, θ_3^1 и θ_{n-2}^1 из (70) в равенства (65) б) и (69) а), получаем следующую систему уравнений на θ_{n-1}^1 и θ_n^1:

$$\begin{cases} 2\theta_{n-1}^1 - 2\theta_n^1 = 0, \\ (2-n)\theta_{n-1}^1 + n\theta_n^1 = 0. \end{cases}$$

Её определитель равен 4, поэтому

$$\theta_2^1 = \ldots = \theta_n^1 = 0$$

при $p > 2$. Если $p = 2$, то при чётном n имеем

$$\theta_2^1 = \theta_4^1 = \ldots = \theta_{n-2}^1 = 0, \quad \theta_3^1 = \theta_5^1 = \ldots = \theta_{n-3}^1 = \theta_{n-1}^1 + \theta_n^1,$$

а при нечётном n

$$\theta_2^1 = \theta_3^1 = \ldots = \theta_{n-3}^1 = 0, \quad \theta_{n-1}^1 = \theta_n^1.$$

Пусть $i = 2$. Из (67) при $i = 2$ и (70) следует, что $\theta_1^2 = (n-1)\theta_n^2 + (3-n)\theta_{n-1}^2$. Подставив выражения θ_3^2 и θ_{n-2}^2 из (70), а также найденное выражение θ_1^2 в уравнения (65) б) и (69) б), получаем следующую систему уравнений на θ_{n-1}^2 и θ_n^2:

$$\begin{cases} 2\theta_{n-1}^2 - 2\theta_n^2 = 0, \\ (4 - 2n)\theta_{n-1}^2 + 2n\theta_n^2 = 0. \end{cases}$$

Её определитель равен 8, поэтому

$$\theta_1^2 = \theta_3^2 = \ldots = \theta_n^2 = 0$$

при $p > 2$. Если $p = 2$, то

$$\theta_j^2 = (n - j)(\theta_{n-1}^2 + \theta_n^2), \quad j = 1, 3, \ldots, i - 1.$$

Пусть теперь $i > 2$. Из уравнений (68) б) и (66) находим, что

$$\theta_j^i = j\theta_1^i, \quad j = 2, \ldots, i - 1. \tag{71}$$

Подставим выражения θ_{i+1}^i, θ_{i+2}^i из (70) и θ_{i-1}^i, θ_{i-2}^i из (71) в уравнения (67), (68) а) и (65) б). В результате получим следующую систему уравнений на θ_1^i, θ_{n-1}^i и θ_n^2:

$$\begin{cases} (1 + i)\theta_1^i + (n - i - 3)\theta_{n-1}^i + (1 + i - n)\theta_n^i = 0, \\ (1 - i)\theta_1^i + (i + 1 - n)\theta_{n-1}^i + (n + 1 - i)\theta_n^i = 0, \\ 2\theta_{n-1}^i - 2\theta_n^i = 0. \end{cases} \tag{72}$$

Определитель системы (72) равен 8, поэтому

$$\theta_1^i = \ldots = \theta_n^i = 0,$$

когда $p > 2$.

Пусть $p = 2$. Тогда при чётном n система (72) вырождается в одно уравнение

$$(1 + i)(\theta_1^i + \theta_{n-1}^i + \theta_n^i) = 0.$$

Отсюда и из формул (70), (71) получаем, что

$$\theta_2^i = \theta_4^i = \ldots = \theta_{n-2}^i = 0$$

и при чётном i

$$\theta_1^i = \theta_3^i = \ldots = \theta_{n-3}^i = \theta_{n-1}^i + \theta_n^i,$$

а при нечётном i

$$\theta_1^i = \theta_3^i = \ldots = \theta_{i-2}^i, \quad \theta_{i+2}^i = \theta_{i+4}^i = \ldots = \theta_{n-3}^i = \theta_{n-1}^i + \theta_n^i.$$

При нечётном n система (72) вырождается в одно уравнение

$$(1+i)\theta_1^i + i(\theta_{n-1}^i + \theta_n^i) = 0.$$

Отсюда и из формул (70), (71) получаем, что

$$\theta_1^i = \ldots = \theta_{i-1}^i = \theta_{i+1}^i = \theta_{i+3}^i = \ldots = \theta_{n-2}^i = 0,$$
$$\theta_{i+2}^i = \theta_{i+4}^i = \ldots = \theta_{n-3}^i = \theta_{n-1}^i + \theta_n^i$$

при чётном i, а при нечётном i

$$\theta_2^i = \theta_4^i = \ldots = \theta_{i-1}^i = \theta_{i+1}^i = \theta_{i+2}^i = \ldots = \theta_{n-2}^i = 0,$$
$$\theta_1^i = \theta_3^i = \ldots = \theta_{i-2}^i, \quad \theta_{n-1}^i = \theta_n^i.$$

Случай $i = n$. Система на θ_j^n состоит из уравнений

$$\text{а) } 2\theta_{n-1}^n - \theta_{n-2}^n = 0, \quad \text{б) } 3\theta_{n-2}^n - 2\theta_{n-1}^n - 2\theta_{n-3}^n = 0, \quad \text{в) } 2\theta_1^n - \theta_2^n = 0 \tag{73}$$

и уравнений

$$2\theta_j^n - \theta_{j-1}^n - \theta_{j+1}^n = 0, \quad j = 2, \ldots, n-3. \tag{74}$$

Из уравнений (73) в) и (74) находим, что

$$\theta_j^n = j\theta_1^n, \quad j = 2, \ldots, n-3. \tag{75}$$

Подставим выражения θ_{n-3}^n, θ_{n-2}^n из (75) в равенства (73) а) и (73) б). В результате получим следующую систему уравнений на θ_1^n и θ_{n-1}^n:

$$\begin{cases} (2-n)\theta_1^n + 2\theta_{n-1}^n = 0, \\ n\theta_1^n - 2\theta_{n-1}^n = 0. \end{cases}$$

Её определитель равен -4, поэтому

$$\theta_1^n = \ldots = \theta_{n-1}^n = 0$$

при $p > 2$. Если же $p = 2$, то

$$\theta_1^n = \ldots = \theta_{n-2}^n = 0$$

при нечётном n, а при чётном n

$$\theta_1^n = \theta_3^n = \ldots = \theta_{n-1}^n, \quad \theta_2^n = \theta_4^n = \ldots = \theta_{n-2}^n = 0.$$

Ввиду известной симметрии порядка два диаграммы Дынкина типа D_n, $n > 4$, случай $i = n-1$ получается из случая $i = n$.

Случай $i = n-2$. Система на θ_j^n состоит из уравнений

$$\text{а) } 2\theta_n^{n-2} - \theta_{n-1}^{n-2} - \theta_{n-3}^{n-2} = 0, \quad \text{б) } 3\theta_{n-1}^{n-2} - \theta_n^{n-2} - \theta_{n-3}^{n-2} = 0, \tag{76}$$

$$\text{а) } 3\theta_{n-3}^{n-2} - \theta_n^{n-2} - \theta_{n-1}^{n-2} - 2\theta_{n-4}^{n-2} = 0, \quad \text{б) } 2\theta_1^{n-2} - \theta_n^{n-2} = 0 \tag{77}$$

и, если $n > 5$, уравнений

$$2\theta_j^{n-2} - \theta_{j-1}^{n-2} - \theta_{j+1}^{n-2} = 0, \quad j = 2, \dots, n-3. \tag{78}$$

Из уравнений (77) б) и (78) находим, что

$$\theta_j^{n-2} = j\theta_1^{n-2}, \quad j = 2, \dots, n-3. \tag{79}$$

Подставим выражения θ_{n-4}^{n-2} и θ_{n-3}^{n-2} из (79) в равенства (76) а), (76) б) и (77) а). В результате получим следующую систему уравнений на θ_1^{n-2}, θ_{n-1}^{n-2} и θ_n^{n-2}:

$$\begin{cases} (3-n)\theta_1^{n-2} - \theta_{n-1}^{n-2} + 3\theta_n^{n-2} = 0, \\ (3-n)\theta_1^{n-2} + 3\theta_{n-1}^{n-2} - \theta_n^{n-2} = 0, \\ (n-1)\theta_1^{n-2} - \theta_{n-1}^{n-2} - \theta_n^{n-2} = 0. \end{cases} \tag{80}$$

Её определитель равен -16, поэтому

$$\theta_j^{n-2} = 0$$

для $j = 1, \dots, n-3, n-1, n$ при $p > 2$.

Пусть $p = 2$. Тогда система (80) вырождается в одно уравнение

$$(1-n)\theta_1^{n-2} + \theta_{n-1}^{n-2} + \theta_n^{n-2} = 0.$$

Отсюда и из формул (79) получаем, что

$$0 = \theta_2^{n-2} = \theta_4^{n-2} = \ldots = \theta_{n-3}^{n-2}, \quad \theta_1^{n-2} = \theta_3^{n-2} = \ldots = \theta_{n-4}^{n-2} = 0, \quad \theta_{n-1}^{n-2} = \theta_n^{n-2}$$

при нечётном n и

$$0 = \theta_2^{n-2} = \theta_4^{n-2} = \ldots = \theta_{n-4}^{n-2}, \quad \theta_1^{n-2} = \theta_3^{n-2} = \ldots = \theta_{n-3}^{n-2} = \theta_{n-1}^{n-2} + \theta_n^{n-2}$$

при n чётном.

Случай $i = n-3$. Система на θ_j^n состоит из уравнений

$$2\theta_n^{n-3} - \theta_{n-2}^{n-3} = 2\theta_{n-1}^{n-3} - \theta_{n-2}^{n-3} = 3\theta_{n-2}^{n-3} - 2\theta_n^{n-3} - 2\theta_{n-1}^{n-3} - \theta_{n-4}^{n-3} = 0, \tag{81}$$

уравнения

$$3\theta_1^2 - \theta_3^2 = 0$$

при $n = 5$, уравнений

$$3\theta_{n-4}^{n-3} - 2\theta_{n-5}^{n-3} - \theta_{n-2}^{n-3} = \theta_1^{n-3} - \theta_2^{n-3} = 0, \tag{82}$$

когда $n > 5$, а также уравнений

$$2\theta_j^{n-2} - \theta_{j-1}^{n-2} - \theta_{j+1}^{n-2} = 0, \quad j = 2, \dots, n-5, \tag{83}$$

при $n > 6$.

Из равенства $3\theta_1^2 - \theta_3^2 = 0$ при $n = 5$ и уравнений (82), (83) находим, что

$$\theta_j^{n-3} = j\theta_1^{n-3}, \quad j = 2, \dots, n-4, n-2. \tag{84}$$

Подставим выражения θ_{n-4}^{n-3} и θ_{n-2}^{n-3} из (84) в равенства (81). В результате получим следующую систему уравнений на θ_1^{n-3}, θ_{n-1}^{n-3} и θ_n^{n-3}:

$$\begin{cases} (2-n)\theta_1^{n-3} + 2\theta_n^{n-3} = 0, \\ (2-n)\theta_1^{n-2} + 2\theta_{n-1}^{n-3} = 0, \\ (2n-2)\theta_1^{n-3} - 2\theta_{n-1}^{n-3} - 2\theta_n^{n-3} = 0. \end{cases}$$

Её определитель равен -8, поэтому

$$\theta_j^{n-2} = 0$$

для $j = 1, \ldots, n-4, n-2, n-1, n$ при $p > 2$. Если $p = 2$, тогда

$$\theta_1^{n-3} = 0$$

при чётном n и, значит, в силу (84)

$$\theta_j^{n-2} = 0$$

для $j = 1, \ldots, n-4, n-2$. При нечётном n имеем

$$0 = \theta_2^{n-3} = \theta_4^{n-3} = \ldots = \theta_{n-2}^{n-3}, \quad \theta_1^{n-3} = \theta_3^{n-3} = \ldots = \theta_{n-5}^{n-3}.$$

Аналогично рассматриваются типы E_8, E_7, E_6 и F_4. Используя полученные результаты, нетрудно убедиться в справедливости следующего предложения.

Предложение 4. *Пусть тождественный по модулю подгруппы $\Phi(J^{m-1})$ автоморфизм φ группы $S\Phi(\mathbb{Z}_{p^m})$ удовлетворяет условию* (Б). *Тогда с точностью до умножения φ на диагональный, внутренний, центральный и элементарные гиперцентральные автоморфизмы можно считать, что $x_r^\varphi(1) = x_r(1)$ для всех $r \in \Pi(\Phi)$.*

В силу предложений 4 и 1 можно считать, что $x_r^\varphi(1) = x_r(1)$ для всех $r \in \Phi$, если группа $S\Phi(\mathbb{Z}_{p^m})$ отлична от групп $S\Phi(\mathbb{Z}_{2^m})$, где $\Phi = B_n$, $\Phi = C_n$ или $\Phi = F_4$. В оставшихся случаях имеет место предложение 5.

Предложение 5. *Пусть $\Phi = B_n$, $\Phi = C_n$ или $\Phi = F_4$. Если автоморфизм φ группы $S\Phi(\mathbb{Z}_{p^m})$ тождествен по модулю подгруппы $\Phi(J^{m-1})$ и $x_r^\varphi(1) = x_r(1)$ для всех $r \in \Pi(\Phi)$, тогда существует такой гиперцентральный автоморфизм ψ, что $x_r^{\psi\varphi}(1) = x_r(1)$ для всех $r \in \Phi$.*

Доказательство. Нетрудно проверить, что ψ является произведением центрального автоморфизма и гиперцентральных автоморфизмов вида (19)—(22). □

5. Автоморфизмы, тождественные по модулю $\Phi(J^{m-1})$, III

В этом разделе изучаются автоморфизмы группы $S\Phi(\mathbb{Z}_{p^m})$, тождественные на $U\Phi(\mathbb{Z}_{p^m})$ и тождественные по модулю $\Phi(J^{m-1})$ на подгруппе $U\Phi^-(J)$.

Пусть автоморфизм $\varphi \in \mathrm{Aut}(S\Phi(\mathbb{Z}_{p^m}))$ удовлетворяет условию

$$x_r^{\varphi}(1) = x_r(1) \text{ для всех } r \in \Phi^+ \text{ и для любого } r \in \Phi^-$$
$$x_r^{\varphi}(p) = x_r(p) \cdot h_r \cdot \prod_{w \in \Phi} x_w(\lambda_w^r), \text{ где } h_r \in H(J^{m-1}) \text{ и } \lambda_w^r \in J^{m-1}. \tag{B}$$

Лемма 12. *Автоморфизм φ тождествен на подгруппе $U\Phi(\mathbb{Z}_{p^m}) \cdot \Phi(J^2)$.*

Доказательство. Пусть $r \in \Phi^-$ и $v_r = x_r(-p)\varphi(x_r(p))$. Тогда $\varphi(x_r(p)) = x_r(p)v_r$ и $v_r \in \Phi(J^{m-1})$. Из соотношения (1) и перестановочности элементов $x_r(p)$ и v_r следует, что $\varphi(x_r(np)) = x_r(np)v_r^n$ для всякого целого числа n. Отсюда при n, кратном p, получаем, что $v_r^n = 1$, и поэтому $\varphi(x_r(np)) = x_r(np)$. Преобразовав соотношение (5) к виду

$$h_r(1-tu) = x_r(-(1-tu)^{-1}t^2u)[x_r(t), x_{-r}(u)]x_{-r}((1-tu)^{-1}tu^2)$$

и положив $t = np^2$, $u = 1$, видим, что $\varphi(h_r(1-np^2) = h_r(1-np^2)$ для всякого целого n. Лемма доказана. □

Лемма 13. *Если для фиксированных $r \in \Phi^-$ и $w \in \Phi$ выполняется хотя бы одно из условий*

A1) $w \in \Phi^-$ *и* $r - w \notin \Phi_0^-$,

A2) *существует такой* $q \in \Phi^+$, *что* $w + q \in \Phi$, $r + q \notin \Phi_0^-$ *и* $w - q \notin \Phi$,

A3) *существуют такие* $q, s \in \Phi^+$, *что* $r+q, w+q, w+q+s \in \Phi$, $r+q+s \notin \Phi_0^-$ *и* $w-q, w-s, w-q-s, w+q-s \notin \Phi$,

то $\lambda_w^r = 0$.

Доказательство. Зафиксируем корень $r \in \Phi^-$, и пусть $q \in \Phi^+$. Используя коммутаторное тождество $[xy, z] = [x, z]^y[y, z]$, получим, что

$$\varphi([x_r(p), x_q(1)]) = [\varphi(x_r(p)), \varphi(x_q(1))] = \\ = [x_r(p)v_r, x_q(1)] = [x_r(p), x_q(1)]^{v_r}[v_r, x_q(1)].$$

Элементы $[x_r(p), x_q(1)]$ и v_r перестановочны, так как лежат в подгруппах $\Phi(J)$ и $\Phi(J^{m-1})$ соответственно. Поэтому $\varphi([x_r(p), x_q(1)]) = [x_r(p), x_q(1)][v_r, x_q(1)]$.

Допустим, что $r + q \notin \Phi_0^-$. Тогда $[x_r(p), x_q(1)] \in U\Phi(J) \cdot \Phi(J^2)$ и поэтому по лемме 12 $\varphi([x_r(p), x_q(1)]) = [x_r(p), x_q(1)]$, а значит, $[v_r, x_q(1)] = 1$. В то же время

$$[v_r, x_q(1)] = \left[h_r \prod_{w \in \Phi} x_w(\lambda_w^r), x_q(1)\right] = [h_r, x_q(1)] \prod_{w \in \Phi} [x_w(\lambda_w^r), x_q(1)] = \\ = [h_r, x_q(1)]x_q(-\lambda_{-q}^r)h_q(1+\lambda_{-q}^r) \times \\ \times \prod_{w, w+q \in \Phi,\ w-q \notin \Phi} x_{w+q}(\lambda_w^r N_{w,q}) \prod_{w, w+2q \in \Phi} x_{w+2q}(\lambda_{w+q}^r N_{w+q,q} + \lambda_w^r c_{21,qw}). \tag{85}$$

Зафиксируем корень w. Если $r - w \notin \Phi_0$, то, полагая в (85) $q = -w$, получаем, что $\lambda_w^r = 0$. Если корни r и w вместе с корнем q удовлетворяют условию A2), то из (85) следует, что $\lambda^r_w N_{w,q} = 0$. Но $w - q \notin \Phi$, поэтому $N_{w,q} = \pm 1$, а значит, $\lambda^r_w = 0$.

Пусть $q, s \in \Phi^+$. Как и выше, получаем, что

$$\varphi([[x_r(p), x_q(1)], x_s(1)) = [[x_r(p), x_q(1)], x_s(1)][[v_r, x_q(1)], x_s(1)].$$

Если $r + q + s \notin \Phi_0^-$, то $[[x_r(p), x_q(1)], x_s(1)] \in U\Phi(J) \cdot \Phi(J^2)$, и поэтому по лемме 12

$$\varphi([[x_r(p), x_q(1)], x_s(1)]) = [[x_r(p), x_q(1)], x_s(1)].$$

В этом случае $[[v_r, x_q(1)], x_s(1)] = 1$. С другой стороны, ввиду (85) имеем

$$\begin{aligned}
&[[v_r, x_q(1)], x_s(1)] = [[h_r, x_q(1)], x_s(1)][x_q(-\lambda^r_{-q}), x_s(1)]x_s(-(h_q, s)\lambda^r_{-q}) \times \\
&\quad \times \prod_{w, w+q \in \Phi,\ w-q \notin \Phi} [x_{w+q}(\lambda^r_w N_{w,q}), x_s(1)] \times \\
&\quad \times \prod_{w, w+2q \in \Phi} [x_{w+2q}(\lambda^r_{w+q} N_{w+q,q} + \lambda^r_w c_{21,qw}), x_s(1)]. \qquad (86)
\end{aligned}$$

Зафиксируем корень w и предположим, что r, w, q, s удовлетворяют условию А3). Тогда $x_{w+q+s}(\lambda^r_w N_{w,q} N_{w+q,s})$ — единственный сомножитель из правой части равенства (86), который лежит в корневой подгруппе X_{w+q+s}. Действительно, если предположить, что корень $w + q + s$ совпадает с одной из сумм $w' + q + 2s$, $w' + 2q + s$, $w' + 2q + 2s$, то среди $w - q$, $w - s$, $w - q - s$ есть хотя бы один корень, что невозможно. Так как $w - q, w + q - s \notin \Phi$, то обе константы $N_{w,q}$ и $N_{w+q,s}$ равны ± 1, а значит, $\lambda^r_w = 0$. Лемма доказана. $\square$

Корень $w \neq r_0$ будем называть *r-экстремальным*, если он не удовлетворяет ни одному из условий А1)—А3).

Лемма 14. *Пусть Φ — система корней ранга больше двух. Следующие корни и только они являются $(-r_0)$-экстремальными*:

$$\begin{aligned}
A_n\colon &\quad r_0 - r_1,\ r_0 - r_n,\ r_0 - r_1 - r_n; \\
B_n\colon &\quad r_0 - r_2,\ r_0 - r_1 - 2r_2 - r_3,\ r_1 + \cdots + r_n,\ r_3 + \cdots + r_n,\ r_1, \\
&\quad - r_2 - \cdots - r_n; \\
C_n\colon &\quad r_0 - r_1,\ r_0 - 2r_1,\ r_0 - 2r_1 - r_2; \\
D_n\colon &\quad r_0 - r_2,\ r_0 - r_1 - 2r_2 - r_3,\ r_1 \text{ и если } n = 4, \text{ то } r_3; \\
E_8\colon &\quad r_0 - r_8,\ 2r_1 + +2r_2 + 3r_3 + 4r_4 + 3r_5 + 2r_6 + r_7; \\
E_7\colon &\quad r_0 - r_1,\ r_2 + r_3 + 2r_4 + 2r_5 + 2r_6 + r_7; \\
E_6\colon &\quad r_0 - r_2,\ r_1 + r_3 + r_4 + r_5 + r_6; \\
F_4\colon &\quad r_0 - r_1,\ r_2 + 2r_3 + 2r_4,\ r_1 + 2r_2 + 3r_3 + 2r_4, \\
&\quad r_2 + 2r_3 + r_4,\ -r_1 - r_2 - r_3.
\end{aligned}$$

Доказательство. Обозначим через w корень, который не удовлетворяет ни одному из условий А1)—А3) при $r = -r_0$. Тогда $-w \notin \Pi(\Phi)$. В самом деле, если $r_0+w\notin\Phi$, то корень w удовлетворяет условию A1). Если $r_0+w\in\Phi$, то, полагая $q=r_0+w$, $s=r_0$, видим, что корень w удовлетворяет условию A3).

Так как $w\neq r_0$ и $-w\notin\Phi$, то найдётся такой простой корень q, что $w+q\in\Phi$. Если $r_0-q\notin\Phi$ и все корни системы корней Φ имеют одинаковую длину, то w удовлетворяет условию A2). Значит, если Φ типа A_n, D_n или E_6, E_7, E_8, то $(-r_0)$-экстремальные корни находятся среди корней, удовлетворяющих следующему условию:

A$'$) если $q\in\Pi(\Phi)$ и $w+q\in\Phi$, то $r_0-q\in\Phi$.

Обращаясь к [1, табл. I—IV], легко видеть, что разность r_0-q, где $q\in\Pi(\Phi)$, лежит в Φ тогда и только тогда, когда $q=r_1$ или r_n, если $\Phi=A_n$, $q=r_2$, если $\Phi=D_n$ или $\Phi=E_6$, $q=r_1$, если $\Phi=E_7$, наконец, $q=r_8$, если $\Phi=E_8$. Снова обращаясь к таблицам, находим, что условию A$'$) среди отрицательных корней удовлетворяет только корень $-r_0$, а среди положительных, отличных от r_0, следующие:

$$
\begin{aligned}
A_n&: \quad r_0-r_1,\ r_0-r_n,\ r_0-r_1-r_n;\\
D_n&: \quad r_0-r_2,\ r_0-r_1-2r_2-r_3,\ r_1 \text{ и если } n=4, \text{ то } r_3;\\
E_8&: \quad r_0-r_8,\ 2r_1+2r_2+3r_3+4r_4+3r_5+2r_6+r_7;\\
E_7&: \quad r_0-r_1,\ r_2+r_3+2r_4+2r_5+2r_6+r_7;\\
E_6&: \quad r_0-r_2,\ r_1+r_3+r_4+r_5+r_6.
\end{aligned}
$$

Однако корень $-r_0$ не является $(-r_0)$-экстремальным, поскольку удовлетворяет условию A3). В этом нетрудно убедиться, положив $s=r_0$ и $q=r_0-r$, где $r\in\Pi(\Phi)$ и $r_0-r\in\Phi$. В то же время нетрудно убедиться, что оставшиеся корни действительно являются $(-r_0)$-экстремальными.

Рассмотрим системы корней типов B_n, C_n и F_4. Предположим сначала, что $w\in\Phi^-$. Так как w не удовлетворяет условию A1) и по доказанному выше $w\neq r_0$, то $w+r_0\in\Phi$. Обращаясь к таблицам из [1], видим, что для w существуют следующие возможности:

$$
\begin{aligned}
B_n&: \quad -e_1\pm e_j,\ -e_2\pm e_j,\ j=3,\ldots,n,\ -e_1,\ -e_2;\\
C_n&: \quad -e_1\pm e_j,\ j=2,\ldots,n;\\
F_4&: \quad -e_1\pm e_j,\ -e_1\pm e_j,\ j=3,4,\ -e_1,\ -e_2,\ (-e_1-e_2\pm e_3\pm e_4)/2.
\end{aligned}
$$

Однако в случае $\Phi=B_n$ корни $-e_1$ и $-e_1\pm e_j$, $j=3,\ldots,n$, корни $-e_2-e_j$, $j=3,\ldots,n$, и корни $-e_2+e_j$, $j=4,\ldots,n$, удовлетворяют условию A2) при q, равном e_1-e_2, e_j и $e_{j-1}-e_j$ соответственно, а $-(-e_2+e_3)\in\Pi(\Phi)$. В случае $\Phi=C_n$ корень $-e_1-e_2$ и корни $-e_1\pm e_j$, $j=3,\ldots,n$, удовлетворяют условию A2) при q, равном $2e_2$ и $e_2\mp e_j$ соответственно, а $-(-e_1+e_2)\in\Pi(\Phi)$. Наконец, в случае $\Phi=F_4$ все перечисленные корни, кроме $-e_2$, тоже удовлетворяют условию A2) при подходящем q из множества r_2, r_3, r_4, r_2+r_3. Оставшийся корень $-e_2$, равный $-r_2-\ldots-r_n$, когда $\Phi=B_n$, и равный $-r_1-r_2-r_3$, если $\Phi=F_4$, является $(-r_0)$-экстремальным.

Предположим теперь, что $w\in\Phi^+$ и рассмотрим отдельно каждый тип.

Пусть $\Phi = B_n$. Можно считать, что $w + r_2 \in \Phi$ или w — короткий корень, поскольку иначе w удовлетворяет условию A2). Предположим, что $w + r_2 \in \Phi$. Тогда w совпадает с одним из следующих корней: $e_3 \pm e_j$, $j = 4, \dots, n$, или e_3, $e_1 - e_2$, $e_1 + e_3$. Корни $e_3 - e_j$, $j = 4, \dots, n$, и $e_3 + e_j$, $j = 5, \dots, n$, удовлетворяют условию A2) при q, равном e_j и $e_{j-1} - e_j$ соответственно. Оставшиеся корни $e_1 + e_3 = r_0 - r_2$, $e_3 + e_4 = r_0 - r_1 - 2r_2 - r_3$, $e_3 = r_3 + \ldots + r_n$, $e_1 - e_2 = r_1$ являются $(-r_0)$-экстремальными, что нетрудно проверить.

Допустим, что w — короткий корень. Тогда $w = e_j$, $j = 1, \dots, n$. Корни e_2 и e_j, $j = 4, \dots, n$, удовлетворяют условию A2) при q, равном $e_1 - e_2$ и $e_{j-1} - e_j$ соответственно. Случай $w = e_3$ рассмотрен выше, а корень $e_1 = r_1 + \ldots + r_n$ является $(-r_0)$-экстремальным.

Пусть $\Phi = C_n$. Можно считать, что $w + r_1 \in \Phi$ или $w + s, w - s \in \Phi$ для некоторого $s \in \Pi(\Phi)$, иначе w удовлетворяет условию A2). Отсюда следует, что w совпадает с одним из следующих корней: $2e_j$, $j = 2, \dots, n$, или $e_2 \pm e_j$, $j = 3, \dots, n$, или $e_j + e_{j+1}$, $j = 1, \dots, n-1$. Однако корни $2e_j$, $j = 3, \dots, n$, корни $e_2 - e_j$, $j = 3, \dots, n$, и $e_2 + e_j$, $j = 4, \dots, n$, удовлетворяют условию A2) при q, равном соответственно $e_2 - e_j$, $2e_j$ и $e_{j-1} - e_j$. Оставшиеся корни $e_1 + e_2 = r_0 - r_1$, $2e_2 = r_0 - 2r_1$, $e_2 + e_3 = r_0 - 2r_1 - r_2$, очевидно, являются $(-r_0)$-экстремальными.

Пусть $\Phi = F_4$. Можно считать, что $w + r_2 \notin \Phi$, так как иначе w удовлетворяет условию A2). Поэтому w находится среди корней $e_j + e_3$, $j = 1, 2, 4$, e_j или $e_j - e_4$, $j = 1, 2, 3$, или $(e_1 \pm e_2 \pm e_3 - e_4)/2$, $(e_1 + e_2 + e_3 + e_4)/2$. Однако, кроме корней $(e_1 - e_2 + e_3 + e_4)/2 = r_2 + 2r_3 + r_4$, $e_1 - e_2 = r_2 + 2r_3 + 2r_4$, $e_1 = r_1 + 2r_2 + 3r_3 + r_4$, $e_1 + e_3 = r_0 - r_1$, которые, как нетрудно проверить, являются $(-r_0)$-экстремальными, остальные удовлетворяют условию A2) при подходящем q из множества r_3, r_4, $r_2 + r_3$. Лемма доказана. □

Предложение 6. *Пусть автоморфизм φ удовлетворяет условию* (B). *Тогда с точностью до умножения φ на внутренний и центральный автоморфизмы, а также на автоморфизмы* (23)—(25) *можно считать, что $x_r^{\varphi}(1) = x_r(1)$ для всех $r \in \Phi^+$ и $x_{-r_0}^{\varphi}(p) = x_{-r_0}(p)h$, где $h \in H(J^{m-1})$.*

Доказательство. Из леммы 13 следует, что

$$x_{-r_0}^{\varphi}(p) = x_{-r_0}(p) \cdot h \cdot \prod_s x_s(\lambda_s), \quad h \in H(J^{m-1}, \quad \lambda_s \in J^{m-1},$$

где s пробегает множество $(-r_0)$-экстремальных корней, которые перечислены в лемме 14. Домножив φ на подходящие автоморфизмы вида (23), получим утверждение предложения для типов A_n, B_n и E_6, E_7, E_8. В оставшихся случаях можно считать, что

$$x_{-r_0}^{\varphi}(p) = x_{-r_0}(p) \cdot h \cdot x_{r_1 + \ldots + r_n}(\lambda_1) x_{-r_2 - \ldots - r_n}(\lambda_2),$$

если $\Phi = B_n$,

$$x_{-r_0}^{\varphi}(p) = x_{-r_0}(p) \cdot h \cdot x_{r_0 - 2r_1 - r_2}(\mu),$$

если $\Phi = C_n$, наконец,

$$x^{\varphi}_{-r_0}(p) = x_{-r_0}(p) \cdot h \cdot x_{r_1+2r_2+3r_3+2r_4}(\eta_1) x_{r_2+2r_3+r_4}(\eta_2) x_{-r_1-r_2-r_3}(\eta_3),$$

если $\Phi = F_4$.

Если $p > 2$, то из инвариантности соотношения $1 = [x_{-r_0}(p), x_{r_i}(1)]$, где $i = n$, если $\Phi = B_n$, $i = 2$, если $\Phi = C_n$, $i = 3, 4$, если $\Phi = F_4$, и обратимости всех констант $c_{ij,rs}$ в кольце $\mathbb{Z}_{p^m}$ следует, что все элементы λ_1, λ_2, μ и η_1, η_2, η_3 равны нулю. Значит, утверждение справедливо и для типов B_n, C_n, F_4, когда $p > 2$.

Пусть $p = 2$. Домножив φ на подходящие автоморфизмы вида (25), получим утверждение предложения для типа C_n, а когда $\Phi = F_4$, можно считать, что

$$x^{\varphi}_{-r_0}(p) = x_{-r_0}(p) \cdot h \cdot x_{r_1+2r_2+3r_3+2r_4}(\eta_1) x_{-r_1-r_2-r_3}(\eta_3).$$

Домножив φ слева на внутренний автоморфизм, индуцированный элементом $x_{e_1}(\lambda)$, где λ — корень уравнения $2x = \lambda_2$ ($2x = \eta_3$), когда $\Phi = B_n$ (соответственно $\Phi = F_4$), подходящий автоморфизм вида (24) и центральный автоморфизм вида

$$x_{-r_0}(u) \to x_{-r_0}(u) x_{e_1}(\theta u), \quad \theta \in J^{m-2},$$

получаем требуемое и в оставшихся случаях. Предложение доказано. □

6. Автоморфизмы, тождественные по модулю $\Phi(J^{m-1})$, IV

Пусть автоморфизм φ группы $S\Phi(\mathbb{Z}_{p^m})$ удовлетворяет условию

$$\begin{aligned} &x^{\varphi}_r(1) = x_r(1) \text{ для всех } r \in \Phi^+ \text{ и} \\ &x^{\varphi}_{-r_0}(p) = x_{-r_0}(p) h_{r_1}(1+\mu_1) \ldots h_{r_n}(1+\mu_n), \quad \mu_1, \ldots, \mu_n \in J^{m-1}. \end{aligned} \tag{Г}$$

Исследуем разложение автоморфизма φ в произведение элементарных автоморфизмов.

Пусть $r \in \Pi(\Phi)$ и $r_0 - r \notin \Phi$, тогда

$$1 = [x^{\varphi}_r(1), x^{\varphi}_{-r_0}(p)] = x_r((h_{r_1}, r)\mu_1 + \ldots + (h_{r_n}, r)\mu_n)$$

и, значит,

$$(h_{r_1}, r)\mu_1 + \ldots + (h_{r_n}, r)\mu_n = 0.$$

Заставив r пробегать все простые корни с условием $r_0 - r \notin \Phi$, получим систему уравнений на элементы μ_i, которая в зависимости от типа Φ состоит из следующих уравнений:

$$\begin{array}{lll} A_n & (n > 2): & 2\mu_i - \mu_{i-1} - \mu_{i+1} = 0,\ i = 2, \ldots, n-1; \\ B_n & (n > 2): & 2\mu_1 - \mu_2 = 2\mu_{n-1} - 2\mu_n - \mu_{n-2} = 2\mu_n - \mu_{n-1} = 0, \\ & & 2\mu_i - \mu_{i-1} - \mu_{i+1} = 0,\ i = 2, \ldots, n-2; \\ C_n & (n > 2): & 2\mu_n - 2\mu_{n-1} = 0,\ 2\mu_i - \mu_{i-1} - \mu_{i+1} = 0,\ i = 2, \ldots, n-1; \end{array}$$

$$
\begin{array}{ll}
D_n\quad (n>4)\colon & 2\mu_n-\mu_{n-2}=2\mu_{n-1}-\mu_{n-2}=2\mu_{n-2}-\mu_{n-3}-\mu_{n-1}-\mu_n=0,\\
 & 2\mu_1-\mu_2=0,\ 2\mu_i-\mu_{i-1}-\mu_{i+1}=0,\ i=2,\dots,n-3;\\
D_4\colon & 2\mu_1-\mu_2=2\mu_3-\mu_2=2\mu_4-\mu_2=0;\\
F_4\colon & 2\mu_2-\mu_1-2\mu_3=2\mu_3-\mu_2-\mu_4=2\mu_4-\mu_3=0;\\
E_8\colon & 2\mu_1-\mu_3=2\mu_3-\mu_1-\mu_4=2\mu_4-\mu_2-\mu_3-\mu_5=2\mu_2-\mu_4=0,\\
 & 2\mu_5-\mu_4-\mu_6=2\mu_6-\mu_5-\mu_7=2\mu_7-\mu_6-\mu_8=0;\\
E_7\colon & 2\mu_3-\mu_1-\mu_4=2\mu_4-\mu_2-\mu_3-\mu_5=2\mu_2-\mu_4=0,\\
 & 2\mu_5-\mu_4-\mu_6=2\mu_6-\mu_5-\mu_7=2\mu_7-\mu_6=0;\\
E_6\colon & 2\mu_1-\mu_3=2\mu_3-\mu_1-\mu_4=2\mu_4-\mu_2-\mu_3-\mu_5=0,\\
 & 2\mu_5-\mu_4-\mu_6=2\mu_6-\mu_5=0.
\end{array}
$$

Разрешая полученные системы, получим

$$
\begin{array}{ll}
A_n\colon & \mu_i=(i-1)\mu_2-(i-2)\mu_1,\ i=3,\dots,n;\\
B_n\colon & \mu_2=\dots=\mu_{n-1}=2\mu_n,\ 2\mu_1=2\mu_n;\\
C_n,\ p>2\colon & \mu_1=\dots=\mu_n;\\
C_n,\ p=2\colon & \mu_1=\mu_3=\dots,\ \mu_2=\mu_4=\dots;\\
D_n,\ n>3,\ p>2\colon & \mu_2=\mu_3=\dots=\mu_{n-2}=2\mu_1=2\mu_{n-1}=2\mu_n;\\
D_n,\ n=2k>4,\ p=2\colon & \mu_2=\mu_4=\dots=\mu_{n-2}=0,\\
 & \mu_3=\mu_5=\dots=\mu_{n-3}=\mu_{n-1}+\mu_n;\\
D_n,\ n=2k+1,\ p=2\colon & \mu_2=\mu_3=\dots=\mu_{n-2}=0,\ \mu_{n-1}=\mu_n;\\
D_4,\ p=2\colon & \mu_2=0;\\
F_4\colon & \mu_1=2\mu_4,\ \mu_2=3\mu_4,\ \mu_3=2\mu_4;\\
E_8,\ p>2\colon & \mu_2=\mu_7=3\mu_1/2,\ \mu_3=\mu_6=2\mu_1,\ \mu_4=3\mu_1,\\
 & \mu_5=5\mu_1/2,\ \mu_8=\mu_1;\\
E_8,\ p=2\colon & \mu_1=\mu_3=\mu_4=\mu_6=\mu_8=0,\ \mu_2=\mu_5=\mu_7;\\
E_7,\ p>2\colon & \mu_1=\mu_2=\mu_6=2\mu_7,\ \mu_3=\mu_5=3\mu_7,\ \mu_4=4\mu_7;\\
E_7,\ p=2\colon & \mu_1=\mu_4=\mu_6=0,\ \mu_5=\mu_7,\ \mu_3=\mu_2+\mu_7;\\
E_6,\ p\neq 3\colon & \mu_2=\mu_3=\mu_5=2\mu_1,\ \mu_4=3\mu_1,\ \mu_6=\mu_1;\\
E_6,\ p=3\colon & \mu_3=2\mu_1,\ \mu_5=2\mu_6,\ \mu_4=0,\ \mu_2=\mu_1-2\mu_6.
\end{array}
$$

Учитывая разложения кокорня h_{r_0}

$$
\begin{array}{ll}
A_n,\ C_n\ (n>2)\colon & h_{r_1}+\dots+h_{r_n};\\
B_n\qquad (n>2)\colon & h_{r_1}+2h_{r_2}+\dots+2h_{r_{n-1}}+h_{r_n};\\
D_n\qquad (n>4)\colon & h_{r_1}+2h_{r_2}+\dots+2h_{r_{n-2}}+h_{r_{n-1}}+h_{r_n};\\
F_4\colon & 2h_{r_1}+3h_{r_2}+2h_{r_3}+h_{r_4};\\
E_8\colon & 2h_{r_1}+3h_{r_2}+4h_{r_3}+6h_{r_4}+5h_{r_5}+4h_{r_6}+3h_{r_7}+2h_{r_8};
\end{array}
$$

E_7: $\qquad 2h_{r_1} + 2h_{r_2} + 3h_{r_3} + 4h_{r_4} + 3h_{r_5} + 2h_{r_6} + h_{r_7};$

E_6: $\qquad h_{r_1} + 2h_{r_2} + 2h_{r_3} + 3h_{r_4} + 2h_{r_5} + h_{r_6},$

получаем, что $h = h_{r_0}(1+\mu_1)$, когда Φ типа B_n, C_n, D_n, E_6 и $p > 2$, $h = h_{r_0}(1+\mu_4)$, если $\Phi = F_4$, $h = h_{r_0}(1+\mu_1/2)$, если $\Phi = E_8$ и $p > 2$, $h = h_{r_0}(1+\mu_2)$, если $\Phi = E_8$ и $p = 2$, $h = h_{r_0}(1+\mu_7)$, если $\Phi = E_7$ и $p > 2$. Домножая в этих случаях φ на внутренний автоморфизм, индуцированный элементом $x_{r_0}(\lambda)$, где λ — корень уравнения $px + \mu_1 = 0$ (соответственно $px + \mu_4 = 0$, $px + \mu_1/2 = 0$, $2x + \mu_2 = 0$, $px + \mu_7 = 0$), а затем на центральный автоморфизм
$$x_{-r_0}(u) \to x_{-r_0}(u)x_{r_0}(\lambda^2 u),$$
получим автоморфизм, тождественный на элементах $x_r(1)$, $r \in \Phi^+$, и $x_{-r_0}(p)$.

В оставшихся случаях элемент h допускает следующие разложения:

A_n: $\qquad h = h_{r_0}(1+\mu_1) \cdot \prod h_{r_i}(1+(i-1)(\mu_1+\mu_2));$

$B_n,\ p=2$: $\qquad h = h_{r_0}(1+\mu_1) \cdot h_{r_n}(1+\mu_1+\mu_n);$

$C_n,\ p=2$: $\qquad h = h_{r_0}(1+\mu_2) \cdot h_{r_1}(1+\mu_1+\mu_2)h_{r_3}(1+\mu_1+\mu_2)\ldots;$

$D_n,\ n=2k+1,\ p=2$: $\qquad h = h_{r_0}(1+\mu_1) \cdot h_{r_{n-1}}(1+\mu_1+\mu_n)h_{r_n}(1+\mu_1+\mu_n);$

$E_7,\ p=2$: $\qquad h = h_{r_0}(1+\mu_7) \cdot h_{r_2}(1+\mu_2)h_{r_3}(1+\mu_3);$

наконец,
$$h = h_{r_0}(1+\mu_1) \cdot h_{r_2}(1+(\mu_6-\mu_1))h_{r_5}(1-(\mu_6-\mu_1))h_{r_6}(1+(\mu_6-\mu_1)),$$
если $\Phi = E_6$ и $p = 2$, и
$$h = h_{r_0}(1+\mu+\mu_n)\cdot h_{r_{n-1}}(1+\mu)h_{r_n}(1+\mu)\cdot h_{r_1}(1+\mu_{n-1}+\mu_n)h_{r_3}(1+\mu_{n-1}+\mu_n)\ldots,$$
где $\mu = \mu_1 + \mu_{n-1}$, если $\Phi = D_n$, $n = 2k \geqslant 4$ и $p = 2$. Отсюда видно, что, домножив φ на внутренний автоморфизм, индуцированный элементом $x_{r_0}(\lambda)$ при подходящем λ, центральный автоморфизм и автоморфизмы вида (26)—(28), во всех случаях получим автоморфизм, тождественный на элементах $x_r(1)$, $r \in \Phi^+$, и $x_{-r_0}(p)$, в частности тождественный на всей группе $S\Phi(\mathbb{Z}_{p^m})$, если $\Phi \neq C_n$ или $\Phi \neq 2$.

Таким образом, во всех случаях, за исключением $\Phi = C_n$ и $p = 2$, нами доказано следующее утверждение.

Предложение 7. *Пусть автоморфизм φ удовлетворяет условию* (Г). *Тогда φ раскладывается в произведение внутреннего и центрального автоморфизмов и автоморфизмов вида* (26)—(30).

Доказательство. Пусть $\Phi = C_n$ и $p = 2$. В силу доказанного выше можно считать, что $x_r^{\varphi}(1) = x_r(1)$ для всех $r \in \Phi^+$ и $x_{-r_0}^{\varphi}(2) = x_{-r_0}(2)$. Кроме того, из леммы 13 следует, что
$$x_{r_1-r_0}^{\varphi}(2) = x_{r_1-r_0}(2) \cdot h \cdot \prod x_s(\lambda_s), \quad h \in H(J^{m-1}), \quad \lambda_s \in J^{m-1},$$
где s пробегает множество $(r_1 - r_0)$-экстремальных корней.

Лемма 15. *Корни r_0, $r_0 - r_1$, $r_0 - r_1 - r_2$, $r_0 - 2r_1 - 2r_2$, $r_0 - 2r_1 - 2r_2 - r_3$ и только они являются $(r_1 - r_0)$-экстремальными.*

Доказательство. Корни $r_1, \ldots, r_{n-1}, r_{n-1} + r_n$ являются базой подсистемы корней типа D_n, которую образуют короткие корни $\pm(e_i \pm e_j)$, $1 \leqslant i < j \leqslant n$. Корень $r_0 - r_1$ является максимальным в D_n. Поэтому по лемме 14 среди коротких корней $(r_1 - r_0)$-экстремальными могут быть только корни $r_0 - r_1$, $r_0 - r_1 - r_2$, $r_0 - 2r_1 - 2r_2 - r_3$ и r_1. Нетрудно видеть, что все перечисленные корни ни одному из условий A1)—A3) не удовлетворяет.

Рассмотрим длинные корни $\pm 2e_i$, $1 \leqslant i \leqslant n$. Корни $-2e_i$ при $i \geqslant 3$ удовлетворяют условию A1). Корни $-2e_i$, $i = 1, 2$, удовлетворяют условию A3). Чтобы убедиться в этом, достаточно выбрать $q = e_i + e_3$ и $s = e_1 + e_2$. Если $i \neq 1, 3$, то корни $2e_i$ удовлетворяют условию A2) при $q = r_{i-1}$. Лемма доказана. □

Таким образом, можно считать, что

$$x^{\varphi}_{r_1-r_0}(2) = \\ = x_{r_1-r_0}(2) \cdot h \cdot x_{r_0-r_1}(\lambda_1) x_{r_0-r_1-r_2}(\lambda_2) x_{r_0-2r_1-2r_2}(\lambda_3) x_{r_0-2r_1-2r_2-r_3}(\lambda_4).$$

Домножив φ на центральный автоморфизм вида

$$\left.\begin{array}{ll} x_{r_1-r_0}(u) \to x_{r_1-r_0}(u) x_{r_0-r_1}(\lambda u), & u \in J, \\ x_{2r_1-r_0}(u) \to x_{2r_1-r_0}(u) x_{r_0-r_1}(\lambda u), & \end{array}\right\}$$

где λ — корень уравнения $2x = \lambda_1$, и подходящие автоморфизмы вида (29) и (30), можно считать, что

$$x^{\varphi}_{r_1-r_0}(2) = x_{r_1-r_0}(2) \cdot h \cdot x_{r_0-2r_1-2r_2}(\lambda_3).$$

Из инвариантности соотношения

$$[x_{r_1-r_0}(2), x_{r_1+r_2}(N_{r_1-r_0, r_1+r_2})] = [x_{r_1-r_0}(2), x_{r_2}(N_{r_1-r_0, r_2}), x_{r_1}(N_{r_1+r_2-r_0, r_1})]$$

вытекает равенство

$$x_{2r_1+r_2-r_0}(2) x_{r_1+r_2}(\theta) x_{r_0-r_1-r_2}(\lambda_3) x_{r_0}(\lambda_3) = \\ = x_{2r_1+r_2-r_0}(2) x_{r_1+r_2}(\mu) x_{r_0-r_1-r_2}(\lambda_3) x_{r_0-r_1}(\lambda_3) x_{r_0}(\lambda_3),$$

и значит, $\lambda_3 = 0$.

Пусть $h = h_{r_1}(1+\mu_1) \ldots h_{r_n}(1+\mu_n)$. Из перестановочности элемента $x_{r_1-r_0}$ с элементами $x_{r_i}(1)$, когда $i = 3, \ldots, n-1$, вытекает, что $2\mu_i - \mu_{i-1} - \mu_{i+1} = 0$ для данных i. Кроме того,

$$x^{\varphi}_{r_1-r_0}(\pm 4) = [x^{\varphi}_{r_1-r_0}(2), x^{\varphi}_{r_1}(1)] = x_{2r_1-r_0}(\pm 4)[h, x_{r_1}(1)],$$

а с другой стороны, по лемме 12

$$x^{\varphi}_{r_1-r_0}(\pm 4) = x_{r_1-r_0}(\pm 4).$$

Поэтому $x_{r_1}(\mu_2) = [h, x_{r_1}(1)] = 1$. Отсюда и из полученных выше равенств на элементы μ_i следует, что все элементы μ_i с чётными индексами равны нулю и $\mu_3 = m_5 = \ldots$. Домножив φ на внутренний автоморфизм, индуцированный элементом $x_{r_0-r_1}(\mu)$, где μ — корень уравнения $2x = \mu_1 + \mu_3$, и центральные автоморфизмы вида $x_{r_1}(t) \to x_{r_1}(t)x_{r_0}(2t\mu)$ и

$$\left.\begin{array}{ll} x_{r_1-r_0}(u) \to x_{r_1-r_0}(u)h_{r_1}(1+\mu' u)h_{r_3}(1+\mu' u)\ldots, & u \in J, \\ x_{2r_1-r_0}(u) \to x_{2r_1-r_0}(u)h_{r_1}(1+\mu' u)h_{r_3}(1+\mu' u)\ldots, & \end{array}\right\}$$

где μ' — корень уравнения $2x = \mu_3$, получим автоморфизм, тождественный на указанных в предложении 1 порождающих группы $SC_n(\mathbb{Z}_{2^m})$, а значит, и на всей группе. Предложение доказано. □

Доказательство основной теоремы проведём индукцией по m. Автоморфизмы группы $S\Phi(\mathbb{Z}_p) = U\Phi^+(\mathbb{Z}_p)$ описаны в [8, 9], и для них справедливо указанное разложение.

Пусть φ — произвольный автоморфизм группы $S\Phi(\mathbb{Z}_{p^m})$ и $m > 1$. Ввиду изоморфизма

$$S\Phi(\mathbb{Z}_{p^m})/\Phi(J^{m-1}) \simeq S\Phi(\mathbb{Z}_{p^{m-1}})$$

и характеристичности подгруппы $\Phi(J^{m-1})$ φ индуцирует автоморфизм $\bar{\varphi}$ группы $S\Phi(\mathbb{Z}_{p^{m-1}})$. В силу индуктивного предположения $\bar{\varphi}$ раскладывается в произведение внутреннего $i_{\bar{g}}$, $\bar{g} \in S\Phi(\mathbb{Z}_{p^{m-1}})$, диагонального $d_{\bar{\chi}}$, $\bar{\chi} \in \mathrm{Hom}(\Phi, \mathbb{Z}^{\#}_{p^{m-1}})$, графового Γ_Φ автоморфизмов и автоморфизмов вида (7)—(30). Обозначим через ζ естественный гомоморфизм кольца $\mathbb{Z}_{p^m}$ на кольцо $\mathbb{Z}_{p^{m-1}}$, через g — прообраз элемента $\bar{g}$ относительно гомоморфизма групп $S\Phi(\mathbb{Z}_{p^m})$ и $S\Phi(\mathbb{Z}_{p^{m-1}})$, индуцированного ζ, наконец, через χ — тот гомоморфизм из $\mathrm{Hom}(\Phi, \mathbb{Z}^{\#}_{p^m})$, для которого $\zeta(\chi(r)) = \bar{\chi}(r)$, и положим $\varphi' = \Gamma_\Phi^{-1} d_\chi^{-1} i_g^{-1}\varphi$. Автоморфизм $\bar{\varphi}'$ индуцирует автоморфизм $\bar{\varphi}'$, который является произведением центрального автоморфизма и автоморфизмов вида (7)—(30). Нетрудно проверить, что автоморфизм $\bar{\varphi}'$ на самом деле тождественный. Следовательно, автоморфизм φ' является тождественным по модулю конгруэнц-подгруппы $\Phi(J^{m-1})$. Применяя последовательно предложения 3—6, получаем утверждение теоремы. □

Литература

[1] Бурбаки Н. Группы и алгебры Ли. Главы IV-VI. — М.: Мир, 1972.

[2] Вапнэ Ю. Е. Центральные ряды и ряды коммутантов некоторых матричных групп // Сиб. мат. журн. — 1971. — Т. 12, № 3. — С. 497—504.

[3] Колесников С. Г. Коммутаторное строение и автоморфизмы обобщённых конгруэнц-подгрупп: Дис.... канд. физ.-мат. наук. — Красноярск, 1997.

[4] Колесников С. Г. Нижние центральные ряды силовских 2-подгрупп симплектической и ортогональной групп над кольцом $\mathbb{Z}_{2^m}$ // Алгебра и логика. — 1998. — Т. 37, № 4. — С. 413—431.

[5] Колесников С. Г. Автоморфизмы силовских p-подгрупп групп Шевалле, определённых над кольцами вычетов целых чисел // Алгебра и логика. — 2004. — Т. 43, № 1. — С. 32—59.

[6] Колесников С. Г. Автоморфизмы силовских p-подгрупп групп Шевалле малых рангов над кольцом $\mathbb{Z}_{p^m}$ // Изв. Гомельского ун-та. — 2006. — Т. 36, № 3. — С. 137—146.

[7] Коуровская тетрадь. — 15-е изд. — Новосибирск, 2002.

[8] Левчук В. М. Автоморфизмы унипотентных подгрупп групп лиева типа малых рангов // Алгебра и логика. — 1990. — Т. 29, № 2. — С. 141—161.

[9] Левчук В. М. Автоморфизмы унипотентных подгрупп групп Шевалле // Алгебра и логика. — 1990. — Т. 29, № 3. — С. 315—338.

[10] Левчук В. М. Коммутаторное строение некоторых подгрупп групп Шевалле // Укр. мат. журн. — 1992. — Т. 44, № 6. — С. 786—795.

[11] Холл М. Теория групп. — М.: ИЛ, 1962.

[12] Carter R. Simple groups of Lie type. — New York: Wiley, 1972.

[13] Gibbs J. A. Automorphisms of certain unipotent groups // J. Algebra. — 1970. — Vol. 14, no. 2. — P. 203—228.