РОССИЙСКАЯ АКАДЕМИЯ НАУК
УРАЛЬСКОЕ ОТДЕЛЕНИЕ

ТРУДЫ ИНСТИТУТА МАТЕМАТИКИ И МЕХАНИКИ

Том 13, № 1 2007

ТРУДЫ
ИНСТИТУТА МАТЕМАТИКИ И МЕХАНИКИ УрО РАН

Том 13
№ 1

ГРУППЫ И ГРАФЫ

СБОРНИК НАУЧНЫХ ТРУДОВ

Екатеринбург
2007

Труды Института математики и механики УрО РАН. Том 13, № 1. Группы и графы: Сб. науч. трудов. Екатеринбург: УрО РАН, 2007. 198 с.
ISBN 5–7691–1843–1.

Настоящий выпуск представляет собой сборник трудов международной школы-конференции по теории групп, посвященной 75-летию со дня рождения Альберта Ивановича Старостина (Нальчик, 10-14 июля 2006 г.). Сборник предназначен для научных работников, аспирантов и студентов, специализирующихся в алгебре и комбинаторике.

ISBN 5–7691–1843–1

Т $\dfrac{63(07)}{8П6(03) - 1998}$ ПВ–2007

СОДЕРЖАНИЕ

Том 13 № 1 2007

УДК 512.54

О ДВОЙНЫХ ГРУППАХ ФРОБЕНИУСА

В. А. Антонов, С. Г. Чеканов

Изучаются двойные группы Фробениуса. Получены некоторые свойства минимального контрпримера к гипотезе В.Д. Мазурова об этих группах. При некоторых дополнительных ограничениях гипотеза подтверждена.

Пусть p, q и r — различные простые числа. Группу $G = P \leftthreetimes (\langle x\rangle \leftthreetimes \langle y\rangle)$, в которой P является p-группой, $|x| = q$, $|y| = r$, и каждая из подгрупп $P \leftthreetimes \langle x\rangle$ и $\langle x\rangle \leftthreetimes \langle y\rangle$ является группой Фробениуса, назовем *двойной группой Фробениуса типа* (p, q, r). В дальнейшем если G — двойная группа Фробениуса типа (p, q, r), то через P, $\langle x\rangle$ и $\langle y\rangle$ условимся обозначать силовские p-, q- и r-подгруппы группы G соответственно.

В.Д. Мазуров выдвинул следующую гипотезу.

Гипотеза. *Если в двойной группе Фробениуса типа (p, q, r) подгруппа $C_P(y)$ имеет экспоненту p, то и подгруппа P имеет экспоненту p.*

В связи с задачей описания конечных простых групп с таким же множеством порядков элементов, как у двойной группы Фробениуса, представляет интерес случай, когда $p = 3$, $q = 5$ и $r = 2$.

В предлагаемой работе изучаются двойные группы Фробениуса типа $(p, q, 2)$. Получен ряд общих свойств таких групп, установлены некоторые свойства минимального контрпримера к гипотезе В.Д. Мазурова, при некоторых дополнительных ограничениях (в частности, для групп типа $(3, 5, 2)$) эта гипотеза подтверждена.

В дальнейшем будут использоваться следующие известные результаты.

Предложение 1 ([1, следствия 0.4 и 0.5]). *Если на π-группе P действует π'-группа автоморфизмов H, то $P = [P, H] \cdot C_P(H)$. Если при этом группа P абелева, то $P = [P, H] \times C_P(H)$.*

Предложение 2 ([2, теорема 5.8.15]). *Если p_1 и p_2 — простые числа, то любая подгруппа порядка p_1p_2 из дополнительного множителя группы Фробениуса является циклической группой.*

Из предложения 2 следует, в частности, что двойная группа Фробениуса типа (p, q, r) не может быть группой Фробениуса и, следовательно, $C_P(y) \neq 1$.

Предложение 3 ([2, теорема 3.6.6]). *Если группа P имеет экспоненту 3 и порождается n элементами, то $|P| \le 3^k$, где $k = n + \binom{n}{2} + \binom{n}{3}$.*

Непосредственным следствием предложения 1 является следующая лемма.

Лемма 1. *Если на π-группе P действует π'-группа автоморфизмов H, то для любого элемента $h \in H$ и любой инвариантной в группе $P \leftthreetimes H$ подгруппы B из P выполняется равенство*

$$C_{P/B}(h) = (C_P(h) \cdot B)/B.$$

Д о к а з а т е л ь с т в о. Пусть $A/B = C_{P/B}(h)$. Тогда $[A,h] \le B$ и из равенства $A = [A,h] \cdot C_A(h)$ следует, что $A = B \cdot C_P(h)$. Лемма доказана.

Заметим еще, что если A — инвариантная подгруппа двойной группы Фробениуса типа (p,q,r) и $P > A > 1$, то каждая из групп $A \leftthreetimes (\langle x \rangle \leftthreetimes \langle y \rangle)$ и G/A также является двойной группой Фробениуса типа (p,q,r) (см. предложение 1). Поэтому при изучении двойных групп Фробениуса с условием $\exp(C_P(y)) = p$ можно применять метод математической индукции.

Некоторым уточнением предложения 1 для случая $|H| = 2$ является следующий известный результат [2, гл. 1, § 4, упр. 14]. Поскольку в [2] дается лишь указание к упражнению 14, мы приводим для полноты изложения свое доказательство, основанное на другой идее.

Лемма 2. *Пусть p — нечетное простое число и P — конечная p-группа, на которой действует группа $\langle y \rangle$ порядка 2. Тогда для любого элемента $a \in P$ существуют единственные элементы $a_1,\ a_2$ из P такие, что $a = a_1 \cdot a_2$, $a_1^y = a_1$ и $a_2^y = a_2^{-1}$.*

Д о к а з а т е л ь с т в о. Если группа P абелева, то $P = [P,y] \times C_P(y)$ и утверждение теоремы очевидно. В общем случае проведем индукцию по ступени нильпотентности группы P.

Пусть $a \in P$ и $Z = Z(P)$. В силу предположения индукции $aZ = a_1Z \cdot a_2Z$, где $a_1,\ a_2 \in P$, $(a_1Z)^y = a_1Z$ и $(a_2Z)^y = a_2^{-1}Z$. Поэтому $a = a_1a_2z$ для некоторого $z \in Z$. Так как подгруппа $\langle a_1, Z \rangle$ абелева, то $a_1 = c_1d_1$, где $c_1,\ d_1 \in \langle a_1, Z \rangle$, $c_1^y = c_1$ и $d_1^y = d_1^{-1}$. Если $a_1^y = a_1z_1$, где $z_1 \in Z$, то из $c_1d_1^{-1} = (c_1d_1)^y = c_1d_1z_1$ следует, что $d_1^{-2} = z_1$, т.е. $d_1 \in Z$. Подгруппа $\langle a_2, Z \rangle$ также абелева и снова $a_2 = c_2d_2$, где $c_2,\ d_2 \in \langle a_2, Z \rangle$, $c_2^y = c_2$ и $d_2^y = d_2^{-1}$. Покажем, что $c_2 \in Z$. В самом деле, так как $c_2, d_2 \in \langle a_2, Z \rangle$ и

$$c_2d_2^{-1} = a_2^y = (a_2)^{-1}z_2 = d_2^{-1}c_2^{-1}z_2$$

для некоторого $z_2 \in Z$, то $c_2^2 = z_2 \in Z$, т.е. $c_2 \in Z$. Так как $a = a_1a_2z$ для некоторого $z \in Z$, то $a = c_1d_1c_2d_2z$. Так как $z = z_1z_2$, где $z_1,\ z_2 \in Z$, $z_1^y = z_1$ и $z_2^y = z_2^{-1}$, то $a = (c_1c_2z_1)(d_1d_2z_2)$ — искомое представление.

Докажем теперь единственность такого представления. Пусть $a_1a_2 = b_1b_2$, где $b_1,\ b_2 \in P$, $b_1^y = b_1$ и $b_2^y = b_2^{-1}$. Тогда

$$b_2a_2^{-1} = b_1^{-1}a_1 = (b_1^{-1}a_1)^y = (b_2a_2^{-1})^y = b_2^{-1}a_2.$$

Отсюда $b_2^2 = a_2^2$. Так как $\langle a_2 \rangle = \langle a_2^2 \rangle$, то $[a_2, b_2] = 1$. Это означает, что $(b_2a_2^{-1})^2 = b_1^2a_2^{-2} = 1$, т.е. $b_2 = a_2$. Но тогда и $b_1 = a_1$. Лемма доказана.

Лемма 3. *В двойной группе Фробениуса типа $(p,q,2)$ любая минимальная инвариантная в группе G подгруппа из P является минимальной x-допустимой подгруппой.*

Д о к а з а т е л ь с т в о. Обозначим через n показатель числа p по модулю q. И пусть A — минимальная инвариантная подгруппа группы G, а B — минимальная x-допустимая подгруппа из A. Если $B < A$, то $A = B \times B^y$. Выберем в группе B базис $\{a_1, a_2, \ldots, a_n\}$ так, что $a_{i+1} = a_i^x$ для $i = 1, 2, \ldots, n-1$, а в группе B^y базис $\{b_1, b_2, \ldots, b_n\}$ так, что $a_1^y = b_1$ и $b_{i+1} = b_i^x$ для $i = 1, 2, \ldots, n-1$. Если $f(t) = t^n + \alpha_1t^{n-1} + \alpha_2t^{n-2} + \cdots + \alpha_{n-1}x + \alpha_n$ и $g(t) = t^n + \beta_1t^{n-1} + \beta_2t^{n-2} + \cdots + \beta_{n-1}x + \beta_n$ — минимальные многочлены оператора x пространств B и B^y в выбранных базисах, то $a_n^x = a_1^{x^n} = a_1^{-\alpha_1x^{n-1} - \alpha_2x^{n-2} - \ldots - \alpha_{n-1}x - \alpha_n}$ и $b_n^x = b_1^{x^n} = b_1^{-\beta_1x^{n-1} - \beta_2x^{n-2} - \ldots - \beta_{n-1}x - \beta_n}$.

Из теоремы 2.7.3 из [2] следует, что число n четно. Пусть $n = 2k$. Тогда из $p^{2k} \equiv 1(q)$ получаем, что $p^k \equiv -1(q)$. Так как множество корней многочлена $f(t)$ совпадает с множеством $\{x^{p^i} | i \in Z\}$, то x^{-1} является корнем $f(x)$. Отметим, что

$$a_{i+1}^y = a_1^{x^iy} = a_1^{yx^{-i}} = b_1^{x^{-i}}.$$

Аналогично, $b_{i+1}^y = a_1^{x^{-i}}$.

Так как

$$b_1^{x^{-n}} = b_1^{-\beta_1 x^{1-n} - \beta_2 x^{2-n} - \ldots - \beta_{n-1} x^{-1} - \beta_n} = a_n^{yx^{-1}} = a_n^{xy}$$
$$= (a_1^{-\alpha_1 x^{n-1} - \alpha_2 x^{n-2} - \ldots - \alpha_{n-1} x - \alpha_n})^y = a_1^{y(-\alpha_1 x^{1-n} - \alpha_2 x^{2-n} - \ldots - \alpha_{n-1} x^{-1} - \alpha_n)}$$
$$= b_1^{-\alpha_1 x^{1-n} - \alpha_2 x^{2-n} - \ldots - \alpha_{n-1} x^{-1} - \alpha_n},$$

то $f(t) = g(t)$. Но тогда подгруппа $B_0 = \langle a_1 b_1 \rangle \times \langle a_2 b_2 \rangle \times \ldots \times \langle a_n b_n \rangle$ x-допустима, и из

$$(a_i b_i)^y = (a_1 b_1)^{x^{1-i}} = (a_1 b_1)^{x^{(i-1)p^k}} \in B_0$$

следует, что $B_0 \lhd G$, что противоречит минимальности A. Лемма доказана.

Лемма 4. *Пусть G — двойная группа Фробениуса типа $(p, q, 2)$. Тогда $|C_P(y)| = \sqrt{|P|}$.*

Доказательство. Предположим сначала, что P является минимальной нормальной подгруппой группы G. Пусть $a \in C_P(y) \setminus \{1\}$. Из леммы 3 следует, что $P = \prod\limits_{k=0}^{n-1} \langle a^{x^k} \rangle$, где n — показатель числа p по модулю q. Заметим, что

$$(a^{x^k} \cdot a^{x^{-k}})^y = a^{x^k y} \cdot a^{x^{-k} y} = a^{yx^{-k}} \cdot a^{yx^k} = a^{x^{-k}} \cdot a^{x^k} = a^{x^k} \cdot a^{x^{-k}},$$

т.е. $a^{x^k} \cdot a^{x^{-k}} \in C(y)$ для любого числа k.

Так как элемент x индуцирует автоморфизм абелевой группы P, то можно считать, что $x \in \mathrm{End}(P)$. Если $a^{x^k} \cdot a^{x^{-k}} \in \langle a^{x^i} \cdot a^{x^{-i}} | i = 0, 1, \ldots, k-1 \rangle$, то в кольце эндоморфизмов группы P для некоторых чисел α_i выполняется равенство

$$x^k + x^{-k} = \sum_{i=0}^{k-1} \alpha_i (x^i + x^{-i}).$$

Так как $\exp(P) = p$, то $p\varphi = 0$ для любого автоморфизма φ группы P. Поэтому можно считать, что $\alpha_i \in GF(p)$ для всех i. Умножая полученное выше равенство на x^k, получаем, что x является корнем многочлена степени $2k$. Поэтому $2k \geq n$. Если число n четно, $n = 2m$, то $k \geq m$. Но тогда элементы $a, (a^x \cdot a^{-x}), \ldots, (a^{x^{m-1}} \cdot a^{x^{1-m}})$ независимы. Поэтому $|C_P(y)| \geq p^m = \sqrt{|P|}$. Если же $n = 2m + 1$, то из $2k \geq n$ следует, что $k \geq m + 1$ и $|C_P(y)| \geq p^{m+1}$. В любом случае $|C_P(y)| \geq \sqrt{|P|}$. Так как элементы y и xy сопряжены, то $|C_P(y)| = |C_P(xy)|$, и из $C_P(y) \cap C_P(xy) \leq C_P(x) = 1$ следует, что

$$|P| \geq |C_P(y) \times C_P(xy)| = |C_P(y)|^2.$$

Поэтому число n четно и $|C_P(y)| = \sqrt{|P|}$.

В общем случае проведем индукцию по порядку P. Пусть A — минимальная инвариантная подгруппа группы G. По уже доказанному $|C_A(y)| = \sqrt{|A|}$. Кроме того, в силу предположения индукции $|C_{P/A}(y)| = \sqrt{|P/A|}$. Так как $C_{P/A}(y) = (C_P(y) \cdot A)/A$, то

$$\sqrt{|P/A|} = |(C_P(y) \cdot A)/A| = |C_P(y)/C_A(y)| = \frac{|C_P(y)|}{|C_A(y)|}$$

и

$$|C_P(y)| = \sqrt{|P/A|} \cdot |C_A(y)| = \sqrt{|P/A|} \cdot \sqrt{|A|} = \sqrt{|P|}.$$

Лемма 4 доказана.

Замечание. Пусть $M = \{a \in P \,|\, a^y = a^{-1}\}$ и $N = \{[a, y] \,|\, a \in P\}$. Из лемм 2 и 4 следует, что $|M| = \sqrt{|P|}$. Если $a = a_1 a_2$, где $a_1^y = a_1$ и $a_2^y = a_2^{-1}$, то $[a, y] = [a_2, y]$, и из $|M| = \sqrt{|P|}$ следует, что и $|N| = \sqrt{|P|}$.

Теорема 1. *Если в двойной группе Фробениуса типа $(p,q,2)$ нижний слой группы P, т.е. подгруппа $\Omega(P) = \langle a \in P \mid a^p = 1\rangle$, и подгруппа $C_P(y)$ имеют экспоненту p, то $\exp(P) = p$.*

Доказательство. Предположим, что $\Omega(P) < P$. Так как $C_P(y) \leq \Omega(P)$, то в силу леммы 1 элемент y действует на фактор-группе $P/\Omega(P)$ без неподвижных точек, что противоречит замечанию, сделанному после предложения 2. Теорема доказана.

Следствие 1. *Если в двойной группе Фробениуса типа $(p,q,2)$ подгруппа P регулярна (в частности, если ее ступень нильпотентности меньше p) и $C_P(y)$ имеет экспоненту p, то $\exp(P) = p$.*

Доказательство следует из того, что p-группа ступени нильпотентности, меньшей p, регулярна [2, теорема 3.10.2], а в силу [2, лемма 3.10.5] в регулярной p-группе P выполняется равенство

$$\Omega(P) = \{a \in P \mid a^p = 1\}.$$

Как уже отмечалось, утверждение леммы 1 позволяет проводить индукцию по порядку P. Отметим следующие свойства минимального контрпримера к гипотезе Мазурова.

Лемма 5. *Пусть $G = P \leftthreetimes (\langle x\rangle \leftthreetimes \langle y\rangle)$ — минимальный контрпример к гипотезе Мазурова и n — показатель p по модулю q. Тогда*

1) *ступень нильпотентности группы P не меньше p;*

2) *$Z(P)$ является единственной минимальной инвариантной подгруппой группы G, и $|Z(P)| = p^n$;*

3) *P имеет экспоненту p^2 и $\Phi(P) = P'$ — группа экспоненты p;*

4) *P порождается как элементами порядка p^2, так и элементами порядка p и представима в виде произведения двух подгрупп экспоненты p;*

5) *$|P : P'| \in \{p^n, p^{2n}\}$.*

Доказательство. Пусть G — минимальный контрпример к гипотезе Мазурова. Тогда группа P нерегулярна и, следовательно, ее ступень нильпотентности не меньше p. В силу следствия из теоремы 1, $\exp(Z(P)) = p$. Обозначим через Z произвольную неединичную инвариантную в группе G подгруппу из $Z(P)$. Так как $C_{P/Z}(y) = C(y) \cdot Z/Z$ имеет экспоненту p, то в силу предположения индукции $\exp(P/Z) = p$. Если $Z(P)$ содержит две минимальные инвариантные в G подгруппы, то по теореме Ремака [2, лемма 1.9.6] $\mathrm{Exp}(P) = p$. Поэтому такая подгруппа только одна. Если Z — эта подгруппа, то в силу теоремы Машке [2, теорема 1.17.7] будем иметь $Z(P) = Z \times Z_0$, где $Z_0 \lhd G$. Но тогда $Z = Z(P)$, т.е. $Z(P)$ является единственной минимальной инвариантной подгруппой группы G. В силу леммы 3 $|Z(P)| = p^n$, где n — показатель числа p по модулю q.

В силу предположения индукции можно считать, что любая инвариантная в группе G собственная подгруппа группы P имеет экспоненту p. В частности, экспоненту p имеет подгруппа Фраттини $\Phi(G)$ группы P. Так как $P/Z(P)$ имеет экспоненту p, то $\mho(P) = \langle a^p \mid a \in P\rangle \leq Z(P)$, и в силу минимальности $Z(P)$ получаем, что $\mho(P) = Z(P)$. Это означает, что $\exp(P) = p^2$. Кроме того, из минимальности $Z(P)$ следует, что $Z(P) \leq P'$. Поэтому $\Phi(P) = P' \cdot \mho(P) = P'$.

Так как подгруппа, порожденная элементами порядка p^2, инвариантна в G, то P порождается элементами порядка p^2. Отметим еще, что из включения $P' \cdot C_P(y) \leq \Omega(P)$ и леммы 1 следует, что элемент y действует на $P/\Omega(P)$ без неподвижных точек. Но тогда $P = \Omega(P)$, т.е. P порождается и элементами простого порядка. Более того, так как по лемме 4 имеем $|C_P(y)| = \sqrt{|P|} = |C_P(xy)|$ и $C_P(y) \cap C_P(xy) = \{1\}$, то $P = C_P(y) \cdot C_P(xy)$, т.е. P представима в виде произведения двух подгрупп экспоненты p.

Пусть a — элемент порядка p^2. По лемме 3 имеем $A/P' = \prod\limits_{i=1}^{n} \langle a^{x^{i-1}} P'\rangle$, где n — показатель p по модулю q. Если $A \neq P$, то A не y-допустима. Но тогда $A \cdot A^y = P$. Поэтому индекс $|P : P'|$ равен либо p^n, либо p^{2n}. Лемма 5 доказана.

Рассмотрим теперь случай, когда $p = 3$ и $q = 5$.

Теорема 2. *Пусть G — двойная группа Фробениуса типа $(3,5,2)$. Если $|P| = 3^{12}$ и $C_P(y)$ имеет экспоненту 3, то P нильпотентна ступени не выше двух.*

Доказательство. Предположим противное. Тогда ступень P равна 3 и в силу леммы 3 все факторы центрального ряда $P > P' > Z = Z(P) > 1$ являются элементарными абелевыми группами порядка 3^4. В силу следствия из теоремы 1 подгруппа P' тоже является элементарной абелевой группой. Выберем в группах P/P', P'/Z и Z циклические относительно x базисы. Это означает, что

$$P/P' = \prod_{i=1}^{4}\langle a_iP'\rangle, \qquad P'/Z = \prod_{i=1}^{4}\langle c_iZ\rangle, \qquad Z(P) = \prod_{i=1}^{4}\langle z_i\rangle,$$

где $(a_iP')^x = a_{i+1}P'$, $(c_iZ)^x = c_{i+1}Z$ и $z_i^x = z_{i+1}$ для $i = 1,2,3$. Так как $x^5 = 1$, то, отождествляя элемент x с соответствующим элементом из $\mathrm{End}(H)$, где $H \in \{P/P', P'/Z, Z(P)\}$, получим $x^4 = -x^3 - x^2 - x - 1$. Поэтому действие элемента x на каждой из этих групп определяется матрицей

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

Из п. 4 леммы 5 следует, что можно считать все a_i элементами порядка 3.

Так как $P/P' = \prod\limits_{i=1}^{4}\langle (aP')^{x^{i-1}}\rangle$ для любого неединичного элемента $aP' \in P/P'$, то будем считать, что $a_1 \in C_P(y)$. Тогда

$$(a_2P')^y = (a_1P')^{xy} = (a_1P')^{yx^{-1}} = (a_1P')^{x^{-1}} = a_1^{-1}a_2^{-1}a_3^{-1}a_4^{-1}P'.$$

Аналогично получаем, что $(a_3P')^y = a_4P'$ и $(a_4P')^y = a_3P'$, т.е. действие элемента y на P/P' задается матрицей

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

Тогда $C_{P/P'}(y) = \langle a_1P'\rangle \times \langle a_3a_4P'\rangle$. В силу леммы 1 можно считать, что элементы a_1 и a_3a_4 лежат в $C(y)$ и, следовательно, каждый из элементов a_3a_4, $a_1a_3a_4$ и $a_1^{-1}a_3a_4$ имеет порядок 3. (На самом деле в $C(y)$ лежит элемент a_3a_4c для некоторого $c \in P'$. Но так как в дальнейшем нас будут интересовать только тройные коммутаторы, то множителем c можно пренебречь.)

Заметим, что если a и b — элементы порядка 3 из P, то

$$(ab)^3 = a^3b^3[b,a]^3[b,a,b]^2[b,a,a] = [b,a,b]^{-1}[b,a,a].$$

Это означает, что $(ab)^3 = 1$ тогда и только тогда, когда $[b,a,b] = [b,a,a]$.

Из равенств $[a_1, a_3a_4, a_1] = [a_1, a_3a_4, a_3a_4]$ и $[a_1^{-1}, a_3a_4, a_1^{-1}] = [a_1^{-1}, a_3a_4, a_3a_4]$ следует, что $[a_1, a_3a_4, a_1] = [a_1, a_3a_4, a_3a_4] = 1$. Кроме того, из $|a_3a_4| = 3$ получим $[a_3, a_4, a_3] = [a_3, a_4, a_4]$, т.е. $[a_3, a_4, a_3a_4^{-1}] = 1$.

Для удобства перейдем в группах P/P', $P'/Z(P)$ и $Z(P)$ к аддитивной форме записи. Кроме того, положим $\overline{a} = aZ(P)$ для любого элемента $a \in P$.

Если $[\overline{a}_i, \overline{a}_j] = \sum\limits_{k=1}^{4} t_{ijk}\overline{c}_k$, то $T_k = (t_{ijk})$ — антисимметрическая матрица порядка 4 над полем $GF(3)$. Для любых $a, b \in P$ выполняется равенство

$$[\overline{a}, \overline{b}] = \sum_{k=1}^{n} \left([a]'T_k[b]\right)\overline{c}_k,$$

где через $[a]$ и $[b]$ обозначены столбцы координат элементов aP' и bP' в базисе $\{a_iP' | i = 1,2,3,4\}$, а штрих означает транспонирование. Действуя на a и b элементом x, получим

$$[\overline{a}^x, \overline{b}^x] = \sum_{k=1}^{4}([a]'X'T_kX[b])\overline{c}_k.$$

Однако

$$[\overline{a}^x, \overline{b}^x] = [\overline{a}, \overline{b}]^x = \left(\sum_{k=1}^{n}[a]'T_k[b] \cdot \overline{c}_k\right)^x.$$

Так как для любого $\overline{c} \in P'/Z(P)$ выполняется равенство $[c^x] = X \cdot [c]$, где через $[c]$ обозначается столбец координат вектора $\overline{c}$ в базисе $\{c_iZ | i = 1,2,3,4\}$, то, приравнивая коэффициенты при $\overline{c}_k$ в полученных выше равенствах и учитывая произвольность элементов a и b, получаем

$$(X'T_1X,\ X'T_2X,\ X'T_3X,\ X'T_4X) = (T_1,\ T_2,\ T_3,\ T_4) \cdot X'$$

$$= (-T_4,\ T_1 - T_4,\ T_2 - T_4,\ T_3 - T_4).$$

Отсюда

$$T_4 = -X'T_1X, \quad T_3 = X'T_4X + T_4, \quad T_2 = X'T_3X + T_4 \qquad (*)$$

и

$$T_1 + X'T_1X + (X')^2T_1X^2 + (X')^3T_1X^3 + (X')^4T_1X^4 = 0.$$

Обозначим через L аддитивную группу антисимметрических матриц порядка 4 над полем $GF(3)$. Действие элемента x на L зададим равенством $T^x = X'TX$ для любой матрицы T из L. Так как $|L| = 3^6$, то из равенства $L = [L,x] \oplus C_L(x)$ (см. предложение 1) следует, что $|C_L(x)| = 3^2$ и $|[L,x]| = 3^4$. Поэтому, если T — произвольная ненулевая матрица из $[L,x]$, то

$$[L,x] = \langle T\rangle \oplus \langle T^x\rangle \oplus \langle T^{x^2}\rangle \oplus \langle T^{x^3}\rangle.$$

В качестве матрицы T_1 в предыдущих рассуждениях может выступать любая ненулевая матрица из $[L,x]$. Предположим для определенности, что

$$T = \begin{pmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \qquad \text{Тогда} \qquad T^x = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 1 \\ 0 & 1 & 0 & -1 \\ -1 & -1 & 1 & 0 \end{pmatrix},$$

$$T^{x^2} = \begin{pmatrix} 0 & -1 & 1 & 0 \\ 1 & 0 & -1 & 0 \\ -1 & 1 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{pmatrix} \qquad \text{и} \qquad T^{x^3} = \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 1 & -1 \\ 0 & -1 & 0 & 1 \\ 0 & 1 & -1 & 0 \end{pmatrix}.$$

Поэтому

$$T_1 = k_1T + k_2T^x + k_3T^{x^2} + k_4T^{x^3}$$

$$= \begin{pmatrix} 0 & k_1 - k_3 - k_4 & k_3 & k_2 \\ -k_1 + k_3 + k_4 & 0 & -k_2 - k_3 + k_4 & k_2 - k_4 \\ -k_3 & k_2 + k_3 - k_4 & 0 & -k_1 - k_2 + k_3 + k_4 \\ -k_2 & -k_2 + k_4 & k_1 + k_2 - k_3 - k_4 & 0 \end{pmatrix}.$$

Отсюда по формулам (*) последовательно получаем

$$T_4 = \begin{pmatrix} 0 & k_2+k_3-k_4 & -k_2+k_4 & -k_1+k_4 \\ -k_2-k_3+k_4 & 0 & k_1+k_2-k_3-k_4 & -k_1+k_3 \\ k_2-k_4 & -k_1-k_2+k_3+k_4 & 0 & k_1-k_2-k_3 \\ k_1-k_4 & k_1-k_3 & -k_1+k_2+k_3 & 0 \end{pmatrix},$$

$$T_3 = \begin{pmatrix} 0 & k_1-k_2+k_4 & -k_1-k_2+k_3+k_4 & -k_1+k_3+k_4 \\ -k_1+k_2-k_4 & 0 & -k_1+k_3-k_4 & -k_1+k_2+k_3 \\ k_1+k_2-k_3-k_4 & k_1-k_3+k_4 & 0 & k_2-k_3+k_4 \\ k_1-k_3-k_4 & k_1-k_2-k_3 & -k_2+k_3-k_4 & 0 \end{pmatrix},$$

$$T_2 = \begin{pmatrix} 0 & -k_1+k_2-k_3+k_4 & -k_1+k_3+k_4 & -k_1+k_2+k_3 \\ k_1-k_2+k_3-k_4 & 0 & k_1-k_2+k_3 & k_2+k_3-k_4 \\ k_1-k_3-k_4 & -k_1+k_2-k_3 & 0 & -k_1+k_2-k_4 \\ k_1-k_2-k_3 & -k_2-k_3+k_4 & k_1-k_2+k_4 & 0 \end{pmatrix}.$$

Поэтому в аддитивной форме записи

$[\overline{a}_1, \overline{a}_3\overline{a}_4] = (k_2+k_3)\overline{c}_1 + (k_1+k_2-k_3+k_4)\overline{c}_2 + (k_1-k_2-k_3-k_4)\overline{c}_3 + (-k_1-k_2-k_4)\overline{c}_4$, и

$[a_1, [a_1, a_3a_4]] = (k_2+k_3)[a_1, c_1] + (k_1+k_2-k_3+k_4)[a_1, c_2] + (k_1-k_2-k_3-k_4)[a_1, c_3] + (-k_1-k_2-k_4)[a_1, c_4] = 0$.

Действуя на это равенство элементами x, x^2 и x^3, получим

$(k_1+k_2+k_4)[a_2, c_1] + (k_1-k_2+k_3+k_4)[a_2, c_2] + (-k_1-k_2-k_3-k_4)[a_2, c_3] + (-k_1-k_3)[a_2, c_4] = 0$,

$(k_1+k_3)[a_3, c_1] + (-k_1+k_2+k_3+k_4)[a_3, c_2] + (-k_1-k_2-k_3+k_4)[a_3, c_3] + (-k_2-k_4)[a_3, c_4] = 0$,

$(k_2+k_4)[a_4, c_1] + (k_1+k_2+k_3+k_4)[a_4, c_2] + (-k_1-k_2+k_3-k_4)[a_4, c_3] + (-k_1-k_3-k_4)[a_4, c_4] = 0$.

Действуя этими же элементами на равенство

$[a_3a_4, [a_1, a_3a_4]] = (k_2+k_3)[a_3, c_1] + (k_1+k_2-k_3+k_4)[a_3, c_2] + (k_1-k_2-k_3-k_4)[a_3, c_3] + (-k_1-k_2-k_4)[a_3, c_4] + (k_2+k_3)[a_4, c_1] + (k_1+k_2-k_3+k_4)[a_4, c_2] + (k_1-k_2-k_3-k_4)[a_4, c_3] + (-k_1-k_2-k_4)[a_4, c_4] = 0$,

получим равенства

$(-k_1-k_2-k_4)[a_1, c_1] + (-k_1+k_2-k_3-k_4)[a_1, c_2] + (k_1+k_2+k_3+k_4)[a_1, c_3] + (k_1+k_3)[a_1, c_4] + (-k_1-k_2-k_4)[a_2, c_1] + (-k_1+k_2-k_3-k_4)[a_2, c_2] + (k_1+k_2+k_3+k_4)[a_2, c_3] + (k_1+k_3)[a_2, c_4] + (-k_1-k_2-k_4)[a_3, c_1] + (-k_1+k_2-k_3-k_4)[a_3, c_2] + (k_1+k_2+k_3+k_4)[a_3, c_3] + (k_1+k_3)[a_3, c_4] = 0$,

$(-k_1-k_3)[a_2, c_1] + (k_1-k_2-k_3-k_4)[a_2, c_2] + (k_1+k_2+k_3-k_4)[a_2, c_3] + (k_2+k_4)[a_2, c_4] + (-k_1-k_3)[a_3, c_1] + (k_1-k_2-k_3-k_4)[a_3, c_2] + (k_1+k_2+k_3-k_4)[a_3, c_3] + (k_2+k_4)[a_3, c_4] + (-k_1-k_3)[a_4, c_1] + (k_1-k_2-k_3-k_4)[a_4, c_2] + (k_1+k_2+k_3-k_4)[a_4, c_3] + (k_2+k_4)[a_4, c_4] = 0$,

$(k_2+k_4)[a_1, c_1] + (k_1+k_2+k_3+k_4)[a_1, c_2] + (-k_1-k_2+k_3-k_4)[a_1, c_3] + (-k_1-k_3-k_4)[a_1, c_4] + (k_2+k_4)[a_2, c_1] + (k_1+k_2+k_3+k_4)[a_2, c_2] + (-k_1-k_2+k_3-k_4)[a_2, c_3] + (-k_1-k_3-k_4)[a_2, c_4] = 0$.

Аналогично из равенства

$[a_3a_4^{-1}, [a_3, a_4]] = (-k_1-k_2+k_3+k_4)[a_3, c_1] + (-k_1+k_2-k_4)[a_3, c_2] + (k_2-k_3+k_4)[a_3, c_3] + (k_1-k_2-k_3)[a_3, c_4] + (k_1+k_2-k_3-k_4)[a_4, c_1] + (k_1-k_2+k_4)[a_4, c_2] + (-k_2+k_3-k_4)[a_4, c_3] + (-k_1+k_2+k_3)[a_4, c_4] = 0$

получаем равенства

$(-k_1+k_2+k_3)[a_1, c_1] + (k_1-k_3+k_4)[a_1, c_2] + (k_1-k_2+k_3-k_4)[a_1, c_3] + (-k_1-k_2+k_4)[a_1, c_4] + (-k_1+k_2+k_3)[a_2, c_1] + (k_1-k_3+k_4)[a_2, c_2] + (k_1-k_2+k_3-k_4)[a_2, c_3] + (-k_1-k_2+k_4)[a_2, c_4] + (-k_1+k_2+k_3)[a_3, c_1] + (k_1-k_3+k_4)[a_3, c_2] + (k_1-k_2+k_3-k_4)[a_3, c_3] + (-k_1-k_2+k_4)[a_3, c_4] + (k_1-k_2-k_3)[a_4, c_1] + (-k_1+k_3-k_4)[a_4, c_2] + (-k_1+k_2-k_3+k_4)[a_4, c_3] + (k_1+k_2-k_4)[a_4, c_4] = 0$,

$(k_1+k_2-k_4)[a_1, c_1] + (-k_2+k_3-k_4)[a_1, c_2] + (-k_1+k_2-k_3)[a_1, c_3] + (-k_1+k_3+k_4)[a_1, c_4] + (-k_1-k_2+k_4)[a_2, c_1] + (k_2-k_3+k_4)[a_2, c_2] + (k_1-k_2+k_3)[a_2, c_3] + (k_1-k_3-k_4)[a_2, c_4] + (-k_1-k_2+k_4)[a_3, c_1] + (k_2-k_3+k_4)[a_3, c_2] + (k_1-k_2+k_3)[a_3, c_3] + (k_1-k_3-k_4)[a_3, c_4] + (-k_1-k_2+k_4)[a_4, c_1] + (k_2-k_3+k_4)[a_4, c_2] + (k_1-k_2+k_3)[a_4, c_3] + (k_1-k_3-k_4)[a_4, c_4] = 0$,

$(k_1-k_3-k_4)[a_1, c_1] + (-k_1+k_2-k_3+k_4)[a_1, c_2] + (k_1-k_2+k_4)[a_1, c_3] + (k_2+k_3-k_4)[a_1, c_4] + (-k_1+k_3+k_4)[a_2, c_1] + (k_1-k_2+k_3-k_4)[a_2, c_2] + (-k_1+k_2-k_4)[a_2, c_3] + (-k_2-k_3+k_4)[a_2, c_4] = 0$.

Если $[a_i, c_j] = \sum\limits_{r=1}^{4} s_{ijr} z_r$, где $z_r \in Z(P)$, i, $j \in \{1,2,3,4\}$, то положим $S_r = (s_{ijr})$. Как и выше, матрицы S_r должны удовлетворять уравнению

$$S_r + X'S_rX + (X')^2S_rX^2 + (X')^3S_rX^3 + (X')^4S_rX^4 = 0.$$

Но тогда справедливы равенства

$-[a_1,c_1]+[a_1,c_2]+[a_1,c_3]+[a_1,c_4]+[a_2,c_1]-[a_2,c_2]+[a_2,c_3]+[a_2,c_4]+[a_3,c_1]+[a_3,c_2]-[a_3,c_3]+[a_3,c_4]+[a_4,c_1]+[a_4,c_2]+[a_4,c_3]-[a_4,c_4]=0,$

$-[a_1,c_2]+[a_1,c_3]-[a_2,c_2]+[a_2,c_4]-[a_3,c_1]+[a_3,c_2]-[a_3,c_3]-[a_3,c_4]+[a_4,c_1]-[a_4,c_2]=0;$

$-[a_1,c_3]+[a_1,c_4]-[a_2,c_1]-[a_2,c_2]+[a_2,c_3]-[a_2,c_4]+[a_3,c_1]-[a_3,c_3]+[a_4,c_2]-[a_4,c_3]=0;$

$-[a_1,c_1]+[a_1,c_2]-[a_2,c_1]+[a_2,c_3]-[a_3,c_1]+[a_3,c_4]+[a_4,c_1]-[a_4,c_2]-[a_4,c_3]-[a_4,c_4]=0.$

В результате имеем однородную систему из 16 уравнений с 16 неизвестными $[a_i, c_j]$, $i, j = 1,2,3,4$. Непосредственная проверка показывает, что определитель основной матрицы этой системы не равен нулю ни при каких значениях $k_i \in GF(3)$, не равных нулю одновременно (авторами сделан просчет всех 80 случаев). Это означает, что $[a_i, c_j] = 0$ для всех i и j, т.е. $[P, P'] = 1$. Теорема доказана.

Теорема 3. *Пусть G двойная группа Фробениуса типа $(3,5,2)$. Если $C_P(y)$ имеет экспоненту 3, то подгруппа P нильпотентна ступени не выше двух и, следовательно, имеет экспоненту 3.*

Доказательство. Проведем индукцию по порядку группы G. Пусть G — минимальный контрпример к теореме, $Z = Z(P)$ и $P/P' = \prod\limits_{i=1}^{k} A_i/P'$, где A_i/P' — минимальные инвариантные подгруппы группы G/P' $(1 \le i \le k)$. Предположим сначала, что $k = 1$. Тогда $|P/P'| = 3^4$. Так как P/Z имеет экспоненту 3 и $P' = \Phi(P)$, то в силу предложения 3 $|P/Z| \le 3^{14}$. С учетом леммы 3 $|P/Z| = 3^{12}$. Из теоремы 2 следует, что ступень нильпотентности группы P/Z не превосходит 2. Так как P'/Z порождается простыми коммутаторами вида $[a,b]Z$, то из $|P/P'| = 3^4$ следует $|P'/Z| \le 3^6$. Но тогда $|P'/Z| = 3^4$ и $|P| = 3^{12}$, что противоречит утверждению теоремы 2.

Предположим теперь, что $k > 1$. В силу предположения индукции каждая из подгрупп A_i нильпотентна ступени не выше двух. Покажем, что $A_i' \le Z$. Так как группа A_i/A_i' элементарная абелева, то в силу теоремы Машке $A_i/A_i' = P'/A_i' \times B_i/A_i'$ для некоторой подгруппы B_i. Из $|A_i/P'| = 3^4$ следует, что $|B_i/A_i'| = 3^4$. Если группа B_i абелева, то

$$A_i' = [P', B_i] \le [P', P] \le Z.$$

Предположим, что группа B_i неабелева. Из $A_i' \le Z(B_i)$ и $|B_i/A_i'| = 3^4$ следует, что $|B_i'| \le 3^6$. Но тогда $|B_i'| = 3^4$, т.е. $B_i' \le Z(P)$, и снова $A_i' = [P', B_i] \cdot B_i' \le Z$. В частности, $|B_i/Z| = 3^4$. Так как $[B_i, B_j] < B_i \cap B_j$, то $[B_i, B_j] \le Z$. Отсюда

$$[A_i, A_j] = A_i' \cdot A_j' \cdot [A_i, A_j] = A_i' \cdot A_j' \cdot [B_iB_j, P'] \cdot [B_i, B_j] \le Z(P).$$

В силу произвольности чисел i и j, $P' \le Z$. Теорема доказана.

Поступила 19.10.2006

СПИСОК ЛИТЕРАТУРЫ

1. **Гаген Т. М.** Некоторые вопросы теории конечных групп // К теории конечных групп. М.: Мир, 1979. С. 13–97.
2. **Huppert B.** Endliche Gruppen, I. Berlin: Springer-Verlag, 1967.

ТРУДЫ ИНСТИТУТА МАТЕМАТИКИ И МЕХАНИКИ УрО РАН

Том 13 № 1 2007

УДК 512.54

О НЕКОТОРЫХ ПАРАХ НЕПРИВОДИМЫХ ХАРАКТЕРОВ ГРУПП S_n И A_n[1]

В. А. Белоногов

Автор продолжает изучение пар полупропорциональных неприводимых характеров конечных групп. Интерес к таким исследованиям поддерживается замеченной ранее связью между наличием или отсутствием у группы такой пары и локальным строением этой группы. В настоящей статье изучается вопрос о наличии таких пар у знакопеременных групп A_n. Рассматривается также более общая задача описания пар неприводимых характеров симметрической группы S_n, имеющих одно и то же множество корней на одном из множеств A_n и $S_n \setminus A_n$. Найдены все такие пары неприводимых характеров симметрической группы S_n в случае, когда длины главных диагоналей диаграмм Юнга, соответствующих этим характерам, не превосходят двух.

Введение

В настоящей работе изучаются пары неприводимых характеров группы S_n, имеющие одно и то же множество корней на одном из множеств A_n и $S_n \setminus A_n$, и, как следствие, пары равнокорневых и также полупропорциональных (определение напоминается ниже) неприводимых характеров группы A_n. Принципиальный план такого изучения был предложен в статье [10] (в теореме А и основанных на ней предложениях 4.1, 5.1 и 6.1). Там же приведены предпосылки и обоснование такого изучения. Вкратце повторим их здесь.

Функции φ и ψ из некоторого множества G в поле $\mathbb{C}$ называются *полупропорциональными*, если они не пропорциональны и для некоторого подмножества M из G пропорциональны ограничения φ и ψ на M и их ограничения на $G \setminus M$. В работах автора [1,3–5,7], первоначально связанных с понятием D-блока, изучались пары полупропорциональных неприводимых характеров конечных групп. В некоторых классах групп обнаружилась определённая связь между наличием или отсутствием у группы такой пары и локальным строением этой группы. Например, у квазипростых групп лиева типа $\mathrm{L}_2(q)$, $\mathrm{SL}_2(q)$, $\mathrm{L}_3(q)$, $\mathrm{SL}_3(q)$, $\mathrm{U}_3(q)$ и $\mathrm{SU}_3(q)$ такие пары отсутствуют при чётных q и присутствуют при нечётных q, за исключением групп $\mathrm{L}_2(5)$, $\mathrm{L}_2(7)$ и $\mathrm{L}_2(9)$ (изоморфных группам $\mathrm{L}_2(4)$, $\mathrm{L}_3(2)$ и $\mathrm{PSp}_4(2)'$ соответственно).

В статье [6] описаны такие пары характеров в симметрических группах и начато исследование таких пар в знакопеременных группах. Для различных неприводимых характеров φ и ψ группы S_n ($n \in \mathbb{N}$) оказались равносильными [6, теорема 1] следующие условия:

(1) φ и ψ полупропорциональны,

(2) φ и ψ имеют одно и то же множество корней,

(3) φ и ψ ассоциированы (т. е. $\psi = \varphi\xi$, где ξ — линейный характер группы S_n с ядром A_n).

В случае произвольных конечных групп равносильность условий (1) и (2) — исключительная редкость. Не равносильны они и для знакопеременных групп, и изучение этих условий в таких группах представляет интерес. Имеются пары φ, ψ неприводимых характеров группы A_n со свойством (2), и не известно ни одной такой пары со свойством (1).

Одна из целей, к которой стремится автор, — получить некоторые подтверждения следующей гипотезы из [6] (см. абзац перед теоремой 2).

[1]Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (проект 04-01-00463) и РФФИ-ГФЕН Китая (проект 05-01-39000).

Гипотеза 1. *Знакопеременная группа A_n при любом $n \in \mathbb{N}$ не имеет полупропорциональных неприводимых характеров.*

Некоторым шагом в доказательстве гипотезы 1 является следующий результат (в нём $P(n)$ обозначает множество всех разбиений числа n, и χ^α — неприводимый характер группы S_n, соответствующий разбиению $\alpha \in P(n)$; см. § 1 для деталей).

Предложение 1 [6, теорема 2]. *Пусть φ и ψ — полупропорциональные неприводимые характеры группы A_n. Тогда φ и ψ являются ограничениями на A_n некоторых неприводимых характеров χ^α и χ^β группы S_n $(\alpha, \beta \in P(n))$. Более того, ни одно из разбиений α и β не является крюком.*

Дальнейшим продвижением в доказательстве гипотезы 1 является следующая теорема, полученная в этой статье.

Теорема А. *Пусть φ и ψ — полупропорциональные неприводимые характеры группы A_n. Тогда φ и ψ являются ограничениями на A_n некоторых неприводимых характеров χ^α и χ^β группы S_n $(\alpha, \beta \in P(n))$, причём длины главных диагоналей диаграмм Юнга разбиений α и β отличаются не более, чем на единицу, и хотя бы одна из этих длин — не меньше трёх.*

Согласно теореме B из [9] в заключение теоремы А можно добавить утверждение: $\chi^\alpha(1) = \chi^\beta(1)$. (Таким образом, для групп A_n справедлива следующая *гипотеза о полупропорциональных характерах*: если φ и ψ — полупропорциональные неприводимые характеры конечной группы, то $\varphi(1) = \psi(1)$. Её справедливость доказана для всех упомянутых выше классов групп.)

Ввиду предложения 1 и известной связи между неприводимыми характерами групп S_n и A_n (см. предложения 1.3–1.5) гипотеза 1 равносильна следующей гипотезе.

Гипотеза 2. *Если χ^α и χ^β — неприводимые характеры группы S_n $(\alpha, \beta \in P(n))$, полупропорциональные на A_n, то одно из разбиений α и β самоассоциировано.*

Аналогично, изучение равнокорневых, т. е. имеющих одно и то же множество корней, неприводимых характеров группы A_n равносильно изучению неприводимых характеров группы S_n, равнокорневых на A_n. (Как обычно, корень функции $\varphi : G \to \mathbb{C}$ есть элемент $x \in G$ такой, что $\varphi(x) = 0$.) Метод изучения последней ситуации, избранный автором (использующий результаты типа леммы 3.5), требует также изучения неприводимых характеров группы S_n, равнокорневых на разности $S_n \setminus A_n$.

Теорема А является следствием предложения 1 и теорем 4.1, 5.1 и 6.1, дающих в совокупности описание всех пар неприводимых характеров χ^α и χ^β группы S_n $(\alpha, \beta \in P(n))$, имеющих одно и то же множество корней на одном из множеств A_n и $S_n \setminus A_n$, при дополнительном условии, что каждая из длин главных диагоналей диаграмм Юнга разбиений α и β не превосходит двух (см. также замечание в конце статьи). Последние три теоремы составляют основной результат работы. Мы объединим их в следующей теореме Б. Для $\varepsilon \in \{1, -1\}$ положим $S_n^\varepsilon := \begin{cases} S_n^+ := A_n, & \text{если } \varepsilon = 1, \\ S_n^- := S_n \setminus A_n, & \text{если } \varepsilon = -1. \end{cases}$ Условие $\alpha \neq' \beta$ (объясняемое в § 1) лишь исключает тривиальные случаи; оно равносильно тому, что характеры χ^α и χ^β различны и не ассоциированы. Исчезновение (обращение в нуль) характеров χ^α и χ^β на S_n^ε также есть тривиальный случай; согласно предложению 1.2 оно равносильно тому, что $\varepsilon = -1$ и разбиения α и β оба самоассоциированы.

Теорема Б. *Пусть χ^α и χ^β — неприводимые характеры группы S_n, имеющие одни и те же корни на S_n^ε при некотором $\varepsilon = \pm 1$, но не исчезающие тождественно на S_n^ε, причём $\alpha \neq' \beta$. Предположим, что $d(\alpha) \leq 2$ и $d(\beta) \leq 2$. Тогда верно одно из следующих утверждений:*

(1) $n = 3, \ \varepsilon = +1, \ \{\alpha, \beta\} =' \{(3), \ (2,1)\}$;

(2) $n = 4, \ \varepsilon = -1, \ \{\alpha, \beta\} =' \{(4), \ (3,1)\}$;

(3) $n = 4,\ \varepsilon = +1,\ \{\alpha, \beta\} =' \{(4),\ (2,2)\};$
(4) $n = 5,\ \varepsilon = -1,\ \{\alpha, \beta\} =' \{(5),\ (3,2)\};$
(5) $n = 6,\ \varepsilon = +1,\ \{\alpha, \beta\} =' \{(5,1),\ (3,3)\};$
(6) $n = 7,\ \varepsilon = +1,\ \{\alpha, \beta\} =' \{(5,2),\ (4,3)\};$
(7) $n = 7,\ \varepsilon = -1,\ \{\alpha, \beta\} =' \{(6,1),\ (4,3)\};$
(8) $n = 8,\ \varepsilon = +1,\ \{\alpha, \beta\} =' \{(6,1^2),\ (3,3,2)\};$
(9) $n = 8,\ \varepsilon = -1,\ \{\alpha, \beta\} =' \{(6,2),\ (5,3)\};$
(10) $n = 9,\ \varepsilon = -1,\ \{\alpha, \beta\} =' \{(6,3),\ (5,2^2)\};$
(11) $n = 9,\ \varepsilon = -1,\ \{\alpha, \beta\} =' \{(5,4),\ (4,3,2)\};$
(12) $n = 9,\ \varepsilon = -1,\ \{\alpha, \beta\} =' \{(7,1^2),\ (4,4,1)\};$
(13) $n = 10,\ \varepsilon = -1,\ \{\alpha, \beta\} =' \{(7,2,1),\ (5,4,1)\};$
(14) $n = 10,\ \varepsilon = -1,\ \{\alpha, \beta\} =' \{(7,3),\ (5,2,2,1)\};$
(15) $n = 11,\ \varepsilon = +1,\ \{\alpha, \beta\} =' \{(6,3,2),\ (5,4,2)\};$
(16) $n = 11,\ \varepsilon = -1,\ \{\alpha, \beta\} =' \{(8,1^3),\ (4,4,2,1)\};$
(17) $n = 14,\ \varepsilon = -1,\ \{\alpha, \beta\} =' \{(9,3,2),\ (6,3,2^2,1)\};$
(18) $n = 14,\ \varepsilon = -1,\ \{\alpha, \beta\} =' \{(8,3,2,1),\ (6,5,2,1)\};$
(19) $n = 16,\ \varepsilon = -1,\ \{\alpha, \beta\} =' \{(8,4,2^2),\ (7,5,2^2)\}.$

В § 1 работы приводятся необходимые сведения из теории представлений симметрических и знакопеременных групп, а в § 2 формулируется теорема A из [10], упомянутая в первом абзаце этого введения, а также определения и некоторые свойства функций h, f, h' и f', участвующих в её формулировке. Для удобства читателя здесь повторяются некоторые нужные для дальнейшего определения и результаты из §§ 1, 2 статьи [10]. Параграф 3 содержит ряд лемм, постоянно используемых в доказательствах основных теорем. Сами теоремы доказываются в §§ 4–6.

Обозначения, используемые в этой статье, в основном стандартны (см., например, [2] и [11]). В частности, $\mathrm{Cl}(G)$ — множество всех классов сопряжённых элементов группы G; g^G — класс сопряжённых элементов группы G, содержащий элемент $g \in G$; $\mathrm{Irr}(G)$ — множество всех неприводимых комплексных характеров группы G; $\varphi|_K$ — ограничение классовой функции φ группы G на её подмножестве K; $\mathbb{C}$, $\mathbb{Q}$, $\mathbb{Z}$ и $\mathbb{N}$ — множества всех комплексных, рациональных, целых и натуральных чисел соответственно; $\dot\cup$ — знак объединения попарно не пересекающихся множеств. Запись $A := B$ (читается: A по определению равно B) означает, что A есть обозначение для B. Если $\alpha = (a_1, \ldots, a_k)$ и $\beta = (b_1, \ldots, b_l)$ — конечные последовательности, то $\alpha * \beta$ обозначает последовательность $(a_1, \ldots, a_k, b_1, \ldots, b_l)$.

Если φ и ψ — классовые функции группы G, $S \subseteq G$ и функции $\varphi|_S$ и $\psi|_S$ имеют одно и то же множество корней, то мы говорим, что φ и ψ *имеют одно и то же множество корней на* S, и пишем “$\varphi \sim \psi$ на S” (знак “$\sim$” можно читать как “эквивалентно”). Также мы говорим, что φ и ψ *пропорциональны* или *полупропорциональны на* S, если $\varphi|_S$ и $\psi|_S$ пропорциональны или полупропорциональны соответственно.

Обозначения, связанные с разбиениями, напоминаются в § 1. Там вводятся также некоторые новые обозначения, в частности, бинарные отношения $='$ и $\in'$.

Всюду далее n обозначает натуральное число.

1. Разбиения и характеры групп S_n и A_n

Множество всех неприводимых характеров и множество всех классов сопряжённых элементов симметрической группы S_n находятся во взаимно однозначном соответствии с множеством $P(n)$ всех разбиений числа n [11,12]. Если α — такое разбиение, то χ^α и C_α обозначают соответствующие ему неприводимый характер и класс сопряжённых элементов группы S_n соответственно, а g_α обозначает некоторый элемент из C_α (когда конкретный вид элемента класса не важен). Напомним некоторые определения.

Разбиением натурального числа n называется последовательность $\alpha = (a_1, \ldots, a_l)$ натуральных чисел такая, что $a_1 \geq \ldots \geq a_l$ и $n = a_1 + \ldots + a_l$. Длину l разбиения α обозначают через $l(\alpha)$ и полагают $|\alpha| := n$. *Знаком* разбиения $\alpha \in P(n)$ называется число $\mathrm{sign}(\alpha) := (-1)^{n-l(\alpha)}$, а также знак этого числа. Разбиение α имеет знак $+$ если и только если $C_\alpha \subseteq A_n$. Каждому разбиению $\alpha = (a_1, \ldots, a_l) \in P(n)$ сопоставляется его *диаграмма Юнга* (или просто *диаграмма*) $[\alpha] := \{(i,j) \mid 1 \leq i \leq l,\ 1 \leq j \leq a_i\}$. На рисунке её обычно изображают в виде l-строчной таблицы, состоящей из n равных квадратных клеток, так, что i-я строка имеет a_i клеток, и начальные клетки всех строк находятся в одном столбце. Клетки (элементы) вида (i,i) диаграммы образуют её *главную диагональ*. Говорят, что разбиения α и β *ассоциированы*, если диаграмма одного из них получается из диаграммы другого отражением относительно главной диагонали. Разбиение, ассоциированное с α, обозначается через α'. Множество всех клеток (i,j) диаграммы $[\alpha]$ таких, что $[\alpha]$ не содержит клетки $(i+1, j+1)$, называется её *границей*.

Крюком диаграммы $[\alpha]$ (или разбиения α) с вершиной (i,j) называется множество $H^\alpha_{ij} := \{(i,j)\} \cup A \cup L$, где $A := \{(i, j+k) \in [\alpha] \mid k \geq 1\}$ (*рука крюка*) и $L := \{(i+k, j) \in [\alpha] \mid k \geq 1\}$ (*нога крюка*). *Косым крюком* с вершиной (i,j) диаграммы $[\alpha]$ называется часть границы диаграммы $[\alpha]$, "вырезанная" крюком H^α_{ij}. Его обозначают через R^α_{ij} или через $R(H^\alpha_{ij})$. Косые крюки диаграммы $[\alpha]$ — это в точности те связные части её границы, после удаления которых из $[\alpha]$ остаётся диаграмма некоторого разбиения (какого-либо меньшего числа). *Длиной* крюка (косого крюка, диагонали, ноги крюка) называется его (или её) мощность. Длина главной диагонали диаграммы $[\alpha]$ обозначается через $d(\alpha)$. Положим $h^\alpha_{ij} := |H^\alpha_{ij}|\ (= |R^\alpha_{ij}|)$. Для любого $\alpha \in P(n)$ определяется разбиение $h(\alpha) := (h^\alpha_{11}, \ldots, h^\alpha_{dd})$, где $d = d(\alpha)$.

Разбиением числа 0 называют пустую (длины 0) последовательность натуральных чисел, обозначаемую через $()$, и считают, что $[()] = \varnothing$ и $()' = ()$. Часто разбиения записывают в условной форме, заменяя подпоследовательность $a, \ldots, a$ длины $m \geq 0$ на a^m. Например, $(4, 3^2, 1) := (4,3,3,1)$ и $(5, 1^0) := (5)$.

Введём несколько новых обозначений. Пусть $\alpha, \beta \in P(n)$ и H есть крюк в $[\alpha]$. Тогда

$\alpha - H$ есть разбиение с диаграммой $[\alpha] \setminus R(H)$;

l_H — длина ноги крюка H;

$\mathrm{H}^\alpha(m)$ — множество всех крюков длины m в $[\alpha]$;

$\mathrm{H}^{\alpha,\beta}(m) := \mathrm{H}^\alpha(m) \cup \mathrm{H}^\beta(m)$;

$\alpha^{ij} := \alpha - H^\alpha_{ij}$;

$H^\alpha_1 := H^\alpha_{11}, \quad h^\alpha_1 := |H^\alpha_1|, \quad \alpha^1 := \alpha - H^\alpha_1\ (= \alpha^{11})$;

$$H^\alpha_2 := \begin{cases} H^\alpha_{12}, \text{ если } h^\alpha_{12} > h^\alpha_{21}, \\ H^\alpha_{21}, \text{ если } h^\alpha_{21} > h^\alpha_{12}, \\ \text{не определено, если } h^\alpha_{12} = h^\alpha_{21}, \end{cases}$$

$h^\alpha_2 := |H^\alpha_2|, \ \ \alpha^2 := \alpha - H^\alpha_2$.

Кроме того, для элементов α, β и подмножеств A, B из $P(n)$ мы пишем:

$\alpha =' \beta$, если $\alpha \in \{\beta, \beta'\}$;

$\alpha \in' B$, если $\alpha \in B$ или $\alpha' \in B$;

$A =' B$, если $\alpha \in' B$ для всех $\alpha \in A$ и $\beta \in' A$ для всех $\beta \in B$ (знаки $='$ и $\in'$ можно прочесть как "квазиравно" и "квазипринадлежит" соответственно). Отрицание отношения $\alpha =' \beta$ обозначается через $\alpha \neq' \beta$.

Предложение 1.1. (1) $\mathrm{Cl}(S_n) = \{C_\alpha \mid \alpha \in P(n)\}$, $|\mathrm{Cl}(S_n)| = |P(n)|$.

(2) $\mathrm{Irr}(S_n) = \{\chi^\alpha \mid \alpha \in P(n)\}$, $|\mathrm{Irr}(S_n)| = |P(n)|$.

(3) $\chi^{(n)} = 1_{S_n}$ *(главный характер группы S_n),* $\chi^{(1^n)} = \xi$ *— знакопеременный характер S_n (линейный характер с ядром A_n).*

(4) $\chi^{\alpha'} = \chi^\alpha \xi$ *для всех $\alpha \in P(n)$ (характеры χ^α и $\chi^{\alpha'}$ называются ассоциированными).*

(5) χ^α *исчезает на $S_n \setminus A_n$ если и только если $\alpha = \alpha'$ ($\alpha \in P(n)$).*

(6) *Неприводимые характеры группы S_n принимают лишь целые значения.*

(Для доказательства см. теоремы 2.1.7, 2.1.8, 2.1.11, 2.3.15 в [11] или утверждения 2.3, 4.12, 6.7 в [12].)

Если множество $\{1,\dots,n\}$ является объединением двух непересекающихся подмножеств Γ и Δ, $g\in S_\Gamma$ и $d\in S_\Delta$, то через $g\times d$ обозначается элемент из S_n, ограничение которого на Γ равно g, а ограничение на Δ равно d. Следующий результат играет очень важную роль в этой статье.

Предложение 1.2 (Теорема Мурнагана—Накаямы). *Пусть $\alpha\in P(n)$, $k\in\mathbb{N}$, x — произвольная перестановка элементов $1,\dots,n-k$, и z — циклическая перестановка остальных k элементов $n-k+1,\dots,n$. Тогда*

$$\chi^\alpha(z\times x)=\sum_{\substack{(i,j)\in[\alpha]\\ h^\alpha_{ij}=k}}(-1)^{l^\alpha_{ij}}\chi^{\alpha^{ij}}(x),$$

где l^α_{ij} — длина ноги крюка H^α_{ij} (при этом считается, что $\chi^{()}(x)=1$, а пустая сумма равна нулю).

(См. теорему 2.4.7 в [11] или утверждение 21.1 в [12].)

Предложение 1.3 [11, 1.2.10]. *Пусть $\alpha=(\alpha_1,\dots,\alpha_l)\in P(n)$ и $C_\alpha\subseteq A_n$. Тогда либо $C_\alpha\in \mathrm{Cl}(A_n)$, либо C_α — объединение двух классов сопряжённых элементов группы A_n. Последнее имеет место если и только если $n>1$, а числа $\alpha_1,\dots,\alpha_l$ нечётны и попарно различны.*

Предложение 1.4 [11, теорема 2.5.7]. *Пусть $n>1$, $P_1(n):=\{\alpha\in P(n)\mid \alpha\neq\alpha'\}$ и $P_2(n):=\{\alpha\in P(n)\mid\alpha=\alpha'\}$.*

(1) *Если $\alpha\in P_1(n)$, то $\chi^\alpha|_{A_n}=\chi^{\alpha'}|_{A_n}\in\mathrm{Irr}(A_n)$.*

(2) *Если $\alpha\in P_2(n)$, то $\chi^\alpha|_{A_n}=\chi^\alpha_+ + \chi^\alpha_-$, где χ^α_+ и χ^α_- — различные характеры из $\mathrm{Irr}(A_n)$, сопряжённые в S_n (какому из них приписать индекс плюс, а какому индекс минус, безразлично).*

(3) *$\mathrm{Irr}(A_n)=I_1\dot\cup I_2$, где*

$I_1=\{\chi^\alpha|_{A_n}\mid\alpha\in P_1(n)\},\ \ |I_1|=\frac12|P_1(n)|,$

$I_2=\{\chi^\alpha_+,\chi^\alpha_-\mid\alpha\in P_2(n)\},\ \ |I_2|=2|P_2(n)|.$

Предложение 1.5 [11, теорема 2.5.13 и лемма 2.3.12]. *Пусть $n>1$, $\alpha\in P(n)$ и $\alpha=\alpha'$. Тогда*

(1) *$C_{h(\alpha)}=x^{A_n}\cup y^{A_n}$ — объединение двух классов сопряжённых элементов группы A_n;*

(2) *$\chi^\alpha_\pm(g)=\frac12\chi^\alpha(g)\in\mathbb{Z}$ для всех $g\in A_n\setminus C_{h(\alpha)}$;*

(3) *$\chi^\alpha(x)=\pm1$ и с точностью до перемены мест x и y*

а) $\chi^\alpha_\pm(x)=\frac12\left(\chi^\alpha(x)\pm\sqrt{\chi^\alpha(x)\prod_{i=1}^{d(\alpha)}h^\alpha_{ii}}\right)$,

б) $\chi^\alpha_\pm(y)=\frac12\left(\chi^\alpha(x)\mp\sqrt{\chi^\alpha(x)\prod_{i=1}^{d(\alpha)}h^\alpha_{ii}}\right)$.

2. О неприводимых характерах, равнокорневых на S_n^ε, и функциях h, f, h', f'

Теорема 2.1 [10, теорема A]. *Пусть χ^α и χ^β — неприводимые характеры группы S_n ($\alpha,\beta\in P(n)$), имеющие одни и те же корни на S_n^ε при некотором $\varepsilon=\pm1$, причём $\alpha\neq'\beta$. Предположим (не ограничивая общности), что $d(\alpha)\le d(\beta)$. Тогда верно одно и только одно из следующих утверждений:*

(0) *$\alpha=\alpha'$, $\beta=\beta'$ и $\varepsilon=-1$ (тривиальный случай);*

(1) *$f(\alpha)=h(\beta)$, $f'(\alpha)=h'(\beta)$, $d(\alpha)+1=d(\beta)$, $\mathrm{sign}(f(\alpha))=\varepsilon$;*

(2) $f(\alpha) = f(\beta)$, $f'(\alpha) = f'(\beta)$, $d(\alpha) = d(\beta)$ *и* $\operatorname{sign}(f(\alpha)) = \varepsilon$;
(3) $h(\alpha) = h(\beta)$, $h'(\alpha) = h'(\beta)$, $d(\alpha) = d(\beta)$ *и* $\operatorname{sign}(h(\alpha)) = \varepsilon$.

В случае (0) характеры χ^α и χ^β принимают нулевые значения на всём множестве S_n^ε (по п. 5 предложения 1.1) и здесь тривиально выполнено условие теоремы; назовём такие пары χ^α и χ^β *тривиальными*. Таким образом, теорема 2.1 подразделяет нетривиальные пары неприводимых характеров χ^α и χ^β, равнокорневых на S_n^ε, на три типа (типы fh, ff и hh, соответствующие условиям (1), (2), и (3)).

Далее приводятся определения функций h, f, h', f' и некоторые их свойства. Разбиение $h(\alpha)$ уже встречалось в § 1. Напомним его определение.

Определение 2.1. *Для любого* $\alpha \in P(n)$ $(n \geq 1)$ $h(\alpha) := (h_{11}^\alpha, \ldots, h_{dd}^\alpha)$, *где* $d = d(\alpha)$.

Предложение 2.1 [11, 2.4.9]. *Пусть* $\alpha \in P(n)$. *Тогда*

(1) $h(\alpha)$ *есть наибольшее (относительно обычного словарного порядка* $\leq$ *) из разбиений* $\beta \in P(n)$ *таких, что* $\chi^\alpha(g_\beta) \neq 0$;
(2) $\chi^\alpha(g_{h(\alpha)}) = \pm 1$.

Определение 2.2 [8]. *Пусть* $\alpha \in P(n)$ *и* $\alpha \neq \alpha'$. *Определим разбиение* $f(\alpha)$ *индукцией по длине* $d(\alpha)$ *главной диагонали* α.

(1) *Если* $d(\alpha) = 1$, *то* $f(\alpha) := (h_2^\alpha,\ n - h_2^\alpha)$.
(2) *Если* $d(\alpha) > 1$, *то*

$$f(\alpha) := \begin{cases} (h_1^\alpha) * f(\alpha^1), & \text{если } \alpha^1 \neq (\alpha^1)', \\ (h_2^\alpha) * f(\alpha^2), & \text{если } \alpha^1 = (\alpha^1)'. \end{cases}$$

Предложение 2.2 [8, теорема 1]. *Пусть* $\alpha \in P(n)$, $n \in \mathbb{N}$ *и* $\alpha \neq \alpha'$. *Тогда*

(1) $f(\alpha) \in P(n)$ *и* $f(\alpha) = f(\alpha')$;
(2) $l(f(\alpha)) = l(h(\alpha)) + 1$ $(= d(\alpha) + 1)$;
(3) $f(\alpha)$ *есть наибольшее из разбиений* β *числа* n, *знак которых противоположен знаку* $h(\alpha)$ *и таких, что* $\chi^\alpha(g_\beta) \neq 0$;
(4) $\chi^\alpha(g_{f(\alpha)}) = \pm 1$.

Определение 2.3 [9]. *Пусть* $\alpha \in P(n)$ *и* $n \geq 3$. *Определим разбиение* $h'(\alpha)$ *индукцией по* $|\alpha^1|$.

(1) *Если* $|\alpha^1| = 0$, *т. е.* $\alpha =' (1 + a, 1^b)$, *где* $a \geq b \geq 0$, *то*

$$h'(\alpha) := \begin{cases} (n-2, 1, 1), & \text{если } b = 0 \ (\text{т. е. } \alpha =' (n)), \\ (a, b, 1), & \text{если } b > 0. \end{cases}$$

(2) *Если* $|\alpha^1| \in \{1, 2\}$, *то*

$$h'(\alpha) := (m, n - m), \quad \text{где} \ \ m = \max\{h_{12}^\alpha, h_{21}^\alpha\}.$$

(3) *Если* $|\alpha^1| \geq 3$, *то* $h'(\alpha) := (h_1^\alpha) * h'(\alpha^1)$.

Предложение 2.3 [9, теорема A]. *Пусть* $\alpha \in P(n)$ *и* $n \geq 3$. *Тогда*

(1) $h'(\alpha) \in P(n)$ *и* $h'(\alpha) = h'(\alpha')$;
(2) $h'(\alpha)$ *имеет тот же знак, что и* $h(\alpha)$;
(3) $\chi^\alpha(g_{h'(\alpha)}) \neq 0$, *но* $\chi^\alpha(g_\gamma) = 0$ *для всех* $\gamma \in P(n)$ *таких, что знак* γ *совпадает со знаком* $h(\alpha)$ *и* $h'(\alpha) < \gamma < h(\alpha)$.

Определение разбиения $f'(\alpha)$ мы дадим здесь в более удобной для использования форме, чем в [9]; a и b обозначают в нём целые неотрицательные числа.

Определение 2.4. *Пусть* $\alpha \in P(n)$, $\alpha \neq \alpha'$ *и* $n \geq 4$. *Определим разбиение* $f'(\alpha)$ *индукцией по* $|\alpha^1|$.

А. *Пусть* $\alpha^1 \neq (\alpha^1)'$.

А1. *Если* $|\alpha^1| \geq 4$, *то* $f'(\alpha) := (h_1^\alpha) * f'(\alpha^1)$.

А2. *Если* $|\alpha^1| = 3$, *т. е.* $\alpha =' (4+a, 4, 1^b)$, *то*

$$f'(\alpha) := \begin{cases} (4+a, 1+b, 3), & \text{если } a > b \geq 2; \\ (3+a, 5, 1), & \text{если } a > b = 1; \\ (4+a, 2, 2), & \text{если } a > b = 0; \\ (4+b, 3+a, 1), & \text{если } b \geq a. \end{cases}$$

А3. *Если* $|\alpha^1| = 2$, *т. е.* $\alpha =' (3+a, 3, 1^b)$, *то*

$$f'(\alpha) := \begin{cases} (3+a, 1+b, 2), & \text{если } a > b > 0; \\ (2+a, 3, 1), & \text{если } a > b = 0; \\ (3+b, 2+a, 1), & \text{если } b \geq a. \end{cases}$$

Б. *Пусть* $\alpha^1 = (\alpha^1)'$.

Б1. *Если* $|\alpha^1| \geq 3$, *то* $f'(\alpha) := (h_2^\alpha) * f'(\alpha^2)$.

Б2. *Если* $|\alpha^1| = 1$, *т. е.* $\alpha =' (2+a, 2, 1^b)$ *с* $a > b \geq 0$, *то*

$$f'(\alpha) := \begin{cases} (2+a, b, 2), & \text{если } b \geq 2; \\ (a, 3+b, 1), & \text{если } b \leq 1 \text{ и } a \geq 3+b; \\ (2+b, 2+b, 2), & \text{если } b \leq 1 \text{ и } a = 2+b \\ & \quad (\text{т. е. } \alpha =' (4,2) \text{ или } \alpha =' (5,2,1)\,); \\ (2+b, 2+b, 1), & \text{если } b \leq 1 \text{ и } a = 1+b \\ & \quad (\text{т. е. } \alpha =' (3,2) \text{ или } \alpha =' (4,2,1)\,). \end{cases}$$

Б3. *Если* $|\alpha^1| = 0$, *т. е.* $\alpha =' (1+a, 1^b)$ *с* $a > b \geq 0$, *то*

$$f'(\alpha) := \begin{cases} (n-2, 2), & \text{если } b = 0 \ \ (\text{т. е. } \alpha =' (n)); \\ (a, b-1, 1^2), & \text{если } b \geq 2; \\ (a-1, 3), & \text{если } b = 1 \text{ и } a \geq 4; \\ (a-1, 1^3), & \text{если } b = 1 \text{ и } a \in \{2,3\} \\ & \quad (\text{т. е. } \alpha =' (3,1) \text{ или } \alpha =' (4,1)). \end{cases}$$

Предложение 2.4 [9, теорема Б]. *Пусть* $\alpha \in P(n)$, $\alpha \neq \alpha'$ *и* $n \geq 4$. *Тогда*

(1) $f'(\alpha) \in P(n)$ *и* $f'(\alpha) = f'(\alpha')$;

(2) $f'(\alpha)$ *имеет тот же знак, что и* $f(\alpha)$;

(3) $\chi^\alpha(g_{f'(\alpha)}) \neq 0$, *но* $\chi^\alpha(g_\gamma) = 0$ *для всех* $\gamma \in P(n)$ *таких, что знак* γ *совпадает со знаком* $f(\alpha)$ *и* $f'(\alpha) < \gamma < f(\alpha)$.

3. Рабочие леммы

Здесь содержатся результаты, используемые при изучении неприводимых характеров группы S_n, имеющих одно и то же множество корней на A_n или на $S_n \setminus A_n$, а также неприводимых характеров S_n, которые пропорциональны или полупропорциональны на каком-либо из этих множеств.

Лемма 3.1. *Пусть* $\alpha \in P(n)$ *и характер* χ^α *группы* S_n *не имеет корней на* S_n^ε *для некоторого* $\varepsilon = \pm 1$ (*т. е.* $\chi^\alpha \sim \chi^{(n)}$ *на* S_n^ε). *Тогда верно одно из следующих утверждений:*

(1) $\alpha =' (n)$ (*n и ε — любые*);
(2) $\alpha =' (2,1)$, $\varepsilon = +1$;
(3) $\alpha =' (2,2)$, $\varepsilon = +1$;
(4) $\alpha =' (3,1)$, $\varepsilon = -1$;
(5) $\alpha =' (3,2)$, $\varepsilon = -1$.

Обратно, в каждом из случаев (1)–(5) χ^α *не имеет корней на* S_n^ε.

Доказательство. Предположим, что утверждение (1) ложно и, в частности, $n \geq 3$.

Пусть $\varepsilon = (-1)^{n+1}$. Тогда разбиения (n) и $(n-2,1,1)$ имеют знак ε и по условию леммы $\chi^\alpha(g_{(n)})$ и $\chi^\alpha(g_{(n-2,1,1)})$ отличны от нуля. Следовательно, по предложению 1.2 $[\alpha]$ имеет крюки длин n и $n-2$, и поэтому $\alpha =' (n-1,1)$. Если $n \geq 5$, то $(n-3,2,1)$ есть разбиение знака ε и в то же время по предложению 1.2 $\chi^\alpha(g_{(n-3,2,1)}) = \chi^{(2,1)}(g_{(2,1)}) = 0$, что противоречит условию леммы. Следовательно, $n \leq 4$ и верно одно из утверждений (2) и (4).

Пусть теперь $\varepsilon = (-1)^n$. Тогда разбиения $(n-1,1)$ и $(n-2,2)$ имеют знак ε. Отсюда, из условия леммы и предложения 1.2 следует, что $[\alpha]$ имеет крюки длин $n-1$ и $n-2$, и поэтому $\alpha =' (n-2,2)$ (так как $\alpha \neq (n)$). Если $n \geq 6$, то $(n-3,3)$ — разбиение знака ε, однако по предложению 1.2 $\chi^\alpha(g_{(n-3,3)}) = 0$ (так как $[\alpha]$ не имеет крюков длины $n-3$) в противоречие с условием леммы. Следовательно, $n \leq 5$ и выполнено одно из утверждений (3) и (5).

Лемма 3.1 доказана.

Лемма 3.2. *Пусть* $\alpha, \beta \in P(n)$ *и* $\varepsilon \in \{1,-1\}$. *Равносильны условия*:
(1) *характеры* χ^α *и* χ^β *пропорциональны на* S_n^ε;
(2) *выполнено по крайней мере одно из условий*:
  (2а) $\alpha =' \beta$;
  (2б) $\varepsilon = -1$, $\alpha = \alpha'$ *и* $\beta = \beta'$.

Доказательство. Это — объединение лемм 3.4 и 3.5 из [6]. (Заметим, что по п. (5) предложения 1.1 в случае (2б) характеры χ^α и χ^β принимают лишь нулевые значения на S_n^ε.)

Лемма 3.3. *Пусть* $\alpha, \beta \in P(n)$ *и* $\chi^\alpha \sim \chi^\beta$ *на* S_n^ε, *где* $\varepsilon \in \{1,-1\}$. *Предположим, что* $[\alpha]$ *или* $[\beta]$ *имеет крюк некоторой длины* m. *Тогда*

$$\sum_{H \in \mathrm{H}^\alpha(m)} (-1)^{l_H} \chi^{\alpha - H} \sim \sum_{K \in \mathrm{H}^\beta(m)} (-1)^{l_K} \chi^{\beta - K} \quad \text{на} \quad S_{n-m}^\delta,$$

где $\delta = (-1)^{m+1}\varepsilon$.

Доказательство. Рассмотрим множество всех элементов группы S_n вида $z \times x$, где $x \in S_{n-m}$ и z — фиксированная циклическая перестановка m элементов $n-m+1, \dots, n$. По предложению 1.2

$$\chi^\alpha(z \times x) = \sum_{H \in \mathrm{H}^\alpha(m)} (-1)^{l_H} \chi^{\alpha - H}(x)$$

и

$$\chi^\beta(z \times x) = \sum_{K \in \mathrm{H}^\beta(m)} (-1)^{l_K} \chi^{\beta - K}(x).$$

Очевидно, $\mathrm{sign}(z \times x) = (-1)^{m+1}\mathrm{sign}(x)$, и потому $z \times x \in S_n^\varepsilon$ если и только если $x \in S_{n-m}^\delta$, где $\delta = (-1)^{m+1}\varepsilon$. Следовательно, при любом $x \in S_{n-m}^\delta$ правые части приведённых выше равенств могут быть равны нулю только одновременно, поскольку по условию леммы левые части обладают этим свойством.

Лемма 3.3 доказана.

З а м е ч а н и е. Как видно из доказательства леммы 3.3, если в её условии знак $\sim$ заменить словом “полупропорционально”, то в её заключении можно знак $\sim$ заменить на “пропорционально или полупропорционально”.

Лемма 3.4. *Пусть $\alpha, \beta \in P(n)$ и $\chi^\alpha \sim \chi^\beta$ на S_n^ε, где $\varepsilon \in \{1, -1\}$. Предположим, что $[\alpha]$ имеет единственный крюк H некоторой длины m, а $[\beta]$ не имеет крюков длины m. Тогда*

$$\alpha - H = (\alpha - H)' \quad \textit{и} \quad \varepsilon = (-1)^m.$$

Д о к а з а т е л ь с т в о. По условию $\mathrm{H}^\alpha(m) = \{H\}$ и $\mathrm{H}^\beta(m) = \varnothing$. По лемме 3.3 $\chi^{\alpha-H} \sim 0$ на S_{n-m}^δ при $\delta = (-1)^{m+1}\varepsilon$ (здесь 0 — нулевой обобщённый характер группы S_{n-m}). Отсюда и из п. (5) утверждения 1.1 следует, что $\alpha - H = (\alpha - H)'$ и $\delta = -1$. Следовательно, $\varepsilon = (-1)^m$.

Лемма 3.4 доказана.

Лемма 3.5. *Пусть $\alpha, \beta \in P(n)$ и $\chi^\alpha \sim \chi^\beta$ на S_n^ε, где $\varepsilon \in \{1, -1\}$. Предположим, что диаграммы $[\alpha]$ и $[\beta]$ имеют точно по одному крюку H и K соответственно некоторой длины m. Тогда*

$$\chi^{\alpha-H} \sim \chi^{\beta-K} \quad \textit{на} \quad S_{n-m}^\delta, \quad \textit{где} \quad \delta = (-1)^{m+1}\varepsilon.$$

Д о к а з а т е л ь с т в о. По условию $\mathrm{H}^\alpha(m) = \{H\}$ и $\mathrm{H}^\beta(m) = \{K\}$. По лемме 3.3 отсюда следует требуемое заключение.

Лемма 3.5 доказана.

Лемма 3.6. *Пусть χ^α и χ^β — неприводимые характеры группы S_n, полупропорциональные на S_n^ε ($\alpha, \beta \in P(n)$). Предположим, что диаграммы $[\alpha]$ и $[\beta]$ имеют точно по одному крюку H и K соответственно некоторой длины m. Тогда $\chi^{\alpha-H}$ и $\chi^{\beta-K}$ пропорциональны или полупропорциональны на S_{n-m}^δ, где $\delta = (-1)^{m+1}\varepsilon$.*

Д о к а з а т е л ь с т в о повторяет доказательство леммы 3.5 с учётом замечания к лемме 3.3. (Это — объединение лемм 3.9 и 3.10 из [6].)

Лемма 3.7. *Пусть $\alpha, \beta \in P(n)$ и $\chi^\alpha \sim \chi^\beta$ на S_n^ε, где $\varepsilon \in \{1, -1\}$. Предположим, что $[\alpha]$ имеет точно два крюка H и K некоторой длины m, а $[\beta]$ не имеет крюков длины m. Тогда верно одно из условий*:

(1) $\varepsilon = (-1)^{m+1}$, $l_H + l_K$ *нечётно и* $\alpha - H =' \alpha - K$;

(2) $\varepsilon = (-1)^m$, *и либо* $\alpha - H =' \alpha - K$, *либо разбиения* $\alpha - H$ *и* $\alpha - K$ *оба самоассоциированы.*

Д о к а з а т е л ь с т в о. Пусть $x \in S_{n-m}$ и z —циклическая перестановка m элементов $n - m + 1, \ldots, n$. Так как β не имеет крюков длины m, то по предложению 1.2

$$\chi^\beta(z \times x) = 0 \quad \text{для всех} \quad x \in S_{n-m}. \tag{3.1}$$

В частности, это верно при любом $x \in S_{n-m}^\delta$, где $\delta = (-1)^{m+1}\varepsilon$, а в этом случае $z \times x \in S_n^\varepsilon$. Следовательно, по (3.1) и по условию леммы $\chi^\alpha(z \times x) = 0$ при $x \in S_{n-m}^\delta$. Поскольку по предложению 3.2 левая часть этого равенства равна $(-1)^{l_H}\chi^{\alpha-H}(x) + (-1)^{l_K}\chi^{\alpha-K}(x)$, то

$$\chi^{\alpha-H}(x) = (-1)^{1+l_H+l_K}\chi^{\alpha-K}(x). \tag{3.2}$$

Таким образом, характеры $\chi^{\alpha-H}$ и $\chi^{\alpha-K}$ группы S_{n-m} пропорциональны на S_{n-m}^δ. Но тогда по лемме 3.2 выполнено одно из условий:

$\delta = 1$ (следовательно, $\varepsilon = (-1)^{m+1}$) и $\alpha - H =' \alpha - K$;

$\delta = -1$ (следовательно, $\varepsilon = (-1)^m$) и либо $\alpha - H =' \alpha - K$,

либо $\alpha - H = (\alpha - H)'$ и $\beta - K = (\beta - K)'$.
Кроме того, при $\delta = 1$ число $l_H + l_K$ нечётно, так как в этом случае равенство (3.2) должно выполняться при $x = 1$.

Лемма 3.7 доказана.

Лемма 3.8. *Пусть* $\alpha, \beta \in P(n)$, $d(\alpha) = d(\beta) = 1$ *(т. е.* α *и* β *— крюки) и* $\chi^\alpha \sim \chi^\beta$ *на* S_n^ε, *где* $\varepsilon \in \{1, -1\}$. *Тогда верно одно из следующих утверждений:*

(1) $\alpha =' \beta$,

(2) $\{\alpha, \beta\} =' \{(3), (2, 1)\}$ *и* $\varepsilon = 1$,

(3) $\{\alpha, \beta\} =' \{(4), (3, 1)\}$ *и* $\varepsilon = -1$.

Д о к а з а т е л ь с т в о. Предположим, что условие (1) не верно. Тогда $n \geq 3$.

Если $\alpha =' (n)$ или $\beta =' (n)$, то по лемме 3.1 верно одно из утверждений (2) и (3).

В противном случае мы можем считать, что $\alpha = (1 + a, 1^b)$, где $a \geq b \geq 1$, $\beta = (1 + c, 1^d)$, где $c \geq d \geq 1$, и (поскольку $\alpha \neq' \beta$) $a > c$. Так как, очевидно, $a + b = c + d$, то отсюда следует, что $a > b$. Следовательно, диаграмма $[\alpha]$ имеет единственный крюк H_{12}^α длины a, а диаграмма $[\beta]$ не имеет крюков такой длины. Тогда по лемме 3.4 должно быть $\alpha^{12} = (\alpha^{12})'$. Но это противоречиво, так как $\alpha^{12} = (1^{1+b})$ и $b > 0$.

Лемма 3.8 доказана.

(Доказательство этой леммы можно завершить, не опираясь на лемму 3.4, заменив последние два предложения следующими.

Для любого $\gamma \in P(1 + b)$ по предложению 1.2

$$\chi^\alpha(g_{(a)*\gamma}) = \pm\chi^{(1+b)}(g_\gamma) = \pm 1 \neq 0 \quad \text{и} \quad \chi^\beta(g_{(a)*\gamma}) = 0.$$

Так как $1 + b \geq 2$, то в качестве γ можно выбрать разбиение любого знака. Следовательно, χ^α и χ^β имеют разные множества корней как на S_n^+, так и на S_n^-, в противоречие с условием леммы.)

4. $\chi^\alpha \sim \chi^\beta$ на S_n^ε. Случай $d(\beta) > d(\alpha) = 1$

Пусть $\alpha, \beta \in P(n)$ такие, что

$$\chi^\alpha \sim \chi^\beta \quad \text{на} \quad S_n^\varepsilon, \quad \text{где} \quad \alpha \neq' \beta \quad \text{и} \quad \varepsilon = \pm 1. \tag{4.1}$$

В этом параграфе мы найдём все тройки $(\alpha, \beta, \varepsilon)$ со свойством (4.1), удовлетворяющие условию $d(\beta) > d(\alpha) = 1$. По теореме 2.1 должно быть верно одно из её утверждений (0)–(3). Естественно, изучения требует лишь случай, когда χ^α и χ^β не исчезают тождественно на S_n^ε. Тогда из условия $d(\beta) > d(\alpha)$ следует, что здесь верно утверждение (1) теоремы 2.1. Поэтому мы можем (и будем) использовать следующее

Предложение 4.1 [10, предложение 4.1]. *Пусть* $\alpha, \beta \in P(n)$,

$$f(\alpha) = h(\beta) \quad \text{и} \quad f'(\alpha) = h'(\beta) \tag{4.2}$$

(следовательно, $\alpha \neq \alpha'$ *и* $n \geq 4$*). Тогда справедливы следующие утверждения.*

(1) *Если* $|\alpha^1| = 0$, *то выполнено одно из следующих условий:*

(1а) $\alpha =' (n)$ *и* $\beta =' (n - 2, 2)$.

(1б) $\alpha =' (n - 1, 1)$ *и* $\beta \in' \{(n - 3, 3), (n - 4, 2, 2)\}$ $(n \geq 6)$.

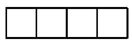
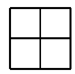
(1в) $\alpha =' (1 + a, 1^b)$ *с* $a \geq 3 + b \geq 5$ *и* $\beta \in' \{(2 + b + c, 2 + b, 1^d), (1 + b + c, 1 + b, 2, 1^d) \mid c + d = a - b - 3\}$.

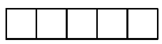
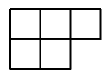
(2) *Если* $|\alpha^1| = 1$, *то* $\alpha =' (2 + a, 2, 1^b)$ *с* $a > b \geq 2$ *и* $\beta =' (1 + b + c, 1 + b, 3, 1^d)$ *с* $c + d = a - b - 1 \geq 0$.

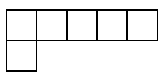
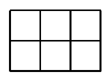
(3) *Если* $|\alpha^1| > 1$ *и* $\alpha^1 = (\alpha^1)'$, *то* $f(\alpha^2) = h(\beta^1)$ *и* $f'(\alpha^2) = h'(\beta^1)$.
(4) *Если* $\alpha^1 \neq (\alpha^1)'$, *то* $f(\alpha^1) = h(\beta^1)$ *и* $f'(\alpha^1) = h'(\beta^1)$.
Обратно, для любых α, β *из пунктов* (1)–(4) *выполнено условие* (4.2).

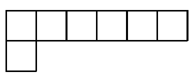
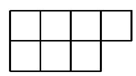
Теорема 4.1. *Пусть* χ^α *и* χ^β — *неприводимые характеры группы* S_n, *имеющие одни и те же корни на* S_n^ε *при некотором* $\varepsilon = \pm 1$, *но не исчезающие тождественно на* S_n^ε. *Предположим, что* $d(\beta) > d(\alpha) = 1$. *Тогда верно одно из следующих утверждений*:
(1) $n = 4, \quad \alpha =' (4), \quad \beta = (2,2), \quad \varepsilon = +1;$
(2) $n = 5, \quad \alpha =' (5), \quad \beta =' (3,2), \quad \varepsilon = -1;$
(3) $n = 6, \quad \alpha =' (5,1), \quad \beta =' (3,3), \quad \varepsilon = +1;$
(4) $n = 7, \quad \alpha =' (6,1), \quad \beta =' (4,3), \quad \varepsilon = -1;$
(5) $n = 8, \quad \alpha =' (6,1^2), \quad \beta = (3,3,2), \quad \varepsilon = +1;$
(6) $n = 9, \quad \alpha =' (7,1^2), \quad \beta =' (4,4,1), \quad \varepsilon = -1;$
(7) $n = 11, \quad \alpha =' (8,1^3), \quad \beta =' (4,4,2,1), \quad \varepsilon = -1.$
Обратно, в каждом из случаев (1)–(7) *выполняется условие теоремы.*

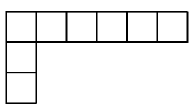
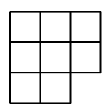
Прежде чем начать доказательство, приведём диаграммы $[\alpha]$ и $[\beta]$ в каждом из случаев (1)–(7). (Заранее зная вид диаграмм, к которым мы должны прийти в итоге действий с общими видами диаграмм $[\alpha]$ и $[\beta]$, даваемых предложением 4.1, легче понимать доказательство.)

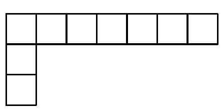
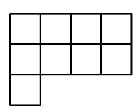
(1) $[\alpha] =$ , $[\beta] =$ , $\varepsilon = +1$,

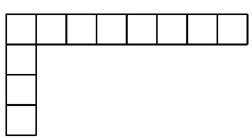
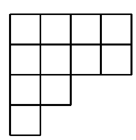
(2) $[\alpha] =$ , $[\beta] =$ , $\varepsilon = -1$,

(3) $[\alpha] =$ , $[\beta] =$ , $\varepsilon = +1$,

(4) $[\alpha] =$ , $[\beta] =$ , $\varepsilon = -1$,

(5) $[\alpha] =$ , $[\beta] =$ , $\varepsilon = +1$,

(6) $[\alpha] =$ , $[\beta] =$ , $\varepsilon = -1$,

(7) $[\alpha] =$ , $[\beta] =$ , $\varepsilon = -1$.

Доказательство. Пусть выполнено условие теоремы 4.1. Как уже замечено в начале этого параграфа, тогда верно утверждение (1) предложения 4.1, т. е.

$$f(\alpha) = h(\beta), \ f'(\alpha) = h'(\beta), \ d(\beta) = d(\alpha) + 1 = 2 \text{ и } \operatorname{sign}(f(\alpha)) = \varepsilon.$$

Так как по предложению 2.2 $l(f(\alpha)) = d(\alpha) + 1 = 2$, то $\operatorname{sign}(f(\alpha)) = (-1)^{n-2}$ и, значит,

$$\varepsilon = (-1)^n. \tag{4.3}$$

Согласно предложению 4.1 должно быть выполнено одно из условий (1а), (1б), (1в) его заключения. Эти условия рассматриваются ниже в случаях А, Б1, Б2, В1, В2.

С л у ч а й А. Пусть $\alpha =' (n)$ и $\beta =' (n-2,2)$.

Тогда χ^{α} — главный или знакопеременный характер группы S_n и, следовательно, по условию теоремы χ^{β} не имеет нулевых значений на S_n^{ε}. Но тогда по лемме 3.1 должно быть верно одно из утверждений (1) и (2) доказываемой теоремы.

С л у ч а й Б1. Пусть $\alpha =' (n-1,1)$ и $\beta =' (n-3,3)$, где $n \geq 6$.

Предположим, что $n \geq 8$. Тогда H_{14}^{α} и H_{13}^{β} — единственные крюки длины $n-4$ в $[\alpha]$ и $[\beta]$ соответственно (вид диаграмм легко себе представить). По лемме 3.5 $\chi^{\alpha^{14}} \sim \chi^{\beta^{13}}$ на S_4^{δ}, где $\delta = \pm 1$. Но это противоречиво, так как значения характеров $\chi^{\alpha^{14}} = \chi^{(3,1)}$ и $\chi^{\beta^{13}} = \chi^{(2,2)}$ на элементах $g_{(3,1)}, g_{(4)}$ разных знаков равны $0,-1$ и $-1,0$ соответственно.

Следовательно, $n = 6$ или $n = 7$, а в этих случаях верны (так как $\varepsilon = (-1)^n$ по (4.3)) соответственно утверждения (3) и (4) доказываемой теоремы.

С л у ч а й Б2. Пусть $\alpha =' (n-1,1)$ и $\beta =' (n-4,2,2)$, где $n \geq 6$.

Можно считать, что $n > 6$, так как в противном случае выполнено условие случая Б1.

Предположим, что $n \geq 8$. Тогда $[\beta]$ не имеет крюков длины $n-4$, а $[\alpha]$ имеет точно один крюк H_{14}^{α} такой длины, и по лемме 3.4 $\alpha^{14} = (\alpha^{14})'$, что противоречиво, так как $\alpha^{14} = (3,1)$.

Следовательно, $n = 7$, $\alpha =' (6,1)$, $\beta =' (3,2,2)$ и $\varepsilon = -1$. Но это противоречиво, так как значения характеров χ^{α} и χ^{β} на элементе $g_{(2^3,1)}$ равны 0 и 3 соответственно.

Итак, при $n > 6$ случай Б2 противоречив.

С л у ч а й В1. Пусть $\alpha =' (1+a,1^b)$ и $\beta =' (2+b+c,2+b,1^v)$, где $b \geq 2$ и $c+v = a-b-3 \geq 0$.

Без ограничения общности можно считать, что диаграммы $[\alpha]$ и $[\beta]$ в этом случае имеют вид, изображённый на рис. 4.1 ($\{a,b,c,d\} \subseteq \mathbb{N} \cup \{0\}$).

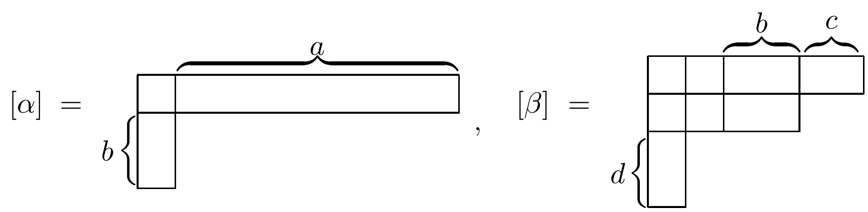


Рис. 4.1

Подсчитаем длины некоторых крюков, которые будут фигурировать в следующих рассуждениях.

$$
\begin{aligned}
h_{11}^{\alpha} &= 1+b+a = n, & h_{11}^{\beta} &= 3+b+c+d = a,\\
h_{12}^{\alpha} &= a = 3+b+c+d, & h_{12}^{\beta} &= 2+b+c,\\
h_{13}^{\alpha} &= a-1 = 2+b+c+d, & h_{13}^{\beta} &= 1+b+c,\\
h_{14}^{\alpha} &= a-2 = 1+b+c+d, & h_{14}^{\beta} &= b+c,\\
h_{21}^{\alpha} &= b, & h_{21}^{\beta} &= 2+b+d.
\end{aligned}
$$

Очевидно, что H_{13}^{α} — единственный крюк длины $a-1$ в $[\alpha]$, причём диаграмма $[\alpha^{13}]$ не самоассоциирована. По лемме 3.4 отсюда следует, что $[\beta]$ имеет крюк длины $a-1 = 2+b+c+d$. Отсюда и из списка длин крюков видно, что

$$\mathrm{H}^{\beta}(a-1) \subseteq \{H_{12}^{\beta}, H_{21}^{\beta}\} \ \text{ и } \ cd = 0. \tag{4.4}$$

С л у ч а й В1.1. Предположим сначала, что $c = d = 0$. Тогда $\mathrm{H}^{\alpha,\beta}(a-1) = \{H_{13}^{\alpha}, H_{12}^{\beta}, H_{21}^{\beta}\}$, откуда по лемме 3.3 и (4.3)

$$\chi^{\alpha^{13}} \sim -\chi^{\beta^{12}} + \chi^{\beta^{21}} \quad \text{на} \quad S_{2+b}^{\delta} \quad \text{при} \quad \delta = (-1)^a \varepsilon = (-1)^{1+b}.$$

Но это противоречиво, так как для элемента $g = g_{(b,1,1)}$ (имеющего знак δ) с помощью предложения 1.2 получаем: $\chi^{\alpha^{13}} = \chi^{(2,1^b)}(g) = (-1)^{b-1}$ и $-\chi^{\beta^{12}}(g)+\chi^{\beta^{21}}(g) = -\chi^{(1+b,1)}(g)+\chi^{(2+b)}(g) = -1+1 = 0$.

С л у ч а й B1.2. Теперь пусть $c = 0$ и $d \neq 0$. Тогда H^{α}_{13} и H^{β}_{21} — единственные крюки длины $a-1 = 2+b+d$ в $[\alpha]$ и $[\beta]$ соответственно, откуда по лемме 3.5 и (4.3)

$$\chi^{\alpha^{13}} \sim \chi^{\beta^{21}} \ \text{ на } \ S^{\delta}_{2+b}, \text{ где } \ \delta = (-1)^a\varepsilon = (-1)^{1+b}. \tag{4.5}$$

Так как $\alpha^{13} = (2,1^b)$, $\beta^{21} = (2+b)$ и в рассматриваемом случае $b \geq 2$, то по лемме 3.8 должно быть $\alpha^{13} = (3,1)'$ и $\beta^{21} = (4)$, т. е.

$$b = 2, \ \alpha = (6+d, 1^2), \ \beta = (4,4,1^d) \ \text{ и } \ \varepsilon = (-1)^d.$$

Если $d \geq 3$, то $[\beta]$ не имеет крюков длины $2+d$, а $[\alpha]$ имеет единственный крюк такой длины: H^{α}_{15}. По лемме 3.4 должно быть $\alpha^{15} = (\alpha^{15})'$, что противоречиво, так как $\alpha^{15} = (4,1^2)$. Поэтому $d \in \{1,2\}$.

Если $d = 2$, то характеры $\chi^{\alpha} = \chi^{(8,1^2)}$ и $\chi^{\beta} = \chi^{(4,4,1^2)}$ принимают на элементе $g_{(5,5)} \in S^{\varepsilon}_{10}$ значения 1 и 0 (так как в $[\beta]$ нет крюка длины 5) соответственно, что противоречит (4.5).

Следовательно, $d = 1$, а тогда $\alpha = (7,1^2)$, $\beta = (4,4,1)$ и $\varepsilon = -1$, т. е. верно утверждение (6) теоремы 4.1.

С л у ч а й B1.3. Пусть, наконец (ввиду (4.4)), $d = 0$ и $c \neq 0$. Предположим, что $c \geq 2$. Тогда H^{α}_{14} и H^{β}_{13} — единственные крюки длины $a-2 = 1+b+c$ в $[\alpha]$ и $[\beta]$ соответственно, и по лемме 3.5

$$\chi^{\alpha^{14}} \sim \chi^{\beta^{13}} \ \text{ на } \ S^{\delta}_{3+b}, \text{ где } \ \delta = (-1)^{a-1}\varepsilon = (-1)^b. \tag{4.6}$$

При этом $\alpha^{14} = (3,1^b)$ и $\beta^{13} = (1+b,2)$. Но, как легко проверить, характеры $\chi^{(3,1^b)}$ и $\chi^{(1+b,1)}$ принимают на элементе $g_{(b+1,1^2)} \in S^{\delta}_{3+b}$ значения 0 и -1 соответственно. Это противоречит (4.6).

Следовательно, $c = 1$. Тогда $n = 5+2b$, $\varepsilon = -1$ по (4.3) и $\mathrm{H}^{\alpha,\beta}(2+b) = \{H^{\alpha}_{14}, H^{\beta}_{13}, H^{\beta}_{21}\}$. По лемме 3.3

$$\chi^{\alpha^{14}} \sim -\chi^{\beta^{13}} + \chi^{\beta^{21}} \ \text{ на } \ S^{\delta}_{3+b}, \ \text{ где } \ \delta = (-1)^{1+b}\varepsilon = (-1)^b. \tag{4.7}$$

Здесь $\alpha^{14} = (3,1^b)$, $\beta^{13} = (1+b,2)$ и $\beta^{21} = (3+b)$. С помощью предложения 1.2 при $g = g_{(b+1,1^2)} \in S^{\delta}_{3+b}$ получаем: $\chi^{\alpha^{14}}(g) = 0$, так как $\alpha^{14} = (3,1^b)$ не имеет крюков длины $b+1$, в то время как $-\chi^{\beta^{13}}(g) + \chi^{\beta^{21}}(g) = -\chi^{(1+b,2)}(g) + \chi^{(3+b)}(g) = 2 \neq 0$. Это противоречит (4.7).

Итак, в случае B1 верно утверждение (6) заключения доказываемой теоремы.

С л у ч а й B2. Пусть $\alpha =' (1+a, 1^b)$ и $\beta =' (1+b+c, 1+b, 2, 1^d)$, где $b \geq 2$, $c+d = a-b-3 \geq 0$.

Без ограничения общности можно считать, что диаграммы $[\alpha]$ и $[\beta]$ в этом случае имеют вид, изображённый на рис. 4.2 ($\{a,b,c,d\} \subseteq \mathbb{N} \cup \{0\}$).

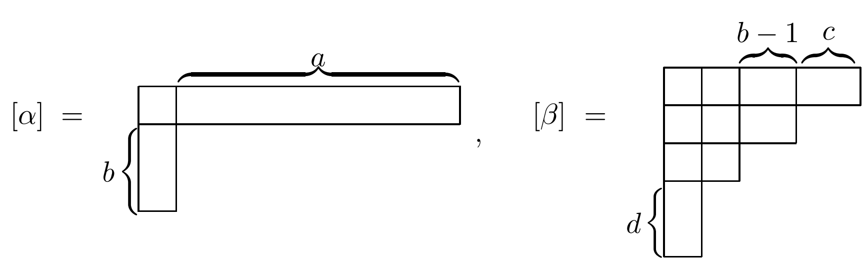


Рис. 4.2

Подсчитаем длины некоторых крюков $[\alpha]$ и $[\beta]$.

$$\begin{aligned}
&h_{11}^{\alpha} = 1+b+a = n, && h_{11}^{\beta} = 3+b+c+d = a,\\
&h_{12}^{\alpha} = a = 3+b+c+d, && h_{12}^{\beta} = 2+b+c,\\
&h_{13}^{\alpha} = a-1 = 2+b+c+d, && h_{13}^{\beta} = b+c,\\
&h_{14}^{\alpha} = a-2 = 1+b+c+d, && \\
&h_{21}^{\alpha} = b, && h_{21}^{\beta} = 2+b+d.
\end{aligned}$$

Согласно (4.3)

$$\varepsilon = (-1)^n = (-1)^{1+a+b} = (-1)^{c+d}. \tag{4.8}$$

Так как H_{12}^{α} и H_{11}^{β} — единственные крюки длины $a = 3+b+c+d$ в $[\alpha]$ и $[\beta]$ соответственно, то по лемме 3.5

$$\chi^{\alpha^{12}} \sim \chi^{\beta^{11}} \ \text{ на } \ S_{1+b}^{\delta}, \ \text{ где } \ \delta = (-1)^{a+1}\varepsilon = (-1)^b. \tag{4.9}$$

Так как $\alpha^{12} = (1^{1+b})$ и $\beta^{11} = (b,1)$, то по лемме 3.8 отсюда следует, что

$$b \in \{2,3\}. \tag{4.10}$$

Очевидно, что H_{13}^{α} — единственный крюк длины $a-1$ в $[\alpha]$, причём диаграмма $[\alpha^{13}]$ не самоассоциирована, так как $b \geq 2$. По лемме 3.4 отсюда следует, что $[\beta]$ имеет крюк длины $a-1 = 2+b+c+d$. Отсюда и из списка длин крюков в β видно, что

$$\mathrm{H}^{\beta}(a-1) \subseteq \{H_{12}^{\beta}, H_{21}^{\beta}\} \ \text{ и } \ cd = 0. \tag{4.11}$$

С л у ч а й B2.1. Предположим, что $c = d = 0$. Если $b = 3$, то $a = 6$, $n = 10$, $\alpha = (7,1^3)$, $\beta = (4,4,2)$ и по (4.8) $\varepsilon = 1$. Но это противоречиво, так как здесь $\chi^{\alpha}(g_{(5,2^2,1)}) = 0$, а $\chi^{\beta}(g_{(5,2^2,1)}) = -2 \neq 0$.

Следовательно, по (4.10) $b = 2$, $n = 8$, $\alpha = (6,1^2)$, $\beta = (3,3,2)$ и $\varepsilon = 1$. Мы получили утверждение (5) теоремы.

С л у ч а й B2.2. Теперь пусть $d = 0$ и $c \neq 0$. Тогда (см. (4.11)) H_{13}^{α} и H_{12}^{β} — единственные крюки длины $a-1 = 2+b+c$ в $[\alpha]$ и $[\beta]$ соответственно, и по лемме 3.5

$$\chi^{\alpha^{13}} \sim \chi^{\beta^{12}} \ \text{ на } \ S_{2+b}^{\delta}, \ \text{ где } \ \delta = (-1)^a\varepsilon = (-1)^{1+b}.$$

Так как $\alpha^{13} = (2,1^b)$ и $\beta^{12} = (b,1^2)$, то отсюда по лемме 3.8 следует, что $\alpha^{13} = (\beta^{12})'$, т. е.

$$b = 2, \ \alpha =' (6+c,1^2), \ \beta =' (3+c,3,2), \ \varepsilon = (-1)^c \tag{4.12}$$

(последнее равенство следует из (4.8)). Если $c > 1$, то для элемента $g = g_{(3+c,1^5)}$, лежащего, очевидно, в S_n^{ε}, имеем $\chi^{\alpha}(g) = \chi^{\alpha^{14}}(1) = 6 \neq 0$ и $\chi^{\beta}(g) = 0$ (так как при $c > 1$ в $[\beta]$ нет крюка длины $3+c$), что противоречит условию теоремы. Следовательно, $c = 1$ и $\varepsilon = -1$. Но это также противоречиво, так как тогда $\chi^{\alpha}(g_{(4,3,1^2)}) = 0$ и $\chi^{\beta}(g_{(4,3,1^2)}) = -1$.

С л у ч а й B2.3. Пусть, наконец, $c = 0$ и $d \neq 0$. Тогда $\beta =' (1+b,1+b,2,1^d)$.

(Хотя здесь $\mathrm{H}^{\alpha,\beta}(a-1) = \{H_{13}^{\alpha}, H_{21}^{\beta}\}$, из этого ничего не извлечёшь, поскольку $\alpha^{13} =' \beta^{21}$.) Если $d > 1$, то $[\beta]$ не имеет крюков длины $1+b+d = h_{21}^{\beta} - 1$ (большей, чем $h_{12}^{\beta} = 2+b$ и чем $h_{31}^{\beta} = 2+d$), а $[\alpha]$ имеет единственный крюк такой длины: H_{14}^{α}. По лемме 3.4 должно быть $\alpha^{14} = (\alpha^{14})'$ и $\varepsilon = (-1)^{1+b+d}$. Так как $\alpha^{14} = (3,1^b)$, то должно быть $b = 2$ и, значит, $\varepsilon = (-1)^{1+d}$. Но это противоречиво, так как по (4.8) $\varepsilon = (-1)^{c+d} = (-1)^d$.

Следовательно, $d = 1$, $\alpha = (5+b,1^b)$, $\beta = (1+b,1+b,2,1)$, $\varepsilon = -1$ и по (4.10) $b \in \{2,3\}$. Случай $b = 2$ противоречив, так как тогда при $g = g_{(4,3,1^2)}$ имеем $\chi^{\alpha}(g) = \chi^{(7,1^2)}(g) = 0$ и

$\chi^\beta(g) = \chi^{(3,3,2,1)}(g) = 1$. Поэтому $b = 3$, и тогда $\alpha = (8, 1^3)$, $\beta = (4, 4, 2, 1)$ и $\varepsilon = -1$, т. е. верно утверждение (7) теоремы.

Таким образом, в случае В2 верно одно из условий (5) и (7) заключения теоремы.

Итак, мы доказали, что если тройка α, β, ε удовлетворяет условию теоремы, то для неё верно одно из утверждений (1)–(7) заключения теоремы.

Обратное утверждение легко получается из рассмотрения таблиц характеров групп S_n при $n \leq 11$ (или с помощью лёгких вычислений, использующих предложение 1.2).

Теорема 4.1 доказана.

5. $\chi^\alpha \sim \chi^\beta$ на S_n^ε. Случай $d(\beta) = d(\alpha) = 2$ и $h_{11}^\alpha > h_{11}^\beta$

В этом и следующем параграфах мы найдём все тройки $(\alpha, \beta, \varepsilon)$ такие, что $\chi^\alpha \sim \chi^\beta$ на S_n^ε и $d(\beta) = d(\alpha) = 2$, при естественном ограничении, что χ^α и χ^β не исчезают тождественно на S_n^ε. В этом параграфе мы примем условие $h_{11}^\alpha > h_{11}^\beta$, а в следующем — условие $h_{11}^\alpha = h_{11}^\beta$. В первом случае по теореме 2.1 должно быть верно её условие (2), и мы можем использовать следующее

Предложение 5.1 [10, предложение 5.1]. *Пусть $\alpha, \beta \in P(n)$, $\alpha \neq' \beta$ и*

$$f(\alpha) = f(\beta), \quad f'(\alpha) = f'(\beta) \tag{5.1}$$

(следовательно, $\alpha \neq \alpha'$, $\beta \neq \beta'$ и $n \geq 4$). Пусть $|\alpha^1| \leq |\beta^1|$. Тогда $d(\alpha) = d(\beta) \geq 2$ и справедливо одно из следующих утверждений (в которых $a, b, c, d \in \mathbb{N} \cup \{0\}$):

(1) $\alpha =' (2 + a, 2, 1^b)$ и $\beta =' (3 + b + c, 3 + b, 1^d)$, где $a > b$, $c + d = a - b - 2$, и выполнено одно из условий:

(1а) $b \geq 2$;

(1б) $b = 1$, $a \geq 5$ и $\beta =' (5, 4, 1^{a-4})$;

(1в) $b = 0$, $a \geq 4$ и $\beta =' (4, 3, 1^{a-3})$;

(1г) $b = 0$, $a \geq 3$ и $\beta =' (1 + a, 3)$

(во всех пунктах утверждения (1) $|\alpha^1| = 1$ и $\beta^1 \neq (\beta^1)'$);

(2) $|\alpha^1| > 1$, $h_{11}^\alpha = h_{11}^\beta$ и выполнено одно из условий:

(2а) $|\alpha^1| = |\beta^1| \geq 4$, $f(\alpha^1) = f(\beta^1)$ и $f'(\alpha^1) = f'(\beta^1)$;

(2б) $\{\alpha, \beta\} =' \{(5 + a, 4, 1), (6, 4, 1^a)\}$, где $a \geq 2$;

(2в) $\{\alpha, \beta\} =' \{(4 + a, 3), (4, 3, 1^a)\}$, где $a \geq 1$

(во всех пунктах утверждения (2) $\alpha^1 \neq (\alpha^1)'$ и $\beta^1 \neq (\beta^1)'$);

(3) $|\alpha^1| > 1$, $h_{11}^\alpha > h_{11}^\beta$, $\alpha^1 = (\alpha^1)'$, $\beta^1 \neq (\beta^1)'$, $f(\alpha^2) = f(\beta^1)$ и $f'(\alpha^2) = f'(\beta^1)$; если, кроме того, $(\beta^1)^1 = ((\beta^1)^1)'$, то $\beta^1 =' \alpha^2$.

Обратно, для любых α, β из пунктов (1)–(3) выполнено условие (5.1).

Теорема 5.1. *Пусть χ^α и χ^β — неприводимые характеры группы S_n, имеющие одни и те же корни на S_n^ε при некотором $\varepsilon = \pm 1$, но не исчезающие тождественно на S_n^ε. Предположим, что $d(\alpha) = d(\beta) = 2$ и $h_{11}^\alpha > h_{11}^\beta$.*

Тогда верно одно из следующих утверждений:

(1) $n = 7$, $\alpha =' (5, 2)$, $\beta =' (4, 3)$, $\varepsilon = +1$;

(2) $n = 8$, $\alpha =' (6, 2)$, $\beta =' (5, 3)$, $\varepsilon = -1$;

(3) $n = 10$, $\alpha =' (7, 2, 1)$, $\beta =' (5, 4, 1)$, $\varepsilon = -1$;

(4) $n = 11$, $\alpha =' (6, 3, 2)$, $\beta =' (5, 4, 2)$, $\varepsilon = +1$;

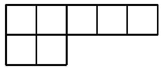
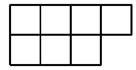
(5) $n = 14$, $\alpha =' (9, 3, 2)$, $\beta =' (6, 3, 2^2, 1)$, $\varepsilon = -1$;

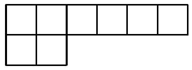
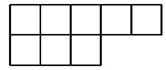
(6) $n = 14$, $\alpha =' (8, 3, 2, 1)$, $\beta =' (6, 5, 2, 1)$, $\varepsilon = -1$;

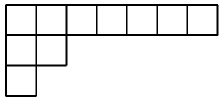
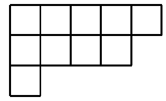
(7) $n = 16$, $\alpha =' (8, 4, 2^2)$, $\beta =' (7, 5, 2^2)$, $\varepsilon = -1$.

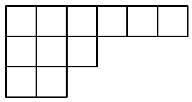
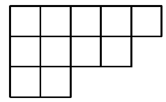
Обратно, в каждом из пунктов (1)–(7) выполнены условия теоремы.

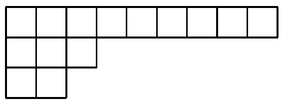
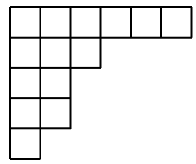
Приведем диаграммы $[\alpha]$ и $[\beta]$ в каждом из случаев (1)–(7):

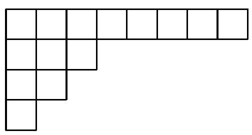
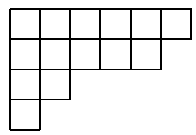
(1) $[\alpha] =$  , $[\beta] =$  , $\varepsilon = +1$,

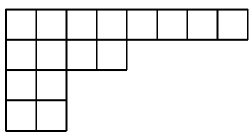
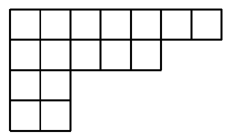
(2) $[\alpha] =$  , $[\beta] =$  , $\varepsilon = -1$,

(3) $[\alpha] =$  , $[\beta] =$  , $\varepsilon = -1$,

(4) $[\alpha] =$  , $[\beta] =$  , $\varepsilon = +1$,

(5) $[\alpha] =$  , $[\beta] =$  , $\varepsilon = -1$,

(6) $[\alpha] =$  , $[\beta] =$  , $\varepsilon = -1$,

(7) $[\alpha] =$  , $[\beta] =$  , $\varepsilon = -1$.

Д о к а з а т е л ь с т в о. Пусть выполнено условие теоремы 5.1. Тогда, как замечено в начале этого параграфа, верно утверждение (2) теоремы 2.1, т. е.

$$f(\alpha) = f(\beta),\ \ f'(\alpha) = f'(\beta),\ \text{и}\ \ \varepsilon = \operatorname{sign}(f(\alpha)) = (-1)^{n-1} \tag{5.2}$$

(последнее равенство следует из того, что по предложению 2.2 $l(f(\alpha)) = d(\alpha)+1 = 3$), причём из неравенства $h_{11}^{\alpha} > h_{11}^{\beta}$ следует, что

$$|\alpha^1| < |\beta^1|.$$

Поэтому верно одно из утверждений (1) и (3) предложения 5.1.

С л у ч а й 1. Пусть $|\alpha^1| = 1$.

Тогда согласно утверждению (1) предложения 5.1 $\alpha =' (2+a, 2, 1^b)$ и $\beta =' (3+b+c, 3+b, 1^d)$, где $a, b, c, d\ \in \mathbb{N} \cup \{0\}$. Не ограничивая общности, мы можем считать, что диаграммы $[\alpha]$ и $[\beta]$ имеют вид, изображённый на рис. 5.1.

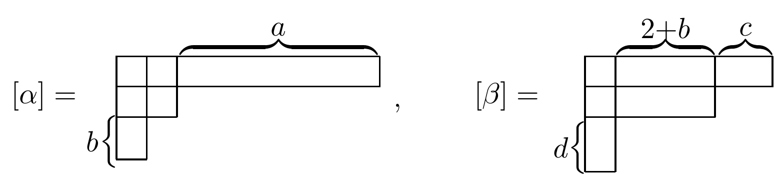


Рис. 5.1

Здесь $n = 4 + a + b = 6 + 2b + c + d$, откуда

$$a = 2 + b + c + d. \tag{5.3}$$

Подсчитаем длины некоторых крюков в $[\alpha]$ и $[\beta]$.

$$\begin{aligned} &h^{\alpha}_{11} = 3 + b + a, && h^{\beta}_{11} = 4 + b + c + d,\\ &h^{\alpha}_{12} = 2 + a = 4 + b + c + d, && h^{\beta}_{12} = 3 + b + c,\\ &h^{\alpha}_{13} = a = 2 + b + c + d, && h^{\beta}_{13} = 2 + b + c,\\ &h^{\alpha}_{21} = 2 + b, && h^{\beta}_{21} = 3 + b + d,\\ &h^{\alpha}_{22} = 1, && h^{\beta}_{22} = 2 + b. \end{aligned}$$

С л у ч а й 1.1. Предположим, что $b \geq 2$.

Если $c = d = 0$, то H^{β}_{12} и H^{β}_{21} — единственные крюки длины $3 + b = 1 + a$ в $[\beta]$, а в $[\alpha]$ нет крюков такой длины. По лемме 3.7 должно быть либо $\beta^{12} = (\beta^{21})'$, либо β^{12} и β^{21} самоассоциированы. Из рис. 5.1 видно, что это не верно. Следовательно, $c + d > 0$.

Если $c = 0$ и $d \neq 0$, то H^{β}_{21} — единственный крюк длины $3 + b + c = 1 + a$ в $[\beta]$, а в $[\alpha]$ нет крюков такой длины. По лемме 3.3 должно быть $\beta^{21} = (\beta^{21})'$, но это противоречиво.

Если же $c \neq 0$ и $d = 0$, то H^{β}_{12} — единственный крюк длины $3 + b = 1 + a$ в $[\beta]$, а в $[\alpha]$ нет крюков такой длины. По лемме 3.4 должно быть $\beta^{12} = (\beta^{12})'$, но это противоречиво.

Таким образом,

$$c \geq 1, \;\; d \geq 1. \tag{5.4}$$

Отсюда и из (5.3) следует, что H^{α}_{13} — единственный крюк длины a в $[\alpha]$. Так как $\alpha^{13} \neq (\alpha^{13})'$, то по лемме 3.4 $[\beta]$ имеет крюк длины $a = 2 + b + c + d$. Из таблицы длин крюков в $[\beta]$ и (5.4) видно, что a может совпадать лишь с h^{β}_{12} или с h^{β}_{21} и, следовательно, возможны лишь следующие случаи:

(а) $\mathrm{H}^{\beta}(a) = \{H^{\beta}_{12}\}$, $\;d = 1$, $\;c \geq 2$;

(б) $\mathrm{H}^{\beta}(a) = \{H^{\beta}_{21}\}$, $\;c = 1$, $\;d \geq 2$;

(в) $\mathrm{H}^{\beta}(a) = \{H^{\beta}_{12}, H^{\beta}_{21}\}$, $\;c = d = 1$.

В случае (а) H^{α}_{13} и H^{β}_{12} — единственные крюки длины a в $[\alpha]$ и $[\beta]$ соответственно. Тогда по лемме 3.5 и (5.2)

$$\chi^{\alpha^{13}} \sim \chi^{\beta^{12}} \;\text{ на }\; S^{\delta}_{4+b}, \;\text{ где }\; \delta = (-1)^{a+1}\varepsilon = (-1)^b.$$

Но это противоречиво, так как на элементе $g_{(b+3,1)}$ из S^{δ}_{4+b} характер $\chi^{\alpha^{13}} = \chi^{(2,2,1^b)}$ принимает значение $(-1)^{1+b}$, а характер $\chi^{\beta^{12}} = \chi^{(2+b,1,1)}$ — значение 0.

В случае (б) H^{α}_{13} и H^{β}_{21} — единственные крюки длины a в $[\alpha]$ и $[\beta]$ соответственно, и по лемме 3.5

$$\chi^{\alpha^{13}} \sim \chi^{\beta^{21}} \;\text{ на }\; S^{\delta}_{4+b}, \;\text{ где }\; \delta = \pm 1.$$

Так как $\beta^{21} = (4 + b)$, то по лемме 3.1 должно быть $\alpha^{13} \in' \{(2, 2), (3.3)\}$, что противоречиво (так как $b \geq 2$).

Следовательно, $\mathrm{H}^{\beta}(a) = \{H^{\beta}_{12}, H^{\beta}_{21}\}$ и $c = d = 1$. Тогда по лемме 3.3

$$\chi^{\alpha^{13}} \sim \chi^{\beta^{12}} + \chi^{\beta^{21}} \;\text{ на }\; S^{\delta}_{4+b}, \;\text{ где }\; \delta == (-1)^{a+1}\varepsilon = (-1)^b.$$

Но это противоречиво, так как на элементе $g_{(b+1,3)}$ из S^{δ}_{4+b} характер $\chi^{\alpha^{13}}$ принимает значение 0, а $\chi^{\beta^{12}} + \chi^{\beta^{21}}$ — значение $1 + 1 = 2$.

Таким образом, случай 1.1 противоречив.

С л у ч а й 1.2. Пусть $b = 0$.

Тогда выполнено одно из условий (1в), (1г) предложения 5.1.

Предположим сначала, что выполнено условие (1г).
Можно считать, что $\alpha = (2+a, 2)$ и $\beta = (1+a, 3)$, где $a \geq 3$. При $a = 3$ получаем условие (1) теоремы: $\alpha = (5,2), \beta = (4,3)$ и $\varepsilon = 1$ (последнее равенство следует из (5.2)). При $a = 4$ получаем условие (2) теоремы. Наконец, условие $a \geq 5$ противоречиво, так как тогда H^{α}_{14} — единственный крюк длины $a-1$ в $[\alpha]$, а в $[\beta]$ нет крюков такой длины, и по лемме 3.4 должно быть $\alpha^{14} =' \alpha^{14}$, что не так.

Предположим теперь, что выполнено условие (1в).
Можно считать, что $\alpha = (2+a, 2)$ и $\beta = (4, 3, 1^{a-1})\}$, где $a \geq 4$. Пусть $a \geq 6$. Тогда H^{α}_{14} — единственный крюк длины $a-1$ в $[\alpha]$, а в $[\beta]$ нет крюков такой длины, и по лемме 3.4 должно быть $\alpha^{14} =' \alpha^{14}$, что не так. Пусть $a = 5$. Тогда H^{α}_{14} и H^{β}_{12} — единственные крюки длины $a - 1 = 4$ в $[\alpha]$ и $[\beta]$ соответственно. По лемме 3.5

$$\chi^{\alpha^{14}} \sim \chi^{\beta^{12}} \ \text{ на } \ S_5^{\delta}, \ \delta = \pm 1.$$

Но это противоречиво, так как на элементах $g_{(4,1)}$ и $g_{(5)}$ характер $\chi^{\alpha^{14}} = \chi^{(3,2)}$ принимает значения -1 и 0, а $\chi^{\beta^{12}} = \chi^{(2,1^3)}$ — значения 0 и -1 соответственно. Пусть, наконец, $a = 4$. Тогда характеры $\chi^{\alpha} = \chi^{(6,2)}$ и $\chi^{\beta} = \chi^{(4,3,1)}$ на элементах $g_{(7,1)}$ и $g_{(4,2^2)}$ принимают значения $-1, 2$ и $0, 0$ соответственно. Следовательно, условие (1в) противоречиво.

Таким образом, в случае 1.2 верно одно из утверждений (1), (2) доказываемой теоремы.

С л у ч а й 1.3. Пусть $b = 1$. Тогда выполнено условие (1б) предложения 5.1.

Можно считать, что $\alpha = (6+d, 2, 1)$ и $\beta = (5, 4, 1^d)\}$, где $d \geq 1$. Кроме того, по (5.2) $\varepsilon = (-1)^d$. Пусть $d \geq 4$. Тогда H^{α}_{15} — единственный крюк длины $2+d$ в $[\alpha]$, а в $[\beta]$ нет крюков такой длины, и по лемме 3.4 должно быть $\alpha^{15} = (\alpha^{15})'$, что не так. Случай $d = 3$ противоречив, так как тогда $\alpha = (9,2,1)$, $\beta = (5,4,1^3)\}$, $\varepsilon = -1$, и характеры χ^{α} и χ^{β} на элементе $g_{(6,5,1)}$ принимают значения 1 и 0 соответственно. Если же $d = 2$, то $\alpha = (8,2,1)$, $\beta = (5,4,1^2)\}$, $\varepsilon = 1$, и характеры χ^{α} и χ^{β} на элементе $g_{(5^2,1)}$ принимают значения 1 и 0 соответственно, что противоречиво. Наконец, при $d = 1$ мы получаем условие (3) теоремы.

Таким образом, в случае 1 верно одно из утверждений (1)–(3) теоремы.

С л у ч а й 2. Пусть $|\alpha^1| > 1$.

Тогда верно утверждение (3) предложения 5.1. В частности, $\alpha^1 = (\alpha^1)'$, $\beta^1 \neq (\beta^1)'$,

$$f(\alpha^2) = f(\beta^1), \ f'(\alpha^2) = f'(\beta^1), \ \beta^1 =' \alpha^2 \tag{5.5}$$

(последнее равенство следует из того, что $(\beta^1)^1 = () = ()'$). Поэтому, не ограничивая общности, мы можем считать, что диаграммы $[\alpha]$ и $[\beta]$ имеют вид, изображённый на рис. 5.2, где a, b, c, d, $s \in \mathbb{N} \cup \{0\}$, $s \geq 1$ и $a > b$ (здесь $\alpha^1 = (1+s, s)$ и $\beta^1 = (\alpha^2)' = (2+s+b, 1^s)$).

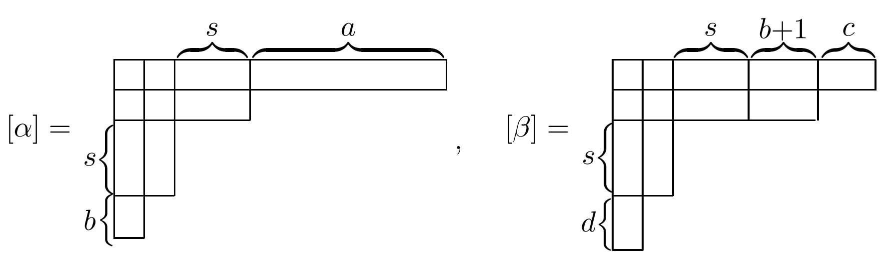


Рис. 5.2

Из равенства мощностей диаграмм $[\alpha]$ и $[\beta]$ имеем:

$$n = 4 + 4s + b + a = 6 + 4s + 2b + c + d, \tag{5.6}$$

откуда

$$a = 2 + b + c + d. \tag{5.7}$$

(Это следует также из равенства $h^{\alpha}_{12} = h^{\alpha}_{2} = h^{\beta}_{11}$, вытекающего из (5.5).) Из (5.2) и (5.6) получаем
$$\varepsilon = (-1)^{1+b+a} = (-1)^{1+c+d}. \tag{5.8}$$

Подсчитаем (учитывая (5.7)) длины некоторых крюков, которые будут фигурировать в следующих рассуждениях.

$$\begin{aligned}
h^{\alpha}_{11} &= 5+2s+2b+c+d, & h^{\beta}_{11} &= 4+2s+b+c+d,\\
h^{\alpha}_{12} &= 4+2s+b+c+d, & h^{\beta}_{12} &= 3+2s+b+c,\\
h^{\alpha}_{13} &= 3+s+b+c+d, & h^{\beta}_{13} &= 2+s+b+c,\\
h^{\alpha}_{21} &= 2+2s+b, & h^{\beta}_{21} &= 3+2s+b+d,\\
h^{\alpha}_{22} &= 1+2s, & h^{\beta}_{22} &= 2+2s+b,\\
h^{\alpha}_{31} &= 1+s+b, & h^{\beta}_{31} &= 1+s+d.
\end{aligned}$$

Этот список нужно иметь в виду, когда далее в случае 2 будут устанавливаться какие-либо соотношения между длинами крюков.

При проведении следующих рассуждений полезно иметь перед глазами некоторые “остаточные диаграммы” для $[\alpha]$ и $[\beta]$; см. рис. 5.3.

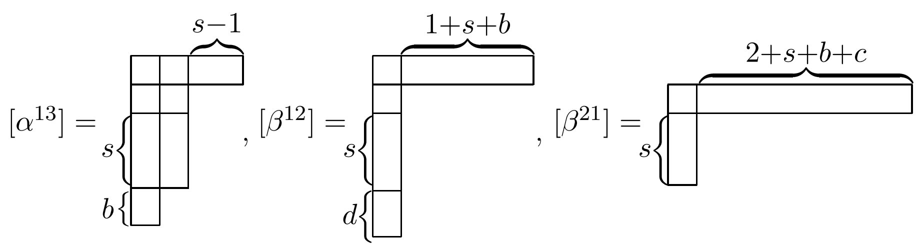


Рис. 5.3

Предположим, что $c = d$. Тогда
$$\mathrm{H}^{\beta}(h^{\beta}_{12}) = \{H^{\beta}_{12}, H^{\beta}_{21}\}. \tag{5.9}$$

Если $[\alpha]$ не имеет крюков длины $h^{\beta}_{12} = h^{\beta}_{21}$, то по лемме 3.7 должно быть либо $\beta^{12} =' \beta^{21}$, либо разбиения β^{12} и β^{21} оба самоассоциированы. Однако ни одно из этих условий не верно. Следовательно, $[\alpha]$ имеет крюк длины h^{β}_{12}. Таким крюком может быть только крюк H^{α}_{13}, так как $h^{\alpha}_{21} < h^{\beta}_{12} < h^{\alpha}_{12}$. Отсюда и из (5.9) получаем:
$$\mathrm{H}^{\alpha,\beta}(h^{\beta}_{12}) = \{H^{\alpha}_{13}, H^{\beta}_{12}, H^{\beta}_{21}\}. \tag{5.10}$$

Кроме того, из равенства $h^{\alpha}_{13} = h^{\beta}_{12} = h^{\beta}_{21}$ следует, что
$$c = d = s.$$

Из (5.10) по лемме 3.3 получаем (с учётом предыдущего равенства)
$$\chi^{\alpha^{13}} \sim (-1)^{1+s}\chi^{\beta^{12}} + \chi^{\beta^{21}} \quad \text{на} \quad S^{\delta}_{m}, \tag{5.11}$$
где $m = 3+2s+b+c$ и $\delta = (-1)^{h^{\alpha}_{13}+1}\varepsilon = (-1)^{1+s+b}$ (по (5.8)).

Предположим, что $s > 1$. Тогда $h^{\alpha}_{14} = 1+b+3s$ и $\mathrm{H}^{\alpha,\beta}(1+b+23) = \{H^{\alpha}_{14}\}$. Отсюда по лемме 3.4 следует, что $\alpha^{14} = (\alpha^{14})'$. Но это невозможно, так как при $s > 1$ $\alpha^{14} = (2+s, 3, 2^s, 1^b)$. Следовательно,
$$c = d = s = 1 \tag{5.12}$$

и соотношение (5.11) имеет вид

$$\chi^{\alpha^{13}} \sim \chi^{\beta^{12}} + \chi^{\beta^{21}} \quad \text{на} \quad S^{\delta}_{6+b}, \quad \text{где} \quad \delta = (-1)^b. \tag{5.13}$$

Вычислим значения левой и правой частей этого соотношения на элементе $x := g_{(1+b,1^5)}$ знака δ (используя рис. 5.3 и (5.12)). Если $b > 2$, то диаграмма α^{13} не имеет крюка длины $1+b$ и потому по предложению 1.2 $\chi^{\alpha^{13}}(x) = 0$. Но значение правой части рассматриваемого соотношения на x равно (снова по предложению 1.2) $\chi^{(4,1)'}(1) + \chi^{(4,1)}(1) \neq 0$. Следовательно, $b \leq 2$. При $b = 0$ значения левой и правой частей соотношения (5.13) на элементе $g_{(3,3)}$ знака δ $(= 1)$ равны соответственно 2 и 0, а при $b = 2$ значения этих частей на элементе $g_{(4,4)}$ знака δ равны соответственно 0 и -2. Оба случая противоречивы. Поэтому $b = 1$, $\alpha = (8,3,2,1)$, $\beta = (6,5,2,1)$, $\delta = -1$.

Таким образом, при $c = d$ верно утверждение (6) теоремы и далее мы будем считать, что

$$c \neq d. \tag{5.14}$$

Предположим, что $h^{\alpha}_{13} \leq h^{\alpha}_{21}$, т. е. $1 + c + d \leq s$.
Тогда число $h^{\beta}_{21} = 3{+}2s{+}b{+}d$ меньше, чем h^{α}_{12}, но больше, чем $h^{\alpha}_{21} = 2{+}2s{+}b$, и, следовательно, чем h^{α}_{13}. Поэтому

$$[\alpha] \text{ не имеет крюков длины } h^{\beta}_{21}. \tag{5.15}$$

Покажем, что H^{β}_{21} — единственный крюк длины h^{β}_{21} в $[\beta]$. Если $d > c$, то это очевидно, так как тогда $h^{\beta}_{21} > h^{\beta}_{12}$. Если же $c \geq d$ и, следовательно, ввиду (5.14) $c > d$, то $h^{\beta}_{12} > h^{\beta}_{21} > h^{\beta}_{13}$ (второе неравенство следует из того, что $s \geq 1 + c + d$), и поэтому снова H^{β}_{21} — единственный крюк длины h^{β}_{21} в $[\beta]$. Отсюда и из (5.15) по лемме 3.4 следует, что разбиение β^{21} должно быть самоассоциированным. Но это противоречиво, так как $\beta^{21} = (3 + s + b + c, 1^s)$.

Таким образом, предположение $h^{\alpha}_{13} \leq h^{\alpha}_{21}$ противоречиво, и, следовательно,

$$h^{\alpha}_{13} > h^{\alpha}_{21}, \quad \text{т. е.} \quad c + d \geq s. \tag{5.16}$$

Тогда, очевидно,

$$H^{\alpha}_{13} \text{ — единственный крюк длины } h^{\alpha}_{13} \text{ в } [\alpha]. \tag{5.17}$$

Предположим, что в $[\beta]$ нет крюка длины h^{α}_{13}. Тогда по лемме 3.4 должно быть $\alpha^{13} = (\alpha^{13})'$. Но это не так: $\alpha^{13} = (1 + s, 2^{1+s}, 1^b)$. Следовательно, $[\beta]$ имеет крюк такой длины.

Пусть $H = H^{\beta}_{ij}$ — некоторый крюк длины h^{α}_{13} в $[\beta]$. Тогда ввиду (5.16) $h^{\beta}_{ij} = h^{\alpha}_{13} = 3 + s + b + c + d > 2 + 2s + b = h^{\beta}_{22}$. Поэтому $i = 1$ или $j = 1$. Рассмотрим эти случаи отдельно.

С л у ч а й 2.1. Пусть $H = H^{\beta}_{1j}$.

Ясно, что $j \geq 2$, а так как $h^{\alpha}_{13} = 3 + s + b + c + d > h^{\beta}_{13}$, то

$$H = H^{\beta}_{12}.$$

Тогда $h^{\alpha}_{13} = h^{\beta}_{12}$, т. е. $3 + s + b + c + d = 3 + 2s + b + c$, откуда

$$d = s. \tag{5.18}$$

По (5.14) $c \neq d$. Если $d > c$, т. е. $h^{\beta}_{21} > h^{\beta}_{12}$, то H^{β}_{21} — единственный крюк длины h^{β}_{21} в $[\beta]$, а в $[\alpha]$ нет крюков такой длины ($h^{\alpha}_{12} > h^{\beta}_{21} > h^{\beta}_{12} = h^{\alpha}_{13} > h^{\alpha}_{21}$). Тогда по лемме 3.4 разбиение β^{21} должно быть самоассоциированным. Но это противоречиво, что видно из рис. 5.3. Следовательно, $c > d$, т. е. $h^{\beta}_{12} > h^{\beta}_{21}$. Тогда H^{α}_{13} и H^{β}_{12} — единственные крюки длины $m := h^{\alpha}_{13} = h^{\beta}_{12}$ в $[\alpha]$ и $[\beta]$ соответственно, и согласно лемме 3.5

$$\chi^{\alpha^{13}} \sim \chi^{\beta^{12}} \quad \text{на} \quad S^{\delta}_{n-m}, \quad \text{где} \quad \delta = \pm 1.$$

Рассмотрим диаграммы $[\alpha^{13}]$ и $[\beta^{12}]$ (рис 5.3). $[\alpha^{13}]$ имеет единственный крюк $H_{11}^{\alpha^{13}}$ длины $2+2s+b$, а в $[\beta^{12}]$ ввиду (5.18) нет крюков такой длины. Тогда по лемме 3.4 разбиение $\alpha^{13}-H_{11}^{\alpha^{13}}=(1^{1+s})$ должно быть самоассоциированным. Но это противоречиво, так как $s>0$. Следовательно, случай 2.1 невозможен.

С л у ч а й 2.2. Пусть $H=H_{i1}^{\beta}$.

Ясно, что $j\geq 2$, а так как $h_{13}^{\alpha}=3+s+b+c+d>h_{31}^{\beta}$, то

$$H=H_{21}^{\beta}.$$

Тогда $h_{13}^{\alpha}=h_{21}^{\beta}$, т. е. $3+s+b+c+d=3+2s+b+d$, откуда

$$c=s. \tag{5.19}$$

Так как $h_{21}^{\beta}=h_{13}^{\alpha}>h_{13}^{\beta}$ и $h_{21}^{\beta}\neq h_{12}^{\beta}$ по (5.14) ($c\neq d$), то H_{21}^{β} — единственный крюк длины h_{21}^{β} в $[\beta]$. Отсюда и из (5.17) по лемме 3.5

$$\chi^{\alpha^{13}}\sim\chi^{\beta^{21}} \quad \text{на} \quad S_{n-m}^{\delta}\,, \quad \text{где} \quad m=h_{13}^{\alpha} \quad \text{и} \quad \delta=(-1)^{m+1}\varepsilon.$$

Рассмотрим диаграммы $[\alpha^{13}]$ и $[\beta^{21}]$. Из рис 5.3 видно, что $[\alpha^{13}]$ и $[\beta^{21}]$ имеют точно по одному крюку длины $1+2s$, это — $H_{12}^{\alpha^{13}}$ и $H_{1k}^{\beta^{21}}$ с $k=3+b$ (ввиду (5.19)) соответственно. Поэтому по лемме 3.5, положив $\tilde{\alpha}=\alpha^{13}$ и $\tilde{\beta}=\beta^{21}$, имеем

$$\chi^{\tilde{\alpha}^{12}}\sim\chi^{\tilde{\beta}^{1k}} \quad \text{на} \quad S_{2+s+b}^{\theta}\,, \quad \text{где} \quad \theta=\pm 1.$$

Так как здесь $\tilde{\alpha}^{12}=(1^{2+s+b})$ и $\tilde{\beta}^{1k}=(2+b,1^{s})$, то по лемме 3.8 выполнено одно из следующих условий:

(а) $\tilde{\alpha}^{12}=(1^3)$, $\tilde{\beta}^{1k}=(2,1)$, $\theta=1$;

(б) $\tilde{\alpha}^{12}=(1^4)$, $\tilde{\beta}^{1k}=(3,1)$, $\theta=-1$;

(в) $\tilde{\alpha}^{12}=(1^4)$, $\tilde{\beta}^{1k}=(3,1)'$, $\theta=-1$.

С л у ч а й 2.2а. Пусть выполнено условие (а).

Тогда $b=0$, $s=c=1$, $a=3+d$ (использованы (5.19) и (5.7)) и диаграммы $[\alpha]$ и $[\beta]$ имеют вид, изображённый на рис. 5.4.

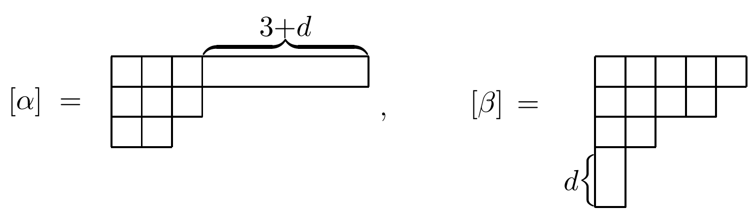


Рис. 5.4

Если $d>3$ или $d=2$, то H_{14}^{α} — единственный крюк длины $3+d$ в $[\alpha]$, а в $[\beta]$ нет крюков такой длины. Тогда по лемме 3.4 $\varepsilon=(-1)^{3+d}=(-1)^{1+d}$. Но это противоречит (5.8), согласно которому $\varepsilon=(-1)^{1+c+d}=(-1)^{d}$. Следовательно, $d\leq 3$ и $d\neq 2$. Кроме того, $d\neq 1$, так как $c\neq d$ по (5.14). Поэтому $d\in\{0,3\}$.

Если $d=0$, то $\alpha=(6,3,2)$, $\beta=(5,4,2)$, $\varepsilon=1$, $n=11$, т. е. верно утверждение (4) доказываемой теоремы.

Если $d=3$, то $\alpha=(9,3,2)$, $\beta=(6,3,2^2,1)$, $\varepsilon=-1$, $n=14$, т. е. верно утверждение (5) доказываемой теоремы.

С л у ч а й 2.2б. Пусть выполнено условие (б). Тогда $b=1$, $s=c=1$, $a=4+d$ и диаграммы $[\alpha]$ и $[\beta]$ имеют вид, изображённый на рис. 5.5.

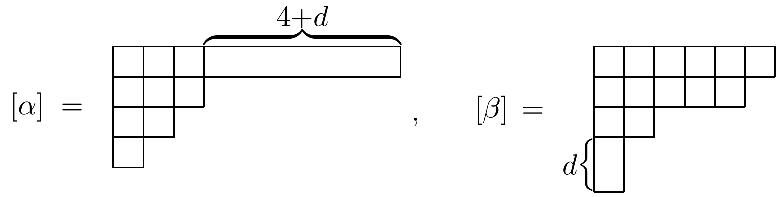


Рис. 5.5

Если $d > 3$ или $d = 2$, то, как видно из рис. 5.5, H^α_{14} есть единственный крюк длины $4 + d$ в $[\alpha]$, а в $[\beta]$ нет крюков такой длины. Тогда по лемме 3.4 должно быть $\alpha^{14} = (\alpha^{14})'$, что противоречиво. Следовательно, $d \leq 3$ и $d \neq 2$. Кроме того, $d \neq 1$, так как $c \neq d$ по (5.14). Поэтому $d \in \{0, 3\}$.

Если $d = 0$, то H^β_{12} есть единственный крюк длины 7 в $[\beta]$, а в $[\alpha]$ нет крюков такой длины. Тогда по лемме 3.4 должно быть $\beta^{12} = (\beta^{12})'$, что противоречиво, так как $\beta^{12} = (4, 1^2)$.

Если $d = 3$, то, как видно из рис. 5.5, $\mathrm{H}^{\alpha,\beta}(7) = \{H^\alpha_{14}, H^\beta_{12}\}$. По лемме 3.5, $\chi^{\alpha^{14}} \sim \chi^{\beta^{12}}$ на S^δ_9, где $\delta = (-1)^{7+1}\varepsilon = \varepsilon = -1$, т. е. $\chi^{(4,3,2)} \sim \chi^{(6,1^3)}$ на S^-_9, что противоречит теореме 4.1.

Таким образом, случай 2.2б противоречив.

С л у ч а й 2.2в. Пусть выполнено условие (в).

Тогда $b = 0$, $s = c = 2$, $a = 4 + d$ и диаграммы $[\alpha]$ и $[\beta]$ имеют вид, изображённый на рис. 5.6.

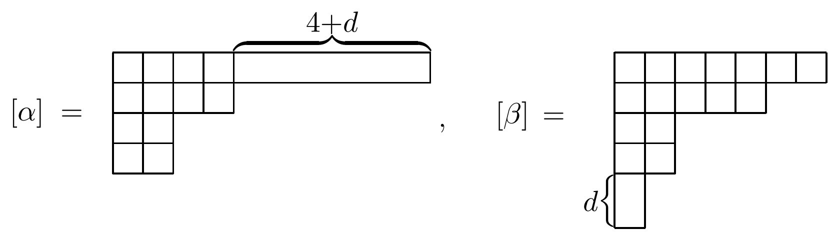


Рис. 5.6

Из рис. 5.6 видим, что при $d > 0$ H^α_{14} есть единственный крюк длины $6 + d$ в $[\alpha]$, а при $d \notin \{0, 3\}$ в $[\beta]$ нет крюков такой длины, и, следовательно, по лемме 3.4 должно быть $\alpha^{14} = (\alpha^{14})'$, что противоречиво. Поэтому $d \in \{0, 3\}$.

Если $d = 0$, то $\alpha = (8, 4, 2^2)$, $\beta = (7, 5, 2^2)$, $\varepsilon = -1$, т. е. верно утверждение (7) теоремы 5.1.

Пусть $d = 3$. Тогда $\mathrm{H}^{\alpha,\beta}(9) = \{H^\alpha_{14}, H^\beta_{12}\}$. По лемме 3.5 $\chi^{\alpha^{14}} \sim \chi^{\beta^{12}}$ на S^δ_{10}, где $\delta = (-1)^{9+1}\varepsilon = \varepsilon = -1$, т. е. $\chi^{(4,4,2)} \sim \chi^{(7,1^3)}$ на S^-_{10}, что противоречит теореме 5.1.

Случай 2.2в противоречив.

Таким образом, в случае 2 верно одно из утверждений (4)–(7) теоремы 5.1.

Итак, мы доказали, что если тройка α, β, ε удовлетворяет условию теоремы, то для неё верно одно из условий (1)–(7) заключения теоремы.

Обратное утверждение легко получается из рассмотрения таблиц характеров групп S_n при $n \leq 11$ или с помощью предложения 1.2.

Теорема 5.1 доказана.

6. $\chi^\alpha \sim \chi^\beta$ на S^ε_n. Случай $d(\alpha) = d(\beta) = 2$ и $h^\alpha_{11} = h^\beta_{11}$

В этом параграфе завершается исследование случая, когда $\chi^\alpha \sim \chi^\beta$ на S^ε_n и $d(\beta) = d(\alpha) = 2$. При этом мы будем использовать как предложение 5.1, так и следующее предложение 6.1.

Для любого $\gamma \in P(n)$ с $d := d(\gamma)$ определим разбиения $\gamma(1), \ldots, \gamma(d)$ индуктивно следующим образом: $\gamma(1) := \gamma$ и $\gamma(i+1) := (\gamma(i))^1$ при $1 \leq i < d$. Имея в виду способ изображения диаграмм на рисунке, можно записать (условно) $[\gamma(m)] := \cup^d_{i=m} H^\gamma_{ii}$ и, в частности, $[\gamma(d)] = H^\gamma_{dd}$ и $[\gamma(d-1)] = H^\gamma_{d-1,d-1} \cup H^\gamma_{dd}$.

Предложение 6.1 [10, предложение 6.1]. *Пусть* $\alpha, \beta \in P(n)$, $\alpha \neq' \beta$,

$$h(\alpha) = h(\beta) \quad \textit{и} \quad h'(\alpha) = h'(\beta)$$

(в частности, $n \geq 3$ *и* $|\alpha^1| = |\beta^1|$*). Тогда* $d(\alpha) = d(\beta) =: d$ *и справедливо одно из следующих утверждений:*

(1) $|\alpha^1| = 0$ *и* $\{\alpha, \beta\} =' \{(n), (n-1, 1)\}$;

(2) $|\alpha^1| = 2$ *и* $\{\alpha, \beta\} =' \{(3+a, 3, 1^b), (3+b, 3, 1^a)\}$, *где* $a, b \in \mathbb{N} \cup \{0\}$ *и* $a \neq b$;

(3) $|\alpha^1| \geq 3$ *и выполнено одно из условий:*

(3*а*) $h^\alpha_{dd} =: m \geq 3$ *и либо* $\alpha(d) =' \beta(d)$, *либо* $\{\alpha(d), \beta(d)\} =' \{(m), (m-1, 1)\}$;

(3*б*) $h^\alpha_{dd} =: 2$ *и либо* $\alpha(d-1) =' \beta(d-1)$, *либо* $\{\alpha(d-1), \beta(d-1)\} =' \{(3+a, 3, 1^b), (3+b, 3, 1^a)\}$ *при некоторых* $a, b \in \mathbb{N} \cup \{0\}$ *с* $a \neq b$.

Обратно, для любых α, β *из пунктов* (1)–(3) *выполнены условия этого предложения.*

Теорема 6.1. *Пусть* χ^α *и* χ^β — *неприводимые характеры группы* S_n, *имеющие одни и те же корни на* S^ε_n *при некотором* $\varepsilon = \pm 1$, *но не исчезающие тождественно на* S^ε_n, *причём* $\alpha \neq' \beta$. *Предположим, что* $d(\alpha) = d(\beta) \leq 2$ *и* $h^\alpha_{11} = h^\beta_{11}$. *Тогда верно одно из следующих утверждений:*

(1) $n = 3$, $\{\alpha, \beta\} =' \{(3), (2, 1)\}$, $\varepsilon = 1$;

(2) $n = 4$, $\{\alpha, \beta\} =' \{(4), (3, 1)\}$, $\varepsilon = -1$;

(3) $n = 9$, $\{\alpha, \beta\} =' \{(6, 3), (5, 2, 2)\}$, $\varepsilon = -1$;

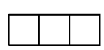
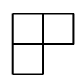
(4) $n = 9$, $\{\alpha, \beta\} =' \{(5, 4), (4, 3, 2)\}$, $\varepsilon = -1$;

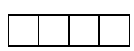
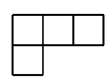
(5) $n = 10$, $\{\alpha, \beta\} =' \{(7, 3), (5, 2, 2, 1)\}$, $\varepsilon = -1$.

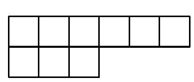
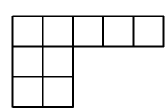
(В случаях (1)–(4) $\varepsilon = \operatorname{sign}(h(\alpha))$, *а в случае* (5) $\varepsilon = \operatorname{sign}(f(\alpha))$.*)*

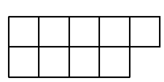
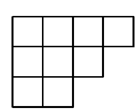
Обратно, в каждом из пунктов (1)–(5) *выполнены условия теоремы.*

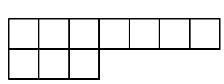
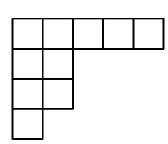
Приведём диаграммы $[\alpha]$ и $[\beta]$ в каждом из случаев (1)–(5) (предполагая, что $\alpha \geq \alpha'$, $\beta \geq \beta'$ и $\alpha > \beta$):

(1) $[\alpha] =$  , $[\beta] =$  , $\varepsilon = +1$,

(2) $[\alpha] =$  , $[\beta] =$  , $\varepsilon = -1$,

(3) $[\alpha] =$  , $[\beta] =$  , $\varepsilon = -1$,

(4) $[\alpha] =$  , $[\beta] =$  , $\varepsilon = -1$,

(5) $[\alpha] =$  , $[\beta] =$  , $\varepsilon = -1$.

Д о к а з а т е л ь с т в о. Если $d(\alpha) = d(\beta) = 1$, то согласно лемме 3.8 выполнено одно из утверждений (1) и (2) заключения теоремы.

Далее мы предполагаем, что

$$d(\alpha) = d(\beta) = 2.$$

Так как H^α_{11} и H^β_{11} — единственные крюки длины $r := h^\alpha_{11} = h^\beta_{11}$ в $[\alpha]$ и $[\beta]$ соответственно, то согласно лемме 3.5

$$\chi^{\alpha^1} \sim \chi^{\beta^1} \text{ на } S^\delta_{n-r}, \text{ где } \delta = (-1)^{r+1}\varepsilon.$$

Но тогда по лемме 3.8 выполнено одно из условий:

(А) $\alpha^1 =' \beta^1$,

(Б) $\{\alpha^1, \beta^1\} =' \{(3), (2,1)\}$ и $\varepsilon = (-1)^{r+1}$ $(\delta = 1)$,

(В) $\{\alpha^1, \beta^1\} =' \{(4), (3,1)\}$ и $\varepsilon = (-1)^{r}$ $(\delta = -1)$.

Поэтому дальнейшее доказательство теоремы 6.1 распадается на следующие 3 случая.

С л у ч а й А. Пусть $\alpha^1 =' \beta^1$.

Без ограничения общности можно считать, что диаграммы $[\alpha]$ и $[\beta]$ в этом случае имеют вид, изображённый на рис. 6.1, где $\{s, t, a, b, c, d\} \subseteq \mathbb{N} \cup \{0\}$.

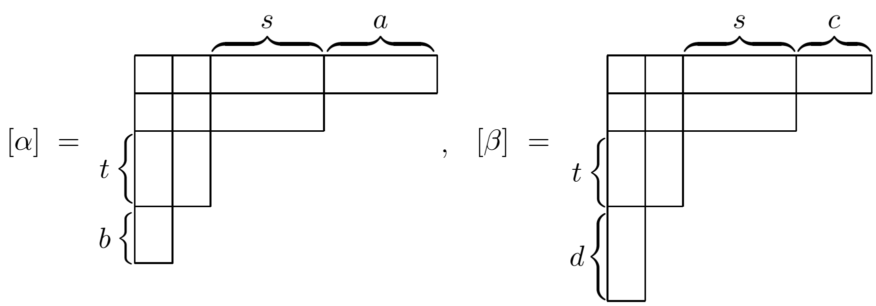


Рис. 6.1

Поскольку $h_{11}^{\alpha} = h_{11}^{\beta}$, то
$$a + b = c + d. \tag{6.1}$$

Согласно теореме 2.1 выполнено одно из условий:

(a1) $h(\alpha) = h(\beta)$, $h'(\alpha) = h'(\beta)$, $\mathrm{sign}(h(\alpha)) = \varepsilon$;

(a2) $f(\alpha) = f(\beta)$, $f'(\alpha) = f'(\beta)$, $\mathrm{sign}(f(\alpha)) = \varepsilon$.

Применив предложения 5.1 и 6.1, видим, что в любом случае
$$|\alpha^1| \geq 2.$$

Случай $|\alpha^1| \geq 3$ мы будем рассматривать независимо от того, выполнено условие (a1) или (a2) (легко заметить, что при $|\alpha^1| = 3$ выполнено условие (a1), а при $|\alpha^1| \geq 4$ выполнены как условия $h(\alpha) = h(\beta)$, $h'(\alpha) = h'(\beta)$, так и условия $f(\alpha) = f(\beta)$, $f'(\alpha) = f'(\beta)$). Однако при $|\alpha^1| = 2$ необходимо рассмотреть случаи (a1) и (a2) отдельно.

С л у ч а й А1. Пусть $|\alpha^1| = 2$ и выполнено условие (a1).

Тогда согласно предложению 6.1 $\alpha =' (3 + a, 3, 1^b)$ и $\beta =' (3 + b, 3, 1^a)$, где $\{a, b\} \subseteq \mathbb{N} \cup \{0\}$ и $a \neq b$. Без ограничения общности можно считать, что диаграммы $[\alpha]$ и $[\beta]$ имеют вид, изображённый на рис. 6.2.

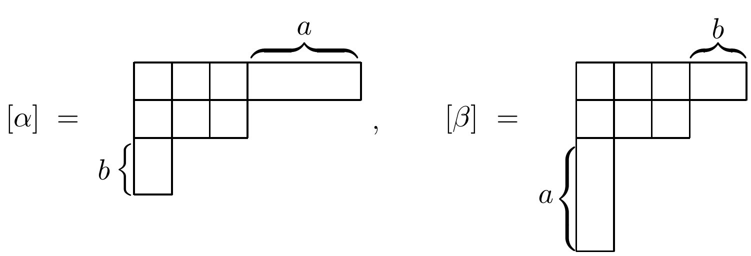


Рис. 6.2

Можно считать, что $a > b$. Очевидно, H^{α}_{12} и H^{β}_{21} — единственные крюки длины $3+a$ в $[\alpha]$ и $[\beta]$ соответственно. Следовательно, по лемме 3.5 $\chi^{\alpha^{12}} \sim \chi^{\beta^{21}}$ на S^{δ}_{3+b}, где $\delta = (-1)^a\varepsilon$. Поскольку $\alpha^{12} =' (2+b,1)$ и $\beta^{21} = (3+b)$, то по лемме 3.1

$$b \in \{0,1\}.$$

Предположим, что $b = 1$. Если $s > 2$, то H^{α}_{13} — единственный крюк длины $2+a$ в $[\alpha]$, а в $[\beta]$ нет крюков такой длины. По лемме 3.4 $\alpha^{13} = (\alpha^{13})'$, что противоречиво (см. рис. 6.2). Следовательно, $a = 2$. В этом случае $\alpha =' (5,3,1)$, $\beta =' (4,3,1^2)$ и условие предложения 6.1 не выполняется, так как на элементах $g_{(5,3,1)}$ и $g_{(4,3,1^2)}$ характер χ^{α} принимает значение 0, а χ^{β} — значения 1 и -1 соответственно.

Следовательно, $b = 0$. Если $a \geq 5$, то H^{α}_{15} и H^{β}_{41} — единственные крюки длины $a-1$ в $[\alpha]$ и $[\beta]$ соответственно. Тогда по лемме 3.5 $\chi^{\alpha^{15}} \sim \chi^{\beta^{41}}$ на S^{δ}_{7}, где $\delta = \pm 1$, что противоречиво, так как значения этих характеров на элементах $g_{(3,3,1)}$ и $g_{(2^3,1)}$ равны $2,0$ и $0,-3$ соответственно. Поэтому $a \leq 4$. Легко увидеть, что при $a \in \{1,2,4\}$ условие предложения 6.1 не выполняется (например, при $a = 4$ на элементах $g_{(7,3^2,1)}$ и $g_{(7,2,1)}$ характер χ^{α} принимает значения 3 и 0, а χ^{β} — значения 0 и -1 соответственно), а при $a = 3$ верно утверждение (3).

Таким образом, в случае A1 верно утверждение (3) доказываемой теоремы.

С л у ч а й A2. Пусть $|\alpha^1| = 2$ и выполнено условие (а2).

Согласно предложению 5.1 выполнено его утверждение (2в), и не ограничивая общности можно считать, что $\alpha = (4+a,3)$ и $\beta = (4,3,1^a)$, где $a \in \mathbb{N}$. Диаграммы $[\alpha]$ и $[\beta]$ имеют вид, изображённый на рис. 6.3.

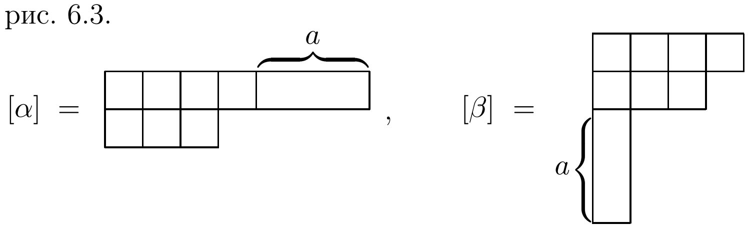


Рис. 6.3

Если $a > 3$, то H^{α}_{14} — единственный крюк длины $1+a$ в $[\alpha]$, а в $[\beta]$ нет крюков такой длины. По лемме 3.4 $\alpha^{14} = (\alpha^{14})'$, что противоречиво (см. рис. 6.3). Следовательно,

$$a \in \{1,2,3\}.$$

При $a = 1$ имеем $\alpha = (5,3)$, $\beta = (4,3,1)$, и условие теоремы 6.1 не выполняется, так как на элементах $g_{(5,3)}$ и $g_{(4,2,2)}$ разных знаков характер χ^{α} принимает значения $1,-2$, а χ^{β} — значения $0,0$ соответственно.

При $a = 2$ имеем $\alpha = (6,3)$, $\beta = (4,3,1^2)$, что также противоречиво, так как на элементах $g_{(6,3)}$ и $g_{(4,3,2)}$ характер χ^{α} принимает значения $1,0$, а χ^{β} — значения $0,-1$ соответственно.

Следовательно, $a = 3$, $\alpha = (7,3)$ и $\beta = (5,2^2,1) = (4,3,1^3)'$. При этом $\varepsilon = -1$, так как на элементе $g_{(7,3)}$ характеры χ^{α} и χ^{β} принимают значения 1 и 0 соответственно.

Таким образом, в случае A2 верно утверждение (5) доказываемой теоремы.

С л у ч а й A3. Пусть $|\alpha^1| \geq 3$, т. е. (см. рис. 6.1)

$$s + t \geq 2. \tag{6.2}$$

Пусть M есть множество всех максимальных элементов из $\{a,b,c,d\}$. Поскольку мы можем поменять местами разбиения α и β и заменить любое из них на ассоциированное с ним, то достаточно рассмотреть лишь два случая: $M = \{a\}$ и $M = \{a,d\}$.

С л у ч а й A3.1. Пусть $M = \{a\}$, т. е.

$$a > b,\ a > c,\ a > d \ \text{ и, следовательно, }\ b < c,\ b < d. \tag{6.3}$$

Тогда H_{12}^{α} — единственный крюк длины $2+s+t+a$ в $[\alpha]$, а в $[\beta]$ крюков такой длины нет. По лемме 3.4 $\alpha^{12} = (\alpha^{12})'$ и $\varepsilon = (-1)^{h_{12}^{\alpha}} = (-1)^{s+t+a}$. Так как $[\alpha^{12}]$ есть крюк с длиной руки s и длиной ноги $1+t+b$, то отсюда следует, что

$$s = 1 + t + b \tag{6.4}$$

и

$$\varepsilon = (-1)^{1+b+a}. \tag{6.5}$$

Без ограничения общности можно считать, что диаграммы $[\alpha]$ и $[\beta]$ в рассматриваемом случае имеют вид, изображённый на рис. 6.4 ($\{t, a, b, c, d\} \subseteq \mathbb{N} \cup \{0\}$). Очевидно, $a + b = c + d$.

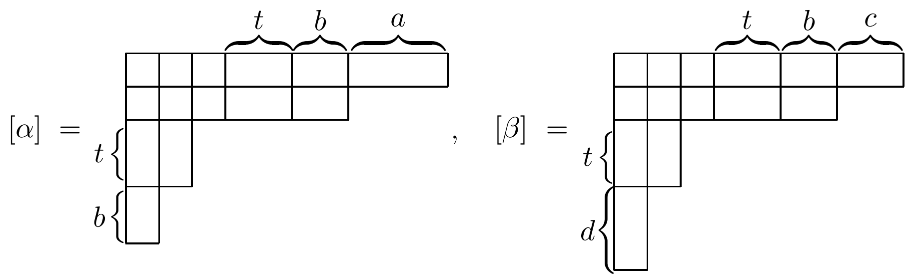


Рис. 6.4

Из (6.2) и (6.4) следует, что

$$t + b \geq 1. \tag{6.6}$$

Подсчитаем длины некоторых крюков, которые будут фигурировать в следующих рассуждениях.

$$\begin{aligned}
h_{12}^{\alpha} &= 3 + 2t + b + a, & h_{12}^{\beta} &= 3 + 2t + b + c,\\
h_{13}^{\alpha} &= 2 + t + b + a, & h_{13}^{\beta} &= 2 + t + b + c,\\
h_{14}^{\alpha} &= 1 + t + b + a, & h_{14}^{\beta} &= 1 + t + b + c,\\
h_{21}^{\alpha} &= 3 + 2t + b + b, & h_{21}^{\beta} &= 3 + 2t + b + d,\\
h_{22}^{\alpha} &= 2 + 2t + b, & h_{22}^{\beta} &= 2 + 2t + b,\\
h_{31}^{\alpha} &= 1 + t + b, & h_{31}^{\beta} &= 1 + t + d.
\end{aligned}$$

Этот список нужно иметь в виду, когда далее в случае А3.1 будут устанавливаться какие-либо соотношения между длинами крюков из $[\alpha]$ и $[\beta]$.

Предположим, что в $[\beta]$ нет крюков длины h_{13}^{α}. Тогда, как легко увидеть из приведённого выше списка, $\mathrm{H}^{\alpha,\beta}(h_{13}^{\alpha})$ может совпадать лишь с одним из следующих множеств:

$$\{H_{13}^{\alpha}\},\ \{H_{13}^{\alpha}, H_{21}^{\alpha}\},\ \{H_{13}^{\alpha}, H_{22}^{\alpha}\}.$$

В первом случае по лемме 3.4 $\alpha^{13} = (\alpha^{13})'$ и $\varepsilon = (-1)^{h_{13}^{\alpha}} = (-1)^{t+b+a}$, и тогда (см. диаграмму $[\alpha^{13}]$ на рис. 6.5) должно быть $t = 0$ и $\varepsilon = (-1)^{b+a}$. Однако последнее противоречит (6.5). Во втором случае по лемме 3.7 либо $\alpha^{13} =' \alpha^{21}$, либо разбиения α^{13} и α^{21} самоассоциированы. Но это не так, поскольку $\alpha^{21} \notin \{\alpha^{13}, (\alpha^{13})', (\alpha^{21})'\}$. Так же с помощью леммы 3.7 получаем противоречие в третьем случае.

Следовательно, $[\beta]$ имеет крюк длины $h_{13}^{\alpha} = 2 + t + b + a$. Из списка длин крюков в $[\beta]$ и (6.3) видно, что

$$\mathrm{H}^{\beta}(h_{13}^{\alpha}) \subseteq \{H_{12}^{\beta}, H_{21}^{\beta}\}. \tag{6.7}$$

Следовательно, $h_{13}^{\alpha} \in \{h_{12}^{\beta}, h_{21}^{\beta}\}$, а так как числа h_{12}^{β} и h_{21}^{β} больше, чем h_{21}^{α} (см. приведённый выше список длин крюков и (6.3)), то

$$\mathrm{H}^{\alpha}(h_{13}^{\alpha}) = \{H_{13}^{\alpha}\}. \tag{6.8}$$

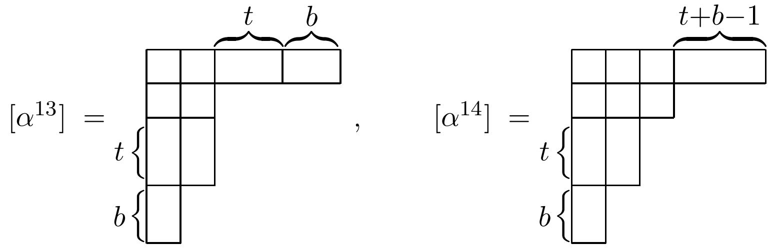


Рис. 6.5

С л у ч а й А3.1.1. Пусть $c = d$, т. е. $\mathrm{H}^\beta(h^\alpha_{13}) = \{H^\beta_{12}, H^\beta_{21}\}$.

Тогда $h^\alpha_{13} = h^\beta_{12} = h^\beta_{21}$, откуда $a = 1 + t + c$, и теперь с помощью (6.1) и (6.5) получаем $d = 1 + t + b$ и $\varepsilon = (-1)^{1+b+a} = (-1)^{1+2c} = -1$. Таким образом,

$$a = 2 + 2t + b, \;\; c = d = 1 + t + b, \;\; \varepsilon = -1. \tag{6.9}$$

При этом $n = 8{+}6t{+}4b = 2m$, где $m = 4{+}3t{+}2b = h^\alpha_{13}$. По лемме 3.3 из равенств $H^\alpha(m) = \{H^\alpha_{13}\}$ и $H^\beta(m) = \{H^\beta_{12}, H^\beta_{21}\}$ (см. (6.7) и (6.8)), учитывая, что длины ног крюков H^β_{12} и H^β_{21} равны соответственно $1 + t$ и $t + d = 1 + 2t + b$, получаем

$$\chi^{\alpha^{13}} \;\sim\; (-1)^{1+t}\chi^{\beta^{12}} + (-1)^{1+b}\chi^{\beta^{21}} \;\;\text{на}\;\; S^\delta_m, \;\;\text{где}\;\; \delta = (-1)^t \tag{6.10}$$

($\delta = (-1)^{m+1}\varepsilon$). Вычислим значения обеих частей этого отношения на элементе $g = g_{(2+2t+2b,2+t)} \in S^\delta_m$, используя вид диаграмм $[\alpha^{13}]$ (см. рис. 6.5), $[\beta^{12}] = [(2 + t + b, 1^{2+2t+b})]$, $[\beta^{21}] = [(4 + 2t + 2b, 1^t)]$ и предложение 1.2. При $b > 0$ имеем $\chi^{\alpha^{13}}(g) = \chi^{\beta^{12}}(g) = 0$ (так как $[\alpha^{13}]$ и $[\beta^{12}]$ не имеют крюков длины $2 + 2t + 2b$) и $\chi^{\beta^{21}}(g) = \chi^{(2,1^t)}(g_{(2+t)}) = (-1)^t \neq 0$. Это противоречит (6.10). Поэтому

$$b = 0, \;\; \text{и по (6.9)} \;\; a = 2 + 2t, \;\; c = d = 1 + t \;\; \text{и} \;\; n = 8 + 6t.$$

По (6.6) $t > 0$. Тогда H^α_{14} — единственный крюк длины $3 + 3t$ в $[\alpha]$, а в $[\beta]$ нет крюков такой длины ($h^\beta_{12} = h^\beta_{21} = 4 + 3t$, $h^\beta_{13} = 3 + 2t$). По лемме 3.4 должно быть $\alpha^{14} = (\alpha^{14})'$, что возможно (см. рис. 6.5) лишь при $t = 1$. Таким образом, должно быть

$$\alpha = (8, 4, 2), \;\; \beta = (6, 4, 2, 1^2) \;\; \text{и} \;\; \chi^\alpha \sim \chi^\beta \text{ на } S^-_{14}.$$

Однако в противоречие с этим при $g = g_{(6,1^8)} \in S^-_{14}$ имеем $\chi^\alpha(g) = -\chi^{\alpha^{14}}(1) \neq 0$ и $\chi^\beta(g) = 0$ ($[\beta]$ не имеет крюков длины 6).

Таким образом, случай $c = d$ противоречив.

С л у ч а й А3.1.2. Пусть $c > d$.

В этом случае согласно (6.7) и (6.8) H^α_{13} и H^β_{12} — единственные крюки длины h^α_{13} в $[\alpha]$ и $[\beta]$ соответственно. Поэтому по лемме 3.5

$$\chi^{\alpha^{13}} \sim \chi^{\beta^{12}} \;\;\text{на}\;\; S^\delta_k, \;\;\text{где}\;\; k = n - h^\alpha_{13} \;\;\text{и}\;\; \delta = \pm 1.$$

Поскольку $\beta^{12} = (2 + t + b, 1^{1+t+d})$ — крюк, а $d(\alpha^{13}) = 2$, то согласно теореме 4.1 выполнено её заключение с β^{12} и α^{13} на месте α и β соответственно. В частности, α^{13} или $(\alpha^{13})'$ должно совпадать с одним из разбиений: (2,2), (3,2), (3,3), (4,3), (3,3,2), (4,4,1), (4,4,2,1). Однако каждый из этих случаев противоречив, что непосредственно видно из рассмотрения диаграммы $[\alpha^{13}]$ (см. рис. 6.5) и из того, что $t + b \geq 1$ (ввиду (6.6)). Поэтому случай А3.1.2 ($c > d$) невозможен.

С л у ч а й А3.1.3. Пусть $d > c$.

В этом случае согласно (6.7) и (6.8) H_{13}^{α} и H_{21}^{β} — единственные крюки длины h_{13}^{α} в $[\alpha]$ и $[\beta]$ соответственно. Поэтому по лемме 3.4

$$\chi^{\alpha^{13}} \sim \chi^{\beta^{21}} \quad \text{на} \quad S_k^{\delta}, \quad \text{где} \quad k = n - h_{13}^{\alpha} \quad \text{и} \quad \delta = \pm 1.$$

Поскольку $\beta^{21} = (3+t+b+c, 1^t)$ — крюк, а $d(\alpha^{13}) = 2$, то согласно теореме 4.1 выполнено её заключение с β^{21} и α^{13} на месте α и β соответственно. Однако это заключение противоречиво по той же по причине, что и в случае A3.1.2.

Поэтому противоречив случай A3.1.3, а вместе с ним и случай A3.1.

С л у ч а й A3.2. Пусть $M = \{a, d\}$, т. е. (ввиду (6.1))

$$a = d > c = b.$$

В этом случае $s \neq t$, так как иначе $\alpha =' \beta$. Без ограничения общности можно считать, что

$$s > t \tag{6.11}$$

и диаграммы $[\alpha]$ и $[\beta]$ имеют вид, изображённый на рис. 6.1 с $d = a$ и $c = b$.

Тогда H_{12}^{α} и H_{21}^{β} — единственные крюки длины $h_{12}^{\alpha} = 2+s+t+a$ в $[\alpha]$ и $[\beta]$ соответственно. Поэтому по лемме 3.5

$$\chi^{\alpha^{12}} \sim \chi^{\beta^{21}} \quad \text{на} \quad S_k^{\delta}, \quad \text{где} \quad k = n - h_{12}^{\alpha} \quad \text{и} \quad \delta = \pm 1.$$

Поскольку $\alpha^{12} = (1+s, 1^{1+t+b})$ и $\beta^{21} = (2+s+b, 1^t)$ — крюки, то по лемме 3.8 выполнено одно из следующих условий:

$\alpha^{12} =' \beta^{21}$,

$\{\alpha^{12}, \beta^{21}\} =' \{(3), (2,1)\}$ и $\delta = 1$,

$\{\alpha^{12}, \beta^{21}\} =' \{(4), (3,1)\}$ и $\delta = -1$.

В первом случае, очевидно, должно быть $s = t$, а это противоречит (6.11). Во втором случае должно быть $\beta^{21} = (3)$ и $\alpha^{12} = (2,1)$; первое из этих равенств вместе с (6.11) влечёт $t = 0$, $s = 1$, $b = 0$ в противоречие с тем, что по (6.6) $t + b \geq 1$. В третьем случае должно быть $\beta^{21} = (4)$ и $\alpha^{12} =' (3,1)$. Из первого равенства и из (6.11) получаем $t = 0$, $s + b = 2$, а так как по (6.2) $s + t \geq 2$, то $s = 2$, $b = 0$ и, следовательно, $t + b = 0$ в противоречие с (6.6).

Таким образом, случаи A3.1 и A3.2 противоречивы и, значит, противоречив случай A3.

С л у ч а й Б. Пусть $\{\alpha^1, \beta^1\} =' \{(3), (2,1)\}$ и $\varepsilon = (-1)^{h_{11}^{\alpha}+1}$.

Без ограничения общности можно считать, что диаграммы $[\alpha]$ и $[\beta]$ в рассматриваемом случае имеют вид, изображённый на рис. 6.6, где $\{a, b, c, d\} \subseteq \mathbb{N} \cup \{0\}$.

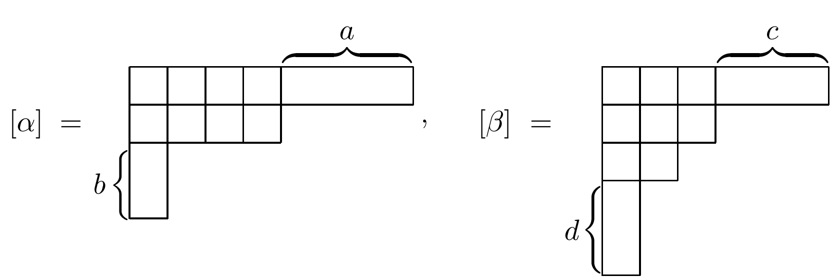


Рис. 6.6

Нам потребуются следующие длины крюков из $[\alpha]$ и $[\beta]$.

$$h_{11}^{\alpha} = 5 + b + a, \qquad h_{11}^{\beta} = 5 + d + c,$$

$$h_{12}^{\alpha} = 4 + a, \qquad h_{12}^{\beta} = 4 + c,$$

$$h^{\alpha}_{13} = 3 + a, \qquad h^{\beta}_{13} = 2 + c,$$
$$h^{\alpha}_{14} = 2 + a, \qquad h^{\beta}_{14} = c,$$
$$h^{\alpha}_{21} = 4 + b, \qquad h^{\beta}_{21} = 4 + d,$$
$$h^{\alpha}_{22} = 3, \qquad h^{\beta}_{22} = 3,$$
$$h^{\alpha}_{31} = b, \qquad h^{\beta}_{31} = 2 + d.$$

Так как по условию $h^{\alpha}_{11} = h^{\beta}_{11}$, то отсюда получаем

$$a + b = c + d \tag{6.12}$$

и

$$\varepsilon = (-1)^{b+a}. \tag{6.13}$$

Поскольку мы можем заменить β на β' и $\beta^1 = (\beta^1)'$, то можно предполагать, что

$$c \geq d. \tag{6.14}$$

Пусть M есть множество всех максимальных элементов из $\{a, b, c, d\}$. Очевидно (ввиду (6.12) и (6.14)), что возможны лишь следующие случаи:

$M = \{a\}$, $M = \{a, c\}$, $M = \{a, b, c, d\}$, $M = \{b\}$, $M = \{b, c\}$, $M = \{c\}$.

С л у ч а й Б1. Пусть $M = \{a\}$, т. е.

$$a > b,\ a > c,\ a > d \ \text{ и, следовательно, }\ b < c,\ b < d.$$

Тогда H^{α}_{12} — единственный крюк длины $4 + a$ в $[\alpha]$, а в $[\beta]$ нет крюков такой длины. По лемме 3.4 $\alpha^{12} = (\alpha^{12})'$ и

$$\varepsilon = (-1)^{a}. \tag{6.15}$$

Так как $[\alpha^{12}]$ есть крюк с длиной руки 2 и длиной ноги $1 + b$, то из $\alpha^{12} = (\alpha^{12})'$ следует, что $b = 1$. Но тогда по (6.13) имеем $\varepsilon = (-1)^{a+b} = (-1)^{a+1}$ в противоречие с (6.15). Следовательно, случай Б1 невозможен.

С л у ч а й Б2. Пусть $M = \{a, c\}$, т. е. $a = c > d = b$.

В этом случае H^{α}_{12} и H^{β}_{12} — единственные крюки длины $4 + a$ в $[\alpha]$ и $[\beta]$ соответственно. По лемме 3.5

$$\chi^{\alpha^{12}} \sim \chi^{\beta^{12}} \ \text{ на }\ S^{\delta}_{4+b} \ \ (\delta = \pm 1).$$

Поскольку $\alpha^{12} = (3, 1^{1+b}) \neq' (4 + b)$ и $\beta^{12} = (2, 1^{2+b}) \neq' (4 + b)$, то по лемме 3.8 должно быть $\alpha^{12} =' \beta^{12}$. Это возможно лишь при $b = 0$. Таким образом, $\alpha = (4 + a, 4)$, $\beta = (3 + a, 3, 2)$, $n = 8 + a$. Предположим, что $a > 1$. Тогда H^{α}_{13} — единственный крюк длины $3 + a$ в $[\alpha]$, а в $[\beta]$ нет крюков такой длины. По лемме 3.4 $\alpha^{13} = (\alpha^{13})'$. Но это невозможно, так как $\alpha^{13} = (3, 2)$.

Поэтому $a = 1$, $\alpha = (5, 4)$, $\beta = (4, 3, 2)$, $n = 9$ и (по (6.13)) $\varepsilon = (-1)^{b+a} = -1$.

Таким образом, в случае Б2 α, β, ε удовлетворяют утверждению (4) теоремы 6.1.

С л у ч а й Б3. Пусть $M = \{a, b, c, d\}$, т. е. $a = b = c = d$.

По (6.13) $\varepsilon = (-1)^{b+a} = 1$. При $a = 0$ разбиения $\alpha = (4, 4)$ и $\beta = (3, 3, 2) = \beta'$ не удовлетворяют условию теоремы, так как $\chi^{\alpha}(g_{(3^2,1^2)}) = 2$ и $\chi^{\beta}(g_{(3^2,1^2)}) = 0$.

Пусть $a \geq 1$. Тогда H^{α}_{13} — единственный крюк длины $3 + a$ в $[\alpha]$, а в $[\beta]$ нет крюков такой длины. По лемме 3.4 $\alpha^{13} = (\alpha^{13})'$. Так как $\alpha^{13} = (3, 2, 1^{a})$, то отсюда следует, что $a = 1$. Тогда $\alpha = (5, 4, 1)$, $\beta = (4, 3, 2, 1)$, и условия теоремы 6.1 нарушены, так как $\chi^{\alpha}(g_{(5,2^2,1)}) = 1$ и $\chi^{\beta}(g_{(5,2^2,1)}) = 0$.

Следовательно, случай Б3 невозможен.

С л у ч а й Б4. Пусть $M = \{b\}$, т. е.

$$b > a,\ b > c \geq d \ \text{ и, следовательно, }\ a < d \leq c.$$

В этом случае H^α_{21} — единственный крюк длины $4+b$ в $[\alpha]$, а в $[\beta]$ нет крюков такой длины. По лемме 3.4 $\alpha^{21} = (\alpha^{21})'$. Но это противоречиво, так как $\alpha^{21} = (4+b)$. Следовательно, случай Б4 невозможен.

С л у ч а й Б5. Пусть $M = \{b, c\}$, т. е. $b = c > d = a$.

Тогда $h^\alpha_{21} = h^\beta_{12} = 4 + b$ — вторая по величине из длин крюков в α и β, и H^α_{21} и H^β_{12} — единственные крюки длины $4 + b$ в $[\alpha]$ и $[\beta]$ соответственно. По лемме 3.5

$$\chi^{\alpha^{21}} \sim \chi^{\beta^{12}} \text{ на } S^\delta_{4+a} \quad (\delta = \pm 1).$$

Поскольку $\alpha^{21} = (4+a)$ и $\beta^{12} = (2, 1^{2+a})$, то по лемме 3.8 должно быть $\alpha^{21} = (4)$ и $\beta^{12} = (3, 1)'$, т. е. (с учётом (6.13))

$$a = 0, \quad n = 8 + b \geq 9, \quad \varepsilon = (-1)^b.$$

Предположим, что $b \geq 3$. Тогда в $[\alpha]$ нет крюков длины $2 + b$, а $[\beta]$ имеет единственный крюк H^β_{13} такой длины. По лемме 3.4 $\beta^{13} = (\beta^{13})'$. Но это невозможно, так как $\beta^{13} = (2^3)$.

Поэтому $b \in \{1, 2\}$. Но это противоречиво, так как характеры χ^α и χ^β принимают при $b = 1$ (тогда $\varepsilon = -1$) значения 0 и -1 соответственно на элементе $g_{(4,3,1^2)}$, а при $b = 2$ (тогда $\varepsilon = 1$) значения 0 и -1 соответственно на элементе $g_{(7,3)}$. Случай Б5 невозможен.

С л у ч а й Б6. Пусть $M = \{c\}$, т. е.

$$c > a, \ c > b, \ c > d \ \text{ и } \ d < a, \ d < b.$$

Тогда в $[\alpha]$ нет крюков длины $4 + c$, а $[\beta]$ имеет единственный крюк H^β_{12} такой длины. По лемме 3.4 $\beta^{12} = (\beta^{12})'$. Но это невозможно, так как разбиение $\beta^{12} = (2, 1^{2+d})$ не самоассоциировано. Случай Б6 противоречив.

Итак, в случае Б α, β, ε удовлетворяют утверждению (4) теоремы 6.1.

С л у ч а й В. Пусть $\{\alpha^1, \beta^1\} =' \{(4), (3, 1)\}$ и $\varepsilon = (-1)^{h^\alpha_{11}}$.

Без ограничения общности можно считать, что диаграммы $[\alpha]$ и $[\beta]$ в рассматриваемом случае имеют вид, изображённый на рис. 6.7, где $\{a, b, c, d\} \subseteq \mathbb{N} \cup \{0\}$.

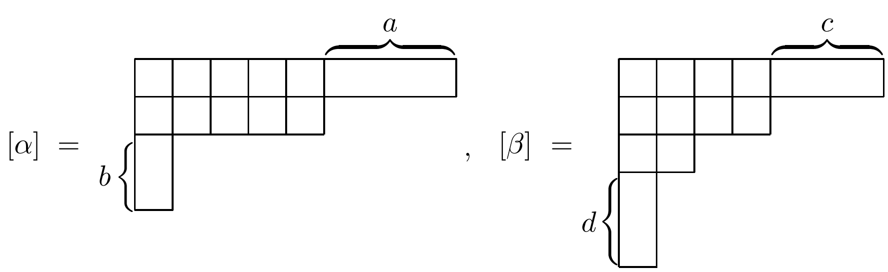


Рис. 6.7

Нам потребуются следующие длины крюков из $[\alpha]$ и $[\beta]$.

$$\begin{aligned}
&h^\alpha_{11} = 6 + b + a, && h^\beta_{11} = 6 + d + c,\\
&h^\alpha_{12} = 5 + a, && h^\beta_{12} = 5 + c,\\
&h^\alpha_{13} = 4 + a, && h^\beta_{13} = 3 + c,\\
&h^\alpha_{14} = 3 + a, && h^\beta_{14} = 2 + c,\\
&h^\alpha_{21} = 5 + b, && h^\beta_{21} = 5 + d,\\
&h^\alpha_{22} = 4, && h^\beta_{22} = 4,\\
&h^\alpha_{31} = b, && h^\beta_{31} = 2 + d.
\end{aligned}$$

Отсюда получаем
$$a + b = c + d \tag{6.16}$$
(поскольку $h_{11}^{\alpha} = h_{11}^{\beta}$) и
$$\varepsilon = (-1)^{b+a}. \tag{6.17}$$

Пусть M есть множество всех максимальных элементов из $\{a, b, c, d\}$. Ввиду (6.16) возможны лишь следующие случаи:

$M = \{a\}$, $M = \{b\}$, $M = \{c\}$, $M = \{d\}$, $M = \{a, c\}$, $M = \{a, d\}$, $M = \{b, c\}$, $M = \{b, d\}$, $M = \{a, b, c, d\}$.

С л у ч а й B1. Пусть $M = \{a\}$, т. е.
$$a > b,\ a > c,\ a > d \ \text{ и, следовательно, } \ b < c,\ b < d.$$

Тогда H_{12}^{α} — единственный крюк длины $5 + a$ в $[\alpha]$, а в $[\beta]$ нет крюков такой длины. По лемме 3.4 $\alpha^{12} = (\alpha^{12})'$ и
$$\varepsilon = (-1)^{1+a}. \tag{6.18}$$
Так как $[\alpha^{12}]$ есть крюк с длиной руки 3 и длиной ноги $1 + b$, то из $\alpha^{12} = (\alpha^{12})'$ следует, что $b = 2$. Отсюда и из (6.17) следует $\varepsilon = (-1)^{a+b} = (-1)^a$ в противоречие с (6.18). Следовательно, случай B1 невозможен.

С л у ч а й B2. Пусть $M = \{b\}$.

Тогда H_{21}^{α} — единственный крюк длины $5 + b$ в $[\alpha]$, а в $[\beta]$ нет крюков такой длины. По лемме 3.4 $\alpha^{21} = (\alpha^{21})'$. Но это противоречиво, так как $\alpha^{21} = (5 + a)$. Следовательно, случай B2 невозможен.

С л у ч а й B3. Пусть $M = \{c\}$.

Тогда H_{12}^{β} — единственный крюк длины $5 + c$ в $[\beta]$, а в $[\alpha]$ нет крюков такой длины. По лемме 3.4 $\beta^{12} = (\beta^{12})'$ и $\varepsilon = (-1)^{h_{12}^{\beta}} = (-1)^{1+c}$. Поскольку $\beta^{12} = (3, 1^{2+d})$, то $d = 0$ и тогда по (6.17) и (6.16) $\varepsilon = (-1)^{a+b} = (-1)^c$, что противоречит полученному выше. Следовательно, случай B3 невозможен.

С л у ч а й B4. Пусть $M = \{d\}$.

Понятно, что H_{21}^{β} — единственный крюк длины $5+d$ в $[\beta]$, а в $[\alpha]$ нет крюков такой длины. По лемме 3.4 $\beta^{21} = (\beta^{21})'$. Но это противоречиво, так как $\beta^{21} = (4 + c, 1)$. Следовательно, случай B4 невозможен.

С л у ч а й B5. Пусть $M = \{a, c\}$, т. е. $a = c > d = b$.

В этом случае H_{12}^{α} и H_{12}^{β} — единственные крюки длины $5+a$ в $[\alpha]$ и $[\beta]$ соответственно. По лемме 3.5
$$\chi^{\alpha^{12}} \sim \chi^{\beta^{12}} \ \text{ на } \ S_{5+b}^{\delta} \ \ (\delta = \pm 1).$$
Так как $\alpha^{12} = (4, 1^{1+b})$ и $\beta^{12} = (3, 1^{2+b})$, то по лемме 3.8 должно быть $\alpha^{12} =' \beta^{12}$, откуда $b = 1$ и, следовательно,
$$\alpha = (5 + a, 5, 1),\ \beta = (4 + a, 4, 2, 1),\ n = 11 + a \geq 13.$$

Предположим, что $a \neq 2$. Тогда H_{13}^{α} — единственный крюк длины $4 + a$ в $[\alpha]$, а в $[\beta]$ нет крюков такой длины. По лемме 3.4 $\alpha^{13} = (\alpha^{13})'$. Но это невозможно, так как $\alpha^{13} = (4, 2, 1)$.

Поэтому $a = 2$, $\alpha = (7, 5, 1)$, $\beta = (6, 4, 2, 1)$, $n = 11$ и (по (6.18)) $\varepsilon = (-1)^{b+a} = -1$. Тогда $\mathrm{H}^{\alpha}(6) = \{H_{13}^{\alpha}, H_{21}^{\alpha}\}$, $\mathrm{H}^{\beta}(6) = \{H_{21}^{\beta}\}$ и по лемме 3.3
$$\chi^{\alpha^{13}} + \chi^{\alpha^{21}} \sim \chi^{\beta^{21}} \ \text{ на } \ S_7^{\delta}, \ \text{ где } \ \delta = (-1)^7 \varepsilon = 1.$$

Но это противоречиво, так как на элементе $g_{(4,2,1)} \in S_7^\delta$ характеры $\chi^{\alpha^{13}} + \chi^{\alpha^{21}}$ и $\chi^{\beta^{21}}$ принимают значения $1+1 \neq 0$ и 0 соответственно. Случай B5 невозможен.

С л у ч а й B6. Пусть $M = \{a, d\}$, т. е. $a = d > c = b$.

В этом случае H_{12}^α и H_{21}^β — единственные крюки длины $5+a$ в $[\alpha]$ и $[\beta]$ соответственно. По лемме 3.5

$$\chi^{\alpha^{12}} \sim \chi^{\beta^{21}} \ \text{ на } \ S_{5+b}^\delta \ \ (\delta = \pm 1).$$

Так как $\alpha^{12} = (4, 1^{1+b})$ и $\beta^{21} = (4+b, 1)$, то по лемме 3.8 должно быть $b = 0$ и, следовательно,

$$\alpha = (5+a, 5), \ \beta = (4, 4, 2, 1^a), \ n = 10 + a.$$

Предположим, что $a > 1$. Тогда H_{13}^α — единственный крюк длины $4+a$ в $[\alpha]$, а в $[\beta]$ нет крюков такой длины. По лемме 3.4 $\alpha^{13} = (\alpha^{13})'$. Но это невозможно, так как $\alpha^{13} = (4, 2)$.

Поэтому $a = 1$, $\alpha = (6, 5)$, $\beta = (4, 4, 2, 1)$, $n = 11$ и (по (6.18)) $\varepsilon = (-1)^{b+a} = -1$. Но это противоречиво, так как характеры χ^α и χ^β принимают значения 2 и 0 соответственно на элементе $g_{(5,4,1^2)} \in S_{11}^-$. Случай B6 невозможен.

С л у ч а й B7. Пусть $M = \{b, c\}$, т. е. $b = c > d = a$.

В этом случае H_{21}^α и H_{12}^β — единственные крюки длины $5+b$ в $[\alpha]$ и $[\beta]$ соответственно. По лемме 3.5

$$\chi^{\alpha^{21}} \sim \chi^{\beta^{12}} \ \text{ на } \ S_{5+a}^\delta \ \ (\delta = \pm 1). \tag{6.19}$$

Так как $\alpha^{21} = (5+a)$ и $\beta^{12} = (3, 1^{2+a})$, то по лемме 3.8 условие (6.19) противоречиво. Случай B7 невозможен.

С л у ч а й B8. Пусть $M = \{b, d\}$, т. е. $b = d > c = a$.

В этом случае H_{21}^α и H_{21}^β — единственные крюки длины $5+b$ в $[\alpha]$ и $[\beta]$ соответственно. По лемме 3.5

$$\chi^{\alpha^{21}} \sim \chi^{\beta^{21}} \ \text{ на } \ S_{5+a}^\delta \ \ (\delta = \pm 1).$$

Но это условие противоречит лемме 3.8, так как $\alpha^{21} = (5+a)$ и $\beta^{12} = (4+a, 1)$. Случай B8 невозможен.

С л у ч а й B9. Пусть $M = \{a, b, c, d\}$, т. е. $a = b = c = d$.

По (6.18) $\varepsilon = 1$. Легко увидеть, что H_{13}^α — единственный крюк длины $4+a$ в $[\alpha]$, а в $[\beta]$ нет крюков такой длины. По лемме 3.4 $\alpha^{13} = (\alpha^{13})'$. Так как $\alpha^{13} = (4, 2, 1^a)$, то должно быть $a = 2$ и $n = 14$. В этом случае H_{14}^α и H_{13}^β — единственные крюки длины $3+a = 5$ в $[\alpha]$ и $[\beta]$ соответственно. По лемме 3.5

$$\chi^{\alpha^{14}} \sim \chi^{\beta^{13}} \ \text{ на } \ S_9^\delta, \ \text{ где } \ \delta = \varepsilon = 1.$$

Но это противоречиво, так как характеры $\chi^{\alpha^{14}} = \chi^{(4,3,1^2)}$ и $\chi^{\beta^{13}} = \chi^{(3,2^2,1^2)}$ принимают значения 1 и 0 соответственно на элементе $g_{(5,3,1)}$. Случай B9 невозможен.

Таким образом, случай B противоречив.

Итак, мы доказали, что если тройка α, β, ε удовлетворяет условию теоремы, то для неё верно одно из условий (1)–(5) заключения теоремы.

Обратное утверждение легко получается из рассмотрения таблиц характеров групп S_n при $n \leq 10$ (или с помощью лёгких вычислений, использующих предложение 1.2).

Теорема 6.1 доказана.

З а м е ч а н и е. Объединением теорем 4.1, 5.1, 6.1 является теорема Б. Легко проверить, что *в пунктах* (1), (3), (8) *и только в этих пунктах теоремы Б* χ^α *и* χ^β *полупропорциональны на* A_n.

И из предложения 1 вытекает теорема А.

Поступила 15.10.2006

СПИСОК ЛИТЕРАТУРЫ

1. **Белоногов В. А.** Взаимодействия и D-блоки в конечных группах // Подгрупповая структура групп. Свердловск: УрО АН СССР. 1988. С. 4–44.
2. **Белоногов В. А.** Представления и характеры в теории конечных групп. Свердловск: УрО АН СССР, 1990. 380 с.
3. **Белоногов В. А.** О малых взаимодействиях в конечных группах // Тр. Ин-та математики и механики УрО РАН. Екатеринбург, 1992. Т. 2. С. 3–18.
4. **Белоногов В. А.** Малые взаимодействия в группах $\mathrm{GL}_3(q)$, $\mathrm{GU}_3(q)$, $\mathrm{PGL}_3(q)$ и $\mathrm{PGU}_3(q)$ // Тр. Ин-та математики и механики УрО РАН. Екатеринбург, 1996. Т. 4. С. 17–47.
5. **Белоногов В. А.** Малые взаимодействия в группах $\mathrm{SL}_3(q)$, $\mathrm{SU}_3(q)$, $\mathrm{PSL}_3(q)$ и $\mathrm{PSU}_3(q)$ // Тр. Ин-та математики и механики УрО РАН. Екатеринбург, 1998. Т. 5. С. 3–27.
6. **Белоногов В. А.** О неприводимых характерах групп S_n и A_n // Сиб. мат. журн. 2004. Т. 45, № 5. С. 977–994.
7. **Белоногов В. А.** К гипотезе о полупропорциональных характерах // Сиб. мат. журн. 2005. Т. 46, № 2. С. 299–314.
8. **Белоногов В. А.** О нулях в таблицах характеров групп S_n и A_n // Алгебра и логика. 2005. Т. 44, № 1. С. 24–43.
9. **Белоногов В. А.** О нулях в таблицах характеров групп S_n и A_n. II // Алгебра и логика. 2005. Т. 44, № 6. С. 643–663.
10. **Белоногов В. А.** О равнокорневых неприводимых характерах групп S_n и A_n. // Алгебра и логика. 2007. Т. 46, № 1. С. 3–25.
11. **James G., Kerber A.** The representation theory of the symmetric group. London: Addison–Wesley, 1981. 510 p.
12. **Джеймс Г.** Теория представлений симметрических групп. М.: Мир, 1982. 214 с.

ТРУДЫ ИНСТИТУТА МАТЕМАТИКИ И МЕХАНИКИ УрО РАН

Том 13 № 1 2007

УДК 519.14

ДИСТАНЦИОННО РЕГУЛЯРНЫЙ ГРАФ С МАССИВОМ ПЕРЕСЕЧЕНИЙ {8,7,5;1,1,4} И ЕГО АВТОМОРФИЗМЫ[1]

И. Н. Белоусов, А. А. Махнев

Найдены возможные порядки и подграфы неподвижных точек дистанционно регулярного графа с массивом пересечений $\{8,7,5;1,1,4\}$. Доказано, что такой граф не является вершинно транзитивным.

Введение

Мы рассматриваем неориентированные графы без петель и кратных ребер. Для вершины a графа Γ через $\Gamma_i(a)$ обозначим i-окрестность вершины a, т. е. подграф, индуцированный Γ на множестве всех вершин, находящихся на расстоянии i от a. В дальнейшем под окрестностью вершины понимается ее 1-окрестность. Положим $[a]=\Gamma(a)$, $a^\perp=\{a\}\cup[a]$.

Пусть Γ — граф, $a,b\in\Gamma$, число вершин в $[a]\cap[b]$ обозначается через $\mu(a,b)$ (соответственно, через $\lambda(a,b)$), если a,b находятся на расстоянии 2 (соответственно, смежны) в Γ, а подграф $[a]\cap[b]$, индуцированный графом Γ, называется *μ-подграфом* (соответственно, *λ-подграфом*). Если Γ — граф диаметра d и $i\le d$, то через Γ_i обозначается граф с тем же множеством вершин, что и Γ, в котором две вершины смежны тогда и только тогда, когда они находятся на расстоянии i в Γ.

Степенью вершины называется число вершин в ее окрестности. Граф Γ называется *регулярным степени* k, если степень любой вершины a из Γ равна k. Граф Γ назовем *реберно регулярным с параметрами* (v,k,λ), если он имеет v вершин, регулярен степени k и каждое его ребро лежит в λ треугольниках. Граф Γ — *вполне регулярный граф с параметрами* (v,k,λ,μ), если он реберно регулярен с параметрами (v,k,λ) и $[a]\cap[b]$ состоит из μ вершин для любых двух вершин a,b, находящихся на расстоянии 2 в Γ. Вполне регулярный граф диаметра 2 называется *сильно регулярным графом.*

Система инцидентности $(X,\mathcal{L})$, где X — множество точек и $\mathcal{L}$ — множество прямых, называется *α-частичной геометрией порядка* (s,t), если каждая прямая имеет ровно $s+1$ точку, каждая точка лежит ровно на $t+1$ прямой (прямые пересекаются не более чем по одной точке) и для любой точки a, не лежащей на прямой L, найдется ровно α прямых, проходящих через a и пересекающих L (обозначение геометрии — $pG_\alpha(s,t)$). *Точечным графом* геометрии точек и прямых называется граф, вершинами которого являются точки геометрии, и две различные вершины смежны, если они лежат на прямой. Легко понять, что точечный граф частичной геометрии $pG_\alpha(s,t)$ сильно регулярен с параметрами: $v=(s+1)(1+st/\alpha)$, $k=s(t+1)$, $\lambda=(s-1)+(\alpha-1)t$, $\mu=\alpha(t+1)$. Сильно регулярный граф, имеющий вышеуказанные параметры, называется *псевдогеометрическим графом для $pG_\alpha(s,t)$.*

Если вершины u,w находятся на расстоянии i в Γ, то через $b_i(u,w)$ (через $c_i(u,w)$) обозначим число вершин в пересечении $\Gamma_{i+1}(u)$ ($\Gamma_{i-1}(u)$) с $\Gamma(w)$. Граф Γ диаметра d называется *дистанционно регулярным с массивом пересечений* $\{b_0,b_1,\dots,b_{d-1};c_1,\dots,c_d\}$, если значения $b_i(u,w)=b_i$ и $c_i(u,w)=c_i$ не зависят от выбора вершин u,w на расстоянии i в Γ для любого $i=0,...,d$. Заметим, что для дистанционно регулярного графа b_0 — это степень графа, $c_1=1$.

[1]Работа выполнена при поддержке РФФИ (проект 05-01-00046) и РФФИ-ГФЕН Китая (проект 05-01-39000).

Граф Γ называется *вершинно транзитивным*, если для любых двух вершин u, w найдется автоморфизм g графа Γ такой, что $u^g = w$. Граф Γ диаметра d называется *дистанционно транзитивным*, если для любого $i \in \{0, ..., d\}$ и для любых двух пар вершин (u, w) и (y, z) с $d(u, w) = d(y, z) = i$ найдется автоморфизм g графа Γ такой, что $(u^g, w^g) = (y, z)$. Для подмножества Y автоморфизмов графа Γ через $\mathrm{Fix}(Y)$ обозначается подграф, индуцированный на множестве всех вершин графа Γ, неподвижных относительно любого автоморфизма из Y.

Графом Грюнберга — Кегеля (графом простых чисел) конечной группы G называется граф, вершинами которого являются простые делители $|G|$, а два делителя p, r смежны в этом графе, если G содержит элемент порядка pr.

Для изучения возможных порядков и подграфов неподвижных точек автоморфизмов дистанционно регулярных графов Г. Хигмен предложил оригинальный метод, использующий теорию характеров конечных групп. В монографии [1] П. Камерон излагает этот метод, но применяет его только к изучению инволютивных автоморфизмов сильно регулярного графа с параметрами (3250,57,0,1). Позднее в работах [2–4] изучались автоморфизмы сильно регулярных графов с малыми числами пересечений.

В данной работе изучаются автоморфизмы гипотетического дистанционно регулярного графа Γ с массивом пересечений $\{8, 7, 5; 1, 1, 4\}$ на 135 вершинах. Этот граф имеет спектр $\{8^1, 3^{54}, -1^{50}, -4^{30}\}$, а граф Γ_3 (граф с теми же вершинами, что и в Γ, но вершины смежны тогда и только тогда, когда они на расстоянии 3 в Γ) сильно регулярен с параметрами $(135, 70, 37, 35)$. Интерес к графу Γ вызван тем, что его существование неизвестно, зато известно существование сильно регулярного графа $\overline{\Delta}$ с параметрами $(135, 64, 28, 30)$, дополнительного к Γ_3, и можно попытаться построить Γ, стирая некоторые ребра в $\overline{\Delta}$ с помощью подходящей группы автоморфизмов графа $\overline{\Delta}$.

Теорема. *Пусть Γ — дистанционно регулярный граф, имеющий массив пересечений $\{8, 7, 5; 1, 1, 4\}$, $G = \mathrm{Aut}(\Gamma)$, g — элемент из G простого порядка p и $\Omega = \mathrm{Fix}(g)$. Тогда верно одно из утверждений*:

(1) *$p = 3$ или 5 и Ω — пустой граф*;

(2) *$p = 7$ и Ω является двухвершинной кликой*;

(3) *$p = 2$ и либо*

(*i*) *Ω состоит из вершин, попарно находящихся на расстоянии 3 в Γ, и $|\Omega| = 3, 5, 7, 9$ или 11, либо*

(*ii*) *Ω содержит две вершины степени 4, восемь вершин степени 2 и одну или три вершины степени 0, либо*

(*iii*) *Ω содержит шестиугольник и единственную изолированную вершину.*

Следствие. *Вершинно транзитивные дистанционно регулярные графы с массивом пересечений $\{8, 7, 5; 1, 1, 4\}$ не существуют.*

1. Вспомогательные результаты

В этом параграфе приведены результаты, используемые в доказательстве теоремы.

Лемма 1.1. *Пусть Δ — произвольный сильно регулярный граф, имеющий параметры $(135, 70, 37, 35)$. Тогда Δ является псевдогеометрическим графом для $pG_7(14, 4)$, имеет собственные значения 7 и -5 кратностей 50 и 84 соответственно и*

(1) *для клики L имеем $|L| \le 15$, причем в случае равенства каждая вершина вне L смежна точно с 7 вершинами из L*;

(2) *$|C| \le 9$ для любой коклики C из Δ, причем равенство достигается тогда и только тогда, когда каждая вершина вне C смежна точно с 5 вершинами из C.*

Д о к а з а т е л ь с т в о. Легко заметить, что граф Δ является псевдогеометрическим графом для $pG_7(14, 4)$, поэтому он имеет собственные значения 7 и -5 кратностей 50 и 84 соответственно.

Для клики L граница Хоффмана [5, предложение 1.3.2] дает оценку $|L| \le 1 + 70/5 = 15$, причем в случае равенства каждая вершина вне L смежна точно с 7 вершинами из L.

Далее, $|C| \le 135 \cdot 5/75 = 9$ для любой коклики C из Δ, причем равенство достигается тогда и только тогда, когда каждая вершина вне C смежна точно с 5 вершинами из C (граница Хоффмана для коклик).

Лемма 1.2. *Пусть* Γ — *дистанционно регулярный граф с массивом пересечений* $\{8,7,5;1,1,4\}$. *Тогда граф* $\Delta = \Gamma_3$ *является сильно регулярным с параметрами* $(135,70,37,35)$ *и для чисел пересечения графа* Γ *верны равенства*

(1) $p^1_{11} = 0$, $p^1_{21} = 7$, $p^1_{32} = 35$, $p^1_{22} = 14$, $p^1_{33} = 35$,

(2) $p^2_{11} = 1$, $p^2_{12} = 2$, $p^2_{13} = 5$, $p^2_{32} = 30$, $p^2_{33} = 35$, $p^2_{22} = 23$,

(3) $p^3_{12} = 4$, $p^3_{22} = 24$, $p^3_{13} = 4$, $p^3_{23} = 28$ *и* $p^3_{33} = 37$.

Д о к а з а т е л ь с т в о. Напомним, что для вершин u, w, находящихся на расстоянии l, через p^l_{ij} обозначается число вершин z с $d(u,z) = i$ и $d(z,w) = j$. Заметим, что $p^2_{12} = a_2$, $p^3_{13} = a_3$. По лемме 4.1.7 из [5] получим

$p^1_{ii-1} = c_i k_i/k$, $p^1_{ii} = a_i k_i/k$, $p^1_{ii+1} = b_i k_i/k$,

$p^i_{i-22} = c_{i-1}c_i/\mu$, $p^{i-1}_{i+12} = b_{i-1}b_i/\mu$, $p^2_{i-1i+1} = k_i c_i b_i/(kb_1)$,

$p^{i-1}_{i2} = b_{i-1}(a_i + a_{i-1} - a_1)/\mu$, $p^{i+1}_{i2} = c_{i+1}(a_i + a_{i+1} - a_1)/\mu$.

Имеем $a_1 = 0$, $a_2 = 2$ и $a_3 = 4$. Далее, $k_1 = 8$, $k_2 = 56$ и $k_3 = 70$. Поэтому $p^1_{21} = c_2k_2/k = 7$ и $p^1_{32} = c_3k_3/k = 4 \cdot 70/8 = 35$.

Аналогично, $p^1_{11} = a_1k_1/k = 0$, $p^1_{22} = a_2k_2/k = 14$ и $p^1_{33} = a_3k_3/k = 35$.

Далее, $p^3_{12} = c_2c_3/\mu = 4$, $p^2_{13} = k_2c_2b_2/(kb_1) = 5$, $p^3_{22} = p^3_{12}(a_2 + a_3 - a_1)/\mu = 24$ и $p^2_{32} = b_2(a_3 + a_2 - a_1)/\mu = 30$. Поэтому $p^2_{33} = 70 - p^2_{23} - p13^2 = 35$.

Снова по лемме 4.1.7 из [5] получим $p^2_{22} = (p^2_{11}b_1 + p^2_{12}(a_2 - a_1) + p^2_{13}c_3 - p^2_{02}b_0)/\mu = 23$, $p^3_{23} = (p^3_{12}b_2 + p^3_{13}(a_3 - a_1) - p^3_{03}b_0)/\mu = 28$ и $p^3_{33} = (p^3_{22}b_2 + p^3_{23}(a_3 - a_2) - p^3_{13}b_1)/c_3 = 37$.

Теперь очевидно, что граф Γ_3 является сильно регулярным с параметрами (135,70,37,35). Лемма доказана.

Интересно, что граница Хоффмана для коклик дистанционно регулярного графа [5, предложение 1.3.2] с массивом пересечений $\{8,7,5;1,1,4\}$ равна 45, причем любая вершина вне произвольной 45-коклики C смежна точно с 4 вершинами из C.

2. Характеры конечных групп и автоморфизмы дистанционно регулярных графов

Доказательство теоремы опирается на предложенный Хигменом метод работы с автоморфизмами дистанционно регулярного графа, представленный в третьей главе монографии Камерона [1]. При этом графу Γ диаметра d на n вершинах отвечает симметричная схема отношений $(X, \mathcal{R})$ с d классами, где X — множество вершин графа, R_0 — отношение равенства на X, и для $i \le 1$ класс R_i состоит из пар (u, w) таких, что $d(u,w) = i$. Для $u \in \Gamma$ положим $n_i = |\Gamma_i(u)|$. Классу R_i отвечает граф Γ_i на множестве вершин X, в котором вершины u, w смежны, если $(u,w) \in R_i$. Пусть A_i — матрица смежности графа Γ_i для $i > 0$ и $A_0 = I$ — единичная матрица. Тогда $A_iA_j = \sum p^l_{ij}A_l$ для подходящих неотрицательных целых p^l_{ij}.

Пусть P_i — матрица, в которой на месте (j,l) стоит p^l_{ij}. Тогда собственные значения $k = p_1(0), ..., p_1(d)$ матрицы P_1 являются собственными значениями графа Γ кратностей $m_0 = 1, ..., m_d$. Заметим, что матрица P_j является значением некоторого рационального многочлена от P_1, поэтому упорядочение собственных значений матрицы P_1 задает порядок на множестве собственных значений матрицы P_j. Матрицы P и Q, у которых на месте (i,j) стоят $p_j(i)$ и $q_j(i) = m_jp_i(j)/n_i$ соответственно, называются первой и второй матрицей собственных значений схемы и связаны равенством $PQ = QP = |X|I$, где I — единичная матрица порядка $d+1$.

Предложение. *Пусть u_j и w_j — левый и правый собственные векторы матрицы P_1, отвечающие собственному значению $p_1(j)$ и имеющие первую координату* 1. *Тогда кратность m_j собственного значения $p_1(j)$ равна* $\dfrac{n}{\langle u_j, w_j\rangle}$.

Доказательство. См. теорему 17.12 из [6].

Фактически из доказательства теоремы 17.12 следует, что w_j являются столбцами матрицы P и $m_j u_j$ являются строками матрицы $Q = \|Q_{ij}\|$.

Подстановочное представление группы $G = \mathrm{Aut}(\Gamma)$ на вершинах графа Γ обычным образом дает матричное представление ψ группы G в $GL(n, \mathbf{C})$. Пространство $\mathbf{C}^n$ является ортогональной прямой суммой $W_0 \oplus ... \oplus W_d$ собственных G-инвариантных подпространств матрицы смежности A_1 графа Γ. Для любого $g \in G$ матрица $\psi(g)$ перестановочна с A_1, поэтому подпространство W_i является $\psi(G)$-инвариантным. Пусть χ_i — характер проекции представления ψ на подпространство W_i. Тогда [1, § 3.7] для $g \in G$ получим $\chi_i(g) = n^{-1}\sum_{j=0}^{d} Q_{ij}\alpha_j(g)$, где $\alpha_j(g)$ — число точек x из X таких, что $(x, x^g) \in R_j$. Заметим, что значения характеров являются целыми алгебраическими числами, и поэтому, если в соответствии с выписанным равенством $\chi_i(g)$ — число рациональное (например, если все Q_{ij} рациональные), то на самом деле $\chi_i(g)$ — обыкновенное целое число.

С этого момента и до конца статьи Γ — дистанционно регулярный граф с массивом пересечений $\{8, 7, 5; 1, 1, 4\}$, а $G = \mathrm{Aut}(\Gamma)$. Тогда, очевидно,

$$P_1 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 8 & 0 & 1 & 0 \\ 0 & 7 & 2 & 4 \\ 0 & 0 & 5 & 4 \end{pmatrix}.$$

Лемма 2.1. *Пусть u_j и w_j — левый и правый собственные векторы матрицы P_1, отвечающие собственному значению $p_1(j)$ и имеющие первую координату* 1. *Тогда*

(1) $u_0 = (1, 1, 1, 1)$, $w_0 = (1, 8, 56, 70)^t$,

(2) $u_1 = (1, 3/8, 1/56, -1/14)$, $w_1 = (1, 3, 1, -5)^t$,

(3) $u_2 = (1, -1/8, -1/8, 1/10)$, $w_2 = (1, -1, -7, 7)^t$,

(4) $u_3 = (1, -1/2, 1/7, -1/14)$, $w_3 = (1, -4, 8, -5)^t$.

Доказательство сводится к прямым вычислениям. Рассмотрим, например, случай $p_1(1) = 3$. Тогда

$$P_1 - 3I = \begin{pmatrix} -3 & 1 & 0 & 0 \\ 8 & -3 & 1 & 0 \\ 0 & 7 & -1 & 4 \\ 0 & 0 & 5 & 1 \end{pmatrix}.$$

Если $(P_1 - 3I)(1, x_2, x_3, x_4)^t = 0$, то $x_2 = 3$, $x_3 = 1$, $x_4 = -5$, поэтому $w_1 = (1, 3, 1, -5)^t$. Аналогично вычисляется u_1.

Лемма 2.2. *Пусть $g \in G$ и χ_2 (соответственно, χ_3) — характер проекции представления ψ на собственное подпространство размерности* 50 (*соответственно,* 30). *Тогда* $\chi_2(g) = (5\alpha_0(g) + \alpha_3(g))/12 - 25/4$, $\chi_3(g) = (7\alpha_0(g) + 3\alpha_2(g) + 2\alpha_3(g))/21 - 15$.

Доказательство. По лемме 2.1 имеем

$$Q = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 54 & 81/4 & 27/28 & -27/7 \\ 50 & -25/4 & -25/4 & 5 \\ 30 & -15 & 30/7 & -15/7 \end{pmatrix}.$$

Поэтому $\chi_2(g) = 1/135(50\alpha_0(g) - 25\alpha_1(g)/4 - 25\alpha_2(g)/4 + 5\alpha_3(g))$ и $\chi_2(g) = (40\alpha_0(g) - 5\alpha_1(g) - 5\alpha_2(g) + 4\alpha_3(g))/108$. Подставляя $\alpha_1(g) + \alpha_2(g) = 135 - \alpha_0(g) - \alpha_3(g)$, получим $\chi_2(g) = (5\alpha_0(g) + \alpha_3(g))/12 - 25/4$.

Далее, $\chi_3(g) = 1/135(30\alpha_0(g) - 15\alpha_1(g) + 30\alpha_2(g)/7 - 15\alpha_3(g)/7)$. Подставляя $\alpha_1(g) = 135 - \alpha_0(g) - \alpha_2(g) - \alpha_3(g)$, получим $\chi_3(g) = (7\alpha_0(g) + 3\alpha_2(g) + 2\alpha_3(g))/21 - 15$.

Лемма 2.3. *Пусть g — автоморфизм простого порядка p графа Γ, $\mathrm{Fix}(g)$ — пустой граф и γ — число $\langle g\rangle$-орбит, являющихся кликами в графе Γ_3. Тогда выполняется одно из утверждений*:

(1) $p = 5$ *и либо*

(*i*) $\gamma = 3$, Γ *имеет* 24 *пятиугольные $\langle g\rangle$-орбиты и число орбит, в которых вершина смежна с ее образом под действием g, равно* $17, 12$ *или* 7, *либо*

(*ii*) Γ *имеет* 17 *пятиугольных $\langle g\rangle$-орбит и число орбит, в которых вершина смежна с ее образом под действием g, равно* 12 *или* 5, *либо*

(*iii*) Γ *имеет* 10 *пятиугольных $\langle g\rangle$-орбит и число орбит, в которых вершина смежна с ее образом под действием g, равно* 5, *либо*

(*iv*) Γ *имеет* 9 *пятиугольных $\langle g\rangle$-орбит и число орбит, в которых вершина смежна с ее образом под действием g, равно* 8 *или* 1, *либо*

(*v*) Γ *имеет* 2 *пятиугольные $\langle g\rangle$-орбиты и число орбит, в которых вершина смежна с ее образом под действием g, равно* 1;

(2) $p = 3$, $(\alpha_2(g), \alpha_3(g)) = (24, 111)$ *или* $(108, 27)$.

Доказательство. Так как $135 = 5 \cdot 27$, то $p = 3$ или 5. Из целочисленности $\chi_2(g)$ следует, что $\alpha_3(g)/3 - 1$ делится на 4 и $\alpha_3(g) = 12s + 3$ для некоторого неотрицательного целого числа s. Из целочисленности $\chi_3(g)$ следует, что $\alpha_2(g) + 2\alpha_3(g)/3$ делится на 7.

Пусть $p = 5$. Тогда $\alpha_3(g) = 15$ или 75. Если $\alpha_3(g) = 15$, то $\alpha_2(g) + 10$ делится на 7 и $\alpha_2(g) = 25, 60$ или 95. Если $\alpha_3(g) = 75$, тогда $\alpha_2(g) + 50$ делится на 7 и $\alpha_2(g) = 20$ или 55. Теперь тройка $(\alpha_1(g), \alpha_2(g), \alpha_3(g))$ совпадает с (95,25,15), (60,60,15), (25,95,15), (40,20,75) или (5,55,75).

Если вершина u смежна с u^g, то $u^{\langle g\rangle}$ — пятиугольник и $d(u, u^{g^2}) = 2$. Если $d(u, u^g) = 3$, то в графе Γ_3 орбита $u^{\langle g\rangle}$ является пятиугольником или кликой. Пусть γ — число кликовых $\langle g\rangle$-орбит в графе Γ_3. Тогда $\alpha_2(g^2) - \alpha_1(g) - (\alpha_3(g) - \gamma)$ — число $\langle g\rangle$-орбит, в которых вершины попарно находятся на расстоянии 2 в графе Γ. Ясно, что указанное число совпадает с $\alpha_2(g) - \alpha_1(g^2) - (\alpha_3(g^2) - \gamma)$.

Если $\alpha_1(g) = 95$, то $\alpha_2(g^2) = 95$, $\gamma = 3$ и Γ имеет 24 пятиугольные $\langle g\rangle$-орбиты. Если $\alpha_1(g) = 60$, то $\alpha_2(g^2) = 60$ или 95. В первом случае $\gamma = 3$ и Γ имеет 24 пятиугольные $\langle g\rangle$-орбиты. Во втором случае Γ имеет 17 пятиугольных $\langle g\rangle$-орбит.

Если $\alpha_1(g) = 40$, то $\alpha_2(g^2) = 55, 60$ или 95. В случае $\alpha_2(g^2) = 55$ граф Γ имеет 9 пятиугольных $\langle g\rangle$-орбит, а в двух оставшихся случаях имеем $\alpha_1(g^2) > \alpha_2(g)$.

Если $\alpha_1(g) = 25$, то $\alpha_2(g^2) = 25, 55, 60$ или 95. В случае $\alpha_2(g^2) = 25$ граф Γ имеет 24 пятиугольные $\langle g\rangle$-орбиты и $\gamma = 3$. В случае $\alpha_2(g^2) = 95$ граф Γ имеет 10 пятиугольных $\langle g\rangle$-орбит. В случае $\alpha_2(g) = 55$ получим противоречие с равенством $\alpha_2(g^2) - \alpha_1(g) - (\alpha_3(g) - \gamma) = \alpha_2(g) - \alpha_1(g^2) - (\alpha_3(g^2) - \gamma)$. Наконец, в случае $\alpha_2(g^2) = 60$ граф Γ имеет 17 пятиугольных $\langle g\rangle$-орбит.

Если $\alpha_1(g) = 5$, то $\alpha_2(g^2) = 20, 25, 55, 60$ или 95. В случае $\alpha_2(g^2) = 20$ граф Γ имеет 9 пятиугольных $\langle g\rangle$-орбит и $\gamma = 3$. В случаях $\alpha_2(g) = 25$ или 60 получим $\alpha_2(g) < \alpha_1(g^2)$. В случае $\alpha_2(g) = 95$ получим противоречие с равенством $\alpha_2(g^2) - \alpha_1(g) - (\alpha_3(g) - \gamma) = \alpha_2(g) - \alpha_1(g^2) - (\alpha_3(g^2) - \gamma)$. Наконец, в случае $\alpha_2(g^2) = 55$ граф Γ имеет 2 пятиугольных $\langle g\rangle$-орбиты. Итак, в случае $p = 5$ выполняется утверждение (1).

Пусть $p = 3$. Так как $a_1 = 0$, то $\alpha_1(g) = 0$, поэтому $\chi_2(g) = 5 - \alpha_2(g)/12$, $\chi_3(g) = (\alpha_2(g) - 45)/7$. Отсюда $\alpha_2(g) = 24$ или 108, $\alpha_3(g) = 111$ или 27 соответственно.

Лемма 2.4. *Если Ω содержит вершину a, то $p \le 7$ и либо $p = 2$, либо $p = 7$, Ω является двухвершинной кликой, $\alpha_3(g) = 77$ и $\alpha_1(g) + \alpha_2(g) = 56$.*

Доказательство. Если $p > 7$, то $[a] \subset \Omega$ и ввиду связности Γ получим $\Gamma = \Omega$, противоречие.

Пусть $p = 7$. Тогда $|\Omega|$ сравнимо с 2 по модулю 7 и степень любой вершины в графе Ω равна 1 или 8. Если степень a в Ω равна 8, то для различных вершин $b, c \in [a]$ получим $[b] \cap \Gamma_3(c) \subset \Omega$, так как $p^2_{13} = 5$. Поэтому $[b] \subset \Omega$, и в силу связности Γ получим $\Gamma = \Omega$, противоречие.

Значит, Ω — объединение изолированных ребер. Если $b \in \Omega$ и $d(a, b) = i$, то $i \ne 2$, иначе $[a] \cap [b] \subset \Omega$. Если $i = 3$, то $[a] \cap \Gamma_3(b) \subset \Omega$, так как $p^3_{13} = 4$. Поэтому $[a] \subset \Omega$, противоречие. Итак, $\Omega = \{a, b\}$ является кликой.

Из целочисленности $\chi_2(g)$ следует, что $\alpha_3(g) - 5$ делится на 12. Отсюда $\alpha_3(g) = 77$ и $\alpha_1(g) + \alpha_2(g) = 56$. Если $p = 7$, то выполняется утверждение (1).

Пусть $p = 5$. Тогда $|\Omega|$ делится на 5 и степень любой вершины в графе Ω равна 3 или 8. Если $b \in \Omega$ и $d(a, b) = 3$, то $[b] \cap \Gamma_3(a) \subset \Omega$, так как $p^3_{13} = 4$. Отсюда $[a] \cup [b] \subset \Omega$. Для $c \in \Gamma_2(b) \cap [a]$ получим $|[c] \cap \Gamma_3(b)| = 5$, причем $[c] \cap \Gamma_3(b)$ содержит вершину a из Ω, поэтому $[c] \subset \Omega$ и Ω содержит шар радиуса 2 с центром a. Если $u \in \Gamma - \Omega$, то $|[u] \cap \Gamma_2(a)| = 4$, противоречие с тем, что $|[u] \cap [u^g]| \ge 4$.

Таким образом, диаметр графа Ω равен 2. По теореме 1.17.1 из [5] граф Ω сильно регулярен и поэтому является графом Петерсена.

Из целочисленности $\chi_2(g)$ следует, что $\alpha_3(g) = 25$ или 85. Если $\alpha_3(g) = 25$, то $\alpha_2(g) = 30$ или 65, если же $\alpha_3(g) = 85$, то $\alpha_2(g) = 25$. Таким образом, $(\alpha_1(g), \alpha_2(g), \alpha_3(g))$ совпадает с (70,30,25), (35,65,25) или (15,25,85). Так как $d(u, u^g) = 2$ для вершины u, смежной с вершиной из Ω, то $\alpha_2(g) \ge 50$, поэтому $\alpha_1(g) = 35$, $\alpha_2(g) = 65$ и $\alpha_3(g) = 25$. Но если вершины u, u^g смежны, то $d(u, u^{g^2}) = 2$ и $\alpha_2(g^2) \ge 85$, противоречие.

Пусть $p = 3$. Тогда $|\Omega|$ делится на 3 и степень любой вершины в графе Ω равна 2, 5 или 8. Пусть $b \in \Omega$. Если $d(a, b) = 3$, то ввиду леммы 1.3 подграф $\Omega(a)$ содержит 1 или 4 вершины из $\Gamma_2(b)$, 1 или 4 вершины из $\Gamma_3(b)$, подграф Ω содержит по вершине из $\Gamma_2(b) \cap \Gamma_3(a)$ и из $\Gamma_3(a) \cap \Gamma_3(b)$.

Если $d(a, b) = 2$, то $\Omega(a)$ содержит вершину из $[b]$, 2 вершины из $\Gamma_2(b)$, 2 или 5 вершин из $\Gamma_3(b)$, Ω содержит по 2 вершины из $\Gamma_2(a) \cap \Gamma_2(b)$ и из $\Gamma_3(a) \cap \Gamma_3(b)$. В частности, если $\Gamma_2(a)$ пересекает Ω, то степень a в Ω не меньше 5.

Если $d(a, b) = 1$, то $\Omega(a)$ содержит вершину из $\Gamma_2(b)$, Ω содержит по 2 вершины из $\Gamma_2(a) \cap \Gamma_2(b)$, из $\Gamma_2(a) \cap \Gamma_3(b)$ и из $\Gamma_3(a) \cap \Gamma_3(b)$. Таким образом, степень любой вершины в графе Ω равна 5 или 8.

Допустим, что Ω содержит вершину степени 8. Тогда Ω содержит вершину b степени 8, смежную с вершиной a, имеющей степень 5 в Ω. Пусть $u \in [a] - \Omega$. Так как $a_2 = 2$, то $\Omega(b) \cap \Gamma_2(u)$ содержит вершину c. Для $w \in [c] \cap [u]$ подграф $[c] \cap \Gamma_2(a)$ содержит 3 вершины w, w^g, w^{g^2}, противоречие с тем, что $a_2 = 2$.

Итак, Ω — регулярный граф степени 5 диаметра 3 с $a_2 = b_2 = 2$. Так как каждая вершина из $\Gamma - \Omega$ смежна не более чем с одной вершиной из Ω, то $3|\Omega| \le 135 - |\Omega|$, поэтому $|\Omega| \le 33$, $|\Omega_2(a)| = 20$ и $|\Omega_3(a)| \le 7$. Теперь число ребер между $\Omega_2(a)$ и $\Omega_3(a)$ равно 40, но не больше $7 \cdot 4$, противоречие. Лемма доказана.

3. Инволютивные автоморфизмы графа Γ

В этом параграфе предполагается, что t — инволютивный автоморфизм графа Γ и $\Omega = \mathrm{Fix}(t)$ содержит вершину a. Ω^i состоит из вершин, имеющих степень $2i$ в Ω, $\omega_i = |\Omega^i|$. Тогда $\sum \omega_i = |\Omega| = \alpha_0(t)$ и $8\omega_0 + 6\omega_1 + 4\omega_2 + 2\omega_3 = \alpha_2(t)$.

Лемма 3.1. *Выполняются следующие утверждения*:

(1) *если* Ω *является кокликой, то* $d(u,w)=3$ *для любых двух вершин* u,w *из* Ω, *и* $|\Omega|=3,5,7,9$ *или* 11;

(2) *если* $a,e\in\Omega$ *и* $d(a,e)\geq 2$, *то* $|\Gamma_2(a)\cap\Omega(e)|=|\Omega(a)\cap\Gamma_2(e)|$ *и любая связная компонента графа* $\Omega\cap\Gamma_2(a)$ *является одновершинным графом или многоугольником*;

(3) *если* Ω *содержит вершину* b *степени* 2 *и* $\Omega(b)=\{a,c\}$, *то вершина* c *изолирована в* $\Omega\cap\Gamma_2(a)$;

(4) Ω *не содержит вершин степени* 8 *и* $\alpha_1(t)+\alpha_3(t)\neq 0$.

Доказательство. Пусть $p=2$. Тогда $|\Omega|$ нечетно и степень любой вершины в графе Ω четна. Пусть $b\in\Omega$. Если $d(a,b)=3$, то ввиду леммы 1.3 подграф $\Omega(a)$ содержит четное число вершин из $\Gamma_2(b)$, подграф Ω содержит четное число вершин из $\Gamma_2(a)\cap\Gamma_2(b)$, а также из $\Gamma_2(a)\cap\Gamma_3(b)$ и нечетное число вершин из $\Gamma_3(a)\cap\Gamma_3(b)$.

Если $d(a,b)=2$, то $\Omega(a)$ содержит вершину из $[b]$, 0 или 2 вершины из $\Gamma_2(b)$ и нечетное число вершин из $\Gamma_3(b)$; подграф Ω содержит нечетное число вершин из $\Gamma_2(a)\cap\Gamma_2(b)$, а также из $\Gamma_3(a)\cap\Gamma_3(b)$.

Если $d(a,b)=1$, то $\Omega(a)$ содержит нечетное число вершин из $\Gamma_2(b)$, подграф Ω содержит нечетное число вершин из $\Gamma_2(a)\cap\Gamma_3(b)$, а также из $\Gamma_3(a)\cap\Gamma_3(b)$. Таким образом, если вершина b изолирована в графе Ω, то $\Omega-\{b\}\subset\Gamma_3(b)$.

Допустим, что Ω является ω-кокликой. Тогда Ω состоит из вершин, находящихся попарно на расстоянии 3, и по лемме 1.2 получим $|\Omega|\leq 15$. Для вершины u, находящейся на расстоянии 2 от u^t, подграф $[u]\cap[u^t]$ содержит вершину из Ω, поэтому $\alpha_2(t)=8\omega$. Так как p^2_{33} и p^2_{22} нечетны, то для $u\in[a]-\Omega$ подграфы $\Gamma_2(u)\cap\Gamma_2(u^t)$ и $\Gamma_3(u)\cap\Gamma_3(u^t)$ пересекают Ω, и $|\Omega|\geq 3$.

Из целочисленности $\chi_2(t)=(5\alpha_0(t)+\alpha_3(t))/12-25/4$ следует, что $\alpha_3(t)=12s+3-5\omega$ для некоторого целого числа s. Из целочисленности $\chi_3(t)=(7\alpha_0(t)+3\alpha_2(t)+2\alpha_3(t))/21-15$ заключаем, что $4s+1$ делится на 7. Отсюда $s=5$, $\alpha_3(t)=63-5\omega$, $\alpha_1(t)=72-4\omega$ и $\omega<13$. Итак, если Ω является кокликой, то выполняется утверждение (1).

Пусть $a,e\in\Omega$. Если $b\in\Gamma_2(a)\cap\Omega(e)$, то $[a]\cap[b]$ содержит единственную вершину из Ω, поэтому $|\Gamma_2(a)\cap\Omega(e)|\leq|\Omega(a)\cap\Gamma_2(e)|$. Симметрично, $|\Gamma_2(e)\cap\Omega(a)|\leq|\Omega(e)\cap\Gamma_2(a)|$, поэтому $|\Gamma_2(e)\cap\Omega(a)|=|\Omega(e)\cap\Gamma_2(a)|$. Так как степень любой вершины в графе $\Omega\cap\Gamma_2(a)$ равна 0 или 2, то любая связная компонента графа $\Omega\cap\Gamma_2(a)$ является одновершинным графом или многоугольником. Утверждение (2) доказано.

Допустим, что степень вершины b в графе Ω равна 2, и положим $\Omega(b)=\{a,c\}$. Если $\Omega(c)\cap\Gamma_2(a)$ содержит вершину d, то $\Omega(b)$ содержит две вершины из $\Gamma_2(d)$, противоречие. Утверждение (3) доказано.

Допустим, что $\alpha_1(t)=\alpha_3(t)=0$. Тогда $\alpha_2(t)=135-\alpha_0(t)$. Из целочисленности $\chi_2(t)=(5\alpha_0(t)+\alpha_3(t))/12-25/4$ следует, что $\alpha_0(t)/3$ сравнимо с 1 по модулю 4 и $\alpha_0(t)=12s+3$. Из целочисленности $\chi_3(t)=(7\alpha_0(t)+3\alpha_2(t)+2\alpha_3(t))/21-15$ заключаем, что $\alpha_2(t)=14r$ и $12s+3+14r=135$. Отсюда $r=6$, $s=4$, $\alpha_0(t)=51$ и $|\Omega|=51$. Далее, для $u\in\Gamma-\Omega$ и $a\in[u]\cap\Omega$ подграф $\Gamma_2(u)\cap\Gamma_2(u^t)$ содержит не более 6 вершин из $\Omega(a)$ и не более 7 вершин из $\Omega-a^{\perp}$, и тогда $|\Omega|\leq 49$. Противоречие.

Пусть вершина a имеет степень 8 в Ω. Ввиду утверждения (1) каждая вершина из $\Omega\cap\Gamma_3(a)$ смежна с 4 вершинами из графа $\Omega\cap\Gamma_2(a)$, и поэтому $\Omega\cap\Gamma_2(a)$ является регулярным графом степени 2. Ввиду утверждения (2) степень каждой вершины из $[a]$ в Ω не меньше 4. Поэтому $|\Omega\cap\Gamma_2(a)|\geq 24$, $|\Omega\cap\Gamma_3(a)|\geq 6$ и $|\Omega|\geq 39$.

Как показано выше, некоторая вершина u из $\Gamma-\Omega$ не смежна с вершинами из Ω. Если $d(u,u^t)=1$, то $|\Gamma_2(u)\cap\Gamma_2(u^t)|=14$ и $|\Omega\cap\Gamma_2(u)|\leq 6$. В этом случае вершина из $\Gamma_2(u)\cap\Gamma_2(u^t)-\Omega$ смежна с 4 или 5 вершинами из $\Gamma_3(u)\cap\Gamma_3(u^t)$ и $|\Omega|\leq 6+(35-3)$, противоречие. Если же $d(u,u^t)=3$, то $|\Gamma_2(u)\cap\Gamma_2(u^t)|=24$ и $|\Omega\cap\Gamma_2(u)|\leq 8$. Пусть $w\in\Gamma_2(u)\cap\Gamma_2(t)-\Omega$. Тогда $[w]$ содержит не более двух вершин из $\Gamma_2(u)\cap\Gamma_3(u^t)$ и не менее трех вершин из $\Gamma_3(u)\cap\Gamma_3(u^t)$. Таким образом, число ребер между $\Gamma_2(u)\cap\Gamma_2(u^t)-\Omega$ и $\Gamma_3(u)\cap\Gamma_3(u^t)-\Omega$ не меньше 48. Однако каждая вершина из $\Gamma_3(u)\cap\Gamma_3(u^t)$ смежна не более чем с 4 вершинами из $\Gamma_2(u)\cap\Gamma_2(u^t)-\Omega$ и $|\Gamma_3(u)\cap\Gamma_3(u^t)-\Omega|\geq 12$. Противоречие с тем, что тогда $|\Omega\cap\Gamma_3(u)|\leq 23$ и $|\Omega|\leq 31$.

Лемма 3.2. *Если некоторая вершина z изолирована в Ω, но Ω не является кокликой, то $|\Omega|\leq 15$, степень каждой вершины в Ω не больше 4 и либо Ω содержит две вершины степени 4, восемь вершин степени 2 и одну или три вершины степени 0, либо Ω содержит шестиугольник и изолированную вершину.*

Д о к а з а т е л ь с т в о. При условиях леммы $\Omega-\{z\}\subset\Gamma_3(z)$ и для любой вершины $a\in\Omega-\{z\}$ подграф $[a]\cap\Gamma_2(z)$ содержит 4 вершины, не лежащие в Ω. В частности, степень вершины a в графе Ω не больше 4. Заметим, что каждая вершина из $\Omega-\{z\}$ смежна с 4 вершинами из $\Gamma_2(z)$, а некоторая вершина из $\Gamma_2(z)$ смежна не более чем с одной вершиной из Ω. Так как $|\Gamma_2(z)|=56$, то $|\Omega-\{z\}|\leq 14$.

Допустим, что степень вершины a в графе Ω равна 4. Если $\Omega(a)$ содержит вершину b, имеющую степень 4 в Ω, то Ω содержит 5 вершин из $a^{\perp}$, не менее 6 вершин из $\Gamma_2(a)$ и не менее 3 вершин из $\Gamma_3(a)\cap\Gamma_2(b)$. В этом случае $|\Omega|=15$, Ω содержит 12 вершин степени 2 и $\Gamma_3(z)-\Omega$ содержит 24 вершины, смежные с вершинами из Ω. Поэтому $\alpha_1(t)+\alpha_3(t)=70-14-24=32$, $\alpha_2(t)=8+4\cdot 2+6\cdot 12=88$. Из целочисленности $\chi_2(t)=(5\alpha_0(t)+\alpha_3(t))/12-25/4$ следует, что $\alpha_3(t)=12s$. Из целочисленности $\chi_3(t)=(7\alpha_0(t)+3\alpha_2(t)+2\alpha_3(t))/21-15$ заключаем, что $2s+1$ делится на 7. Отсюда $s=3$ и $\alpha_3(t)=36$, противоречие.

Пусть $b\in\Omega(a)$. Если $\Omega(b)-\{a\}$ содержит вершину c, имеющую степень 4 в графе Ω, то $\Omega\cap\Gamma_2(b)$ содержит 6 вершин и $|\Omega\cap\Gamma_3(b)|=9$, противоречие. Значит, $\Omega(a)=\{b_1,...,b_4\}\subseteq\Omega^2$ и $\Omega(b_i)=\{a,c_i\}$. Если $e\in\Omega(c_1)-\{b_1\}$, то $\Omega\cap\Gamma_2(b_1)=\{b_2,b_3,b_4,e\}$ и каждая вершина c_j смежна с e, поэтому степень c_j в графе Ω равна 2 и степень e в графе Ω равна 4. Таким образом, подграф $\Delta=\{a,e,b_1,..,b_4,c_1,...,c_4\}$ является связной компонентой графа Ω. Пусть $|\Omega|=10+i$. Тогда $\alpha_2(t)=8i+4\cdot 2+6\cdot 8=56+8i$ и $\alpha_1(t)+\alpha_3(t)=69-9i$. Из целочисленности $\chi_2(t)=(5\alpha_0(t)+\alpha_3(t))/12-25/4$ следует, что $\alpha_3(t)=12s-5i+1$. Из целочисленности $\chi_3(t)=(7\alpha_0(t)+3\alpha_2(t)+2\alpha_3(t))/21-15$ заключаем, что $s+3$ делится на 7. Отсюда $s=4$, $\alpha_3(t)=49-5i$ и $\alpha_1(t)=20-4i$. Заметим, что для любых двух вершин z,z', изолированных в Ω, подграф $\Gamma_2(z')\cap\Gamma_2(z'')$ содержит 24 вершины, 8 из которых попадают в $[a]\cup[e]$. Если $i=5$, то для любых трех вершин z,z',z'', изолированных в Ω, подграф $\Gamma_2(z')\cap\Gamma_2(z'')$ содержит 24 вершины из $\Gamma_3(z)$, противоречие. Значит, $i\leq 3$.

Пусть степень каждой вершины в Ω равна 0 или 2. Тогда каждая связная компонента графа Ω является одновершинным графом или шестиугольником. Допустим, что Ω содержит два изолированных 6-цикла $\Phi=\{a_1,...,a_6\}$ и $\Psi=\{b_1,...,b_6\}$. Тогда $|\Gamma_2(a_1)\cap\Gamma_2(a_2)|=14$ и каждая вершина из Ψ смежна с 2 вершинами из $\Gamma_2(a_1)\cap\Gamma_2(a_2)$. Далее, a_3 смежна с 2 вершинами из $\Gamma_2(a_1)$, попадающими в $\Gamma_2(a_1)\cap\Gamma_2(a_2)$. Противоречие с тем, что число ребер между Ω и $\Gamma_2(a_1)\cap\Gamma_2(a_2)$ не меньше 16.

Пусть Ω содержит шестиугольник и β изолированных вершин. Тогда $\alpha_2(t)=8\beta+36$ и $\alpha_1(t)+\alpha_3(t)=93-9\beta$. Из целочисленности $\chi_2(t)=(5\alpha_0(t)+\alpha_3(t))/12-25/4$ следует, что $\alpha_3(t)=12s-5\beta-3$, $\alpha_1(t)=96-12s-4\beta$. Из целочисленности $\chi_3(t)=(7\alpha_0(t)+3\alpha_2(t)+2\alpha_3(t))/21-15$ следует, что $s-1$ делится на 7, поэтому $s=1$, $\alpha_3(t)=9-5\beta$ и $\beta=1$. Лемма доказана.

В леммах 3.3–3.6 предполагается, что Ω не содержит изолированных вершин.

Лемма 3.3. *Выполняются следующие утверждения*:

(1) *если Ω^1 содержит смежные вершины a,b и степень вершины c из $\Omega(a)-\{b\}$ в графе Ω равна i, то для связной компоненты Δ графа Ω, содержащей a, получим $|\Delta|=2+2i$*;

(2) *подграф Ω^1 является кокликой*;

(3) *окрестность каждой вершины из Ω^1 содержится в Ω^3.*

Д о к а з а т е л ь с т в о. Пусть $\Omega(c)=\{a,d_1,...,d_{i-1}\}$ и $\Omega(b)=\{a,e\}$. Каждая вершина f_j из $\Omega(d_j)\cap\Gamma_3(a)$ смежна с двумя вершинами из $\Omega\cap\Gamma_2(a)$, поэтому f_j смежна с e. Тогда степень d_j в графе Ω равна 2 и степень e в графе Ω равна i. Таким образом, степень f_j в Ω равна 2 и подграф $\{c, a, b, e, d_1, .., d_{i-1}, f_1, ..., f_{i-1}\}$ является связной компонентой графа Ω. Утверждение (1) доказано.

Пусть Δ — связная компонента графа Ω, содержащая смежные вершины a, b из Ω^1. По утверждению (1) имеем $|\Delta| = 6, 10$ или 14. Положим $\Phi = \Omega \cap \Gamma_3(a)$.

Если Δ является шестиугольником, то каждая вершина из Φ смежна с 4 вершинами из $\Gamma_2(a) - \Omega$. Далее, $|\Gamma_2(a) - \Omega| = 54$ и $\Gamma_2(a) - \Omega$ содержит $12+4+2$ вершин, смежных с вершинами из $\Omega(a)$. Поэтому $4|\Phi| \leq 36$, и подграф Φ не содержит вершин степени 6 и ребер графа Ω^1. Если z — вершина степени 4 графа Φ, то $\Phi(z) \subset \Omega^1$ (иначе $|\Phi| > 9$). Поэтому $\Phi_2(z)$ является 4-кликой, противоречие.

Пусть $|\Delta| = 10$. Тогда $|\Gamma_2(a) - \Omega| = 52$ и $\Gamma_2(a) - \Omega$ содержит $10 + 8 + 6$ вершин, смежных с вершинами из $\Delta - \{a\}$. Поэтому $4|\Omega \cap \Gamma_3(a)| \leq 28$ и $|\Omega \cap \Gamma_3(a)| \leq 7$. Аналогичное противоречие получим в случае $|\Delta| = 14$. Утверждение (2) доказано.

Пусть $a \in \Omega^1$ и $\Omega(a)$ содержит две вершины b, c из Ω^2, $\Omega(b) \cap \Gamma_2(a) = \{b_1, b_2, b_3\}$ и $\Omega(c) \cap \Gamma_2(a) = \{c_1, c_2, c_3\}$. Тогда $\Omega \cap \Gamma_2(a)$ является кокликой и каждая вершина из $\Omega(b_i) - \{b\}$ смежна с вершиной из $\{c_1, c_2, c_3\}$. Поэтому степени вершин b_j, c_i в Ω не больше 4.

Если $\Omega(b) \subset \Omega^1$, то $\Omega(c) \subset \Omega^1$ и вершины c_1, c_2, c_3 можно упорядочить так, что $[b_i] \cap [c_i]$ содержит вершину e_i. По структуре шара радиуса 3 с центром b_1 подграф $[e_1] \cap [e_j]$ содержит единственную вершину e_{1j}, попадающую в Ω^1 для $j \in \{2, 3\}$. Далее, шар радиуса 3 в Ω с центром e_{12} содержит вершины b_1, c_1, e_{13} из $[e_1]$, вершины b_2, c_2, e_{23} из $[e_2]$ и вершины b, c, e_3 из $\Gamma_3(e_{12})$. Таким образом, a лежит в связной компоненте Ψ графа Ω, $|\Psi| = 15$, и $\Psi = \Omega$. Далее, $\omega_1 = 10$, $\omega_2 = 5$, $\alpha_2(t) = 60 + 20 = 80$ и $\alpha_1(t) + \alpha_3(t) = 40$. Из целочисленности $\chi_2(t) = (5\alpha_0(t) + \alpha_3(t))/12 - 25/4$ следует, что $\alpha_3(t) = 12s$. Из целочисленности $\chi_3(t) = (7\alpha_0(t) + 3\alpha_2(t) + 2\alpha_3(t))/21 - 15$ следует, что $s + 3$ делится на 7, противоречие.

Если степень вершины b_1 в графе Ω равна 4, то вершины e_1, e_2, e_3 из $\Omega(b_1) \cap \Gamma_3(a)$ можно упорядочить так, что e_i смежна с c_i. Без ограничения общности некоторая вершина из $\Omega(b_2) \cap \Gamma_3(a)$ смежна с c_1. Тогда степень вершины c_1 в графе Ω равна 4 и вершины d_1, d_2, d_3 из $\Omega(c_1) \cap \Gamma_3(a)$ можно упорядочить так, что d_i смежна с b_i (очевидно, $d_1 = e_1$). Если одна из вершин b_2, b_3, c_2, c_3 имеет степень 4 в графе Ω, то все эти вершины имеют степень 4 в графе Ω.

Допустим, что вершины b_2, b_3, c_2, c_3 имеют степень 2 в графе Ω. Тогда каждая из вершин d_2, d_3, e_2, e_3 имеет в графе Ω степень, не меньшую 4. Так как $\Omega(b) \cap \Gamma_2(b_2)$ содержит две вершины из Ω^1, то степень e_2 в графе Ω равна 4. По структуре шара радиуса 3 с центром b_2 подграф $[d_i] \cap [e_2]$ содержит вершину f_{i2}, имеющую степень 2 в графе Ω. Теперь $\Gamma_2(a) - \Omega$ содержит 50 вершин, $8 + 12$ из которых смежны с вершинами из $\Omega \cap ([a] \cup \Gamma_2(a))$, и число ребер между $\Omega \cap \Gamma_3(a)$ и $\Gamma_2(a) - \Omega$ не больше 30. Однако, $\Omega \cap \Gamma_3(a)$ содержит 5 вершин, смежных с парами вершин из $\Omega \cap \Gamma_2(a)$, и 4 вершины f_{ij}. Таким образом, $|\Omega| = 19$ и вершина z из Ω, не попадающая в $\cup_{i=1}^{3}(\Gamma_2(b_i) \cap \Omega)$, изолирована в Ω. Противоречие с леммой 3.2.

Допустим, что вершины b_2, b_3, c_2, c_3 имеют степень 4 в Ω. Через g_{ij} обозначим вершину, смежную с b_i, c_j. Тогда $\Gamma_2(a) - \Omega$ содержит 50 вершин, $8 + 12$ из которых смежны с вершинами из $\Omega \cap ([a] \cup \Gamma_2(a))$, и число ребер между $\Omega \cap \Gamma_3(a)$ и $\Gamma_2(a) - \Omega$ не больше 30. Между тем $\Omega \cap \Gamma_3(a)$ содержит точно 9 вершин $\{g_{ij}\}$, смежных с парами вершин из $\Omega \cap \Gamma_2(a)$, и не более трех вершин, не смежных с вершинами из $\Omega \cap \Gamma_2(a)$. Таким образом, $|\Omega| = 19$ или 21. Если $|\Omega| = 19$, то $\Omega \cap \Gamma_3(a) - \{g_{ij}\}$ содержит единственную вершину z. Так как z не может быть смежна с 4 вершинами из $\{g_{ij}\}$, то можно считать, что z смежна с g_{11}, g_{22}. Отсюда степени вершин g_{11}, g_{22} в графе Ω равны 4 и g_{11}, g_{22} смежны с g_{33}. Противоречие с тем, что $[g_{11}] \cap [g_{22}] = \{g_{33}, z\}$.

Значит, $|\Omega| = 21$ и из целочисленности $\chi_2(t) = (5\alpha_0(t) + \alpha_3(t))/12 - 25/4$ следует, что $\alpha_3(t) = 6s$. Если подграф $\{g_{ij}\}$ не является кокликой, то он содержит многоугольник Σ. Без ограничения общности g_{11} принадлежит Σ и $\Sigma(g_{11}) \subset \{g_{22}, g_{23}, g_{32}, g_{33}\}$. Для определенности пусть $\Sigma(g_{11}) = \{g_{22}, g_{23}\}$. Тогда $\Sigma(g_{22}) \subset \{g_{11}, g_{13}, g_{31}, g_{33}\}$ и $g_{33} \in \Sigma(g_{22})$, противоречие. Поэтому подграф $\{g_{ij}\}$ является кокликой.

Далее, $\Omega \cap \Gamma_3(a) - \{g_{ij}\}$ содержит 3 вершины z_1, z_2, z_3, и каждая вершина из $\{g_{ij}\}$ смежна с четным числом вершин из $\{z_1, z_2, z_3\}$. Если вершины z_1, z_2, z_3 попарно не смежны, то $\omega_1 = 10$, $\omega_2 = 11$ и некоторая вершина из Ω^2 смежна с 2 вершинами из Ω^1, противоречие.

Если вершина z_1 смежна с z_2, z_3, то каждая вершина из $\{g_{ij}\}$ смежна не более чем с одной вершиной из $\{z_1, z_2, z_3\}$, противоречие.

Итак, можно считать, что вершины z_2, z_3 не смежны с z_1, но z_2 смежна с z_3. В этом случае можно считать, что $z_1, z_2 \in \Omega^2$ и $z_3 \in \Omega^1$. Поэтому $\omega_1 = 7$, $\omega_2 = 14$, $\alpha_2(t) = 42 + 56$ и $\alpha_1(t) + \alpha_3(t) = 26$. Из целочисленности $\chi_3(t) = (7\alpha_0(t) + 3\alpha_2(t) + 2\alpha_3(t))/21 - 15$ следует, что s делится на 7, противоречие.

Допустим, что $\Omega(a)$ содержит вершину b из Ω^2 и вершину c из Ω^3. Положим $\beta_i = |(\Omega(b) - \{a\}) \cap \Omega^i|$, $\gamma_i = |(\Omega(c) - \{a\}) \cap \Omega^i|$. Тогда $\beta_2 + \beta_3 = 3$, $\gamma_2 + \gamma_3 = 5$ и $2\beta_2 + 3\beta_3 = 2\gamma_2 + 3\gamma_3$. Отсюда $\gamma_2 - \beta_2 = 6$ и $\beta_3 - \gamma_3 = 4$, противоречие. Итак, $\Omega(a)$ содержит две вершины b, c из Ω^3. Лемма доказана.

Лемма 3.4. *Выполняются следующие утверждения:*

(1) *если* $\alpha_1(t) \neq 0$, *то* $|\Omega| \leq 29$;

(2) $\omega_3 \neq 0$.

Доказательство. Пусть $d(u, u^t) = 1$. Так как $p^1_{22} = 14$, то $|\Omega \cap \Gamma_2(u)| \leq 6$. Если $w \in \Gamma_2(u) \cap \Gamma_2(u^t)$, то $[w]$ содержит либо по вершине из $\Gamma_2(u) \cap \Gamma_3(u^t)$ и из $\Gamma_3(u) \cap \Gamma_2(u^t)$ и 4 вершины из $\Gamma_3(u) \cap \Gamma_3(u^t)$, либо вершину из $\Gamma_2(u) \cap \Gamma_2(u^t)$ и 5 вершин из $\Gamma_3(u) \cap \Gamma_3(u^t)$. В частности, число ребер между $\Gamma_2(u) \cap \Omega$ и $\Gamma_3(u) \cap \Gamma_3(u^t)$ не больше 30.

Пусть $e \in \Gamma_3(u) \cap \Gamma_3(u^t) \cap \Omega$ и $[e]$ содержит i вершин из $\Gamma_2(u) \cap \Gamma_3(u^t)$. Тогда $[u]$ содержит по $4 - i$ вершин из $\Gamma_2(u) \cap \Gamma_2(u^t)$ и из $\Gamma_3(u) \cap \Gamma_3(u^t)$. Так как $\omega_0 = 0$, то $i < 4$. Пусть число вершин из $\Gamma_3(u) \cap \Omega$, смежных с 3 вершинами из $\Gamma_2(u) \cap \Gamma_3(u^t)$, равно γ.

Пусть $|\Gamma_2(u) \cap \Omega| \leq 4$. Тогда число вершин из $\Gamma_3(u) \cap \Omega$, смежных с 2 вершинами из $\Gamma_2(u) \cap \Gamma_2(u^t) - \Omega$, не больше 5, а смежных с 2 вершинами из $\Gamma_2(u) \cap \Gamma_2(u^t) \cap \Omega$, не меньше $|\Omega| - 4 - 5 - \gamma$. Так как число ребер между $\Gamma_2(u) \cap \Omega$ и $\Gamma_3(u) \cap \Omega$ не меньше $\gamma + 2(|\Omega| - 9 - \gamma)$, но не больше 20, то $|\Omega| \leq 19 + \gamma/2$.

Если $|\Gamma_2(u) \cap \Omega| = 6$, то число вершин из $\Gamma_3(u) \cap \Omega$, смежных с 2 вершинами из $\Gamma_2(u) \cap \Gamma_2(u^t) - \Omega$, не больше 4, а смежных с 2 вершинами из $\Gamma_2(u) \cap \Gamma_2(u^t) \cap \Omega$, не меньше $|\Omega| - 6 - 4 - \gamma$. Так как число ребер между $\Gamma_2(u) \cap \Omega$ и $\Gamma_3(u) \cap \Omega$ не меньше $\gamma + 2(|\Omega| - 10 - \gamma)$, но не больше 30, то $|\Omega| \leq 25 + \gamma/2$. Утверждение (1) следует из того, что $\gamma \leq 11$.

Допустим, что $\omega_3 = 0$. По лемме 3.3 имеем $\omega_1 = 0$, поэтому $\alpha_0(t) = \omega_2$, $\alpha_2(t) = 4\omega_2$ и $\alpha_1(t) + \alpha_3(t) = 135 - 5\omega_2$. Из целочисленности $\chi_2(t) = (5\alpha_0(t) + \alpha_3(t))/12 - 25/4$ следует, что $\alpha_3(t) = 12s - 5(\omega_2 - 3)$ и $\alpha_1(t) = 120 - 12s$. Из целочисленности $\chi_3(t) = (7\alpha_0(t) + 3\alpha_2(t) + 2\alpha_3(t))/21 - 15$ заключаем, что $3\omega_2 + s + 3$ делится на 7. Так как $5\omega_2 < 135$, то $|\Omega| < 27$. Заметим, что $s \leq 10$ и в случае $|\Omega| = 25$ получим $s = 10$.

Если $s = 10$, то $\alpha_1(t) = \omega_1 = 0$ и $\omega_2 = 7r + 5 = 19$. В этом случае для $a \in \Omega$ имеем $|\Gamma_2(a) \cap \Omega| = 12$ и $|\Gamma_3(a) \cap \Omega| = 2$. Противоречие с тем, что число ребер между $\Gamma_2(a) \cap \Omega$ и $\Gamma_3(a) \cap \Omega$ не меньше 12, но не больше 8. Итак, $s < 10$ и $|\Omega| \leq 23$. Если $|\Omega| = 23$, то $s + 2$ делится на 7, $s = 5$ и $\alpha_3(t) = -40$. Если $|\Omega| = 21$, то $s = 4$ и $\alpha_3(t) = -42$. Если $|\Omega| = 19$, то $s + 4$ делится на 7, $s = 4$ и $\alpha_3(t) = -32$.

Но для $a \in \Omega$ шар радиуса 2 с центром a содержит $1 + 4 + 12$ вершин. Лемма доказана.

Лемма 3.5. *Если вершина a имеет степень 6 в графе Ω, $[a] - \Omega = \{w, w^t\}$, то выполняются следующие утверждения:*

(1) *если вершина b изолирована в графе $\Omega \cap \Gamma_2(a)$, то связная компонента графа $\Gamma_2(a)$, содержащая b, является шестиугольником;*

(2) $|(\Omega - a^\perp) \cap \Gamma_2(w) \cap \Gamma_2(w^t)| \leq 7$, *и степень каждой вершины из $\Omega \cap \Gamma_3(w) \cap \Gamma_3(w^t)$ в графе Ω не меньше 4;*

(3) $17 \leq |\Omega|$ *и некоторая вершина из $\Omega \cap \Gamma_2(a)$ имеет степень 2 в $\Omega \cap \Gamma_2(a)$;*

(4) $|\Omega \cap \Gamma_2(a)| \geq 12$, *причем равенство достигается, если (a) $\Omega \cap \Gamma_2(a)$ является объединением шестиугольника и 6-коклики, и (b) $\Omega(a)$ содержит по три вершины из Ω^1 и из Ω^3.*

Доказательство. Пусть вершина a имеет степень 6 в графе Ω, $[u] - \Omega = \{w, w^t\}$. Допустим, что $b \in \Omega \cap \Gamma_2(a)$ и $[b] \cap \Gamma_2(a) = \{f, f^t\}$. Без ограничения общности, $[a] \cap [f] = \{w\}$. Пусть $[f] \cap \Gamma_2(a) = \{b, g\}$. Тогда $g \notin \Omega$ и $[a] \cap [g] = \{w^t\}$. Если вершины g, g^t смежны, то $[g] \cap [w] = \{f, g^t\}$, противоречие. Пусть $[g] \cap \Gamma_2(a) = \{f, h\}$. Если $h \notin \Omega$, то $[a] \cap [h] = \{w\}$, противоречие с тем, что тогда $[g] \cap [w] = \{f, h\}$. Значит, $h \in \Omega$ и связная компонента графа $\Gamma_2(a)$, содержащая b, является шестиугольником. Утверждение (1) доказано.

Подграф $\Gamma_2(w) \cap \Gamma_2(w^t)$ содержит 6 вершин из $\Omega(a)$ и не более 7 вершин вне $a^\perp$. Покажем, что степень каждой вершины b из $\Omega \cap \Gamma_3(w) \cap \Gamma_3(w^t)$ в графе Ω не меньше 4. Если $d(a, b) = 3$, то $[a] \cap \Gamma_2(b)$ содержит 4 вершины из Ω. Если же $d(a, b) = 2$, то степень a в графе $\Omega \cap \Gamma_2(b)$ равна 2. В любом случае по лемме 3.1 степень b в графе Ω не меньше 4. Утверждение (2) доказано.

Так как шар радиуса 2 с центром a содержит не менее 13 вершин из Ω, то $|\Omega| \geq 15$. Если $|\Omega| = 15$, то Ω содержит по одной вершине степеней 4 и 6 и 13 вершин степени 2, противоречие с леммой 3.3.

Пусть каждая вершина из $\Omega \cap \Gamma_2(a)$ изолирована в $\Omega \cap \Gamma_2(a)$. Тогда по утверждению (1) каждая вершина из $\Omega \cap \Gamma_2(a)$ лежит в шестиугольнике из $\Gamma_2(a)$ и пересечение шара радиуса 2, имеющего центр a, с Ω содержит 13 вершин. Пусть $\Delta_1, \Delta_2, ..., \Delta_3$ — различные шестиугольники из $\Gamma_2(a)$, содержащие по 2 вершины из Ω. Так как $\Omega \cap \Gamma_3(a)$ содержит единственную вершину, смежную с 2 вершинами из $\Omega \cap \Gamma_2(a)$ и не менее 3 вершин, смежных с 4 вершинами из $\Omega \cap \Gamma_2(a)$, то $|\Omega| = 17$. Далее, число ребер между $\Omega \cap \Gamma_3(a)$ и $\Omega \cap \Gamma_2(a)$ равно 14, поэтому $\Omega \cap \Gamma_2(a)$ содержит 2 вершины, смежные с единственной вершиной из $\Omega \cap \Gamma_3(a)$, и 4 вершины, смежные с 3 вершинами из $\Omega \cap \Gamma_3(a)$. Каждая вершина из $\Omega \cap \Gamma_3(a)$, смежная с 4 вершинами из $\Omega \cap \Gamma_2(a)$, смежна с 2 вершинами из Δ_i для единственного индекса i. Обозначим эту вершину через e_i. Пусть $d \in \Omega \cap \Gamma_3(a) - \{e_1, ..., e_3\}$, $b, c \in \Omega(d) \cap \Gamma_2(a)$. Без ограничения общности, $b \in \Delta_1$, $c \in \Delta_2$. Заметим, что вершины b, c смежны с тройками вершин из $\Omega \cap \Gamma_3(a)$. Если c смежна с e_1, то $[b] \cap [c]$ содержит d, e_1. Значит, e, c смежны с e_3 и $[d] \cap [e_3]$ содержит b, c, противоречие. Утверждение (3) доказано.

Заметим, что $|\Omega \cap \Gamma_2(a)| \geq 12$, причем равенство достигается, если $\Omega \cap \Gamma_2(a)$ является объединением шестиугольника и 6-коклики, и $\Omega(a)$ содержит по три вершины из Ω^1 и из Ω^3.

Лемма 3.6. *Параметр ω_1 равен 0.*

Доказательство. Пусть $\omega_1 \neq 0$, $a \in \Omega^1$ и $\Omega(a)$ содержит две вершины b, c из Ω^3.

Покажем, что $\Omega \cap \Gamma_2(b)$ является объединением шестиугольника и 6-коклики и $\Omega(b)$ содержит по три вершины из Ω^1 и из Ω^2.

Заметим, что $\Gamma_2(a) - \Omega$ содержит 46 вершин, причем число ребер между $\Gamma_2(a) - \Omega$ и $\Omega \cap (\Gamma_2(a) \cup [a])$ равно $20 + 4$. Поэтому число ребер между $\Gamma_2(a) - \Omega$ и $\Omega \cap \Gamma_3(a)$ не больше 22. Таким образом, число вершин в $\Gamma_3(a) \cap \Gamma_2(b) \cap \Omega$ не больше 11, и по лемме 3.5 $\Omega(b) - \{a\}$ содержит 2 вершины из Ω^1 и 3 из Ω^2 и $\Omega \cap \Gamma_2(b)$ является объединением шестиугольника и 6-коклики.

Положим $[b] - \Omega = \{w, w^t\}$. Ввиду леммы 3.5 подграф $\Gamma_2(w) \cap \Gamma_2(w^t)$ содержит 6 вершин из $\Omega(b)$ и $\Gamma_3(b) \cap \Omega$ содержит единственную вершину, смежную с двумя вершинами из $\Gamma_2(b) \cap \Omega$. Противоречие с тем, что $\Omega^3 \cap \Gamma_2(b)$ содержит 3 вершины, каждая из которых смежна с вершиной из $\Omega^1 \cap \Gamma_3(b)$.

Лемма 3.7. *Подграф Ω содержит изолированную вершину.*

Доказательство. Допустим, что подграф Ω не содержит изолированных вершин. Для $a \in \Omega^3$ ввиду леммы 3.6 получим $|\Omega \cap \Gamma_2(a)| \geq 18$ и $|\Omega \cap \Gamma_3(a)| \geq 6$. Таким образом, $\Omega \geq 31$, и по лемме 3.4 получим $\alpha_1(t) = 0$. Отсюда $\alpha_0(t) = \omega_2 + \omega_3$, $\alpha_2(t) = 4\omega_2 + 2\omega_3$ и

$\alpha_3(t) = 135 - 5\omega_2 - 3\omega_3$. Из целочисленности $\chi_2(t) = (5\alpha_0(t) + \alpha_3(t))/12 - 25/4$ следует, что $\omega_3 = 6s$. Из целочисленности $\chi_3(t) = (7\alpha_0(t) + 3\alpha_2(t) + 2\alpha_3(t))/21 - 15$ заключаем, что $\omega_2 + 2$ делится на 7 и $\omega_2 = 5$ или 19.

Если $\omega_2 = 5$, то найдется вершина $a \in \Omega^3$, не смежная с вершинами из Ω^2, $|\Omega \cap \Gamma_2(a)| \geq 30$ и $|\Omega \cap \Gamma_3(a)| \geq 8$. Противоречие с тем, что тогда $\Omega = 45$. Значит, $\omega_2 = 19$ и $\omega_3 = 12$. Теперь $\Omega(a) \subset \Omega^2$, иначе $|\Omega \cap \Gamma_2(a)| \geq 20$ и $|\Omega \cap \Gamma_3(a)| \geq 5$, противоречие.

Теперь $\Gamma_3(a)$ содержит не более 6 вершин из Ω^3 и $\Gamma_2(a)$ содержит не менее 5 вершин из Ω^3 и число ребер между $\Omega \cap \Gamma_2(a)$ и $\Omega \cap \Gamma_3(a)$ не меньше $5 \cdot 3 + 13$. Противоречие с тем, что тогда $|\Omega \cap \Gamma_3(a)| \geq 7$. Лемма доказана.

Теорема следует из результатов §§ 2 и 3.

4. Граф Γ не является вершинно транзитивным

Пусть G — группа всех автоморфизмов графа Γ. Из лемм 2.3, 2.4 следует, что $\pi(G) \subseteq \{2,3,5,7\}$. Зафиксируем вершину a графа Γ и через H обозначим стабилизатор вершины a в группе G. Тогда $\pi(H) \subset \{2,7\}$ и $|G:H|$ делит $3^3 \cdot 5$. Так как H не может действовать транзитивно на 70-вершинном графе $\Gamma_3(a)$, то граф Γ не является дистанционно транзитивным.

Лемма 4.1. *Допустим, что группа G содержит элемент f порядка pr, где p, r — различные простые числа, $p < r$. Тогда $p = 2$ и $r = 3$.*

Д о к а з а т е л ь с т в о. Положим $g = f^r$ и $\Omega = \mathrm{Fix}(g)$. Пусть $p = 2$. Тогда $r = 3, 5$ или 7. В случае $r = 7$ подграф Ω является 7-кокликой и числа $\alpha_i(g)$ делятся на 7. Противоречие с тем, что $\alpha_1(g) = 44$. В случае $r = 5$ подграф Ω является 5-кокликой и числа $\alpha_i(g)$ делятся на 5. Противоречие с тем, что $\alpha_1(g) = 52$.

Пусть $p = 3$. Ввиду леммы 2.4 подграф Ω является пустым. Если $r = 7$, то двухвершинный подграф $\mathrm{Fix}(f^p)$ содержится в Ω, противоречие. Значит, $r = 5$ и числа $\alpha_i(g)$ делятся на 5. Противоречие с леммой 2.3.

Пусть $p = 5$. Ввиду леммы 2.4 подграф Ω является пустым. Далее, $r = 7$ и двухвершинный подграф $\mathrm{Fix}(f^p)$ содержится в Ω, противоречие. Лемма доказана.

Лемма 4.2. *Выполняются следующие утверждения*:

(1) *группа G не содержит регулярных подгрупп*;

(2) *если $b_i \in \Gamma_i(a)$, F_i — стабилизатор в H вершины b_i, то $|F_1|$ делит 7, $|F_2| = 1$ и $|F_3|$ делит 4*;

(3) *если S — силовская 2-подгруппа из H, то $|S|$ делит 8.*

Д о к а з а т е л ь с т в о. Пусть U — регулярная подгруппа из G. Тогда $|U| = 3^3 5$. Так как порядок группы $GL(3,3)$ не делится на 5, то силовская 5-подгруппа из U централизует силовскую 3-подгруппу из U. Противоречие с леммой 2.6. Утверждение (1) доказано.

Так как группа F_1 действует полурегулярно на $[a] - \{b_1\}$, то $|F_1|$ делит 7. Ввиду леммы 2.4 имеем $|F_2| = 1$. Так как группа F_3 действует полурегулярно на 4-вершинном подграфе $\Gamma_2(a) \cap [b_3]$, то $|F_3|$ делит 4. Утверждение (2) доказано.

Так как S действует на 70-вершинном подграфе $\Gamma_3(a)$, то $\Gamma_3(a)$ имеет одно- или двухэлементную S-орбиту. Если b_3 — элемент из этой орбиты, то $|S : F_3|$ делит 2 и $|S|$ делит 8. Лемма доказана.

Из леммы 4.2 следует, что Γ не является графом Кэли.

Лемма 4.3. *Граф Γ не является вершинно транзитивным.*

Д о к а з а т е л ь с т в о. Пусть группа $G = \mathrm{Aut}(\Gamma)$ действует вершинно транзитивно на Γ. Так как любой дистанционно регулярный граф с импримитивной группой автоморфизмов является двудольным или антиподальным, то G действует примитивно на множестве вершин графа Γ. Далее, число вершин графа равно 135, поэтому цоколь G_0 группы G является простой неабелевой группой. Положим $H_0 = G_0 \cap H$. Так как группа G_0 транзитивна на множестве вершин графа Γ, то $|G_0 : H_0| = 3^3 \cdot 5$. По лемме 4.1 порядок группы G делит $2^3 3^3 5 \cdot 7$.

По лемме 4.1 граф Грюнберга — Кегеля группы G является несвязным. Списки простых групп и информация о компонентах несвязного графа Грюнберга — Кегеля имеются в лемме 4 из [7]. Однако в нашем случае можно воспользоваться результатами, не зависящими от классификации конечных простых групп. Если силовская 2-подгруппа S из G абелева, то по [8, 9] группа G_0 изоморфна $L_2(8)$, $L_2(q)$ ($q \equiv 3, 5 \pmod 8$), ${}^2G_2(3^{2n-1})$ или J_1. Если же S неабелева, то она является диэдральной группой порядка 8 и по [10] группа G_0 изоморфна $L_2(q)$ ($q \equiv 7, 9 \pmod{16}$) или A_7. Так как $|G_0|$ делит $2^3 3^3 5 \cdot 7$, то группа G_0 изоморфна $L_2(q)$ или A_7. Но $|G_0|$ делится на $3^3 5$, поэтому группа G_0 изоморфна $L_2(3^3)$, противоречие с тем, что 13 не делит $|G|$. Лемма и следствие доказаны.

Поступила 23.11.2006

СПИСОК ЛИТЕРАТУРЫ

1. **Cameron P. J.** Permutation groups // London Math. Soc. Student Texts № 45. Cambridge: Cambridge University Press, 1999.
2. **Махнев А. А., Падучих Д. В.** Об автоморфизмах графа Ашбахера // Алгебра и логика. 2001. Т. 40, № 2. С. 125–134.
3. **Махнев А. А., Носов В. В.** Об автоморфизмах сильно регулярных графов с $\lambda = 0$, $\mu = 2$ // Мат. сборник. 2004. Т. 185, № 3. С. 47–68.
4. **Махнев А. А., Минакова И. М.** Об автоморфизмах графов с $\lambda = 1$, $\mu = 2$ // Дискрет. математика. 2004. Т. 16, № 1. С. 95–104.
5. **Brouwer A. E., Cohen A. M., Neumaier A.** Distance-regular graphs. Berlin: Springer-Verlag; New York; Heidelberg, 1989.
6. **Cameron P. J., Lint J. van.** Graphs, Codes and Designs // London Math. Soc. Student Texts № 22. Cambridge: Cambridge University Press, 1991.
7. **Кондратьев А. С., Мазуров В. Д.** Распознавание знакопеременных групп простой степени // Сиб. мат. журн. 2000. Т. 41, № 2. С. 359–369.
8. **Walter J.** The characterization of finite groups with abelian Sylow 2-subgroups // Ann. Math. 1969. V. 89. P. 405–514.
9. **Bombieri E.** Thompson's problem ($\sigma^2 = 3$) // Invent. Math. 1980. V. 58. P. 77–100.
10. **Gorenstein D., Walter J.** The characterization of finite groups with dihedral Sylow 2-subgroups, I-IV // Ill. J. Math. 1962. V. 6. P. 553-593; J. Algebra. 1965. V. 2. P. 85–151; P. 218–270; P. 354–393.

Том 13 № 1 2007

УДК 512.54

ГЕОМЕТРИЧЕСКАЯ ЭКВИВАЛЕНТНОСТЬ ГРУПП[1]

В. В. Блудов, Б. В. Гусев

На основе понятия геометрической эквивалентности групп определяются новые классы групп — геометрические многообразия групп. Рассматриваются различные свойства этих классов, в том числе их связь с квазимногообразиями и предмногообразиями групп. Приведены примеры нильпотентных групп без кручения, геометрически не эквивалентных своим минимальным пополнениям, а также пример геометрически не эквивалентных центрально метабелевых групп, порождающих одинаковые квазимногообразия.

Введение

В серии работ Б.И. Плоткина [19–22] и Г. Баумслага, А. Мясникова, В.Н Ремесленникова, В.А Романькова [2, 3, 17] были заложены основы алгебраической геометрии над группами. В этих работах, наряду с общими вопросами, было введено понятие геометрической эквивалентности групп, рассмотрены основные свойства этого понятия и поставлены открытые вопросы. В настоящей работе изучаются свойства этой геометрической эквивалентности и вводятся новые классы групп — геометрические многообразия групп (определение 2.2). Эти классы групп замкнуты относительно подгрупп и относительно геометрической эквивалентности и обладают другими интересными свойствами. В частности, классы нильпотентных и разрешимых групп являются геометрическими многообразиями (следствие 2.6). Авторы не ставили целью рассмотреть самую общую ситуацию с классами алгебр, хотя основные результаты, представленные в работе, можно распространить на различные алгебраические системы, а также на G-группы (т.е. группы с выделенными константами).

В § 1 работы приводятся предварительные сведения, основные определения и обозначения. Это сделано не только для удобства читателя, но также из-за того, что некоторые определения и обозначения в нашей статье несколько отличаются от аналогичных в цитированных выше работах.

В § 2 определяются геометрические многообразия групп и рассматриваются их свойства (утверждения 2.2–2.4, 2.6, следствия 2.1–2.6 и теорема 2.1).

В § 3 рассматривается вопрос Б.И. Плоткина о геометрической эквивалентности конечно порожденных нильпотентных групп без кручения и их минимальных пополнений (под полной группой здесь понимается группа G, в которой любое уравнение вида $x^n = a$, $n \in \mathbb{N}$, $a \in G$ имеет решение). Приводится ряд примеров конечно порожденных нильпотентных групп ступеней три, четыре, пять (примеры 3.1–3.3), минимальные пополнения которых геометрически не эквивалентны исходным группам. Здесь же приводится критерий геометрической эквивалентности нильпотентных групп без кручения и их минимальных пополнений (теорема 3.1) и, как следствие, получена геометрическая эквивалентность двуступенно нильпотентных групп и их минимальных пополнений (следствие 9). При этом группа $N_{3,4}$ из примера 3.1 также решает вопрос 1.1 из работы [4] о существовании трехступенно нильпотентных упорядоченных групп, всякий автоморфизм которых сохраняет порядок (теорема 3.3).

В § 4 рассматривается связь геометрических многообразий и квазимногообразий. Доказано, что для любого класса $\mathfrak{X}$ групп геометрическое многообразие, порожденное $\mathfrak{X}$,

[1]Работа выполнена при финансовой поддержке РФФИ (проект 03-01-00320).

содержится в квазимногообразии, порожденном $\mathfrak{X}$ (утверждение 4.1). С использованием результатов предыдущего параграфа показано, что квазимногообразие, порожденное нильпотентной группой без кручения, не обязательно совпадает с квазимногообразием, порожденным минимальным пополнением этой группы (теорема 4.1). Далее рассматривается вопрос о геометрической эквивалентности групп, порождающих одно и то же квазимногообразие, поставленный Б.И. Плоткиным в [18] (вопрос 14.71). В работе А. Мясникова и В. Ремесленникова [17] приведены примеры G-групп, которые геометрически не эквивалентны, но порождают одинаковые квазимногообразия. Для групп без констант такие примеры приведены в работах С. Шелаха и Р. Гебеля [9] и В.В. Блудова [5]. Пример центрально метабелевых групп, представленный в [5], более детально изложен в данной работе (пример 4.1).

Результаты, представленные в работе, частично анонсированы в [5–8].

1. Определения и предварительные сведения

1.1. Геометрическая эквивалентность

Напомним определения основных понятий, связанных с геометрической эквивалентностью групп (см. [19, 21, 22]).

Пусть $F = F(X)$ — свободная группа с множеством свободных порождающих X и G — некоторая группа. При $X = \{x_1, \ldots, x_n\}$ получаем свободную группу ранга n, которую обозначаем также через $F(x_1, \ldots, x_n)$. Множество всех гомоморфизмов из F в G обозначим через $\mathrm{Hom}(F, G)$. Возникает соответствие Галуа между подмножествами группы F и подмножествами из $\mathrm{Hom}(F, G)$: подмножеству $S \subseteq F$ ставится в соответствие подмножество

$$S' = \{\varphi \in \mathrm{Hom}(F, G) \mid S \subseteq \ker \varphi\},$$

а подмножеству $T \subseteq \mathrm{Hom}(F, G)$ ставится в соответствие подмножество

$$T' = \bigcap_{\varphi \in T} \ker \varphi.$$

Дважды применяя указанное соответствие, получаем явный вид подмножеств $S'' \subseteq F$ и $T'' \subseteq \mathrm{Hom}(F, G)$:

$$S'' = (S')' = \bigcap_{S \subseteq \ker \varphi,\ \varphi \in \mathrm{Hom}(F, G)} \ker \varphi,$$

$$T'' = (T')' = \left\{\psi \in \mathrm{Hom}(F, G) \mid \bigcap_{\varphi \in T} \ker \varphi \subseteq \ker \psi\right\}.$$

Определение 1.1 (Б.И. Плоткин [19, 20, 22]). Подмножество S свободной группы F (соответственно $T \subseteq \mathrm{Hom}(F, G)$) называется *$G$-замкнутым*, если $S = S''$ (соответственно $T = T''$). Пересечение всех G-замкнутых подмножеств, содержащих S, называется *G-замыканием* S и обозначается через $\mathrm{Cl}_G(S)$.

Определение 1.2 (Б.И. Плоткин [19, 20, 22]). Группы G и H называются *геометрически эквивалентными*, если для любой свободной группы F конечного ранга всякое подмножество S группы F является G-замкнутым тогда и только тогда, когда оно H-замкнуто.

Непосредственно из определений 1.1 и 1.2 следует

Утверждение 1.1. *Если группа K является подгруппой группы H, H — подгруппа группы G ($K < H < G$) и группы K, G геометрически эквивалентны, то группа H геометрически эквивалентна группам K и G.*

1.2. Уравнения в группах

Обычно (см. [12]) под уравнением в группе G понимается формальное выражение

$$W(x_1, \dots, x_n, a_1, \dots, a_k) = 1, \tag{1.1}$$

где $W = W(x_1, \dots, x_n, a_1, \dots, a_k)$ — элемент свободного произведения $G * F(x_1, \dots, x_n)$ группы G и свободной группы $F(x_1, \dots, x_n)$. При этом предполагается, что W не содержится в подгруппе, сопряженной с G. Последнее требование гарантирует, что W содержит явно хотя бы одну переменную. И это существенно в исследованиях, связанных с возможностью решения такого уравнения или в самой группе G, или в некоторой группе $\widetilde{G}$, содержащей исходную группу в качестве подгруппы. Однако в наших исследованиях мы не исключаем случай фиктивного вхождения переменных в уравнение (1.1), поэтому выражение (1.1) называем уравнением в группе G для произвольного $W \in G * F(x_1, \dots, x_n)$. При этом количество переменных, явно входящих в уравнение $W = 1$, называется *числом переменных* уравнения. Множество уравнений $S = \{W_i \mid i \in I\}$ с ограниченным в совокупности числом переменных называется *системой уравнений*. С каждой системой уравнений S связано множество решений $V(S)$ этой системы в группе G.

Определение 1.3 (Г. Баумслаг, А. Мясников, В. Ремесленников [2]). Набор из n элементов $(h_1, \dots, h_n) \in G^n$ называется *решением* уравнения

$$W(x_1, \dots, x_n, a_1, \dots, a_k) = 1$$

(соответственно системы уравнений S), если в группе G выполняется равенство

$$W(h_1, \dots, h_n, a_1, \dots, a_k) = 1$$

(соответственно

$$W_i(h_1, \dots, h_n, a_1, \dots, a_k) = 1$$

для всех $W_i \in S$). Множество всех решений уравнения W (соответственно системы уравнений S) обозначается через $V(W)$ (соответственно $V(S)$).

Точно так же с каждым подмножеством $R \subseteq G^n$ связывается система уравнений $S(R)$ по правилу

$$W \in S(R) \Longleftrightarrow R \in V(W).$$

Определение 1.4 (Г. Баумслаг, А. Мясников, В. Ремесленников [2]). Уравнение W называется *следствием системы уравнений* S в группе G, если $V(S) \subseteq V(W)$. Множество всех следствий системы S в группе G называется *G-замыканием* системы S и обозначается через $\mathrm{Cl}_G(S)$. Аналогично, решение $(h_1, \dots, h_n)$ называется *следствием множества* $R \subseteq G^n$, если $(h_1, \dots, h_n) \in V(S(R))$, т.е. если $(h_1, \dots, h_n)$ принадлежит множеству решений всякой системы уравнений, для которой R является множеством решений. Множество всех следствий подмножества $R \subseteq G^n$ называется *G-замыканием* подмножества R и обозначается через $\mathrm{Cl}_G(R)$. Две системы уравнений называются *эквивалентными относительно группы* G, если их G-замыкания совпадают.

Указанные выше связи между множеством всех следствий системы S и множеством решений системы являются соответствием Галуа и совпадают с G-замыканием из определения 1.1; т.е., если подмножество S конечно порожденной свободной группы рассматривается как система уравнений в группе G, то $\mathrm{Cl}_G(S)$ в определениях 1.1 и 1.4 совпадают.

Определение 1.5 (Г. Баумслаг, А. Мясников, В.Н. Ремесленников [2]). Группа G называется *нетеровой по уравнениям*, если всякая система уравнений эквивалентна относительно группы G своей конечной подсистеме.

Б.И. Плоткин [22] называет нетеровы по уравнениям группы *геометрически нетеровыми*. На языке геометрической эквивалентности нетеровость по уравнениям для группы G означает, что для всякого подмножества S конечно порожденной свободной группы существует конечное подмножество $S_0 \subseteq S$, для которого $\mathrm{Cl}_G(S_0) = \mathrm{Cl}_G(S)$. Важность класса геометрически нетеровых групп подчеркивает утверждение 1.5, приведенное в следующем пункте.

1.3. Квазимногообразия

Напомним основные определения (см., например, [11, 15]). Формулы вида

$$(\forall x_1 \dots x_k)(f(x_1, \dots, x_k) = 1)$$

называются *тождествами* или *тождественными соотношениями*, а формулы вида

$$(\forall x_1 \dots x_k)\Big(\bigwedge_{i=1}^{s} f_i(x_1, \dots, x_k) = 1 \Rightarrow f_{s+1}(x_1, \dots, x_k) = 1\Big)$$

называются *квазитождествами.* Здесь $f, f_1, \dots, f_{s+1}$ представляют термы от переменных $x_1, \dots, x_k$.

Определение 1.6. Класс $\mathfrak{R}$ алгебраических систем называется *многообразием* (*квазимногообразием*), если существует такая совокупность S тождеств (квазитождеств), что $\mathfrak{R}$ состоит из тех и только тех систем, в которых истинны все формулы из S.

Так как каждое тождество равносильно соответствующему квазитождеству, то каждое многообразие является и квазимногообразием.

Определение 1.7. Абстрактный класс $\mathfrak{R}$ алгебр называется *предмногообразием* (или *реплично полным классом*), если он содержит одноэлементную алгебру E и замкнут относительно подалгебр и прямых произведений.

В основном мы придерживаемся стандартных обозначений. Через $\mathrm{S}\mathfrak{X}$, $\mathrm{C}\mathfrak{X}$ и $\mathrm{L}\mathfrak{X}$ обозначаются соответственно замыкание класса $\mathfrak{X}$ соответственно относительно взятия подгрупп, относительно взятия декартовых произведений и локальное замыкание класса $\mathfrak{X}$ ($G \in \mathrm{L}\mathfrak{X}$, если всякая конечно порожденная подгруппа группы G принадлежит $\mathfrak{X}$). Через $\mathrm{pvar}\ \mathfrak{X}$, $\mathrm{qvar}\ \mathfrak{X}$ и $\mathrm{var}\ \mathfrak{X}$ обозначаются соответственно предмногообразие, квазимногообразие и многообразие, порожденное классом $\mathfrak{X}$. Известно [15], что $\mathrm{pvar}\ \mathfrak{X}$ замкнуто относительно декартовых произведений и подгрупп, $\mathrm{qvar}\ \mathfrak{X}$ замкнуто относительно декартовых произведений, подгрупп и ультрапроизведений, а $\mathrm{var}\ \mathfrak{X}$ замкнуто относительно декартовых произведений, подгрупп и гомоморфизмов. Кроме того, для любого класса $\mathfrak{X}$ имеют место следующие включения: $\mathrm{pvar}\ \mathfrak{X} \subseteq \mathrm{qvar}\ \mathfrak{X} \subseteq \mathrm{var}\ \mathfrak{X}$.

В дальнейшем в нашей работе используются следующие известные результаты:

Утверждение 1.2. (А.И. Мальцев [15]). *Группа G тогда и только тогда принадлежит предмногообразию, порожденному группами H_α, $\alpha \in A$, когда G изоморфно вкладывается в декартово произведение групп H_α.*

Утверждение 1.3. (Б.И. Плоткин [19]). *Всякая группа геометрически эквивалентна любой своей декартовой степени.*

Утверждение 1.4. (Б.И. Плоткин [19]). *Если группы G_1 и G_2 геометрически эквивалентны, то* $\mathrm{qvar}\ G_1 = \mathrm{qvar}\ G_2$ *и* $\mathrm{var}\ G_1 = \mathrm{var}\ G_2$.

Утверждение 1.5. (А. Мясников, В. Ремесленников [17]). *Геометрически нетеровы группы геометрически эквивалентны тогда и только тогда, когда они порождают одинаковые квазимногообразия.*

Следствие 1.1. (Б.И. Плоткин [18], вопрос 14.71). *Нильпотентные группы геометрически эквивалентны тогда и только тогда, когда они определяют одно и то же квазимногообразие.*

1.4. Пополнения нильпотентных групп без кручения

Группа G называется *полной* или *делимой*, если уравнение $x^n = g$ имеет решение в группе G для любого натурального n и любого $g \in G$.

Определение 1.8. (А.И. Мальцев [14]). Если полная нильпотентная группа без кручения $G^\sharp$ содержит подгруппу G такую, что каждый элемент $G^\sharp$ в подходящей положительной степени содержится в G, то $G^\sharp$ называется *пополнением* группы G.

Теорема 1.1. (А.И. Мальцев [14], см. также [10]). *Каждая нильпотентная группа без кручения G содержится в нильпотентной группе без кручения $G^\sharp$, являющейся пополнением G. Если $G_1^\sharp$ и $G_2^\sharp$ два пополнения группы G, то между ними существует, и притом единственный, изоморфизм, продолжающий тождественный автоморфизм группы G.*

Теорема 1.1 устанавливает единственность пополнений нильпотентных групп. Поэтому пополнение нильпотентной группы также называют ее *минимальным пополнением.*

Лемма 1.1 (А.И. Мальцев [13], см. также [12]). *Если нильпотентная группа G имеет конечную систему порождающих и каждый ее порождающий в некоторой положительной степени содержится в подгруппе D, то индекс D в G конечен.*

Следствие 1.2. *Пусть G — нильпотентная группа без кручения и $G^\sharp$ — ее пополнение. Тогда для любой конечно порожденной подгруппы $H < G^\sharp$ найдется натуральное число n такое, что $H^n \leq G$.*

Доказательство. По определению 1.8 любой элемент подгруппы H в некоторой положительной степени принадлежит G. Пусть

$$D = \langle x^k \in G \mid x \in H, k \in N \rangle.$$

По построению $D \leq G$ и $D \leq H$. Поскольку всякая подгруппа конечно порожденной нильпотентной подгруппы конечно порождена [10], то D — конечно порожденная подгруппа группы H. По лемме 1.1 D имеет конечный индекс в H и, значит, найдется нормальная в H подгруппа $D_1 \leq D$ также конечного индекса в H [10, 12]. Если n — порядок факторгруппы H/D_1, то любой элемент подгруппы H в степени n попадает в $D_1 \leq D \leq G$. □

Следующая лемма приводится с доказательством, в котором (в отличие от работы [14]) не используются сведения из теории алгебр Ли.

Лемма 1.2. (А.И. Мальцев [14]). *Пусть G — нильпотентная группа ступени нильпотентности k и H — ее подгруппа, порожденная элементами $h_i^{n^k}$, $h_i \in G$, $n \in \mathbb{N}$, $i \in I$, где I — некоторое множество индексов. Тогда уравнение $x^n = h$ имеет решение в группе G для любого $h \in H$.*

Доказательство. Воспользуемся хорошо известными формулами, справедливыми для каждого натурального n и для любого набора элементов $x_1, \ldots, x_r$ любой нильпотентной группы:

$$x_1^n \cdot \cdots \cdot x_r^n = (x_1 \cdot \cdots \cdot x_r)^n \cdot U(x_1, \ldots, x_r), \tag{1.2}$$

где $U(x_1, \ldots, x_r)$ — произведение коммутаторов вида $[x_{i_1}, \ldots, x_{i_s}]$ от $x_1, \ldots, x_r$;

$$[x_1, \ldots, x_i^n, \ldots, x_r] = [x_1, \ldots, x_i, \ldots, x_r]^n \cdot w_1 \cdot \cdots \cdot w_q, \qquad 1 \leq i \leq r, \tag{1.3}$$

$w_1 \cdot \cdots \cdot w_q$ — произведение коммутаторов (весов, строго больших r), явно зависящих от $x_1, \ldots, x_i, \ldots, x_r$.

Представим элемент h в виде произведения порождающих элементов подгруппы H и их обратных: $h = h_{i_1}^{\varepsilon_1 n^k} \cdot \dots \cdot h_{i_s}^{\varepsilon_s n^k}$, $\varepsilon_1, \dots, \varepsilon_s = \pm 1$, $i_1, \dots, i_s \in I$. Индукцией по $t = 1, 2, \dots, k$ покажем, что h представляется в виде

$$h = (V_t(h_{i_1}, \dots, h_{i_s}))^n \cdot W_t, \tag{1.4}$$

где V_t — групповое слово от переменных $h_{i_1}, \dots, h_{i_s}$, а W_t — произведение коммутаторов весов, строго бо́льших t, от элементов $h_{i_1}^{\varepsilon_1 n^{k_1}}, \dots, h_{i_s}^{\varepsilon_s n^{k_s}}$, причем в каждый из таких коммутаторов явно входит хотя бы один из элементов $h_{i_j}^{\varepsilon_j n^{k_j}}$ с условием $k_j \geq k - t$.

При $t = 1$ представление (1.4) получается из формулы (1.2) при $r = s$, $x_j = h_{i_j}^{\varepsilon_j n^{k-1}}$, $j = 1, \dots, s$. При этом в коммутаторы из произведения U каждая из переменных входит с показателем $\varepsilon_j n^{k-1}$.

Пусть представление (1.4) выполняется для данного t. Докажем существование такого представления для $t+1$. По предположению индукции каждый коммутатор u веса $t+1$ из произведения W_t содержит переменную $h_{i_j}^{\varepsilon_j n^{k_j}}$ с условием $k_j \geq k - t$. (Если в произведении W_t нет коммутаторов веса $t+1$, то данное представление выполняется и при $t+1$.) Каждый коммутатор u_α веса $t+1$ из произведения W_t представим по формуле (1.3), выбрав в качестве переменной x_i указанную выше переменную $h_{i_j}^{\varepsilon_j}$ с показателем n^{k_j} и с условием $k_j \geq k - t$:

$$u_\alpha = \left[*, \dots, h_{i_j}^{\varepsilon_j n^{k_j}}, \dots, *\right] = \left[*, \dots, h_{i_j}^{\varepsilon_j n^{k_j - 1}}, \dots, *\right]^n \cdot w_1 \cdot \dots \cdot w_q = v_\alpha^n \cdot w_1 \cdot \dots \cdot w_q. \tag{1.5}$$

При этом веса коммутаторов $w_1, \dots, w_q$ строго больше $t+1$, и каждый из них содержит переменную $h_{i_j}^{\varepsilon_j}$ с показателем $n^{k_j - 1}$ и с условием $k_j - 1 \geq k - (t+1)$. Заменим в W_t коммутаторы u_α на их представления (1.5), перенесем все v_α^n влево и представим их по формуле (1.2). Получившиеся дополнительные коммутаторы имеют вес строго больше $t+1$ и имеют вхождение переменных вида $h_{i_j}^{\varepsilon_j}$ с показателями n^{k_j} и с условием $k_j > k - (t+1)$. Таким образом, W_t получает представление

$$W_t = (u_{\alpha_1} \cdot \dots \cdot)^n \cdot W_{t+1} = U_t^n \cdot W_{t+1}$$

и W_{t+1} — произведение коммутаторов весов, строго бо́льших $t+1$, с вхождениями переменных в степенях не менее, чем $k - (t+1)$. Снова воспользуемся представлением (1.2) при $r = 2$, $x_1 = V_t(h_{i_1}, \dots, h_{i_s})$, $x_2 = U_t$ и получим $h = (V_t U_t)^n \cdot U(V_t, U_t) W_{t+1}$, что доказывает утверждение индукции.

При $t = k$, где k — ступень нильпотентности исходной группы G, из (1.4) получаем: $h = (V_k(h_{i_1}, \dots, h_{i_s}))^n$, и лемма доказана. $\square$

В вопросах, связанных с пополнением нильпотентных групп, важную роль играет понятие изолированной подгруппы.

О п р е д е л е н и е 1.9. Подгруппа H группы G называется *изолированной*, если из $g^n \in H$ следует $g \in H$ для любого элемента $g \in G$ и любого целого $n > 0$. *Изолятором* подгруппы H группы G называется наименьшая изолированная подгруппа группы G, содержащая подгруппу H. Изолятор подгруппы H обозначаем через $\mathrm{I}(H)$.

2. Геометрические многообразия

Геометрическая эквивалентность групп не переходит на подгруппы. Более того, существуют группы, которые геометрически не эквивалентны никаким своим собственным подгруппам (см. примеры 3.1–3.3). В этом параграфе мы определим новый класс групп — геометрическое многообразие, которое замкнуто относительно геометрической эквивалентности, подгрупп и декартовых степеней и локально замкнуто.

В первом пункте параграфа вводится определение геометрического многообразия и приводятся непосредственные следствия из определения, а во втором указывается связь геометрических многообразий с предмногообразиями и другими классами групп.

2.1. Определения и вспомогательные результаты

Введем на классе групп отношение предпорядка $\preceq$, задающее отношение порядка на классах геометрически эквивалентных групп.

О п р е д е л е н и е 2.1. Пусть H и G — произвольные группы. Если для любой конечно порожденной свободной группы F всякое H-замкнутое подмножество будет G-замкнутым, то пишем $H \preceq G$ и говорим, что геометрия H слабее геометрии G (или что геометрия G сильнее геометрии H).

Отношение $\preceq$ естественным образом связано с геометрической эквивалентностью и обладает следующими свойствами, которые вытекают непосредственно из определения 2.1.

Утверждение 2.1. *Для произвольных групп K, H, G справедливы следующие утверждения*:

(1) $G \preceq G$,

(2) $K \preceq H \preceq G \Rightarrow K \preceq G$,

(3) *группы H и G геометрически эквивалентны тогда и только тогда, когда $H \preceq G$ и $G \preceq H$.*

О п р е д е л е н и е 2.2. Класс $\mathfrak{K}$ групп называется *геометрическим многообразием*, если соотношения $G \in \mathfrak{K}$ и $H \preceq G$ влекут за собой $H \in \mathfrak{K}$.

Утверждение 2.2. *Объединение и пересечение любого непустого семейства геометрических многообразий образует геометрическое многообразие.*

Д о к а з а т е л ь с т в о. Пусть класс групп $\mathfrak{K}$ является объединением (соответственно, пересечением) геометрических многообразий $\mathfrak{K}_i$, $i \in I$ и $H \preceq G \in \mathfrak{K}$. В этом случае $G \in \mathfrak{K}_i$ для некоторого (соответственно, для каждого) $i \in I$. Поскольку $H \preceq G$, то $H \in \mathfrak{K}_i$ для этого (соответственно, для каждого) $i \in I$ и, следовательно, $H \in \mathfrak{K}$. □

Утверждение 2.2 позволяет определить геометрическое многообразие, порожденное абстрактным классом групп $\mathfrak{X}$, как пересечение всех геометрических многообразий, содержащих класс $\mathfrak{X}$ (или, что то же самое, как минимальное геометрическое многообразие, содержащее $\mathfrak{X}$). Для геометрического многообразия, порожденного классом групп $\mathfrak{X}$, используем обозначение gvar $\mathfrak{X}$. Из утверждения 2.1 следует, что

$$\operatorname{gvar} \mathfrak{X} = \{H \preceq G \mid G \in \mathfrak{X}\} \tag{2.1}$$

для любого класса групп $\mathfrak{X}$.

Утверждение 2.3. *Если $H \preceq G$, то любая конечно порожденная подгруппа группы H вкладывается в подходящую декартову степень группы G.*

Д о к а з а т е л ь с т в о. Пусть K — конечно порожденная подгруппа группы H, и F — конечно порожденная свободная группа такая, что $K \cong F/N$ для некоторой нормальной подгруппы N в F. В этом случае N замкнута относительно H. Из $H \preceq G$ следует, что N замкнуто относительно G и поэтому является пересечением ядер гомоморфизмов $\varphi : F \to G$ таких, что $N \subseteq \ker \varphi$. Тогда по теореме Ремака [10] F/N, а с ней и K вкладываются в декартову степень группы G. □

Всякий гомоморфизм из свободной группы F в подгруппу H группы G является и гомоморфизмом из F в G, поэтому непосредственно из определения 2.1 получаем следующее

Утверждение 2.4. *$H \preceq G$ для всякой подгруппы H группы G.*

Теперь приведем свойства геометрических многообразий. Из утверждения 2.4 и определения 2.2 получаем замкнутость относительно подгрупп, подклассов и геометрической эквивалентности:

Следствие 2.1. *Для произвольных классов групп $\mathfrak{X}$, $\mathfrak{Y}$ имеет место следующее:*
(1) $\mathrm{S}\mathfrak{X} \subseteq \mathrm{gvar}\ \mathfrak{X}$;
(2) $\mathfrak{X} \subseteq \mathfrak{Y} \Rightarrow \mathrm{gvar}\ \mathfrak{X} \subseteq \mathrm{gvar}\ \mathfrak{Y}$;
(3) *если группы G и H геометрически эквивалентны и H содержится в геометрическом многообразии $\mathfrak{K}$, то $G \in \mathfrak{K}$;*
(4) *если $\mathfrak{K}$ — геометрическое многообразие групп, то $\mathrm{gvar}\ \mathfrak{K} = \mathfrak{K}$.*

Утверждение 2.5. *Если $H_\alpha \preceq G_\alpha$, $\alpha \in A$, то*

$$\prod_{\alpha \in A} H_\alpha \preceq \prod_{\alpha \in A} G_\alpha.$$

Д о к а з а т е л ь с т в о. Пусть подмножество T свободной группы F конечного ранга замкнуто относительно группы $\overline{H} = \prod_{\alpha \in A} H_\alpha$. Тогда $T = \bigcap_{\varphi \in \Phi} \ker \varphi$ для подходящего множества Φ гомоморфизмов из F в $\overline{H}$. Для каждого $\alpha \in A$ зафиксируем проекцию π_α декартова произведения $\prod_{\alpha \in A} H_\alpha$ на группу H_α и рассмотрим множество гомоморфизмов $\Phi_\alpha = \{\varphi_\alpha = \varphi\pi_\alpha \mid \varphi \in \Phi\}$. Определим подмножество $T_\alpha \subseteq F$, полагая

$$T_\alpha = \bigcap_{\varphi_\alpha \in \Phi_\alpha} \ker \varphi_\alpha.$$

Получили, что T_α, $\alpha \in A$, замкнуты относительно H_α. Ввиду условия $H_\alpha \preceq G_\alpha$, утверждение 2.4 влечет за собой $G_\alpha \preceq \prod G_\alpha$, а утверждение 2.1 — соотношение $H_\alpha \preceq \prod G_\alpha$. Следовательно, T_α замкнуты относительно $\prod G_\alpha$ и, значит, для каждого $\alpha \in A$ существует множество гомоморфизмов Ψ_α из свободной группы F в $\prod_{\alpha \in A} G_\alpha$ такое, что

$$T_\alpha = \bigcap_{\psi_\alpha \in \Psi_\alpha} \ker \psi_\alpha.$$

Вернемся к подмножеству T и покажем, что $T = \bigcap T_\alpha$. По построению каждый гомоморфизм φ_α есть произведение гомоморфизмов π_α и φ. Кроме того, $\ker \varphi\pi_\alpha \supseteq \ker \varphi$ и $T_\alpha \supseteq T$ для всех $\alpha \in A$. Следовательно, $T \subseteq \bigcap T_\alpha$. Если $\bigcap T_\alpha \setminus T \neq \varnothing$, то найдутся такие $t \in \bigcap T_\alpha$, что $t \notin T$. Значит, существуют $t \in F$ и $\varphi \in \Phi$, для которых $\varphi(t) \neq 1$. Но в таком случае найдется $\alpha \in A$, для которого $\varphi_\alpha(t) \neq 1$. Это противоречит тому, что $t \in \bigcap T_\alpha$. Таким образом,

$$T = \bigcap_{\psi_\alpha \in \Psi_\alpha,\ \alpha \in A} \ker \psi_\alpha.$$

Следовательно, множество T замкнуто относительно декартова произведения $\prod_{\alpha \in A} G_\alpha$, и, значит, $\prod_{\alpha \in A} H_\alpha \preceq \prod_{\alpha \in A} G_\alpha$. □

Утверждение 2.6. *Геометрическое многообразие замкнуто относительно декартовых степеней.*

Д о к а з а т е л ь с т в о. Пусть $\mathfrak{K}$ — геометрическое многообразие и $G \in \mathfrak{K}$. По утверждению 1.3 всякая группа геометрически эквивалентна любой своей декартовой степени, тогда, по следствию 2.1, декартова степень группы G принадлежит $\mathfrak{K}$. □

2.2. Геометрические многообразия и предмногообразия

Следующий пример показывает, что геометрические многообразия в общем случае не замкнуты относительно декартовых произведений.

Пример 2.1. Пусть $\mathfrak{X} = \{Z_2,\ Z_3\}$ — две конечные циклические группы порядков два и три соответственно. Хорошо известно, что $Z_2 \times Z_3 = Z_6$. Покажем, что $Z_6 \notin \mathrm{gvar}\ \mathfrak{X}$. В свободной группе $F_1 = F(x)$ подгруппа $\langle x^6 \rangle$, являясь ядром гомоморфизма из F_1 на Z_6, замкнута относительно Z_6, но не замкнута относительно Z_2, и, следовательно, $Z_6 \preceq Z_2$ не выполняется. Аналогично не выполняется то, что $Z_6 \preceq Z_3$. В силу (2.1) $Z_6 \notin \mathrm{gvar}\ \mathfrak{X}$ и $\mathrm{gvar}\ \mathfrak{X}$ не замкнуто относительно декартовых произведений.

Хотя геометрические многообразия не замкнуты относительно прямых и тем более декартовых произведений, они все же замкнуты относительно декартовых степеней (см. утверждение 2.6). В случае, если геометрическое многообразие $\mathfrak{R}$ замкнуто относительно декартовых произведений, оно, будучи замкнутым относительно подгрупп (следствие 2.1), является предмногообразием и, более того, в этом случае $\mathfrak{R}$ становится локально замкнутым (см. лемму 2.2 ниже). Отметим также, что если класс $\mathfrak{X}$ замкнут относительно декартовых произведений, то и $\mathrm{gvar}\ \mathfrak{X}$ замкнут относительно декартовых произведений. Это следует из утверждения 2.5.

Теперь рассмотрим один частный случай, когда геометрическое многообразие замкнуто относительно декартовых произведений.

Лемма 2.1. *Если в классе $\mathfrak{X}$ есть наибольший элемент относительно отношения $\preceq$, то* $\mathrm{gvar}\ \mathfrak{X}$ *замкнут относительно декартовых произведений.*

Доказательство. Пусть G — наибольший элемент в классе $\mathfrak{X}$ и H_α, $\alpha \in A$ — семейство групп из класса $\mathfrak{X}$. По условию леммы $H_\alpha \preceq G$ для каждого α, а из утверждения 2.5 следует, что $\overline{H} = \prod H_\alpha \preceq \prod G_\alpha$. По утверждению 2.6 $\prod G_\alpha \in \mathfrak{X}$, а по определению геометрического многообразия $\overline{H} \in \mathrm{gvar}\ \mathfrak{X}$. □

Лемма 2.2. *Если геометрическое многообразие замкнуто относительно декартовых произведений, то оно локально замкнуто.*

Доказательство. Пусть $\mathfrak{K}$ — геометрическое многообразие, замкнутое относительно декартовых произведений, и $G_i \in \mathfrak{X}$, где G_i — конечно порожденные подгруппы группы G и $i \in I$. По условию $\prod G_i \in \mathfrak{K}$. Поскольку всякий гомоморфизм конечно порожденной свободной группы в группу G является также и гомоморфизмом в группу $\prod G_i$, то $G \preceq \prod G_i$, что влечет за собой $G \in \mathfrak{K}$. По определению локальной замкнутости лемма доказана. □

Теорема 2.1. *Если геометрическое многообразие, порожденное классом $\mathfrak{K}$ групп, замкнуто относительно декартовых произведений, то* $\mathrm{gvar}\ \mathfrak{K} = \mathrm{Lpvar}\ \mathfrak{K}$.

Доказательство. По следствию 2.1 геометрическое многообразие $\mathrm{gvar}\ \mathfrak{K}$ замкнуто относительно подгрупп. По условию теоремы $\mathrm{gvar}\ \mathfrak{K}$ замкнуто относительно декартовых произведений, и по лемме 2.2 $\mathrm{gvar}\ \mathfrak{K}$ локально замкнуто. Следовательно, $\mathrm{gvar}\ \mathfrak{K} = \mathrm{Lpvar}\ (\mathrm{gvar}\ \mathfrak{K})$. Поскольку $\mathrm{Lpvar}\ (\mathrm{gvar}\ \mathfrak{K}) \supseteq \mathrm{Lpvar}\ \mathfrak{K}$, то $\mathrm{gvar}\ \mathfrak{K} \supseteq \mathrm{Lpvar}\ \mathfrak{K}$. Пусть теперь $H \in \mathrm{gvar}\ \mathfrak{K}$. В этом случае $H \preceq G$ для некоторой группы G из класса $\mathfrak{K}$. По утверждению 2.3 всякая конечно порожденная подгруппа $K \leq H$ вкладывается в подходящую декартову степень группы G и, следовательно, принадлежит $\mathrm{pvar}\ \mathfrak{K}$. Таким образом, $H \in \mathrm{Lpvar}\ \mathfrak{K}$, $\mathrm{gvar}\ \mathfrak{K} \subseteq \mathrm{Lpvar}\ \mathfrak{K}$ и, значит, $\mathrm{gvar}\ \mathfrak{K} = \mathrm{Lpvar}\ \mathfrak{K}$. □

Следствие 2.2. *Если класс групп $\mathfrak{X}$ замкнут относительно декартовых произведений, то* $\mathrm{gvar}\ \mathfrak{X} = \mathrm{Lpvar}\ \mathfrak{X}$.

Доказательство следует из утверждения 2.5 и теоремы 2.1. □

Следствие 2.3. *Геометрическое многообразие, порожденное одной группой, совпадает с локальным замыканием предмногообразия, порожденного этой группой.*

Д о к а з а т е л ь с т в о. Класс, состоящий из одной группы G, имеет наибольший элемент относительно предпорядка $\preceq$, это сама группа G. По лемме 2.1 геометрическое многообразие $\mathrm{gvar}\, G$ замкнуто относительно декартовых произведений, а по теореме 2.1 $\mathrm{gvar}\, G = \mathrm{Lpvar}\, G$. □

Следствие 2.4. *$H \preceq G$ тогда и только тогда, когда любая конечно порожденная подгруппа группы H вкладывается в подходящую декартову степень группы G.*

Д о к а з а т е л ь с т в о следует из утверждения 2.3 и следствия 2.3. □

Следствие 2.5. *Всякое многообразие (квазимногообразие) групп образует геометрическое многообразие. Предмногообразие групп образует геометрическое многообразие тогда и только тогда, когда оно локально замкнуто.*

Следствие 2.6. *Класс нильпотентных групп и класс разрешимых групп образуют геометрические многообразия.*

Д о к а з а т е л ь с т в о следует из утверждения 2.2 и следствия 2.5. □

3. Пополнения нильпотентных групп и геометрическая эквивалентность

В этом параграфе рассматриваются условия, при которых нильпотентные группы без кручения геометрически эквивалентны своим минимальным пополнениям, и приводятся примеры нильпотентных групп, геометрически не эквивалентных своим минимальным пополнениям (примеры 3.1–3.3). Кроме того, эти группы геометрически не эквивалентны никаким своим собственным подгруппам.

3.1. Геометрическая эквивалентность нильпотентных групп и их пополнений

В этом пункте приведены необходимые и достаточные условия (теорема 3.1) геометрической эквивалентности нильпотентных групп и их минимальных пополнений. Как следствие, получена геометрическая эквивалентность двуступенно нильпотентных групп без кручения и их пополнений (следствие 3.1). Как и ранее (см. п. 1.4), через $G^\sharp$ обозначаем минимальное пополнение нильпотентной группы G. Через H^n обозначается вербальная подгруппа, порожденная n-ми степенями элементов группы H.

Лемма 3.1. *Пусть N — нильпотентная группа без кручения и H — подгруппа группы N такая, что $\mathrm{I}(H) = N$, где $\mathrm{I}(H)$ — изолятор подгруппы H. Тогда из геометрической эквивалентности H и $H^\sharp$ следует геометрическая эквивалентность N и $N^\sharp$.*

Д о к а з а т е л ь с т в о. Из $H \le N \le N^\sharp$ следует $H \preceq N \preceq N^\sharp$. Поскольку $H^\sharp = I(H)^\sharp = N^\sharp$ и H геометрически эквивалентна $H^\sharp$, то $N^\sharp = H^\sharp \preceq H$ и все группы H, N, $H^\sharp$, $N^\sharp$ геометрически эквивалентны между собой. □

Теорема 3.1. *Пусть G — нильпотентная группа без кручения и $G^\sharp$ — ее минимальное пополнение. Для геометрической эквивалентности групп G и $G^\sharp$ необходима и достаточна геометрическая эквивалентность группы G подгруппам G^n при каждом натуральном n.*

Д о к а з а т е л ь с т в о. Пусть группы G и $G^\sharp$ геометрически эквивалентны. Покажем геометрическую эквивалентность G и G^n, $n \in \mathbb{N}$. Поскольку $G^n \leq G$, то достаточно установить $G \preceq G^n$. Пусть $H \leq G$ — конечно порожденная подгруппа и $h_1, \ldots, h_s$ — ее система порождающих. Решим в группе $G^\sharp$ уравнения $x_i^n = h_i$ и обозначим: $h_i^{\frac{1}{n}} = x_i$, $H^{\frac{1}{n}} = \langle h_1^{\frac{1}{n}}, \ldots, h_s^{\frac{1}{n}} \rangle$. Поскольку $H^{\frac{1}{n}} \leq G^\sharp$, то $H^{\frac{1}{n}} \preceq G^\sharp$ и, значит, $H^{\frac{1}{n}} \preceq G$. По следствию 2.4 $H^{\frac{1}{n}}$ вкладывается в декартову степень группы G, но тогда H вкладывается в декартову степень группы G^n. Снова используем следствие 2.4 и получаем $G \preceq G^n$.

Пусть группа G геометрически эквивалентна подгруппам G^n, $n \in \mathbb{N}$. Покажем геометрическую эквивалентность групп G и $G^\sharp$. Как и ранее, $G \leq G^\sharp$, поэтому достаточно установить $G^\sharp \preceq G$. Снова рассмотрим конечно порожденную подгруппу $H = \langle h_1, \ldots, h_s \rangle < G^\sharp$. По следствию 1.2 найдем натуральное n такое, что $H^n \leq G$. Пусть k — ступень нильпотентности группы G. По условию G геометрически эквивалентна подгруппе G^{n^k}, что влечет за собой $H^n \preceq G^{n^k}$. По следствию 2.4 существует вложение φ подгруппы H^n в декартову степень $\prod_{i\in I} G_i^{n^k}$, здесь G_i — изоморфные копии группы G. По теореме 1.1 вложение φ однозначно продолжается до вложения φ группы $(H^n)^\sharp = H^\sharp$ в группу $(\prod_{i\in I} G_i^{n^k})^\sharp = (\prod_{i\in I} G_i)^\sharp$. Через $\varphi_i(h_j^n)$, $i \in I$, $j = 1, \ldots, s$ обозначим i-е координаты элементов $\varphi(h_j^n)$ в декартовой степени $\prod_{i\in I} G_i^{n^k}$. По лемме 1.2 в группах G_i решаются уравнения $x_{i,j}^n = \varphi_i(h_j^n)$, а ввиду однозначности извлечения корней в нильпотентных группах без кручения $\varphi_i(h_j) \in G_i$, $i \in I$, $j = 1, \ldots, s$. Таким образом, подгруппа H вкладывается в декартову степень группы G и, по следствию 2.4, $H \preceq G$. Снова используя следствие 2.4, получаем $G^\sharp \preceq G$. □

Следствие 3.1. *Двуступенно нильпотентные группы без кручения геометрически эквивалентны своим минимальным пополнениям.*

Д о к а з а т е л ь с т в о. Пусть N — двуступенно нильпотентная группа без кручения и $H < N$ — ее конечно порожденная подгруппа. В факторгруппе $H/I(H')$ выберем базис $\overline{h}_1, \ldots, \overline{h}_k$ и через $h_1, \ldots, h_k$ обозначим прообразы этих базисных элементов. Также выберем базис $c_1, \ldots, c_s$ в коммутанте группы H. Пусть $H_1 = \langle h_1, \ldots, h_k, c_1, \ldots, c_s \rangle$. Из выбора базисных элементов следует, что $I(H_1) = H$. В силу леммы 3.1 достаточно показать, что подгруппа H_1 геометрически эквивалентна своему минимальному пополнению $H_1^\sharp$. Пусть $V(h_1, \ldots, h_k, c_1, \ldots, c_s) = 1$ есть соотношение в группе H_1. Это соотношение можно переписать в виде

$$h_1^{n_1} \cdot \ldots \cdot h_k^{n_k} c_1^{m_1} \cdot \ldots \cdot c_s^{m_s} W([h_i, h_j]) = 1, \tag{3.1}$$

где $W([h_i, h_j])$ — групповое слово от коммутаторов $[h_i, h_j]$, $i, j = 1, \ldots, k$. Переходя к факторгруппе $H_1/I(H')$, получим, что $n_1 = \cdots = n_k = 0$. Таким образом, соотношение (3.1) должно иметь вид

$$c_1^{m_1} \cdot \ldots \cdot c_s^{m_s} W([h_i, h_j]) = 1.$$

В этом случае при отображении $\varphi_n : h_i \mapsto h_i^n$, $c_j \mapsto c_j^{n^2}$ получаем $[h_i, h_j]^{\varphi_n} = [h_i, h_j]^{n^2}$ и соотношение (3.1) сохраняется. Поскольку группа H_1 не имеет кручения, то φ_n продолжается до изоморфизма H_1 на $\langle h_1^n, \ldots, h_k^n, c_1^{n^2}, \ldots, c_s^{n^2} \rangle < H_1^n$, и по теореме 3.1 H_1 геометрически эквивалентна $H_1^\sharp$. □

3.2. Примеры

В этом параграфе приводятся различные примеры, показывающие, что в общем случае нильпотентные группы без кручения могут быть геометрически не эквивалентны своим минимальным пополнениям. Для доказательства этого факта используется теорема 3.1. Отметим также, что по следствию 3.1 такие примеры могут быть только среди нильпотентных групп ступеней нильпотентности не менее трех.

П р и м е р 3.1. Пусть $N_{3,4}$ — трехступенно нильпотентная группа с порождающими a, b, c, d и определяющими соотношениями

$$
\begin{gathered}
[a,[a,b]] = [a,b,b] = [a,[c,d]] = [a,d,d] = 1, \\
[b,[b,c]] = [b,[c,d]] = [c,[c,d]] = [c,d,d] = 1,
\end{gathered} \tag{3.2}
$$

$$
[a,[b,c]] \cdot [a,c,b] = [a,[b,d]] \cdot [a,d,b] = 1, \tag{3.3}
$$

$$
\begin{gathered}
[a,[a,d]] \cdot [b,c,c]^{-1} = [a,[a,c]] \cdot [b,[b,d]]^{-1} = 1, \\
[a,c,b] \cdot [b,d,d]^{-1} = [a,c,c] \cdot [b,d,c]^{-1} = [a,d,b] \cdot [a,d,c]^{-1} = 1,
\end{gathered} \tag{3.4}
$$

$$
[a,b] \cdot [a,c,c]^{-1} = [c,d] \cdot [a,[a,c]]^{-1} = 1. \tag{3.5}
$$

П р и м е р 3.2. $N_{4,3}$ — четырехступенно нильпотентная группа с порождающими a, b, c и определяющими соотношениями

$$
\begin{gathered}
[a,[a,[a,c]]] = [a,[a,b,b]] = [a,[a,c,c]] = [a,b,b,b] = 1, \\
[a,[b,c,c]] = [b,[b,c,c]] = [b,c,c,c] = 1, \\
[a,[a,c,b]] \cdot [a,b,[a,c]] = [a,[b,[b,c]]] \cdot [a,[b,c],b]^2 \cdot [a,c,b,b] = 1, \\
[a,[a,c]] \cdot [a,[a,c,b]] = [a,b,b] \cdot [a,[b,c],b] = [b,c,c] \cdot [a,c,[b,c]] = 1.
\end{gathered}
$$

П р и м е р 3.3. $N_{5,2}$ — пятиступенно нильпотентная группа с порождающими a, b и определяющими соотношениями

$$
\begin{gathered}
[a,[a,[a,[a,b]]]] = [a,[a,b,b,b]] = [a,b,b,b,b] = [a,[a,[a,b,b]]] \cdot [a,[a,b],[a,b]]^{-1} = 1, \\
[a,[a,[a,b]]] \cdot [a,[a,b],[a,b]]^{-1} \cdot [a,b,[a,b,b]]^{-1} = [a,b,b,b] \cdot [a,b,[a,b,b]]^{-1} = 1.
\end{gathered}
$$

Рассмотрим подробно пример 3.1. По построению группа $N_{3,4}$ трехступенно нильпотентна. Проверим, что эта группа не имеет кручения. Для этого представим ее как факторгруппу свободной трехступенно нильпотентной группы $N = N(x_1, x_2, x_3, x_4)$ по изолированной нормальной подгруппе. Для этого берем последовательно факторгруппы N по изолированным подгруппам центров, пользуясь тем, что центр нильпотентной группы без кручения изолирован и что подгруппа A конечно порожденной абелевой группы B изолирована, когда факторгруппа B/A свободна. Выберем в N коммутаторный базис [16], например, $U = \{u_1, \ldots, u_{30}\}$, где:

$$
\begin{gathered}
u_1 = x_1, \qquad u_2 = x_2, \qquad u_3 = x_3, \qquad u_4 = x_4, \qquad u_5 = [x_1,x_2], \qquad u_6 = [x_1,x_3], \\
u_7 = [x_1,x_4], \qquad u_8 = [x_2,x_3], \qquad u_9 = [x_2,x_4], \qquad u_{10} = [x_3,x_4], \\
u_{11} = [x_1,[x_1,x_2]], \qquad u_{12} = [x_1,[x_1,x_3]], \qquad u_{13} = [x_1,[x_1,x_4]], \qquad u_{14} = [x_1,x_2,x_2], \\
u_{15} = [x_1,[x_2,x_3]], \qquad u_{16} = [x_1,[x_2,x_4]], \qquad u_{17} = [x_1,x_3,x_2], \qquad u_{18} = [x_1,x_3,x_3], \\
u_{19} = [x_1,[x_3,x_4]], \qquad u_{20} = [x_1,x_4,x_2], \qquad u_{21} = [x_1,x_4,x_3], \qquad u_{22} = [x_1,x_4,x_4], \\
u_{23} = [x_2,[x_2,x_3]], \qquad u_{24} = [x_2,[x_2,x_4]], \qquad u_{25} = [x_2,x_3,x_3], \qquad u_{26} = [x_2,[x_3,x_4]], \\
u_{27} = [x_2,x_4,x_3], \qquad u_{28} = [x_2,x_4,x_4], \qquad u_{29} = [x_3,[x_3,x_4]], \qquad u_{30} = [x_3,x_4,x_4].
\end{gathered}
$$

Каждый элемент $g \in N$ однозначно представляется в виде

$$
g = u_1^{n_1} \cdot \cdots \cdot u_{30}^{n_{30}}, \qquad n_1, \ldots, n_{30} \in \mathbb{Z}.
$$

Пусть $u'_{17} = u_{15}u_{17}$, $u'_{20} = u_{16}u_{20}$ и $K_1 = \langle u_{11}, u_{14}, u'_{17}, u'_{20}, u_{19}, u_{22}, u_{23}, u_{26}, u_{29}, u_{30} \rangle$. Подгруппа K_1 содержится в центре $\zeta(N)$ группы N, факторгруппа $\zeta(N)/K_1$ — свободная абелева группа и поэтому K_1 — нормальная изолированная подгруппа. Таким образом, факторгруппа $N_1 = N/K_1$ не имеет кручения. В качестве коммутаторного базиса группы N_1 можно взять $V = \{v_1, \ldots, v_{20}\}$, где $v_i = u_i K_1$ при $1 \le i < 11$, $v_{11} = u_{12}K_1$, $v_{12} = u_{13}K_1$, $v_{13} = u_{15}K_1$, $v_{14} = u_{16}K_1$, $v_{15} = u_{18}K_1$, $v_{16} = u_{21}K_1$, $v_{17} = u_{24}K_1$, $v_{18} = u_{25}K_1$, $v_{19} = u_{27}K_1$, $v_{20} = u_{28}K_1$. При этом $u_{11}K_1 = K_1$, $u_{14}K_1 = K_1$, $u_{17}K_1 = u_{15}^{-1}K_1 = v_{13}^{-1}$, $u_{19}K_1 = K_1$, $u_{20}K_1 = u_{16}^{-1}K_1 = v_{14}^{-1}$, $u_{22}K_1 = K_1$, $u_{23}K_1 = K_1$,$u_{26}K_1 = K_1$, $u_{29}K_1 = K_1$, $u_{30}K_1 = K_1$.

Отметим, что в группе N_1 выполняются соотношения (3.2), (3.3) при $a = v_1$, $b = v_2$, $c = v_3$, $d = v_4$.

Элементы u_{11}, u_{14}, $u_{15}u_{17}$, $u_{16}u_{20}$ принадлежат K_1, поэтому $[v_1, v_5] = [x_1, [x_1, x_2]]K_1 = K_1$, $[v_5, v_2] = [x_1, x_2, x_2]K_1 = K_1$, $[v_5, v_3] = [x_1, x_2, x_3]K_1 = [x_1, [x_2, x_3]] \cdot [x_1, x_3, x_2]K_1 = K_1$, $[v_5, v_4] = [x_1, x_2, x_4]K_1 = [x_1, [x_2, x_4]] \cdot [x_1, x_4, x_2]K_1 = K_1$ и v_5 лежит в центре группы N_1. Аналогично показывается, что $v_{10} = [x_3, x_4]K_1$ лежит в центре группы N_1. Поскольку группа N_1 трехступенно нильпотентна, то в центре группы N_1 также лежат элементы $v_{11}, \ldots, v_{20}$.

Обозначим: $v'_{11} = v_{10}v_{11}^{-1}$, $v'_{15} = v_5 v_{15}^{-1}$, $v'_{16} = v_{14}v_{16}$, $v'_{17} = v_{11}v_{17}^{-1}$, $v'_{18} = v_{12}v_{18}^{-1}$, $v'_{19} = v_{15}v_{19}^{-1}$, $v'_{20} = v_{13}v_{20}$. Подгруппа $K_2 = \langle v'_{11}, v'_{15}, v'_{16}, v'_{17}, v'_{18}, v'_{19}, v'_{20}\rangle$ является изолированной подгруппой центра группы N_1, и, следовательно, факторгруппа $N_2 = N_1/K_2$ не имеет кручения.

Положим: $w_i = v_i K_2$, $i = 1, \ldots, 10$, $w_{11} = v_{12}K_2$, $w_{12} = v_{13}K_2$, $w_{13} = v_{14}K_2$. При $a = w_1$, $b = w_2$, $c = w_3$, $d = w_4$ в группе N_2 выполняются соотношения (3.2)–(3.5), и в качестве $N_{3,4}$ можно взять группу N_2. Непосредственные вычисления показывают, что элементы $a = w_1, \ldots, d = w_4$ порождают группу $N_{3,4}$, не принадлежат ее второму гиперцентру $\zeta_2(N_{3,4})$ и образуют базис свободной абелевой группы $N_{3,4}/\zeta_2(N_{3,4})$; элементы $w_6 = [a, c]$, $w_7 = [a, d]$, $w_8 = [b, c]$, $w_9 = [b, d]$ порождают второй гиперцентр, не принадлежат центру группы и образуют базис свободной абелевой группы $\zeta_2(N_{3,4})/\zeta(N_{3,4})$; элементы

$$\begin{gathered} [a, b] = w_5, \qquad [c, d] = w_{10}, \\ [a, [a, d]] = w_{11}, \qquad [a, [b, c]] = w_{12}, \qquad [a, [b, d]] = w_{13} \end{gathered} \tag{3.6}$$

образуют базис центра группы $N_{3,4}$. В целом элементы $w_1, \ldots, w_{13}$ образуют коммутаторный базис группы $N_{3,4}$, т.е. элементы группы $N_{3,4}$ имеют однозначное представление вида

$$g = w_1^{n_1} w_2^{n_2} \cdot \cdots \cdot w_{13}^{n_{13}}.$$

При этом коммутаторы, не входящие в базис $w_5, \ldots, w_{13}$, имеют следующее представление:

$$\begin{gathered} [a, [a, b]] = [a, b, b] = [a, [c, d]] = [a, d, d] = 1, \\ [b, [b, c]] = [b, [c, d]] = [c, [c, d]] = [c, d, d] = 1, \\ [a, [a, c]] = [b, [b, d]] = w_{10}, \qquad [a, c, b] = [b, d, d] = w_{12}^{-1}, \\ [a, c, c] = [b, d, c] = w_5, \qquad [a, d, b] = [a, d, c] = w_{13}^{-1}, \qquad [b, c, c] = w_{11}. \end{gathered} \tag{3.7}$$

Рассмотрим свойства эндоморфизмов группы $N_{3,4}$. Введем обозначения для образов порождающих группы $N_{3,4}$ при эндоморфизме $\varphi : N_{3,4} \to N_{3,4}$:

$$\begin{gathered} a^\varphi = a^{n_{11}} b^{n_{12}} c^{n_{13}} d^{n_{14}} U_1, \qquad b^\varphi = a^{n_{21}} b^{n_{22}} c^{n_{23}} d^{n_{24}} U_2, \\ c^\varphi = a^{n_{31}} b^{n_{32}} c^{n_{33}} d^{n_{34}} U_3, \qquad d^\varphi = a^{n_{41}} b^{n_{42}} c^{n_{43}} d^{n_{44}} U_4, \end{gathered} \tag{3.8}$$

где $U_i \in N'_{3,4}$, $i = 1, \ldots, 4$.

Составим матрицу из показателей n_{ij} в формулах (3.8):

$$A_\varphi = \begin{pmatrix} n_{11} & n_{12} & n_{13} & n_{14} \\ n_{21} & n_{22} & n_{23} & n_{24} \\ n_{31} & n_{32} & n_{33} & n_{34} \\ n_{41} & n_{42} & n_{43} & n_{44} \end{pmatrix}.$$

Рассмотрим отдельно невырожденный ($|A_\varphi| \neq 0$) и вырожденный ($|A_\varphi| = 0$) случаи.

Лемма 3.2. *Пусть φ — эндоморфизм группы $N_{3,4}$ и $|A_\varphi| \neq 0$. Тогда φ является* IA-*автоморфизмом:*

$$a^\varphi = aU_1, \qquad b^\varphi = bU_2, \qquad c^\varphi = cU_3, \qquad d^\varphi = dU_4, \qquad U_1, \ldots, U_4 \in N'_{3,4}. \tag{3.9}$$

Д о к а з а т е л ь с т в о. Поскольку φ — гомоморфизм, то соотношения (3.2)–(3.5) индуцируют соответствующие соотношения в подгруппе $N_{3,4}^\varphi \leq N_{3,4}$. Рассмотрим соотношения (3.5) по модулю $\zeta(N_{3,4})$:

$$1 \equiv [a^\varphi, b^\varphi] \equiv [a,c]^{\delta_{12}^{13}} [a,d]^{\delta_{12}^{14}} [b,c]^{\delta_{12}^{23}} [b,d]^{\delta_{12}^{24}} \pmod{\zeta(N_{3,4})},$$

где $\delta_{ij}^{ks} = \begin{vmatrix} n_{ik} & n_{is} \\ n_{jk} & n_{js} \end{vmatrix}$. В силу того что элементы $[a,c], [a,d], [b,c], [b,d]$ образуют базис в $\zeta_2(N_{3,4})/\zeta(N_{3,4})$, имеют место равенства: $\delta_{12}^{13} = \delta_{12}^{14} = \delta_{12}^{23} = \delta_{12}^{24} = 0$.

Так как по условию $|A_\varphi| \neq 0$, то δ_{12}^{12} и δ_{12}^{34} одновременно не могут равняться нулю. Допустим, что $\delta_{12}^{12} \neq 0$. Если $n_{13} \neq 0$, то, не теряя общности, считаем $n_{13} = 1$, и из равенства $\delta_{12}^{13} = 0$ следует, что $n_{21} = n_{11}n_{23}$, а из $\delta_{12}^{23} = 0$ следует, что $n_{22} = n_{12}n_{23}$. Подставляя значения n_{21} и n_{22} в δ_{12}^{12}, получим противоречие: $n_{11}n_{12}n_{23} - n_{11}n_{12}n_{23} \neq 0$. Следовательно, $n_{13} = 0$. Меняя в матрице 3-й и 4-й столбцы, находим, что $n_{14} = 0$. Рассуждая таким же образом, доказываем, что если $\delta_{12}^{12} \neq 0$, то $n_{13} = n_{14} = n_{23} = n_{24} = 0$.

Теперь рассмотрим второе равенство в (3.5) по модулю $\zeta(N_{3,4})$:

$$1 \equiv [c^\varphi, d^\varphi] \equiv [a,c]^{\delta_{34}^{13}} [a,d]^{\delta_{34}^{14}} [b,c]^{\delta_{34}^{23}} [b,d]^{\delta_{34}^{24}} \pmod{\zeta(N_{3,4})}.$$

Это дает $\delta_{34}^{13} = \delta_{34}^{14} = \delta_{34}^{23} = \delta_{34}^{24} = 0$, а для δ_{34}^{12} и δ_{34}^{34} получаем 2 случая: $\delta_{34}^{12} \neq 0$, $n_{33} = n_{34} = n_{43} = n_{44} = 0$ или $\delta_{34}^{34} \neq 0$, $n_{31} = n_{32} = n_{41} = n_{42} = 0$.

Объединяя эти случаи и учитывая, что $|A_\varphi| \neq 0$, получим, что исходная матрица принимает один из двух видов:

$$A_1 = \begin{pmatrix} n_{11} & n_{12} & 0 & 0 \\ n_{21} & n_{22} & 0 & 0 \\ 0 & 0 & n_{33} & n_{34} \\ 0 & 0 & n_{43} & n_{44} \end{pmatrix} \qquad \text{или} \qquad A_2 = \begin{pmatrix} 0 & 0 & n_{13} & n_{14} \\ 0 & 0 & n_{23} & n_{24} \\ n_{31} & n_{32} & 0 & 0 \\ n_{41} & n_{42} & 0 & 0 \end{pmatrix}.$$

Если $A_\varphi = A_1$, то

$$\begin{aligned} a^\varphi &= a^{n_{11}} b^{n_{12}} U_1, \qquad & b^\varphi &= a^{n_{21}} b^{n_{22}} U_2, \\ c^\varphi &= c^{n_{33}} d^{n_{34}} U_3, \qquad & d^\varphi &= c^{n_{43}} d^{n_{44}} U_4, \end{aligned} \tag{3.10}$$

где $U_i \in N'_{3,4} = \zeta_2(N_{3,4})$. Положим для определенности

$$U_i = [a,c]^{m_{i1}} [a,d]^{m_{i2}} [b,c]^{m_{i3}} [b,d]^{m_{i4}} V_i, \tag{3.11}$$

где $m_{i1}, \ldots, m_{i4} \in \mathbb{Z}$, $V_i \in \zeta(N_{3,4})$, $i = 1, \ldots, 4$.

Рассмотрим соотношение $[b^\varphi, [b^\varphi, c^\varphi]] = 1$, индуцированное соотношением из (3.2). Воспользуемся представлением (3.10) для b^φ и c^φ, коммутаторными соотношениями и представлениями (3.7) для коммутаторов. Получим

$$1 = [b^\varphi, [b^\varphi, c^\varphi]] = [a^{n_{21}} b^{n_{22}} U_2, [a^{n_{21}} b^{n_{22}} U_2, c^{n_{33}} d^{n_{34}} U_3]]$$

$$= [a,[a,c]]^{n_{21}^2 n_{33}} \cdot [a,[a,d]]^{n_{21}^2 n_{34}} \cdot [a,[b,c]]^{n_{21} n_{22} n_{33}} \cdot [a,[b,d]]^{n_{21} n_{22} n_{34}}$$

$$\times [b,[a,c]]^{n_{21} n_{22} n_{33}} \cdot [b,[a,d]]^{n_{21} n_{22} n_{34}} \cdot [b,[b,c]]^{n_{22}^2 n_{33}} \cdot [b,[b,d]]^{n_{22}^2 n_{34}}$$

$$= [c,d]^{n_{21}^2 n_{33}+n_{22}^2 n_{34}} \cdot [a,[a,d]]^{n_{21}^2 n_{34}} \cdot [a,[b,d]]^{2n_{21}n_{22}n_{34}} \cdot [a,[b,c]]^{n_{21}n_{22}n_{33}}.$$

Произведение степеней базисных элементов равно единице только в одном случае, когда показатели степени равны нулю. Имеем следующие равенства:

$$n_{21}^2 n_{33} + n_{22}^2 n_{34} = 0, \tag{3.12}$$

$$n_{21}^2 n_{34} = 0. \tag{3.13}$$

Допустим, что $n_{21} \neq 0$. Тогда (3.13) дает $n_{34} = 0$, что вместе с (3.12) влечет за собой $n_{33} = 0$, а это противоречит тому, что $\delta_{34}^{34} \neq 0$. Следовательно, $n_{21} = 0$. Учитывая, что $\delta_{12}^{12} \neq 0$, получаем $n_{11} \neq 0$ и $n_{22} \neq 0$. Теперь из (3.12) следует, что $n_{34} = 0$, и ввиду того, что $\delta_{34}^{34} \neq 0$, имеем: $n_{33} \neq 0$ и $n_{44} \neq 0$.

Рассмотрим еще одно соотношение $[a^\varphi, d^\varphi, d^\varphi] = 1$, индуцированное соотношением из (3.2):

$$1 = [a^\varphi, d^\varphi, d^\varphi] = [a^{n_{11}} b^{n_{12}} U_1, c^{n_{43}} d^{n_{44}} U_4, c^{n_{43}} d^{n_{44}} U_4]$$

$$= [a,c,c]^{n_{11}n_{43}^2} \cdot [a,c,d]^{n_{11}n_{43}n_{44}} \cdot [a,d,c]^{n_{11}n_{43}n_{44}} \cdot [a,d,d]^{n_{11}n_{44}^2}$$

$$\times [b,c,c]^{n_{12}n_{43}^2} \cdot [b,c,d]^{n_{12}n_{43}n_{44}} \cdot [b,d,c]^{n_{12}n_{43}n_{44}} \cdot [b,d,d]^{n_{12}n_{44}^2}$$

$$= [a,b]^{n_{11}n_{43}^2+2n_{12}n_{43}n_{44}} \cdot [a,[b,d]]^{-n_{11}n_{43}n_{44}} \cdot [a,[a,d]]^{n_{12}n_{43}^2} \cdot [b,[b,c]]^{-n_{12}n_{44}^2}.$$

Это приводит к равенствам

$$n_{11}n_{44}n_{43} = 0, \qquad n_{12}n_{44}^2 = 0.$$

Поскольку $n_{11} \neq 0$ и $n_{44} \neq 0$, то необходимо $n_{43} = 0$ и $n_{12} = 0$. Матрица A_1 приобретает вид:

$$A_1 = \begin{pmatrix} n_{11} & 0 & 0 & 0 \\ 0 & n_{22} & 0 & 0 \\ 0 & 0 & n_{33} & 0 \\ 0 & 0 & 0 & n_{44} \end{pmatrix}.$$

Рассмотрим соотношения из (3.4) при отображении группы $N_{3,4}$ в H с учетом предыдущих вычислений. Из соотношения $[a^\varphi, d^\varphi, b^\varphi] \cdot [a^\varphi, d^\varphi, c^\varphi]^{-1} = 1$ получаем

$$n_{22} = n_{33}. \tag{3.14}$$

Из соотношения $[a^\varphi, c^\varphi, c^\varphi] \cdot [b^\varphi, d^\varphi, c^\varphi]^{-1} = 1$ получаем $n_{11}n_{33} = n_{22}n_{44}$ и, учитывая (3.14), получаем

$$n_{11} = n_{44}. \tag{3.15}$$

Из соотношения $[a^\varphi, c^\varphi, b^\varphi] \cdot [b^\varphi, d^\varphi, d^\varphi]^{-1} = 1$ получаем $n_{11}n_{33} = n_{44}^2$ и, учитывая (3.15), получаем

$$n_{33} = n_{44}. \tag{3.16}$$

Учитывая равенства (3.14), (3.15), (3.16), получаем, что все диагональные элементы матрицы равны между собой, т.е. $n_{11} = n_{22} = n_{33} = n_{44} = n$. Таким образом,

$$a^\varphi = a^n U_1, \qquad b^\varphi = b^n U_2, \qquad c^\varphi = c^n U_3, \qquad d^\varphi = d^n U_4, \tag{3.17}$$

где $U_i \in N'_{3,4} = \zeta_2(N_{3,4})$.

Рассмотрим соотношение $[a^\varphi, b^\varphi] \cdot [a^\varphi, c^\varphi, c^\varphi]^{-1} = 1$ из (3.5) с учетом представления (3.17) для образов порождающих и представления (3.11) для $U_1, \ldots, U_4$. Имеем

$$[a^\varphi, b^\varphi] = [a^n \cdot [a,c]^{m_{11}} [a,d]^{m_{12}} [b,c]^{m_{13}} [b,d]^{m_{14}} V_1, b^n \cdot [a,c]^{m_{21}} [a,d]^{m_{22}} [b,c]^{m_{23}} [b,d]^{m_{24}} V_2]$$

$$= [a,b]^{n^2} \cdot [a,[a,c]]^{nm_{21}}[a,[a,d]]^{nm_{22}}[a,[b,c]]^{nm_{23}}[a,[b,d]]^{nm_{24}}$$
$$\times [a,c,b]^{nm_{11}}[a,d,b]^{nm_{12}}[b,c,b]^{nm_{13}}[b,d,b]^{nm_{14}}$$
$$= [a,b]^{n^2} \cdot [c,d]^{nm_{21}-nm_{14}} \cdot [a,[a,d]]^{nm_{22}} \cdot [a,[b,c]]^{nm_{23}-nm_{11}} \cdot [a,[b,d]]^{nm_{24}-nm_{12}};$$
$$[a^\varphi, c^\varphi, c^\varphi] = [a,c,c]^{n^3} = [a,b]^{n^3}.$$

Сравнивая показатели при базисных элементах, получаем $n^2 = n^3$ и $n = 1$. Таким образом, в случае $A_\varphi = A_1$ выполняется (3.9) и φ — IA-автоморфизм.

Пусть теперь $A_\varphi = A_2$. В этом случае

$$\begin{aligned} a^\varphi &= c^{n_{13}}d^{n_{14}}U_1, \qquad & b^\varphi &= c^{n_{23}}d^{n_{24}}U_2, \\ c^\varphi &= a^{n_{31}}b^{n_{32}}U_3, \qquad & d^\varphi &= a^{n_{41}}b^{n_{42}}U_4, \end{aligned} \tag{3.18}$$

где $U_i \in N'_{3,4} = \zeta_2(N_{3,4})$.

Используя представления (3.18) для образов базисных элементов, рассмотрим соотношения $[a^\varphi, d^\varphi, d^\varphi] = 1$ и $[b^\varphi, [b^\varphi, c^\varphi]] = 1$, индуцированные соотношениями из (3.2):

$$[a^\varphi, d^\varphi, d^\varphi] = [c^{n_{13}}d^{n_{14}}U_1, a^{n_{41}}b^{n_{42}}U_4, a^{n_{41}}b^{n_{42}}U_4]$$
$$= [c,a,a]^{n_{13}n_{41}^2}[c,a,b]^{n_{13}n_{41}n_{42}}[c,b,a]^{n_{13}n_{41}n_{42}}[c,b,b]^{n_{13}n_{42}^2}$$
$$\times [d,a,a]^{n_{14}n_{41}^2}[d,a,b]^{n_{14}n_{41}n_{42}}[d,b,a]^{n_{14}n_{41}n_{42}}[d,b,b]^{n_{14}n_{42}^2}$$
$$= [c,d]^{n_{13}n_{41}^2+n_{14}n_{42}^2} \cdot [a,[a,d]]^{n_{14}n_{41}^2} \cdot [a,[b,c]]^{2n_{13}n_{41}n_{42}} \cdot [a,[b,d]]^{2n_{14}n_{41}n_{42}} = 1.$$

Приравниваем к нулю показатели при базисных коммутаторах и получаем

$$n_{13}n_{41}^2 + n_{14}n_{42}^2 = 0, \qquad n_{14}n_{41}^2 = 0.$$

Если $n_{14} \neq 0$, то из второго равенства имеем $n_{41} = 0$, что вместе с первым равенством дает $n_{42} = 0$, а это невозможно ввиду $\delta_{34}^{12} \neq 0$. Таким образом,

$$n_{14} = 0, \qquad n_{41} = 0, \qquad n_{13} \neq 0, \qquad n_{24} \neq 0. \tag{3.19}$$

Имеем

$$[b^\varphi, [b^\varphi, c^\varphi]] = [c^{n_{23}}d^{n_{24}}U_2, [c^{n_{23}}d^{n_{24}}U_2, a^{n_{31}}b^{n_{32}}U_3]]$$
$$= [c,[c,a]]^{n_{23}^2n_{31}}[c,[c,b]]^{n_{23}^2n_{32}}[c,[d,a]]^{n_{23}n_{24}n_{31}}[c,[d,b]]^{n_{23}n_{24}n_{32}}$$
$$\times [d,[c,a]]^{n_{24}n_{23}n_{31}}[d,[c,b]]^{n_{24}n_{23}n_{32}}[d,[d,a]]^{n_{24}^2n_{31}}[d,[d,b]]^{n_{24}^2n_{32}}$$
$$= [a,b]^{n_{23}^2n_{31}+2n_{24}n_{24}n_{32}} \cdot [a,[a,d]]^{n_{23}^2n_{32}} \cdot [a,[b,c]]^{-n_{24}^2n_{32}} \cdot [a,[b,d]]^{-2n_{24}n_{23}n_{31}} = 1.$$

Отсюда

$$n_{23}^2n_{31} + 2n_{24}n_{24}n_{32} = 0, \qquad n_{24}^2n_{32} = 0.$$

Ввиду (3.19) $n_{24} \neq 0$, следовательно, $n_{32} = 0$, а $n_{31} \neq 0$. Теперь из первого равенства и из $\delta_{12}^{34} \neq 0$ получаем $n_{23} = 0$, $n_{42} \neq 0$. Таким образом,

$$\begin{aligned} a^\varphi &= c^{n_{13}}U_1, \qquad & b^\varphi &= d^{n_{24}}U_2, \\ c^\varphi &= a^{n_{31}}U_3, \qquad & d^\varphi &= b^{n_{42}}U_4, \end{aligned} \tag{3.20}$$

где $n_{13}n_{24}n_{31}n_{42} \neq 0$, $U_i \in N'_{3,4} = \zeta_2(N_{3,4})$.

Наконец, рассмотрим соотношение $[a^\varphi, [a^\varphi, c^\varphi]] = [b^\varphi, [b^\varphi, d^\varphi]]$, индуцированное соотношением из (3.4):

$$[a^\varphi, [a^\varphi, c^\varphi]] = [c,[c,a]]^{n_{13}^2n_{31}} = [a,b]^{n_{13}^2n_{31}} = [b^\varphi, [b^\varphi, d^\varphi]] = [d,[d,b]]^{n_{24}^2n_{42}} = [a,[b,c]]^{-n_{13}^2n_{31}}.$$

Это влечет за собой $n_{13}^2n_{31} = 0$, что противоречит соотношениям $|A_\varphi| = n_{13}n_{24}n_{31}n_{42} \neq 0$. Таким образом, случай $A_\varphi = A_2$ невозможен. □

Лемма 3.3. *Пусть φ — эндоморфизм группы $N_{3,4}$ и $|A_\varphi| = 0$, тогда $\zeta(N_{3,4}) \leq \ker\varphi$.*

Доказательство. Из линейной зависимости строк матрицы A_φ следует, что найдутся целые t_1, t_2, t_3, t_4, не все равные нулю, для которых

$$a^{t_1\varphi}b^{t_2\varphi}c^{t_3\varphi}d^{t_4\varphi}U = 1, \tag{3.21}$$

где $U \in N'_{3,4} = \zeta_2(N_{3,4})$.

Из равенства (3.21) получаем

$$[[a^{t_1\varphi}b^{t_2\varphi}c^{t_3\varphi}d^{t_4\varphi}U, x^\varphi], y^\varphi] = [a,x,y]^{t_1\varphi}[b,x,y]^{t_2\varphi}[c,x,y]^{t_3\varphi}[d,x,y]^{t_4\varphi} = 1.$$

Придавая переменным x и y последовательно значения a, b, c, d и учитывая, что эндоморфизм φ сохраняет соотношения (3.2)–(3.5), получим следующие равенства:

1) $x = a$, $y = a$

$$[b,a,a]^{t_2\varphi} \cdot [c,a,a]^{t_3\varphi} \cdot [d,a,a]^{t_4\varphi} = [c,d]^{t_3\varphi} \cdot [a,[a,d]]^{t_4\varphi} = 1, \tag{3.22}$$

2) $x = a$, $y = b$

$$[b,a,b]^{t_2\varphi} \cdot [c,a,b]^{t_3\varphi} \cdot [d,a,b]^{t_4\varphi} = [a,[b,c]]^{-t_3\varphi} \cdot [a,[b,d]]^{-t_4\varphi} = 1, \tag{3.23}$$

3) $x = b$, $y = b$

$$[a,b,b]^{t_1\varphi} \cdot [c,b,b]^{t_3\varphi} \cdot [d,b,b]^{t_4\varphi} = [c,d]^{t_4\varphi} = 1, \tag{3.24}$$

4) $x = a$, $y = c$

$$[b,a,c]^{t_2\varphi} \cdot [c,a,c]^{t_3\varphi} \cdot [d,a,c]^{t_4\varphi} = [a,b]^{-t_3\varphi} \cdot [a,[b,d]]^{-t_4\varphi} = 1, \tag{3.25}$$

5) $x = c$, $y = a$

$$[a,c,a]^{t_1\varphi} \cdot [b,c,a]^{t_2\varphi} \cdot [d,c,a]^{t_4\varphi} = [c,d]^{-t_1\varphi} \cdot [a,[b,c]]^{-t_2\varphi} = 1, \tag{3.26}$$

6) $x = c$, $y = c$

$$[a,c,c]^{t_1\varphi} \cdot [b,c,c]^{t_2\varphi} \cdot [d,c,c]^{t_4\varphi} = [a,b]^{t_1\varphi} \cdot [a,[a,d]]^{t_2\varphi} = 1, \tag{3.27}$$

7) $x = b$, $y = c$

$$[a,b,c]^{t_1\varphi} \cdot [c,b,c]^{t_3\varphi} \cdot [d,b,c]^{t_4\varphi} = [a,b]^{-t_4\varphi} \cdot [a,[a,d]]^{-t_3\varphi} = 1, \tag{3.28}$$

8) $x = c$, $y = b$

$$[a,c,b]^{t_1\varphi} \cdot [b,c,b]^{t_2\varphi} \cdot [d,c,b]^{t_4\varphi} = [a,[b,c]]^{-t_1\varphi} = 1, \tag{3.29}$$

9) $x = a$, $y = d$

$$[b,a,d]^{t_2\varphi} \cdot [c,a,d]^{t_3\varphi} \cdot [d,a,d]^{t_4\varphi} = [a,[b,d]]^{t_3\varphi} = 1, \tag{3.30}$$

10) $x = d$, $y = a$

$$[a,d,a]^{t_1\varphi} \cdot [b,d,a]^{t_2\varphi} \cdot [c,d,a]^{t_3\varphi} = [a,[a,d]]^{-t_1\varphi} \cdot [a,[b,d]]^{-t_2\varphi} = 1, \tag{3.31}$$

11) $x = b$, $y = d$

$$[a,b,d]^{t_1\varphi} \cdot [c,b,d]^{t_3\varphi} \cdot [d,b,d]^{t_4\varphi} = [a,b]^{-t_3\varphi} \cdot [a,[b,c]]^{t_4\varphi} = 1, \tag{3.32}$$

12) $x = d$, $y = b$

$$[a,d,b]^{t_1\varphi} \cdot [b,d,b]^{t_2\varphi} \cdot [c,d,b]^{t_3\varphi} = [c,d]^{-t_2\varphi} \cdot [a,[b,d]]^{-t_1\varphi} = 1, \tag{3.33}$$

13) $x = c$, $y = d$

$$[a, c, d]^{t_1\varphi} \cdot [b, c, d]^{t_2\varphi} \cdot [d, c, d]^{t_4\varphi} = [a, b]^{t_2\varphi} \cdot [a, [b, d]]^{-t_1\varphi} = 1. \tag{3.34}$$

Покажем, что при любых нетривиальных наборах t_1, t_2, t_3, t_4 все базисные элементы $[a, b]$, $[c, d]$, $[a, [a, d]]$, $[a, [b, c]]$, $[a, [b, d]]$ центра группы $N_{3,4}$ отображаются эндоморфизмом φ в единицу.

Пусть $t_1 \neq 0$. Тогда из (3.29) следует, что $[a, [b, c]]^\varphi = 1$. С учетом полученного, из (3.26) следует $[c, d]^\varphi = 1$. Теперь (3.33) дает $[a, [b, d]]^\varphi = 1$, (3.31) дает $[a, [a, d]]^\varphi = 1$ и (3.27) дает $[a, b]^\varphi = 1$.

Пусть $t_1 = 0$ и $t_2 \neq 0$. Применяя последовательно (3.27), (3.26), (3.31), (3.33) и (3.34), получаем $[a, [a, d]]^\varphi = 1$, $[a, [b, c]]^\varphi = 1$, $[a, [b, d]]^\varphi = 1$, $[c, d]^\varphi = 1$ и $[a, b]^\varphi = 1$.

Пусть $t_1 = t_2 = 0$ и $t_3 \neq 0$. Тогда из (3.30), (3.23), (3.25), (3.28) и (3.22) вытекает $[a, [b, d]]^\varphi = 1$, $[a, [b, c]]^\varphi = 1$, $[a, b]^\varphi = 1$, $[a, [a, d]]^\varphi = 1$ и $[c, d]^\varphi = 1$.

Пусть $t_1 = t_2 = t_3 = 0$ и $t_4 \neq 0$. Тогда из (3.22), (3.23), (3.24), (3.28) и (3.32) получаем $[a, [a, d]]^\varphi = 1$, $[a, [b, d]]^\varphi = 1$, $[c, d]^\varphi = 1$, $[a, b]^\varphi = 1$ и $[a, [b, c]]^\varphi = 1$. □

Леммы 3.2 и 3.3 справедливы и для групп в примерах 3.2 и 3.3. Пример 3.3 рассмотрен в работе [4], а разбор примера 3.2 оставляем читателю. Отметим, что в примере 3.1 используется группа с четырьмя порождающими, в примере 3.2 — группа с тремя порождающими, но ее ступень нильпотентности увеличена до четырех, а в примере 3.3 — группа ступени нильпотентности пять с двумя порождающими. Таким образом, во всех этих примерах сумма числа порождающих и ступени нильпотентности равна семи. По-видимому, для нильпотентных групп без кручения ступени нильпотентности k с r порождающими леммы 3.2 и 3.3 не выполняются, если $r + k < 7$. Значение лемм 3.2 и 3.3 раскрывается ниже в утверждении 3.1, следствии 3.2 и теореме 3.2.

Утверждение 3.1. *Если G — конечно порожденная нильпотентная группа без кручения, и для каждого эндоморфизма $\varphi : G \to G$ либо $\ker\varphi \supseteq \zeta(G)$, либо φ — автоморфизм, то группа G геометрически не эквивалентна никакой своей собственной подгруппе.*

Доказательство. Пусть k — ступень нильпотентности и r — число порождающих группы G. Представим G как факторгруппу свободной группы F ранга r по нормальной подгруппе S. По определению S является G-замкнутой подгруппой. Покажем, что S не H-замкнута для любой собственной подгруппы $H < G$. Рассмотрим $\overline{S}$ — замыкание подгруппы S относительно H: $\overline{S} = \bigcap_{i\in I} \ker\varphi_i$, где $\{\varphi_i \mid i \in I\}$ — подмножество всех гомоморфизмов φ из F в H, для которых $S \subseteq \ker\varphi$. Пусть $\varphi_i(F) \leq H$ — образ группы F в H при гомоморфизме φ_i. Поскольку $S \subseteq \ker\varphi_i$ и $F/S \cong G$, то φ_i индуцирует эндомоморфизм $\widetilde{\varphi}_i$ из G на $\varphi_i(F)$. Этот эндоморфизм не может быть автоморфизмом, поскольку $H \neq G$, следовательно, $\zeta(G) \leq \ker\widetilde{\varphi}$ и поэтому ступень нильпотентности $\varphi_i(F)$ строго меньше k. А это значит, что $\gamma_k(F) \leq \ker\varphi_i$ для всех $i \in I$, откуда $\gamma_k(F) \leq \overline{S}$. Но $\gamma_k(F) \nleq S$, поскольку ступень нильпотентности F/S равна k. Таким образом, $S \neq \overline{S}$, S не H-замкнута и G геометрически не эквивалентна H. □

Следствие 3.2. *Группы $N_{3,4}$, $N_{4,3}$ и $N_{5,2}$ из примеров* 3.1–3.3 *геометрически не эквивалентны никаким своим собственным подгруппам.*

Теорема 3.2. *Существуют нильпотентные группы без кручения, геометрически не эквивалентные своим минимальным пополнениям. При этом такие группы существуют в многообразии нильпотентных групп ступеней* 3, 4 *и* 5.

Доказательство. По следствию 3.2 группы $N_{3,4}$, $N_{4,3}$ и $N_{5,2}$ из примеров 3.1–3.3 геометрически не эквивалентны никаким своим собственным подгруппам, в частности подгруппам $N^2_{3,4}$, $N^2_{4,3}$, $N^2_{5,2}$ соответственно. По теореме 3.1 эти группы не могут быть геометрически эквивалентными своим минимальным пополнениям. □

В заключение отметим еще одно свойство группы $N_{3,4}$ из примера 3.1, которое решает вопрос 1.1 из работы [4] о существовании трехступенно нильпотентных упорядоченных групп, всякий автоморфизм которых сохраняет порядок.

Теорема 3.3. *Существует трехступенно нильпотентная линейно упорядоченная группа G, всякий автоморфизм которой сохраняет порядок группы. При этом* $\mathrm{Aut}\, G$ *— тоже линейно упорядоченная группа.*

Доказательство. По лемме 3.2 всякий автоморфизм группы $N_{3,4}$ является IA-автоморфизмом. Упорядочим группу $N_{3,4}$ так, чтобы ее выпуклые подгруппы составляли нижний центральный ряд. Заметим, что нижний центральный ряд группы $N_{3,4}$ совпадает с ее верхним центральным рядом, а потому состоит из изолированных подгрупп. По лемме 2 из работы [4] IA-автоморфизмы действуют тождественно на факторах нижнего центрального ряда и, следовательно, сохраняют порядок группы. $\square$

4. Геометрическая эквивалентность и квазимногообразия

Связь геометрической эквивалентности с квазимногообразиями рассматривалась в работах [17, 19, 21, 22]. В этих работах было показано, что если группы геометрически эквивалентны, то они порождают одинаковые квазимногообразия, а также рассматривались условия, при которых и обратное утверждение верно. Так, например, нетеровы по уравнениям группы (в частности, нильпотентные и линейные группы) геометрически эквивалентны тогда и только тогда, когда они порождают одинаковые квазимногообразия [17]. Для произвольных групп это утверждение может оказаться неверным. Такие примеры приведены в работах [5, 9] (для абстрактных групп) и в [17] для групп с выделенными константами. Ниже (пример 4.1) будет подробно рассмотрен случай, когда две центрально-метабелевы группы порождают одно и то же квазимногообразие, но геометрически не эквивалентны. А сейчас приведем утверждение, непосредственно вытекающее из утверждения 2.4 и следствия 2.5.

Утверждение 4.1. *Для любого класса групп $\mathfrak{X}$ выполняется включение*

$$\mathrm{gvar}\, \mathfrak{X} \subseteq \mathrm{qvar}\, \mathfrak{X}.$$

Для геометрически нетеровых групп имеет место более сильное утверждение.

Утверждение 4.2. *Геометрическое многообразие, порожденное геометрически нетеровой группой, совпадает с квазимногообразием, порожденным этой группой.*

Доказательство. Пусть G — геометрически нетерова группа. По утверждению 4.1 $\mathrm{gvar}\, G \leq \mathrm{qvar}\, G$. Покажем, что $\mathrm{qvar}\, G \leq \mathrm{gvar}\, G$. Предположим противное: существует группа $H \in \mathrm{qvar}\, G$, для которой $H \not\preceq G$. В этом случае в свободной группе конечного ранга $F(x_1, \dots, x_n)$ найдется подмножество S, замкнутое относительно H, но не замкнутое относительно G. Пусть $\overline{S} = \mathrm{Cl}_G(S)$ — замыкание S относительно G, $u \in \overline{S} \setminus S$. Ввиду геометрической нетеровости группы G найдется конечное подмножество $S_0 = \{v_1, \dots, v_k\} \subseteq S$ такое, что $\mathrm{Cl}_G(S_0) = \overline{S}$. Поскольку $u \in \overline{S}$, то в группе G выполнено квазитождество

$$(\forall x_1 \dots x_n)\Big(\bigwedge_{i=1}^{s} v_i(x_1, \dots, x_n) = 1 \Rightarrow u(x_1, \dots, x_n) = 1\Big).$$

Оно выполняется и в группе H, поскольку $H \in \mathrm{qvar}\, G$. Значит, $u \in \mathrm{Cl}_H(S) = S$, что противоречит выбору элемента u.

Теперь рассмотрим связь квазимногообразий, порожденных нильпотентной группой без кручения и ее минимальным пополнением. По теореме Г. Баумслага [1], многообразие, порожденное нильпотентной группой без кручения, совпадает с многообразием, порожденным минимальным пополнением этой группы. Как показывает приведенная ниже теорема, этот результат не распространяется на квазимногообразия нильпотентных групп.

Теорема 4.1. *Квазимногообразие, порожденное нильпотентной группой без кручения, не обязательно совпадает с квазимногообразием, порожденным минимальным пополнением этой группы.*

Доказательство. По следствию 1.1 нильпотентные группы геометрически эквивалентны тогда и только тогда, когда они определяют одно и то же квазимногообразие. По теореме 3.2 существуют нильпотентные группы без кручения, геометрически не эквивалентные своим минимальным пополнениям. Например, группы из примеров 3.1–3.3. Следовательно, квазимногообразия, порожденные такими группами, отличаются от квазимногообразий, порожденных их минимальными пополнениями. □

В заключение приведем пример двух центрально-метабелевых групп, порождающих одно и то же квазимногообразие, но геометрически не эквивалентных.

Пример 4.1. Построение примера начнем с двуступенно нильпотентной группы B с порождающими b_i, $i \in \mathbb{Z}$, и дополнительными соотношениями:

$$[b_i, b_j] = [b_{i+k}, b_{j+k}], \qquad i, j, k \in \mathbb{Z}.$$

Обозначим коммутаторы $[b_j, b_0]$, $j \in \mathbb{N}$ через c_i. Элементы b_i, $i \in \mathbb{Z}$, и c_j, $j \in \mathbb{N}$, образуют базис нильпотентной группы B, т.е. каждый элемент $g \in B$ имеет однозначное представление следующего вида:

$$g = b_{i_1}^{n_1} \cdot \dots \cdot b_{i_k}^{n_k} \cdot c_{j_1}^{m_1} \cdot \dots \cdot c_{j_s}^{m_1}, \qquad i_1, \dots, i_k, n_1, \dots, n_k, m_1, \dots, m_s \in \mathbb{Z}, \qquad k, s, j_1, \dots, j_s \in \mathbb{N}.$$

Группа B допускает автоморфизм $a : b_i \mapsto b_{i+1}$. Построим полупрямое произведение группы B на бесконечную циклическую группу $\langle a \rangle$ согласно этому автоморфизму: $A = B \rtimes \langle a \rangle$. Отметим, что группа A порождается двумя элементами a и $b = b_0$, а из определяющих соотношений группы B следует, что A является центральным расширением свободной абелевой группы $C = \langle c_j \mid j \in \mathbb{N} \rangle$ с помощью метабелевой группы $\langle b \rangle \wr \langle a \rangle$ — сплетения двух бесконечных циклических групп. Из свойств полупрямого произведения получаем, что каждый элемент g группы A имеет однозначное представление следующего вида:

$$g = a^n \cdot h, \quad \text{где } h \in B,\ n \in \mathbb{Z}.$$

Ввиду указанных представлений для элементов групп A и B система уравнений $x_n^n = g$, $n \in \mathbb{N}$ не имеет решений в группе A при $g \neq 1$, поскольку в группе A нет нетривиальных бесконечно делимых элементов.

Определим последовательность групп A_i, $i \in \mathbb{N}$, полагая $A_1 = A$, а при $i > 1$ в качестве A_i берем факторгруппу группы A по нормальной подгруппе, порожденной следующими элементами из центра группы A:

$$[b, b^{a^k}]^k [b, b^a]^{-1}, \qquad 1 < k \leq i. \tag{4.1}$$

Нетрудно заметить, что не только в группе A, но и в каждой из групп A_i нет нетривиальных бесконечно делимых элементов. А это значит, что в прямом произведении $G = \prod_{i \in \mathbb{N}} A_i$ также нет нетривиальных бесконечно делимых элементов. В дальнейшем нам понадобятся две последовательности элементов $\{g_i\}_{i \in \mathbb{N}}$ и $\{h_i\}_{i \in \mathbb{N}}$ группы G, которые определим следующим образом: обозначим через $\overline{a}_i$, $\overline{b}_i$ образы элементов $a, b \in A$ при естественном гомоморфизме A на A_i, $i \in \mathbb{N}$ и положим $g_i = \{x_{i,j}\}_{i,j\in\mathbb{N}}$, $h_i = \{y_{i,j}\}_{i,j\in\mathbb{N}}$, где

$$x_{i,j}, y_{i,j} \in A_i, \qquad x_{i,j} = \begin{cases} \overline{a}_i, & \text{если } i = j, \\ 1, & \text{если } i \neq j, \end{cases} \qquad y_{i,j} = \begin{cases} \overline{a}_i, & \text{если } i = j, \\ 1, & \text{если } i \neq j, \end{cases} \qquad i, j \in \mathbb{N}.$$

Рассмотрим $\widetilde{G} = G^{\mathbb{N}}/U$ — ультрастепень группы G по неглавному ультрафильтру. Известно (см., например, [15]), что группы G и $\widetilde{G}$ определяют одно и то же квазимногообразие. Покажем, что эти группы геометрически не эквивалентны. Для этого найдем в свободной группе $F = F(x, y)$ подгруппу S, замкнутую относительно $\widetilde{G}$, но не G-замкнутую. Определим в группе $\widetilde{G}$ подгруппу $H = \langle \alpha, \beta \rangle$, где α и β представляются по модулю ультрафильтра последовательностями $\{g_i\}_{i\in\mathbb{N}}$ и $\{h_i\}_{i\in\mathbb{N}}$ соответственно. Через S обозначим ядро гомоморфизма свободной группы $F(x, y)$ на H. Ввиду (4.1) во всех группах A_i при $i \geq k$ выполняются соотношения $[\overline{b}_i, \overline{b}_i^{\overline{a}_i^k}]^k[\overline{b}_i, \overline{b}_i^{\overline{a}_i}]^{-1} = 1$. По свойствам ультрапроизведения в группе $\widetilde{G}$ выполнено соотношение $[\beta, \beta^{\alpha^k}]^k[\beta, \beta^{\alpha}]^{-1} = 1$ и, значит,

$$[y, y^{x^k}]^k \cdot [y, y^x]^{-1} \in S \qquad \text{для всех } k \in \mathbb{N}.$$

Отметим также, что $[\beta, \beta^{\alpha}] \neq 1$ в подгруппе H, откуда $[y, x^y] \notin S$. Поскольку подгруппа S является ядром гомоморфизма свободной группы $F(x, y)$ в группу $\widetilde{G}$, то она $\widetilde{G}$-замкнута. Покажем, что S не G-замкнута. Действительно, при любом гомоморфизме $\varphi : F(x, y) \to G$ с условием $S \leq \ker\varphi$ имеем $[y, x^y]^{\varphi} = 1$, поскольку элемент $[y, x^y]$ отображается в бесконечно делимый элемент группы G, а в этой группе нет нетривиальных бесконечно делимых элементов. Таким образом, $[y, y^x]$ принадлежит замыканию S относительно G, $[y, y^x] \notin S$, и S не G-замкнута.

Поступила 19.10.2006

СПИСОК ЛИТЕРАТУРЫ

1. **Baumslag G.** On the residual nilpotence of some varietal products // Trans. Amer. Math. Soc. 1963. V. 109. P. 357–365.
2. **Baumslag G., Miasnikov A., Remeslennikov V.** Algebraic geometry over groups I: Algebraic sets and ideal theory // J. Algebra. 1999. V. 219. P. 16–79.
3. **Baumslag G., Miasnikov A. and Roman'kov V.** Two theorems about equationally Noetherian groups // J. Algebra. 1997. V. 194. P. 654–664.
4. **Bludov V.** Ordered groups in which every automorphism preserves the order // Ordered Algebraic Structures: Nanjing / Ed. by W.C. Holland. Amsterdam: Gordon and Breach, 2001. P. 23–28.
5. **Bludov V.** Геометрическая эквивалентность групп и квазимногообразия // Логика и приложения: Тез. междунар. конф. Новосибирск, 2000. С. 18.
6. **Блудов В.В., Гусев Б.В.** Геометрическая эквивалентность нильпотентных групп // Комбинаторные и вычислительные методы в математике: Тез. докл. междунар. конф. Омск, 1998. С. 31–32.
7. **Блудов В.В., Гусев Б.В.** О геометрической эквивалентности групп // Алгебра и линейная оптимизация: Тр. междунар. семинара, посвященного 90-летию со дня рожд. С.Н. Черникова. Екатеринбург, 2002. С. 59–65.
8. **Блудов В.В., Гусев Б.В.** О геометрических многообразиях групп // Алгебра и ее приложения: Тез. докл. междунар. конф. Красноярск: КГУ, 2002. С. 18–19.
9. **Göbel R. and Shelah S.** Radicals and Plotkin's problem concerning geometrically equivalent groups // Proc. Amer. Math. Soc. 2002. V. 130, no. 3. P. 673–674.
10. **Каргаполов А.И., Мерзляков Ю.И.** Основы теории групп. М.: Наука, 1996.
11. **Кон П.** Универсальная алгебра. М.: Наука, 1968.
12. **Курош А.Г.** Теория групп. М.: Наука, 1967.
13. **Мальцев А.И.** Об одном классе однородных пространств // Изв. АН СССР. Математика. 1949. Т. 13, № 1. С. 9–32 (см. также: Избранные труды. М.: Наука, 1976. Т. 1. С. 220–240).

14. **Мальцев А.И.** Нильпотентные группы без кручения // Изв. АН СССР. Математика. 1949. Т. 13, № 3. С. 201–212 (см. также: Избранные труды. М.: Наука, 1976. Т. 1. С. 241–251).
15. **Мальцев А.И.** Алгебраические системы. М.: Наука, 1970.
16. **Мельников О.В., Ремесленников В.Н., Романьков В.А. и др.** Общая алгебра. М.: Наука, 1990. Т. 1.
17. **Miasnikov A., Remeslennikov V.** Algebraic geometry over groups II: Logical Foundations // J. Algebra. 2000. V. 234. C. 225–276.
18. Нерешенные вопросы теории групп: Коуровская тетрадь. Новосибирск: Новосиб. гос. ун-т, 2002.
19. **Plotkin B.** Varieties of algebras and algebraic varieties // Israel J. of Math. 1996. V. 96. C. 511–522.
20. **Plotkin B.** Algebraic geometry in universal algebra // Междунар. алг. конф. памяти Д.К.Фаддеева. Санкт-Петербург, 1997. С. 99–100.
21. **Plotkin B.** Seven Lectures on Universal Algebraic Geometry: Preprint no. 1 //Jerusalem: Institute of Mathematics, Hebrew University, 2000–2001.
22. **Plotkin B.** Some problems in nonclassical algebraic geometry // Ukrain. Math. J. 2002. V. 54, no. 6. C. 1019-1026.

ТРУДЫ ИНСТИТУТА МАТЕМАТИКИ И МЕХАНИКИ УрО РАН

Том 13 № 1 2007

УДК 512.542

О СУЩЕСТВОВАНИИ КАРТЕРОВЫХ ПОДГРУПП[1]

Е. П. Вдовин

В работе получен критерий существования картеровой подгруппы в конечной группе в терминах нормального ряда. Приведен пример, показывающий, что критерий не может быть переформулирован в терминах композиционного ряда. В заключение дана классификация картеровых подгрупп в почти простых группах.

Введение

Напомним, что нильпотентная самонормализуемая подгруппа группы G называется *картеровой подгруппой*. Согласно классическому результату, полученному Картером [1], любая конечная разрешимая группа содержит картеровы подгруппы и все они сопряжены. Говорят, что конечная группа G удовлетворяет условию **(C)**, если для любого ее неабелева композиционного фактора S и любой ее нильпотентной подгруппы N картеровы подгруппы группы $\langle \mathrm{Aut}_N(S), S\rangle$ либо не существуют, либо сопряжены (определение группы $\mathrm{Aut}_N(S)$ дано ниже). В работе [2] доказано, что если конечная группа удовлетворяет условию **(C)**, то ее картеровы подгруппы сопряжены. В недавней работе [3, теорема 10.1] доказано, что в любой почти простой группе с известным цоколем картеровы подгруппы сопряжены. Таким образом, по модулю классификации конечных простых групп в любой конечной группе картеровы подгруппы сопряжены. В настоящей работе под конечной группой мы всегда имеем в виду конечную группу, удовлетворяющую **(C)**, и поэтому результаты работы не зависят от классификации конечных простых групп. Существуют конечные группы без картеровых подгрупп, минимальным примером является группа Alt_5. В работе мы даем критерий существования картеровых подгрупп в терминах нормального ряда.

Если G — группа, A, B, H — подгруппы группы G и $B \trianglelefteq A$ (т.е. B нормальна в A), то $N_H(A/B) = N_H(A) \cap N_H(B)$. Если $x \in N_H(A/B)$, то x индуцирует автоморфизм $Ba \mapsto Bx^{-1}ax$ группы A/B. Таким образом, существует гомоморфизм группы $N_H(A/B)$ в $\mathrm{Aut}(A/B)$. Образ этого гомоморфизма обозначается через $\mathrm{Aut}_H(A/B)$, в то время как его ядро обозначается через $C_H(A/B)$. В частности, если $S = A/B$ — композиционный фактор группы G, то для любой $H \leq G$ группа $\mathrm{Aut}_H(A/B)$ определена.

Пусть $G = G_0 \geq G_1 \geq \ldots \geq G_n = \{e\}$ — неуплотняемый нормальный ряд группы G (напомним, что по предположению G удовлетворяет **(C)**). Тогда $G_i/G_{i+1} = T_{i,1} \times \ldots \times T_{i,k_i}$, где $T_{i,1} \simeq \ldots \simeq T_{i,k_i} \simeq T_i$ и T_i — простая группа. Если $i \geqslant 1$, то обозначим через $\overline{K}_i$ картерову подгруппу группы G/G_i (если она существует) и через K_i ее полный прообраз в G/G_{i+1}. Если $i = 0$, то $\overline{K}_0 = \{e\}$ и $K_0 = G/G_1$. Мы говорим, что конечная группа G удовлетворяет условию **(E)**, если для любых i, j либо $\overline{K}_i$ не существует, либо $\mathrm{Aut}_{K_i}(T_{i,j})$ содержит картерову подгруппу.

Следующая лемма показывает, что гомоморфный образ картеровой подгруппы вновь является картеровой подгруппой. Мы будем постоянно использовать этот факт.

[1]Работа выполнена при финансовой поддержке РФФИ (проект 05–01–00797), гранта Президента РФ (МК–1455.2005.1) и СО РАН (грант № 29 для молодых ученых и интеграционный проект 2006.1.2).

Лемма 1 ([3], лемма 2.1). *Пусть G — конечная группа, K — картерова и N — нормальная подгруппы группы G. Предположим, что KN удовлетворяет* **(C)** *(это условие автоматически выполнено, если G удовлетворяет* **(C)** *или если N разрешима) или $KN = G$. Тогда KN/N является картеровой подгруппой группы G/N.*

1. Критерий

Лемма 2. *Пусть G — конечная группа, H — нормальная подгруппа группы G и S — композиционный фактор группы G/H (следовательно, также группы G). Тогда $\mathrm{Aut}_G(S) = \mathrm{Aut}_{G/H}(S)$.*

Д о к а з а т е л ь с т в о. Обозначим G/H через $\overline{G}$ и пусть A, B таковы, что $S = A/B$ и $H \leq B \leq A$. Заметим, что существует сюръективный гомоморфизм

$$\varphi : \mathrm{Aut}_G(S) \to \mathrm{Aut}_{\overline{G}}(S),$$

определенный правилом

$$\begin{tikzcd} \mathrm{Aut}_G(S) = \left(N_G(A) \cap N_G(B)\right)/C_G(A/B) \arrow[d, "\varphi"] \\ \left(N_G(A) \cap N_G(B)\right)/\left(HC_G(A/B)\right) = \mathrm{Aut}_{\overline{G}}(S). \end{tikzcd}$$

Поскольку $F^*(\mathrm{Aut}_G(S)) = S \cap \mathrm{Ker}(\varphi) = \{e\}$, то $\mathrm{Ker}(\varphi) = \{e\}$. $\square$

Далее нам потребуется дополнительная информация о строении картеровых подгрупп в группах специального вида. Пусть A' — группа с нормальной подгруппой T'. Рассмотрим прямое произведение $A_1 \times \ldots \times A_k$, где $A_1 \simeq \ldots \simeq A_k \simeq A'$, и его нормальную подгруппу $T = T_1 \times \ldots \times T_k$, где $T_1 \simeq \ldots \simeq T_k \simeq T'$. Рассмотрим симметрическую группу Sym_k, действующую на $A_1 \times \ldots \times A_k$ по правилу $A_i^s = A_{i^s}$ для всех $s \in S$, и определим X равным полупрямому произведению $(A_1 \times \ldots \times A_k) \leftthreetimes \mathrm{Sym}_k$ (подстановочное сплетение групп A' и Sym_k). Обозначим через A прямое произведение $A_1 \times \ldots \times A_k$ и через π_i проекцию $\pi_i : A \to A_i$. Справедлива следующая лемма.

Лемма 3. *Пусть G — такая подгруппа группы X, что $T \leq G$, группа $G/(G \cap T)$ нильпотентна и $(G \cap A)^{\pi_i} = A_i$. Предположим также, что A разрешима. Тогда если K — картерова подгруппа группы G, то $(K \cap A)^{\pi_i}$ — картерова подгруппа группы A_i.*

Д о к а з а т е л ь с т в о. Предположим, что утверждение неверно и пусть G — контрпример минимального порядка с минимальным k. Тогда $S = G/(G \cap A)$ примитивна. Докажем это. Сначала допустим, что S не является транзитивной, тогда $S \leq \mathrm{Sym}_{k_1} \times \mathrm{Sym}_{k-k_1}$, значит, $G \leq G_1 \times G_2$. Если мы обозначим через $\psi_i : G \to G_i$ естественный гомоморфизм, то $G^{\psi_i} = G_i$ удовлетворяет условиям леммы и $K^{\psi_i} = K_i$ является картеровой подгруппой группы G_i. Очевидно, $(G \cap A)^{\pi_j} = (G_i \cap A^{\psi_i})^{\pi_j}$, где $i = 1$, если $j \in \{1, \ldots, k_1\}$, и $i = 2$, если $j \in \{k_1 + 1, \ldots, k\}$, т. е. следующие диаграммы коммутативны:

$$\begin{tikzcd} G \cap A \arrow[rr, "\pi_j"] \arrow[dr, "\psi_1"'] & & A_j, \\ & G_1 \cap A^{\psi_1} \arrow[ur, "\pi_j"'] & \end{tikzcd} \qquad \begin{tikzcd} G \cap A \arrow[rr, "\pi_j"] \arrow[dr, "\psi_2"'] & & A_j, \\ & G_2 \cap A^{\psi_2} \arrow[ur, "\pi_j"'] & \end{tikzcd}$$

и по индукции мы получаем утверждение леммы; противоречие с выбором G. Если S транзитивна, но не примитивна, пусть

$$\Omega_1 = \{T_1, \ldots, T_m\}, \qquad \Omega_2 = \{T_{m+1}, \ldots, T_{2m}\}, \ldots, \qquad \Omega_l = \{T_{(l-1)m+1}, \ldots, T_{lm}\}$$

— система импримитивности. Тогда S содержит нетривиальную нетранзитивную нормальную подгруппу

$$F' \leq \underbrace{\mathrm{Sym}_m \times \ldots \times \mathrm{Sym}_m}_{l \text{ раз}},$$

где $k = m \cdot l$. Рассмотрим полный прообраз F группы F' в X. Тогда $G \cap F \leq F_1 \times \ldots \times F_l$. Обозначим через $\psi_i : F \to F_i$ естественную проекцию, тогда $(G \cap F)^{\psi_i} = F_i$. Заметим, что все группы F_i удовлетворяют условиям леммы и, если мы определим $T_i' = T_{(i-1)m+1} \times \ldots \times T_{im}$, то G удовлетворяет условиям леммы с $T' = T_1' \times \ldots \times T_l'$ и $A' = F$. Легко доказать по индукции, что $(K \cap F)^{\psi_i}$ является картеровой подгруппой группы F_i и, если $j \in \{m \cdot (i-1)+1, \ldots m \cdot i\}$, то $\left((K \cap F)^{\psi_i} \cap A^{\psi_i}\right)^{\pi_j}$ является картеровой подгруппой группы A_j. Поскольку $(G \cap A)^{\pi_j} = \left((K \cap F)^{\psi_i} \cap A^{\psi_i}\right)^{\pi_j}$ (для подходящего i), мы получаем утверждение леммы вопреки выбору G. Значит, S примитивна.

Пусть Y' — минимальная нормальная подгруппа группы G, содержащаяся в T (если Y' тривиальна, то T тривиальна и доказывать нечего, поскольку в этом случае G нильпотентна). Таким образом, Y' является нормальной элементарной абелевой p-группой. Пусть $Y_i = (Y')^{\pi_i}$, тогда $Y = Y_1 \times \ldots \times Y_k$ — нетривиальная нормальная подгруппа группы G (Y является подгруппой группы G, поскольку $T \leq G$). Пусть $\overline{\pi}_i : (G \cap A) \to A_i/Y_i = \overline{A}_i$ — проекция, соответствующая проекции π_i. Обозначим через $\overline{K} = KY/Y$ соответствующую картерову подгруппу группы $\overline{G} = G/Y$. Тогда $\overline{G}$ удовлетворяет условиям леммы. По индукции доказывается, что $(\overline{K} \cap \overline{A})^{\overline{\pi}_i}$ является картеровой подгруппой группы $\overline{A}_i$. Пусть K_1 — полный прообраз группы $\overline{K}$ в G и пусть Q — холлова p'-подгруппа группы K_1. Тогда $(Q \cap A)^{\pi_i}$ является холловой p'-подгруппой группы $(K_1 \cap A)^{\pi_i}$. Из доказательства теоремы 20.1.4 в [4] легко получаем, что $K = N_{K_1}(Q)$ является картеровой подгруппой группы G, а $(N_{K_1 \cap A}(Q \cap A))^{\pi_i}$ — картеровой подгруппой группы A_i. Таким образом, нам нужно показать, что $(N_{K_1 \cap A}(Q \cap A))^{\pi_i} = (N_{K_1 \cap S}(Q))^{\pi_i}$. По индукции устанавливается равенство $(N_{\overline{K} \cap \overline{A}}(\overline{A} \cap \overline{Q}))^{\overline{\pi}_i} = (N_{\overline{K} \cap \overline{G}}(\overline{Q}))^{\overline{\pi}_i}$. Таким образом, нам необходимо доказать, что $(N_Y(Q \cap A))^{\pi_i} = (N_Y(Q))^{\pi_i}$. Заметим, что $(N_Y(Q \cap A))^{\pi_i} \leq N_{Y_i}((Q \cap A)^{\pi_i})$.

Поскольку S является примитивной подгруппой группы Sym_k, то $k = r$ — простое число, а $S = \langle s \rangle$ — циклическая группа. Если $r = p$, то $Q \cap A = Q$, и доказывать нечего. В противном случае пусть h — r-элемент из K, порождающий S по модулю $K \cap A$. Очевидно, $Q = (Q \cap A)\langle h \rangle$. Пусть $t \in Y_i$ — элемент группы $N_{Y_i}((Q \cap A)^{\pi_i})$. Тогда $(t \cdot t^h \cdot \ldots \cdot t^{h^{r-1}}) \in N_Y(Q)$ и $t^{\pi_i} = (t \cdot t^h \cdot \ldots \cdot t^{h^{r-1}})^{\pi_i}$, значит, $(N_Y(Q \cap A))^{\pi_i} \leq N_{Y_i}((Q \cap A)^{\pi_i}) \leq (N_Y(Q))^{\pi_i} \leq (N_Y(Q \cap A))^{\pi_i}$. $\Box$

Теорема 1. *Конечная группа G, удовлетворяющая условию* **(C)***, содержит картерову подгруппу тогда и только тогда, когда она удовлетворяет условию* **(E)**.

Д о к а з а т е л ь с т в о. Докажем сначала часть “только тогда”. Пусть H — минимальная нормальная подгруппа группы G. Тогда $H = T_1 \times \ldots \times T_k$, где $T_1 \simeq \ldots \simeq T_k \simeq T$ и T — простая группа.

Если T — циклическая группа простого порядка, то группа $\mathrm{Aut}(T)$ разрешима и содержит картерову подгруппу. Предположим, что T — неабелева простая группа. Очевидно, K является картеровой подгруппой группы KH. По [2, лемма 3] мы получаем, что $\mathrm{Aut}_{KH}(T_i)$ содержит картерову подгруппу для всех i. Индукция по порядку группы завершает доказательство необходимости.

Теперь докажем часть “тогда”. Вновь предположим противное: G не содержит картеровых подгрупп, но удовлетворяет **(E)** и имеет минимальный порядок. Пусть H — минимальная нормальная подгруппа группы G. Тогда $H = T_1 \times \ldots \times T_k$, где $T_1 \simeq \ldots \simeq T_k \simeq T$ (T — конечная простая группа).

По определению G/H удовлетворяет **(E)**, тогда по выбору G существует картерова подгруппа $\overline{K}$ группы $\overline{G} = G/H$. Пусть K — полный прообраз подгруппы $\overline{K}$, тогда K удовлетворяет **(E)**. Если $K \neq G$, то по выбору G группа K содержит картерову подгруппу K'. Заметим, что K' является картеровой подгруппой группы G. Действительно, предположим, что $x \in N_G(K') \setminus K'$. Поскольку $K'H/H = \overline{K}$ является картеровой подгруппой группы $\overline{G}$, мы получаем, что $x \in K$. Но K' является картеровой подгруппой группы K, таким образом $x \in K'$. Значит, $G = K$, т. е. G/H нильпотентна.

Если H абелева, то G разрешима, следовательно, G содержит картерову подгруппу, противоречие. Значит, T — неабелева простая конечная группа. Покажем сначала, что централизатор $M = C_G(H)$ тривиален. Предположим противное. Поскольку T — неабелева простая группа, то $M \cap H = \{e\}$, и поэтому группа M нильпотентна. По лемме 2 мы получаем, что G/M удовлетворяет **(E)**. По выбору G группа G/M содержит картерову подгруппу $\overline{K}$. Пусть K' — полный прообраз группы $\overline{K}$ в G. Тогда группа K' разрешима, следовательно, содержит картерову подгруппу K. Как и раньше, мы получаем, что K является картеровой подгруппой группы G, противоречие. Значит, $C_G(H) = \{e\}$.

Поскольку H является минимальной нормальной подгруппой группы G, мы получаем, что $\mathrm{Aut}_G(T_1) \simeq \mathrm{Aut}_G(T_2) \simeq \ldots \simeq \mathrm{Aut}_G(T_k)$. Таким образом, существует мономорфизм

$$\varphi : G \to (\mathrm{Aut}_G(T_1) \times \ldots \times \mathrm{Aut}_G(T_k)) \leftthreetimes \mathrm{Sym}_k = G_1,$$

и мы отождествляем G с G^φ. Обозначим через K_i картерову подгруппу группы $\mathrm{Aut}_G(T_i)$ и через A подгруппу $\mathrm{Aut}_G(T_1) \times \ldots \times \mathrm{Aut}_G(T_k)$. Поскольку G/H нильпотентна, то $K_iT_i = \mathrm{Aut}_G(T_i)$ и $G_1 = (K_1T_1 \times \ldots \times K_kT_k) \leftthreetimes \mathrm{Sym}_k$. Пусть $\pi_i : G \cap A \to (G \cap A)/C_{(G\cap A)}(T_i)$ — канонические проекции. Поскольку $G/(G \cap A)$ транзитивна, мы получаем, что $(G \cap A)^{\pi_i} = K_iT_i$.

Поскольку $\mathrm{Aut}_{G\cap A}(T_i) = K_iT_i$, то группа $G \cap A$ удовлетворяет **(E)**. По выбору G она содержит картерову подгруппу M. По [2, лемма 3] мы получаем, что M^{π_i} является картеровой подгруппой группы K_iT_i, следовательно, мы можем предполагать $M^{\pi_i} = K_i$. В частности, если $R = (K_1 \cap T_1) \times \ldots \times (K_k \cap T_k)$, то $M \leq N_G(R)$. Ввиду [3] картеровы подгруппы в любой конечной группе сопряжены. Поскольку $(G \cap A)/H$ нильпотентна, мы получаем, что $G \cap A = MH$, значит, $G = N_G(M)H$. Более того, $N_G(M) \cap A = M$, значит, $N_G(M)$ разрешима. Поскольку M нормализует R и $M^{\pi_i} = K_i$, мы получаем, что $N_G(M)$ нормализует R, значит, $N_G(M)R$ разрешима. Следовательно, она содержит картерову подгруппу K. По лемме 3 (если в ней $T = R$) $(K \cap A)^{\pi_i}$ есть картерова подгруппа группы $(N_G(M)R \cap A)^{\pi_i}$, поэтому $(K \cap A)^{\pi_i} = K_i$. Предположим, что $x \in N_G(K) \setminus K$. Поскольку $G/H = N_G(M)H/H = KH/H$, то $x \in H$. Следовательно, $x^{\pi_i} \in (N_G(K) \cap A)^{\pi_i} \leq N_{T_i}((K \cap A)^{\pi_i}) = K_i$. Поскольку $\bigcap_i \mathrm{Ker}(\pi_i) = \{e\}$, то $x \in R \leq N_G(M)R$. Но K есть картерова подгруппа группы $N_G(M)R$, значит, $x \in K$. Это противоречие завершает доказательство. $\square$

2. Пример

В данном параграфе мы построим пример, показывающий, что мы не можем заменить условие **(E)** более слабым условием: $\mathrm{Aut}_G(S)$ содержит картерову подгруппу для каждого композиционного фактора S группы G. Этот пример показывает также, что расширение группы с картеровой подгруппой при помощи группы, содержащей картерову подгруппу, может не иметь картеровой подгруппы.

Рассмотрим $L = \Gamma SL_2(3^3) = PSL_2(3^3) \leftthreetimes \langle\varphi\rangle$, где φ — полевой автоморфизм группы $PSL_2(3^3)$. Пусть $X = (L_1 \times L_2) \leftthreetimes \mathrm{Sym}_2$, где $L_1 \simeq L_2 \simeq L$ и, если $\sigma = (1, 2) \in \mathrm{Sym}_2 \setminus \{e\}$, $(x, y) \in L_1 \times L_2$, то $\sigma(x, y)\sigma = (y, x)$ (подстановочное сплетение группы L и Sym_2). Обозначим через $H = PSL_2(3^3) \times PSL_2(3^3)$ минимальную нормальную подгруппу группы X и через M прямое произведение $L_1 \times L_2$. Пусть $G = (H \leftthreetimes \langle(\varphi, \varphi^{-1})\rangle) \leftthreetimes \mathrm{Sym}_2$ — подгруппа группы X. Тогда справедливы следующие утверждения:

1. Для любого композиционного фактора S группы G группа $\mathrm{Aut}_G(S)$ содержит картерову подгруппу.

2. Подгруппа $G \cap M$ нормальна в G и содержит картерову подгруппу.

3. $G/(G \cap M)$ — нильпотентная группа.

4. G не содержит картеровых подгрупп.

Докажем эти утверждения.

1. Очевидно, нам нужно проверить утверждение лишь для неабелевых композиционных факторов. Любой неабелев композиционный фактор S группы G изоморфен $PSL_2(3^3)$ и $\mathrm{Aut}_G(S) = L$. Ввиду [3, теорема 7.1] (теорема 3 ниже) мы получаем, что L содержит картерову подгруппу (совпадающую с силовской 3-подгруппой).

2. Поскольку группа $(G \cap M)/H$ нильпотентна, из утверждения 1 мы получаем, что $G \cap M$ удовлетворяет **(E)** и поэтому содержит картерову подгруппу (легко убедиться, что силовская 3-подгруппа группы $G \cap M$ является картеровой подгруппой группы $G \cap M$).

3. Очевидно.

4. Предположим, что K является картеровой подгруппой группы G. Тогда KH/H является картеровой подгруппой группы G/H. Но G/H есть неабелева группа порядка 6, значит, $G/H \simeq \mathrm{Sym}_3$ и KH/H есть силовская 2-подгруппа группы G/H. Из [2, лемма 3] следует, что $\mathrm{Aut}_K(PSL_2(3^3))$ является картеровой подгруппой группы $\mathrm{Aut}_{KH}(PSL_2(3^3)) = PSL_2(3^3)$. Но $PSL_2(3^3)$ не содержит картеровых подгрупп ввиду [3, теорема 7.1] (теорема 3 ниже).

3. Классификация картеровых подгрупп

В [3, лемма 2.5] доказано, что картерова подгруппа конечной группы G содержит силовскую 2-подгруппу S группы G в том и только в том случае, если $N_G(S) = SC_G(S)$. Будем говорить, что конечная группа G удовлетворяет условию **(ESyl2)**, если для ее силовской 2-подгруппы S выполнено условие $N_G(S) = SC_G(S)$. Для удобства читателя приведем здесь основные классификационные теоремы из [3].

Теорема 2 ([3, теорема 6.1]). *Пусть G — конечная присоединенная группа лиева типа над полем характеристики p, а $\overline{G}$ и σ выбраны так, что $O^{p'}(\overline{G}_\sigma) \leq G \leq \overline{G}_\sigma$ и группа $O^{p'}(G)$ изоморфна $D_4(q)$ или ${}^3D_4(q^3)$. Предположим, что τ — графовый автоморфизм порядка 3 группы $O^{p'}(G)$ (напомним, что для группы $G \simeq {}^3D_4(q^3)$ автоморфизм τ — это такой автоморфизм, множество неподвижных точек которого изоморфно $G_2(q)$). Обозначим через A_1 подгруппу группы $\mathrm{Aut}(D_4(q))$, порожденную внутренне-диагональными и полевыми автоморфизмами, а также графовым автоморфизмом порядка 2. Пусть подгруппа $A \leq \mathrm{Aut}(O^{p'}(G))$ такова, что $A \not\leq A_1$ (если $O^{p'}(G) \simeq D_4(q)$), и K — картерова подгруппа группы A. Предположим также, что $G = A \cap \overline{G}_\sigma$ и $A = KG$. Тогда справедливо одно из следующих утверждений:*

(а) *$G \simeq {}^3D_4(q^3)$, $(|A : G|, 3) = 1$, q нечетно и K содержит силовскую 2-подгруппу группы A;*

(б) *$(|A : G|, 3) = 3$, q нечетно, $\tau \in A$ и, с точностью до сопряжения элементом из G, подгруппа K содержит силовскую 2-подгруппу группы $C_A(\tau) \in \Gamma G_2(q)$, и $\tau \in K$;*

(в) *$(|A : G|, 3) = 3$, $q = 2^t$, $|A : G| = 3t$, $A = G \leftthreetimes \langle \tau, \varphi \rangle$, где φ — полевой автоморфизм порядка t, перестановочный с τ и, с точностью до сопряжения элементом из G, подгруппа K содержит силовскую 2-подгруппу группы $C_G(\langle \tau, \varphi \rangle_{2'}) \simeq G_2(2^{t_{2'}})$, и $\tau \in K$;*

(г) *$O^{p'}(G) \simeq D_4(p^{3t})$, p нечетно, факторгруппа A/G циклическая, $\tau \notin A$, $A = G \leftthreetimes \langle \zeta \rangle$, где, для некоторого натурального m, $\zeta = \tau\varphi^m$ является графово-полевым автоморфизмом, и, с точностью до сопряжения элементом из G, $K = Q \leftthreetimes \langle \zeta \rangle$, где Q является силовской 2-подгруппой группы $C_G(\zeta_{2'}) \simeq {}^3D_4(p^{3t/|\zeta_{2'}|})$.*

В частности, картеровы подгруппы группы A сопряжены.

Теорема 3 ([3, теорема 7.1]). *Пусть G — конечная присоединенная группа лиева типа (G не обязательно простая) над полем характеристики p, а $\overline{G}$ и σ выбраны так, что $O^{p'}(\overline{G}_\sigma) \leq G \leq \overline{G}_\sigma$. Предположим также, что $G \not\simeq {}^3D_4(q^3)$. Выберем подгруппу A группы $\mathrm{Aut}(O^{p'}(\overline{G}_\sigma))$, для которой выполнено равенство $A \cap \overline{G}_\sigma = G$, и, если $O^{p'}(G) = D_4(q)$, предположим, что A содержится в подгруппе A_1, определенной в формулировке теоремы 2. Пусть K — картерова подгруппа группы A и $A = KG$.*

Тогда выполнено в точности одно из следующих утверждений:

(а) *G определена над полем характеристики 2, $A = \langle G, \zeta g, t\rangle$, где t — 2-элемент, K содержится в нормализаторе некоторой t-инвариантной подгруппы Бореля группы G;*

(б) *$G \simeq PSL_2(3^t)$, полевой автоморфизм ζ лежит в A, $|\zeta| = t$ нечетно, и, с точностью до сопряжения в G, выполнено равенство $K = Q \leftthreetimes \langle\zeta\rangle$, где Q является силовской 3-подгруппой группы $G_{\zeta_{3'}}$;*

(в) *$A = {}^2G_2(3^{2n+1}) \leftthreetimes \langle\zeta\rangle$, $|\zeta| = 2n+1$ и с точностью до сопряжения в G выполнено равенство $K = (K \cap G) \leftthreetimes \langle\zeta\rangle$ и $K \cap {}^2G_2(3^{2n+1}) = Q \times P$, где Q порядка 2 и $|P| = 3^{|\zeta|_3}$;*

(г) *p не делит $|K \cap G|$ и K содержит силовскую 2-подгруппу группы A.*

В частности, картеровы подгруппы группы A сопряжены.

Приведем также следующие две технические леммы, которые будут использоваться при классификации картеровых подгрупп в почти простых группах.

Лемма 4 ([2, лемма 5]). *Пусть K — картерова подгруппа конечной группы G с центром $Z(K)$. Предположим также, что $e \neq z \in Z(K)$ и $C_G(z)$ удовлетворяет условию* **(C)**. *Тогда справедливы следующие утверждения:*

(1) *Любая подгруппа Y, содержащая K и удовлетворяющая условию* **(C)**, *самонормализуема в G.*

(2) *Никакой элемент, сопряженный с z в G, кроме z, не лежит в $Z(G)$.*

(3) *Если H — картерова подгруппа группы G, не сопряженная с K, то z не сопряжен ни с каким элементом из центра группы H.*

В частности, централизатор $C_G(z)$ самонормализуем в G, и z не сопряжен ни с какой степенью $z^k \neq z$.

Лемма 5 ([3, лемма 2.9]). *Пусть G — конечная группа, H — такая подгруппа группы G, что $|G : H| = 2^t$ и любой элемент нечетного порядка группы G лежит в H. Тогда если H удовлетворяет условию* **(ESyl2)**, *то и G ему удовлетворяет.*

Ввиду условия **(E)** и теоремы 1 изучение картеровых подгрупп в конечных группах сводится к классификации картеровых подгрупп в почти простых группах A, удовлетворяющих дополнительному условию, что группа $A/F^*(A)$ нильпотентна. Классификация картеровых подгрупп в группах, удовлетворяющих такому условию, получена ранее различными авторами, и мы приведем ее здесь в форме, удобной для использования.

Докажем сначала следующую теорему, которая показывает, что если в некоторой подгруппе S группы $\mathrm{Aut}(G)$ существует картерова подгруппа, то она существует и в любой бóльшей подгруппе A ($S \leq A \leq \mathrm{Aut}(G)$, здесь G — известная конечная простая группа).

Теорема 4. *Пусть G — конечная простая группа, удовлетворяющая условию* **(C)**, *и A — почти простая группа с цоколем G. Предположим, что A содержит такую подгруппу S, что $G \leq S$ и S содержит картерову подгруппу. Тогда A содержит картерову подгруппу.*

Доказательство. Пусть K — картерова подгруппа группы S. Очевидно, можно считать, что $S = KG$, а $A \neq S$.

Предположим, что либо $G \simeq \mathrm{Alt}_n$ для некоторого $n \geqslant 5$, либо G является спорадической. Поскольку по [5, лемма 2.10] любой элемент нечетного простого порядка группы G сопряжен со своей нетривиальной степенью и поскольку $|\mathrm{Aut}(G) : G|$ является степенью двойки, из лемм 4 и 5 вытекает, что если некоторая группа S, $G \leq S \leq \mathrm{Aut}(G)$, содержит картерову подгруппу K, то K совпадает с силовской 2-подгруппой группы S. Так как $|A : S|$ является степенью двойки, утверждение теоремы в этом случае следует из леммы 5.

Предположим, что $G = {}^3D_4(q^3)$. По [6, теорема 1.2 (vi)] каждый элемент группы G сопряжен со своим обратным. Если q нечетно, то по [3, лемма 4.3] K является силовской 2-подгруппой группы S. Поэтому из леммы 5 и [3, лемма 4.3] следует, что A удовлетворяет условию **(ESyl2)** и поэтому содержит картерову подгруппу. Если q четно, то из теорем 2 и 3 следует, что либо $|\mathrm{Aut}(G) : S| = 3$ и всякая картерова подгруппа группы S является картеровой подгруппой группы A, либо $|\mathrm{Aut}(G) : S| = 2$ и (в силу $A \neq S$) A содержит такую подгруппу M индекса 3, для которой выполняется утверждение (а) теоремы 3 (при $G = M$) и картерова подгруппа группы M является картеровой подгруппой группы A.

Предположим, что G является группой лиева типа, $G \not\simeq {}^3D_4(q^3)$ и, если $G \simeq D_4(q)$, то $S \leq A_1$, где подгруппа $A_1 \leq \mathrm{Aut}(D_4(q))$ определена в теореме 2.

Тогда для $G = S$ выполняется одно из утверждений (а)–(г) теоремы 3. Рассмотрим все эти случаи по отдельности.

Предположим, что для S выполняется утверждение (а). В этом случае $|\mathrm{Aut}(G) : S| \leq 2$ и поэтому для любой группы A такой, что $S \leq A \leq \mathrm{Aut}(G)$, имеем (в силу $A \neq S$) $A = \mathrm{Aut}(G)$. Тогда выполняется утверждение (а) теоремы 3 (при $G = A$) и A содержит картерову подгруппу.

Предположим, что для S выполняется утверждение (б). Тогда $|\mathrm{Aut}(G) : S| = 2$ и $A = \mathrm{Aut}(G)$, а группа $\widehat{G} = \mathbf{P}GL_2(3^t)$ удовлетворяет условию **(ESyl2)**, значит, по [3, лемма 4.3] группа A также удовлетворяет условию **(ESyl2)** и по [3, лемма 2.5] содержит картерову подгруппу.

Предположим, что для S выполняется утверждение (в) теоремы 3. Тогда $S = \mathrm{Aut}(G) = A$, противоречие.

Предположим, что для S выполняется утверждение (г) теоремы 3. По [3, лемма 3.6] группа $S \cap \widehat{G}$ удовлетворяет условию **(ESyl2)**. По [3, лемма 4.5] любая подгруппа A группы $\mathrm{Aut}(G)$, содержащая $S \cap \widehat{G}$, также удовлетворяет условию **(ESyl2)**, значит, по [3, лемма 2.5] содержит картерову подгруппу.

Предположим теперь, что $G = D_4(q)$ и теорема 2 выполняется для $G = S$. Поскольку графовые автоморфизмы порядка 2 и 3 не коммутируют, лишь один из них может содержаться в нильпотентной подгруппе. Таким образом, мы можем предполагать, что лишь один из них содержится в A. Тогда для любой подгруппы A, содержащей S, выполняется либо теорема 2, либо теорема 3 (а), если q четно, либо теорема 3 (г), если q нечетно, т. е. A содержит картерову подгруппу. □

Таблицы, приведенные ниже, устроены следующим образом. В первом столбце указана простая группа S, в группе A автоморфизмов которой ($S \leq A \leq \mathrm{Aut}(S)$) классифицируются картеровы подгруппы. Во втором столбце приведены условия на подгруппу A группы $\mathrm{Aut}(S)$, при которых A содержит картерову подгруппу. В третьем столбце приведено строение картеровой подгруппы K. Для всех подгрупп, лежащих между S и A, картеровы подгруппы не существуют. Через $P_r(G)$ обозначена силовская r-подгруппа группы G. Через φ обозначен полевой автоморфизм группы лиева типа S, через τ — графовый автоморфизм максимального порядка группы лиева типа S, содержащийся в K (поскольку графовые автоморфизмы порядка 2 и 3 группы $D_4(q)$ не коммутируют, лишь один из них может содержаться в K). Если A не содержит графовых автоморфизмов, то мы полагаем $\tau = e$. Через ψ обозначен полевой автоморфизм максимального порядка группы S, содержащийся в A (он является степенью φ, но $\langle\psi\rangle$ может не совпадать с $\langle\varphi\rangle$). Если G — разрешимая группа, то через $K(G)$ обозначена картерова подгруппа группы G. В таблице 3 $\chi=\varphi^{|\varphi|_2}$, а через ζ обозначен графово-полевой автоморфизм порядка $2t$ группы $A_2(2^{2t})$. Для проверки условия **(ESyl2)** в почти простой группе мы используем результаты работ [7] и [8].

Т а б л и ц а 1

Группы автоморфизмов знакопеременных групп, содержащие картеровы подгруппы

Группа S	Условия на A	Строение K
Alt_5	$A=\mathrm{Sym}_5$	$K=P_2(\mathrm{Sym}_5)$
Alt_n, $n\geqslant 6$	отсутствуют	$K=N_A(P_2(S))$

Т а б л и ц а 2

Группы автоморфизмов спорадических групп, содержащие картеровы подгруппы

Группа S	Условия на A	Строение K
J_2, J_3, Suz, HN	$A=\mathrm{Aut}(S)$	$K=P_2(A)$
$\not\simeq J_1, J_2, J_3, Suz, HN$	отсутствуют	$K=P_2(A)$

Т а б л и ц а 3

Группы автоморфизмов классических групп, содержащие картеровы подгруппы

Группа S	Условия на A	Строение K
$A_1(q)$, $q\equiv\pm1 \pmod 8$	отсутствуют	$K=N_A(P_2(S))$
$A_1(q)$, $q\equiv\pm3 \pmod 8$	$\widehat{S}\leq A$	$K=N_A(P_2(\widehat{S}))$
$A_n(2^t)$, $t\geq 2$, если $n=1$	$\varphi g\in A$, $g\in\widehat{S}$	$K=\langle\varphi,\tau\rangle\leftthreetimes S_{\varphi_{2'}}$
$A_2(2^{2t})$, $3\nmid t$	$\langle S,\zeta g\rangle\leq A\leq S\rightthreetimes\langle\zeta\rangle$, $C_{A\cap\widehat{S}}(\chi)\simeq PGU_3(2)$	$K=\langle\zeta g\rangle\times K(PGU_3(2))$
$A_n(q)$, q нечетно, $n\geq 2$	отсутствуют	$K=P_2(A)\times K(O(N_A(P_2(A))))$
${}^2A_2(2^{2t})$, t нечетно, $3\nmid t$	$\langle S,\chi g\rangle\leq A\leq\widehat{S}\rightthreetimes\langle\chi\rangle$ $C_{A\cap\widehat{S}}(\chi)\simeq PGU_3(2)$ $C_{A\cap\widehat{S}}(\chi)\simeq PSU_3(2)$	$K=\langle\chi\rangle\times K(PGU_3(2))$ $K=\langle\chi\rangle\times P_2(PSU_3(2))$
${}^2A_2(2^{2t})$	$A=\mathrm{Aut}(S)$	$K=\langle\varphi\rangle\leftthreetimes P_2(S_\chi)$
${}^2A_n(q^2)$, q нечетно	отсутствуют	$K=P_2(A)\times K(O(N_A(P_2(A))))$
${}^2A_n(2^{2t})$, $n\geq 3$	$A=\mathrm{Aut}(S)$	$K=\langle\varphi\rangle\leftthreetimes P_2(S_{\varphi_{2'}})$
$B_2(q)$, $q\equiv\pm1 \pmod 8$	отсутствуют	$K=P_2(A)\times K(O(N_A(P_2(A))))$
$B_2(2^t)$, $t\geq 2$	$\varphi\in A$	$K=\langle\varphi,\tau\rangle\leftthreetimes P_2((S_\tau)_\varphi)$
$B_2(q)$, $q\equiv\pm3 \pmod 8$	$\widehat{S}\leq A$	$K=P_2(A)\times K(O(N_A(P_2(A))))$
$B_n(q)$, q нечетно, $n\geq 3$	отсутствуют	$K=P_2(A)\times K(O(N_A(P_2(A))))$
$C_n(q)$, $q\equiv\pm1 \pmod 8$	отсутствуют	$K=P_2(A)\times K(O(N_A(P_2(A))))$
$C_n(q)$, $q\equiv\pm3 \pmod 8$	$\widehat{S}\leq A$	$K=P_2(A)\times K(O(N_A(P_2(A))))$
$C_n(2^t)$, $n\geq 3$	$A=\mathrm{Aut}(S)$	$K=\langle\varphi\rangle\times P_2(S_{\varphi_{2'}})$

Т а б л и ц а 3 (окончание)

Группа S	Условия на A	Строение K
$D_4(q)$, q нечетно	отсутствуют	если $\|\tau\| \leq 2$, то $K = P_2(A) \times K(O(N_A(P_2(A))))$; если $\|\tau\| = 3$, то $K = \langle \tau, \psi \rangle \leftthreetimes P_2(S_\tau)$
$D_4(2^t)$	$\varphi \in A$	если $\|\tau\| \leq 2$, то $K = \langle \tau, \varphi \rangle \leftthreetimes P_2(S_{\varphi_{2'}})$; если $\|\tau\| = 3$, то $K = \langle \tau, \varphi \rangle \leftthreetimes P_2((S_\tau)_{\varphi_{2'}})$
$D_n(q)$, q нечетно, $n \geq 5$	отсутствуют	$K = P_2(A) \times K(O(N_A(P_2(A))))$
$D_n(2^t)$, $n \geq 5$	$\varphi \in A$	$K = \langle \tau, \varphi \rangle \leftthreetimes P_2(S_{\varphi_{2'}})$
${}^2D_n(q^2)$, q нечетно	отсутствуют	$K = P_2(A) \times K(O(N_A(P_2(A))))$
${}^2D_n(2^{2t})$	$A = \mathrm{Aut}(S)$	$K = \langle \varphi \rangle \leftthreetimes P_2(S_{\varphi_{2'}})$

Т а б л и ц а 4

Группы автоморфизмов исключительных групп лиева типа, содержащие картеровы подгруппы

Группа S	Условия на A	Строение K
${}^2B_2(2^{2n+1})$, $n \geqslant 1$	$A = \mathrm{Aut}(S)$	$K = \langle \varphi \rangle \times P_2({}^2B_2(2))$
$({}^2F_4(2))'$	отсутствуют	$K = P_2(A)$
${}^2F_4(2^{2n+1})$, $n \geqslant 1$	$A = \mathrm{Aut}(S)$	$K = \langle \varphi \rangle \times P_2({}^2F_4(2))$
${}^2G_3(3^{2n+1})$	$A = \mathrm{Aut}(G)$	$\langle \varphi \rangle \leftthreetimes (2 \times P)$, где $\|P\| = 3^{\|\varphi\|_3}$
остальные, q нечетно	отсутствуют	$K = P_2(A) \times K(O(N_A(P_2(A))))$
остальные, $q = 2^t$	$\varphi \in A$	$\langle \tau, \varphi \rangle \leftthreetimes P_2(S_{\varphi_{2'}})$

В качестве следствия из таблиц отметим следующий интересный результат.

Лемма 6. *Пусть S — известная конечная простая группа, $S \not\simeq J_1$ и $G = \mathrm{Aut}(S)$. Тогда группа G содержит картерову подгруппу.*

Д о к а з а т е л ь с т в о. Если S не является группой лиева типа и отлична от J_1, то ввиду [7, теоремы 2 и 3] группа ее автоморфизмов $\mathrm{Aut}(S)$ удовлетворяет **(ESyl2)** и содержит картерову подгруппу. Далее, если S — группа лиева типа над полем четной характеристики, то $\mathrm{Aut}(S)$ содержит картерову подгруппу ввиду теоремы 3 (2). Если S — группа лиева типа над полем нечетной характеристики и $S \not\simeq {}^2G_2(3^{2n+1})$, то $\widehat{S}$ удовлетворяет **(ESyl2)**, следовательно, содержит картерову подгруппу. По теореме 4 группа $\mathrm{Aut}(S)$ содержит картерову подгруппу. Наконец, если $S \simeq {}^2G_2(3^{2n+1})$, то $\mathrm{Aut}(S)$ содержит картерову подгруппу ввиду теоремы 3, утверждение (4). $\square$

Автор выражает благодарность Виктору Даниловичу Мазурову за обсуждение статьи, которое позволило существенно улучшить первоначальный вариант.

Поступила 08.06.2006

СПИСОК ЛИТЕРАТУРЫ

1. **Carter R.W.** Nilpotent self-normalizing subgroups of soluble groups // Math. Z. 1961. T. 75. C. 136–139.
2. **Вдовин Е.П.** О проблеме сопряженности для картеровых подгрупп // Сиб. мат. журн. 2006. Т. 47, № 4. С. 725–730.
3. **Вдовин Е.П.** Картеровы подгруппы в конечных почти простых группах // Алгебра и логика. 2007. Т. 46, № 3. С. 260–314.
4. **Каргаполов М.И., Мерзляков Ю.И.** Основы теории групп. М.: Наука, Физматлит, 1996.
5. **Tamburini M.C., Vdovin E.P.** Carter subgroups of finite groups // J. Algebra. 2002. V. 255, no 1. C. 148–163.
6. **Tiep P.H., Zalesski A.E.** Real conjugacy classes in algebraic groups and finite groups of Lie type // J. Group Theory. 2005. V. 8, no 3. C 291–315.
7. **Кондратьев А.С.** Нормализаторы силовских 2-подгрупп в конечных простых группах // Мат. заметки. 2005. Т. 78, № 3. С. 368–376.
8. **Кондратьев А.С., Мазуров В.Д.** 2-сигнализаторы конечных простых групп // Алгебра и логика. 2003. Т. 42, № 5. С. 594–623.

ТРУДЫ ИНСТИТУТА МАТЕМАТИКИ И МЕХАНИКИ УрО РАН

Том 13 № 1 2007

УДК 512.542

О ПОРЯДКАХ ЭЛЕМЕНТОВ В НАКРЫТИЯХ ПРОСТЫХ ГРУПП $L_n(q)$ И $U_n(q)$[1]

А. В. Заварницин, В. Д. Мазуров

Мы доказываем, что если конечная простая линейная или унитарная группа, определенная над полем характеристики p и имеющая достаточно большую размерность по сравнению с p, действует на конечномерном векторном пространстве над некоторым полем той же характеристики p, то соответствующее полупрямое произведение содержит элемент, порядок которого отличен от всех порядков элементов исходной простой группы.

Введение

Спектром $\omega(G)$ конечной группы G называется множество порядков ее элементов. Поведение спектра при расширениях групп является популярным предметом изучения. Так, в классической работе Холла и Хигмена [1] рассматриваются порядки p-элементов в накрытии G некоторой p-разрешимой группы $H = G/N$ в случае, когда N — элементарная абелева p-группа и H действует точно на N при сопряжении в G. В последние годы широко изучается проблема распознаваемости групп по спектру. Напомним, что конечная группа G называется *распознаваемой* (по спектру), если для любой конечной группы H равенство $\omega(G) = \omega(H)$ влечет за собой изоморфизм $G \cong H$. Очевидно, что любая распознаваемая группа G должна удовлетворять следующему свойству

$$(*) \qquad \omega(H) \neq \omega(G) \text{ для любого собственного накрытия } H \text{ группы } G,$$

где под собственным накрытием G мы понимаем группу H с такой нетривиальной нормальной подгруппой N, что $H/N \cong G$. Хотя свойство $(*)$ слабее распознаваемости, его проверка для некоторых групп может быть очень трудоемкой. В работе [3] было показано, что все конечные неразрешимые симметрические и знакопеременные группы удовлетворяют свойству $(*)$. Достаточно проверять свойство $(*)$ в случае, когда H — расщепляемое расширение элементарной абелевой p-группы N с помощью G, причем G действует неприводимо на N. Для группы G, изоморфной простой группе $\mathrm{PSL}_3(q)$, в единственном известном доказательстве [4] свойства $(*)$ используется явное описание неприводимых эквихарактеристических модулей для G. В этой работе мы рассматриваем аналогичную проблему для групп $L_n^\varepsilon(q)$, где $\varepsilon \in \{+,-\}$ и $L_n^+(q) = \mathrm{PSL}_n(q)$, $L_n^-(q) = \mathrm{PSU}_n(q)$. Группы из следующего списка будем называть исключительными:

$$\begin{gathered} L_5^\varepsilon(2^m), L_6^\varepsilon(3^m), L_7^\varepsilon(3^m), L_{10}^\varepsilon(3^m), L_{11}^\varepsilon(5^m), L_{18}^\varepsilon(5^m), \text{ где } \varepsilon \in \{+,-\}, m \geqslant 1; \\ U_6(2), U_7(2), U_9(2), U_{10}(2), U_{11}(2), U_{18}(2), U_5(3), U_8(3), U_{11}(3). \end{gathered} \tag{1}$$

Теорема 1. *Пусть $\varepsilon \in \{+,-\}$ и $L = L_n^\varepsilon(q)$ — простая группа, где $q = p^m$. Предположим, что $n \geqslant p$, $n \neq p+1$ и L не является исключительной. Если L действует на векторном пространстве W над полем характеристики p, то $\omega(WL) \neq \omega(L)$, где WL — естественное полупрямое произведение W на L.*

[1]Работа выполнена при финансовой поддержке РФФИ (проект 05-01-00797) и Сибирского отделения Российской академии наук (грант 29 для молодых ученых и интеграционный проект 2006.1.2).

Из этой теоремы вместе с результатами из [5] следует, что группы $L_n^+(q)$, где $q = p^m$, удовлетворяют $(*)$, если n достаточно велико по сравнению с p. Отметим, что вопрос о справедливости свойства $(*)$ для всех групп $L_n(q)$ при $n \geqslant 3$ включен в “Коуровскую тетрадь” [10, Проблема 14.60]. Другим следствием нашего результата является подтверждение следующей гипотезы из [9].

Следствие 1. *Проективные специальные линейные группы $L_n(2)$ распознаваемы по спектру для всех $n \geqslant 3$.*

Доказательство. Допустим противное: для некоторой группы $G = L_n(2)$, где $n \geqslant 3$, найдется группа H наименьшего порядка такая, что $\omega(H) = \omega(G)$, но $H \ncong G$. Тогда из предложения 1 в [9] следует, что пара (G, H) — контрпример к свойству $(*)$, причем $H \cong NG$, где N — элементарная абелева 2-группа. Из теоремы 1 вытекает, что $n = 3$ или 5. Однако группы $L_3(2)$ и $L_5(2)$ распознаваемы по спектру [7, 8]. Противоречие. □

1. Предварительные результаты

На протяжении работы $\mathbb{Z}_m$ будет обозначать циклическую группу порядка m и $\mathbb{F}_q$ — конечное поле из q элементов. Если $\alpha \in \mathbb{F}_{q^2}$, то положим $\overline{\alpha} = \alpha^q$. Если V — невырожденное унитарное векторное пространство, то ортогональное разложение $V = V_1 \oplus V_2$ называется *невырожденным*, если V_1 и V_2 — невырожденные подпространства в V. Обозначим $\mathrm{SL}_n^-(q) = \mathrm{SU}_n(q)$ и $\mathrm{SL}_n^+(q) = \mathrm{SL}_n(q)$. Аналогичное соглашение касается проективных групп $L_n^\varepsilon(q) = \mathrm{PSL}_n^\varepsilon(q)$, где $\varepsilon \in \{+,-\}$. Если $\varepsilon = +$, то пусть V — векторное пространство над $F = \mathbb{F}_q$, а если $\varepsilon = -$, то пусть V — невырожденное унитарное векторное пространство над $F = \mathbb{F}_{q^2}$. Предположим, что $n = \dim V > 1$, и пусть $\{e_1, \ldots, e_n\}$ — (ортонормированный) базис пространства V. Если $V = V_1 \oplus V_2$ — (невырожденное ортогональное) разложение, то мы обозначим через $\mathrm{SL}^\varepsilon(V_1, V_2)$ подгруппу в $\mathrm{SL}^\varepsilon(V)$, которая стабилизирует V_1 и централизует V_2.

Лемма 1. *Пусть V — естественный n-мерный FH-модуль для группы $H = \mathrm{SL}_n^\varepsilon(q)$, где $q = p^m$. Предположим, что $V = V_1 \oplus V_2$ — (невырожденное ортогональное) разложение и K — циклическая подгруппа в $\mathrm{SL}^\varepsilon(V_1, V_2)$ порядка, взаимно простого с p. Если $\dim V_2 \geqslant (n-1)/2$, то K оставляет неподвижным некоторый ненулевой вектор в любом RH-модуле, где R — поле характеристики p.*

Доказательство. См. [15]. □

Если $1 \leqslant i \neq j \leqslant n$, то пусть $W_{ij} = \langle e_i, e_j \rangle_F$, а W'_{ij} — подпространство, порожденное всеми e_k при $k \neq i, j$. Обозначим $S_{ij} = \mathrm{SL}^\varepsilon(W_{ij}, W'_{ij}) \cong \mathrm{SL}_2^\varepsilon(q)$. Аналогично определим $S_{123} \cong \mathrm{SL}_3^\varepsilon(q)$, если $n \geqslant 3$.

Лемма 2. *Группа $\mathrm{SL}^\varepsilon(V)$ порождается своими подгруппами S_{12}, S_{23}, ..., $S_{n-1,n}$ за исключением случая $(\varepsilon, q) = (-, 2)$ и $n > 2$, в котором $\mathrm{SL}^-(V)$ порождается подгруппами S_{123}, S_{34}, S_{45}, ..., $S_{n-1,n}$.*

Доказательство. Если $\varepsilon = +$, то хорошо известно, что $\mathrm{SL}^+(V)$ порождается трансвекциями $t_{ij}(a)$ при $1 \leqslant i \neq j \leqslant n$ и $a \in F$ (это можно доказать, используя метод Гаусса). Из формулы $[t_{ij}(a), t_{jk}(b)] = t_{ik}(ab)$ при различных i, j, k следует, что $\mathrm{SL}^+(V)$ на самом деле порождается с помощью $t_{i,i+1}(a)$ и $t_{i+1,i}(a)$ при $1 \leqslant i < n$ и $a \in F$. Поскольку $S_{i,i+1} = \langle t_{i,i+1}(a), t_{i+1,i}(a) \mid a \in F \rangle$, то получаем требуемое.

Унитарный аналог этого факта не столь хорошо известен. Некоторая растянутость следующего рассуждения компенсируется тем, что мы реально описываем алгоритм разложения элемента из $\mathrm{SL}^-(V)$ в произведение элементов порождающих подгрупп $S_{i,i+1}$ и, возможно,

S_{123}. Пусть $\varepsilon = -$. Можно считать, что $n > 2$. Обозначим $S = \mathrm{SL}^-(V)$. Заметим, что любой элемент $s \in S_{ij}$ в базисе $\{e_i, e_j\}$ имеет матрицу

$$\begin{pmatrix} \chi & -\overline{\eta} \\ \eta & \overline{\chi} \end{pmatrix} \tag{2}$$

для некоторых $\chi, \eta \in F$, удовлетворяющих условию $\chi\overline{\chi} + \eta\overline{\eta} = 1$. Достаточно показать, что S порождается подгруппами S_{ij} при $i \neq j$ (и дополнительно подгруппой S_{123} при $q = 2$). В самом деле, если $j > i+1$, то $S_{ij}^{u_{i,i+1}} = S_{i+1,j}$, где матрица элемента $u_{kl} \in S_{kl}$ в базисе $\{e_k, e_l\}$ равна

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}. \tag{3}$$

Поэтому $S_{ij} \leqslant \langle S_{i,i+1}, \dots, S_{j-1,j} \rangle$.

Выберем $a \in S$. Достаточно показать, что умножением a справа на подходящий элемент из S_{ij} (из S_{123} при $q = 2$) можно получить элемент b, централизующий e_1. В самом деле, в таком случае b будет стабилизировать $\langle e_1 \rangle^{\perp}$, и мы сможем применить индукцию по размерности при $q > 2$. Если же $q = 2$, то, сопрягая b с помощью $u_{1,n}$, получим элемент, централизующий e_n, и также применим индукцию.

Пусть (a_{ij}) — матрица элемента a в базисе $\{e_1, \dots, e_n\}$. Пусть r — число ненулевых элементов в первой строке $[a_{11}, \dots, a_{1n}]$ матрицы (a_{ij}). Тогда $1 \leqslant r \leqslant n$. Дальше применяем индукцию по r. Можно считать (умножая, если необходимо, на подходящий элемент $u_{ij} \in S_{ij}$, определенный выше), что $a_{11}, \dots, a_{1r}$ отличны от нуля и $a_{1,r+1} = \ldots = a_{1n} = 0$. Если $r = 1$, то $a_{11}\overline{a_{11}} = 1$ и, умножая a на элемент $s \in S_{12}$, матрица которого в базисе $\{e_1, e_2\}$ равна

$$\begin{pmatrix} a_{11}^{-1} & 0 \\ 0 & (\overline{a_{11}})^{-1} \end{pmatrix}, \tag{4}$$

мы приведем a к требуемому виду. Предположим, что $r \geqslant 2$. Если для некоторого j, $1 < j \leqslant r$, имеет место $a_{11}\overline{a_{11}} + a_{1j}\overline{a_{1j}} = c \neq 0$, то существует такое $\sigma \in F\backslash\{0\}$, что $\sigma\overline{\sigma} = c$, и мы положим $\chi = \overline{a_{11}}/\sigma$, $\eta = \overline{a_{1j}}/\sigma$. Тогда $\chi\overline{\chi} + \eta\overline{\eta} = 1$. Пусть s — элемент из S_{1j}, имеющий матрицу (2) в базисе $\{e_1, e_j\}$. Тогда для матрицы элемента $b = as$ имеем $b_{11} = a_{11}\chi + a_{1j}\eta \neq 0$, $b_{1j} = -a_{11}\overline{\eta} + a_{1j}\overline{\chi} = 0$, и индукцией по r получаем требуемое.

Следовательно, можно считать, что $a_{1j}\overline{a_{1j}} = -a_{11}\overline{a_{11}} = \nu$ при $1 < j \leqslant r$. Заметим, что это влечет за собой $r \geqslant 3$, поскольку в случае $r = 2$ получилось бы $a_{11}\overline{a_{11}} + a_{12}\overline{a_{12}} = 1$ ввиду унитарности a, противоречие. Если мы найдем такое $s \in S_{23}$, что элемент b_{12} матрицы $b = as$ удовлетворяет неравенству $b_{12}\overline{b_{12}} \neq \nu$, то по предыдущему рассуждению мы сможем уменьшить r и использовать индукцию.

Если $q > 2$, то существуют такие ненулевые $\chi, \eta \in F$, что $\chi\overline{\chi} + \eta\overline{\eta} = 1$. Положим $\tau = a_{12}/a_{13}$. Если соотношение

$$\tau\chi\overline{\eta} + \overline{\tau\chi}\eta \neq 0 \tag{5}$$

не выполнено, то мы заменим χ на $\chi\mu$, где $\mu \in F$ удовлетворяет соотношениям $\mu\overline{\mu} = 1$ и $\mu \neq \pm 1$ (такое μ всегда найдется). Тогда $\chi\overline{\chi} + \eta\overline{\eta} = 1$ и выполнено (5), поскольку в противном случае мы получили бы $\mu = \overline{\mu}$, то есть $\mu^2 = 1$, противоречие. Теперь пусть $s \in S_{23}$ имеет матрицу (2) в базисе $\{e_1, e_j\}$. Тогда

$$b_{12}\overline{b_{12}} = (a_{12}\chi + a_{13}\eta)(\overline{a_{12}\chi} + \overline{a_{13}\eta}) = \nu + a_{12}\overline{a_{13}}\chi\overline{\eta} + \overline{a_{12}}a_{13}\overline{\chi}\eta \neq \nu$$

ввиду (5), что и требовалось.

Пусть, наконец, $q = 2$. Тогда рассматриваемый выше элемент s не всегда существует в S_{23}. В этом случае найдется элемент $s \in S_{123}$, который аннулирует элементы a_{12} и a_{13}. Из унитарности a имеем $1 = a_{11}\overline{a_{11}} + \ldots + a_{1r}\overline{a_{1r}} = r\nu$, откуда следует, что r нечетно и $\nu = 1$. В частности, норма элемента $v = a_{11}e_1 + a_{12}e_2 + a_{13}e_3$ равна 1. Поскольку S_{123} действует транзитивно на векторах из $\langle e_1, e_2, e_3\rangle$ с нормой 1 (см. лемму 2.10.5 в [11]), то существует такое $s \in S_{123}$, что $vs = e_1$. Лемма доказана. $\square$

Отметим, что при $\varepsilon = -$, $q = 2$ и $n > 2$ группы S_{ij} мономиальны в базисе $\{e_1, \ldots, e_n\}$ и порождают (собственную) мономиальную подгруппу в $\mathrm{SL}^-(V)$.

Лемма 3. *Пусть $V = U \oplus C$ — такое (невырожденное ортогональное) разложение пространства V, определенного выше, что $\dim C > \dim U$. Если $(\varepsilon, q, \dim V, \dim U) \neq (-, 2, 3, 1)$, то*

$$\mathrm{SL}^\varepsilon(V) = \big\langle\, \mathrm{SL}^\varepsilon(U_0, C_0) \;\mid\; U_0 > U,\; C_0 < C,\; \dim U_0 = \dim C,\; V = U_0 \oplus C_0 \big\rangle, \tag{6}$$

где разложение $V = U_0 \oplus C_0$ предполагается невырожденным и ортогональным в случае $\varepsilon = -$.

Доказательство. Пусть $u = \dim U$, $c = \dim C$. Можем считать, что $u \geqslant 1$. Тогда $c \geqslant 2$. Выберем (ортонормированные) базисы $\{e_1, \ldots, e_u\}$ для U и $\{e_{u+1}, \ldots, e_n\}$ для C. Обозначим через S правую часть равенства (6). Сначала покажем, что $S_{i,i+1} \leqslant S$ при $1 \leqslant i < n$, где S_{ij} определены так же, как перед леммой 2 по отношению к (ортонормированному) базису $\{e_1, \ldots, e_n\}$ пространства V. Заметим, что $S_{1j} \leqslant S$ для любого $j > 1$. В самом деле, поскольку $u \leqslant c - 1$, то можно положить $U_0 = \langle e_1, \ldots, e_c\rangle_F$, если $j \leqslant c$, и $U_0 = \langle e_1, \ldots, e_{c-1}, e_j\rangle_F$, если $j > c$. Тогда, обозначив $C_0 = \langle e_k \,|\, e_k \notin U_0\rangle_F$, получим $S_{1j} \leqslant \mathrm{SL}^\varepsilon(U_0, C_0)$. Из леммы 2 следует, что $S_{i,i+1} \leqslant \langle S_{1i}, S_{1,i+1}\rangle \cong \mathrm{SL}_3^\varepsilon(q)$, тогда $S_{i,i+1} \leqslant S$. Если либо $q > 2$, либо $(\varepsilon, q) = (+, 2)$, то требуемое следует из леммы 2. Если $(\varepsilon, q) = (-, 2)$, то также необходимо показать, что $S_{123} \leqslant S$. Предыдущее рассуждение проходит и тогда, когда либо $u \geqslant 2$, либо $u = 1$ и $c \geqslant 3$. А именно, в этих случаях можно положить $U_0 = \langle e_1, \ldots, e_c\rangle_F$ и $C_0 = \langle e_k \,|\, e_k \notin U_0\rangle_F$. Тогда $S_{123} \leqslant \mathrm{SL}^\varepsilon(U_0, C_0) \leqslant S$. $\square$

Если $\mathrm{SL}^\varepsilon(V) \cong \mathrm{SU}_3(2)$ и $\dim U = 1$, то равенство (6) не имеет места; можно показать, что в этом случае его правая часть является собственной подгруппой в $\mathrm{SU}_3(2)$ порядка 54.

Лемма 4. *Пусть $V = U \oplus C$ — такое (невырожденное ортогональное) разложение определенного выше пространства V, что $\dim C > \dim U$, и $a \in \mathrm{SL}^\varepsilon(U, C)$. Предположим, что $(\varepsilon, q, \dim V, \dim U) \neq (-, 2, 3, 1)$ и группа $\mathrm{SL}^\varepsilon(V)$ так действует на конечной группе или конечномерном пространстве G, что $\mathrm{SL}^\varepsilon(V)$ не централизует $C_G(a)$. Тогда $\mathrm{SL}^\varepsilon(C, U)$ также не централизует $C_G(a)$.*

Доказательство. Рассуждаем от противного. Пусть сначала G — конечная группа. Имеем $C_G(a) \leqslant C_G\big(\mathrm{SL}^\varepsilon(C, U)\big)$. Поскольку элемент a сопряжен в $\mathrm{SL}^\varepsilon(V)$ с элементом $\mathrm{SL}^\varepsilon(C, U)$, то мы получаем $\big|C_G\big(\mathrm{SL}^\varepsilon(C, U)\big)\big| = |C_G(a)|$, и поэтому $C_G\big(\mathrm{SL}^\varepsilon(C, U)\big) = C_G(a)$.

Пусть $U_0 \leqslant V$ — (невырожденное) подпространство размерности $\dim C$ и $U_0 \geqslant U$. Можно выбрать $C_0 \leqslant C$ так, что $V = U_0 \oplus C_0$ — (невырожденное ортогональное) разложение пространства V. Тогда $a \in \mathrm{SL}^\varepsilon(U_0, C_0)$ и $\big|C_G\big(\mathrm{SL}^\varepsilon(U_0, C_0)\big)\big| = \big|C_G\big(\mathrm{SL}^\varepsilon(C, U)\big)\big| = |C_G(a)|$. Следовательно, $C_G\big(\mathrm{SL}^\varepsilon(U_0, C_0)\big) = C_G(a)$. Теперь из леммы 3 следует, что $\mathrm{SL}^\varepsilon(V)$ порождена всевозможными такими подгруппами $\mathrm{SL}^\varepsilon(U_0, C_0)$ и, следовательно, централизует $C_G(a)$, противоречие.

Если G — векторное пространство, то можно применить то же рассуждение с заменой порядка подгруппы из G на размерность подпространства из G. $\square$

Пусть $t > 1$ и n — натуральные числа, а $\varepsilon \in \{+, -\}$. Если существует простое число, делящее $t^n - (\varepsilon 1)^n$ и не делящее $t^i - (\varepsilon 1)^i$ при $1 \leqslant i < n$, то мы обозначим его через $t_{[\varepsilon n]}$ и назовем *примитивным делителем* числа $t^n - (\varepsilon 1)^n$. Примитивный делитель может не существовать или быть не единственным. Следующая лемма обобщает известную теорему Жигмонди [12].

Лемма 5. *Пусть $t, n > 1$ — натуральные числа. Тогда для любого $\varepsilon \in \{+, -\}$ существует примитивный делитель $t_{[\varepsilon n]}$ числа $t^n - (\varepsilon 1)^n$, за исключением следующих случаев.*

(i) $\varepsilon = +$, $n = 6$, $t = 2$;

(ii) $\varepsilon = +$, $n = 2$, $t = 2^l - 1$ *для некоторого* $l \geqslant 2$;
(iii) $\varepsilon = -$, $n = 3$, $t = 2$;
(iv) $\varepsilon = -$, $n = 2$, $t = 2^l + 1$ *для некоторого* $l \geqslant 0$.

Доказательство. Пункты (i) и (ii) составляют утверждение теоремы Жигмонди. Предположим, что $\varepsilon = -$. Будем рассуждать от противного. Если n нечетно, то можно считать, что $n > 1$ и $(n,t) \neq (3,2)$. Можно взять в качестве $t_{[-n]}$ делитель $t_{[2n]}$ (примитивный делитель $t_{[2n]}$, очевидно, существует).

Если $i < n$ четно, то $t_{[-n]} \nmid t^i - (-1)^i$ по определению. Предположим, что $t_{[-n]} \mid t^i + 1$ для некоторого нечетного $i < n$. Тогда $t_{[2n]} = t_{[-n]} \mid t^{2i} - 1$ и $2i < 2n$, противоречие. Отсюда следует пункт (iii).

Следовательно, $n = 2m$ четно. Если m четно, то можно взять в качестве $t_{[-n]}$ делитель $t_{[n]}$, который всегда существует. Тогда $t_{[-n]} \nmid t^i - (-1)^i$ для четных $i < n$ по определению. Предположим, что $t_{[-n]} \mid t^i + 1$ для некоторого нечетного $i < n$. Тогда $t_{[n]} = t_{[-n]} \mid t^{2i} - 1$. С другой стороны $t_{[n]} \mid t^n - 1$. Следовательно, $t_{[n]} \mid t^{(n,2i)} - 1$. Поскольку $(n, 2i) \leqslant n$, то $(n, 2i) = n$ по определению $t_{[n]}$. Но тогда $m \mid i$, что невозможно ввиду четности m и нечетности i.

Если m нечетно и $m > 1$, то можно взять в качестве $t_{[-n]}$ делитель $t_{[m]}$. Если $t_{[-n]} \mid t^i - 1$ для некоторого положительного четного $i < n$, то $n > 2$, $i = 2j$ для некоторого $j < m$, и $t_{[m]} \mid t^{(m,i)} - 1$. Однако $(m, i) = (m, j) \leqslant j < m$, что противоречит определению $t_{[m]}$.

Если $t_{[-n]} \mid t^i + 1$ для некоторого нечетного $i < n$, то $t_{[m]} \mid t^{(m,2i)} - 1$. Однако $(m, 2i) = (m, i) \leqslant m$ и, значит, $(m, i) = m$ ввиду выбора $t_{[m]}$. Поэтому $m \mid i$. Поскольку $n = 2m > i$, то $m = i$ и число $t_{[m]}$ делит как $t^m + 1$, так и $t^m - 1$. Значит, $t_{[m]} = 2$ и t нечетно. Но тогда $m = 1$, поскольку $t_{[m]}$ нечетно при $m > 1$, противоречие.

Пусть, наконец, $n = 2$. Тогда любой нечетный простой делитель числа $t - 1$ может быть примитивным делителем $t_{[-2]}$ числа $t^2 - 1$. Однако, если $t - 1$ есть степень двойки, то $t^2 - 1$, очевидно, не имеет примитивных делителей вида $t_{[-2]}$, откуда следует пункт (iv). $\square$

В следующей лемме мы обобщаем пункт (1) леммы 5 из [13] и исправляем небольшую неточность в приведенном там доказательстве.

Лемма 6. *Пусть n и q такие натуральные числа, что $L_n^\varepsilon(q)$ — простая группа и существует примитивный простой делитель $r = q_{[\varepsilon n]}$ числа $q^n - (\varepsilon 1)^n$. Тогда $L_n^\varepsilon(q)$ содержит подгруппу Фробениуса с ядром порядка r и циклическим дополнением порядка n. Более того, если n нечетно или q четно, то такая подгруппа Фробениуса существует уже в $\mathrm{SL}_n^\varepsilon(q)$.*

Доказательство. Заметим, что r нечетно, поскольку $n > 1$. Пусть $G = \mathrm{SL}(\overline{F})$, где $F = \mathbb{F}_q$ и $\overline{F}$ — алгебраическое замыкание поля F. Определим эндоморфизм Фробениуса σ группы G следующим образом: $\sigma = \big[(a_{ij}) \mapsto (a_{ij}^q)\big]$, если $\varepsilon = +$, и $\sigma = \big[(a_{ij}) \mapsto (a_{ij}^q)^{-T}\big]$, если $\varepsilon = -$. Тогда $C_G(\sigma) \cong \mathrm{SL}_n^\varepsilon(q)$. Обозначим через D диагональную подгруппу в G. Определим

$$w = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \dots & & & & \dots \\ 0 & 0 & 0 & \dots & 1 \\ (-1)^{n-1} & 0 & 0 & \dots & 0 \end{pmatrix} \in G$$

и заметим, что $w^\sigma = w$ и элемент $w_0 = w^n$ равен $(-1)^{n-1}e$, где e — единичный элемент из G. Определим также $\sigma_w = \sigma \circ c_w^{-1}$, где c_w — сопряжение группы G с помощью w. Заметим, что $T = C_D(\sigma_w)$ — циклическая группа порядка $\dfrac{q^n - (\varepsilon 1)^n}{q - \varepsilon 1}$.

Пусть $t \in T$ — элемент порядка r. Поскольку $t^w = t^\sigma = t^{\varepsilon q}$, циклическая группа $\langle t \rangle$ является w-инвариантной. Обозначим $F = \langle t, w \rangle$ и заметим, что $F \cap Z = \langle w_0 \rangle$, где $Z = Z(G)$. Допустим, что $t^{w^l} \in \langle w_0 \rangle$ для некоторого $l \in \mathbb{N}$. Тогда элемент $t^{(\varepsilon q)^l - 1}$ имеет порядок, делящий 2, и, значит, r делит $2(q^l - (\varepsilon 1)^l)$. Поскольку r нечетно, имеем $r \mid \left(q^l - (\varepsilon 1)^l, q^n - (\varepsilon 1)^n\right) = q^{(l,n)} - (\varepsilon 1)^{(l,n)}$. Поэтому $(l,n) = n$, $l \mid n$, и $w^l \in \langle w_0 \rangle$. Значит, факторгруппа FZ/Z — группа Фробениуса с ядром порядка r и циклическим дополнением порядка n. Так как группа $\langle w_0 \rangle$ тривиальна тогда и только тогда, когда либо n нечетно, либо q четно, то мы получим оба утверждения леммы, если покажем, что F сопряжена в G с некоторой подгруппой из $C_G(\sigma)$.

По теореме Ленга — Стейнберга существует такой элемент $g \in G$, что $w = g^{-1} g^{\sigma}$. Поэтому

$$({}^g t)^{\sigma} = {}^{gw}(t^{\sigma}) = {}^g(t^{\sigma_w}) = {}^g t, \qquad ({}^g w)^{\sigma} = {}^{gw}(w^{\sigma}) = {}^{gw} w = {}^g w.$$

Следовательно, ${}^g F \leqslant C_G(\sigma)$. □

Лемма 7. (i) *Если $x \geqslant 36$ — вещественное число, то отрезок $[2x/3, x-7]$ содержит по меньшей мере одно простое число.*

(ii) *Любое непростое натуральное число $f \neq 1, 4, 6$ является суммой попарно различных простых чисел.*

Доказательство. (i) Если $x < 99$, то утверждение можно проверить непосредственно. Предположим, что $x \geqslant 99$. Существует такое число $a \in [0, 3)$, что $2x/3 + a = 3s$ для некоторого натурального числа s. Отрезок $[3s, 4s]$ содержит простое число (см. [14]). Достаточно показать, что $4s \leqslant x - 7$. Имеем $4s = 8x/9 + 4a/3 < 8x/9 + 4 = x - 7 + (11 - x/9) \leqslant x - 7$.

(ii) Докажем утверждение индукцией по f. При $f < 36$ требуемое проверяется вручную. Предположим, что $f \geqslant 36$. По пункту (i) отрезок $[2f/3, f-7]$ содержит простое число p. Поскольку $f - p \geqslant 7$, то по индукции получаем $f - p = p_1 + \ldots + p_k$, где $k \geqslant 1$ и все p_i попарно различные простые числа. Заметим, что p отлично от всех p_i, поскольку $p_i \leqslant f - p < p$. Отсюда следует требуемое. □

Лемма 8. *Пусть натуральное число n и простое число p удовлетворяют соотношениям $n \geqslant p$ и $n \neq p+1$. Если $(p,n) \notin \{(2,5), (3,6), (3,7), (3,10), (5,11), (5,18)\}$, то существуют $t \geqslant 1$, $k \geqslant 0$ и такие попарно взаимно простые натуральные числа $b_1, \ldots, b_k$, бóльшие единицы, что*

$$\begin{gathered} n = p^t + b_1 + \ldots + b_k, \\ b_i < (n - b_1 - b_2 - \ldots - b_{i-1})/2 \quad \forall\ i = 1, \ldots, k. \end{gathered} \tag{7}$$

При этом для всех $i = 1, \ldots, k$ можно взять $b_i > 3$, если $p = 2$, $n \neq 5, 6, 7, 9, 10, 11, 18$, и $b_i > 2$, если $p = 3$, $n \neq 5, 6, 7, 8, 10, 11$.

Доказательство. Пусть n и p такие, как в формулировке. Будем рассуждать индукцией по n при фиксированном p. Если $n < 36$, то требуемое разложение может быть найдено вручную[2]. Предположим, что $n \geqslant 36$.

Допустим сначала, что $n < 2p$. Тогда $p \geqslant 7$. Если $n - p \neq 4, 6$, то по пункту (ii) леммы 7 получаем нужное разложение $n - p = b_1 + \ldots + b_k$, где b_i — попарно различные простые числа. В самом деле, в этом случае выполнено $b_i \leqslant n - p < p$, тогда $b_i < (p + b_i)/2 = (n - b_1 - \ldots - b_{i-1} - b_{i+1} - \ldots - b_k)/2 \leqslant (n - b_1 - \ldots - b_{i-1})/2$. Если же $n = p + 4$ или $n = p + 6$, то это и есть требуемое разложение (7), поскольку $p \geqslant 7$.

Значит, можно считать, что $n \geqslant 2p$. Выберем простое b_1 из отрезка $[n/3, n/2 - 7]$, существующее по лемме 7 (i). Пусть $n_0 = n - b_1$. Тогда $n_0 - p \geqslant n - (n/2 - 7) - p = (n/2 - p) + 7 > 1$ и $n_0 \geqslant n/2 + 7 > 18$. Поэтому пара (n_0, p) не является исключительной, и по индукции получаем

$$n_0 = p^t + b_2 + \ldots + b_k \tag{8}$$

для некоторых $t \geqslant 1$ и $k \geqslant 0$, где числа b_i $(i = 2, \ldots, k)$ попарно взаимно просты, и $1 < b_i < (n_0 - b_2 - \ldots - b_{i-1})/2$. Значит, $b_i < (n - b_1)/2 \leqslant b_1$, все $b_2, \ldots, b_k$ отличны от простого числа

[2]Это разложение было вычислено для всех допустимых пар (p, n) при $n < 36$ (см. сводную таблицу в приложении).

b_1 и поэтому взаимно просты с ним. Следовательно, равенство (8) дает требуемое разложение $n = p^t + b_1 + b_2 + \ldots + b_k$. $\square$

Пусть q — степень простого числа и $\varepsilon \in \{+,-\}$. Для натурального числа b определим

$$q^*_{[\varepsilon b]} = \begin{cases} q_{[\varepsilon b]}, & \text{если } q_{[\varepsilon b]} \text{ существует,} \\ 9, & \text{если } (\varepsilon, b, q) = (+, 6, 2), \\ 2^l, & \text{если } (\varepsilon, b, q) = (+, 2, 2^l - 1) \text{ при } l \geqslant 2, \\ 2^l, & \text{если } (\varepsilon, b, q) = (-, 2, 2^l + 1) \text{ при } l \geqslant 2. \end{cases}$$

Отметим, что $q^*_{[\varepsilon b]}$ не определено только при $(\varepsilon, b, q) \in \{(-,2,2), (-,2,3), (-,3,2)\}$ и что

$$q^*_{[\varepsilon b]} \mid \big(q^s - (\varepsilon 1)^s\big) \iff b \mid s, \tag{9}$$

если $q^*_{[\varepsilon b]}$ определено, и в этом случае группа $\mathrm{SL}^\varepsilon_b(q)$ содержит неприводимый элемент порядка $q^*_{[\varepsilon b]}$ при дополнительном условии, что $b > 1$.

Лемма 9. *Пусть q — степень простого числа p и $\varepsilon \in \{+,-\}$. Пусть $n = p^t + b_1 + \ldots + b_k$, где $t \geqslant 0$, $k \geqslant 0$, а все числа $b_i > 1$ и попарно взаимно просты. Если $(\varepsilon, q) = (-, 2)$, то пусть также $b_i \neq 2, 3$ для всех i. Если же $(\varepsilon, q) = (-, 3)$, то пусть $b_i \neq 2$ для всех i. Положим $r_i = q^*_{[\varepsilon b_i]}$. Тогда $p^{t+1} r_1 \cdot \ldots \cdot r_k \notin \omega(\mathrm{SL}^\varepsilon_n(q))$.*

Д о к а з а т е л ь с т в о. Сначала заметим, что ввиду (9) все r_i попарно взаимно просты и не делятся на p. Предположим, что существует $a \in \mathrm{SL}^\varepsilon_n(q)$ порядка $p^{t+1} r_1 \cdot \ldots \cdot r_k$. Пусть $\zeta_1, \ldots, \zeta_n$ — характеристические корни элемента a. Поскольку жорданова форма элемента a содержит блок размера не менее $p^t + 1$, то среди корней ζ_i есть по крайней мере $p^t + 1$ одинаковых. Элемент $a^{p^{t+1}}$ полупрост, имеет порядок $r_1 \cdot \ldots \cdot r_k$ и характеристические корни $\mu_i = \zeta_i^{p^{t+1}}$, $i = 1, \ldots, n$. Отметим, что $r_1 \cdot \ldots \cdot r_k$ — наименьшее общее кратное чисел $|\mu_1|, \ldots, |\mu_n|$. Положим $R_i = \{\mu_j \mid r_i \text{ делит } |\mu_j|\}$ при $i = 1, \ldots, k$. Все множества R_i непусты, но, возможно, пересекаются. Кроме того множество $\{\mu_1, \ldots, \mu_n\}$ является объединением непересекающихся орбит O_i относительно действия отображения Фробениуса $\mu \mapsto \mu^{\varepsilon q}$. Корни в одной орбите попарно различны, каждая орбита O_i содержится в некотором множестве $R_{i'}$, и длина орбиты каждого корня μ_j из любого множества R_j делится на b_j в силу (9). Ввиду взаимной простоты чисел b_i длина объединения $R = \cup_j R_j$ не менее $b_1 + \ldots + b_k$. Кроме того, среди корней μ_i есть как минимум $p^t + 1$ одинаковых, которые должны принадлежать разным орбитам. Если какой-то из этих корней лежит в некотором множестве R_j, то все равные ему тоже лежат в R_j, и $|R| \geqslant b_1 + \ldots + (p^t + 1) b_j + \ldots + b_k > n$. В противном случае общее число элементов μ_j не менее $b_1 + \ldots + b_k + (p^t + 1) > n$. В обоих случаях получаем противоречие. $\square$

Лемма 10. *Если группа Фробениуса KC с ядром K и циклическим дополнением $C = \langle c \rangle$ порядка n действует точно на векторном пространстве V над полем ненулевой характеристики p, взаимно простой с порядком ядра K, то минимальный многочлен элемента c на V равен $x^n - 1$. В частности, полупрямое произведение VC содержит элемент порядка $p \cdot n$ и* $\dim C_V(c) > 0$.

Д о к а з а т е л ь с т в о. См. лемму 1 в [6]. $\square$

Лемма 11. *Пусть $\varepsilon \in \{+,-\}$ и $L = L^\varepsilon_n(q)$ — простая группа, где $q = p^m$. Если $G \cong \mathbb{Z}_p \times L$, то $\omega(G) \not\subseteq \omega(L)$.*

Д о к а з а т е л ь с т в о. При $n = 2$ утверждение хорошо известно. Пусть $n > 2$. Если $r = q^*_{[\varepsilon(n-1)]}$ определено, то L содержит элемент порядка r и $pr \notin \omega(\mathrm{SL}^\varepsilon_n(q))$ по лемме 9, откуда следует требуемое. В противном случае тройка (ε, n, q) совпадает с $(-,3,3)$ или с $(-,4,2)$, и тогда $3 \cdot 7 \in \omega\big(\mathbb{Z}_3 \times U_3(3)\big) \setminus \omega\big(U_3(3)\big)$ и $2 \cdot 5 \in \omega\big(\mathbb{Z}_2 \times U_4(2)\big) \setminus \omega\big(U_4(2)\big)$. $\square$

2. Доказательство теоремы

Следующая теорема является переформулировкой нашего главного результата (теорема 1), представленного во введении.

Теорема 2. *Пусть* $\varepsilon \in \{+,-\}$ *и* $L = L_n^{\varepsilon}(q)$ $(q = p^m)$ *— простая группа, действующая на векторном пространстве* W *над полем характеристики* p*. Предположим, что* $n \geqslant p$, $n \neq p+1$ *и* $(p,n) \notin \{(2,5),(3,6),(3,7),(3,10),(5,11),(5,18)\}$*. Пусть, кроме того,* $n \neq 6,7,9,10,11,18$ *при* $(\varepsilon,q) = (-,2)$ *и* $n \neq 5,8,11$ *при* $(\varepsilon,q) = (-,3)$*. Тогда* $\omega(WL) \neq \omega(L)$*.*

Д о к а з а т е л ь с т в о. По лемме 11 можно считать, что L действует точно на W. Мы можем поднять представление группы L на W до (нетривиального) представления группы $S = \mathrm{SL}_n^{\varepsilon}(q)$.

Пусть $n = p^t + b_1 + \ldots + b_k$ — разложение числа n, существование которого утверждается в лемме 8. Если $(\varepsilon,q) = (-,2)$, то мы предполагаем, что $b_i > 3$, а если $(\varepsilon,q) = (-,3)$, то $b_i > 2$ для всех i. Пусть $r_i = q^*_{[\varepsilon b_i]}$ (по предположению это число определено для всех i).

Достаточно показать, что для любого нетривиального S-модуля W над полем характеристики p существует такой элемент $a \in WS$ порядка $c = p^{t+1} r_1 \cdot \ldots \cdot r_k$, что циклическая группа $\langle a \rangle$ тривиально пересекается с центром $Z(S)$. В самом деле, если это выполнено, то по лемме 9 получим $c \in \omega(WL) \setminus \omega(L)$ ввиду включения $\omega(L) \subseteq \omega(S)$.

Применим индукцию по k. Если $k = 0$, то $n = p^t$ и по лемме 6 группа S содержит подгруппу Фробениуса R с ядром порядка $q_{[\varepsilon n]}$ (этот примитивный делитель, очевидно, существует) и циклическим дополнением порядка p^t (лемма 6 может быть применена, поскольку либо $n = p^t$ нечетно, либо $q = p^m$ четно). Так как R действует точно на W, то из леммы 10 следует, что $p^{t+1} \in \omega(WS)$, и очевидно также, что циклическая подгруппа в WS порядка p^{t+1} тривиально пересекается с центром $Z(S)$.

Предположим, что $k > 0$. Пусть V — естественный n-мерный FS-модуль с (ортонормированным) базисом $\{e_1,\ldots,e_n\}$, где $F = \mathbb{F}_q$. Положим $U = \langle e_1,\ldots,e_{b_1}\rangle_F$ и $U' = \langle e_{b_1+1},\ldots,e_n\rangle_F$. Пусть h_1 — неприводимый элемент из $\mathrm{SL}^{\varepsilon}(U,U')$ порядка r_1. Так как $1 < b_1 < n/2$, то $W_1 = C_W(h_1) \neq 0$ по лемме 1, и группа $S_1 = \mathrm{SL}^{\varepsilon}(U',U) \cong \mathrm{SL}^{\varepsilon}_{n_1}(q)$ действует нетривиально на W_1 по лемме 4, где $n_1 = p^t + b_2 + \ldots + b_n$. По индукции существует $a_1 \in W_1S_1$ порядка $c_1 = p^{t+1} r_2 \cdot \ldots \cdot r_k$. Положим $a = h_1 a_1$. Так как $[h_1,a_1] = 1$ и r_1 взаимно просто с c_1, то $|a| = c$, и по построению ясно, что $a^{p^{t+1}} \in S$ централизует в V подпространство размерности p^t, откуда получаем $\langle a \rangle \cap Z(S) = 1$. □

3. Приложение

В таблице приведено разложение чисел $n < 36$ в виде $n = p^t + b_1 + \ldots + b_k$ для всех допустимых пар (n,p), существование которого утверждается в лемме 8. Если $p = 2$ и $n \neq 6,7,9,10,11,18$, то $b_i \neq 2,3$. Если $p = 3$ и $n \neq 5,8,11$, то $b_i \neq 2$.

(n,p)	$n = p^t + b_1 + \ldots + b_k$	(n,p)	$n = p^t + b_1 + \ldots + b_k$	(n,p)	$n = p^t + b_1 + \ldots + b_k$
$(2,2)$	$2=2$	$(20,7)$	$20=7+9+4$	$(29,2)$	$29=8+9+7+5$
$(3,3)$	$3=3$	$(20,11)$	$20=11+9$	$(29,3)$	$29=9+13+7$
$(4,2)$	$4=4$	$(20,13)$	$20=13+7$	$(29,5)$	$29=5+13+7+4$
$(5,3)$	$5=3+2$	$(20,17)$	$20=17+3$	$(29,7)$	$29=7+14+5+3$
$(5,5)$	$5=5$	$(21,2)$	$21=8+9+4$	$(29,11)$	$29=11+13+5$
$(6,2)$	$6=4+2$	$(21,3)$	$21=9+7+5$	$(29,13)$	$29=13+13+3$
$(7,2)$	$7=4+3$	$(21,5)$	$21=5+9+5+2$	$(29,17)$	$29=17+12$
$(7,5)$	$7=5+2$	$(21,7)$	$21=7+9+5$	$(29,19)$	$29=19+10$
$(7,7)$	$7=7$	$(21,11)$	$21=11+10$	$(29,23)$	$29=23+6$
$(8,2)$	$8=8$	$(21,13)$	$21=13+8$	$(29,29)$	$29=29$
$(8,3)$	$8=3+3+2$	$(21,17)$	$21=17+4$	$(30,2)$	$30=8+13+5+4$
$(8,5)$	$8=5+3$	$(21,19)$	$21=19+2$	$(30,3)$	$30=9+13+8$
$(9,2)$	$9=4+3+2$	$(22,2)$	$22=8+9+5$	$(30,5)$	$30=5+13+7+3+2$
$(9,3)$	$9=9$	$(22,3)$	$22=9+10+3$	$(30,7)$	$30=7+13+7+3$
$(9,5)$	$9=5+4$	$(22,5)$	$22=5+7+5+3+2$	$(30,11)$	$30=11+14+5$
$(9,7)$	$9=7+2$	$(22,7)$	$22=7+7+5+3$	$(30,13)$	$30=13+14+3$
$(10,2)$	$10=8+2$	$(22,11)$	$22=11+9+2$	$(30,17)$	$30=17+13$
$(10,5)$	$10=5+3+2$	$(22,13)$	$22=13+9$	$(30,19)$	$30=19+11$

$(10,7)$	$10 = 7 + 3$	$(22,17)$	$22 = 17 + 5$	$(30,23)$	$30 = 23 + 7$
$(11,2)$	$11 = 4 + 5 + 2$	$(22,19)$	$22 = 19 + 3$	$(31,2)$	$31 = 8 + 11 + 7 + 5$
$(11,3)$	$11 = 9 + 2$	$(23,2)$	$23 = 8 + 11 + 4$	$(31,3)$	$31 = 9 + 15 + 7$
$(11,7)$	$11 = 7 + 4$	$(23,3)$	$23 = 9 + 11 + 3$	$(31,5)$	$31 = 5 + 15 + 7 + 4$
$(11,11)$	$11 = 11$	$(23,5)$	$23 = 5 + 11 + 5 + 2$	$(31,7)$	$31 = 7 + 15 + 7 + 2$
$(12,2)$	$12 = 8 + 4$	$(23,7)$	$23 = 7 + 11 + 5$	$(31,11)$	$31 = 11 + 13 + 7$
$(12,3)$	$12 = 9 + 3$	$(23,11)$	$23 = 11 + 7 + 5$	$(31,13)$	$31 = 13 + 13 + 5$
$(12,5)$	$12 = 5 + 5 + 2$	$(23,13)$	$23 = 13 + 10$	$(31,17)$	$31 = 17 + 14$
$(12,7)$	$12 = 7 + 5$	$(23,17)$	$23 = 17 + 6$	$(31,19)$	$31 = 19 + 12$
$(13,2)$	$13 = 8 + 5$	$(23,19)$	$23 = 19 + 4$	$(31,23)$	$31 = 23 + 8$
$(13,3)$	$13 = 9 + 4$	$(23,23)$	$23 = 23$	$(31,29)$	$31 = 29 + 2$
$(13,5)$	$13 = 5 + 5 + 3$	$(24,2)$	$24 = 8 + 11 + 5$	$(31,31)$	$31 = 31$
$(13,7)$	$13 = 7 + 6$	$(24,3)$	$24 = 9 + 11 + 4$	$(32,2)$	$32 = 8 + 13 + 7 + 4$
$(13,11)$	$13 = 11 + 2$	$(24,5)$	$24 = 5 + 11 + 5 + 3$	$(32,3)$	$32 = 9 + 15 + 8$
$(13,13)$	$13 = 13$	$(24,7)$	$24 = 7 + 11 + 6$	$(32,5)$	$32 = 5 + 13 + 7 + 5 + 2$
$(14,2)$	$14 = 8 + 6$	$(24,11)$	$24 = 11 + 11 + 2$	$(32,7)$	$32 = 7 + 13 + 7 + 5$
$(14,3)$	$14 = 9 + 5$	$(24,13)$	$24 = 13 + 11$	$(32,11)$	$32 = 11 + 13 + 8$
$(14,5)$	$14 = 5 + 5 + 4$	$(24,17)$	$24 = 17 + 7$	$(32,13)$	$32 = 13 + 15 + 4$
$(14,7)$	$14 = 7 + 5 + 2$	$(24,19)$	$24 = 19 + 5$	$(32,17)$	$32 = 17 + 15$
$(14,11)$	$14 = 11 + 3$	$(25,2)$	$25 = 8 + 12 + 5$	$(32,19)$	$32 = 19 + 13$
$(15,2)$	$15 = 8 + 7$	$(25,3)$	$25 = 9 + 11 + 5$	$(32,23)$	$32 = 23 + 9$
$(15,3)$	$15 = 9 + 6$	$(25,5)$	$25 = 5 + 11 + 5 + 4$	$(32,29)$	$32 = 29 + 3$
$(15,5)$	$15 = 5 + 7 + 3$	$(25,7)$	$25 = 7 + 11 + 5 + 2$	$(33,2)$	$33 = 8 + 13 + 7 + 5$
$(15,7)$	$15 = 7 + 5 + 3$	$(25,11)$	$25 = 11 + 11 + 3$	$(33,3)$	$33 = 9 + 16 + 5 + 3$
$(15,11)$	$15 = 11 + 4$	$(25,13)$	$25 = 13 + 12$	$(33,5)$	$33 = 5 + 13 + 7 + 5 + 3$
$(15,13)$	$15 = 13 + 2$	$(25,17)$	$25 = 17 + 8$	$(33,7)$	$33 = 7 + 16 + 7 + 3$
$(16,2)$	$16 = 16$	$(25,19)$	$25 = 19 + 6$	$(33,11)$	$33 = 11 + 15 + 7$
$(16,3)$	$16 = 9 + 7$	$(25,23)$	$25 = 23 + 2$	$(33,13)$	$33 = 13 + 13 + 7$
$(16,5)$	$16 = 5 + 7 + 4$	$(26,2)$	$26 = 8 + 11 + 7$	$(33,17)$	$33 = 17 + 16$
$(16,7)$	$16 = 7 + 7 + 2$	$(26,3)$	$26 = 9 + 12 + 5$	$(33,19)$	$33 = 19 + 14$
$(16,11)$	$16 = 11 + 5$	$(26,5)$	$26 = 5 + 11 + 7 + 3$	$(33,23)$	$33 = 23 + 10$
$(16,13)$	$16 = 13 + 3$	$(26,7)$	$26 = 7 + 11 + 5 + 3$	$(33,29)$	$33 = 29 + 4$
$(17,2)$	$17 = 8 + 5 + 4$	$(26,11)$	$26 = 11 + 11 + 4$	$(33,31)$	$33 = 31 + 2$
$(17,3)$	$17 = 9 + 8$	$(26,13)$	$26 = 13 + 11 + 2$	$(34,2)$	$34 = 8 + 15 + 7 + 4$
$(17,5)$	$17 = 5 + 7 + 3 + 2$	$(26,17)$	$26 = 17 + 9$	$(34,3)$	$34 = 9 + 13 + 7 + 5$
$(17,7)$	$17 = 7 + 7 + 3$	$(26,19)$	$26 = 19 + 7$	$(34,5)$	$34 = 5 + 13 + 9 + 5 + 2$
$(17,11)$	$17 = 11 + 6$	$(26,23)$	$26 = 23 + 3$	$(34,7)$	$34 = 7 + 13 + 9 + 5$
$(17,13)$	$17 = 13 + 4$	$(27,2)$	$27 = 8 + 13 + 6$	$(34,11)$	$34 = 11 + 16 + 7$
$(17,17)$	$17 = 17$	$(27,3)$	$27 = 9 + 13 + 5$	$(34,13)$	$34 = 13 + 16 + 5$
$(18,2)$	$18 = 4 + 7 + 5 + 2$	$(27,5)$	$27 = 5 + 13 + 5 + 4$	$(34,17)$	$34 = 17 + 15 + 2$
$(18,3)$	$18 = 9 + 5 + 4$	$(7)27,$	$27 = 7 + 13 + 5 + 2$	$(34,19)$	$34 = 19 + 15$
$(18,7)$	$18 = 7 + 8 + 3$	$(27,11)$	$27 = 11 + 13 + 3$	$(34,23)$	$34 = 23 + 11$
$(18,11)$	$18 = 11 + 7$	$(27,13)$	$27 = 13 + 11 + 3$	$(34,29)$	$34 = 29 + 5$
$(18,13)$	$18 = 13 + 5$	$(27,17)$	$27 = 17 + 10$	$(34,31)$	$34 = 31 + 3$
$(19,2)$	$19 = 8 + 7 + 4$	$(27,19)$	$27 = 19 + 8$	$(35,2)$	$35 = 8 + 13 + 9 + 5$
$(19,3)$	$19 = 9 + 7 + 3$	$(27,23)$	$27 = 23 + 4$	$(35,3)$	$35 = 9 + 17 + 5 + 4$
$(19,5)$	$19 = 5 + 7 + 5 + 2$	$(28,2)$	$28 = 8 + 13 + 7$	$(35,5)$	$35 = 5 + 13 + 7 + 5 + 3 + 2$
$(19,7)$	$19 = 7 + 7 + 5$	$(28,3)$	$28 = 9 + 13 + 6$	$(35,7)$	$35 = 7 + 17 + 8 + 3$
$(19,11)$	$19 = 11 + 8$	$(28,5)$	$28 = 5 + 13 + 7 + 3$	$(35,11)$	$35 = 11 + 17 + 7$
$(19,13)$	$19 = 13 + 6$	$(28,7)$	$28 = 7 + 13 + 5 + 3$	$(35,13)$	$35 = 13 + 17 + 5$
$(19,17)$	$19 = 17 + 2$	$(28,11)$	$28 = 11 + 13 + 4$	$(35,17)$	$35 = 17 + 13 + 5$
$(19,19)$	$19 = 19$	$(28,13)$	$28 = 13 + 13 + 2$	$(35,19)$	$35 = 19 + 16$
$(20,2)$	$20 = 8 + 7 + 5$	$(28,17)$	$28 = 17 + 11$	$(35,23)$	$35 = 23 + 12$
$(20,3)$	$20 = 9 + 8 + 3$	$(28,19)$	$28 = 19 + 9$	$(35,29)$	$35 = 29 + 6$
$(20,5)$	$20 = 5 + 7 + 5 + 3$	$(28,23)$	$28 = 23 + 5$	$(35,31)$	$35 = 31 + 4$

Поступила 8.06.2006

СПИСОК ЛИТЕРАТУРЫ

1. **Hall P., Higman G.** The p-length of p-soluble groups and reduction theorems for Burnside's problem // Proc. London Math. Soc., Ser. III. 1956. V. 6. P. 1–42.
2. **Mazurov V.D.** Characterizations of groups by arithmetic properties // Algebra Colloq. 2004. V. 11, no. 1. P. 129–140.
3. **Заварницин А.В., Мазуров В.Д.** О порядках элементов в накрытиях симметрических и знакопеременных групп // Алгебра и логика. 1999. Т. 38, № 3. С. 296–315.
4. **Заварницин А.В.** Веса неприводимых $\mathrm{SL}_3(q)$-модулей в характеристике определения // Сиб. мат. журн. 2004. Т. 45, № 2. С. 319–328.
5. **Заварницин А.В.** Порядки элементов в накрытиях $L_n(q)$ и распознавание знакопеременной группы A_{16}: Препринт № 48 // Новосибирск: НИИДМИ, 2000.
6. **Мазуров В.Д.** О множестве порядков элементов конечной группы // Алгебра и логика. 1994. Т. 33, № 1. С. 81–89.
7. **Brandl R., Shi W.** The characterization of $\mathrm{PSL}_2(q)$ by its element orders // J. Algebra. 1994. V. 163, no. 1. P. 109–114.
8. **Darafsheh M.R., Moghaddamfar A.R.** Corrigendum: Characterization of the groups $\mathrm{PSL}_5(2)$, $\mathrm{PSL}_6(2)$ and $\mathrm{PSL}_7(2)$ [*Comm. Algebra*, **29**, no. 1 (2001), 465–475] // Comm. Algebra. 2003. V. 31, no. 9. P. 4651–4653.

9. **Grechkoseeva M.A., Lucido M.S., Mazurov V.D., Moghaddamfar A.R., Vasil'ev A.V.** On recognition of the projective special linear groups over the binary field // Sib. Elektron. Mat. Izv. 2005. V. 2. P. 253–263.
10. Нерешенные вопросы теории групп: Коуровская тетрадь. Новосибирск: Ин-т математики СО РАН, 1999.
11. **Kleidman P., Liebeck M.** The subgroup structure of the finite classical groups // London Math. Soc. Lect. Note Ser. Cambridge: Cambridge University Press, 1990. V. 129.
12. **Zsigmondy K.** Zur Theorie der Potenzreste // Monatsh. für Math. und Phys. 1892. V. 3. C. 256–284.
13. **Васильев А.В., Гречкосеева М.А.** О распознавании по спектру конечных простых линейных групп над полями характеристики 2 // Сиб. мат. журн. 2005. Т. 46, № 4. С. 749–758.
14. **Hanson D.** On a theorem of Sylvester and Schur // Canad. Math. Bull. 1973. V. 16. P. 195–199.
15. **Suprunenko I.D., Zalesskii A.E.** Fixed vectors for elements in modules for algebraic groups // Intern. J. Algebra Comput. 2007. V. 17, no. 4. P. 773–785.

ТРУДЫ ИНСТИТУТА МАТЕМАТИКИ И МЕХАНИКИ УрО РАН

Том 13 № 1 2007

УДК 519.14

КВАЗИТЕЛА, АССОЦИИРОВАННЫЕ С АВТОМОРФИЗМОМ АДДИТИВНОЙ ГРУППЫ КОНЕЧНОГО ПОЛЯ[1]

А. П. Ильиных

Предлагается конструкция конечных квазител, основанная на использовании специальных автоморфизмов аддитивных групп конечных полей.

В [1] введен класс конечных квазител, соответствующих автоморфизму аддитивной группы конечного поля нечетной характеристики. В работе [2] приведены примеры таких квазител, а в [3] эта конструкция перенесена на случай поля четной характеристики. В настоящей заметке вводится класс конечных квазител, соответствующих автоморфизму аддитивной группы произвольного конечного поля, причем конструкция этих квазител сочетает идеи построения квазитела нечетной характеристики из [1] с конструкцией квазитела четной характеристики из [3].

Пусть $F = GF(q)$, $F^* = F \setminus \{0\}$, n — фиксированное целое число. Пусть $f \in \mathrm{Aut}(F,+)$ — произвольный автоморфизм аддитивной группы поля F. Рассмотрим два подмножества Δ и $-\Delta$ в F^*, где

$$\Delta = \{x^f x^n \mid x \in F^*\} \quad \text{и} \quad -\Delta = \{-x \mid x \in \Delta\}.$$

Предположим, что для автоморфизма f выполнено следующее условие:

$$F^* = \Delta \cup -\Delta. \tag{1}$$

Если $\mathrm{char} F = 2$, то $\Delta = -\Delta$, и вместо (1) имеем

$$F^* = \Delta.$$

Пусть $\mathrm{char} F > 2$. Если n — нечетно, то $(-x)^f(-x)^n = x^f x^n$ для всех $x \in F^*$ и, следовательно, $\mid \Delta \mid \leqslant (q-1)/2$. В силу (1) и равенства $\mid F^* \mid = q-1$ имеем $\mid \Delta \mid = (q-1)/2$ и $\Delta \cap -\Delta = \varnothing$. Если n — четно, то $(-x)^f(-x)^n = -x^f x^n$ для всех $x \in F^*$ и $\Delta = -\Delta$. С учетом (1) имеем $F^* = \Delta$.

Рассмотрим группу $(\mathcal{P},+)$, где $\mathcal{P} = \{(x,y) \mid x,y \in F\}$, и $(x,y)+(z,t) = (x+z, y+t)$. Пусть $\mathcal{L}_0$ — множество подгрупп в группе $\mathcal{P}$, обозначаемых через H, V и L_ε^k, где $k \in F^*$ и $\varepsilon = \pm 1$, и определяемых следующим образом:

$$H = \{(x,0) \mid x \in F\}, \quad V = \{(0,x) \mid x \in F\},$$

$$L_1^k = \{(xk, x^f k^{-n}) \mid x \in F\}, \tag{2}$$

$$L_{-1}^k = \{(-xk, x^f k^{-n}) \mid x \in F\}. \tag{3}$$

Если $\mathrm{char} F = 2$ или $\mathrm{char} F > 2$ и n — четно, то $L_{-1}^{-k} = L_1^k$, что влечет за собой $\mid \mathcal{L}_0 \mid \leqslant q+1$.

Если $\mathrm{char} F > 2$ и n — нечетно, то $L_1^{-k} = L_1^k$, $L_{-1}^{-k} = L_{-1}^k$, и снова $\mid \mathcal{L}_0 \mid \leqslant q+1$.

Рассмотрим инцидентностную структуру $\mathcal{A}_f = (\mathcal{P}, \mathcal{L}, I)$, где множество прямых имеет вид $\mathcal{L} = \{L + x \mid L \in \mathcal{L}_0, x \in \mathcal{P}\}$, а I индуцируется отношением принадлежности.

[1]Работа выполнена при частичной финансовой поддержке РФФИ (проект 06-01-00378).

Теорема 1. *$\mathcal{A}_f$ — аффинная плоскость трансляций.*

Д о к а з а т е л ь с т в о. Согласно [4] достаточно проверить, что подгруппы $L \in \mathcal{L}_0$ образуют расщепление группы $\mathcal{P}$. Так как $|\,\mathcal{L}_0\,| \leqslant q+1$, $|\,L\,| = q$, $|\,\mathcal{P}\,| = q^2$, то для этого требуется лишь установить, что любой элемент $p = (a, b)$ содержится в некоторой подгруппе из $\mathcal{L}_0$. Если $ab = 0$, то $p \in H$ или $p \in V$. Пусть $ab \neq 0$.

Подстановка $(x, y) \mapsto (xm, ym^{-n})$, где $m \in F^*$, переставляет подгруппы $L \in \mathcal{L}_0$. Поэтому считаем $a = 1$, $p = (1, b)$. Из (2) и (3) получаем

$$(1, b) \in L_1^k \Leftrightarrow b = (k^{-1})^f k^{-n} \text{ для некоторого } k \in F^* \Leftrightarrow b \in \Delta,$$
$$(1, b) \in L_{-1}^k \Leftrightarrow b = -(k^{-1})^f k^{-n} \text{ для некоторого } k \in F^* \Leftrightarrow b \in -\Delta.$$

Следовательно,

$$(1, b) \in L_\varepsilon^k, \text{ где } b = \varepsilon(k^{-1})^f k^{-n} \text{ и } \varepsilon = \pm 1. \tag{4}$$

Теорема доказана.

Следуя [5, п. 20.3, рис. 11], введем координаты и найдем тернар плоскости $\mathcal{A}_f$. Пусть π — проективная плоскость с бесконечно удаленной прямой XY, соответствующая плоскости $\mathcal{A}_f$. Рассмотрим тернар R, соответствующий четверке точек $(0, e, X, Y)$, где $0 = (0, 0)$, $e = (1, 1^f)$. При этом прямая $x = 0$ в π равна $V \cup \{Y\}$, прямая $y = 0$ равна $H \cup \{X\}$. Припишем точке (a, a^f) прямой $0e$ координаты $[a, a]$ (координаты точек из $\mathcal{P}$ будут записываться с использованием прямых скобок в виде $[x, y]$, а сами элементы из $\mathcal{P}$ — с использованием круглых скобок в виде (a, b)). Тогда

$$\text{точка } (a, b^f) \text{ имеет координаты } [a, b]. \tag{5}$$

По теореме 20.4.6 из [5] R — система Веблена–Веддерберна (квазитело), $R = (F, \oplus, \circ, 0, 1)$. Явный вид операций $\oplus$ и $\circ$ в R дается следующей теоремой.

Теорема 2. *Квазитело R плоскости $\mathcal{A}_f$ состоит из элементов поля F. Сложение $\oplus$ в R совпадает со сложением в поле F, а умножение $\circ$ однозначно определено следующими равенствами, где $a, b \in F$:*

$$a \circ (b^f b^n)^{f^{-1}} = \big((ab)^f b^n\big)^{f^{-1}}, \tag{6}$$
$$a \circ (-b^f b^n)^{f^{-1}} = -\big((ab)^f b^n\big)^{f^{-1}}. \tag{7}$$

Д о к а з а т е л ь с т в о. Пусть $b \in F$ и L — прямая $y = x \oplus b$ проективной плоскости π, соответствующей $\mathcal{A}_f$. Тогда $L = \{[x, x \oplus b] \mid x \in F\} \cup \{[1]\}$ и, следовательно, L содержит точки из $\mathcal{P}$ вида $(x, x^f + b^f)$, где $x \in F$. По (5) $(x, x^f + b^f) = [x, (x^f + b^f)^{f^{-1}}]$. Отсюда с учетом $f^{-1} \in \mathrm{Aut}(F, +)$ получаем $x \oplus b = (x^f + b^f)^{f^{-1}} = x + b$. Таким образом, $x \oplus b = x + b$ для всех $x, b \in F$.

Остается проверить, что

$$a \circ \varepsilon(b^f b^n)^{f^{-1}} = \varepsilon\big((ab)^f b^n\big)^{f^{-1}} \text{ для } \varepsilon = \pm 1.$$

Найдем произведение $x \circ m$ для $x, m \in F$, где $m \neq 0$. Прямая $y = x \circ m$ содержит точки $[0, 0] = (0, 0)$ и $[1, m] = (1, m^f)$. По (4) при $b = m^f$ получаем $(1, m^f) \in L_\varepsilon^k$, где $m^f = \varepsilon(k^{-1})^f k^{-n}$, $m = (\varepsilon(k^{-1})^f k^{-n})^{f^{-1}}$. Имеем $L_\varepsilon^k = \{[xk, \varepsilon(x^f k^{-n})^{f^{-1}}] \mid x \in F\}$. Поэтому $xk \circ (\varepsilon(k^{-1})^f k^{-n})^{f^{-1}} = \varepsilon(x^f k^{-n})^{f^{-1}}$. Полагая $a = xk$, $b = k^{-1}$, получаем требуемое равенство $a \circ \varepsilon(b^f b^n)^{f^{-1}} = \varepsilon((ab)^f b^n)^{f^{-1}}$.

Теорема доказана.

З а м е ч а н и е. Пусть f — произвольный автоморфизм аддитивной группы конечного поля F с условием (1). Пусть, кроме того, m — произвольный элемент из F^* и f_1 — автоморфизм аддитивной группы поля F с условием

$$x^{f_1} = mx^f.$$

Тогда для f_1 выполнено условие (1) и тернар R_1 для f_1 совпадает с тернаром R для f.

Действительно, множество $\Delta_1 = \{x^{f_1}x^n \mid x \in F^*\}$ для f_1 равно $m\Delta$. Поэтому $F^* = \Delta_1 \cup -\Delta_1$. Далее, в обоих тернарах R и R_1 сложение совпадает со сложением в поле F. Умножение в тернаре R задано равенствами (6) и (7). Для умножения вида (6) в тернаре R_1 имеем совпадение с умножением в тернаре R:

$$a \circ (b^{f_1}b^n)^{f_1^{-1}} = \Big((ab)^f b^n m m^{-1}\Big)^{f^{-1}} = \Big((ab)^f b^n\Big)^{f^{-1}}.$$

Аналогично совпадают умножения вида (7). Поэтому тернар R_1 для f_1 совпадает с тернаром R для f.

Заметим, что отсюда следует также совпадение плоскостей для f и f_1. Таким образом, заменяя f на подходящий f_1, можно при построении плоскости считать, что $1^f = 1$.

Поступила 19.10.2006

СПИСОК ЛИТЕРАТУРЫ

1. **Ильиных А.П.** О плоскости Геринга и ассоциированных с ней блок-схемах // Мат. заметки. 1996. Т. 60, вып. 6. С. 873–881.
2. **Ильиных А.П.** Класс квазител, ассоциированных с автоморфизмом аддитивной группы конечного поля нечетной характеристики // Междунар. семинар по теории групп, посвященный 70-летию А.И.Старостина и 80-летию Н.Ф.Сесекина. Тез. докл. Екатеринбург, 2001. С. 92-94.
3. **Ильиных А.П.** Класс квазител, ассоциированных с автоморфизмом аддитивной группы конечного поля четной характеристики // Междунар. семинар по теории групп, посвященный 70-летию А.И.Старостина и 80-летию Н.Ф.Сесекина. Тез. докл. Екатеринбург, 2001. С. 90-91.
4. **Dembowsky P.** Finite geometries. Berlin etc.: Springer, 1968.
5. **Холл М.** Теория групп. М.: ИЛ., 1963.

Том 13 № 1 2007

УДК 512.54

НИЛЬПОТЕНТНЫЕ АЛГЕБРЫ И ИХ ПРИМЕНЕНИЯ[1]

Л. С. Казарин

Работа посвящена строению конечных нильпотентных алгебр и их применениям, в первую очередь к строению произведений групп. Затрагиваются некоторые вопросы, касающиеся применения нильпотентных алгебр и родственных им структур к построению рекуррентных последовательностей.

1. Введение

Ассоциативная алгебра $R \neq 0$ называется *нильпотентной* класса нильпотентности $n = n(R) \geq 1$, если $R^n \neq 0$ и $R^{n+1} = 0$. Другими словами, если произведение любых $n+1$ элементов алгебры R равно нулю и существует n элементов в R, произведение которых отлично от нуля. Нильпотентные алгебры известны давно. Их роль в теории ассоциативных алгебр важна ввиду того, что радикал Джекобсона любой конечномерной ассоциативной алгебры является нильпотентной алгеброй, а факторалгебра по этому радикалу полупроста. Существуют важные классы групповых алгебр, строение которых почти полностью определяется радикалом Джекобсона. Именно, если G — конечная p-группа, F — поле характеристики p, то фундаментальный идеал J алгебры $F[G]$ является нильпотентной алгеброй коразмерности 1 (Л.Е. Диксон). Более того, если G и H — конечные абелевы p-группы, а F — поле характеристики p, то изоморфизм алгебр $F[G]$ и $F[H]$ влечет за собой изоморфизм G и H (В.Е. Дескинс).

Другой важный пример доставляет множество всех верхних треугольных квадратных матриц размера $n \times n$ с коэффициентами из некоторого поля F с нулевой главной диагональю. В нашей терминологии (в этом месте немного отличающейся от общепринятой) это нильпотентная алгебра класса нильпотентности $n-1$.

Нильпотентные алгебры весьма интенсивно изучались в конце 60-х — начале 70-х гг. прошлого столетия: имеются две монографии [27] и [17], удачно дополняющие друг друга. Свойствам групповой алгебры конечной p-группы посвящен содержательный обзор [10].

Весьма важной конструкцией (Н. Джекобсон), связанной с нильпотентными алгебрами, является *присоединенная группа* алгебры. Если R — любая ассоциативная алгебра, то можно определить с помощью кольцевых операций $+$ и $\cdot$ новую бинарную операцию $\circ$ по следующему правилу: $a \circ b = ab + a + b$. В том случае, когда алгебра нильпотентна, множество R с операцией $\circ$, обозначаемое через R°, является группой. (Если поле, над которым определена алгебра, имеет характеристику p, то R° является p-группой.) Более того, этим свойством обладают радикальные кольца и алгебры, в частности, ниль-алгебры, т.е. алгебры, в которых для любого элемента существует такое натуральное число n, что n-я степень этого элемента равна нулю. В нашем случае будут рассматриваться лишь конечные нильпотентные алгебры. По классическому результату Веддерберна конечномерная ниль-алгебра нильпотентна.

В дальнейшем, если не оговорено противное, рассматривается конечная нильпотентная алгебра над полем F характеристики p (*p-алгебра*).

Принятые обозначения в основном стандартны, однако для удобства читателя напомним некоторые. Через R^n обозначается n-я степень алгебры R, т.е. идеал, порожденный всеми

[1]Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (проект 05–01–01018).

произведениями вида $x_1x_2\dots x_n$, где $x_1, x_2, \dots, x_n \in R$. В частности, $R^1 = R$. Подалгебра алгебры R, порожденная элементами $x_1, x_2, \dots, x_k$, обозначается через $\langle\langle x_1, x_2, \dots, x_k\rangle\rangle$, тогда как подпространство, натянутое на эти же элементы, — через $\langle x_1, x_2, \dots, x_k\rangle$. Подалгебра $R^{(i)}$ коммутативной p-алгебры R есть подалгебра, состоящая из всех p^i-х степеней алгебры R, а $R_{(i)} = \{a \in R \mid a^{p^i} = 0\}$. Очевидно, что $R/R_{(i)} \simeq R^{(i)}$. Минимальное число образующих алгебры R обозначается через $d(R)$, а класс нильпотентности через $n(R)$.

2. Некоторые открытые проблемы

Несмотря на долгую историю, многие естественные проблемы, касающиеся нильпотентных алгебр, остаются открытыми даже в коммутативном случае. Выяснено, например, что существует бесконечно много попарно неизоморфных нильпотентных алгебр размерности 6 над полем нулевой характеристики. Количество попарно неизоморфных нильпотентных алгебр размерности n над полем $GF(q)$ может быть записано в виде $q^{\alpha n^3}$, где $\alpha = 4/27 + O(n^{-1/3})$ [17, теорема 5.2.11]. Любопытно, что асимптотически тот же результат справедлив и для всех алгебр над $GF(q)$, причем полупростые алгебры размерности $n \geq 1$ в этом множестве составляют явное меньшинство: их не больше, чем $2^{n-1}e^{n/e}$ [17, гл. 5]. Таким образом, почти все ассоциативные алгебры данной размерности нильпотентны! Кстати, асимптотика того же вида известна и для количества p-групп порядка p^n.

Как видно из предыдущего обсуждения, задача полного описания всех нильпотентных алгебр данной размерности весьма проблематична. Для размерности не выше 4 описание получено в [17] в случае алгебр положительной характеристики и для размерности не выше 5 в [27] в случае нулевой характеристики. Имеется более 25000 нильпотентных алгебр размерности 6 над полем $GF(2)$ и 267 2-групп порядка 2^6. Поэтому представляет интерес более грубая классификация алгебр по свойствам их присоединенных групп.

Легко показать, что любая конечная p-группа может быть реализована как подгруппа присоединенной группы некоторой p-алгебры. Однако p-группа не всегда является присоединенной группой некоторой p-алгебры. Например, циклическая группа порядка p^3 не может быть присоединенной группой p-алгебры. Интересно, как устроена p-группа, которая не является присоединенной группой p-алгебры, каковы ее сложностные характеристики. Удивительно, но даже для коммутативной p-алгебры неизвестно строение присоединенной группы (имеются в виду параметры, определяющие ее точное строение). По-другому этот же вопрос можно сформулировать так:

Какова группа единиц (т.е. обратимых элементов) конечномерной коммутативной p-алгебры?

Даже в случае максимальной абелевой подгруппы силовской p-подгруппы группы $GL_n(p)$ ответ неизвестен, что отмечено впервые в [27] и неоднократно другими авторами.

Одним из первых результатов в рассматриваемом круге вопросов была теорема, доказанная в 1971 г. Н. Эггертом, учеником Р. Крузе [13].

Теорема 1 (Эггерт [13]). *Пусть R — коммутативная p-алгебра над совершенным полем, причем* $\dim R^{(1)} \leq 2$. *Тогда* $\dim R \geq 2p$.

Эта теорема дала основание Эггерту выдвинуть довольно смелую гипотезу, которая и получила название “гипотеза Эггерта”:

Гипотеза Эггерта. *Пусть R — коммутативная p-алгебра. Тогда* $\dim R \geq p \dim R^{(1)}$.

Удивительным следствием этой гипотезы, обнаруженным Эггертом, является полное описание в случае положительного ответа присоединенной группы произвольной коммутативной p-алгебры R. А именно, в этом случае существуют такие однопорожденные нильпотентные алгебры $L_1, L_2, \dots L_k$, что сумма их размерностей равна размерности алгебры R, а

$$R^\circ \simeq L_1^\circ \times L_2^\circ \cdots \times L_k^\circ.$$

Речь не идет о разложении самой алгебры R в прямую сумму подалгебр L_i. Такого разложения, как легко показать, может и не быть. Но сама теорема о строении присоединенной группы, сводящая структуру присоединенной группы коммутативной нильпотентной алгебры к строению присоединенных групп однопорожденных нильпотентных алгебр, была бы более чем удовлетворительным ответом на поставленный выше вопрос, обнаруживая аналогию с теоремой о конечнопорожденных абелевых группах.

Список из 10 нерешенных вопросов о нильпотентных алгебрах и их присоединенных группах содержится в [8].

3. Присоединенная группа нильпотентной алгебры

Обсудим известные к настоящему времени результаты о строении присоединенной группы конечной нильпотентной алгебры. Л. Фишер и К. Элдридж (1969) классифицировали все конечные кольца с циклической присоединенной группой, а Б. Горлов (1995) описал p-алгебры с метациклической присоединенной группой. Группы, вошедшие в список, оказались порядка не выше p^2 при $p > 2$ и не выше 16 при $p = 2$. Б. Амберг и Л. Казарин (1999) классифицировали p-группы, не имеющие элементарных абелевых подгрупп ранга 3. В случае $p > 2$ присоединенная группа p-алгебры размерности не меньше $p(p+1)/2$ имеет элементарную абелеву подгруппу ранга p, а при $p = 2$ и $\dim R > 6$ присоединенная группа 2-алгебры R содержит элементарную абелеву подгруппу порядка 8. Полностью описано строение присоединенной группы однопорожденной нильпотентной алгебры. Наконец, ими же определены присоединенные группы нильпотентных алгебр размерности не выше 5:

Теорема 2. *Пусть R — некоммутативная нильпотентная алгебра над полем $GF(p)$, причем $\dim R \le 5$. Тогда выполняется одно из следующих утверждений*:

(*i*) *R° имеет класс нильпотентности 2 и экспоненту p*;

(*ii*) *R° — одна из 5 групп класса нильпотентности 3, $p \le 3$;*

(*iii*) *R° имеет класс нильпотентности 2, экспоненту p^2, коммутант порядка не более p^2, и $\Phi(R^\circ) \le Z(R^\circ)$.*

В действительности описание группы R° в теореме 2 получено в терминах образующих и определяющих соотношений, а здесь изложена лишь качественная сторона этого описания.

Группа класса нильпотентности 2 и экспоненты p всегда является присоединенной группой некоторой p-алгебры. Пусть P — конечная специальная p-группа экспоненты p и класса нильпотентности 2. Следующая остроумная конструкция принадлежит Л.А. Калужнину [17]. Отображение $x \to x^2$ для нечетного p в группе P является взаимно однозначным отображением, и потому операция извлечения корня квадратного из элементов группы P также определена однозначно. Определим кольцевые операции $+$ и $\cdot$ на P следующим образом:

$$x \cdot y = xyx^{-1}y^{-1} = [x^{-1}, y^{-1}];$$

$$x + y = xy\sqrt{y \cdot x}.$$

По [17, теорема 1.6.7] относительно операций $+$ и $\cdot$ группа P является нильпотентной алгеброй класса нильпотентности 2 над полем $GF(p)$. Верно и обратное: всякая некоммутативная нильпотентная алгебра R над $GF(p)$, удовлетворяющая соотношению $R^3 = 0$, т.е. класса нильпотентности 2, имеет двухступенно нильпотентную присоединенную группу (в которой умножение имеет вид $x \circ y = x + y + x \cdot y$), являющуюся группой экспоненты p. Позднее результат Калужнина немного обобщили А. Бовди, Л. Моран и Р. Тенч, показавшие, что 2-группа класса 2 и экспоненты 4 также является присоединенной группой некоторой нильпотентной алгебры.

Обозначим через $d(R)$ (соответственно, $d(R^\circ)$) минимальное число образующих алгебры R (группы R°). Понятно, что $d(R) \le d(R^\circ)$, хотя неравенство может быть строгим даже для коммутативных нильпотентных алгебр. Хорошо известно, что любая p-группа вкладывается в p-группу с двумя образующими. Однако присоединенные группы нильпотентных алгебр, как правило, имеют большое число образующих. Первый результат в данном направлении следующий:

Теорема 3. *Пусть R — p-алгебра, причем $d(R^\circ) = 2$. Тогда* $\dim R \le 5$.

В частности, отсюда следует и упомянутый выше результат Горлова. Следующий результат принадлежит Л. Казарину и П. Соулсу [16].

Теорема 4. *Пусть R — p-алгебра, $p \ge 3$, причем $d(R) \le 2$ и $d(R^\circ) = 3$. Тогда* $\dim R \le 9$.

Предыдущие теоремы наталкивают на мысль, что размерность p-алгебры ограничена функцией от минимального числа образующих ее присоединенной группы и, возможно, числа p. Разумеется, это верно для коммутативной p-алгебры.

Важную роль во всех вопросах, связанных с изучением присоединенной группы нильпотентной алгебры, играет аналогия между конечными p-группами и конечномерными нильпотентными алгебрами. В теории p-групп весьма плодотворным оказалось изучение групп с малым коклассом, т.е. групп порядка p^n и класса нильпотентности $c(G)$, у которых разность $n - c(G)$ невелика. Например, группы кокласса 1 — группы максимального класса в обычной терминологии.

Как показал Крузе [17], конечная p-группа порядка p^n может быть присоединенной группой некоторой нильпотентной алгебры лишь в случае, когда ее класс нильпотентности не превосходит $(n+1)/2$. Б. Амберг и Л. Казарин [6] усилили этот результат, показав, что если произведение порядков факторов нижнего центрального ряда конечной p-группы G, превосходящих p^3, ограничено некоторой константой C, а G является присоединенной группой некоторой p-алгебры, то $|G|$ не превосходит функции от p и C.

Существенную роль в доказательстве сыграла теорема из [4], показывающая, что если $\dim(R) - n(R) \le n(R) - 3 + d(R)$, то существует такая однопорожденная подалгебра L алгебры R, что $\dim L = n(R)$. Тем самым алгебра “кокласса”, меньшего, чем класс нильпотентности, содержит большýю однопорожденную подалгебру, что и определяет успех в решении указанного вопроса. Отметим, что нильпотентные алгебры с $\dim R - n(R) \le 2$ изучались в [27] при условии, что рассматриваемое поле имело нулевую характеристику.

Продолжая тему о параллелизме между группами и нильпотентными алгебрами, упомянем два результата из [8] об алгебрах, похожих на минимальные неабелевы группы (группы Миллера — Морено [20]).

Теорема 5. *Пусть R — нильпотентная алгебра над полем F размерности не менее 4, все собственные подалгебры которой имеют класс нильпотентности не более n, тогда как $n(R) \ge 2n$. Тогда R — однопорожденная алгебра размерности $2n$ или $2n+1$.*

Следующая теорема — аналог известного результата [18, теорема 2].

Теорема 6. *Пусть R — такая нильпотентная алгебра над полем F, что каждая подалгебра R коразмерности m имеет класс нильпотентности не выше n, тогда как класс $n(R)$ не меньше $n+1$. Тогда выполнены следующие утверждения*:

(*i*) *R имеет систему образующих из не более чем $m+n$ элементов*;

(*ii*) *класс нильпотентности R ограничен некоторой функцией $f(m,n)$, где $f(1,n) = 2n+1$*;

(*iii*) *размерность R ограничена функцией $g(m,n)$, где $g(1,n) < 2(n+1)^{n+1}$ и $g(m,n) \le m + g(1,n) - 1$*;

(iv) *если существует нильпотентная алгебра A класса нильпотентности $n(A) = k > n$ с минимальным числом образующих $d(A) = d$, все собственные подалгебры которой имеют класс нильпотентности не выше n, то существует нильпотентная алгебра R с этим свойством размерности, не меньшей* $\dfrac{d^{k+1}-1}{d-1}$.

4. Градуированные алгебры и функции Гильберта

Существует один важный класс алгебр, естественным образом связанный с рассматриваемым кругом вопросов. Это градуированные алгебры.

Пусть R — ассоциативное коммутативное нетерово кольцо с единицей, градуированное с помощью множества неотрицательных целых чисел. Тогда

$$R = R_0 \oplus R_1 \oplus R_2 \dots,$$

где $R_i R_j \subseteq R_{i+j}$ для любых $i, j \geq 0$. При этом $1 \in R_0$. Если $R_0 = F$ — поле и R является F-алгеброй в обычном смысле, то R называется G-алгеброй (градуированной алгеброй). Предположение о нетеровости R означает конечную порожденность R, так что R_i будет конечномерным векторным пространством над F для любого i. Функция Гильберта для R определяется следующим образом:

$$H(R, n) = \dim_F R_n$$

для всех неотрицательных целых чисел n. В частности, $H(R, 0) = 1$. Ненулевой элемент $x \in R_n$ для некоторого $n \geq 0$ называется однородным степени n. Для нулевого элемента удобно считать его степень равной $-\infty$. Так как R конечно порождена, то имеется конечное число однородных образующих степени 1, порождающих вместе с единичным элементом R как алгебру. Пусть это будут элементы $x_1, x_2, \dots, x_d$. Если $A = F[Y_1, Y_2, \dots Y_d]$ — коммутативное кольцо многочленов над F с независимыми переменными $Y_1, Y_2 \dots, Y_d$, то существует сохраняющий степень гомоморфизм $\pi : A \to R$, переводящий Y_i в x_i. При этом $A = A_0 + A_1 + \dots$ также является G-алгеброй (со стандартной градуировкой). Заметим, что минимальное число d однородных образующих степени 1 алгебры R равно размерности пространства R_1, т.е. $H(R, 1)$. Таким образом, произвольную G-алгебру R можно рассматривать как факторалгебру алгебры многочленов.

В случае, когда R — коммутативная p-алгебра над полем F, ей можно сопоставить некоторую G-алгебру аналогично тому, как это делается в случае конечных p-групп. Для этого требуется сначала вложить R в алгебру с единицей $\widehat{R}$, а затем, выбрав минимальную систему образующих в R, объявить ее однородной системой образующих степени 1 ассоциированной G-алгебры $U = U(R)$. Дальнейшая процедура более или менее стандартна. При этом однородные компоненты U_i для $i \geq 1$ будут изоморфны факторам R^i/R^{i+1} как векторным пространствам над F. Естественно, при этом некоторая информация о строении R будет потеряна, но сохранится важная информация о размерностях факторов R^i/R^{i+1}, определяющих векторфункцию, которую мы также будем называть функцией Гильберта алгебры R. Для краткости в дальнейшем вводится обозначение $d_i = d_i(R) = \dim R^i/R^{i+1}$. Заметим, что если R — коммутативная нильпотентная алгебра над F и K — некоторое расширение поля F, то алгебра $Q = R \otimes_F K$ имеет те же значения функции Гильберта, что и R. Это простое соображение часто оказывается полезным.

Пусть $A = F[Y_1, Y_2, \dots Y_d]$ — кольцо многочленов от d независимых переменных, определенное выше. Следующее определение и теорема, с ним связанная, принадлежат Ф. Маколею (см. [25], где имеются подробные комментарии на эту тему). Непустое множество T мономов вида $Y_1^{\alpha_1} Y_2^{\alpha_2} \dots Y_d^{\alpha_d}$ от переменных $Y_1, Y_2, \dots Y_d$ называется *порядковым идеалом мономов*, если из того, что $t \in T$ и t' делит t, следует, что $t' \in T$.

Теорема 7. *Пусть A — F-алгебра многочленов от d независимых переменных, определенная выше, и R — градуированная G-алгебра, изоморфная $\pi(A)$, где $\pi : A \to R$ — гомоморфизм, сохраняющий степень. Тогда в A существует такой порядковый идеал мономов T, что $\{p(t) | t \in T\}$ является базисом R как векторного пространства над F.*

Из [25, теорема 2.2] следует, что коммутативная нильпотентная алгебра R с заданными значениями $d_i(R)$ функции Гильберта существует тогда и только тогда, когда в связанной с R алгебре A существует такой порядковый идеал мономов T, что $d_i(R) = |\{u \in T | \deg(u) = i\}|$ для любого $i \geq 1$. В качестве следствия из этой теоремы Р. Стенли [25] показал, что если $d_k(R) \leq k$ для некоторого k, то и для всех $m \geq k$ выполнено соотношение $d_m(R) \leq k$. На самом деле имеются некоторые численные соотношения, вытекающие из теоремы 7 и обеспечивающие существование коммутативной нильпотентной алгебры с данными параметрами.

Следующая теорема, также опирающаяся на теорему 7 и представление коммутативной нильпотентной алгебры в виде факторалгебры алгебры многочленов, принадлежит Б. Амбергу и Л. Казарину [8].

Теорема 8. *Пусть R — коммутативная нильпотентная алгебра над полем F, имеющая минимальную систему образующих из d элементов. Тогда выполнены следующие утверждения*:

- (i) *если $d_k \leq k$ для некоторого $k \geq 1$, то $d_j \leq k$ для всех $j \geq k$. При этом, если F — достаточно большое поле, то найдется такой элемент $x \in R$, что $R^j = R^{j-1}x$;*
- (ii) *если существует такое натуральное число $m \geq 2$, что для любого образующего элемента x из минимальной системы образующих алгебры R выполнено $x^{m+1} \in R^{m+1} \setminus R^{m+2}$, то $d_m \geq d_1$. Если $|F| \geq d_1$, а $d_m \leq d_1$, то существует элемент $y \in R \setminus R^2$, для которого $R^{m-1}y^2 \subseteq R^{m+2}$.*

Непосредственные применения связаны с поведением функции Гильберта, о чем будет сказано позже.

5. Произведения конечных групп и нильпотентные алгебры

Пусть $G = AB$ — конечная группа, являющаяся произведением своих подгрупп A и B. Тогда для любого простого числа p существуют такие силовские p-подгруппы A_p и B_p групп A и B соответственно, что $A_pB_p = B_pA_p = G_p$ — силовская p-подгруппа G. Поэтому многие проблемы, касающиеся групп с факторизацией, нередко связаны с изучением более частного вопроса о факторизации p-групп. Когда рассматриваемые свойства подгрупп A и B переносятся на подгруппы и факторгруппы, можно формулировать и доказывать предполагаемый результат по индукции, рассматривая минимальный контрпример. В большинстве случаев этот контрпример есть p-группа $G = AB = AN = BN$, где A, B и N — подгруппы G, причем N нормальна. Я.П. Сысаком [28] найден метод, позволяющий конструировать группу G с такими свойствами, а в некоторых случаях свести ее изучение к изучению присоединенной группы p-алгебры.

Рассмотрим этот метод более подробно. Пусть R — произвольная p-алгебра. Присоединенная группа R° алгебры R действует на ее аддитивной группе $R^+ = N$, ставя в соответствие элементам $a \in R^\circ$ и $r \in R$ элемент $r + ra$. Соответствующее полупрямое произведение $G(R) = NA = NB = AB$ с нормальной подгруппой N называется *ассоциированной группой алгебры* R. Обе подгруппы A и B изоморфны R°, а N изоморфна R^+. В этом случае также $A \cap B = A \cap N = B \cap N = 1$.

В рассматриваемой ситуации подгруппа N группы G всегда абелева. Используя модификацию этих идей с локальным почти-кольцом вместо радикального кольца R, можно сконструировать также ситуацию “трижды факторизуемых” групп, когда нормальная подгруппа N группы G может не быть абелевой [8].

В случае, когда сомножители A и B являются абелевыми p-группами, ситуация обратима и произведение $G = AB = AN = BN$ с нормальной подгруппой N и свойством $A \cap B = A \cap N = N \cap B = 1$ изоморфно ассоциированной группе коммутативной нильпотентной алгебры [1, утверждение 6.1.4].

Если конечная p-группа $G = AB$ — произведение подгрупп A и B, ранги Прюфера которых ограничены числом r, то, как было доказано Д.И. Зайцевым и Л. Казариным (1981), ранг Прюфера группы G ограничен полиномиальной функцией от r (см. по этому поводу [1, теорема 4.3.5]). Этот результат был существенно улучшен в [3]:

Теорема 9. *Пусть конечная p-группа $G = AB$ — произведение подгрупп A и B и $r(A) \leq r(B)$. Если $p \geq 3$, то нормальный ранг $r_n(G)$ удовлетворяет неравенству:*

$$r_n(G) \leq 2r(A)(\lceil \log_2 r(A) \rceil + 1) + r(A) + r(B).$$

Как следствие, отсюда получается оценка ранга Прюфера группы G через ранги A и B, близкая к линейной.

Теорема 10. *Пусть конечная p-группа $G = AB$ — произведение подгрупп A и B, чьи ранги Прюфера не превосходят r. Если $p \geq 3$, то ранг Прюфера G удовлетворяет неравенству:*

$$r(G) \leq 4r(\lceil \log_2 r \rceil + 2)^2.$$

Случай, когда ранги сомножителей A и B группы $G = AB$ невелики, представляет особый интерес. При $p > 2$ Б. Хупперт показал, что конечная p-группа, являющаяся произведением двух циклических групп, метациклическая [15, 3.11.5]. Аналогичный результат справедлив для произведения метациклических групп (Амберг и Казарин (1997)). Именно, если $p > 3$, то ранг Прюфера произведения не превосходит 4. При $p = 3$ существует 3-группа $G = AB$ ранга Прюфера 5, являющаяся произведением двух метациклических абелевых групп. Отметим также, что для любого наперед заданного k и любого $p > 2k$ произведение двух абелевых групп (или, в более общем случае, двух регулярных p-групп), ранги Прюфера которых не превосходят k, имеет ранг, не превосходящий $2k$.

Доказательства этих фактов теоретико-групповые. Они дают информацию и о строении p-алгебр над конечным полем:

Теорема 11. *Пусть R — p-алгебра и $p > 2$. Тогда*

$$\dim R \leq 2r(R^{\circ})(\lceil \log_2 r(R^{\circ}) \rceil + 1).$$

Если R коммутативна, то

$$\dim R \leq r(R^{\circ})(\lceil \log_p (p/(p-1) r(R^{\circ}) \rceil + 1).$$

Удивительно, что разница между коммутативным и некоммутативным случаями не столь велика.

Однако в случае, когда алгебра R является коммутативной, существует надежда, что имеется линейная оценка для ранга произведения двух p-групп. Она основана на следующем результате [6]:

Предложение 1. *Пусть конечная группа $G = AB$ — произведение двух абелевых p-подгрупп A и B. Если гипотеза Эггерта верна, то ранг Прюфера $r(G)$ группы G удовлетворяет неравенству*

$$r(G) \leq 2(r(A) + r(B)) + \frac{p}{(p-1)} \min\{r(A), r(B)\}.$$

Заметим, что оценка экспоненты произведения двух p-групп ограничена некоторой функцией, зависящей от экспонент сомножителей и ступени разрешимости группы, что замечено еще Д.И. Зайцевым. В случае, когда A и B абелевы, эта экспонента делит произведение экспонент сомножителей (Хольт и Хаулетт, см. [1, 3.3.1]). В общем случае вопрос о нахождении хорошей оценки остается открытым.

Ступень разрешимости произведения трех попарно перестановочных циклических групп может быть сколь угодно велика [1, с. 208]. Соответствующий пример построен Маркони (1987). Рассмотрим множество матриц $G_{p,n}$, $p > 2$, вида

$$x = \begin{pmatrix} 1+pa & pb \\ pc & 1+pd \end{pmatrix},$$

где a, b, c, d — вычеты по модулю p^n, причем $\det\ x = 1$. Группа $G_{p,n}$ имеет порядок p^{3n-3} и является произведением циклических подгрупп A, B и C, порожденных матрицами

$$\begin{pmatrix} 1+pu & 0 \\ 0 & (1+pu)^{-1} \end{pmatrix}, \qquad \begin{pmatrix} 1+pu & 0 \\ u^{-1}-u & (1+pu)^{-1} \end{pmatrix} \qquad \text{и} \qquad \begin{pmatrix} 1+pu & u-u^{-1} \\ 0 & (1+pu)^{-1} \end{pmatrix}$$

соответственно. Здесь u пробегает множество вычетов по модулю p^{n-1}. Тогда $G_{p,n} = ABC$, где каждая из подгрупп изоморфна мультипликативной группе кольца вычетов по модулю p^n. В частности, подгруппы A, B и C — циклические, а ступень разрешимости не меньше, чем p, если $n > 2^p$.

6. Гипотеза Эггерта

Связь проблемы ранга произведения двух групп со строением p-алгебры и была стартовой точкой для цикла исследований, предпринятых Амбергом и Казариным [2–8], для выяснения строения конечных нильпотентных алгебр. Гипотеза Эггерта, важная и сама по себе, оказалась весьма трудной. Заметим, что еще в 1976 г. Р. Батиста [9] установил справедливость гипотезы для случая $\dim R^{(1)} = 3$. Этот же результат был передоказан в 1998 г. (Стэк [24]). Амберг и Казарин доказали ее для случая, когда $\dim R^{(1)} = 4$. При этом попутно выяснилось, что для линейности оценки ранга произведения двух примарных групп через ранги сомножителей достаточно доказать, что размерность R связана с размерностью $\dim R^{(1)}$ следующим соотношением:

$$\dim R \geq c \dim R^{(1)},$$

где c — некоторая константа, бо́льшая 2. При этом указанную слабую форму гипотезы Эггерта достаточно доказать для алгебр, у которых имеется тождество $x^{p^2} = 0$.

Один из последних результатов в этом направлении, полученных К. Маклином и независимо Амбергом и Казариным, следующий:

Теорема 12. *Пусть R — коммутативная p-алгебра класса нильпотентности p. Тогда гипотеза Эггерта справедлива.*

Это первый случай, когда на размерность подалгебры $R^{(1)}$ в доказательстве гипотезы Эггерта не накладывается ограничений.

В действительности К. Маклин отправлялся сразу от случая градуированных нильпотентных алгебр и добился на этом пути поразительных достижений. Укажем следующие его результаты [19]:

Теорема 13. *Пусть R — градуированная коммутативная p-алгебра. Гипотеза Эггерта справедлива в каждом из следующих случаев*:

(i) *R имеет минимальную систему образующих из двух элементов*;

(*ii*) $(R^{(1)})^4 = 0$ *и* $p = 2$;

(*iii*) $(R^{(1)})^3 = 0$.

В своем частном письме Маклин утверждает, что для градуированной коммутативной нильпотентной алгебры R над $GF(p^m)$ ему удалось доказать, что $\dim R \geq (p-1)\dim R^{(1)}$. Таким образом, по крайней мере для градуированных алгебр ситуация существенно прояснилась.

Для нильпотентных алгебр наилучший к настоящему времени результат получен в [6]: *если* $\dim R^{(1)} \leq 4$, *то гипотеза Эггерта справедлива.*

7. Тройные факторизации групп и почти-кольца

Ранее уже упоминались результаты Я. Сысака и П. Хуберта, обращающие конструкции, когда встречается тройная факторизация $G = AB = AN = NB$ при $A \cap B = A \cap N = B \cap N = 1$. Здесь мы рассмотрим подход П. Хуберта, позволяющий не накладывать на нормальную подгруппу N в этом произведении условие абелевости.

Напомним, что (левым) *почти-кольцом* называется алгебраическая система R с двумя бинарными операциями $+$ и $\cdot$, удовлетворяющая следующим постулатам:

(N1) $(R,+)$ — группа с нейтральным элементом 0;

(N2) $(R,\cdot)$ — ассоциативная полугруппа;

(N3) выполнен левый закон дистрибутивности: $x(y+z) = xy + xz$ для любых $x, y, z \in R$.

Если R содержит единичный элемент, т.е. такой элемент $1 \in R$, что $1 \cdot x = x \cdot 1$ для любого $x \in R$, то говорят, что R — почти-кольцо с единицей.

Типичный пример почти-кольца доставляет множество $M(G)$ отображений $\alpha : G \to G$ конечной группы, записываемой аддитивно, в себя. При этом операции сложения и умножения в $M(G)$ определяются следующим образом:

$$(\alpha + \beta)(x) = \alpha(x) + \beta(x); \qquad (\alpha\beta)(x) = \alpha(\beta(x))$$

для любых $\alpha, \beta \in M(G)$, $x \in G$.

Следующие два определения задают основную конструкцию для групп с тройной факторизацией в рассматриваемом выше смысле.

Определение 1. Пусть R — почти-кольцо с единицей 1 и $U \leq R^+$ — такая подгруппа аддитивной группы R^+ почти-кольца R, что $U + 1$ является подгруппой группы единиц почти-кольца R, обозначаемой далее через $R^\times$. Тогда U называется *конструктивной подгруппой* в R.

Если U — конструктивная подгруппа в R, то $1 \notin U$, так как иначе $0 \in U$, а нуль — необратимый элемент. Обозначим через A подгруппу $(U+1)$ группы $R+1$. Заметим, что разность двух элементов из A содержится в U. В самом деле, если $a, b \in A$, то $a-1, b-1 \in U$, а тогда $(a-b) = (a-1)-(b-1) \in U$. Отсюда сразу следует, что для $u, v \in U$, $a = u+1 \in A$, $b = v+1 \in A$ имеем $(u+1)v = a(b-1) = ab - b \in U$.

Обозначим теперь подгруппу U^+ через N. Легко убедиться, что A действует на N с помощью умножения: $a \cdot u \in U$ для любых $a \in A, u \in N$.

Определение 2. Пусть R — почти-кольцо с единицей 1, $N = U \leq R^+$ — конструктивная подгруппа аддитивной группы R^+ и $A = (U+1)$. Тогда полупрямое произведение $N \rtimes A = G(R,U) = G$ называется *ассоциированной группой* для конструктивной подгруппы U почти-кольца R.

Как обычно, множество элементов группы $G = G(R,U)$ будет записываться в виде пар (x,y), где $x \in A$, $y \in N$, причем множество пар вида $(x,0)$ будет отождествляться с A, а множество пар вида $(0,y)$ с N. Рассмотрим теперь “диагональную подгруппу” $B = \{(u+1)^{-1}, u) \mid u \in U\}$.

Оказывается, что $G = AN = BN = AB$, причем $A \cap B = A \cap N = B \cap N = 1$.

Таким образом, получилась группа с тройной факторизацией.

Замечательный результат, полученный П. Хубертом, таков.

Теорема 14. *Пусть $G = AN = NB = AB$ — группа с тройной факторизацией, где N нормальна в G и $A \cap B = A \cap N = B \cap N = 1$. Тогда почти-кольцо $M(N)$ содержит такую конструктивную подгруппу $U \leq R^+$, изоморфную A, что $G \simeq G(R, U)$.*

Хубертом получена серия результатов, касающихся так называемых локальных почти-колец, содержащих довольно много кандидатов на роль конструктивных подгрупп.

8. Группы Судзуки и алгебры Судзуки

Согласно [15, с. 299–300] неабелева 2-группа, отличная от обычной или обобщенной группы кватернионов, обладающая группой автоморфизмов, транзитивной на множестве инволюций, называется 2-*группой Судзуки.* Имеется два типа 2-групп Судзуки класса нильпотентности 2. 2-группа Судзуки P принадлежит первому типу, если $|Z(P)| = q = 2^n$ и $|P| = q^3$. Примерами таких групп служат силовские 2-подгруппы простой группы $U_3(q)$.

2-группы Судзуки второго типа (с $|P| = q^2$, $|Z(P)| = q$) исчерпываются, согласно [15, теорема 8.7.9], группами $A(n, \Theta)$, определение которых мы сейчас напомним.

Пусть $F = GF(2^n)$, r — число, делящее n, и Θ — автоморфизм поля F порядка r. Тогда множество матриц вида

$$y = \begin{pmatrix} 1 & \alpha & \beta \\ 0 & 1 & \Theta(\alpha) \\ 0 & 0 & 1 \end{pmatrix}, \qquad \alpha, \beta \in F,$$

называется 2-*группой Судзуки* $A(n, \Theta)$. Она изоморфна силовской 2-подгруппе группы ${}^2B_2(2^n)$, если n — нечетное число.

Определим нечетный аналог 2-групп Судзуки $P = A_p(n, \Theta)$ аналогично тому, как это сделано в работах Ханаки [14] и Сагирова [23]. Пусть $F = GF(p^n)$, $n = mk$ и Θ — автоморфизм порядка k поля F. Элементы группы P — это упорядоченные пары (a, b) элементов поля F с операцией

$$(a, b)(c, d) = (a + c, b + d + a\Theta(c)).$$

Группу $P = A_p(n, \Theta)$ будем называть *p-группой Судзуки.* Порядок группы P равен q^2, где $q = p^n$. Отметим, что $A(n, \Theta) = A_2(n, \Theta)$.

Множество верхних треугольных матриц вида

$$y = \begin{pmatrix} \lambda & \beta & \alpha \\ 0 & \lambda & \Theta(\beta) \\ 0 & 0 & \lambda \end{pmatrix},$$

где $\alpha, \beta, \in GF(q)$, $q = p^n$, $\lambda \in GF(p)$, Θ — нетривиальный автоморфизм поля $F = GF(q)$, отвечающий p-группе Судзуки, является некоммутативной ассоциативной локальной алгеброй вида $A = 1 \cdot GF(p) \oplus R$ (где R — нильпотентная алгебра, состоящая из всех матриц указанного вида с нулевой главной диагональю), аналогичной кольцу Галуа, использовавшемуся ранее для построения рекуррентных последовательностей.

Группа $A_p(n, \Theta)$ является для алгебры R присоединенной группой, в которой умножение любых элементов x и y задается следующим образом: $x \circ y = x \cdot y + x + y$, где $x \cdot y$ — произведение этих элементов в алгебре R. Тот факт, что $A_p(n, \Theta)$ — присоединенная группа алгебры R, записывается в виде $R^\circ = A_p(n, \Theta)$.

Если $q = p^n$ и $|\Theta| = n$, то неабелева группа $A_p(n, \Theta)$ имеет ранг Прюфера, равный $n + 1$, и ассоциированная группа $G(R)$ для алгебры нильпотентных матриц, определенных выше, является группой ранга $3n$. Это, похоже, первый пример для $p > 2$, когда ранг произведения двух p-групп оказывается существенно больше, чем сумма рангов. При этом указанная граница не зависит от p, являя контраст со случаем произведения двух абелевых групп.

Очевидно, что любой автоморфизм p-алгебры Судзуки R является и автоморфизмом группы $A_p(n,\Theta)$.

Группа автоморфизмов 2-группы Судзуки $A(n,\Theta)$ рассматривалась в работе Е.Г. Брюхановой [11].

Определим следующие подгруппы группы автоморфизмов алгебры R (и группы P= $A_p(n,\Theta) = R^\circ$):

$A_1 = \{\phi \in \mathrm{Aut}(P) | (a,b)^\phi = (a, \psi(a) + b)\}$, где $\psi = \psi_\phi$ — линейное преобразование поля $GF(q)$, рассматриваемого как векторное пространство над $GF(p)$.

$A_2 = \{\phi \in \mathrm{Aut}(P) | (a,b)^\phi = (da, d\Theta(d)b)\}$, где $d = d_\phi$ — ненулевой элемент поля $GF(q) = F$.

$A_3 = \{\phi \in \mathrm{Aut}(P) | (a,b)^\phi = (a^{p^r}, b^{p^r})\}$, где $r = r_\phi \leq n-1$.

Описание группы автоморфизмов p-алгебры Судзуки R $(p > 2)$ в явном виде получено В.М. Сидельниковым и автором без использования тонких соображений, понадобившихся для случая $p = 2$:

Теорема 15. *Пусть R — p-алгебра Судзуки с $P = A_p(n,\Theta) = R^\circ$ и $G = \mathrm{Aut}(R)$. Тогда $G = A_1 \rtimes A_2 \rtimes A_3$, где A_1, A_2, A_3 определены выше. В частности, $|\mathrm{Aut}(R)| = p^{n^2}(p^n-1)n$.*

Вообще говоря, группа автоморфизмов группы, являющейся присоединенной группой некоторой нильпотентной алгебры, не обязана совпадать с группой автоморфизмов алгебры. Однако для группы $A_p(n,\Theta)$ совпадение имеет место:

Теорема 16. *Пусть G — группа автоморфизмов p-группы Судзуки $P = A_p(n,\Theta)$ и R — соответствующая p-алгебра. Если $(|\Theta|, 2p) = 1$, то $G = \mathrm{Aut}(R)$.*

Любопытным свойством p-групп и алгебр Судзуки является то обстоятельство, что множество орбит групп их автоморфизмов оказывается очень маленьким. Таким образом, можно утверждать, что эти группы являются весьма однородными, что делает их близкими к векторным пространствам и полезными в разных приложениях.

9. Некоторые приложения

1. Было бы весьма самонадеянно предлагать вниманию читателя все комбинаторные приложения, возникающие из теории, развитой Р. Стенли и его последователями. Имеется огромная область математики, связанная с изучением коммутативных градуированных алгебр. Хорошее введение можно найти в недавнем препринте В. Брунса (Commutative Algebra arising from the Anand–Dumir–Gupta conjectures. Univ. Osnabrueck, 2005) и статьях Р. Стенли [25, 26]. Отметим, что главный объект исследования — многочлены от n переменных по модулю некоторого идеала — интересен как алгебраистам, так и алгебраическим геометрам и топологам, а также прикладникам. При этом одна из основных задач — перечисление граней симплициальных комплексов с заданными дополнительными условиями — сводится к доказательству существования коммутативной нильпотентной алгебры с заданными значениями функции Гильберта. Разумеется, нельзя обойти и конструкцию Голода, приведшую к построению серии замечательных примеров групп и алгебр. Упрощение примера Голода получено в [22]. Для теории конечных групп эти исследования, как показано выше, также интересны.

2. Непосредственной мотивацией для автора были задачи, связанные с изучением рекуррентных последовательностей над некоторыми алгебраическими структурами. Классическая постановка задачи такова. Имеется некоторая конечная алгебраическая структура R, в которой есть две операции — сложение и умножение. Определим рекуррентную последовательность $\{x_n\}$ глубины k следующим образом:

$$x_n = \sum_{i=1}^{k} a_i x_{n-i},$$

где начальные значения $x_0, x_1, \dots x_k$ и коэффициенты a_i содержатся в R. Хотелось бы изучить поведение этих последовательностей, например, найти их максимально возможный период, распределение значений. В случае, когда R — конечное поле, задача хорошо известна, и имеется вполне удовлетворительная теория. Большой цикл работ А.А. Нечаева посвящен исследованиям рекуррентных последовательностей над кольцом Галуа, которое определяется следующим образом.

Пусть R — локальное кольцо с нильпотентным радикалом $J(R) = pR$, где p — характеристика поля вычетов $R/J(R)$. Тогда R называется *кольцом Галуа*.

Эти кольца начал изучать В. Крулль в 1923 г. под названием Grundringen. Простейшие примеры — кольцо Галуа $GR(q^n, p^n)$, имеющее q^n элементов и характеристику p^n, причем $GF(p^m) = GR(p^m, p)$, и кольцо $Z_{p^n} = GR(p^n, p^n)$. Заметим, что радикал кольца Галуа является однопорожденной нильпотентной алгеброй, а все идеалы главные. Известно также, что два (конечных) кольца Галуа изоморфны тогда и только тогда, когда у них одни и те же характеристика и порядок.

Имеется много приложений линейных рекуррентных последовательностей над кольцами Галуа как для получения псевдослучайных последовательностей, пригодных к использованию по методу Монте-Карло, так и для нужд криптографии и теории кодирования. В частности, в этом контексте выясняется строение кодов Кердока.

3. Представляется интересным использование других структур. В частности, локальных колец, почти-колец и нильпотентных алгебр. Работа в этом направлении только начата. Интересны в этом отношении и специальные классы алгебр, например, алгебры Судзуки. Группы Судзуки также интересны для построения новой системы ключевого обмена (криптосистемы с открытым ключом).

4. Логарифмирование по модулю целого числа N существенно облегчается, если известно разложение $\phi(N)$ на множители и имеется большая степень простого числа, делящая $\phi(N)$. Техника так называемых частных Ферма позволяет в ряде случаев свести задачу логарифмирования к задаче быстрого возведения в степень.

5. Разумеется, важным является выяснение строения максимальной коммутативной подалгебры алгебры верхних треугольных матриц (проблема Супруненко). Если гипотеза Эггерта будет доказана, эта проблема также будет решена.

6. Представление конечной группы, содержащее регулярное представление заданной небольшой подгруппы, интересно для получения плотных сферических упаковок и кодов на n-мерной евклидовой сфере. С формальной точки зрения любая конечная группа, имеющая факторизацию в виде $G = AB$ с $A \cap B = 1$, таким представлением обладает. Экспериментальная работа в этом направлении дала некоторые интересные результаты [12].

Автор выражает глубокую признательность своим коллегам и постоянным соавторам Б. Амбергу и В.М. Сидельникову, совместная работа с которыми стимулировала написание этой статьи.

Программа, вычисляющая присоединенную группу конечной нильпотентной алгебры разработана недавно А. Коноваленко и П. Соулсом (P.Soules). Автор благодарен П. Соулсу за информацию об этом.

Поступила 16.01.2007

СПИСОК ЛИТЕРАТУРЫ

1. **Amberg B., Franciosi S., de Giovanni F.** Products of groups. Oxford: Clarendon Press, 1992.
2. **Amberg B., Kazarin L.** On the rank of a finite product of two p-groups // Proc. intern. conf. “Groups — Korea 1994”. Berlin: de Gruyter, 1995. P. 1–8.
3. **Amberg B., Kazarin L.** On the rank of the product of two finite p-groups and nilpotent p-algebras // Comm. Algebra. 1999. Vol. 27, no. 8. P. 3895–3907.
4. **Amberg B., Kazarin L.** On the adjoint group of a finite nilpotent p-algebra // J. Math. Sci. Algebra, 13. 2000. Vol. 102, no. 3. P. 3979–3997.

5. **Амберг Б., Казарин Л.С.** О размерности нильпотентной алгебры // Мат. заметки. 2001. Т. 70, № 4. С. 483–490.
6. **Amberg B., Kazarin L.** Commutative nilpotent p-algebras with small dimension // Topics in infinite groups. Quad. Mat. Caserta: Seconda Univ. Napoli, 2001. Vol. 8. P. 1–20.
7. **Amberg B., Kazarin L.** On the central series of the adjoint group of a nilpotent p-algebra // Publ. Math. Debrecen, 2003. Vol. 63, no. 3. P. 473–482.
8. **Amberg B., Kazarin L.** Nilpotent algebras and factorized p-groups // Proc. intern. conf. "Groups – St. Andrews 2005".
9. **Bautista R.** Units of finite algebras // Ann. Inst. Mat. Univ. Nac. Autónoma. México, 1976. Vol. 16, no. 2. P. 1–78.
10. **Bovdi A.A.** The group of units of a group algebra of characteristic p // Publ. Math. Debrecen, 1998. Vol. 52, no. 1–2. P. 193–244.
11. **Брюханова Е.Г.** О группах автоморфизмов 2-автоморфных 2-групп // Алгебра и логика. 1981. Т. 20, № 1. С. 5–21.
12. **Dorofeev A.Yu., Kazarin L.S., Sidel'nikov V.M., Tuzhilin M.E.** Matrix groups related to the quaternion group and spherical orbit codes // Designes, Codes and Cryptography. 2005. Vol. 37, no. 3. P. 391–404.
13. **Eggert N.H.** Quasi-regular groups of finite commutative nilpotent algebras // Pac. J. Math. 1971. Vol. 36. P. 631–634.
14. **Hanaki A.** A condition on lengths of conjugacy classes and character degrees // Osaka J.Math. 1996. Vol. 33, no. 1. P. 207–216.
15. **Huppert B., Blackburn N.** Finite Groups II. New York: Springer, 1982.
16. **Kazarin L., Soules P.** Finite nilpotent p-algebras whose adjoint group has 3 generators // JP J. Algebra, Number Theory and Applications. 2004. Vol. 4, no. 1. P. 113–127.
17. **Kruse R.L., Price D.T.** Nilpotent rings. New York: Gordon and Breach, 1969.
18. **MacDonald I.D.** Generalizations of a classical theorem about nilpotent groups // Ill. J. Math. 1964. Vol. 8. P. 556–570.
19. **McLean K.R.** Eggert's conjecture on nilpotent algebras // Comm. Algebra. 2004. Vol. 32. P. 997–1006.
20. **Miller G.A., Moreno H.C.** Non-abelian groups in which every proper subgroup is abelian // Trans. Amer. Math. Soc. 1903. Vol. 4. P. 398–404.
21. **Moran L.E., Tench R.N.** Normal complements in mod p envelopes // Isr. J. Math. 1977. Vol. 27. P. 331–338.
22. **Ol'shanskii A.Yu.** A simplification of Golods example // Proc. Intern. Conf. "Groups — Korea, 1994". Berlin: de Gruyter, 1995. P. 263–265.
23. **Сагиров И.А.** Степени неприводимых характеров 2-групп Судзуки // Мат. заметки. 1999. Т. 66, № 2. С. 258–263.
24. **Stack C.** Some results on the structure of finite nilpotent algebras over fields of prime characteristic // J. Comb. Math. Comb. Comp. 1998. Vol. 28. P. 327–335.
25. **Stanley R.P.** Hilbert functions of graded algebras // Adv. in Math. 1978. Vol. 28. P. 57–83.
26. **Stanley R.P.** Combinatorial reciprocity theorems // Adv. in Math. 1974. Vol. 14. P. 194–253.
27. **Suprunenko D.A., Tyshkevich R.I.** Commutative matrices. New York: Academic Press, 1968.
28. **Sysak Ya.P.** Some examples of factorized groups and their relation to group theory // Proc. Intern. Conf. "Infinite Groups 1994". Berlin: de Gruyter, 1995. P. 263–265.

ТРУДЫ ИНСТИТУТА МАТЕМАТИКИ И МЕХАНИКИ УрО РАН

Том 13 № 1 2007

УДК 512.542.7

МНОЖЕСТВА С ТРИВИАЛЬНЫМИ ГЛОБАЛЬНЫМИ СТАБИЛИЗАТОРАМИ ДЛЯ ПРИМИТИВНЫХ ГРУПП ПОДСТАНОВОК, НЕ ЯВЛЯЮЩИХСЯ ПОЧТИ ПРОСТЫМИ[1]

А. В. Коныгин

Получено описание таких примитивных и не являющихся почти простыми групп подстановок G на конечных множествах X, что глобальный стабилизатор любого подмножества множества X в группе G нетривиален.

1. Введение

В [3] доказано, что (с точностью до подстановочного изоморфизма) существует лишь конечное число примитивных групп подстановок G на конечных множествах X таких, что $\mathrm{Alt}(X) \not\leq G$ и глобальный стабилизатор любого подмножества R множества X в группе G нетривиален (т.е. $G_{\{R\}} \neq 1$). В связи с этим представляет интерес вопрос об описании таких примитивных групп подстановок G на конечных множествах X, что $G_{\{R\}} \neq 1$ для любого подмножества R множества X [3]. Вместе с тем актуальным является и вопрос (не рассматриваемый в [3]) о явном виде подмножества R множества X со свойством $G_{\{R\}} = 1$ (в случае его существования).

В настоящей работе оба эти вопроса рассмотрены в случае, когда группа G не является почти простой. Напомним, что группа G называется *почти простой*, если $\mathrm{Inn}(T) \trianglelefteq G \leq \mathrm{Aut}(T)$ для некоторой простой неабелевой группы T. Описанию почти простых групп G таких, что $G_{\{R\}} \neq 1$ для любого подмножества R множества X, будет посвящена отдельная работа.

Теорема. *Пусть G — примитивная группа подстановок, не являющаяся почти простой, на конечном множестве X. Тогда либо существует подмножество R множества X со свойством $G_{\{R\}} = 1$, либо группа G подстановочно изоморфна одной из следующих групп:*
(i) S_3 *в естественном подстановочном представлении степени* 3;
(ii) S_4 *в естественном подстановочном представлении степени* 4;
(iii) A_4 *в естественном подстановочном представлении степени* 4;
(iv) $AGL(1,5)$ *в естественном подстановочном представлении степени* 5;
(v) D_{10} *в естественном подстановочном представлении степени* 5;
(vi) $AGL(1,7)$ *в естественном подстановочном представлении степени* 7;
(vii) $AGL(2,3)$ *в естественном подстановочном представлении степени* 9;
(viii) $ASL(2,3)$ *в естественном подстановочном представлении степени* 9;
(ix) *подгруппа порядка* 144 *группы* $AGL(2,3)$ *в естественном подстановочном представлении степени* 9;
(x) $AGL(3,2)$ *в естественном подстановочном представлении степени* 8;
(xi) *подгруппа порядка* 168 *группы* $AGL(3,2)$ *в естественном подстановочном представлении степени* 8.

[1]Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (проект № 06-01-00378).

Условия теоремы позволяют получить явный вид подмножества R в случае его существования.

Пусть G — группа подстановок на конечном множестве X. Определим число $D(G)$ как минимальное натуральное число n, для которого существует функция $\chi : X \to \{1, \ldots, n\}$ такая, что из условий $g \in G$ и $\chi(g(x)) = \chi(x)$ для всех $x \in X$ следует $g = 1$. Аналогичное понятие для групп автоморфизмов графов было введено в [1]. Сформулированная выше теорема утверждает, что если примитивная группа G не является почти простой, то либо $D(G) \leq 2$, либо G подстановочно изоморфна одной из групп (i)–(xi) из теоремы.

2. Определения и вспомогательные утверждения

Пусть G — конечная группа подстановок на множестве X и $R \subseteq X$. Через $G_{\{R\}}$ будем обозначать глобальный стабилизатор подмножества R в группе G, т.е. $G_{\{R\}} = \{g \in G \mid g(R) = R\}$. Через G_R будем обозначать поточечный стабилизатор подмножества R в группе G, т.е. $G_R = \{g \in G \mid g(r) = r$ для любого $r \in R\}$. Заметим, что если $H \leq G$, то $D(H) \leq D(G)$. Симметрическая (знакопеременная) группа степени k обозначается через S_k (A_k). Для произвольной группы G через $\mathrm{Inv}(G)$ обозначим множество ее инволюций. Напомним, что элемент $g \in G$ называется строго вещественным, если $hgh = g^{-1}$ для некоторой инволюции h из $\mathrm{Inv}(G)$.

Под графом всюду далее понимается конечный неориентированный граф без петель и кратных ребер. Если Γ — граф, то $V(\Gamma)$ — множество вершин графа Γ и $E(\Gamma)$ — множество его ребер. Для $x \in V(\Gamma)$ через $\Gamma(x)$ будем обозначать окрестность вершины x в графе Γ, т.е. множество вершин графа Γ, смежных с x в Γ.

Доказательство теоремы основывается на теореме О'Нэна — Скотта [8]. Пусть G — примитивная группа подстановок на конечном множестве X. Положим $|X| = n$, $x \in X$, $B = \mathrm{Soc}(G)$. Поскольку группа G примитивна, то $B \cong T^k$, где T — простая группа. Теорема О'Нэна — Скотта утверждает, что конечная примитивная и не являющаяся почти простой группа подстановок G подстановочно изоморфна группе одного из следующих типов.

I. $B = \mathbb{Z}_p^k$, $G \leq AGL(k,p)$ — аффинная группа, действующая на точках k-мерного пространства над полем из p элементов, $G_x = G \cap GL(k,p)$ — неприводимая подгруппа группы $GL(k,p)$.

II. $k \geq 2$, T — неабелева группа.

II (a). Пусть

$$W = \Big\{(a_1, \ldots, a_k).\pi \mid a_i \in \mathrm{Aut}(T),\ \pi \in S_k,\ a_i \equiv a_j (\mathrm{mod}\ \mathrm{Inn}(T)),\ i,j \in \{1, \ldots, k\}\Big\},$$

где элементы $\pi \in S_k$ переставляют естественным образом компоненты a_i. Тогда имеем $W = B(\mathrm{Out}(T) \times S_k) \leq (\mathrm{Aut}(T))^k S_k$ (где S_k естественным образом переставляет множители).

Положив
$$W_x = \Big\{(a, \ldots, a).\pi \mid a \in \mathrm{Aut}(T),\ \pi \in S_k\Big\}$$
(и взяв в качестве X множество левых смежных классов W по W_x), получим примитивное представление группы W степени $|T|^{k-1}$. При $1 \leq i \leq k$ пусть T_i — подгруппа группы B, состоящая из элементов, все проекции которых, отличные от i-й, единичны, $\mathcal{T} = \{T_1, \ldots, T_k\}$. Группа W естественным образом действует на множестве $\mathcal{T}$. Пусть $G \leq W$ и P — группа подстановок, индуцированная действием группы G на $\mathcal{T}$. Скажем, что G — группа типа II (a), если $B \leq G$ и либо P примитивна на $\mathcal{T}$, либо $k = 2$ и $P = 1$.

II (b). Пусть H — группа подстановок на конечном множестве Y, причем H — либо почти простая примитивная группа подстановок, либо примитивная группа подстановок типа II (a). Положим $W = H\mathrm{wr}S_l$, где $l > 1$. Группа W естественным образом действует на $X = Y^l$. Пусть $K = \mathrm{Soc}(H)$, $B = K^l < W$. Скажем, что G — группа типа II (b), если $B \leq G \leq W$ и G транзитивно переставляет l множителей группы K^l.

II (c). Пусть P — транзитивная группа подстановок на множестве $\{1, \ldots, k\}$, $Q = P_1$ (стабилизатор единицы в P). Предположим, что существует гомоморфизм $\phi : Q \to \mathrm{Aut}(T)$ такой, что $\mathrm{Inn}(T) \le \mathrm{Im}(\phi)$. Положим

$$B = \Big\{ f : P \to T \mid f(ab) = f(a)^{\phi(b)},\ a \in P,\ b \in Q \Big\}.$$

Тогда B — группа относительно поточечного умножения, $B \cong T^k$. Пусть P действует на B следующим образом:

$$f^a(a') = f(aa'),\ f \in B,\ a, a' \in P.$$

Пусть G — соответствующее полупрямое произведение групп B и P, $G_x = P$ (таким образом, X есть множество левых смежных классов группы G по подгруппе P). Так определенная группа G является группой типа II (c), если она примитивна. Заметим, что в этом случае группа G содержится в группе $H \mathrm{wr} S_k$, где $H \cong T \times T$ — группа типа II (a).

Доказательство теоремы в случае, когда группа G — группа типа I, дается в § 3; в случае, когда группа G — группа типа II (a), — в § 4; в случае, когда группа G — группа типа II (b) или II (c), — в § 5.

Следующие предложения 1–12, касающиеся свойств конечных простых неабелевых групп, потребуются нам лишь при доказательстве теоремы в случае, когда группа G — группа типа II (a) (при $k \ne 2$ достаточно предложения 1).

Предложение 1 является одним из основных результатов работы [9].

Предложение 1. *Пусть T — конечная простая неабелева группа. Тогда либо $T = U_3(3)$, либо T порождается двумя элементами, один из которых есть инволюция, а другой — строго вещественный. В частности, для произвольной конечной простой группы T существуют элементы $t_1, t_2 \in T$ такие, что $C_{\mathrm{Aut}(T)}(t_1) \cap C_{\mathrm{Aut}(T)}(t_2) = 1$.*

Предложения 2–12, носящие технический характер, можно усилить, однако и в настоящем виде они позволяют доказать теорему.

Предложение 2. *Пусть $T = A_n$, где $n \ge 8$. Тогда существуют элементы $s_1, s_2 \in T$ такие, что $T = \langle s_1, s_2 \rangle$, $|s_1| \ne |s_2|$, $|s_1| \ne |s_1^{-1}s_2|$, $|s_2| \ne |s_1^{-1}s_2|$, $s_1^{\mathrm{Aut}(T)} = (s_1^{-1})^{\mathrm{Aut}(T)}$, $s_2^{\mathrm{Aut}(T)} = (s_2^{-1})^{\mathrm{Aut}(T)}$ и*

$$(*) \qquad |\mathrm{Inv}(\mathrm{Aut}(T))| + 3|s_1^{\mathrm{Aut}(T)}| + 2|s_2^{\mathrm{Aut}(T)}| < |T|.$$

Доказательство. Положим $s_1 = (123)$ и $s_2 = (12)(3...n)$, если n четное, и $s_2 = (3...n)$, если n нечетное. Непосредственно проверяется, что $|s_1| \ne |s_2|$, $|s_1| \ne |s_1^{-1}s_2|$ и $|s_2| \ne |s_1^{-1}s_2|$. Кроме того, хорошо известно, что $A_n = \langle s_1, s_2 \rangle$.

Докажем неравенство $(*)$. Известно, что если $s \in S_n$ и s в своем разложении на независимые циклы имеет c_i циклов длины i, $i \in \{1, ..., n\}$, то

$$|s^{S_n}| = \frac{n!}{\prod_{i=1}^n i^{c_i} \prod_{i=1}^n c_i!}.$$

Следовательно,

$$|\mathrm{Inv}(S_n)| = \sum_{k=1}^{\lfloor \frac{n}{2} \rfloor} \frac{n!}{2^k (n-2k)! k!}.$$

Кроме того, $|s_1^{S_n}| = \dfrac{n!}{3(n-3)!}$ и $|s_2^{S_n}| = \dfrac{n!}{2(n-2)}$. Поскольку

$$\sum_{k=1}^{\lfloor \frac{n}{2} \rfloor} \frac{n!}{2^k (n-2k)! k!} + 3\frac{n!}{3(n-3)!} + 2\frac{n!}{2(n-2)} < \frac{n!}{2}$$

при $n \ge 8$, то предложение доказано. □

Предложение 3. *Пусть $T = A_7$. Тогда существуют элементы s_1, $s_2 \in T$ такие, что $T = \langle s_1, s_2\rangle$, $|s_1| = 2$, $|s_2| \neq |s_1^{-1}s_2|$ и*

$$(**)\qquad |\mathrm{Inv}(\mathrm{Aut}(T))| + 3|s_1^{\mathrm{Aut}(T)}| + 4|C_T(s_1)||\mathrm{Out}(T)| < |T|.$$

Доказательство. Существуют s_1 и s_2 из T такие, что $T = \langle s_1, s_2\rangle$, $|s_1| = 2$, $|s_2| = 7$ и $|s_1^{-1}s_2| = 5$. Для группы T и так выбранных s_1 и s_2 неравенство $(**)$ проверяется непосредственно. □

Для конечной группы T положим $m(T) = \min\{|T : C_T(x)| \mid 1 \neq x \in \mathrm{Aut}(T)\}$.

Из [4] и предложения 1 следует справедливость следующего утверждения.

Предложение 4. *Пусть T — спорадическая простая группа, отличная от M_{11}, M_{12}, M_{22}, M_{23}, M_{24}, J_2, HS. Тогда существуют элементы s_1, $s_2 \in T$ такие, что $T = \langle s_1, s_2\rangle$, $|s_1| = 2$, $s_2^{\mathrm{Aut}(T)} = (s_2^{-1})^{\mathrm{Aut}(T)}$ и*

$$7\sqrt{\frac{2}{m(T)}} + 2\frac{|\mathrm{Out}(T)|}{m(T)} + \frac{1}{m(T)} < 1.$$

Предложение 5. *Пусть $T = M_{11}$. Тогда существуют элементы s_1, $s_2 \in T$ такие, что $T = \langle s_1, s_2\rangle$, $|s_1| = 2$, $|s_2| \neq |s_1^{-1}s_2|$, $s_2^{\mathrm{Aut}(T)} = (s_2^{-1})^{\mathrm{Aut}(T)}$ и*

$$|\mathrm{Inv}(\mathrm{Aut}(T))| + 3|s_1^{\mathrm{Aut}(T)}| + 2|s_2^{\mathrm{Aut}(T)}| < |T|.$$

Доказательство. Поскольку $T = M_{11}$, то $|T| = 7920$ и $|\mathrm{Inv}(\mathrm{Aut}(T))| = 165$. Пусть s_1 и s_2 — стандартные порождающие группы T, указанные в [11]. Имеем $|s_1| = 2$, $|s_2| = 4$, $|s_1^{-1}s_2| = 11$ и $s_2^{\mathrm{Aut}(T)} = (s_2^{-1})^{\mathrm{Aut}(T)}$. С использованием [4] проверяется, что $|s_1^{\mathrm{Aut}(T)}| = 165$ и $|s_2^{\mathrm{Aut}(T)}| = 1980$. Следовательно, выбранные s_1 и s_2 обладают требуемыми свойствами. □

Предложение 6. *Пусть T — одна из групп: M_{12}, M_{22}, M_{23}, M_{24}, J_2, HS. Тогда существуют элементы s_1, $s_2 \in T$ такие, что $T = \langle s_1, s_2\rangle$, $|s_1| = 2$, $|s_2| \neq |s_1^{-1}s_2|$ и*

$$|\mathrm{Inv}(\mathrm{Aut}(T))| + 3|s_1^{\mathrm{Aut}(T)}| + 4|s_2^{\mathrm{Aut}(T)}| < |T|.$$

Доказательство. Пусть s_1 и s_2 — стандартные порождающие группы T, указанные в [11]. Тогда с использованием [4] проверяется, что для T, s_1 и s_2 выполняются свойства, указанные в таблице 1.

Таблица 1

T	$\|T\|$	$\|\mathrm{Inv}(\mathrm{Aut}(T))\|$	$\|s_1\|$	$\|s_1^{\mathrm{Aut}(T)}\|$	$\|s_2\|$	$\|s_2^{\mathrm{Aut}(T)}\|$	$\|s_1^{-1}s_2\|$
M_{12}	95040	1683	2	≤ 495	3	≤ 4400	11
M_{22}	443520	2871	2	≤ 1155	4	≤ 41580	11
M_{23}	10200960	3795	2	≤ 3795	4	≤ 318780	23
M_{24}	244823040	43263	2	≤ 31878	3	≤ 226688	23
J_2	604800	165	2	≤ 2520	3	≤ 17360	7
HS	44352000	165	2	≤ 5775	5	≤ 24200	11

Непосредственная проверка показывает, что выбранные s_1 и s_2 обладают требуемыми свойствами. □

Предложение 7. *Пусть $T = L_2(q)$, где $q \geq 11$ или $q = 8$. Тогда существуют элементы s_1, $s_2 \in T$ такие, что $T = \langle s_1, s_2\rangle$, $|s_1| = 2$, $|s_2| \neq |s_1^{-1}s_2|$, $s_2^{\mathrm{Aut}(T)} = (s_2^{-1})^{\mathrm{Aut}(T)}$ и*

$$(***)\qquad |\mathrm{Inv}(\mathrm{Aut}(T))| + 3|s_1^{\mathrm{Aut}(T)}| + 2|s_2^{\mathrm{Aut}(T)}| < |T|.$$

Д о к а з а т е л ь с т в о. Положим $q = p^k$. Нам потребуются следующие известные факты [6, 7].

(i) Если $k = 1$, то $L_2(q) = \langle x, y\rangle$, где $|x| = 2$, $|x| = 3$ и $|xy| = p$.

(ii) Если $p = 2$ и $k > 1$, то $L_2(q) = \langle x, y\rangle$, где $|x| = 2$, $|x| = 3$ и $|xy| = q - 1$.

(iii) Если $p \neq 2$, и $k > 1$, то $L_2(q) = \langle x, y\rangle$, где $|x| = 2$, $|x| = 3$ и $|xy| = \dfrac{q-1}{2}$.

(iv) В группе $L_2(q)$ имеется всего один класс инволюций. Мощность этого класса равна $q^2 - 1$ при $q \equiv 0 (\mathrm{mod}\ 2)$, $\dfrac{q(q-1)}{2}$ при $q \equiv -1 (\mathrm{mod}\ 4)$ и $\dfrac{q(q+1)}{2}$ при $q \equiv 1 (\mathrm{mod}\ 4)$

(v) Если $p = 3$, то в группе $L_2(q)$ имеется два класса элементов порядка 3. Эти классы переставляются внешним автоморфизмом и имеют мощности, равные $\dfrac{q^2-1}{2}$.

(vi) Если $p \neq 3$, то в группе $L_2(q)$ имеется всего один класс элементов порядка 3. Если $q \equiv -1 (\mathrm{mod}\ 3)$, то мощность этого класса равна $q(q-1)$. Если $q \equiv 1 (\mathrm{mod}\ 3)$, то мощность этого класса равна $q(q+1)$.

(vii) $|L_2(q)| = \dfrac{q(q^2-1)}{(2, q-1)}$.

(viii) Если $p = 2$ и k — нечетное, то $|\mathrm{Inv}(\mathrm{Aut}(T))| = |\mathrm{Inv}(T)| = q^2 - 1$.

(ix) Если $p = 2$ и k — четное, то $|\mathrm{Inv}(\mathrm{Aut}(T))| = |\mathrm{Inv}(T)| + \dfrac{\sqrt{q}(q+1)}{2} = q^2 - 1 + \dfrac{\sqrt{q}(q+1)}{2}$.

(x) Если $p \neq 2$ и k — нечетное, то $|\mathrm{Inv}(\mathrm{Aut}(T))| = |\mathrm{Inv}(T)| + \dfrac{q(q-\delta)}{2} = q^2$, где $|\delta| = 1$ и $\delta \equiv q (\mathrm{mod}\ 4)$.

(xi) Если $p \neq 2$ и k — четное, то $|\mathrm{Inv}(\mathrm{Aut}(T))| = |\mathrm{Inv}(T)| + \dfrac{q(q-\delta)}{2} + \sqrt{q}(q+1) = q^2 + \sqrt{q}(q+1)$, где $|\delta| = 1$ и $\delta \equiv q (\mathrm{mod}\ 4)$.

Полагаем $s_1 = x$ и $s_2 = y$, где x и y — из пунктов (i)–(iii). Неравенство $(***)$ проверяется непосредственно с использованием перечисленных свойств группы $L_2(q)$. □

Предложение 8. *Пусть T — конечная простая группа лиева типа, отличная от $L_2(q)$ $(q \geq 4)$, $L_3(q)$ $(q \leq 13)$, $L_4(q)$ $(q \leq 5)$, $L_5(q)$ $(q \leq 3)$, $L_6(2)$, $L_7(2)$, $U_3(q)$ $(q \leq 8)$, $U_4(q)$ $(q \leq 3)$, $U_5(2)$, $S_4(4)$, $S_4(5)$, $S_6(2)$, $S_8(2)$, $O_8^-(2)$, $O_{10}^-(2)$, $O_8^+(2)$, $O_8^+(3)$, $Suz(8)$, $G_2(3)$, $G_2(4)$, $F_4(2)$, $F_4(3)$, ${}^2F_4(2)'$, ${}^2E_6(2)$, $E_7(2)$, $E_7(3)$. Тогда существуют элементы s_1, $s_2 \in T$ такие, что $T = \langle s_1, s_2\rangle$, $|s_1| = 2$, $s_2^{\mathrm{Aut}(T)} = (s_2^{-1})^{\mathrm{Aut}(T)}$ и*

$$7\sqrt{\frac{2}{m(T)}} + 2\frac{|s_2^{\mathrm{Aut}(T)}|}{|T|} + \frac{1}{m(T)} < 1.$$

Д о к а з а т е л ь с т в о. Известно [9, 10], что если T является конечной простой группой лиева типа, отличной от $U_3(3)$, то T порождается двумя элементами s_1 и s_2, где $s_1^2 = 1$, а элемент s_2, выбираемый из тора, является строго вещественным и полупростым.

Пусть T — конечная простая группа лиева типа, отличная от групп, перечисленных в условии предложения 8. Тогда из [9, 10] с использованием [4] следует, что существуют элементы s_1, s_2 такие, что $T = \langle s_1, s_2\rangle$, $s_1^2 = 1$, $s_2^{\mathrm{Aut}(T)} = (s_2^{-1})^{\mathrm{Aut}(T)}$, причем для T и s_2 выполняются свойства, указанные в таблице 2.

Непосредственная проверка показывает теперь, что s_1 и s_2 обладают требуемыми свойствами. □

Т а б л и ц а 2

T	$m(T)$	$\frac{\lvert s_2^{\mathrm{Aut}(T)}\rvert}{\lvert T\rvert}$
$A_n(q), n \geq 2$	≥ 233	$\leq \frac{2\log_p(q)(n+1,q-1)}{q^n-1}$
${}^2A_n(q), n \geq 2$	≥ 279	$\leq \frac{2\log_p(q)(n+1,q+1)(q+1)}{q^{n+1}-(-1)^{n+1}}$
$B_n(q), n \geq 2, p = 2$	≥ 350	$\leq \frac{2\log_p(q)}{q^n-1}$
$C_n(q), p = 2$	≥ 314	$\leq \frac{\log_p(q)}{q^n-1}$
$C_n(q), p \neq 2$	≥ 314	$\leq \frac{4\log_p(q)}{q^n-1}$
${}^2D_n(q), n \geq 2, (4, q^n+1) = 4$	≥ 764	$\leq \frac{32\log_p(q)}{(q^{n-1}+1)(q-1)}$
${}^2D_n(q), n \geq 2, (4, q^n+1) = 2$	≥ 764	$\leq \frac{8\log_p(q)}{(q^{n-1}+1)(q-1)}$
${}^2D_n(q), n \geq 2, (4, q^n+1) = 1$	≥ 764	$\leq \frac{2\log_p(q)}{(q^{n-1}+1)(q-1)}$
$D_n(q), n \geq 5$, n нечетное, $(4, q^n-1) = 4$	≥ 495	$\leq \frac{16\log_p(q)}{q^n-1}$
$D_n(q), n \geq 5$, n нечетное, $(4, q^n-1) = 2$	≥ 495	$\leq \frac{8\log_p(q)}{q^n-1}$
$D_n(q), n \geq 5$, n нечетное, $(4, q^n-1) = 1$	≥ 495	$\leq \frac{2\log_p(q)}{q^n-1}$
$D_n(q), n \neq 4$, n четное, $(4, q^n-1) = 4$	≥ 495	$\leq \frac{8\log_p(q)(2,q-1)^2}{(q^{\frac{n}{2}}+(-1)^{\frac{n}{2}})^2}$
$D_n(q), n \neq 4$, n четное, $(4, q^n-1) = 2$	≥ 495	$\leq \frac{4\log_p(q)(2,q-1)^2}{(q^{\frac{n}{2}}+(-1)^{\frac{n}{2}})^2}$
$D_n(q), n \neq 4$, n четное, $(4, q^n-1) = 1$	≥ 495	$\leq \frac{\log_p(q)(2,q-1)^2}{(q^{\frac{n}{2}}+(-1)^{\frac{n}{2}})^2}$
$D_4(q), (4, q^4-1) = 4$	≥ 495	$\leq \frac{24\log_p(q)(2,q-1)^2}{(q^2+1)^2}$
$D_4(q), (4, q^4-1) = 2$	≥ 495	$\leq \frac{12\log_p(q)(2,q-1)^2}{(q^2+1)^2}$
$D_4(q), (4, q^4-1) = 1$	≥ 495	$\leq \frac{3\log_p(q)(2,q-1)^2}{(q^2+1)^2}$
${}^2B_2(q), q = 2^{2n+1}, n \geq 2$	≥ 1000	$\leq \frac{\log_2(q)}{q+\sqrt{2q}+1}$
${}^3D_4(q)$	≥ 818	$\leq \frac{3\log_p(q)}{q^4-q^2+1}$
$G(q)$	≥ 1000	$\leq \frac{\log_p(q)}{q^2-q+1}$
${}^2G_2(q), q = 3^{2n+1}, n > 1$	≥ 1000	$\leq \frac{\log_3(q)}{q+\sqrt{3q}+1}$
$F_4(q)$	≥ 1000	$\leq \frac{\log_p(q)}{q^4-q^2+1}$
${}^2F_4(q), q = 2^{2n+1}, n \geq 1$	≥ 1000	$\leq \frac{\log_p(q)}{q^2+q\sqrt{2q}+q+\sqrt{2q}+1}$
$E_6(q)$	≥ 1000	$\leq \frac{\log_p(q)(3,q-1)}{q^6+q^3+1}$
${}^2E_6(q)$	≥ 1000	$\leq \frac{\log_p(q)(3,q+1)}{q^6-q^3+1}$
$E_7(q), q \neq 2, 3$	≥ 1000	$\leq \frac{\log_p(q)(2,q-1)}{(q^6-q^3+1)(q-1)}$
$E_8(q)$	≥ 1000	$\leq \frac{\log_p(q)}{q^8+q^7-q^5-q^4-q^3+q+1}$

Предложение 9. *Пусть T — одна из групп:* $L_3(3)$, $L_3(4)$, $L_3(5)$, $L_3(7)$, $L_3(8)$, $L_4(3)$, $L_5(2)$ $U_3(3)$, $U_3(4)$, $U_4(2)$, $U_4(3)$, $U_5(2)$, $S_4(4)$, $S_4(5)$, $S_6(2)$, $S_8(2)$, $O_8^-(2)$, $O_{10}^-(2)$, $O_8^+(2)$, $Sz(8)$, $G_2(3)$, $G_2(4)$, $F_4(2)$, ${}^2F_4(2)'$, ${}^2E_6(2)$. *Тогда существуют элементы* s_1, $s_2 \in T$ *такие, что* $T = \langle s_1, s_2\rangle$, $|s_1| = 2$, $|s_2| \neq |s_1^{-1}s_2|$ *и*

$$|\mathrm{Inv}(\mathrm{Aut}(T))| + 3|s_1^{\mathrm{Aut}(T)}| + 4|C_T(s_1)||\mathrm{Out}(T)| < |T|.$$

Доказательство. Пусть s_1 и s_2 — стандартные порождающие группы T, указанные в [11]. Тогда с использованием [4] проверяется, что для T, s_1 и s_2 выполняются свойства, указанные в таблице 3.

Таблица 3

T	$\lvert\mathrm{Out}(T)\rvert$	$\lvert\mathrm{Inv}(T)\rvert$	$\lvert\mathrm{Inv}(\mathrm{Aut}(T))\rvert$	$\lvert s_1\rvert$	$\lvert s_2\rvert$	$\lvert s_1^{-1}s_2\rvert$	$\lvert C_T(s_1)\rvert$
$L_3(3)$	2	117	351	2	3	13	48
$L_3(4)$	12	315	1051	2	4	7	64
$L_3(5)$	2	775	3875	2	3	31	480
$L_3(7)$	6	2793	8379	2	3	19	672
$L_3(8)$	6	4599	37303	2	3	21	3584
$L_4(3)$	4	7371	8451	2	4	13	2880
$L_5(2)$	2	6975	20863	2	5	21	21504
$U_3(3)$	2	63	315	2	6	7	96
$U_3(4)$	4	195	1235	2	3	13	320
$U_4(2)$	2	315	891	2	5	9	576
$U_4(3)$	8	2835	18243	2	6	7	1152
$U_5(2)$	2	3135	22143	2	5	11	82944
$S_4(4)$	4	4335	5695	2	5	17	3840
$S_4(5)$	2	10075	16875	2	3	13	480
$S_6(2)$	1	5103	5103	2	7	9	23040
$S_8(2)$	1	1371135	1371135	2	5	17	8847360
$O_8^-(2)$	2	69615	112591	2	3	17	3072
$O_{10}^-(2)$	2	21999615	58756863	2	5	33	1274019840
$O_8^+(2)$	6	69615	107535	2	5	12	3072
$Sz(8)$	3	455	455	2	4	13	64
$G_2(3)$	2	7371	10179	2	3	13	576
$G_2(4)$	2	69615	90415	2	5	13	61440
$F_4(2)$	2	355384575	447507711	2	3	17	754974720
${}^2F_4(2)'$	2	13455	13455	2	3	13	10240
${}^2E_6(2)$	6	1323080482815	2932165771263	2	3	19	24352464568320

Непосредственная проверка показывает теперь, что выбранные s_1 и s_2 обладают требуемыми свойствами. □

Предложение 10. *Пусть* $T = U_3(5)$. *Тогда существуют элементы* s_1, $s_2 \in T$ *такие, что* $T = \langle s_1, s_2\rangle$, $|s_1| \neq |s_2|$, $|s_1| \neq |s_1^{-1}s_2|$, $|s_2| \neq |s_1^{-1}s_2|$, $s_1^{\mathrm{Aut}(T)} = (s_1^{-1})^{\mathrm{Aut}(T)}$ *и*

$$|\mathrm{Inv}(\mathrm{Aut}(T))| + 3|s_1^{\mathrm{Aut}(T)}| + 4|s_2^{\mathrm{Aut}(T)}| < |T|.$$

Доказательство. Поскольку $T = U_3(5)$, то $|T| = 126000$, $|\mathrm{Inv}(\mathrm{Aut}(T))| = 1575$. Кроме того, согласно [11] существуют такие порождающие s_1 и s_2 группы T, что $|s_1| = 3$, $|s_2| = 5$, $|s_1^{-1}s_2| = 7$ и $s_1^{\mathrm{Aut}(T)} = (s_1^{-1})^{\mathrm{Aut}(T)}$, причем (см. [4]) $|s_1^{\mathrm{Aut}(T)}| = 3500$ и $|s_2^{\mathrm{Aut}(T)}| \leq 15624$. □

Предложение 11. *Пусть* $T = L_3(9)$. *Тогда существуют элементы* s_1, $s_2 \in T$ *такие, что* $T = \langle s_1, s_2 \rangle$, $|s_1| = 2$ *и*

$$2|\mathrm{Inv}(\mathrm{Aut}(T))| + 3|\mathrm{Inv}(T)| + 4|C_T(s_1)||\mathrm{Out}(T)| + \max\{|C_T(x)| \mid 1 \neq x \in \mathrm{Aut}(T)\} < |T|.$$

Доказательство. Поскольку $T = L_3(9)$, то согласно [4] имеем $|T| = 42456960$, $|\mathrm{Inv}(T)| = 7371$, $|\mathrm{Inv}(\mathrm{Aut}(T))| = 80919$, $|\mathrm{Out}(T)| = 4$ и $\max\{|C_T(x)| \mid 1 \neq x \in \mathrm{Aut}(T)\} = 6048$. Согласно предложению 1 существуют элементы s_1, $s_2 \in T$ такие, что $T = \langle s_1, s_2 \rangle$ и $|s_1| = 2$, причем (см. [4]) $|C_T(s_1)| = 5760$. Нетрудно видеть, что для T и s_1 выполняется указанное неравенство. □

Предложение 12. *Пусть* T *— одна из групп:* $L_3(11)$, $L_3(13)$, $L_5(3)$, $O_8^+(3)$, $F_4(3)$, $E_7(2)$, $E_7(3)$. *Тогда существуют элементы* s_1, $s_2 \in T$ *такие, что* $T = \langle s_1, s_2 \rangle$, $|s_1| = 2$, $(s_2^{-1})^{\mathrm{Aut}(T)} = s_2^{\mathrm{Aut}(T)}$ *и*

$$7\sqrt{\frac{2}{m(T)}} + 2\frac{|\mathrm{Out}(T)|}{m(T)} + \frac{1}{m(T)} < 1.$$

Доказательство. Согласно предложению 1 существуют элементы s_1, $s_2 \in T$ такие, что $T = \langle s_1, s_2 \rangle$, $|s_1| = 2$ и $(s_2^{-1})^{\mathrm{Aut}(T)} = s_2^{\mathrm{Aut}(T)}$. С использованием [4] проверяется, что для T выполняются свойства, указанные в таблице 4.

Таблица 4

T	$m(T)$	$\lvert\mathrm{Out}(T)\rvert$
$L_3(11)$	≥ 133	2
$L_3(13)$	≥ 183	6
$L_5(3)$	≥ 121	2
$O_8^+(3)$	≥ 1000	24
$F_4(3)$	≥ 1000	1
$E_7(2)$	≥ 1000	1
$E_7(3)$	≥ 1000	2

Непосредственная проверка показывает, что требуемое неравенство выполняется. □

Предложение 13. *Пусть* T *— одна из групп:* $L_4(4)$, $L_4(5)$, $L_6(2)$, $L_7(2)$. *Тогда существуют элементы* s_1, $s_2 \in T$ *такие, что* $T = \langle s_1, s_2 \rangle$, $|s_1| = 2$, $|s_2| \neq |s_1^{-1}s_2|$ *и*

$$5\sqrt{\frac{2}{m(T)}} + 4\frac{|\mathrm{Out}(T)|}{m(T)} < 1.$$

Доказательство. Пусть s_1 и s_2 — стандартные порождающие группы T, указанные в [11]. Тогда с использованием [4] проверяется, что для T, s_1 и s_2 выполняются свойства, указанные в таблице 5.

Таблица 5

T	$m(T)$	$\lvert\mathrm{Out}(T)\rvert$	$\lvert s_1\rvert$	$\lvert s_2\rvert$	$\lvert s_1^{-1}s_2\rvert$
$L_4(4)$	≥ 85	4	2	4	30
$L_4(5)$	≥ 165	8	2	3	39
$L_6(2)$	≥ 63	2	2	6	63
$L_7(2)$	≥ 127	2	2	7	127

Непосредственная проверка показывает теперь, что выбранные T, s_1 и s_2 обладают требуемыми свойствами. □

3. Доказательство теоремы в случае, когда G — группа типа I

В этом параграфе теорема будет доказана в случае, когда G является группой типа I из теоремы О'Нэна — Скотта (см. § 2).

В рассматриваемом случае $T = \mathbb{Z}_p$ для некоторого простого числа p и $B = \mathbb{Z}_p^k$ является единственной минимальной нормальной подгруппой группы G. Группа B действует регулярно на X, $|X| = p^k$, $G \leq AGL(k,p)$, причем B — группа трансляций из $AGL(k,p)$. Нам будет удобно зафиксировать на X некоторую структуру векторного пространства $V(k,p)$, определяемую группой B. Пусть e_1, e_2, …, e_k — некоторый базис так определенного векторного пространства X.

Ниже будет указано, в случае его существования, подмножество R множества X со свойством $G_{\{R\}} = 1$.

Случай 1. $k \geq 3$ и $p \geq 3$.

Положим $R = \{0, e_1, e_2, \ldots, e_k, 2e_1, 2e_2, \ldots, 2e_k, e_1 + e_2, e_2 + e_3, \ldots, e_{k-1} + e_k, e_1 + 2e_2\}$. Покажем, что $AGL(k,p)_{\{R\}} = 1$. Пусть $g \in AGL(k,p)$ и $g(R) = R$. Заметим, что 0 является единственной точкой из X, через которую проходят k прямых ассоциированного с X аффинного пространства так, что они содержат по 3 точки из R. Тогда $g(0) = 0$. Поскольку этими прямыми являются прямые вида $\langle e_i \rangle$, $i \in \{1, \ldots, k\}$, то для любого $i \in \{1, \ldots, k\}$ имеем $g(\langle e_i \rangle) = \langle e_j \rangle$, где $j \in \{1, \ldots, k\}$. Для произвольных $1 \leq i < j \leq k$ плоскость $\langle e_i, e_j \rangle$ содержит не менее 6 точек из R тогда и только тогда, когда $j = i + 1$. Кроме того, лишь при $i \in \{1, k-1\}$ существует точно одно $j \in \{1, \ldots, k-1\}$ такое, что $|\langle e_i, e_{i+1} \rangle \cap \langle e_j, e_{j+1} \rangle \cap R| = 3$. Поэтому $g(e_k) \in \{e_1, 2e_1, e_k, 2e_k\}$ и $g(e_{k-1}) \in \{e_2, 2e_2, e_{k-1}, 2e_{k-1}\}$. Так как $|\langle e_1, e_2 \rangle \cap R| = 7$, а $|\langle e_k, e_{k-1} \rangle \cap R| = 6$, то $g(\langle e_k, e_{k-1} \rangle) = \langle e_k, e_{k-1} \rangle$. Следовательно, $g(e_k) \in \{e_k, 2e_k\}$ и $g(e_{k-1}) \in \{e_{k-1}, 2e_{k-1}\}$. Поскольку $g(e_k + e_{k-1}) = e_k + e_{k-1}$, то $g(e_k) = e_k$ и $g(e_{k-1}) = e_{k-1}$. Но тогда $g(\langle e_{k-2}, e_{k-1} \rangle) = \langle e_{k-2}, e_{k-1} \rangle$. Продолжая этот процесс, получаем, что $g(e_i) = e_i$ для любого $i \in \{1, \ldots, k\}$, т.е. $g = 1$.

Поскольку $AGL(k,p)_{\{R\}} = 1$, то $G_{\{R\}} = 1$ для произвольной группы $G \leq AGL(k,p)$.

Случай 2. $k \geq 4$ и $p = 2$.

Положим $R = \{0, e_1, e_2, \ldots, e_k, e_1 + e_2, e_2 + e_3, \ldots, e_{k-1} + e_k, e_1 + e_2 + e_3\}$. Покажем, что $AGL(k,2)_{\{R\}} = 1$. Пусть $g \in AGL(k,2)$ и $g(R) = R$. Поскольку 0 является единственной точкой из R, которая содержится в наибольшем количестве двумерных подпространств, содержащих четыре точки из R, в аффинном пространстве, ассоциированном с X, то $g(0) = 0$.

Теперь рассуждения, аналогичные рассуждениям предыдущего случая, показывают, что $g(e_i) = e_i$ для любого $i \in \{1, \ldots, k\}$, т.е. $g = 1$.

Поскольку $AGL(k,2)_{\{R\}} = 1$, то $G_{\{R\}} = 1$ для произвольной группы $G \leq AGL(k,2)$.

Случай 3. $k = 3$ и $p = 2$.

Если $G = AGL(3,2)$ или G — максимальная подгруппа группы $AGL(3,2)$ с $G_x \cong \mathbb{Z}_7 \rtimes \mathbb{Z}_3$, $x \in X$, то подмножества R со свойством $G_{\{R\}} = 1$ не существует.

Остается возможность $G_x \cong \mathbb{Z}_7$, $x \in X$, и в качестве R со свойством $G_{\{R\}} = 1$ можно взять произвольное подмножество множества X, состоящее из трех элементов.

Случай 4. $k = 2$ и $p > 7$.

Положим $R = \{0, e_1, 3e_1, 2e_2, 3e_2\}$. Покажем, что $AGL(2,p)_{\{R\}} = 1$. Пусть $g \in AGL(2,p)$ и $g(R) = R$. Тогда g оставляет на месте прямую, содержащую точки 0 и e_1, и прямую, содержащую точки 0 и e_2. Отсюда легко следует, что $g = 1$.

Поскольку $AGL(2,p)_{\{R\}} = 1$, то $G_{\{R\}} = 1$ для произвольной группы $G \leq AGL(2,p)$.

Случай 5. $k = 2$ и $p = 7$.

Положим $R = \{0, e_1, 3e_1, -e_1, e_2, 2e_2\}$. Покажем, что $AGL(2,7)_{\{R\}} = 1$. Пусть $g \in AGL(2,7)$ и $g(R) = R$. Поскольку $g(0) = 0$, то g оставляет на месте прямую, содержащую точки 0 и e_1, и прямую, содержащую точки 0 и e_2. Тогда $g(e_1) = e_1$ и $g(e_2) = e_2$, т.е. $g = 1$.

Поскольку $AGL(2,7)_{\{R\}} = 1$, то $G_{\{R\}} = 1$ для произвольной группы $G \leq AGL(2,7)$.

Случай 6. $k = 2$ и $p = 5$.

Положим $R = \{0, e_1, 3e_1, e_2, 2e_2, e_1 + e_2.\}$ Покажем, что $AGL(2,5)_{\{R\}} = 1$. Пусть $g \in AGL(2,5)$ и $g(R) = R$. Поскольку $g(0) = 0$, то g оставляет на месте прямую, содержащую точки 0 и e_1, и прямую, содержащую точки 0 и e_2. Тогда $g(e_1) = e_1$ и $g(e_2) = e_2$, т.е. $g = 1$.

Поскольку $AGL(2,5)_{\{R\}} = 1$, то $G_{\{R\}} = 1$ для произвольной группы $G < AGL(2,5)$.

Случай 7. $k = 2$ и $p = 3$.

Если $G = AGL(2,3)$, $G = ASL(2,3)$ или G — подгруппа $AGL(2,3)$ такая, что G_x есть силовская 2-подгруппа из $GL(2,3)$, то подмножества R со свойством $G_{\{R\}} = 1$ не существует.

В случае, когда G — подгруппа группы $AGL(2,3)$, отличная от перечисленных, легко показать, что $G_{\{R\}} = 1$ при $R = \{0, e_1, 2e_1, e_2\}$.

Случай 8. $k = 2$ и $p = 2$.

Если $G \leq AGL(2,2)$, то подмножества R со свойством $G_{\{R\}} = 1$ не существует.

Случай 9. $k = 1$ и $p > 7$.

Положим $R = \{0, e_1, 3e_1\}$. Легко показать, что $AGL(1,p)_{\{R\}} = 1$.

Поскольку $AGL(1,p)_{\{R\}} = 1$, то $G_{\{R\}} = 1$ для произвольной группы $G \leq AGL(1,p)$.

Случай 10. $k = 1$ и $p = 7$.

Если $G = AGL(1,7)$, то подмножества R со свойством $G_{\{R\}} = 1$ не существует.

Пусть $G < AGL(1,7)$, тогда $|G_x| \in \{2,3\}$. Если $|G_x| = 2$, то группа G подстановочно изоморфна D_{14} в естественном действии на 7 точках и $G_{\{R\}} = 1$ при $R = \{0,\ e_1,\ 3e_1\}$. Если $|G_x| = 3$, то легко показать, что $G_{\{R\}} = 1$ при $R = \{0,\ e_1,\ 2e_1\}$.

Случай 11. $k = 1$ и $p = 5$.

Если $G = AGL(1,5)$, то подмножества R со свойством $G_{\{R\}} = 1$ не существует.

Если $G < AGL(1,5)$, то либо G подстановочно изоморфна D_{10} в естественном действии на 5 точках и множества R со свойством $G_{\{R\}} = 1$ не существует, либо $G \cong \mathbb{Z}_5$ и $G_x = 1$, $x \in X$.

Случай 12. $k = 1$ и $p = 3$.

Если $G = AGL(1,3)$, то подмножества R со свойством $G_{\{R\}} = 1$ не существует. В остальных случаях стабилизатор точки единичен.

Случай 13. $k = 1$ и $p = 2$.

В этом случае $G_{\{R\}} = 1$ при $R = \{0\}$.

Справедливость теоремы в случае, когда G — группа типа I, доказана.

З а м е ч а н и е. Из приведенного доказательства следует, что если $G \leq AGL(k,p)$ и существует подмножество множества X, глобальный стабилизатор которого в группе G тривиален, то существует подмножество R множества X такое, что $|R| \leq 3k + 1$ и $G_{\{R\}} = 1$. В то же время очевидно, что если $AGL(k,p)_{\{R\}} = 1$ для некоторого подмножества R множества X, то $|R| > k$.

4. Доказательство теоремы в случае, когда G — группа типа II (a)

В этом параграфе теорема будет доказана в случае, когда G является группой типа II (a) из теоремы О'Нэна — Скотта (см. § 2).

Имеем

$$W = \{(a_1,\ \ldots,\ a_k).\pi \mid a_i \in \mathrm{Aut}(T),\ \pi \in S_k,\ a_i \equiv a_j (\mathrm{mod\ Inn}(T)),\ i,j \in \{1,\ \ldots,\ k\}\},$$

где элементы $\pi \in S_k$ переставляют естественным образом компоненты a_i, а действие W на X таково, что

$$W_x = \{(a,\ \ldots,\ a).\pi \mid a \in \mathrm{Aut}(T),\ \pi \in S_k\}$$

для некоторого $x \in X$. Таким образом, элементами множества X являются левые смежные классы $(x_1, \ldots, x_k).1G_x$, где $x_1, \ldots, x_k \in \mathrm{Inn}(T)$, которые нам будет удобно обозначать через $[x_1, \ldots, x_k]$ (следовательно, $[x_1, \ldots, x_k] = [x'_1, \ldots, x'_k]$ тогда и только тогда, когда $x_i^{-1}x'_i = x_j^{-1}x'_j$

для всех $i, j \in \{1, \ldots, k\}$). В этих обозначениях для $g = (g_1, \ldots, g_k).\sigma \in W$ и $[x_1, \ldots, x_k] \in X$ имеем

$$g\big([x_1, \ldots, x_k]\big) = \big[g_1 x_{\sigma(1)}, \ldots, g_k x_{\sigma(k)}\big] = \big[1, g_2 x_{\sigma(2)} x_{\sigma(1)}^{-1} g_1^{-1}, \ldots, g_k x_{\sigma(k)} x_{\sigma(1)}^{-1} g_1^{-1}\big].$$

Для доказательства теоремы в случае, когда G — группа типа II (a), положим $G = W$ и покажем, что существует такое подмножество R множества X, что $G_{\{R\}} = 1$.

Случай 1. $k > 2$.

В силу предложения 1 имеем $C_{\mathrm{Aut}(T)}(t_1) \cap C_{\mathrm{Aut}(T)}(t_2) = 1$ для некоторых элементов t_1, $t_2 \in T$. В качестве множества R возьмем подмножество множества X, состоящее из элементов $[1, 1, \ldots, 1, t_1]$, $[1, 1, \ldots, t_1, t_1]$, $\ldots$, $[1, t_1, \ldots, t_1, t_1]$ и элемента $[1, t_2, \ldots, t_2, t_2]$. Покажем, что если $g = (g_1, \ldots, g_k).\sigma \in G$ и $g(R) = R$, то $g = 1$.

Пусть $K = \{1, \ldots, k\}$ и $i \in K \setminus \{1, k\}$. Тогда i-е координаты элементов из $g(R)$ — это $g_i g_1^{-1}$, $g_i t_1 g_1^{-1}$, $g_i t_2 g_1^{-1}$, если $\sigma(1) = 1$; $g_i g_1^{-1}$, $g_i t_1 g_1^{-1}$, если $1 \neq \sigma(1) < \sigma(i)$; $g_i g_1^{-1}$, $g_i t_1^{-1} g_1^{-1}$, если $1 \neq \sigma(1) > \sigma(i)$. Таким образом, если $\sigma(1) \neq 1$, то множество значений i-й координаты элементов из R состоит не более, чем из двух элементов, что противоречит выбору R. Следовательно, $\sigma(1) = 1$ и $g([x_1, \ldots, x_k]) = [1, g_2 x_{\sigma(2)} g_1^{-1}, \ldots, g_k x_{\sigma(k)} g_1^{-1}]$.

Покажем, что $\sigma(k) = k$ и $g = (g_1, g_1^{t_2}, \ldots, g_1^{t_2}).\sigma$. Пусть $\sigma(k) = i$, где $i \in K$. Тогда множество значений i-й координаты элементов из R состоит из элементов $g_i t_1 g_1^{-1}$, $g_i t_2 g_1^{-1}$ и, в частности, содержит не более двух элементов. По выбору R отсюда следует, что либо $i = 1$, либо $i = k$. Поскольку $\sigma(1) = 1$, то $\sigma(k) = k$, откуда $g_k t_1 g_1^{-1} = t_1$ и $g_k t_2 g_1^{-1} = t_2$. Поскольку теперь $g([1, t_2, \ldots, t_2]) = [1, g_2 t_2 g_1^{-1}, \ldots, g_{k-1} t_2 g_1^{-1}, t_2] \in R$, то $g([1, t_2, \ldots, t_2]) = [1, t_2, \ldots, t_2]$. Поэтому $g_i t_2 g_1^{-1} = t_2$ для любого $i \in K \setminus \{1\}$. Таким образом, имеем $g = (g_1, g_1^{t_2}, \ldots, g_1^{t_2}).\sigma$.

Покажем, что $g_1 = 1$. Имеем $g([1, \ldots, 1, t_1]) = [1, g_1^{t_2} g_1^{-1}, \ldots, g_1^{t_2} g_1^{-1}, g_1^{t_2} t_1 g_1^{-1}] \in R$. Поскольку $t_1 \neq 1$, отсюда следует, что $[1, g_1^{t_2} g_1^{-1}, \ldots, g_1^{t_2} g_1^{-1}, g_1^{t_2} t_1 g_1^{-1}] = [1, 1, \ldots, 1, t_1]$. Таким образом, $g_1^{t_2} g_1^{-1} = 1$ и $g_1^{t_2} t_1 g_1^{-1} = t_1$. Следовательно, $g_1^{t_2} = g_1$ и $t_1 = g_1^{t_2} t_1 g_1^{-1} = g_1 t_1 g_1^{-1}$. Отсюда $g_1 \in C_{\mathrm{Aut}(T)}(t_1) \cap C_{\mathrm{Aut}(T)}(t_2) = 1$.

Итак, $g = (g_1, g_1^{t_2}, \ldots, g_1^{t_2}).\sigma = (1, \ldots, 1).\sigma$, что с учетом $g(R) = R$ влечет за собой, очевидно, $g = 1$.

Случай 2. $k = 2$.

Пусть $s_1 \in T$ и Γ — (неориентированный) граф, построенный по орбиталу группы G на X, содержащему $([1, 1], [1, s_1])$. (Заметим, что этот орбитал самодвойственный, поскольку $(s_1, s_1^2).\pi[1, 1] = [1, s_1]$ и $(s_1, s_1^2).\pi[1, s_1] = [s_1^2, s_1^2] = [1, 1]$ для $\pi \in S_2 \setminus \{1\}$.) Кроме того, если $[1, x], [1, y] \in V(\Gamma)$, то $\{[1, x], [1, y]\} \in E(\Gamma)$ тогда и только тогда, когда $x^{-1} y \in s_1^{\mathrm{Aut}(T)} \cup (s_1^{-1})^{\mathrm{Aut}(T)}$.

Предположим, что $T = A_5$. Положим $s_1 = (12)(34)$ и $s_2 = (135)$. Непосредственно проверяется, что глобальный стабилизатор множества $\{[1, 1], [1, s_2], [1, s_2^2 s_1]\} \cup \Gamma([1, 1])$ в группе G тривиален.

Далее считаем, что $T \neq A_5$. Покажем, что можно выбрать элементы s_1, s_2 и s_3 из T так, что глобальный стабилизатор множества $\{[1, 1], [1, s_1], [1, s_2], [1, s_3]\}$ в группе G тривиален.

Лемма 1. *Пусть $s_1, s_2, s_3 \in T$ таковы, что $C_{\mathrm{Aut}(T)}(s_1) \cap C_{\mathrm{Aut}(T)}(s_2) = 1$, $|s_1| \neq |s_2|$, $|s_1| \neq |s_1^{-1} s_2|$ и выполнены следующие условия:*

(i) *если $g \in \mathrm{Aut}(T)$, $g^2 = 1$, $g s_1 g^{-1} = s_1^{-1}$ и $g s_2 g^{-1} = s_2^{-1}$, то $s_3 \neq g s_3^{-1} g^{-1}$;*

(ii) $s_3 \notin s_1^{\mathrm{Aut}(T)} \cup (s_1^{-1})^{\mathrm{Aut}(T)} \cup s_1 s_1^{\mathrm{Aut}(T)} \cup s_1 (s_1^{-1})^{\mathrm{Aut}(T)} \cup s_2 s_1^{\mathrm{Aut}(T)} \cup s_2 (s_1^{-1})^{\mathrm{Aut}(T)}$;

(iii) *если $g \in C_{\mathrm{Aut}(T)}(s_1)$ и $g^2 = 1$, то $s_3 \neq g s_2 g^{-1}$;*

(iv) *если $g \in \mathrm{Aut}(T)$, $g^2 = 1$ и $g s_1 g^{-1} = s_1^{-1}$, то $s_3 \neq g s_2^{-1} g^{-1}$;*

(v) *если $g \in \mathrm{Aut}(T)$, $g^2 = 1$, $g s_1 g^{-1} = s_1^{-1}$ и $g s_2 g^{-1} = s_1^{-1} s_2$, то $s_3 g s_3^{-1} \neq s_1 g$;*

(vi) *если $g \in C_{\mathrm{Aut}(T)}(s_1)$, $g^2 = s_1^{-1}$ и $g s_2 g^{-1} = s_2^{-1} s_1$, то $s_3 \notin g^{-1} \mathrm{Inv}(\langle T, g \rangle)$;*

(vii) *если $g \in \mathrm{Aut}(T)$, $g^2 = 1$ и $g s_1 g^{-1} = s_1^{-1}$, то $s_3 \neq s_1 g s_2 g^{-1}$;*

(viii) *если* $g \in C_{\mathrm{Aut}(T)}(s_1)$, $g^2 = s_1^{-1}$, *то* $s_3 \neq s_1 g s_2^{-1} g^{-1}$.
Тогда глобальный стабилизатор множества $\{[1,1],\ [1,s_1],\ [1,s_2],\ [1,s_3]\}$ *в группе* G *тривиален.*

Д о к а з а т е л ь с т в о. Пусть $R = \{[1,1],\ [1,s_1],\ [1,s_2],\ [1,s_3]\}$. Покажем, что поточечный стабилизатор множества R тривиален. Предположим, что $(g_1,g_2).\pi \in G_R$. Тогда, очевидно, $g_1 = g_2$ и либо $\pi = 1$ и $g_1 = 1$, либо $\pi \neq 1$ и $g_1^2 = 1$. В последнем случае получаем противоречие с условием (i). Таким образом, $G_R = 1$.

Пусть Δ — подграф графа Γ, порожденный множеством вершин R, и $H = G_{\{R\}}^{\Delta}$ (т.е. H — ограничение группы автоморфизмов $G_{\{R\}}$ графа Γ на подграф Δ). Покажем, что $\{[1,1],[1,s_1]\}$ — единственное ребро в графе Δ. Если $\{[1,1],[1,s_2]\} \in E(\Gamma)$, то $s_2 \in s_1^{\mathrm{Aut}(T)} \cup (s_1^{-1})^{\mathrm{Aut}(T)}$ и, следовательно, $|s_1| = |s_2|$, что противоречит выбору s_1 и s_2. Если $\{[1,1],[1,s_3]\} \in E(\Gamma)$, то $s_3 \in s_1^{\mathrm{Aut}(T)} \cup (s_1^{-1})^{\mathrm{Aut}(T)}$, что противоречит условию (ii). Если $\{[1,s_1],[1,s_2]\} \in E(\Gamma)$, то $s_1^{-1}s_2 \in s_1^{\mathrm{Aut}(T)} \cup (s_1^{-1})^{\mathrm{Aut}(T)}$ и, следовательно, $|s_1| = |s_1^{-1}s_2|$, что противоречит выбору s_1 и s_2. Если $\{[1,s_1],[1,s_3]\} \in E(\Gamma)$, то $s_1^{-1}s_3 \in s_1^{\mathrm{Aut}(T)} \cup (s_1^{-1})^{\mathrm{Aut}(T)}$, что противоречит условию (ii). Наконец, если $\{[1,s_2],[1,s_3]\} \in E(\Gamma)$, то $s_2^{-1}s_3 \in s_1^{\mathrm{Aut}(T)} \cup (s_1^{-1})^{\mathrm{Aut}(T)}$, что противоречит условию (ii). Таким образом, каждый элемент из H оставляет на месте каждое из множеств $\{[1,1],[1,s_1]\}$ и $\{[1,s_2],[1,s_3]\}$.

Покажем, что $H = 1$. Предположим, что существует элемент $(g_1,g_2).\pi \in G_{\{R\}}$ такой, что $(g_1,g_2).\pi[1,1] = [1,1]$, $(g_1,g_2).\pi[1,s_1] = [1,s_1]$, $(g_1,g_2).\pi[1,s_2] = [1,s_3]$ и $(g_1,g_2).\pi[1,s_3] = [1,s_2]$. Тогда из $(g_1,g_2).\pi[1,1] = [1,1]$ следует, что $(g_1,g_2).\pi = (g,g).\pi$ для некоторого $g \in \mathrm{Aut}(T)$. Далее, в силу $(g_1,g_2).\pi[1,s_1] = [1,s_1]$ имеем $g^2 \in C_{\mathrm{Aut}(T)}(s_1)$, а в силу $(g_1,g_2).\pi[1,s_2] = [1,s_3]$ и $(g_1,g_2).\pi[1,s_3] = [1,s_2]$ имеем $g^2 \in C_{\mathrm{Aut}(T)}(s_2)$, что с учетом $C_{\mathrm{Aut}(T)}(s_1) \cap C_{\mathrm{Aut}(T)}(s_2) = 1$ влечет за собой $g^2 = 1$. Если $\pi = 1$, то $s_1^g = s_1$ и $s_3 = s_2^g$, что противоречит условию (iii). Если $\pi \neq 1$, то $s_1^g = s_1^{-1}$ и $s_3 = (s_2^{-1})^g$, что противоречит условию (iv).

Предположим, что существует элемент $(g_1,g_2).\pi \in G_{\{R\}}$ такой, что $(g_1,g_2).\pi[1,1] = [1,s_1]$, $(g_1,g_2).\pi[1,s_1] = [1,1]$, $(g_1,g_2).\pi[1,s_2] = [1,s_2]$ и $(g_1,g_2).\pi[1,s_3] = [1,s_3]$. Если $\pi = 1$, то $(g_1,g_2).\pi = (g,s_1g).1$, где $g \in \mathrm{Aut}(T)$ и $g^2 = 1$. При этом $s_1^g = s_1^{-1}$, $s_2^g = s_1^{-1}s_2$ и $s_3^g = s_1^{-1}s_3$, что противоречит условию (v). Если $\pi \neq 1$, то $(g_1,g_2).\pi = (g,s_1g).\pi$, где $g \in \mathrm{Aut}(T)$ и $g^2 = s_1^{-1}$. При этом $s_1^g = s_1$, $gs_2g^{-1} = s_2^{-1}s_1$ и $gs_3g^{-1} = s_3^{-1}s_1$. Последнее равенство можно переписать как $(gs_3)^2 = 1$, откуда $gs_3 \in \mathrm{Inv}(\mathrm{Aut}(\langle T,g\rangle))$ и, следовательно, $s_3 \in T \cap g^{-1}\mathrm{Inv}(\mathrm{Aut}(\langle T,g\rangle))$. Противоречие с условием (vi).

Предположим, что существует элемент $(g_1,g_2).\pi \in G_{\{R\}}$ такой, что $(g_1,g_2).\pi(1,1) = [1,s_1]$, $(g_1,g_2).\pi(1,s_1) = [1,1]$, $(g_1,g_2).\pi[1,s_2] = [1,s_3]$ и $(g_1,g_2).\pi[1,s_3] = [1,s_2]$. Если $\pi = 1$, то $(g_1,g_2).\pi = (g,s_1g).1$, где $g \in \mathrm{Aut}(T)$ и $g^2 = 1$. При этом $s_1^g = s_1^{-1}$, $s_2^g = s_1^{-1}s_3$ и $s_3^g = s_1^{-1}s_2$, что противоречит условию (vii). Если $\pi \neq 1$, то $(g_1,g_2).\pi = (g,s_1g).1$, где $g \in \mathrm{Aut}(T)$ и $g^2 = s_1^{-1}$. При этом $s_1^g = s_1$ и $s_3 = s_1gs_2^{-1}g^{-1}$, что противоречит условию (viii). □

Лемма 2. *Предположим, что* $T = \langle s_1, s_2\rangle$ *и выполняется по крайней мере одно из следующих условий:*

(i) *порядки* $|s_1|, |s_2|, |s_1^{-1}s_2|$ *попарно различны,* $(s_1^{-1})^{\mathrm{Aut}(T)} = s_1^{\mathrm{Aut}(T)}$, $(s_2^{-1})^{\mathrm{Aut}(T)} = s_2^{\mathrm{Aut}(T)}$ *и* $|\mathrm{Inv}(\mathrm{Aut}(T))| + 3|s_1^{\mathrm{Aut}(T)}| + 2|s_2^{\mathrm{Aut}(T)}| < |T|$;

(ii) $|s_1| = 2$, $|s_2| \neq |s_1^{-1}s_2|$ *и* $|\mathrm{Inv}(\mathrm{Aut}(T))| + 3|s_1^{\mathrm{Aut}(T)}| + 4|C_T(s_1)||\mathrm{Out}(T)| < |T|$;

(iii) $|s_1| = 2$, $(s_2^{-1})^{\mathrm{Aut}(T)} = s_2^{\mathrm{Aut}(T)}$ *и* $7\sqrt{\dfrac{2}{m(T)}} + 2\dfrac{|\mathrm{Out(T)}|}{m(T)} + \dfrac{1}{m(T)} < 1$;

(iv) $|s_1| = 2$, $|s_2| = |s_1^{-1}s_2|$ *и* $|\mathrm{Inv}(\mathrm{Aut}(T))| + 3|s_1^{\mathrm{Aut}(T)}| + 4|s_2^{\mathrm{Aut}(T)}| < |T|$;

(v) $|s_1|=2$, $|s_2|=|s_1^{-1}s_2|$, $(s_2^{-1})^{\mathrm{Aut}(T)}=s_2^{\mathrm{Aut}(T)}$ *и* $|\mathrm{Inv}(\mathrm{Aut}(T))|+3|s_1^{\mathrm{Aut}(T)}|+2|s_2^{\mathrm{Aut}(T)}|<|T|$;

(vi) $|s_1|=2$, $(s_2^{-1})^{\mathrm{Aut}(T)}=s_2^{\mathrm{Aut}(T)}$ *и* $7\sqrt{\dfrac{2}{m(T)}}+2\dfrac{|s_2^{\mathrm{Aut}(T)}|}{m(T)}+\dfrac{1}{m(T)}<1$;

(vii) *порядки* $|s_1|,|s_2|,|s_1^{-1}s_2|$ *попарно различны,* $(s_1^{-1})^{\mathrm{Aut}(T)}=s_1^{\mathrm{Aut}(T)}$ *и* $|\mathrm{Inv}(\mathrm{Aut}(T))|+3|s_1^{\mathrm{Aut}(T)}|+4|s_2^{\mathrm{Aut}(T)}|<|T|$;

(viii) $|s_1|=2$ *и* $2|\mathrm{Inv}(\mathrm{Aut}(T))|+3|\mathrm{Inv}(T)|+4|C_T(s_1)||\mathrm{Out}(T)|+\max\{|C_T(x)|\mid 1\neq x\in\mathrm{Aut}(T)\}<|T|$;

(ix) $|s_1|=2$, $|s_2|\neq|s_1^{-1}s_2|$ *и* $5\sqrt{\dfrac{2}{m(T)}}+4\dfrac{|\mathrm{Out(T)}|}{m(T)}<1$; *Тогда существует элемент* $s_3\in T$ *такой, что* T, s_1, s_2 *и* s_3 *удовлетворяют условию леммы* 1.

Д о к а з а т е л ь с т в о. Для любой конечной группы H четного порядка с $Z(H)=1$ и некоторого $x\in H\setminus\{1\}$, имеем $|\mathrm{Inv}(H)|\le\sqrt{\dfrac{2}{|H:C_H(x)|}}|H|$ (см. доказательство (45.3) в [2]). В частности,

$$|\mathrm{Inv}(T)|\le\sqrt{\frac{2}{m(T)}}|T|, \tag{1}$$

$$|\mathrm{Inv}(\langle T,g\rangle)|\le 2\sqrt{\frac{2}{m(T)}}|T| \tag{2}$$

для любого $g\in\mathrm{Aut}(T)$ с $g^2\in T$.

Далее, если $g\in\mathrm{Aut}(T)$ и $g^2=1$, то

$$\left|\{t\in T\mid gtg^{-1}=t^{-1}\}\right|\le|\mathrm{Inv}(\langle T,g\rangle)| \tag{3}$$

(поскольку из $gtgt=1$ следует $gt\in\mathrm{Inv}(\langle T,g\rangle)$). Кроме того, если $g\in\mathrm{Aut}(T)$ и $s\in T$, то, очевидно,

$$\left|\{t\in T\mid tgt^{-1}=sg\}\right|\le|C_T(g)|. \tag{4}$$

Пусть $T=\langle s_1,s_2\rangle$ и $M_1,\ldots,M_8$ — множества таких элементов $s_3\in T$, что для T, s_1, s_2 и s_3 нарушаются, соответственно, условия (i)–(viii) леммы 1. Тогда нужно доказать, что $T\setminus(M_1\cup\ldots\cup M_8)\neq\varnothing$. Мы покажем, что

$$|M_1\cup\ldots\cup M_8|<|T|. \tag{5}$$

Предположим, что для T, s_1 и s_2 выполняется условие (i). В силу (3) имеем $|M_1|\le|\mathrm{Inv}(\mathrm{Aut}(T))|$. Поскольку $(s_1^{-1})^{\mathrm{Aut}(T)}=s_1^{\mathrm{Aut}(T)}$, то $|M_2|\le 3|s_1^{\mathrm{Aut}(T)}|$. Так как $(s_2^{-1})^{\mathrm{Aut}(T)}=s_2^{\mathrm{Aut}(T)}$, то $|M_3\cup M_4|\le|s_2^{\mathrm{Aut}(T)}|$ и $|M_7\cup M_8|\le|s_2^{\mathrm{Aut}(T)}|$. Поскольку $|s_2|\neq|s_1^{-1}s_2|$, то $|M_5|=|M_6|=0$. Таким образом, справедливо (5).

Предположим, что для T, s_1 и s_2 выполняется условие (ii). В силу (3) имеем $|M_1|\le|\mathrm{Inv}(\mathrm{Aut}(T))|$. Так как $|s_1|=2$, то $|M_2|\le 3|s_1^{\mathrm{Aut}(T)}|$ и $|M_3|+|M_4|+|M_7|+|M_8|\le 4|C_{\mathrm{Aut}(T)}(s_1)|\le 4|C_T(s_1)||\mathrm{Out}(T)|$. Поскольку $|s_2|\neq|s_1^{-1}s_2|$, то $|M_5|=|M_6|=0$. Таким образом, (5) установлено.

Предположим, что для T, s_1 и s_2 выполняется условие (iii). В силу (3) и (2) имеем $|M_1|\le 2\sqrt{\dfrac{2}{m(T)}}|T|$. Поскольку $|s_1|=2$, то в силу (i) имеем $|M_2|\le 3|s_1^{\mathrm{Aut}(T)}|\le 3|\mathrm{Inv}(T)|\le 3\sqrt{\dfrac{2}{m(T)}}|T|$. Кроме того, $|M_3\cup M_4|\le|s_2^{\mathrm{Aut}(T)}|\le\dfrac{|\mathrm{Out}(T)|}{m(T)}|T|$ и $|M_7\cup M_8|\le|s_2^{\mathrm{Aut}(T)}|\le\dfrac{|\mathrm{Out}(T)|}{m(T)}|T|$. В силу (4) имеем $|M_5|\le\dfrac{1}{m(T)}|T|$. В силу (2) имеем $|M_6|\le 2\sqrt{\dfrac{2}{m(T)}}|T|$. Таким образом, справедливо (5).

Предположим, что для T, s_1 и s_2 выполняется условие (iv). Тогда получаем неравенства $|M_1| \leq |\mathrm{Inv}(\mathrm{Aut}(T))|$, $|M_2| \leq 3|s_1^{\mathrm{Aut}(T)}|$ и $|M_3| + |M_4| + |M_7| + |M_8| \leq 4|s_2^{\mathrm{Aut}(T)}|$. Поскольку $|s_2| \neq |s_1^{-1}s_2|$, то $|M_5| = |M_6| = 0$. Таким образом, справедливо (5).

Предположим, что для T, s_1 и s_2 выполняется условие (v). Тогда получаем неравенства $|M_1| \leq |\mathrm{Inv}(\mathrm{Aut}(T))|$ и $|M_2| \leq 3|s_1^{\mathrm{Aut}(T)}|$. Поскольку $(s_2^{-1})^{\mathrm{Aut}(T)} = s_2^{\mathrm{Aut}(T)}$, то $|M_3 \cup M_4| \leq |s_2^{\mathrm{Aut}(T)}|$ и $|M_7 \cup M_8| \leq |s_2^{\mathrm{Aut}(T)}|$. Так как $|s_2| \neq |s_1^{-1}s_2|$, то $|M_5| = |M_6| = 0$. Таким образом, (5) установлено.

Предположим, что для T, s_1 и s_2 выполняется условие (vi). В силу (3) и (2) имеем $|M_1| \leq 2\sqrt{\dfrac{2}{m(T)}}|T|$ и $|M_5| \leq \dfrac{1}{m(T)}$. Поскольку $|s_1| = 2$, то в силу (1) имеем $|M_2| \leq 3|s_1^{\mathrm{Aut}(T)}| \leq 3|\mathrm{Inv}(T)| \leq 3\sqrt{\dfrac{2}{m(T)}}|T|$. Кроме того, $|M_3 \cup M_4| \leq |s_2^{\mathrm{Aut}(T)}|$ и $|M_7 \cup M_8| \leq |s_2^{\mathrm{Aut}(T)}|$. В силу (2) имеем $|M_6| \leq 2\sqrt{\dfrac{2}{m(T)}}$. Таким образом, справедливо (5).

Предположим, что для T, s_1 и s_2 выполняется условие (vii). Тогда получаем неравенства $|M_1| \leq |\mathrm{Inv}(\mathrm{Aut}(T))|$ и $|M_2| \leq 3|s_1^{\mathrm{Aut}(T)}|$. Кроме того, $|M_3| + |M_4| + |M_7| + |M_8| \leq 4|s_2^{\mathrm{Aut}(T)}|$. Так как $|s_2| \neq |s_1^{-1}s_2|$, то $|M_5| = |M_6| = 0$. Таким образом, справедливо (5).

Предположим, что для T, s_1 и s_2 выполняется условие (viii). Тогда получаем неравенства $|M_1| \leq |\mathrm{Inv}(\mathrm{Aut}(T))|$, $|M_2| \leq 3|s_1^{\mathrm{Aut}(T)}|$ и $|M_3| + |M_4| + |M_7| + |M_8| \leq 4|C_T(s_1)||\mathrm{Out}(T)|$. Кроме того, $|M_5| \leq \max\{|C_T(x)| \mid 1 \neq x \in \mathrm{Aut}(T)\}$ и $|M_6| \leq |\mathrm{Inv}(\mathrm{Aut}(T))|$. Таким образом, (5) выполняется.

Предположим, наконец, что для T, s_1 и s_2 выполняется условие (ix). В силу (3) и (2) имеем $|M_1| \leq 2\sqrt{\dfrac{2}{m(T)}}|T|$. Поскольку $|s_1| = 2$, то в силу (1) имеем $|M_2| \leq 3\sqrt{\dfrac{2}{m(T)}}|T|$. Кроме того, $|M_3| + |M_4| + |M_7| + |M_8| \leq 4|s_2^{\mathrm{Aut}(T)}| \leq 4\dfrac{|\mathrm{Out}(T)|}{m(T)}|T|$. Так как $|s_2| \neq |s_1^{-1}s_2|$, то $|M_5| = |M_6| = 0$. Таким образом, справедливо (5). □

Лемма 3. *Пусть T — одна из групп: A_6, $L_2(7)$. Тогда существуют элементы s_1, s_2 и $s_3 \in T$ такие, что T, s_1, s_2 и s_3 удовлетворяют условиям леммы* 1.

Д о к а з а т е л ь с т в о. Пусть $T = A_6$ и s_1, s_2 — стандартные порождающие группы T, указанные в [11]. Имеем $|s_1| = 2$, $|s_2| = 4$ и $|s_1^{-1}s_2| = 5$. Теперь непосредственная проверка показывает, что существует элемент $s_3 \in T$ такой, что для T, s_1, s_2 и s_3 выполняются условия леммы 1.

Пусть $T = L_2(7)$ и s_1, s_2 — стандартные порождающие группы T, указанные в [11]. Имеем $|s_1| = 2$, $|s_2| = 7$ и $|s_1^{-1}s_2| = 3$. Теперь непосредственная проверка показывает, что существует элемент $s_3 \in T$ такой, что для T, s_1, s_2 и s_3 выполняются условия леммы 1. □

Д о к а з а т е л ь с т в о теоремы в случае, когда G — группа типа II (a).

Предположим, что $T = A_n$, где $n \geq 8$. Пусть s_1, s_2 — элементы группы T, выбранные в соответствии с предложением 2. Тогда $T = \langle s_1, s_2 \rangle$ и для T, s_1, s_2 выполнено условие (i) леммы 2. Следовательно, по леммам 2 и 1 найдется такой элемент $s_3 \in T$, что, полагая $R = \big\{[1,1],\ [1,s_1],\ [1,s_2],\ [1,s_3]\big\}$, имеем $G_{\{R\}} = 1$.

Предположим, что $T = A_6$. Пусть s_1, s_2, s_3 — элементы группы T, выбранные в соответствии с леммой 3. Тогда, полагая $R = \big\{[1,1],\ [1,s_1],\ [1,s_2],\ [1,s_3]\big\}$, в силу леммы 1 имеем $G_{\{R\}} = 1$.

Предположим, что $T = A_7$. Пусть s_1, s_2 — элементы группы T, выбранные в соответствии с предложением 3. Тогда $T = \langle s_1, s_2 \rangle$ и для T, s_1, s_2 выполнено условие (ii) леммы 2. Следовательно, по леммам 2 и 1 найдется такой элемент $s_3 \in T$, что, полагая $R = \big\{[1,1],\ [1,s_1],\ [1,s_2],\ [1,s_3]\big\}$, имеем $G_{\{R\}} = 1$.

Предположим, что T — спорадическая простая группа, отличная от групп M_{11}, M_{12}, M_{22}, M_{23}, M_{24}, J_2 и HS. Пусть s_1, s_2 — элементы группы T, выбранные в соответствии с предложением 4. Тогда $T = \langle s_1, s_2\rangle$ и для T, s_1, s_2 выполнено условие (iii) леммы 2. Следовательно, по леммам 2 и 1 найдется такой элемент $s_3 \in T$, что, полагая $R = \big\{[1,1],\ [1,s_1],\ [1,s_2],\ [1,s_3]\big\}$, имеем $G_{\{R\}} = 1$.

Предположим, что $T = M_{11}$. Пусть s_1, s_2 — элементы группы T, выбранные в соответствии с предложением 5. Тогда $T = \langle s_1, s_2\rangle$ и для T, s_1, s_2 выполнено условие (v) леммы 2. Следовательно, по леммам 2 и 1 найдется такой элемент $s_3 \in T$, что, полагая $R = \big\{[1,1],\ [1,s_1],\ [1,s_2],\ [1,s_3]\big\}$, имеем $G_{\{R\}} = 1$.

Предположим, что T — одна из групп: M_{12}, M_{22}, M_{23}, M_{24}, J_2 и HS. Пусть s_1, s_2 — элементы группы T, выбранные в соответствии с предложением 6. Тогда $T = \langle s_1, s_2\rangle$ и для T, s_1, s_2 выполнено условие (iv) леммы 2. Следовательно, по леммам 2 и 1 найдется такой элемент $s_3 \in T$, что, полагая $R = \big\{[1,1],\ [1,s_1],\ [1,s_2],\ [1,s_3]\big\}$, имеем $G_{\{R\}} = 1$.

Предположим, что $T = L_2(q)$, где $q \geq 11$ или $q = 8$. Пусть s_1, s_2 — элементы группы T, выбранные в соответствии с предложением 7. Тогда $T = \langle s_1, s_2\rangle$ и для T, s_1, s_2 выполнено условие (v) леммы 2. Следовательно, по леммам 2 и 1 найдется такой элемент $s_3 \in T$, что, полагая $R = \big\{[1,1],\ [1,s_1],\ [1,s_2],\ [1,s_3]\big\}$, имеем $G_{\{R\}} = 1$.

Предположим, что $T = L_2(7)$. Пусть s_1, s_2, s_3 — элементы группы T, выбранные в соответствии с леммой 3. Тогда, полагая $R = \big\{[1,1],\ [1,s_1],\ [1,s_2],\ [1,s_3]\big\}$, в силу леммы 1 имеем $G_{\{R\}} = 1$.

Предположим, что T — группа лиева типа, отличная от групп: $L_2(q)$ $(q \geq 4)$, $L_3(q)$ $(q \leq 13)$, $L_4(q)$ $(q \leq 5)$, $L_5(q)$ $(q \leq 3)$, $L_6(2)$, $L_7(2)$, $U_3(q)$ $(q \leq 8)$, $U_4(q)$ $(q \leq 3)$, $U_5(2)$, $S_4(4)$, $S_4(5)$, $S_6(2)$, $S_8(2)$, $O_8^-(2)$, $O_{10}^-(2)$, $O_8^+(2)$, $O_8^+(3)$, $Suz(8)$, $G_2(3)$, $G_2(4)$, $F_4(2)$, $F_4(3)$, ${}^2F_4(2)'$, ${}^2E_6(2)$, $E_7(2)$, $E_7(3)$. Пусть s_1, s_2 — элементы группы T, выбранные в соответствии с предложением 8. Тогда $T = \langle s_1, s_2\rangle$ и для T, s_1, s_2 выполнено условие (vi) леммы 2. Следовательно, по леммам 2 и 1 найдется такой элемент $s_3 \in T$, что, полагая $R = \{[1,1],\ [1,s_1],\ [1,s_2],\ [1,s_3]\}$, имеем $G_{\{R\}} = 1$.

Предположим, что T — одна из групп: $L_3(3)$, $L_3(4)$, $L_3(5)$, $L_3(7)$, $L_3(8)$, $L_4(3)$, $L_5(2)$ $U_3(3)$, $U_3(4)$, $U_4(2)$, $U_4(3)$, $U_5(2)$, $S_4(4)$, $S_4(5)$, $S_6(2)$, $S_8(2)$, $O_8^-(2)$, $O_{10}^-(2)$, $O_8^+(2)$, $Sz(8)$, $G_2(3)$, $G_2(4)$, $F_4(2)$, ${}^2F_4(2)'$, ${}^2E_6(2)$. Пусть s_1, s_2 — элементы группы T, выбранные в соответствии с предложением 9. Тогда $T = \langle s_1, s_2\rangle$ и для T, s_1, s_2 выполнено условие (ii) леммы 2. Следовательно, по леммам 2 и 1 найдется такой элемент $s_3 \in T$, что, полагая $R = \big\{[1,1],\ [1,s_1],\ [1,s_2],\ [1,s_3]\big\}$, имеем $G_{\{R\}} = 1$.

Предположим, что $T = U_3(5)$. Пусть s_1, s_2 — элементы группы T, выбранные в соответствии с предложением 10. Тогда $T = \langle s_1, s_2\rangle$ и для T, s_1, s_2 выполнено условие (vii) леммы 2. Следовательно, по леммам 2 и 1 найдется такой элемент $s_3 \in T$, что, полагая $R = \big\{[1,1],\ [1,s_1],\ [1,s_2],\ [1,s_3]\big\}$, имеем $G_{\{R\}} = 1$.

Предположим, что $T = L_3(9)$. Пусть s_1, s_2 — элементы группы T, выбранные в соответствии с предложением 11. Тогда $T = \langle s_1, s_2\rangle$ и для T, s_1, s_2 выполнено условие (viii) леммы 2. Следовательно, по леммам 2 и 1 найдется такой элемент $s_3 \in T$, что, полагая $R = \big\{[1,1],\ [1,s_1],\ [1,s_2],\ [1,s_3]\big\}$, имеем $G_{\{R\}} = 1$.

Предположим, что T — одна из групп: $L_3(11)$, $L_3(13)$, $L_5(3)$, $O_8^+(3)$, $F_4(3)$, $E_7(2)$, $E_7(3)$. Пусть s_1, s_2 — элементы группы T, выбранные в соответствии с предложением 12. Тогда $T = \langle s_1, s_2\rangle$ и для T, s_1, s_2 выполнено условие (iii) леммы 2. Следовательно, по леммам 2 и 1 найдется такой элемент $s_3 \in T$, что, полагая $R = \big\{[1,1],\ [1,s_1],\ [1,s_2],\ [1,s_3]\big\}$, имеем $G_{\{R\}} = 1$.

Предположим, что T — одна из групп: $L_4(4)$, $L_4(5)$, $L_6(2)$, $L_7(2)$. Пусть s_1, s_2 — элементы группы T, выбранные в соответствии с предложением 13. Тогда $T = \langle s_1, s_2\rangle$ и для T, s_1, s_2 выполнено условие (iv) леммы 2. Следовательно, по леммам 2 и 1 найдется такой элемент $s_3 \in T$, что, полагая $R = \big\{[1,1],\ [1,s_1],\ [1,s_2],\ [1,s_3]\big\}$, имеем $G_{\{R\}} = 1$.

Справедливость теоремы в случае, когда G — группа типа II (a), доказана. $\square$

З а м е ч а н и е. Из приведенного доказательства следует, что если G — группа типа

II (a), то существует подмножество R множества X такое, что $G_{\{R\}} = 1$ и кроме того $|R| \leq k$ при $k > 2$, $|R| \leq 4$ при $k = 2$ и $T \neq A_5$.

5. Доказательство теоремы в случае, когда G — группа типа II (b) или II (c)

В этом параграфе теорема будет доказана в случае, когда G является группой типа II (b) или II (c) из теоремы О'Нэна — Скотта (см. § 2).

Положим $W = S_m \mathrm{wr} S_k$, где $m \geq 5$ и $k \geq 2$, и пусть $M = \{1, \dots, m\}$. Имеем

$$W = \bigl\{(h_1, \dots, h_k)\pi \mid h_i \in S_m, \pi \in S_k\bigr\},$$

и если $w = (h_1, \dots, h_k)\pi \in W$, $(x_1, \dots, x_k) \in M^k$, то $w(x_1, \dots, x_k) = (h_1(x_1), \dots, h_k(x_k))^\pi$. В рассматриваемом случае G подстановочно изоморфна подгруппе группы W.

Для доказательства теоремы в случае, когда G — группа типа II (b) или II (c), положим $G = W$ и покажем, что существует такое подмножество R множества X, что $G_{\{R\}} = 1$.

Случай 1. $k = 2$.

Положим $R = \bigl\{(3,2), (i-1,i), (i,i) \mid i \in \{3, \dots, m\}\bigr\}$. Пусть $g = (h_1, h_2)\pi \in G$ и $g(R) = R$. Покажем, что $g = 1$. Поскольку $|\{(3,j) \mid (3,j) \in R\}| = 3$ и $|\{(j,i) \mid (j,i) \in R\}| < 3$ для любого $i \in M$, имеем $\pi = 1$. Так как $|\{(j,2) \mid (j,2) \in R\}| = 1$ и $|\{(j,i) \mid (j,i) \in R\}| \neq 1$ для любого $i \in M \setminus \{2\}$, то имеем $h_2(2) = 2$. Ввиду того, что $|\{(3,j) \mid (3,j) \in R\}| = 3$ и $|\{(i,j) \mid (i,j) \in R\}| < 3$ для любого $i \in M \setminus \{3\}$, мы имеем $h_1(3) = 3$. Следовательно, $g(3,2) = (3,2)$ и $g(3,3) = (3, h_2(3))$. Поскольку $g(3,3) \in R$, то $h_2(3) \in \{3,4\}$. Предположим, что $h_2(3) = 4$. Тогда $g(3,3) = (3,4)$, что с учетом $g(3,4) \in R$ влечет за собой $g(3,4) = (3,3)$. Теперь $g(4,4) = (h_1(4), 3)$, что с учетом $g(4,4) \in R$ влечет за собой $h_1(4) \in \{2,3\}$. Ввиду $h_1(3) = 3$ имеем $h_1(4) = 2$. Следовательно, $g(4,5) = (2, h_2(5))$, откуда с учетом $g(4,5) \in R$ получаем $h_2(5) = 3$, что противоречит $g(4,4) = (2,3)$. Поэтому $h_2(3) = 3$ и $g(3,3) = (3,3)$. Поскольку $g(2,3) \in R$, то с учетом $g(3,3) = (3,3)$ имеем $g(2,3) = (2,3)$. Но если справедливы равенства $g(i-1,i) = (i-1,i)$ и $g(i,i) = (i,i)$ для некоторого $i \in \{3, \dots, m-1\}$, то в силу $g(i,i+1) \in R$ имеем $g(i,i+1) = (i,i+1)$ и, следовательно, с учетом $g(i+1,i+1) \in R$ получаем равенство $g(i+1,i+1) = (i+1,i+1)$. Таким образом, $g = 1$.

Случай 2. $k > 2$.

В качестве элементов подмножества R множества X возьмем упорядоченный набор $(3, 2, 2, \dots, 2)$ и все упорядоченные наборы вида $(j+1, \ \dots, \ j+1)$ и вида $(j, \ \dots, \ j, \ j+1, \ \dots, \ j+1)$, где $j \in \{2, \dots, m-1\}$. Таким образом, $|R| = k(m-2) + 1$. Пусть $g = (h_1, \dots, h_k)\pi \in G$ и $g(R) = R$. Покажем, что $g = 1$.

Положим $K = \{1, \dots, k\}$. Для $i \in K$ и $j \in M$ положим $P_{i,j} = |\{(x_1, \dots, x_k) \mid (x_1, \dots, x_k) \in R, x_i = j\}|$ и $P_i = |\{P_{i,j} \mid j \in M\}|$. Так как $P_{i,1} = 0$ и $P_{i,j} \neq 0$ при всех $i \in K$ и $j \in M \setminus \{1\}$, то $h_i(1) = 1$ для любого $i \in K$. Поскольку $P_1 = 5$ и $P_i < 5$ при $i \in K \setminus \{1\}$, то $\pi(1) = 1$.

Покажем, что $h_i(m) = m$ для любого $i \in K$ и $h_1(m-1) = m-1$. Так как $P_{1,m} = 1$ и $P_{1,j} \neq 1$ при $m \neq j \in M$, то $h_1(m) = m$. С учетом этого $(m, h_{\pi(2)}(m), \dots, h_{\pi(k)}(m)) = (h_1(m), h_{\pi(2)}(m), \dots, h_{\pi(k)}(m)) = g(m, m, \dots, m) \in R$, откуда $h_i(m) = m$ для любого $i \in K$. Теперь $g(m-1, m, \dots, m) = (h_1(m-1), m, \dots, m) \in R$, откуда $h_1(m-1) = m-1$.

Покажем, что $\pi = 1$. Ранее было доказано, что $\pi(1) = 1$ и $h_1(m-1) = m-1$. Предположим, что для некоторого $i \in \{2, \dots, m-1\}$ справедливо $\pi(j) = j$ и $h_j(m-1) = m-1$ для любого $j \leq i-1$. Пусть $x_1 = \ldots = x_i = m-1$ и $x_{i+1} = \ldots = x_k = m$. Тогда в силу $h_{i'}(m) = m$ для любого $i' \in K$ и $g(x_1, \dots, x_k) \in R$, имеем $h_i(m-1) = m-1$ и $\pi(i) = i$. Отсюда следует, что $\pi = 1$.

Предположим, что для некоторого $j' \in \{3, \dots, m\}$ и произвольных $j'' \in \{j'+1, \dots, m\}$, $i \in K$ выполняется $h_i(j'') = j''$. Покажем, что тогда $h_i(j') = j'$ для любого $i \in K$. Поскольку $g(j', j'+1, \dots, j'+1) = (h_1(j'), j', \dots, j') \in R$, то с учетом $h_1(j'+1) = j'+1$ имеем $h_1(j') = j'$.

Предположим, что для некоторого $i \in K$ и всех $i' \in \{1, \ldots, i-1\}$ выполняется равенство $h_{i'}(j') = j'$. Пусть $x_1 = \ldots = x_i = j'$ и $x_{i+1} = \ldots = x_k = j' + 1$. Тогда из $g(x_1, \ldots, x_k) \in R$ с учетом $h_i(j'+1) = j'+1$ следует $h_i(j') = j'$. Таким образом, $h_i(j') = j'$ для любого $i \in K$. Отсюда следует, что $h_i(j) = j$ для произвольных $j \in \{3, \ldots, m\}$, $i \in K$.

Далее, для произвольного $i \in K$ имеем $h_i(2) \in M \setminus \{h_i(3), \ldots, h_i(m)\} = \{1, 2\}$, что с учетом $h_i(1) = 1$ влечет за собой $h_i(2) = 2$. Таким образом, $g = 1$.

Справедливость теоремы в случае, когда G — группа типа II (b) или II (c), доказана. $\square$

Таким образом, доказательство теоремы полностью завершено.

З а м е ч а н и е. Из приведенного доказательства следует, что если $G \leq S_m \mathrm{wr} S_k$, где $m \geq 5$ и $k \geq 2$, то существует подмножество R множества X такое, что $|R| \leq k(m-2)+1$ и $G_{\{R\}} = 1$.

Поступила 19.10.2006

СПИСОК ЛИТЕРАТУРЫ

1. **Albertson M.O., Collins K.L.** Symmetry breaking in graphs // Electron. J. Combin. 1996. Vol. 3. #R18.
2. **Aschbacher M.** Finite group theory. Cambridge: Cambridge University Press, 1993.
3. **Cameron P.J., Neumann P.M., Saxl J.** On groups with no regular orbits on the set of subsets // Arch. Math. 1984. Vol. 43. P. 295–296.
4. **Conway J.H., Curtis R.T., Norton S.P., Parker R.A., Wilson W.A.** Atlas of Finite Groups. Oxford: Clarendon Press, 1985.
5. **Dixon J.D., Mortimer B.** Permutation groups. New York: Springer, 1996.
6. **Fong P., Wong W.J.** A characterization of the finite simple groups $PSp(4,q)$, $G_2(q)$, $D_4^2(q)$, I // Nagoya Math. J. 1969. Vol. 36. P. 143–184.
7. **Gorenstein D., Walter J.H.** The characterization of finite groups with dihedral Sylow 2-subgroups, I // J. Algebra. 1965. Vol. 2. P. 119–151.
8. **Liebeck M.W., Praeger Ch.E., Saxl J.** On the O'Nan–Scott theorem for finite primitive permutation groups // J. Austral. Math. Soc. Series A. 1988. Vol. 44. P. 389–396.
9. **Malle G., Saxl J., Weigel Th.** Generation for classical groups // Geom. Dedicata. 1994. Vol. 49. P. 85–116.
10. **Weigel Th.** Generation of exceptional groups of Lie-type // Geom. Dedicata. 1992. Vol. 41. P. 63–87.
11. **ATLAS of finite group representations.** Version 3.004. http://brauer.maths.qmul.ac.uk.

ТРУДЫ ИНСТИТУТА МАТЕМАТИКИ И МЕХАНИКИ УрО РАН

Том 13 № 1 2007

УДК 512.54+519.17

О ГРАФАХ КЭЛИ ГРУППЫ $\mathbb{Z}^4$, ЯВЛЯЮЩИХСЯ ПРЕДЕЛАМИ МИНИМАЛЬНЫХ ВЕРШИННО-ПРИМИТИВНЫХ ГРАФОВ HA-ТИПА[1]

К. В. Костоусов

В совместной работе М. Гиудичи, Ч. Ли, Ч. Прэгер, А. Сереша и В.И. Трофимова показано, что каждый граф, являющийся пределом вершинно-примитивных графов HA-типа, изоморфен графу Кэли группы $\mathbb{Z}^d$. Ранее автором доказана конечность числа попарно не изоморфных графов Кэли группы $\mathbb{Z}^d$, являющихся пределами минимальных вершинно-примитивных графов HA-типа, при $d \leq 3$ (и получено их явное описание). В настоящей работе построено такое счетное множество попарно не изоморфных графов Кэли группы $\mathbb{Z}^4$, являющихся пределами минимальных вершинно-примитивных графов HA-типа, что вне этого множества имеется с точностью до изоморфизма лишь конечное число таких графов Кэли группы $\mathbb{Z}^4$.

Введение

Всюду далее под графом понимается неориентированный граф без петель и кратных ребер. Множество вершин графа Γ обозначается через $V(\Gamma)$, множество ребер — через $E(\Gamma)$.

Пусть K — абелева группа и M — система порождающих группы K такая, что $M = -M$ и $0 \notin M$. *Графом Кэли группы K, соответствующим системе порождающих M*, называется граф $\Gamma_{K,M}$ с множеством вершин $V(\Gamma_{K,M}) = K$ и множеством ребер $E(\Gamma_{K,M}) = \{\{a,b\}\colon a - b \in M\}$.

Всюду далее d — некоторое целое положительное число. Пусть M — система порождающих группы $\mathbb{Z}^d$ такая, что $M = -M$ и $0 \notin M$. Пусть $\mathrm{Aut}(\Gamma_{\mathbb{Z}^d,M})_0$ — стабилизатор вершины 0 в группе автоморфизмов графа $\Gamma_{\mathbb{Z}^d,M}$. Граф Кэли $\Gamma_{\mathbb{Z}^d,M}$ назовем *минимальным*, если множество M является $\mathrm{Aut}(\Gamma_{\mathbb{Z}^d,M})_0$-орбитой на $\mathbb{Z}^d \setminus \{0\}$ минимальной мощности.

В настоящей работе рассматриваются минимальные графы Кэли группы $\mathbb{Z}^4$. Помимо определенного самостоятельного интереса, вопрос о строении таких графов актуален в связи с исследованием графов, являющихся предельными для множества конечных графов с вершинно-примитивными группами автоморфизмов.

Если X — произвольное множество конечных связных вершинно-примитивных (т.е. допускающих примитивную на множестве вершин группу автоморфизмов) графов, то *предельными* для X называются такие бесконечные связные графы, у которых каждый шар изоморфен шару некоторого графа из X. Описание предельных для X графов позволяет описать типичное локальное строение графов из X.

Пусть H — примитивная группа подстановок на конечном множестве. Группа H называется *примитивной группой HA-типа*, если она содержит регулярную абелеву нормальную подгруппу. Конечный связный граф Γ называется *вершинно-примитивным графом HA-типа*, если он допускает примитивную на $V(\Gamma)$ группу автоморфизмов HA-типа. Конечный связный граф Γ называется *минимальным вершинно-примитивным графом HA-типа*, если он допускает примитивную на $V(\Gamma)$ группу H автоморфизмов HA-типа такую, что валентность Γ не превосходит валентности любого связного графа Δ, для которого $V(\Gamma) = V(\Delta)$ и $H \leq \mathrm{Aut}(\Delta)$ (легко показать, что при этом группа H действует транзитивно на $E(\Gamma)$). Исследование множества минимальных вершинно-примитивных графов HA-типа представляет интерес, поскольку

[1]Работа выполнена при частичной финансовой поддержке РФФИ (проект 06-01-00378).

в некотором смысле они являются самыми естественными графами, допускающими примитивные группы автоморфизмов HA-типа.

По [1, теорема 1.2] граф, являющийся предельным для множества вершинно-примитивных графов HA-типа, является графом Кэли группы $\mathbb{Z}^d$ для некоторого d. В связи с этим возникла задача исследования множеств графов Кэли групп $\mathbb{Z}^d$, являющихся предельными для множества минимальных вершинно-примитивных графов HA-типа при фиксированных d. Легко показать, что каждый граф Кэли группы $\mathbb{Z}^d$, являющийся предельным для множества минимальных вершинно-примитивных графов HA-типа, минимален.

В случае $d = 1$ существует только один минимальный граф Кэли группы $\mathbb{Z}^d$. Этот граф соответствует системе порождающих $M = \{1, -1\}$ и является предельным для множества минимальных вершинно-примитивных графов HA-типа. Согласно [2, теорема 2], при $d = 2, 3$ существует лишь конечное число попарно не изоморфных минимальных графов Кэли группы $\mathbb{Z}^d$ (все они являются предельными для множества минимальных вершинно-примитивных графов HA-типа и перечислены в этой теореме). Однако, согласно теореме из [3], существует счетное число попарно не изоморфных графов Кэли группы $\mathbb{Z}^4$, являющихся предельными для множества минимальных вершинно-примитивных графов HA-типа.

В настоящей работе найдено такое счетное множество графов Кэли группы $\mathbb{Z}^4$, являющихся предельными для множества минимальных вершинно-примитивных графов HA-типа, что вне этого множества имеется с точностью до изоморфизма лишь конечное число минимальных графов Кэли группы $\mathbb{Z}^4$.

Отождествим $\mathbb{Z}^d$ с множеством целочисленных вектор-строк длины d и зафиксируем действие группы $\mathrm{GL}_d(\mathbb{Z})$ целочисленных $d \times d$-матриц с определителями ± 1 умножением справа на этом множестве. Классы сопряженных конечных подгрупп группы $\mathrm{GL}_d(\mathbb{Z})$ будем называть *$\mathbb{Z}$-классами* конечных подгрупп группы $\mathrm{GL}_d(\mathbb{Z})$.

Пусть $G_1, \ldots, G_{N(d)}$ — представители всех $\mathbb{Z}$-классов конечных подгрупп группы $\mathrm{GL}_d(\mathbb{Z})$ (конечность числа $\mathbb{Z}$-классов конечных подгрупп группы $\mathrm{GL}_d(\mathbb{Z})$ следует из теоремы Бибербаха о кристаллографических группах [4, теорема 8.5.10]). Тогда каждый минимальный граф Кэли $\Gamma_{\mathbb{Z}^d,M}$ группы $\mathbb{Z}^d$ изоморфен графу Кэли группы $\mathbb{Z}^d$, соответствующему орбите некоторой из этих групп. Действительно, пусть G — стабилизатор вершины 0 в группе $\mathrm{Aut}(\Gamma_{\mathbb{Z}^d,M})$. Из [2, теорема 3] следует, что группа G естественным образом отождествляется с конечной подгруппой группы $\mathrm{GL}_d(\mathbb{Z})$. Из определения минимального графа Кэли группы $\mathbb{Z}^d$ следует, что $M = xG$ для некоторого $x \in \mathbb{Z}^d$. Далее, имеем $G = a^{-1}G_i a$ для некоторых $a \in \mathrm{GL}_d(\mathbb{Z})$ и $i \in \{1, \ldots, N(d)\}$. Следовательно, по [2, предложение 3(б)] граф $\Gamma_{\mathbb{Z}^d,M}$ изоморфен графу $\Gamma_{\mathbb{Z}^d,Ma^{-1}}$, соответствующему G_i-орбите $Ma^{-1} = xa^{-1}G_i$.

Будем говорить,что конечная подгруппа G группы $\mathrm{GL}_d(\mathbb{Z})$ имеет *бесконечный орбитный тип*, если ее орбитам на $\mathbb{Z}^d$ соответствует счетное число попарно не изоморфных минимальных графов Кэли группы $\mathbb{Z}^d$; в противном случае будем говорить, что группа G имеет *конечный орбитный тип*. Из [2, предложение 3(б)] следует, что свойство конечной подгруппы группы $\mathrm{GL}_d(\mathbb{Z})$ иметь конечный орбитный тип инвариантно при сопряжении элементами из $\mathrm{GL}_d(\mathbb{Z})$. Поэтому можно считать, что это свойство определено для $\mathbb{Z}$-классов конечных подгрупп группы $\mathrm{GL}_d(\mathbb{Z})$.

Из [5, табл. 1] следует, что при $d = 4$ число $\mathbb{Z}$-классов конечных подгрупп группы $\mathrm{GL}_d(\mathbb{Z})$ равно 710. Следующая теорема позволяет заключить, что только три из них имеют бесконечный орбитный тип.

Теорема 1. *С точностью до сопряжения в $\mathrm{GL}_4(\mathbb{Z})$ подгруппы бесконечного орбитного типа группы $\mathrm{GL}_4(\mathbb{Z})$ исчерпываются группами $G_1 = \langle h_1, h_2 \rangle$, $G_2 = \langle f_1, f_2, f_3 \rangle$, $G_3 = \langle G_2, f_4 \rangle$, где*

$$h_1 = \begin{pmatrix} 0 & 0 & -1 & -1 \\ 0 & -1 & -1 & -1 \\ 0 & 0 & 0 & -1 \\ -1 & 1 & 1 & 1 \end{pmatrix}, \qquad h_2 = \begin{pmatrix} 0 & -1 & -1 & -1 \\ 0 & -1 & 0 & -1 \\ 1 & -1 & -1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix},$$

$$f_1 = \begin{pmatrix} -1 & 1 & 1 & 0 \\ -1 & 0 & 0 & -1 \\ -1 & 1 & 1 & 1 \\ 1 & 0 & -1 & 0 \end{pmatrix}, \qquad f_2 = \begin{pmatrix} 0 & -1 & 0 & -1 \\ 1 & -1 & -1 & -1 \\ -1 & 0 & 0 & -1 \\ 0 & 1 & 1 & 1 \end{pmatrix},$$

$$f_3 = \begin{pmatrix} -1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ -1 & 0 & 0 & 0 \\ 1 & -1 & -1 & -1 \end{pmatrix}, \qquad f_4 = \begin{pmatrix} -1 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ -1 & 0 & 1 & 0 \\ 1 & -1 & -1 & -1 \end{pmatrix}.$$

З а м е ч а н и е 1. Легко убедиться, что группы G_1, G_2, G_3, определенные в теореме 1, имеют следующее строение: $G_1 = \langle h_1 \rangle \leftthreetimes \langle h_2 \rangle$, где $|h_1| = 8$, $|h_2| = 3$ и $h_2^{h_1} = h_2^{-1}$; $G_2 = \langle f_1, f_2 \rangle \times \langle f_3 \rangle$, где $\langle f_1, f_2 \rangle \cong Q_8$ и $|f_3| = 3$; $G_3 = \langle f_4 \rangle \leftthreetimes G_2$, где $|f_4| = 2$, $f_1^{f_4} = f_1^{-1}$, $f_2^{f_4} = f_1 f_2$ и $f_3^{f_4} = f_3^{-1}$.

Следующая теорема является основным результатом данной работы.

Теорема 2. (1) *Каждый граф Кэли группы $\mathbb{Z}^4$, соответствующий G_1- или G_2-орбите на $\mathbb{Z}^4$, является предельным для множества минимальных вершинно-примитивных графов HA-типа.*

(2) *Существует с точностью до изоморфизма лишь конечное число минимальных графов Кэли группы $\mathbb{Z}^4$, не соответствующих никакой орбите группы G_1 или группы G_2 на $\mathbb{Z}^4$.*

З а м е ч а н и е 2. Из доказательства теоремы 2 видно, что каждый минимальный граф Кэли группы $\mathbb{Z}^4$, соответствующий G_3-орбите на $\mathbb{Z}^4$, соответствует также G_2-орбите на $\mathbb{Z}^4$.

Статья имеет следующее строение. В § 1 формулируются достаточные условия конечности орбитного типа конечной подгруппы группы $\mathrm{GL}_d(\mathbb{Z})$ и другие вспомогательные результаты. В § 2 с помощью проверки этих условий для всех 710 $\mathbb{Z}$-классов конечных подгрупп группы $\mathrm{GL}_4(\mathbb{Z})$ выясняется, что только три из них могут иметь бесконечный орбитный тип. Эта проверка осуществляется с использованием алгоритмов 1 и 2, реализованных в компьютерной системе GAP [6]. В § 3 доказательство теоремы 1 завершается проверкой того, что три оставшиеся $\mathbb{Z}$-класса конечных подгрупп группы $\mathrm{GL}_4(\mathbb{Z})$ имеют бесконечный орбитный тип. В § 4 содержится доказательство теоремы 2.

1. Вспомогательные результаты

Всюду в настоящем параграфе G — это конечная подгруппа группы $\mathrm{GL}_d(\mathbb{Z})$.

В предложениях 1–5 получены достаточные условия конечности орбитного типа группы G. Заключения предложений 1, 2 и 4 являются более сильными, чем конечность орбитного типа группы G. В предложении 7 (с использованием предложения 6) получено достаточное условие того, что каждый граф Кэли группы $\mathbb{Z}^d$, соответствующий G-орбите, является предельным для множества минимальных вершинно-примитивных графов HA-типа. Для формулировки предложений нам понадобятся следующие обозначения.

Напомним, что $\mathrm{fix}(a) = \{x \in \mathbb{Q}^d : xa = x\}$ для $a \in \mathrm{GL}_d(\mathbb{Z})$ и $G_U = \{g \in G : U \le \mathrm{fix}(g)\}$ для $U \le \mathbb{Q}^d$. Положим

$$m(G) = \min\{|xG| : x \in \mathbb{Q}^d \setminus \{0\}\},$$

$$c_1(G) = \max\{|G_U| : U \le \mathbb{Q}^d,\ \dim(U) \ge 1\},$$

$$c_2(G) = \max\{|G_U| : U \le \mathbb{Q}^d,\ \dim(U) \ge 2\},$$

$$\mathcal{M}_{\mathbb{Q}}(G) = \{xG : x \in \mathbb{Q}^d,\ |xG| = m(G)\},$$

$$\mathcal{M}_{\mathbb{Z}}(G) = \{xG : x \in \mathbb{Z}^d,\ \langle xG \rangle = \mathbb{Z}^d,\ xG = -xG,\ |xG| = m(G)\}.$$

Очевидно, что $m(G) = \min\{|xG| : x \in \mathbb{Z}^d \setminus \{0\}\}$, и, следовательно, множество $\mathcal{M}_{\mathbb{Q}}(G)$ содержит все G-орбиты минимальной мощности на $\mathbb{Z}^d \setminus \{0\}$. Очевидно также, что $c_1(G) = \max\{|G_x| : x \in \mathbb{Z}^d \setminus \{0\}\}$, откуда

$$m(G)c_1(G) = |G|. \tag{1.1}$$

Множества $M_1, M_2 \subseteq \mathbb{Q}^d$ назовем *линейно эквивалентными*, если существует матрица $b \in \mathrm{GL}_d(\mathbb{Q})$ такая, что $M_1 b = M_2$.

Предложение 1. *Пусть $m(G) \leq 2d$. Тогда орбитам группы G с точностью до изоморфизма соответствует не более одного графа Кэли группы $\mathbb{Z}^d$.*

Доказательство. Пусть $\Gamma_{\mathbb{Z}^d,M}$ — граф Кэли группы $\mathbb{Z}^d$, соответствующий G-орбите M. Поскольку $M = -M$, то $M = \{x_1, \ldots, x_n, -x_1, \ldots, -x_n\}$ для некоторых $x_1, \ldots, x_n \in \mathbb{Z}^d$. Поскольку $\langle M\rangle = \mathbb{Z}^d$ и $|M| \leq 2d$, то $n = d$ и векторы $x_1, \ldots, x_d$ линейно независимы над $\mathbb{Q}$.

Пусть $\Gamma_{\mathbb{Z}^d,M'}$ — еще один граф Кэли группы $\mathbb{Z}^d$, соответствующий G-орбите M'. Аналогично получаем, что $M' = \{x'_1, \ldots, x'_d, -x'_1, \ldots, -x'_d\}$ для некоторых $x'_1, \ldots, x'_d \in \mathbb{Z}^d$ и векторы $x'_1, \ldots, x'_d$ линейно независимы над $\mathbb{Q}$. Тогда существует матрица $b \in \mathrm{GL}_d(\mathbb{Q})$ такая, что $x_i b = x'_i$ для $i = 1, \ldots, d$. Следовательно, множества M и M' линейно эквивалентны, и соответствующие им графы $\Gamma_{\mathbb{Z}^d,M}$ и $\Gamma_{\mathbb{Z}^d,M'}$ изоморфны по [2, предложение 3(б)].

Предложение доказано.

Предложение 2. *Пусть группа G циклическая и $c_1(G) = 1$. Тогда орбитам группы G с точностью до изоморфизма соответствует не более одного графа Кэли группы $\mathbb{Z}^d$.*

Доказательство. По условию $G = \langle a\rangle$ для некоторого $a \in \mathrm{GL}_d(\mathbb{Z})$. Имеем

$$a^d + \beta_1 a^{d-1} + \cdots + \beta_{d-1} a + \beta_d E_d = 0, \tag{1.2}$$

где $\lambda^d + \beta_1 \lambda^{d-1} + \cdots + \beta_{d-1}\lambda + \beta_d$ — характеристический многочлен матрицы a.

Индукцией по k покажем, что для любого целого $k \geq d$ существуют такие коэффициенты $\gamma_{1,k}, \ldots, \gamma_{d,k} \in \mathbb{Z}$, что для любого $x \in \mathbb{Z}^d \setminus \{0\}$

$$xa^k = \gamma_{1,k} xa^{d-1} + \gamma_{2,k} xa^{d-2} + \cdots + \gamma_{d,k} x. \tag{1.3}$$

База индукции при $k = d$ следует из (1.2). Предположим теперь, что доказываемое утверждение справедливо для некоторого $k \geq d$ и покажем его справедливость для $k + 1$. Имеем

$$xa^{k+1} = (xa^k)a = (\gamma_{1,k} xa^{d-1} + \gamma_{2,k} xa^{d-2} + \cdots + \gamma_{d,k} x)a,$$

что в силу (1.2) равняется

$$\begin{aligned}&\gamma_{1,k} x(-\beta_1 a^{d-1} - \cdots - \beta_{d-1} a - \beta_d E_d) + \gamma_{2,k} xa^{d-1} + \cdots + \gamma_{d,k} xa \\ &= (\gamma_{2,k} - \gamma_{1,k}\beta_1) xa^{d-1} + \cdots + (\gamma_{d,k} - \gamma_{1,k}\beta_{d-1}) xa - \gamma_{1,k}\beta_d x.\end{aligned}$$

Полагая $\gamma_{i,k+1} = \gamma_{i+1,k} - \gamma_{1,k}\beta_i$ для $i = 1, \ldots, d-1$ и $\gamma_{d,k+1} = -\gamma_{1,k}\beta_d$, завершаем шаг индукции.

Пусть $\Gamma_{\mathbb{Z}^d,M}$ — граф Кэли группы $\mathbb{Z}^d$, соответствующий G-орбите M, и $x \in M$. Тогда векторы $xa^{d-1}, \ldots, xa, x$ линейно независимы над $\mathbb{Q}$ (в противном случае в силу (1.3) ранг xG над $\mathbb{Q}$ был бы меньше d, что противоречит условию $\langle xG\rangle = \langle M\rangle = \mathbb{Z}^d$). Пусть $\Gamma_{\mathbb{Z}^d,M'}$ — еще один граф Кэли группы $\mathbb{Z}^d$, соответствующий G-орбите M', и $x' \in M'$. Аналогично заключаем, что векторы $x'a^{d-1}, \ldots, x'a, x'$ линейно независимы над $\mathbb{Q}$. Следовательно, существует матрица $b \in \mathrm{GL}_d(\mathbb{Q})$ такая, что $xa^i b = x'a^i$ для $i = 0, \ldots, d-1$. Тогда в силу (1.3) имеем $xa^k b = x'a^k$ для любого $k \geq d$. Следовательно, множества M и M' линейно эквивалентны, и соответствующие им графы $\Gamma_{\mathbb{Z}^d,M}$ и $\Gamma_{\mathbb{Z}^d,M'}$ изоморфны по [2, предложение 3(б)]. Предложение доказано.

Предложение 3. *Пусть $c_1(G)>c_2(G)$. Тогда группа G имеет конечный орбитный тип.*

Д о к а з а т е л ь с т в о. Достаточно показать конечность множества $\mathcal{M}_{\mathbb{Z}}(G)$.

Пусть $D = \{U \leq \mathbb{Q}^d : |G_U| = c_1(G)\}$. Покажем, что множество D конечно. Для этого рассмотрим отображение ψ множества D в 2^G, задаваемое формулой $\psi(U) = G_U$ для $U \in D$. Отображение ψ инъективно, поскольку если $G_U = G_{U'}$ для $U, U' \in D$, то $G_{U+U'} = G_U$, откуда в силу $c_1(G)>c_2(G)$ имеем $\dim(U + U') = 1$ и, следовательно, $U = U'$. Таким образом, $|D| \leq 2^{|G|}$.

Из определения множества D следует, что оно G-инвариантно. Пусть D_1 — множество G-орбит на D, т.е. $D_1 = \{\bigcup_{g\in G} Ug : U \in D\}$. Рассмотрим отображение χ множества $\mathcal{M}_{\mathbb{Z}}(G)$ в D_1, задаваемое формулой $\chi(M) = \mathbb{Q}M$ для $M \in \mathcal{M}_{\mathbb{Z}}(G)$. Отображение χ определено корректно, так как для $M \in \mathcal{M}_{\mathbb{Z}}(G)$ и $x \in M$ имеем $|G_{\mathbb{Q}x}| = c_1(G)$, откуда $\mathbb{Q}x \in D$ и, следовательно, $\mathbb{Q}M \in D_1$. Отображение χ инъективно, поскольку если $\mathbb{Q}M = \mathbb{Q}M'$ для $M, M' \in \mathcal{M}_{\mathbb{Z}}(G)$, то в силу $\langle M\rangle = \langle M'\rangle = \mathbb{Z}^d$ и $M = -M$, $M' = -M'$ имеем $M = M'$. Таким образом, $|\mathcal{M}_{\mathbb{Z}}(G)| \leq |D_1| \leq |D|$, и предложение доказано.

Следующее предложение следует из [2, предложение 3(б)].

Предложение 4. *Пусть все элементы из $\mathcal{M}_{\mathbb{Q}}(G)$ попарно линейно эквивалентны. Тогда орбитам группы G с точностью до изоморфизма соответствует не более одного графа Кэли группы $\mathbb{Z}^d$.*

Предложение 5. *Пусть H, G — конечные подгруппы группы $\mathrm{GL}_d(\mathbb{Z})$, группа H имеет конечный орбитный тип, $m(H) = m(G)$ и $H^b < G$ для некоторого $b \in \mathrm{GL}_d(\mathbb{Q})$. Тогда для любого $a \in \mathrm{GL}_d(\mathbb{Q})$ такого, что $G^a < \mathrm{GL}_d(\mathbb{Z})$, группа G^a имеет конечный орбитный тип.*

Д о к а з а т е л ь с т в о. Имеем $H^{ba} < G^a$ и $m(H^{ba}) = m(H) = m(G) = m(G^a)$, откуда $\mathcal{M}_{\mathbb{Z}}(G^a) \subseteq \mathcal{M}_{\mathbb{Z}}(H^{ba})$. Если бы группа G^a имела бесконечный орбитный тип, то и группа H^{ba} имела бы бесконечный орбитный тип, что противоречит конечности орбитного типа группы H. Следовательно, группа G^a имеет конечный орбитный тип и предложение доказано.

Классы сопряженных в $\mathrm{GL}_d(\mathbb{Q})$ конечных подгрупп группы $\mathrm{GL}_d(\mathbb{Z})$ будем называть $\mathbb{Q}$-*классами* конечных подгрупп группы $\mathrm{GL}_d(\mathbb{Z})$. Очевидно, что каждый $\mathbb{Q}$-класс является объединением $\mathbb{Z}$-классов.

Будем говорить, что $\mathbb{Q}$-класс конечных подгрупп группы $\mathrm{GL}_d(\mathbb{Z})$ имеет конечный орбитный тип, если все группы данного $\mathbb{Q}$-класса имеют конечный орбитный тип.

З а м е ч а н и е 3. Условия на группу G в предложениях 1–5 сохраняются при сопряжении группы G элементом из $\mathrm{GL}_d(\mathbb{Q})$. Следовательно, они являются достаточными для того, чтобы $\mathbb{Q}$-класс конечных подгрупп группы $\mathrm{GL}_d(\mathbb{Z})$, содержащий G, имел конечный орбитный тип.

Пусть p — простое число, $\mathbb{Z}_p$ — аддитивная группа вычетов по модулю p и $\pm\mathrm{SL}_d(p)$ — группа $d\times d$-матриц над $\mathbb{Z}_p$ с определителями ±1. Через ϕ_p обозначим гомоморфизм группы $\mathrm{GL}_d(\mathbb{Z})$ в группу $\pm\mathrm{SL}_d(p)$, который каждой матрице $a \in \mathrm{GL}_d(\mathbb{Z})$ ставит в соответствие матрицу $\phi_p(a) \in \pm\mathrm{SL}_d(p)$, элементы которой являются p-вычетами соответствующих элементов матрицы a.

Предложение 6. *Если $c_1(G) = 1$, то существует такое целое число p_0, что для всех простых $p > p_0$ и каждого $x \in \mathbb{Z}_p^d \setminus \{0\}$ справедливо равенство $|x\phi_p(G)| = |\phi_p(G)|$.*

Д о к а з а т е л ь с т в о. Пусть g — неединичный элемент группы G. Тогда $\mathrm{fix}(g) = \{0\}$ и, следовательно, $\det(g-E_d) \neq 0$, где E_d — единичная $d\times d$-матрица. Тогда $\det(g-E_d) \not\equiv 0(p)$ при $p > p_0$, где $p_0 = \max\{|\det(h - E_d)| : h \in G\}$. Следовательно, при $p > p_0$ уравнение $x\phi_p(g) = x$ относительно $x \in \mathbb{Z}_p^d$ имеет только нулевое решение. Предложение доказано.

Предложение 7. *Пусть P — бесконечное множество простых чисел такое, что для каждого $p \in P$ группа $\phi_p(G)$ действует неприводимо на $\mathbb{Z}_p^d$. Тогда справедливы следующие утверждения*:

(1) *Каждый граф Кэли группы $\mathbb{Z}^d$, соответствующий G-орбите, является предельным для множества вершинно-примитивных графов HA-типа.*

(2) *Если, кроме того, $c_1(G) = 1$, то каждый граф Кэли группы $\mathbb{Z}^d$, соответствующий G-орбите, является предельным для множества минимальных вершинно-примитивных графов HA-типа.*

Доказательство. Пусть $\Gamma_{\mathbb{Z}^d,M}$ — граф Кэли группы $\mathbb{Z}^d$, соответствующий G-орбите M. Для каждого $p \in P$ через M_p обозначим образ множества M при естественном гомоморфизме $\mathbb{Z}^d$ на $\mathbb{Z}_p^d$. Очевидно, что M_p является $\phi_p(G)$-орбитой, $\langle M_p \rangle = \mathbb{Z}_p^d$, $M_p = -M_p$ и $0 \notin M_p$. Легко видеть, что граф $\Gamma_{\mathbb{Z}^d,M}$ является предельным для множества графов Кэли $\{\Gamma_{\mathbb{Z}_p^d,M_p} : p \in P\}$.

Пусть $p \in P$. Граф $\Gamma_{\mathbb{Z}_p^d,M_p}$ допускает группу автоморфизмов $\phi_p(G) \leftthreetimes t(\mathbb{Z}_p^d)$, где $t(\mathbb{Z}_p^d)$ — регулярная абелева группа сдвигов на элементы из $\mathbb{Z}_p^d$. Тогда из неприводимости $\phi_p(G)$ следует, что $\phi_p(G) \leftthreetimes t(\mathbb{Z}_p^d)$ является вершинно-примитивной группой HA-типа. Таким образом, граф $\Gamma_{\mathbb{Z}^d,M}$ является предельным для множества вершинно-примитивных графов HA-типа, и утверждение (1) доказано. Если $c_1(G) = 1$, то из предложения 6 следует, что если p достаточно велико, то граф $\Gamma_{\mathbb{Z}_p^d,M_p}$ является минимальным вершинно-примитивным графом HA-типа. Таким образом, утверждение (2) выполнено и предложение доказано.

2. Начало доказательства теоремы 1: проверка достаточных условий конечности орбитного типа для подгрупп группы $\mathrm{GL}_4(\mathbb{Z})$

Опишем алгоритмы 1 и 2 вычисления $c_1(G)$ и $c_2(G)$ соответственно для произвольной конечной подгруппы G группы $\mathrm{GL}_d(\mathbb{Z})$. Они будут использованы для проверки конечности орбитного типа большинства $\mathbb{Q}$-классов конечных подгрупп группы $\mathrm{GL}_d(\mathbb{Z})$.

Из определения $c_1(G)$ следует, что $c_1(G) = \max\{|K| : K \subseteq G, \bigcap_{g \in K} \mathrm{fix}(g) \neq \{0\}\}$. Оценка снизу для $c_1(G)$ вычисляется алгоритмом 1 путем перебора подмножеств множества подпространств $\{\mathrm{fix}(g) : g \in G, \mathrm{fix}(g) \neq \{0\}\}$ пространства $\mathbb{Q}^d$ (будем называть такие подпространства *атомарными*). Для точного вычисления $c_1(G)$ может понадобиться $2^{|G|}$ итераций алгоритма. Для ограничения числа итераций алгоритма вводится параметр T. Если перебор неполный, то алгоритм выдает оценку снизу для $c_1(G)$. Чем больше значение T, тем выдаваемая оценка точнее. Ниже приведена запись алгоритма 1 на неформальном PASCAL-подобном языке программирования.

АЛГОРИТМ 1. ВЫЧИСЛЕНИЕ ОЦЕНКИ СНИЗУ ДЛЯ $c_1(G)$.

Входные данные:

G — конечная подгруппа группы $\mathrm{GL}_d(\mathbb{Z})$,

T — ограничение числа итераций алгоритма.

Результаты:

c — оценка снизу для $c_1(G)$,

b — признак точности оценки c (если оценка точна, то $b =$ И),

D — множество $\{\bigcap_{g \in K} \mathrm{fix}(G) : K \subseteq G, \bigcap_{g \in K} \mathrm{fix}(g) \neq \{0\}, |K| = c_1(G)\}$ (если $b =$ И).

Инициализация:

$V := \varnothing$; // массив атомарных подпространств

for $g \in G$

  if $\mathrm{fix}(g) \neq \{0\}$ **then** добавить $\mathrm{fix}(g)$ в V; **end if;**

end for;

$n :=$ размер(V); // число атомарных подпространств

6. $t := 0$; // номер итерации основного цикла
7. $c := 0$; // текущая оценка снизу для $c_1(G)$
8. $S := \varnothing$; // стек номеров атомарных подпространств
9. $l := 1$; // номер рассматриваемого атомарного подпространства
10. $D := \varnothing$;

Основной цикл:

11. **while** $l \le n$ **and** $t \le T$
12. $t := t + 1$;
13. **while** $V_l \cap \bigcap_{i \in S} V_i = \{0\}$ **and** $l \le n$
14. l:=l+1;
15. **end while;**
16. **if** $l \le n$ **then**
17. добавить l в S;
18. $l := l + 1$;
19. **else**
20. $l :=$ вершина$(S) + 1$;
21. **if** $c <$ размер(S) **then**
22. $c :=$ размер(S);
23. $D := \{\bigcap_{i \in S} V_i\}$;
24. **else if** $c =$ размер(S) **then**
25. $D := D \cup \{\bigcap_{i \in S} V_i\}$;
26. **end if;**
27. удалить вершину из S;
28. **end if**;
29. **end while**;

Выдача результатов:

30. **if** $t \le T$ **then** // $c_1(G) = c$
31. **return** c, И, D;
32. **else** // $c_1(G) \ge c$
33. **return** c, Л;
34. **end if;**

Алгоритм 1 ищет максимальное число атомарных подпространств с непустым пересечением. Этот поиск осуществляется методом бектрекинга [7, с. 124–128] с дополнительным ограничением T числа итераций алгоритма. Сначала в строках 1–4 заполняется массив V атомарных подпространств. Затем в основном цикле алгоритма в соответствии с изменением стека S номеров атомарных подпространств происходит перебор подмножеств множества всех атомарных подпространств (стек S соответствует подмножеству $\{V_i : i \in S\}$). В цикле 13–15 путем последовательного увеличения переменной l ищется атомарное подпространство V_l, имеющее непустое пересечение с атомарными подпространствами, номера которых лежат в S. Если подпространство V_l найдено, то в строке 17 номер l добавляется в S. В противном случае в строке 27 из стека удаляется вершина. При этом в случае необходимости улучшается текущее значение оценки c и изменяется множество D. Гарантией того, что значение переменной S не повторяется в ходе работы алгоритма, служит строка 20, благодаря которой удаленная из стека S вершина не будет опять в него сразу добавлена. Выдача результатов в строках 30–34 происходит в зависимости от того, завершил ли бектрекинг свою работу или был прерван из-за того, что число итераций основного цикла превысило ограничение T.

Для вычисления $c_2(G)$ разработан алгоритм 2, аналогичный по структуре алгоритму 1. Отличия состоят в следующем:

1) Условия $\mathrm{fix}(g) \ne \{0\}$ и $V_l \cap \bigcap_{i \in S} V_i = \{0\}$ (в строках 3 и 13) заменяются, соответственно, на

условия $\dim(\text{fix}(g)) \geq 2$ и $\dim(V_l \cap \bigcap_{i \in S} V_i) < 2$.
2) Алгоритм 2 вычисляет $c_2(G)$ точно, поэтому отсутствует ограничивающий параметр T.

Перейдем к описанию того, как представители 710 $\mathbb{Z}$-классов конечных подгрупп группы $\mathrm{GL}_4(\mathbb{Z})$ могут быть получены при помощи пакета CrystCat компьютерной системы GAP.

В [5, табл. 1] множество всех конечных подгрупп группы $\mathrm{GL}_4(\mathbb{Z})$ разбито на 33 подмножества, названных *кристаллическими системами*, каждое из которых является объединением нескольких $\mathbb{Q}$-классов конечных подгрупп группы $\mathrm{GL}_4(\mathbb{Z})$. При этом введена нумерация кристаллических систем, нумерация $\mathbb{Q}$-классов в каждой кристаллической системе и нумерация $\mathbb{Z}$-классов в каждом $\mathbb{Q}$-классе. Пусть i — номер некоторой кристаллической системы и j — номер $\mathbb{Q}$-класса в ней. Тогда обозначим данный $\mathbb{Q}$-класс через $Q_{i,j}$.

Пакет CrystCat компьютерной системы GAP содержит упомянутую таблицу из [5] в электронном виде. В частности, он содержит следующие три функции (значение первого параметра d каждой из этих функций для наших целей следует брать равным 4).

$\bullet NrQClassesCrystalSystem(d,i)$ выдает число $\mathbb{Q}$-классов в кристаллической системе с номером $i \in \{1,\dots,33\}$.

$\bullet NrZClassesQClass(d,i,j)$ выдает число $\mathbb{Z}$-классов в $\mathbb{Q}$-классе $Q_{i,j}$.

$\bullet MatGroupZClass(d,i,j,k)$ выдает матричную группу, являющуюся представителем k-го $\mathbb{Z}$-класса $\mathbb{Q}$-класса $Q_{i,j}$.

Через $G_{i,j}$ обозначим представителя первого $\mathbb{Z}$-класса $\mathbb{Q}$-класса $Q_{i,j}$, полученного с помощью вызова $MatGroupZClass(4,i,j,1)$.

Ниже приводится таблица, содержащая результаты применения алгоритмов 1, 2, реализованных в компьютерной системе GAP, к каждой из групп $G_{i,j}$.

Строки таблицы соответствуют $\mathbb{Q}$-классам. Строка, соответствующая $\mathbb{Q}$-классу $Q_{i,j}$ содержит следующие семь элементов. Первые пять — это номер строки (полученный в результате определенной сквозной нумерации $\mathbb{Q}$-классов), номер i, номер j, число $\mathbb{Z}$-классов в $\mathbb{Q}$-классе $Q_{i,j}$, порядок $G_{i,j}$. Шестой элемент — это оценка снизу для $c_1(G_{i,j})$, вычисленная с помощью алгоритма 1 при $T = 1000$ (имеет вид "c", если $c_1(G_{i,j}) = c$ и "$\geq c$", если $c_1(G_{i,j}) \geq c$). Седьмой элемент содержит $c_2(G_{i,j})$, вычисленное с помощью алгоритма 2.

Т а б л и ц а

Результаты применения алгоритмов 1,2 к каждому из $\mathbb{Q}$-классов
конечных подгрупп группы $\mathrm{GL}_4(\mathbb{Z})$

Номер строки	i	j	Число $\mathbb{Z}$-классов	$\lvert G_{i,j}\rvert$	c_1	c_2		Номер строки	i	j	Число $\mathbb{Z}$-классов	$\lvert G_{i,j}\rvert$	c_1	c_2
1	1	1	1	1	1	1		2	1	2	1	2	1	1
3	2	1	2	2	2	2		4	2	2	2	2	2	1
5	2	3	2	4	2	2		6	3	1	3	2	2	2
7	3	2	3	4	2	2		8	4	1	6	4	4	4
9	4	2	7	4	4	2		10	4	3	6	4	2	2
11	4	4	6	8	4	4		12	5	1	13	4	4	2
13	5	2	9	8	4	2		14	6	1	12	8	8	4
15	6	2	12	8	4	2		16	6	3	8	16	8	4
17	7	1	2	4	2	2		18	7	2	2	4	4	4
19	7	3	2	8	4	4		20	7	4	4	8	4	4
21	7	5	2	8	4	4		22	7	6	2	8	8	8
23	7	7	2	16	8	8		24	8	1	2	3	3	3
25	8	2	2	6	3	3		26	8	3	3	6	6	6
27	8	4	3	6	3	3		28	8	5	3	12	6	6
29	9	1	1	6	6	6		30	9	2	1	6	3	3

Т а б л и ц а (продолжение)

Номер строки	i	j	Число $\mathbb{Z}$-классов	$\lvert G_{i,j}\rvert$	c_1	c_2		Номер строки	i	j	Число $\mathbb{Z}$-классов	$\lvert G_{i,j}\rvert$	c_1	c_2
31	9	3	1	12	6	6		32	9	4	1	12	12	12
33	9	5	1	12	6	6		34	9	6	2	12	6	6
35	9	7	1	24	12	12		36	10	1	1	4	1	1
37	11	1	1	3	1	1		38	11	2	1	6	1	1
39	12	1	7	4	4	2		40	12	2	6	8	4	2
41	12	3	13	8	8	4		42	12	4	13	8	4	2
43	12	5	11	16	8	4		44	13	1	6	8	8	4
45	13	2	6	8	4	2		46	13	3	6	8	4	2
47	13	4	6	8	8	4		48	13	5	5	16	8	4
49	13	6	6	16	16	8		50	13	7	12	16	8	4
51	13	8	6	16	8	4		52	13	9	5	16	8	4
53	13	10	5	32	8	8		54	14	1	4	6	6	3
55	14	2	4	6	6	3		56	14	3	8	6	6	3
57	14	4	4	12	6	3		58	14	5	4	12	6	3
59	14	6	6	12	12	6		60	14	7	6	12	6	3
61	14	8	6	12	12	6		62	14	9	6	12	6	3
63	14	10	6	24	12	6		64	15	1	2	12	12	6
65	15	2	2	12	6	4		66	15	3	2	12	6	3
67	15	4	2	12	12	6		68	15	5	4	12	6	3
69	15	6	2	24	24	12		70	15	7	4	24	8	6
71	15	8	2	24	12	6		72	15	9	2	24	12	6
73	15	10	4	24	12	6		74	15	11	2	24	12	6
75	15	12	2	48	8	12		76	16	1	3	8	2	2
77	17	1	3	6	2	2		78	17	2	2	12	2	2
79	18	1	3	8	2	2		80	18	2	5	16	4	4
81	18	3	7	16	4	2		82	18	4	5	16	4	2
83	18	5	7	32	8	4		84	19	1	2	16	4	4
85	19	2	2	16	4	4		86	19	3	2	32	8	8
87	19	4	4	32	8	4		88	19	5	2	32	8	4
89	19	6	2	64	16	8		90	20	1	1	12	4	4
91	20	2	1	12	3	3		92	20	3	2	12	4	3
93	20	4	2	24	8	6		94	20	5	1	24	6	6
95	20	6	1	24	6	4		96	20	7	2	24	8	4
97	20	8	1	24	8	8		98	20	9	2	24	6	6
99	20	10	2	24	6	4		100	20	11	2	24	6	3
101	20	12	4	24	8	4		102	20	13	4	24	6	3
103	20	14	1	24	6	6		104	20	15	1	48	8	12
105	20	16	2	48	8	6		106	20	17	2	48	16	8
107	20	18	1	48	8	8		108	20	19	1	48	8	6
109	20	20	4	48	8	6		110	20	21	2	48	8	6
111	20	22	1	96	16	12		112	21	1	2	6	2	2
113	21	2	2	12	2	2		114	21	3	4	12	4	2
115	21	4	2	24	4	2		116	22	1	2	9	3	3
117	22	2	2	18	3	3		118	22	3	3	18	6	6
119	22	4	3	18	6	3		120	22	5	5	18	6	3
121	22	6	3	36	6	6		122	22	7	3	36	6	3
123	22	8	4	36	12	6		124	22	9	5	36	12	6
125	22	10	4	36	6	3		126	22	11	4	72	12	6

Т а б л и ц а (продолжение)

Номер строки	i	j	Число $\mathbb{Z}$-классов	$\lvert G_{i,j}\rvert$	c_1	c_2	Номер строки	i	j	Число $\mathbb{Z}$-классов	$\lvert G_{i,j}\rvert$	c_1	c_2
127	23	1	1	18	6	6	128	23	2	1	36	6	6
129	23	3	1	36	6	6	130	23	4	1	36	12	12
131	23	5	2	36	12	6	132	23	6	2	36	12	6
133	23	7	1	72	12	12	134	23	8	1	72	12	6
135	23	9	2	72	12	6	136	23	10	2	72	12	11
137	23	11	1	144	24	12	138	24	1	6	12	12	3
139	24	2	6	24	12	3	140	24	3	6	24	24	6
141	24	4	6	24	12	3	142	24	5	6	48	8	6
143	25	1	5	24	24	4	144	25	2	5	24	6	3
145	25	3	5	24	24	4	146	25	4	5	24	6	3
147	25	5	5	48	8	4	148	25	6	5	48	8	4
149	25	7	5	48	48	8	150	25	8	5	48	8	4
151	25	9	5	48	8	6	152	25	10	5	48	8	4
153	25	11	5	96	16	8	154	26	1	1	8	1	1
155	26	2	1	16	2	2	156	27	1	1	5	1	1
157	27	2	1	10	1	1	158	27	3	2	10	2	2
159	27	4	1	20	2	2	160	28	1	1	12	1	1
161	28	2	1	24	2	2	162	29	1	3	18	3	3
163	29	2	2	36	3	3	164	29	3	5	36	6	3
165	29	4	4	36	6	3	166	29	5	2	72	5	3
167	29	6	3	72	6	3	168	29	7	4	72	8	6
169	29	8	4	72	6	3	170	29	9	3	144	12	6
171	30	1	1	12	1	1	172	30	2	1	24	2	2
173	30	3	1	24	2	2	174	30	4	2	24	2	2
175	30	5	1	36	3	3	176	30	6	1	48	4	2
177	30	7	1	72	6	6	178	30	8	1	72	6	3
179	30	9	1	72	6	3	180	30	10	1	144	12	6
181	30	11	1	144	12	6	182	30	12	2	144	12	6
183	30	13	1	288	≥ 24	12	184	31	1	4	20	4	2
185	31	2	2	40	4	2	186	31	3	2	60	12	3
187	31	4	2	120	≥ 24	6	188	31	5	2	120	12	3
189	31	6	2	120	12	3	190	31	7	2	240	≥ 24	6
191	32	1	2	8	1	1	192	32	2	2	16	2	2
193	32	3	2	16	2	2	194	32	4	2	16	2	2
195	32	5	3	24	3	3	196	32	6	2	32	4	2
197	32	7	2	32	4	2	198	32	8	2	32	4	4
199	32	9	5	32	4	2	200	32	10	2	32	4	2
201	32	11	3	48	6	3	202	32	12	2	64	8	4
203	32	13	4	64	8	4	204	32	14	4	64	8	4
205	32	15	2	64	8	4	206	32	16	3	96	12	3
207	32	17	2	128	16	8	208	32	18	3	192	24	4
209	32	19	3	192	8	6	210	32	20	3	192	24	4
211	32	21	3	384	48	8	212	33	1	1	24	1	1
213	33	2	1	24	1	1	214	33	3	1	24	1	1
215	33	4	1	48	2	2	216	33	5	1	48	2	2
217	33	6	1	48	2	2	218	33	7	1	72	3	3
219	33	8	1	96	4	2	220	33	9	1	96	4	2
221	33	10	1	96	4	4	222	33	11	1	144	6	3

Т а б л и ц а (продолжение)

Номер строки	i	j	Число $\mathbb{Z}$-классов	$\lvert G_{i,j}\rvert$	c_1	c_2		Номер строки	i	j	Число $\mathbb{Z}$-классов	$\lvert G_{i,j}\rvert$	c_1	c_2
223	33	12	1	192	8	4		224	33	13	1	288	12	3
225	33	14	2	576	≥ 24	6		226	33	15	1	576	≥ 24	4
227	33	16	1	1152	≥ 48	8								

$\mathbb{Q}$-классы конечных подгрупп группы $\mathrm{GL}_4(\mathbb{Z})$, соответствующие строкам 1–156, 158, 162, 164, 165, 168, 184, 186, 191–211 таблицы имеют конечный орбитный тип по предложению 1 и замечанию 3, поскольку для каждого такого $\mathbb{Q}$-класса $Q_{i,j}$ из таблицы имеем $m(G_{i,j}) \leq 8$ в силу (1.1).

С использованием GAP непосредственно проверяется, что группы $G_{27,2}$ и $G_{28,1}$ циклические. Кроме того, из таблицы имеем $c_1(G_{27,2}) = c_1(G_{28,1}) = 1$. Поэтому из предложения 2 и замечания 3 следует, что $\mathbb{Q}$-классы, соответствующие строкам 157 и 160 таблицы, имеют конечный орбитный тип.

$\mathbb{Q}$-классы, соответствующие строкам 166, 167, 169, 170, 176, 178–183, 185, 187–190, 219, 220, 222–227 таблицы имеют конечный орбитный тип по предложению 3 и замечанию 3, поскольку для каждого такого $\mathbb{Q}$-класса $Q_{i,j}$ из таблицы имеем $c_1(G_{i,j}) > c_2(G_{i,j})$.

Следующая лемма нужна для доказательства того, что $\mathbb{Q}$-классы, соответствующие строкам 163, 171 и 214 таблицы, имеют конечный орбитный тип.

Лемма 1. (1) *Для некоторого* $a \in \mathrm{GL}_4(\mathbb{Q})$ *такого, что* $G_{29,2}^a < \mathrm{GL}_4(\mathbb{Z})$, *все элементы из* $\mathcal{M}_{\mathbb{Q}}(G_{29,2}^a)$ *попарно линейно эквивалентны.*

(2) *Все элементы из* $\mathcal{M}_{\mathbb{Q}}(G_{30,1})$ *попарно линейно эквивалентны.*

(3) *Для некоторого* $a \in \mathrm{GL}_4(\mathbb{Q})$ *такого, что* $G_{33,3}^a < \mathrm{GL}_4(\mathbb{Z})$, *все элементы из* $\mathcal{M}_{\mathbb{Q}}(G_{33,3}^a)$ *попарно линейно эквивалентны.*

Д о к а з а т е л ь с т в о. (1) Пусть

$$a = \begin{pmatrix} 1 & 1 & -2 & 1 \\ 2 & -1 & -1 & 2 \\ -1 & 2 & -1 & 2 \\ 1 & 1 & 1 & 1 \end{pmatrix}.$$

Тогда с использованием GAP непосредственно проверяется, что $G_{29,2}^a = \langle g_1, g_2 \rangle$, где

$$g_1 = \begin{pmatrix} 1 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \qquad g_2 = \begin{pmatrix} 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & -1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

и $|G_{29,2}^a| = 36$.

Алгоритм 1 был запущен с входными данными $G = G_{29,2}^a$ и $T = 1000$. В результате было получено $c = 3, b = \text{И}, D = \{U_1, U_2\}$, где $U_1 = \langle (1,0,0,0), (0,1,0,0) \rangle_{\mathbb{Q}}$, $U_2 = \langle (0,0,1,0), (0,0,0,1) \rangle_{\mathbb{Q}}$ (запись $\langle u_1, \dots, u_k \rangle_{\mathbb{Q}}$ обозначает подпространство пространства $\mathbb{Q}^d$, натянутое на векторы $u_1, \dots, u_k \in \mathbb{Q}^d$). Следовательно, $m(G_{29,2}^a) = 12$ по (1.1), и каждый элемент $x \in \mathbb{Q}^4$, для которого $|xG| = 12$, содержится в U_1 или в U_2.

Поскольку для любых $x_1, x_2 \in \mathbb{Q}$ имеем $(0,0,x_2,x_1)g_2 = (x_1,x_2,0,0)$, множество $\mathcal{M}_{\mathbb{Q}}(G_{29,2}^a)$ исчерпывается $G_{29,2}^a$-орбитами вида $(x_1,x_2,0,0)G_{29,2}^a$, где $(x_1,x_2) \in \mathbb{Q}^2 \setminus \{0\}$. Непосредственно проверяется, что для $(x_1,x_2) \in \mathbb{Q}^2 \setminus \{0\}$

$$(1,0,0,0)G_{29,2}^a \begin{pmatrix} x_1 & x_2 & 0 & 0 \\ -x_2 & x_1 + x_2 & 0 & 0 \\ 0 & 0 & x_1 + x_2 & -x_2 \\ 0 & 0 & x_2 & x_1 \end{pmatrix} = (x_1,x_2,0,0)G_{29,2}^a.$$

Поэтому все элементы из $\mathcal{M}_{\mathbb{Q}}(G^a_{29,2})$ попарно линейно эквивалентны, и утверждение (1) доказано.

(2) Имеем $G_{30,1} = \langle g_1, g_2\rangle$, где

$$g_1 = \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & -1 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & -1 & 0 & 0 \end{pmatrix}, \qquad g_2 = \begin{pmatrix} -1 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 1 \\ 0 & 0 & -1 & 0 \end{pmatrix}.$$

Непосредственно проверяется, что для любого $(x_1, x_2, x_3, x_4) \in \mathbb{Q}^4 \setminus \{0\}$

$$(1,0,0,0)G_{30,1} \begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ -x_2 & x_1 + x_2 & -x_4 & x_3 + x_4 \\ -x_3 - x_4 & x_4 & x_1 + x_2 & -x_2 \\ -x_4 & -x_3 & x_2 & x_1 \end{pmatrix} = (x_1, x_2, x_3, x_4)G_{30,1}.$$

Следовательно, все $G_{30,1}$-орбиты на $\mathbb{Q}^4 \setminus \{0\}$ попарно линейно эквивалентны. В частности, все элементы из $\mathcal{M}_{\mathbb{Q}}(G_{30,1})$ попарно линейно эквивалентны, и утверждение (2) доказано.

(3) Пусть

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

Тогда непосредственно с использованием GAP проверяется, что $G^a_{33,3} = \langle g_1, g_2\rangle$, где

$$g_1 = \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & -1 & -1 & -1 \\ 1 & 0 & -1 & 0 \\ -1 & 1 & 1 & 0 \end{pmatrix}, \qquad g_2 = \begin{pmatrix} -1 & 1 & 1 & 0 \\ -1 & 1 & 1 & 1 \\ -1 & 0 & 0 & -1 \\ 1 & -1 & 0 & 0 \end{pmatrix}.$$

Непосредственно проверяется, что для любого $(x_1, x_2, x_3, x_4) \in \mathbb{Q}^4 \setminus \{0\}$

$$(1,0,0,0)G^a_{33,3} \begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ -x_2 & x_1 + x_2 & x_4 & -x_3 + x_4 \\ -x_3 + x_4 & x_2 - x_4 & x_1 + x_2 + x_3 - x_4 & x_2 \\ x_2 - x_4 & -x_2 + x_3 & -x_2 & x_1 + x_3 - x_4 \end{pmatrix}$$
$$= (x_1, x_2, x_3, x_4)G^a_{33,3}.$$

Следовательно, все $G^a_{33,3}$-орбиты на $\mathbb{Q}^4 \setminus \{0\}$ попарно линейно эквивалентны. В частности, все элементы из $\mathcal{M}_{\mathbb{Q}}(G^a_{33,3})$ попарно линейно эквивалентны, и лемма полностью доказана.

Из леммы 1, предложения 4 и замечания 3 следует, что $\mathbb{Q}$-классы конечных подгрупп группы $\mathrm{GL}_4(\mathbb{Z})$, соответствующие строкам 163, 171 и 214, имеют конечный орбитный тип.

С использованием GAP непосредственно проверяется, что

$$G_{27,2} < G_{27,4}, \quad G_{28,1} < G_{28,2}, \quad G^{b_1}_{28,1} < G_{30,2}, \quad G^{b_1}_{28,1} < G_{30,3}, \quad G_{30,1} < G_{30,4}, \quad G_{30,1} < G_{30,5},$$

$$G^{b_2}_{30,1} < G_{30,7}, \quad G_{33,3} < G_{33,5}, \quad G_{33,3} < G_{33,6}, \quad G_{33,3} < G_{33,7}, \quad G_{33,3} < G_{33,10},$$

где

$$b_1 = \begin{pmatrix} -1 & -1 & 0 & 0 \\ 0 & 0 & -1 & 2 \\ 1 & -2 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}, \qquad b_2 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & -1 \\ -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix}.$$

Кроме того, из таблицы имеем

$$m(G_{27,2}) = m(G_{27,4}), \quad m(G_{28,1}) = m(G_{28,2}), \quad m(G_{28,1}) = m(G_{30,2}), \quad m(G_{28,1}) = m(G_{30,3}),$$

$$m(G_{30,1}) = m(G_{30,4}), \quad m(G_{30,1}) = m(G_{30,5}), \quad m(G_{30,1}) = m(G_{30,7}), \quad m(G_{33,3}) = m(G_{33,5}),$$

$$m(G_{33,3}) = m(G_{33,6}), \quad m(G_{33,3}) = m(G_{33,7}), \quad m(G_{33,3}) = m(G_{33,10}).$$

Поэтому из предложения 5 и замечания 3 следует, что $\mathbb{Q}$-классы конечных подгрупп группы $\mathrm{GL}_4(\mathbb{Z})$, соответствующие строкам 159, 161, 172–175, 177, 216–218 и 221 таблицы, имеют конечный орбитный тип.

Мы показали, что все $\mathbb{Q}$-классы конечных подгрупп группы $\mathrm{GL}_4(\mathbb{Z})$, кроме трех, имеют конечный орбитный тип. Исключительные три $\mathbb{Q}$-класса $Q_{33,1}, Q_{33,2}, Q_{33,4}$ соответствуют строкам 212, 213, 215 и, согласно таблице, содержат по одному $\mathbb{Z}$-классу конечных подгрупп группы $\mathrm{GL}_4(\mathbb{Z})$. Представителями этих $\mathbb{Q}$-классов (а, значит, и $\mathbb{Z}$-классов) являются, соответственно, группы G_2, G_1, G_3 из условия теоремы 1, поскольку с использованием GAP непосредственно проверяется, что $G_2 = G_{33,1}^{a_2}$, $G_1 = G_{33,2}^{a_1}$, $G_3 = G_{33,4}^{a_3}$, где

$$a_1 = \begin{pmatrix} 0 & -1 & 0 & -1 \\ 1 & -1 & -1 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & -1 & -1 & -1 \end{pmatrix}, \qquad a_2 = \begin{pmatrix} 1 & 0 & -1 & -1 \\ 1 & -2 & -1 & -1 \\ 1 & 0 & -1 & 1 \\ 2 & -1 & -1 & 0 \end{pmatrix}, \qquad a_3 = \begin{pmatrix} 0 & -1 & -1 & 0 \\ 0 & -1 & -1 & -2 \\ 0 & 1 & -1 & 0 \\ -1 & 0 & -1 & -1 \end{pmatrix}.$$

3. Завершение доказательства теоремы 1: бесконечность орбитного типа групп G_1, G_2, G_3

Для завершения доказательства теоремы 1 теперь достаточно показать, что орбитам каждой из групп G_1, G_2, G_3 соответствует счетное число попарно не изоморфных минимальных графов Кэли группы $\mathbb{Z}^4$.

В доказательстве теоремы из [3] показано, что группа G_1 обладает указанным свойством. Для завершения доказательства теоремы 1 построим счетное множество попарно не изоморфных минимальных графов Кэли группы $\mathbb{Z}^4$, каждый из которых соответствует системе порождающих, являющейся как G_2-, так и G_3-орбитой.

Для целых $n \geq 0$ положим $z_n = (1, 0, 1, 6n + 2)$ и $M_n = z_n G_2$. Заметим, что $z_n f_3 f_4 = z_n$ для каждого $n \geq 0$, и, следовательно, множество M_n является также G_3-орбитой.

Лемма 2. *$\langle M_n \rangle = \mathbb{Z}^4$, $M_n = -M_n$ и $0 \notin M_n$ для каждого $n \geq 0$.*

Доказательство. Для каждого $n \geq 0$ имеем

$$(0,0,-6,-6) = -z_n f_2^{-1} f_1^{-1} f_3^{-1} + z_n f_3 f_1^2 - 2 z_n f_4^{-1} f_3^{-1}$$
$$+ 2 z_n f_1^{-1} f_2^{-1} + z_n f_1^{-1} f_3^{-1} f_4^{-1} + z_n f_4^{-1} f_1^{-1} \in \langle M_n \rangle,$$
$$(1,0,1,2) = z_n f_4^{-1} f_3^{-1} - n((0,0,-6,-6) f_1^{-1} f_2^{-1}$$
$$- (0,0,-6,-6) f_4^{-1} f_3^{-1}) \in \langle M_n \rangle.$$

Следовательно,

$$(0,0,1,0) = (1,0,1,2) f_3 f_1^2 - 2((1,0,1,2) + (1,0,1,2) f_4^{-1} f_1^{-1}) \in \langle M_n \rangle,$$

$$(1,0,0,0) = (0,0,1,0) f_4^{-1} f_3^{-1} \in \langle M_n \rangle,$$
$$(0,0,0,1) = -(0,0,1,0) f_4^{-1} f_1^{-1} \in \langle M_n \rangle,$$

$$(0,1,0,0) = -(0,0,1,0)f_1^{-1}f_2^{-1} \in \langle M_n \rangle,$$

откуда $\langle M_n \rangle = \mathbb{Z}^4$.

Поскольку $f_1^2 = -E_4$, то $M_n = -M_n$. Наконец, условие $0 \notin M_n$ очевидно, и лемма доказана.

Поскольку $G_2 \in Q_{33,1}$, то по таблице из предыдущего параграфа имеем $c_1(G_2) = 1$. Поэтому в силу (1.1) имеем $m(G_2) = |G_2|$, и, следовательно, каждый граф Кэли группы $\mathbb{Z}^4$, соответствующий G_2-орбите, является минимальным. В частности, минимальными являются графы Кэли $\Gamma_{\mathbb{Z}^4, M_n}$ $(n \geq 0)$. Покажем, что среди них существует счетное число попарно не изоморфных.

Лемма 3. *Существует такое число $n_0 \geq 0$, что при каждом $n \geq n_0$ стабилизатор множества M_n как целого в группе $\mathrm{GL}_4(\mathbb{Z})$ совпадает с G_3.*

Доказательство. Пусть $s \in \mathrm{GL}_4(\mathbb{Z})$ и $M_n s = M_n$ для некоторого $n \geq 0$. Нужно показать, что $s \in G_3$.

Поскольку группа G_3 действует транзитивно на множестве M_n, то, умножив s в случае необходимости на подходящий элемент из G_3, будем считать, что

$$z_n s = z_n. \tag{3.4}$$

Далее, имеем

$$z_n f_1 s = m_1, \qquad z_n f_2 s = m_2, \qquad z_n f_3 s = m_3 \tag{3.5}$$

для некоторых $m_1, m_2, m_3 \in M_n$. Непосредственно проверяется, что определитель

$$\begin{vmatrix} z_n \\ z_n f_1 \\ z_n f_2 \\ z_n f_3 \end{vmatrix} = -3(36n^2 + 24n + 1)(12n^2 + 4n + 1) \neq 0.$$

Следовательно, векторы $z_n, z_n f_1, z_n f_2, z_n f_3 \in \mathbb{Q}^4$ линейно независимы. Поэтому из (3.4) и (3.5) имеем

$$s = \begin{pmatrix} z_n \\ z_n f_1 \\ z_n f_2 \\ z_n f_3 \end{pmatrix}^{-1} \begin{pmatrix} z_n \\ m_1 \\ m_2 \\ m_3 \end{pmatrix}. \tag{3.6}$$

Непосредственным перебором всех троек $m_1, m_2, m_3 \in M_n$ проверяется, что либо $m_1 = z_n f_1, m_2 = z_n f_2, m_3 = z_n f_3$, либо $m_1 = z_n f_1 f_4 f_3^{-1}, m_2 = z_n f_2 f_4 f_3^{-1}, m_3 = z_n f_3 f_4 f_3^{-1}$, либо матрица s, определенная по формуле (3.6), содержит (в некоторой позиции, зависящей от m_1, m_2, m_3) элемент вида $\dfrac{w(n)}{3(36n^2 + 24n + 1)(12n^2 + 4n + 1)}$, где $w(n)$ — ненулевой многочлен с целыми коэффициентами от n степени не выше 3. В первом случае имеем $s = E_4 \in G_3$, во втором — $s = f_4 f_3^{-1} \in G_3$, а третий случай невозможен при достаточно больших n, поскольку матрица s является целочисленной.

Лемма доказана.

Зафиксируем число n_0, найденное из леммы 3.

Лемма 4. *Графы $\Gamma_{\mathbb{Z}^d, M_n}$ $(n \geq n_0)$ попарно не изоморфны.*

Доказательство. Пусть $\Gamma_{\mathbb{Z}^d, M_m} \cong \Gamma_{\mathbb{Z}^d, M_k}$ для некоторых $m, k \geq n_0$. Тогда по [2, теорема 3(a)] существует матрица $s \in \mathrm{GL}_4(\mathbb{Z})$ такая, что $M_m s = M_k$, и из леммы 3 следует, что $s \in N_{\mathrm{GL}_4(\mathbb{Z})}(G_3)$. Нормализатор $N_{\mathrm{GL}_4(\mathbb{Z})}(G_3)$, вычисленный с использованием пакета Carat системы GAP, оказался равным G_3. Следовательно, $s \in G_3$ и $M_m = M_m s = M_k$. Но из определения M_n легко следует, что множества M_n различны при различных $n \geq 0$. Следовательно, $m = k$, и лемма доказана.

Итак, $\{\Gamma_{\mathbb{Z}^4, M_n} : n \geq n_0\}$ — искомое счетное множество попарно не изоморфных минимальных графов Кэли группы $\mathbb{Z}^4$, соответствующих G_2-орбитам (равно как и G_3-орбитам). Теорема 1 доказана.

4. Доказательство теоремы 2

Поскольку $G_1 \in Q_{33,2}$, то по таблице из § 2 имеем $c_1(G_1) = 1$. По [3, лемма 5] существует бесконечное множество P_1 простых чисел такое, что для каждого $p \in P_1$ группа $\phi_p(G_1)$ действует неприводимо на $\mathbb{Z}_p^4$. Тогда по утверждению (2) предложения 7 каждый граф Кэли группы $\mathbb{Z}^4$, соответствующий G_1-орбите, является предельным для множества минимальных вершинно-примитивных графов HA-типа.

Как мы уже заметили в предыдущем параграфе, $c_1(G_2) = 1$. Поэтому из предложения 6 следует существование целого числа p_0 такого, что $|\phi_p(G_2)| = |G_2|$ для всех простых $p > p_0$ и $|x\phi_p(G_2)| = |\phi_p(G_2)|$ для каждого $x \in \mathbb{Z}_p^4 \setminus \{0\}$. Теперь положим $P_2 = \{p \in \mathbb{N} : p \text{ — простое}, p > \max\{p_0, 24\}, p \equiv 11 (\operatorname{mod} 12)\}$.

Покажем, что для каждого $p \in P_2$ группа $\phi_p(G_2)$ действует неприводимо на $\mathbb{Z}_p^4$. Предположим противное: пусть для некоторого $p \in P_2$ существует собственное $\phi_p(G_2)$-допустимое подпространство U. Поскольку $p > p_0$, то $\phi_p(G_2)$ действует точно на U. Следовательно, группа $\mathrm{GL}_{\dim(U)}(p)$ содержит подгруппу, изоморфную $Q_8 \times C_3$. Случай $\dim(U) = 1$ невозможен, поскольку циклическая группа $\mathrm{GL}_1(p)$ не содержит подгрупп, изоморфных $Q_8 \times C_3$. Случай $\dim(U) = 3$ сводится к предыдущему, поскольку $p \nmid 24$, и, следовательно, по теореме Машке существует $\phi_p(G_2)$-допустимое подпространство размерности 1. Наконец, последний случай $\dim(U) = 2$ невозможен, поскольку при $p \equiv 11 (\operatorname{mod} 12)$ группа $\mathrm{GL}_2(p)$ не содержит подгрупп, изоморфных $Q_8 \times C_3$.

Из того, что для каждого $p \in P_2$ группа $\phi_p(G_2)$ действует неприводимо на $\mathbb{Z}_p^4$, и утверждения (2) предложения 7 следует, что каждый граф Кэли группы $\mathbb{Z}^4$, соответствующий G_2-орбите, является предельным для множества минимальных вершинно-примитивных графов HA-типа.

Итак, утверждение (1) теоремы 2 доказано.

Поскольку $G_3 \in Q_{33,4}$, то по таблице из § 2 имеем $c_1(G_3) = 2$. Следовательно, $m(G_3) = 24 = m(G_2)$ по (1.1), откуда $\mathcal{M}_{\mathbb{Z}}(G_3) \subseteq \mathcal{M}_{\mathbb{Z}}(G_2)$. Таким образом, каждый минимальный граф Кэли группы $\mathbb{Z}^4$, соответствующий G_3-орбите, соответствует также G_2-орбите. Теперь утверждение (2) теоремы 2 следует из теоремы 1 и утверждения (1) теоремы 2.

Теорема 2 полностью доказана.

Автор выражает благодарность своему научному руководителю В.И. Трофимову за постановку задачи и постоянное внимание к работе.

Поступила 15.11.2006

СПИСОК ЛИТЕРАТУРЫ

1. **Giudici M., Li C.H., Praeger C.E., Seress A. and Trofimov V.** On limit graphs of finite vertex-primitive graphs// J. Comb. Theory. Ser. A. 2007. V. 114. P. 110–134.
2. **Костоусов К.В.** Графы Кэли группы $\mathbb{Z}^d$ и пределы вершинно-примитивных графов HA-типа // Сиб. мат. журн. (в печати).

3. **Костоусов К.В.** Графы Кэли группы $\mathbb{Z}^4$ и пределы минимальных вершинно-примитивных графов HA-типа // Алгебра и логика (в печати).
4. **Цишанг Х., Фогт Э., Колдевай Х.Д.** Поверхности и разрывные группы. М.: Наука, 1988.
5. **Brown H., Bulow H., Neubušer J., Wondratschek H., and Zassenhaus H.** Crystallographic groups of four-dimensional space. New York: John Wiley, 1978.
6. **The GAP Group.** GAP — Groups, Algorithms, and Programming. Version 4.4. Aachen — St. Andrews, 2004 (http://www.gap-system.org).
7. **Рейнгольд Э., Нивергельт Ю., Део Н.** Комбинаторные алгоритмы. Теория и практика. М.: Мир, 1980.

ТРУДЫ ИНСТИТУТА МАТЕМАТИКИ И МЕХАНИКИ УрО РАН

Том 13 № 1 2007

УДК 519.14

ОБ ОДНОРОДНЫХ РАСШИРЕНИЯХ ЧАСТИЧНЫХ ГЕОМЕТРИЙ [1]

А. А. Махнев, М. С. Нирова

Геометрией ранга 2 называется система инцидентности $(P,\mathcal{B})$, где P — множество точек, $\mathcal{B}$ — некоторый набор подмножеств из P, называемых блоками. Две точки называются коллинеарными, если они лежат в общем блоке. Пара (a,B) из $(P,\mathcal{B})$ называется флагом, если точка принадлежит блоку, и антифлагом в противном случае. Геометрия называется φ-однородной (φ — натуральное число), если для любого антифлага (a,B) число точек в блоке B, коллинеарных точке a, равно 0 или φ, и сильно φ-однородной, если это число равно φ. В данной работе исследуются φ-однородные расширения частичных геометрий $pG_\alpha(s,t)$ с $\varphi=s$ и сильно φ-однородные геометрии с $\varphi=s-1$. В частности, полученные ранее Камероном и Фишером результаты по расширениям обобщенных четырехугольников распространяются на случай частичных геометрий.

Введение

Геометрия $\mathcal{S}$ ранга 2 — это система инцидентности $(P,\mathcal{B})$, где P — множество точек, $\mathcal{B}$ — некоторый набор подмножеств из P, называемых блоками. Две точки называются *коллинеарными*, если они лежат в общем блоке. Если $\mathcal{S}$ является геометрией ранга 2, то точечный граф $\Gamma=\Gamma(\mathcal{S})$ — это граф с множеством вершин P, в котором различные вершины смежны, если они коллинеарны. Геометрия $\mathcal{S}$ будет называться *связной, регулярной* и т. д., если граф Γ обладает соответствующими свойствами.

Пара (a,B) из $(P,\mathcal{B})$ называется *флагом*, если точка a принадлежит блоку B, и *антифлагом* в противном случае. Если (a,B) является антифлагом, то через $f(a,B)$ обозначим число точек в B, коллинеарных a. Геометрия называется *φ-однородной* (φ — натуральное число), если для любого антифлага (a,B) число $f(a,B)$ равно 0 или φ, и *сильно φ-однородной*, если это число всегда равно φ.

Вычет $\mathcal{S}_a$ геометрии $\mathcal{S}$ в точке a — это геометрия $(P_a,\mathcal{B}_a)$ ранга 2, где P_a — множество всех точек, коллинеарных a, и $\mathcal{B}_a=\{B-\{a\}\mid a\in B\in\mathcal{B}\}$. Пусть $\mathcal{F}$ — семейство геометрий ранга 2, и всякий вычет $\mathcal{S}_a$ лежит в $\mathcal{F}$. Тогда говорят, что $\mathcal{S}$ является *расширением* $\mathcal{F}$. Геометрия $\mathcal{S}$ называется *треугольной*, если для любых попарно коллинеарных точек a,b,c найдется блок, содержащий все три точки a,b и c. Точечный граф $\Gamma(\mathcal{S}_a)$ — это подграф (возможно, собственный) графа, индуцированного на $\Gamma(a)$ графом Γ. Заметим, что $\Gamma(\mathcal{S}_a)=\Gamma(a)$ для любой точки a тогда и только тогда, когда геометрия $\mathcal{S}$ треугольная.

Если p,q — различные точки геометрии $\mathcal{S}$, то геометрия $\mathcal{S}_{pq}$ имеет множество точек $P_{pq}=P_p\cap P_q$ и множество блоков $\mathcal{B}_{pq}=\{B\cap P_q\mid B\in\mathcal{B}_p$ и $B\cap\mathcal{B}_q$ не пусто$\}$. Положим $|P_{pq}|=\lambda(p,q)$ (соответственно, $\mu(p,q)$), если $d(p,q)$ равно 1 (соответственно, 2) в точечном графе $\Gamma(\mathcal{S})$.

Блоки геометрии $\mathcal{S}$ называются *прямыми*, если различные блоки пересекаются не более чем в одной точке. В этом случае множество блоков называется множеством прямых и мы будем пользоваться неформальным языком, т. е. такими выражениями, как “прямая проходит через точку”, “точка лежит на прямой” и др.

Если $\mathcal{S}$ есть такая геометрия точек и прямых, что каждая прямая имеет ровно $s+1$ точку, каждая точка лежит ровно на $t+1$ прямой ($s>0$, $t>0$) и $\mathcal{S}$ является сильно α-однородной ($\alpha>0$), то тогда $\mathcal{S}$ называется *α-частичной геометрией порядка* (s,t) (для краткости $pG_\alpha(s,t)$

[1]Работа выполнена при поддержке РФФИ (проект 05-01-00046) и РФФИ-ГФЕН Китая (проект 05-01-39000).

или даже pG_α). Связное расширение семейства частичных геометрий pG_α обозначается как EpG_α (или даже EpG).

Можно показать, что в EpG_α-геометрии $\mathcal{S}$ (a) для любого антифлага (a, B), если $f(a, B) \neq 0$, то $f(a, B) \geq \alpha + 1$, и (b) $\mathcal{S}$ является треугольной геометрией тогда и только тогда, когда она $(\alpha + 1)$-однородна.

Если $\mathcal{S}$ — частичная геометрия $pG_\alpha(s, t)$, то двойственная геометрия $(\mathcal{B}, P)$, в которой каждая точка отождествляется с пучком проходящих через нее прямых, является частичной геометрией $pG_\alpha(t, s)$. Обобщенный четырехугольник $GQ(s, t)$ — это частичная геометрия $pG_1(s, t)$. Геометрия $pG_t(s, t)$ является сетью, а $pG_{s+1}(s, t)$ является 2-схемой с $\lambda = 1$. Коклика из $1 + st/\alpha$ точек в точечном графе геометрии $pG_\alpha(s, t)$ называется *овоидом.*

В данной статье мы исследуем φ-однородные геометрии $EpG_\alpha(s, t)$ с $\varphi = s$ и сильно φ-однородные геометрии с $\varphi = s - 1$.

Пусть геометрия $\mathcal{S}$ является φ-однородной $EpG_\alpha(s, t)$. Если $\varphi = s + 2$, то $\mathcal{S}$ называется одноточечным расширением (и граф $\Gamma(\mathcal{S})$ является полным). Например, 3-схема Матье с параметрами $(22, 6, 1)$ — это одноточечное расширение проективной плоскости $PG(2, 4)$.

Если $\varphi = s + 1$, то геометрия $\mathcal{S}$ будет сильно $(s + 1)$-однородной, и Γ является полным многодольным графом $K_{(s+2)\times(1+st/\alpha)}$. В этом случае для любой точки a множество точек вычета $\mathcal{S}_a$ имеет разбиение на $s+1$ овоидов. Среди известных обобщенных четырехугольников только $GQ(s, 1)$, $GQ(1, t)$, $GQ(2^\alpha, 2^\alpha)$, $GQ(q^2, q)$, $GQ(q-1, q+1)$, $GQ(q+1, q-1)$, где q — степень простого числа, допускают разбиение точечного множества на овоиды.

П р и м е р 1. Для любого $t \geq 1$ имеется единственная геометрия $EGQ(1, t)$. Ее точечный граф является полным трехдольным графом $K_{3\times(t+1)}$, а множество блоков совпадает с множеством 3-клик этого графа.

П р и м е р 2. Сильно $(s + 1)$-однородный расширенный четырехугольник $EGQ(s, 1)$ существует при всех $s = q-1$, где q есть степень 2, а при $s = 1$ и $s = 3$ является единственным [1].

Пусть $\pi = PG(2, q)$, a — точка в π, C — гиперовал, содержащий a, а T обозначает группу (порядка q^2) всех элаций с центром в точке a. Точками EGQ являются все точки π, отличные от a; блоками являются прямые, не содержащие a, и трансляции прямой $C-\{P\}$ под действием группы T.

Примеры $(s + 1)$-однородных $EGQ(q - 1, q + 1)$ для $q = 2^n$ построены А. Пасини и Д. Пасечником.

Теорема 1. *Пусть $\mathcal{S}$ является s-однородной геометрией $EpG_\alpha(s, t)$, а $\bar{\Gamma}$ — дополнение к $\Gamma(\mathcal{S})$. Тогда либо $s = 2$ (и геометрия $\mathcal{S}$ известна), либо $\mathcal{S}$ есть $EpG_2(s, 1)$, $\bar{\Gamma}$ является сильно регулярным графом с $\lambda = 0$, $\mu = 2$, и $\mathcal{S}$ есть геометрия вершин и клик графа Γ, соответствующих $\bar{\Gamma}(a)$ для $a \in \bar{\Gamma}$; либо $\mathcal{S}$ сильно s-однородна и одно из следующих утверждений верно*:

(1) $t = \alpha$, *и $\bar{\Gamma}$ есть граф, являющийся квадратной решеткой на $(s + 2)^2$ вершинах*;

(2) $t = 2\alpha$, $s \leq (2\alpha - 1)(\alpha + 1)^2$, $s + \alpha + 1$ *делит* $2s(s + 1)(2\alpha + 1)$, *и $\bar{\Gamma}$ есть треугольный граф на $(s + 2)(2s + 3)$ вершинах.*

П р и м е р 3. Сильно s-однородная геометрия $EGQ(s, 1)$ существует для всех $s = q - 2$, где q есть степень двойки [1].

Пусть $\pi = PG(2, q)$, a и b являются точками π, L есть прямая ab, C — гиперовал, содержащий a и b, а T — это группа всех центральных коллинеаций с центром a и осью, содержащей b. Тогда $|T| = q(q - 1)$, T фиксирует все прямые, проходящие через a, и является точно 2-транзитивной группой на множестве прямых, проходящих через b и отличных от L.

Множество точек геометрии $EGQ(s, 1)$ состоит из точек π, которые не лежат на L, а множество блоков является объединением множества прямых π, не содержащих a или b, и образов $C - \{P, Q\}$ под действием группы элаций T.

П р и м е р 4. Сильно 3-однородная геометрия $EpG_2(3,2)$ существует.

Пусть точечное множество $\mathcal{S}$ есть множество позиций ij квадратной матрицы порядка 5, а множество блоков $\mathcal{B}$ задано наборами $\{1i_1, 2i_2, \ldots, 5i_5\}$, такими, что $(i_1 i_2 ... i_5)$ — перестановка.

Ясно, что $|\mathcal{B}| = 5!/2 = (t+1)(s+1)(s+2)$ для $t=2$, $s=3$ и $f(a,B)=3$ для любого антифлага (a,B).

Далее, для точки $a = xi_x$ имеем $|P_a| = 16$, $|\mathcal{B}_a| = 16$, каждая точка из P_a принадлежит трем блокам из $\mathcal{B}_a$ и каждый блок из $\mathcal{B}_a$ содержит 4 точки из P_a. Таким образом, $(P,\mathcal{B})$ является сильно 3-однородной геометрией $EpG_2(3,2)$.

Теорема 2. *Пусть $\mathcal{S}$ является сильно $(s-1)$-однородной геометрией $EpG_\alpha(s,t)$. Тогда либо $\mathcal{S}$ является геометрией $EpG_{2x}(3x, 3x-1)$ для некоторого нечетного x, либо $\mathcal{S}$ равняется $EGQ(3,1)$, $EGQ(3,9)$, $EpG_2(6,15)$, $EpG_2(7,6)$ или $EpG_3(7,9)$.*

Дж. Тас построил частичную геометрию $pG_{2x}(3x, 3x-1)$ с $x = 3^{2n-2}$ с помощью спреда гиперболической квадрики в проективном пространстве $PG(4n-1,3)$ [2]. К настоящему времени известно существование такого спреда только для случая $n=2$.

Теоремы 1 и 2 обобщают соответствующие результаты П. Камерона и Дж. Фишера [1] по расширениям обобщенных четырехугольников на случай частичных геометрий.

1. Предварительные результаты

В этом разделе доказаны некоторые необходимые вспомогательные результаты.

Лемма 1.1. *Пусть $\mathcal{S}$ является частичной геометрией $pG_\alpha(s,t)$. Тогда $\alpha \le \min\{s+1, t+1\}$ и выполняются следующие утверждения:*

(1) *точечный граф $\Gamma(\mathcal{S})$ является сильно регулярным с $v = (s+1)(1+st/\alpha)$, $k = s(t+1)$, $\lambda = s-1+(\alpha-1)t$, $\mu = \alpha(t+1)$, и $\mathcal{B}$ содержит $(t+1)(1+st/\alpha)$ прямых;*

(2) *$\alpha(s+t+1-\alpha)$ делит $st(s+1)(t+1)$ (условие целочисленности);*

(3) *$(s+1-2\alpha)t \le (s-1)(s+1-\alpha)^2$ (условие Крейна);*

(4) *если $\mathcal{S}$ содержит подгеометрию $pG_\alpha(s',t')$, то $s=s'$ или $s't'+\alpha-1 \le s$.*

Д о к а з а т е л ь с т в о. См. теорему 1.1 статьи [4].

Лемма 1.2. *Пусть $\mathcal{S}$ является φ-однородной геометрией $EpG_\alpha(s,t)$. Тогда точечный граф $\Gamma(\mathcal{S})$ является реберно регулярным с $\lambda = s + st(\varphi-1)/\alpha$. Кроме того, $\alpha\varphi$ делит $st(s+1)(s+2)$, и в случае $\varphi = \alpha+2$ число φ четно.*

Д о к а з а т е л ь с т в о. Для доказательства первого и второго утверждений см. [4, леммы 2.1 и 2.2].

Пусть далее $\varphi = \alpha+2$ и (a,B) является антифлагом с $f(a,B) = \varphi$. По структуре вычета $\mathcal{S}_b$ для $b \in B \cap P_a$ точка a лежит на α прямых в $\mathcal{B}_b$, пересекающих $B\cap P_a$, так что $B \cap P_a$ содержит единственную точку b^* такую, что тройка a, b, b^* не лежит ни в одном из блоков множества $\mathcal{B}$. Ясно, что $(b^*)^* = b$, поэтому число $|B \cap P_a| = \varphi$ четно.

Лемма 1.3. *Пусть $\mathcal{S}$ — сильно φ-однородная геометрия $EpG_\alpha(s,t)$, где $\varphi < s+2$. Тогда точечный граф $\Gamma(\mathcal{S})$ является псевдогеометрическим для $pG_\varphi(s+1, st/\alpha)$ и имеет собственные значения k, $s+1-\varphi$, $-(1+st/\alpha)$.*

Д о к а з а т е л ь с т в о. См. [3, теорема 1.2].

Лемма 1.4. *3-однородное расширение частичной геометрии $pG_2(4,1)$ не существует.*

Д о к а з а т е л ь с т в о. Пусть Γ является точечным графом 3-однородной геометрии $EpG_2(4,1)$. Тогда Γ сильно регулярен с параметрами $(26,15,8,9)$. Так как эта геометрия треугольная, то подграф $\Gamma(a)$ является треугольным графом $T(6)$ для любого $a \in \Gamma$. Значит, окрестности вершин в каждом μ-подграфе графа Γ являются четырехугольниками, что противоречит равенству $\mu = 9$. Лемма доказана.

2. Случай $\varphi = s$

Предположим, что $\mathcal{S}$ есть s-однородное расширение частичной геометрии порядка (s,t), т. е. $EpG_\alpha(s,t)$. Пусть $\bar{\Gamma}$ является дополнением к графу $\Gamma(\mathcal{S})$.

Лемма 2.1. *Допустим, что геометрия $\mathcal{S}$ сильно s-однородна. Тогда либо $t = \alpha$ и $\bar{\Gamma}$ — квадратная $(s+2)\times(s+2)$-решетка, либо $t = 2\alpha$ и $\bar{\Gamma}$ является треугольным графом $T(2s+4)$, где $s \le (2\alpha-1)(\alpha+1)^2$.*

Доказательство. По лемме 1.3 граф Γ имеет собственное значение $s+1-\varphi = 1$, и по теореме Зейделя [6] граф $\bar{\Gamma}$ является одним из следующих графов: решетка или треугольный граф, полный многодольный граф $K_{m\times 2}$, граф Петерсена, Шрикханде, Чанга, Клебша или Шлефли. Заметим, что $\bar{\mu} = v-2k+\lambda = 2t/\alpha$, $\bar{k} = (s+1)st(s+2-\varphi)/(\alpha\varphi) = 2(s+1)t/\alpha$ и $\bar{\mu} < \bar{k}$, поэтому графы $K_{m\times 2}$ исключаются.

Так как граф Петерсена имеет параметры $(10,3,0,1)$, то $2t = \alpha$, $t = 1, \alpha = 2$ и $s = 2$, противоречие с тем, что $\varphi \ge \alpha+1$. В случае графа Клебша граф Γ имеет параметры $(16,5,0,2)$, противоречие с тем, что $\lambda > 0$.

В случае графа Шлефли граф Γ имеет параметры $(27,10,1,5)$ и $\lambda = 1 = s + st(s-1)/\alpha$, поэтому $s = 1$, снова противоречие с тем, что $\varphi \ge \alpha+1$.

Пусть $\bar{\Gamma}$ имеет параметры решетки $(n^2, 2(n-1), n-2, 2)$. Тогда $\alpha = t$. Заметим, что граф Шрикханде имеет параметры решетки при $n = 4$. Но существует единственное расширение обобщенного четырехугольника $EGQ(2,1)$ с $v = 16$, и его точечный граф является дополнением к 4×4-решетке [1, пример 3.8].

Пусть, наконец, $\bar{\Gamma}$ имеет параметры $(n(n-1)/2, 2(n-2), n-2, 4)$ треугольного графа. Тогда $t = 2\alpha$, $n = 2s+4$. По условию Крейна для $pG_\alpha(2\alpha, s)$ имеем $s \le (2\alpha-1)(\alpha+1)^2$. Случай $\alpha = 1$ был рассмотрен в [3, теорема 7.1], поэтому будем считать, что $\alpha \ge 2$. Но тогда $s \ge 3$, $n \ge 10$ и графы Чанга $(n = 8)$ не возникают.

Лемма 2.2. *Пусть $\mathcal{S}$ является s-однородной геометрией $EpG_\alpha(s, 2\alpha)$ с $\alpha > 1$ и α делит s. Тогда $s = 2\alpha(\alpha+1)$.*

Доказательство. Положим $s = x\alpha$. В случае $x = 2\alpha+2$ имеем $s = 2\alpha(\alpha+1)$, и заключение леммы выполняется.

По лемме 1.1 число $2x\alpha(2\alpha+1)(x\alpha+1)$ делится на $x\alpha+\alpha+1$. Далее, числа $x\alpha+\alpha+1$ и $(x\alpha+1)\alpha$ взаимно просты, поэтому $x\alpha+\alpha+1$ делит $2(x,\alpha+1)(x-1, 2\alpha+1)$. Наконец, $(x\alpha+\alpha+1, (x-1)(\alpha+1))$ делит $x-2\alpha-2$ и $x\alpha+\alpha+1$ делит $2(x-2\alpha-2)$.

Пусть $x > 2\alpha+2$. Тогда $x\alpha+\alpha+1 \le 2(x-2\alpha-2)$ и $5\alpha+5 \le x(2-\alpha)$, так что $\alpha = 1$, противоречие. Если $x < 2\alpha+2$, то $x\alpha+\alpha+1 \le 2(2\alpha+2-x)$, поэтому $x(\alpha+2) \le 3\alpha+3$ и $x \le 2$.

Поскольку $s > \alpha$, то $x = 2$ и по условию целочисленности для $EpG_\alpha(2\alpha, 2\alpha)$ число $\alpha(3\alpha+1)$ делит $4\alpha^2(2\alpha+1)^2$. Значит, $\alpha = 1$, что противоречит условию леммы.

Лемма 2.3. *Пусть $\mathcal{S}$ является s-однородной геометрией. Тогда либо $s = 2$ и $\mathcal{S}$ — одна из геометрий примера 9.6 [1], либо $\bar{\Gamma}$ является сильно регулярным графом с $\lambda = 0$, $\mu = 2$, и $\mathcal{S}$ — геометрия вершин и клик графа Γ, соответствующих $\bar{\Gamma}(a)$ для $a \in \bar{\Gamma}$, либо $\mathcal{S}$ сильно однородна.*

Доказательство. Допустим, что $\mathcal{S}$ — контрпример к этой лемме с минимально возможным t. По теореме 7.3 [3] имеем $\alpha > 1$, так что $s \ge 3$. Диаметр графа Γ ограничен величиной $\max\{2, s+5-2\varphi\}$ [5], значит, $d(\Gamma) = 2$.

По выбору $\mathcal{S}$ в ней найдутся точки a, b на расстоянии 2 такие, что $\mathcal{B}_b$ содержит блоки двух типов: блоки L с $f(a,L) = s$ (s-блоки) и блоки D с $f(a,D) = 0$ (0-блоки).

Пусть $\mathcal{D}$ есть геометрия с точечным множеством $P_b - P_a$ и множеством блоков $\{D \in \mathcal{B}_b \mid f(a,D) = 0\}$. Тогда каждый блок из $\mathcal{B}_b$, содержащий две точки u и w множества $P_b - P_a$, является 0-блоком. Таким образом, геометрия $\mathcal{D}$ сильно α-однородна. Следовательно, либо $\mathcal{D}$ есть геометрия точек единственного 0-блока (заметим, что эта возможность не учтена в доказательстве леммы 7.3 в работе [3]), либо $\mathcal{D}$ есть геометрия $pG_\alpha(s,u)$ для некоторого u.

В первом случае число точек в P_{ab} равно $(s+1)st/\alpha$. Далее, каждый блок множества $\mathcal{B}_{ba}$, содержащий точку из $\mathcal{P}_{ab}$, содержит единственную точку из $\mathcal{D}$, поскольку $\varphi = s$. Так что число ребер между точками множеств $\mathcal{D}$ и P_{ab} равно $(t+1)(s+1)st/\alpha$. Однако каждая точка геометрии $\mathcal{D}$ лежит в t блоках из $\mathcal{B}_{ba}$, содержащих по s точек множества P_{ab}, поэтому то же число ребер равно $st(s+1)$. Значит, $\alpha = t+1$ (и этот случай не возникает в расширенном четырехугольнике EGQ).

В случае $pG_\alpha(s,u)$ имеется $(s+1)s(t+1)(t-u)/\alpha = (t-u)(s+1)s(1+su/\alpha)$ ребер между точками геометрии $\mathcal{D}$ и P_{ab}, поэтому $t+1 = \alpha + su$.

Допустим, что выполняется первый случай. Тогда $\alpha = t+1$. Пусть для n_1 точек $r \in P - P_a$ каждый блок множества $\mathcal{B}_r$ является s-блоком, и для n_2 точек $q \in P - P_a$ все точки множества $P_q - P_a$ лежат в единственном 0-блоке. Тогда число ребер между точками множеств P_a и $P - P_a$ равно

$$(1+st/\alpha)(s+1)2st/\alpha = n_1 s(1+st/\alpha) + n_2(s+1)st/\alpha.$$

Если $n_1 \neq 0$, то по целочисленности числа точек в множествах $\mathcal{P}_{PR}$ и $\mathcal{P}_{PQ}$ число $\alpha = t+1$ делит s^2 и $s(s+1)$, поэтому $s = s'\alpha = s'(t+1)$. Далее, $(1+s't)(s+1)2s't = n_1 s(1+s't) + n_2(s+1)s't$ и $s+1$ делит $n_1(1+s't)$. Так как $s't+1$ и $s't+s'+1$ взаимно просты, то $s+1$ делит n_1. Если $n_1 \geq 2(s+1)$, то $n_2 < 0$, если же $n_1 = s+1$, то $(1+s't)(2s't - s) = (1+s't)(s't - s') = n_2 s't$ и $n_2 t = (1+s't)(t-1)$. Поэтому $t = 1$ и $n_2 = 0$, противоречие.

Итак, $n_1 = 0$, граф $\Gamma_2(a)$ разбивается на 0-блоки и $|\Gamma_2(a)| = (st+t+1)/t$. Значит, $t = 1$, $k = (s+1)(s+2)/2$, $\lambda = \mu = s(s+1)/2$, поэтому граф $\bar{\Gamma}$ сильно регулярен с $\lambda = 0$, $\mu = 2$, и $\mathcal{S}$ является геометрией вершин и клик графа Γ, соответствующих $\bar{\Gamma}(a)$ для $a \in \bar{\Gamma}$. Но это противоречит выбору $\mathcal{S}$.

Таким образом, мы доказали, что для любой точки $b \in \Gamma_2(a)$

(1) каждый блок из $\mathcal{B}_b$ является s-блоком или

(2) $\mathcal{S}_b$ содержит подгеометрию $pG_\alpha(s,u)$ с точечным множеством $P_b - P_a$ и множеством блоков $\{D \in \mathcal{B}_b \mid f(a,D) = 0\}$, причем $u = (t+1-\alpha)/s$.

Пусть Φ_i — множество точек графа $\Gamma_2(a)$, удовлетворяющее утверждению (i), $n_i = |\Phi_i|$, $i \in \{1,2\}$. Заметим, что если $q \in \Phi_2$ и точка r лежит в 0-блоке D из $\mathcal{B}_q$, то $r \in \Phi_2$. Следовательно, Φ_2 разбивается на s-однородные подгеометрии $EpG_\alpha(s,u)$. По индукции мы заключаем, что либо $\alpha = 2$, $u = 1$ и $t = s+1$, либо эти подгеометрии сильно однородны, и по лемме 2.1 имеем $u \in \{\alpha, 2\alpha\}$.

Как и выше, у нас имеется равенство для количества ребер между точками множеств P_a и $P - P_a$:

$$(1+st/\alpha)(s+1)2st/\alpha = n_1 s(1+st/\alpha) + n_2(s+1)s(t-u)/\alpha. \qquad (*)$$

В первом случае ($\alpha = 2$, $u = 1$) имеем $(s+1)^2(s(s+1)+2) = n_1(s(s+1)+2) + n_2 s(s+1)$, поэтому $1 + s(s+1)/2$ делит n_2. Если $n_2 > 2 + s(s+1)$, то $n_1 < 0$, что абсурдно. Значит, $n_2 \in \{2+s(s+1), 1+s(s+1)/2\}$. Так как Φ_2 разбивается на подгеометрии $EpG_2(s,1)$, то $(s+1)(s+2)/2$ делит $s(s+1)+2$, поэтому $s+1$ делит 4 и $s = 3$. Противоречие с тем, что $4 \cdot 5/2$ не делит $3 \cdot 4 + 2$.

Предположим теперь, что $u = \alpha$. Тогда $t+1 = \alpha(s+1)$ и по утверждению (2) леммы 1.1 число $\alpha(s - \alpha + \alpha(s+1))$ делит $s(s+1)t(t+1)$, поэтому $\alpha + 1$ делит $(s+1)^2(s+2)$. Далее, α делит $(t+1, st)$, поэтому α делит s. Положим $s = x\alpha$. Тогда $\alpha+1$ делит $(x-1)^2(x-2)$.

Если $n_2 \geq 2(s+2)^2$, то из равенства $(*)$ следует, что $n_1 < 0$, что противоречиво. Значит, $n_2 = 2(s+2)^2$ и равенство $(*)$ принимает вид: $(1+xt)(s+1)2t = n_1(1+xt)\alpha + (s+2)^2(s+1)(t-\alpha)$. Отсюда α делит $2(x+1)$ и $1 + xt = x^2\alpha^2 + x\alpha - x + 1$ делит $(s+1)(s\alpha - 1)(s+2)^2$. Далее,

$(1+xt, s+1) = (x-1, \alpha+1)$, $(1+xt, s\alpha-1) = (xt+s\alpha, s\alpha-1) = (x\alpha+1, s\alpha-1) = (s+1, \alpha+1) = (x-1, \alpha+1)$ и $(1+xt, (s+2)^2) = (1+xt, 3x\alpha+x+3)$. Так как $(1+xt, (x-1)^2) = (1+xt, \alpha+1)$, то $1+xt$ делит $(\alpha+1)(3x\alpha+x+3)$, откуда $x \le 4$.

Если $x = 4$, то $16\alpha^2+4\alpha-3$ делит $(3, \alpha+1)(12\alpha+7)$, поэтому $\alpha = 2$, и 69 не делит $3 \cdot 43$. Если $x = 3$, то $\alpha+1$ делит 4, и $\alpha = 3$. Но тогда $1+xt = 88$ не делит $(x-1)(3x\alpha+x+3) = 66$. Значит, $x = 2$, противоречие с тем, что $4\alpha^2+2\alpha-1$ не делит $6\alpha+5$.

Итак, $u = 2\alpha$, $t+1 = \alpha(2s+1)$, и по лемме 1.1 число $\alpha(s+\alpha(2s+1)-\alpha)$ делит $s(s+1)t(t+1)$, поэтому $2\alpha+1$ делит $(s+1)(2s+1)(2s+3)$. Как и выше, α делит s, и по лемме 2.2 имеем $s = 2\alpha(\alpha+1)$ и $t = \alpha(2\alpha+1)^2$.

Если $n_2 \ge 2(s+2)(2s+3)$, то ввиду равенства $(*)$ имеем $n_1 < 0$, что абсурдно. Значит, $n_2 = (s+2)(2s+3)$ и согласно $(*)$ число $\delta = 1+2(\alpha+1)t$ делит $(s+1)(s+2)(2s+3)(t/\alpha-2)$. Далее, $(\delta, s+1) = (1+2\alpha(\alpha+1)(2\alpha+1)^2, 2\alpha^2+2\alpha+1) = 1$, $(\delta, s+2) = (1+2\alpha(\alpha+1)(2\alpha+1)^2, 2\alpha^2+2\alpha+2)$ делит 7, $(\delta, 2s+3) = (1+2\alpha(\alpha+1)(2\alpha+1)^2, 4\alpha^2+4\alpha+3)$ делит 4 и $(\delta, t/\alpha-2) = (1+2\alpha(\alpha+1)(2\alpha+1)^2, 4\alpha^2+4\alpha-1)$ делит 2. Таким образом, δ делит 14, противоречие. Лемма 2.3 и теорема 1 доказаны.

3. Сильно $(s-1)$-однородные геометрии

Предположим, что $\mathcal{S}$ — сильно $(s-1)$-однородная геометрия $EpG_\alpha(s,t)$. По лемме 1.2 число $\alpha(s-1)$ делит $st(s+1)(s+2)$, поэтому $s-1$ делит $6t$. По лемме 1.3 точечный граф $\Gamma(\mathcal{S})$ является псевдогеометрическим для частичной геометрии $pG_{s-1}(s+1, st/\alpha)$. В частности, он сильно регулярен с параметрами $v = 1+(s+1)(1+st(s+2))/((s-1)\alpha)$, $k = (s+1)(1+st/\alpha)$, $\lambda = s+st(s-2)/\alpha$, $\mu = (s-1)(1+st/\alpha)$, и α делит st. Далее, собственные значения графа Γ равны $k = (s+1)(1+st/\alpha)$, 2 и $-(1+st/\alpha)$. Согласно теореме 4.8 [1], можно считать, что $\alpha \ge 2$, поэтому $s \ge 4$.

Лемма 3.1. *Верны следующие утверждения*:
(1) $\alpha(s+t-1-\alpha)$ *делит* $st(s+1)(t+1)$;
(2) $(s-1)(3+st/\alpha)$ *делит* $s(s+1)(s+2)t(1+st/\alpha)/\alpha$;
(3) *если* $3\alpha = t$ *или* $3\alpha = 2t$, *то* $\mathcal{S}$ — *одна из геометрий* $EpG_2(7,6)$ *или* $EpG_3(7,9)$.

Доказательство. Утверждения (1–2) — не что иное, как условия целочисленности для pG и Γ.

Пусть $t = 3\alpha$. Тогда $\alpha(s-1)$ делит $3s\alpha(s+1)(s+2)$, поэтому $s-1$ делит 18 и $s \in \{4,7,10,19\}$. Кроме того, $\alpha(s+2\alpha+1)$ делит $s(s+1)(3\alpha+1)3\alpha$. В случае $s = 4$ число $2\alpha+5$ делит $60(3\alpha+1)$, поэтому $\alpha \in \{4,5\}$. Противоречие с тем, что $s \ge \alpha+2$.

Если $s = 7$, то $\alpha+4$ делит $3 \cdot 7 \cdot 4(3\alpha+1)$, поэтому $\alpha \in \{2,3,7,8\}$. В этом случае заключение леммы выполняется.

Если $s \in \{10,19\}$, то 27 делит $(s-1)(3+st/\alpha)$, но не делит $s(s+1)(s+2)t(1+st/\alpha)/\alpha$.

Пусть теперь $\alpha = 2\beta$, $t = 3\beta$. Тогда $s-1$ делит 18 и $2(s+\beta+1)$ делит $3s(s+1)(3\beta+1)$, поэтому $s = 4,7,10,19$. Так как 27 делит $s(s+1)(s+2)t(1+st/\alpha)/\alpha$, то $s \in \{4,7\}$. Если $s = 4$, то $\beta+5$ делит $30(3\beta+1)$, поэтому $\beta \in \{1,2\}$. Но геометрия $pG_2(4,3)$ не существует, а $EpG_4(7,6)$ не удовлетворяет условию целочисленности.

Если $s = 7$, то $\beta+8$ делит $84(3\beta+1)$, поэтому $\beta = 4$. Противоречие с тем, что $s \ge \alpha+2$.

Лемма 3.2. *Либо* $\mathcal{S}$ *есть* $EpG_{2y}(3y, 3y-1)$ *с нечетным* y, *либо* $\alpha < t$, $s(s-1)t \le 3(6st+s\alpha-\alpha)$, $s \le 19$, $\bar{\mu} \ne 6$ *и* $\bar{\mu} \ne 9$ *в графе* $\bar{\Gamma}$.

Доказательство. Напомним, что $\bar{\mu} = v-2k+\lambda = 6st/(\alpha(s-1))$. Если $\bar{\mu} = 6$, то $st = (s-1)\alpha$ и s делит α, противоречие.

Пусть $\bar{\mu} = 9$. Тогда $2st = 3(s-1)\alpha$. Следовательно, либо $s = 3\alpha$ и $2t = 3\alpha+1$, либо $s = 3\alpha/2$ и $3\alpha-2t = 2$. В первом случае по утверждению (2) леммы 3.1 число $2(3\alpha-1)$ делит

$(3\alpha+1)(9\alpha+2)$, поэтому $\alpha=1$, противоречие. Во втором случае имеем расширение частичной геометрии $pG_{2y}(3y,3y-1)$, и по утверждению (1) леммы 3.1 число $8y^2$ делит $9y^2(3y+1)(3y-1)$, поэтому y нечетно. В этом случае заключение леммы выполняется.

Пусть $\bar{\mu}\notin\{6,9\}$. Используя оценку для числа лап в графе $\bar{\Gamma}$ [7], имеем $2st/\alpha+2\le 6(6st/((s-1)\alpha)+1)$, поэтому $s(s-1)t\le 18st+2\alpha(s-1)$. Значит, $f(s)=s^2-(19+2\alpha/t)s+2\alpha/t$ не больше 0, поэтому $s<19+2\alpha/t$.

Если $t=\alpha-1$, то α делит s. Следовательно, $s=x\alpha$, а также $s-1$ делит $6(\alpha-1)$ и $x\le 5$. По утверждению (2) леммы 3.1 число $3+x(\alpha-1)$ делит $6(s+1)(s+2)$, значит, $3+x(\alpha-1)$ делит $6(3x-2\alpha-7)$. Для $x=5$ параметр α не больше 4, и $5\alpha-1$ не делит $6(\alpha-1)$, противоречие. Для $x=4$ число $4\alpha-1$ делит 9, а для $x=3$ число $3\alpha-1$ делит 4. В любом случае приходим к противоречию. Наконец, для $x=2$ число $2\alpha-1$ делит 3, и $\mathcal{S}$ есть $EpG_2(4,1)$. Противоречие с леммой 1.4.

Если $t=\alpha$, то $(s-1)(s+3)$ делит $s(s+1)^2(s+2)$, $s-1$ и $s+3$ делят 12, поэтому $s=3$. Но в этом случае $\bar{\mu}=9$, противоречие.

Пусть теперь $t>\alpha$. Тогда $s\le 20$ и $t(s^2-19s)\le 2\alpha(s-1)$. Если $s=20$, то $20t\le 57\alpha$ и $t\le 34$. Далее, $s-1=19$ делит t, поэтому $t=19$, $\alpha(40-\alpha)$ делит $19\cdot 20^2\cdot 21$ и $\alpha\in\{10,12\}$. Но α делит st, поэтому $\alpha=10$, противоречие с утверждением (2) леммы 3.1. Лемма доказана.

До конца статьи будем предполагать, что $\alpha<t$, $s\le 19$ и $\mu\ne 9$.

Лемма 3.3. *Если α делит t, то $t=3\alpha$.*

Доказательство. Пусть $t=y\alpha$. Тогда $s-1$ делит $6y$, и по утверждению (2) леммы 3.1 число $3+sy$ делит $6(s+1)(s+2)$, поэтому $3+sy$ делит $6(s+1,3y-3)(s+2,3y-2)$.

В случае $s=4$ число $3+4y$ делит $6\cdot 5\cdot 3$ и $y\le 7$, поэтому $3+4y=15$ и $t=3\alpha$. В случае $s=6$ число $s-1=5$ делит y, $3+5y$ делит $6\cdot 7\cdot 8$. Поэтому $y=6$, и 11 не делит $7\cdot 8$. В случае $s=8$ число y делится на 7 и $3+7y$ делит $6\cdot 9\cdot 10$. Поэтому $y=7$ и 24 не делит $6(s+1)(s+2)$. В случае $s=10$ имеем $y=3z$ и $1+10z$ делит $11\cdot 12$. Значит, $z=1$ и $t=3\alpha$. В случае $s=12$ имеем $y=11$, и 45 не делит $13\cdot 14$, противоречие.

Если s четно, то либо 3 делит $s-1$, либо $s-1$ делит y и $s\le 12$. Следовательно, $s=16$, $3+16y$ делит $12(s+1)$, поэтому $y=5$ или 10, и $3+sy$ не делит $6(s+1)(s+2)$.

Значит, s нечетно. Если $s=19$, то $y=3z$, и $1+19z$ делит $3\cdot 5\cdot 7$, противоречие.

В случае $s=17$ число 8 делит y и $3+17y$ делит $6\cdot 18\cdot 19$, противоречие.

В случае $s=15$ число 7 делит y и $1+5y$ делит $2\cdot 16\cdot 17$, противоречие.

В случае $s=13$ число y четно и $3+13y$ делит $3\cdot 7\cdot 15$, противоречие.

В случае $s=11$ число 5 делит y и $3+11y$ делит $6\cdot 12\cdot 13$, противоречие.

В случае $s=9$ число 4 делит y и $1+3y$ делит $5\cdot 11$, противоречие.

В случае $s=7$ число $3+7y$ делит $6\cdot 8\cdot 9$, поэтому $y=3$ и $t=3\alpha$.

В случае $s=5$ число y четно и $3+5y$ делит $3\cdot 3\cdot 7$, поэтому $y=12$ и в псевдогеометрическом графе для $pG_4(6,60)$ условия целочисленности выполнены. Однако в этом случае имеем $\alpha\in\{2,3\}$ и в геометриях $pG_2(5,24)$, $pG_3(5,36)$ условия целочисленности нарушаются.

Лемма 3.4. *Если s нечетно, то геометрия $\mathcal{S}$ есть либо $EpG_2(7,6)$, либо $EpG_3(7,9)$.*

Доказательство. Если s — простое число, то α делит t, и ввиду лемм 3.1 и 3.3 заключение леммы выполняется.

Пусть $s=15$. Тогда $t=7y$, и $3+7ys/\alpha$ делит $6\cdot 16\cdot 17$. Если 3 делит ys/α, то $1+7ys/(3\alpha)$ делит $2^5\cdot 17$, противоречие. Значит, 3 не делит ys/α, и $3+7ys/\alpha$ делит $2^5\cdot 17$. Поэтому $3+7ys/\alpha=17$ или $8\cdot 17$. Значит, $ys=2\alpha$ или 19α. В любом случае s делит α, противоречие.

Пусть $s=9$. Тогда 4 делит t, и по лемме 3.3 число 3 делит α. Следовательно, $\alpha=3$ или 6, кроме того, $1+3t/\alpha$ делит $5\cdot 11$. Поэтому $3t\in\{4\alpha,10\alpha,54\alpha\}$. В первом случае $(3t=4\alpha)$ либо $\alpha=6$ и $\bar{\mu}=9$, либо $\alpha=3$, и 11 не делит $st(s+1)(t+1)$. Во втором случае получим противоречие с утверждением (2) леммы 3.1. В третьем случае $\alpha = 6$, $t = 108$, противоречие с утверждением (1) леммы 3.1. Лемма доказана.

В леммах 3.5–3.8 будем предполагать, что s четно.

Лемма 3.5. *Если $s+1$ взаимно просто с $3\alpha + st$, то $\mathcal{S}$ есть $EpG_2(6,15)$.*

Доказательство. Пусть $s+1$ взаимно просто с $3\alpha+st$. По лемме 3.1 число $3\alpha+st$ делит $6\alpha(s+2)$. Тогда $x = 6\alpha(s+2)/(3\alpha+st) \le 5$, $t = 6\alpha/x + (12\alpha - 3\alpha x)/(sx)$ и 3 делит stx. В случае $x = 3$ имеем $t = 2\alpha + \alpha/s$, противоречие. Поэтому $x \ne 3$ и 3 делит st.

Пусть $s = 3w$. Тогда $\alpha \le 3w-2$, $2\alpha(3w+2) = (\alpha+wt)x$ и $wtx = \alpha(6w+4-x)$. Так как $\bar\mu = 6st/(\alpha(s-1))$, то $3w-1$ делит $2t$. В случае $3w-1 = 2t$ получим $\bar\mu = 3s/\alpha$, поэтому α взаимно просто с t и $wx(3w-1) = 2\alpha(6w+4-x)$. Отсюда $x = 6$, $3w = 2\alpha$ и число t не целое. Значит, $t \ge 3w-1$.

Если $x = 1$, то $t = 6\alpha+3\alpha/w$ и $3w-1$ делит 10α. В случае $w = 6$ имеем $\alpha = 17$, противоречие. В случае $w = 5$ имеем $\alpha \in \{5,10\}$ и 7 не делит 10α. В случае $w = 4$ имеем $\alpha \in \{4,8\}$ и 11 не делит 10α. В случае $w = 3$ имеем $t = 7\alpha$ и 8 не делит 10α, поэтому $\alpha = 8$ и $8(9+56+1-8)$ не делит $s(s+1)t(t+1)$. В случае $w = 2$ имеем $\alpha \in \{2,4\}$ и $t \in \{15,30\}$. Так как $4(6+30+1-4)$ не делит $s(s+1)t(t+1)$, то $\mathcal{S}$ является расширением геометрии $pG_2(6,15)$.

Если $x = 2$, то $t = 3\alpha + \alpha/w$ и $3w-1$ делит 4α. Поэтому $\alpha = 2w$ и $w = 3$, противоречие с тем, что $6(9+20+1-6)$ не делит $s(s+1)t(t+1)$.

Если $x = 5$, то $t = 6\alpha/5 - \alpha/(5w)$, противоречие.

Итак, s не делится на 3, поэтому 3 делит t и $s = 3w+1$. Тогда $\alpha \le 3w-1$, $(3\alpha+(3w+1)t)x = 9\alpha(w+1)$ и $x < 3$.

Если $x = 1$, то $t = 3\alpha(3w+2)/(3w+1)$, противоречие. Если $x = 2$, то $t = 3\alpha/2$, α четно и w нечетно. Так как $\bar\mu = 6st/(\alpha(s-1)) = 3(3w+1)/w$, то $w \in \{1,3\}$. Если $w = 1$, то $s = 4, \alpha = 2, t = 3$, противоречие с тем, что частичная геометрия $pG_2(4,3)$ не существует. Если $w = 3$, то $s = 10$, Γ является псевдогеометрическим графом для $pG_9(11,15)$ и нарушается условие целочисленности.

Лемма 3.6. *Если $s \le 10$, то $\mathcal{S}$ является геометрией $EpG_2(6,15)$.*

Доказательство. Пусть $s = 4$. Тогда $\alpha = 2$ и $3(2t+3)$ делит $5 \cdot 6 \cdot 2t(2t+1)$, кроме того, по лемме 3.5 простое число 5 делит $2t+3$. Следовательно, $2t+3 = 15$, $t = 6$, и $s+t+1-\alpha = 9$ не делит $st(s+1)(t+1)$.

Пусть $s = 6$. По лемме 3.5 число 7 делит $3(\alpha+2t)$. Если $\alpha = 4$, то $t+2$ делится на 7 и $t = 7\beta+5$. Далее, $4(7\beta+8)$ делит $42(7\beta+5)(7\beta+6)$ и $7\beta+8$ делит 126, противоречие.

Если $\alpha = 3$, то $2t+3$ делится на 7 и $t = 7\beta+2$. Далее, $3(7\beta+6)$ делит $42(7\beta+2)(7\beta+3)$ и $7\beta+6$ делит 84, поэтому $\beta = 0$, $t = 2$ и $\mathcal{S}$ является расширением геометрии $pG_3(6,2)$. Но в этом случае по лемме 1.2 число $s-1 = \alpha+2$ должно быть четно, противоречие.

Если $\alpha = 2$, то $t+1$ делится на 7 и $t = 7\beta-1$. Далее, $2(7\beta+4)$ делит $42(7\beta-1)7\beta$ и $7\beta+4$ делит $21 \cdot 20$, поэтому $\beta = 8$, $t = 55$, противоречие с тем, что геометрия $EpG_2(6,55)$ не удовлетворяет условию Крейна.

Пусть $s = 8$. Так как $\bar\mu = 6st/(\alpha(s-1))$, то 7 делит t и α четно (так как α делит st, но не делит t). По лемме 3.5 число 3 делит t, поэтому $t = 21\beta$.

Если $\alpha = 6$, то $6(21\beta+3)$ делит $72(21\beta+1)21\beta$ и $7\beta+1$ делит $84 \cdot 6$, поэтому $\beta \in \{1,5\}$. В случае $\beta = 5$ число $6(8+105+1-6)$ не делит $st(s+1)(t+1)$. В случае $\beta = 1$ число $(s-1)(3+st/\alpha)$ не делит $s(s+1)(s+2)t(1+st/\alpha)/\alpha$, противоречие.

Если $\alpha = 4$, то $4(21\beta+5)$ делит $72(21\beta+1)21\beta$, $21\beta+5$ делит $18 \cdot 21 \cdot 20$, поэтому $\beta = 0$, противоречие. Если $\alpha = 2$, то $2(21\beta+7)$ делит $72(21\beta+1)21\beta$, $3\beta+1$ делит $108 \cdot 6$, поэтому $\beta = 1$, противоречие с тем, что $(s-1)(3+st/\alpha) = 7 \cdot 87$ не делит $s(s+1)(s+2)t(1+st/\alpha)/\alpha$.

Пусть $s = 10$. Тогда $t = 3t'$ для некоторого целого числа t', и 11 делит $3\alpha - t$. Поэтому $t' = 11\beta+\alpha$. Если $\alpha = 8$, то $t = 33\beta+24$, $8(33\beta+27)$ делит $110(33\beta+24)(33\beta+25)$ и $11\beta+7$ делит $55 \cdot 12$, противоречие.

Если $\alpha = 7$, то $t = 33\beta + 21$, $7(33\beta + 25)$ делит $110(33\beta + 21)(33\beta + 22)$ и $33\beta + 25$ делит $10 \cdot 12$, противоречие.

Если $\alpha = 6$, то $t = 33\beta + 18$, $6(33\beta + 23)$ делит $110(33\beta + 18)(33\beta + 19)$ и $33\beta + 23$ делит $55 \cdot 20$, противоречие.

Если $\alpha = 5$, то $t = 33\beta + 15$ и $5(33\beta + 21)$ делит $110(33\beta + 15)(33\beta + 16)$ и $11\beta + 7$ делит $10 \cdot 30$, противоречие.

Если $\alpha = 4$, то $t = 33\beta + 12$ и $4(33\beta + 19)$ делит $110(33\beta + 12)(33\beta + 13)$ и $33\beta + 19$ делит $5 \cdot 42$, противоречие.

Если $\alpha = 3$, то $t = 33\beta + 9$ и $3(33\beta + 17)$ делит $110(33\beta + 9)(33\beta + 10)$ и $33\beta + 17$ делит $10 \cdot 56$, противоречие.

Если $\alpha = 2$, то $t = 33\beta + 6$ и $2(33\beta + 15)$ делит $110(33\beta + 6)(33\beta + 7)$ и $11\beta + 5$ делит $5 \cdot 24$, поэтому $\beta = 0$ и $(s-1)(3 + st/\alpha) = 9 \cdot 33$ не делит $s(s+1)(s+2)t(1 + st/\alpha)/\alpha = 5 \cdot 11 \cdot 12 \cdot 6 \cdot 31$.

Лемма 3.7. *Если $s \geq 12$, то $s - 1$ делит t, и $s \neq 14$.*

Д о к а з а т е л ь с т в о. Пусть $s \geq 12$. Если $s - 1$ не делит t, то $s = 16$ и 3 не делит t. Но в этом случае $3 + st/\alpha$ взаимно просто с 6, и $3 + st/\alpha$ делит 17, противоречие.

Пусть $s = 14$. Тогда 13 делит t, и либо $\alpha = 7$, либо α четно. Если $\alpha = 7$, то $2t + 3$ делит $3 \cdot 15$, противоречие.

Если 3 делит $2t/\alpha$, то $1 + st/(3\alpha)$ делит $2 \cdot 15 \cdot 16$. Но $7 \cdot 13$ не делит $\delta - 1$ для любого делителя δ числа $2^5 \cdot 15$. Значит, 3 не делит $2t/\alpha$, и $3 + st/\alpha$ делит $2 \cdot 5 \cdot 16$. Как и выше, пришли к противоречию.

Лемма 3.8. *Параметр s меньше* 12.

Д о к а з а т е л ь с т в о. Пусть $s \in \{12, 16, 18\}$. Согласно леммам 3.5, 3.7 число $s+1$ делит $3\alpha + st$, и $s - 1$ делит t. Если 3 не делит st/α, то $3 + st/\alpha$ делит $2(s + 1)(s + 2)$. Пусть $s = 12$. Тогда 3 делит α, и $3 + 12t/\alpha$ делит $7 \cdot 13$. Значит, $3t/\alpha = 22$ и $\alpha \in \{3, 6\}$ ($\alpha \neq 9$ по лемме 1.2). Следовательно, $t = 22$ или 44, но в каждом случае $s + t + 1 - \alpha$ не делит $st(s + 1)(t + 1)$. Если $s = 16$, то $3 + 16t/\alpha$ делит 17, противоречие. Пусть $s = 18$. Тогда $\alpha = 9$, и 3 не делит t, так что $2t + 3$ делит $19 \cdot 5$. Противоречие с тем, что 17 делит t.

Таким образом, 3 делит st/α, и $1+st/(3\alpha)$ делит $2(s+1)(s+2)$. Пусть $s = 12$. Тогда 11 делит $\delta - 1$ для некоторого делителя δ числа $2^3 \cdot 7$. Поэтому $4t/\alpha = 33 \cdot 11$, $\alpha \in \{4, 8\}$ и $t \in \{363, 726\}$. Но в первом случае нарушается условие Крейна, а во втором число $s+t+1-\alpha = 731$ не делит $st(s + 1)(t + 1)$.

Пусть $s = 16$. Тогда $st/(3\alpha)$ является четным, и $1 + st/(3\alpha)$ делит $17 \cdot 9$. Если $\alpha = 10$, то $1 + 8t/15$ делит $17 \cdot 9$ и t нечетно. Значит, $t = 15$ или $t = 15 \cdot 19$. В любом из этих случаев $s + t + 1 - \alpha$ не делит $st(s + 1)(t + 1)$. Поэтому 5 не делит α, и 5 делит $\delta - 1$ для некоторого δ, являющегося делителем числа $17 \cdot 9$. Следовательно, $16t = 3\alpha \cdot 50$, $\alpha = 8$ и $t = 75$. В этом случае $s + t + 1 - \alpha = 84$ не делит $st(s + 1)(t + 1)$.

Пусть $s = 18$. Тогда $1 + st/(3\alpha)$ делит $19 \cdot 40$, и 17 делит $5 \cdot 2^\beta - 1$ для некоторого $\beta \leq 4$, противоречие. Лемма доказана.

Леммы 3.4, 3.6 и 3.8 доказывают теорему 2.

Поступила 15.11.2006

СПИСОК ЛИТЕРАТУРЫ

1. **Cameron P. J., Hughes D. R., Pasini A.** Extended generalized quadrangles // Geom. Dedicata. 1990. V. 35. P. 193–228.
2. **Thas J. A.** Some results on quadrics and new partial geometries // Simon Stevin. 1981. V. 55. P. 129–139.

3. **Hobart S. A., Hughes D. R.** Extended partial geometries: nets and dual nets // Europ. J. Comb. 1990. V. 11. P. 357–372.
4. **Hobart S. A., Hughes D. R.** *EpG*s with minimal μ. II // Geom. Dedicata. 1992. V. 42. P. 129–138.
5. **Hughes D. R.** Extended partial geometries: dual 2-design // Europ. J. Comb. 1990. V. 11. P. 459–472.
6. **Seidel J. J.** Strongly regular graphs with $(-1, 1, 0)$ adjacency matrix having eigenvalue 3 // Linear Algebra & Appl. 1968. V. 1. P. 281–298.
7. **Brouwer A. E., Lint J. H. van.** Strongly regular graphs and partial geometries // Enumeration & Design / Eds. D. Jackson, S. Vanstone. New York: Academic Press, 1984. P. 85–122.

ТРУДЫ ИНСТИТУТА МАТЕМАТИКИ И МЕХАНИКИ УрО РАН

Том 13 № 1 2007

УДК 519.14

НЕСУЩЕСТВОВАНИЕ ЛОКАЛЬНО $\bar{J}(10,5)$-ГРАФОВ[1]

Д. В. Падучих

В работе доказано несуществование графов, у которых окрестность каждой вершины изоморфна графу $\bar{J}(10,5)$.

Мы будем рассматривать неориентированные графы без петель и кратных ребер. Если не оговорено противное, то под подграфом Δ графа Γ мы будем понимать подграф, индуцированный графом Γ на множестве вершин Δ.

Пусть a — вершина графа Γ. Подграф $\Gamma_i(a)$ всех вершин графа Γ, находящихся на расстоянии i от a, называется *i-окрестностью вершины a*. Положим $\Gamma(a) = \Gamma_1(a)$ (*окрестность a*), $a^\perp = \{a\} \cup \Gamma(a)$.

Пусть $X \subseteq \Gamma$ — некоторое множество вершин. *Сильной* (*слабой*) *окрестностью множества X* назовем подграф $\Gamma(X) = \bigcap_{x\in X}\Gamma(x)$ (подграф $\Gamma\langle\langle X\rangle\rangle = \bigcup_{x\in X}\Gamma(x) - X$). Если $X = \{x_1, x_2, ..., x_n\}$, мы будем писать также $\Gamma(x_1, x_2, ..., x_n)$ для обозначения $\Gamma(X)$ и $\Gamma\langle\langle x_1, x_2, ..., x_n\rangle\rangle$ для обозначения $\Gamma\langle\langle X\rangle\rangle$. В случае, когда понятно, о каком графе Γ идет речь, договоримся использовать запись $[x_1, x_2, ..., x_n]$ вместо $\Gamma(x_1, x_2, ..., x_n)$ и $\langle\langle x_1, x_2, ..., x_n\rangle\rangle$ вместо $\Gamma\langle\langle x_1, x_2, ..., x_n\rangle\rangle$. В случае $X = \{x\}$ сильная и слабая окрестности совпадают, т. е. верны равенства $[x] = \langle\langle x\rangle\rangle = \Gamma(x)$. Если вершины $a, b \in \Gamma$ смежны, то удобно считать, что $[a, b] = \Delta(b)$, где $\Delta = [a]$.

Пусть $\mathcal{F}$ — некоторый класс графов. Граф Γ назовем *локально $\mathcal{F}$-графом*, если окрестность $\Gamma(a)$ для любой вершины $a \in \Gamma$ изоморфна некоторому графу $\Delta \in \mathcal{F}$. Если при этом класс $\mathcal{F}$ содержит единственный граф Δ, то граф Γ назовем *локально Δ-графом.*

Пусть Γ — граф, $a, b \in \Gamma$, число вершин в $\Gamma(a, b)$ обозначается через $\mu(a, b)$ (соответственно, $\lambda(a, b)$), если a, b находятся на расстоянии 2 (соответственно, смежны) в Γ, а $\Gamma(a, b)$ называется *μ-подграфом* (соответственно, *λ-подграфом*).

Степенью вершины называется число вершин в ее окрестности. Граф Γ называется *регулярным степени k*, если степень любой вершины a из Γ равна k, и *реберно регулярным с параметрами (v, k, λ)*, если он имеет v вершин, регулярен степени k и каждое его ребро лежит в λ треугольниках. Граф Γ называется *вполне регулярным графом с параметрами (v, k, λ, μ)*, если он реберно регулярен с параметрами (v, k, λ), а $\Gamma(a, b)$ содержит μ вершин для любых двух вершин a, b на расстоянии 2 в Γ. Вполне регулярный граф диаметра 2 называется *сильно регулярным.* Для подграфа Δ графа Γ через $K_i(\Delta)$ обозначим подграф, индуцированный всеми вершинами из $\Gamma - \Delta$, смежными точно с i вершинами подграфа Δ.

Рассмотрим множества $X = \{x_1, x_2, ..., x_m\}$ и $Y = \{y_1, y_2, ..., y_n\}$. Граф на множестве пар $X \times Y$ называется *прямоугольной $(m \times n)$-решеткой* , если пары (x, y) и (x', y') смежны тогда и только тогда, когда $x = x'$, $y \neq y'$ или $x \neq x'$, $y = y'$. Подграф решетки $X \times Y$, состоящий из всевозможных пар (x, y) таких, что $x \in X'$ и $y \in Y'$ для некоторых подмножеств $X' = \{x_{i_1}, x_{i_2}, ..., x_{i_k}\} \subseteq X$, $Y' = \{y_{j_1}, y_{j_2}, ..., y_{j_l}\} \subseteq Y$, будем называть *подрешеткой решетки $X \times Y$* и обозначать через $(i_1, i_2, ..., i_k; j_1, j_2, ..., j_l)$. Особую роль в работе играют подрешетки вида $(i_1, i_2; j_1, j_2)$, которые мы будем называть *четырехугольниками решетки $X \times Y$*. Множество

[1]Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (проект 05-01-00046).

всех четырехугольников решетки $X \times Y$ мы будем обозначать через $Q(X \times Y)$. Будем говорить, что четырехугольник $(i_1, i_2; j_1, j_2)$ решетки $X \times Y$ отвечает четырем прямым i_1, i_2, j_1, j_2.

Графом Джонсона $J(n,m)$ называется граф, вершинами которого являются m-подмножества данного n-множества X, и вершины a, b смежны тогда и только тогда, когда они пересекаются по $(m-1)$-множеству. При $m = 2$ граф $J(n,m)$ называется *треугольным графом* и обозначается через $T(n)$.

Частным графа Джонсона $J(2m,m)$ называется граф $J^\sigma(2m,m)$, полученный отождествлением каждого m-множества с образом его дополнения под действием подстановки σ на X, где $\sigma^2 = 1$ и σ имеет по крайней мере 8 неподвижных точек. Если $\sigma = 1$, то частное называется *стандартным* и обозначается через $\bar{J}(2m,m)$.

Результат, представленный в данной работе, был получен в рамках более общего исследования графов с заданными ограничениями на строение μ-подграфов [1, 2]. Однако задача исследования локально $\mathcal{F}$-графов представляет интерес сама по себе.

Теорема. *Локально $\bar{J}(10,5)$-графы не существуют.*

1. Предварительные результаты

В этом параграфе приведены предварительные результаты, а также доказаны некоторые утверждения о графе $\bar{J}(10,5)$.

Лемма 1.1. *Если Γ является сильно регулярным графом с параметрами (v,k,λ,μ), то*

(1) $k(k-\lambda-1) = \mu(v-k-1)$ (*прямоугольное соотношение*);

(2) *кратности отличных от k собственных значений $r > 0$ и $l < 0$ равны соответственно*

$$f = \frac{-k(l+1)(k-l)}{(k+rl)(r-l)} \qquad \text{и} \qquad g = \frac{k(r+1)(k-r)}{(k+rl)(r-l)};$$

(3) *либо Γ имеет параметры $(4\mu+1, 2\mu, \mu-1, \mu)$ (половинный случай), либо $(\lambda-\mu)^2 + 4(k-\mu) = (r-l)^2$ и собственные значения r и l графа Γ целые*;

(4) *если собственные значения r и $l = -m$ целые и $m > 1$, то $m-1$ делит $k-\lambda-1$, $\mu = \lambda + m + 1 - (k-\lambda-1)/(m-1)$ и $r - l = m - 1 + (k-\lambda-1)/(m-1)$.*

Д о к а з а т е л ь с т в о. Первые три утверждения леммы хорошо известны и могут быть найдены, например, в [1, гл. 1]. Утверждение (4) доказано в [2, лемма 3.1]. □

Граф $\bar{J}(10,5)$ можно построить, используя конструкцию, описанную в следующей лемме.

Лемма 1.2. *Пусть дана (5×5)-решетка R. Определим граф Γ, полагая в качестве множества его вершин $\{\infty\} \cup R \cup Q(R)$ и задавая смежность по следующим правилам:*

(1) *∞ смежна со всеми вершинами из R*;

(2) *вершина $a \in R$ смежна с четырехугольником $X \in Q(R)$ тогда и только тогда, когда $a \in X$*;

(3) *два четырехугольника $X, X' \in Q(R)$ смежны, если они либо имеют общее ребро, либо изолированы в R (т. е. не имеют общих прямых).*

Тогда граф Γ изоморфен графу $\bar{J}(10,5)$.

Д о к а з а т е л ь с т в о. Хорошо известно, что граф $\bar{J}(10,5)$ является сильно регулярным графом с параметрами $(126,25,8,4)$, окрестности его вершин изоморфны (5×5)-решетке, а μ-подграфы являются четырехугольниками. Возьмем произвольную вершину $a\in\bar{J}(10,5)$ и отождествим ее с ∞; вершины x, не смежные с a, отождествим с μ-подграфами $[a,x]$. Легко видеть, что таким образом мы получаем биекцию $\bar{J}(10,5)$ на граф Γ. Остается показать, что смежности в графах Γ и $\bar{J}(10,5)$ согласованы.

Очевидно, что правила (1)–(2) согласованы со смежностью на $\bar{J}(10,5)$. Согласованность первой части правила (3) вытекает из того, что в решетке четырехугольники X и X' должны пересекаться по ребру, а в $\bar{J}(10,5)$ (сильная) окрестность ребра не содержит 3-коклик.

Докажем согласованность второй части правила (3). Без ограничения общности можно считать, что $a=\{1,2,3,4,5\}$. Заметим, что вершины вида $(a-\{i\})\cup\{j\}$ $(i\in a, j\notin a)$ образуют либо "вертикальную", либо "горизонтальную" прямую в окрестности a, когда мы фиксируем либо i, либо j. Отсюда, без ограничения общности можно считать, что четырехугольники X и X' состоят соответственно из вершин $\{\{1,2,3,4,6\},\{1,2,3,4,7\},\{1,2,3,5,7\},\{1,2,3,5,6\}\}$ и $\{\{1,2,4,5,8\},\{1,2,4,5,9\},\{1,3,4,5,9\},\{1,3,4,5,8\}\}$. Но тогда четырехугольникам X и X' соответствуют вершины $\{1,2,3,6,7\}$ и $\{1,4,5,8,9\}$, которые смежны по определению графа $\bar{J}(10,5)$. $\square$

В следующих двух леммах сформулированы некоторые свойства октаэдров, содержащихся в графе $\bar{J}(10,5)$.

Лемма 1.3. *Пусть a — вершина из $\bar{J}(10,5)$, а X — октаэдр из $\bar{J}(10,5)$ такой, что $a\notin\langle\langle X\rangle\rangle\cup X$. Тогда с точностью до выбора координат на $[a]$ выполняется одно из двух утверждений*:

(1) *$[a]\cap\langle\langle X\rangle\rangle=\Sigma$, где Σ — подрешетка $(1,2;1,2,3,4)$, причем имеется биекция между четырехугольниками из $Q(\Sigma)$ и вершинами из X*;

(2) *$[a]\cap\langle\langle X\rangle\rangle=T$, где T — подграф $(1,2;1,2,3,4)\cup(3,4;2,3,4,5)$, причем имеется биекция между четырехугольниками из $Q(T)$, содержащими ребро $(1,2;1)$ или $(3,4;5)$, и вершинами из X.*

Д о к а з а т е л ь с т в о. Пусть b,c — две несмежные вершины октаэдра X. Тогда $b,c\in Q([a])$, b и c как четырехугольники не пересекаются и по лемме 1.2 имеют либо одну общую прямую, либо две (обе "вертикальные" или обе "горизонтальные") общие прямые. Утверждения (1) и (2) теперь получаются в обоих случаях непосредственным вычислением μ-подграфа $[b,c]$ с помощью леммы 1.2. $\square$

Лемма 1.4. *Граф $\bar{J}(10,5)$ не содержит двух изолированных октаэдров.*

Д о к а з а т е л ь с т в о. Предположим, что $\bar{J}(10,5)$ содержит два изолированных октаэдра X и X'. Возьмем вершину $a\in X$. Поскольку октаэдры X и X' изолированы, имеем $a\notin\langle\langle X'\rangle\rangle\cup X'$. Отсюда по лемме 1.3 получаем, что без ограничения общности подграф $[a]\cap\langle\langle X'\rangle\rangle$ совпадает либо с Σ, либо с T. Теперь заметим, что условие изолированности октаэдров означает, что четырехугольник $X(a)$, с одной стороны, не пересекает $[a]\cap\langle\langle X'\rangle\rangle$, а с другой стороны, не может быть изолированным ни от одного из μ-графов $[a,x']$ $(x'\in X')$. Однако легко видеть, что это условие не выполняется ни в случае $[a]\cap\langle\langle X'\rangle\rangle=\Sigma$, ни в случае $[a]\cap\langle\langle X'\rangle\rangle=T$. Противоречие. $\square$

2. Локально $\bar{J}(10,5)$-графы

Далее мы будем предполагать, что граф Γ — связный локально $\bar{J}(10,5)$-граф, и придем к противоречию.

Лемма 2.1. *Граф* Γ *— вполне регулярный граф диаметра* 3 *с параметрами* $k = 126$, $\lambda = 25$ *и* $\mu = 6$, *причем все* μ-*подграфы в* Γ *являются октаэдрами.*

Д о к а з а т е л ь с т в о. Утверждение о том, что граф Γ является реберно регулярным графом с параметрами $k = 126$ и $\lambda = 25$, вытекает из того, что Γ — локально $\bar{J}(10,5)$-граф. Возьмем в Γ геодезический 2-путь a, b, c. Поскольку вершины a, c лежат в окрестности вершины b, их μ-подграф в $[b]$ является четырехугольником. Таким образом, μ-подграф $[a, c]$ — локально четырехугольный граф, и, следовательно, является объединением изолированных октаэдров. По лемме 1.4 подграф $[a, c]$ содержит только один октаэдр, и утверждение о μ-подграфах доказано.

Остается доказать, что диаметр Γ равен 3. Допустим сначала, что диаметр равен 2. Тогда Γ — сильно регулярный граф с указанными параметрами и наименьшим собственным значением $-m$. По лемме 1.1 получим $6 = 26 + m - 100/(m-1)$, и это уравнение имеет только одно положительное решение $m = 5$. Тогда граф Γ имеет собственные значения $r = 24$ и $l = -5$, противоречие с тем, что $f = 126 \cdot 4 \cdot 131/(6 \cdot 29)$ не является целым числом.

Пусть теперь диаметр Γ больше 3. Возьмем геодезический 4-путь a, b, c, d, e в графе Γ. Тогда μ-подграфы $[c, a]$ и $[c, e]$ — это два изолированных октаэдра, которые содержатся в $[c]$. Противоречие с леммой 1.4. □

Лемма 2.2. *Пусть вершины* a, b *находятся на расстоянии* 2 *в графе* Γ. *Тогда подграф* $[b] \cap K_0([a, b])$ *содержится в* $\Gamma_3(a)$.

Д о к а з а т е л ь с т в о. Очевидно, подграф $[b] \cap K_0([a, b])$ содержится в $\Gamma_2(a) \cup \Gamma_3(a)$. Предположим, что найдется вершина $b' \in [b] \cap \Gamma_2(a)$ такая, что октаэдры $[a, b]$ и $[a, b']$ не пересекаются. По лемме 1.4 существует ребро cc' такое, что $c \in [a, b]$ и $c' \in [a, b']$. Заметим, что вершина c смежна с единственной вершиной c' в октаэдре $[a, b']$, поскольку в октаэдре $[c, b']$ только одна вершина c' не смежна с b. Аналогично, вершина c' смежна с единственной вершиной c в октаэдре $[a, b]$.

Так как вершины a и c' смежны, то в силу леммы 1.2 и замечания из предыдущего параграфа, четырехугольники $[c] \cap [b, a]$ и $[c] \cap [b, c']$ должны быть изолированными. Легко видеть, что эти же четырехугольники можно записать как $[b] \cap [c, d]$ и $[b] \cap [c, b']$, где $d \in [a, b]$ — вершина, не смежная с c. По лемме 1.2 из изолированности четырехугольников $[b] \cap [c, d]$ и $[b] \cap [c, b']$ следует, что вершины d и b' смежны. Противоречие с выбором вершины b'. □

Зафиксируем вершину d из $\Gamma_3(a)$ и положим $\Delta = [d] \cap \Gamma_2(a)$.

Лемма 2.3. *Для любой вершины* $x \in \Delta$ *подграф* $\Delta(x)$ *изоморфен графу* Σ *или графу* T *из леммы* 1.3, *причем граф* Δ *содержит октаэдр* X *такой, что* $\Delta(x) = [d, x] \cap \langle\langle X \rangle\rangle$.

Д о к а з а т е л ь с т в о. Заметим, что подграф $[x]$ содержит октаэдр $[x, a]$ и вершину d такую, что $d \notin \langle\langle [x, a] \rangle\rangle$. Отсюда по лемме 1.3 получаем, что подграф $\Delta(x)$ изоморфен графу Σ или графу T.

Возьмем теперь произвольную вершину $y \in [x, a]$. Очевидно, октаэдр $[d, y]$ содержится в графе Δ, и можно каждой вершине $y \in [x, a]$ сопоставить вершину $y' \in [d, y]$, не смежную с x. Поскольку четырехугольники $[x] \cap [d, y]$ и $[d] \cap [x, y']$ совпадают, а по лемме 1.2 смежность на множествах $\{y \mid y \in [x, a]\}$ и $\{y' \mid y \in [x, a]\}$ однозначно определена взаимным расположением соответствующих четырехугольников из $[d, x]$, то отображение $y \mapsto y'$ является изоморфным вложением октаэдра $[x, a]$ в граф Δ. □

Лемма 2.4. *Пусть* x *— вершина из* Δ *и* $b \in [x, a]$. *Подграф* $\Delta(x)$ *изоморфен* Σ *тогда и только тогда, когда четырехугольники* $[x, a, b]$ *и* $[x, d, b]$ *имеют точно две общие прямые* (*обе "вертикальные" или обе "горизонтальные"*) *в решетке* $[x, b]$.

Д о к а з а т е л ь с т в о. Ввиду леммы 2.2 нам нужно доказать, что утверждение верно для произвольных вершин $x \in \Gamma_2(a)$ и $d \in [x] \cap K_0([x,a])$. Согласно лемме 1.2 мы можем построить подграф $[x]$ по решетке $[x,b]$. При этом с точностью до выбора координат на $[x,b]$ можно считать, что октаэдр $[x,a]$ состоит из вершин четырехугольника $(1,2;1,2)$, самого четырехугольника $(1,2;1,2)$ и вершины b. Так как вершина d не смежна ни с одной из вершин $[x,a]$, то соответствующий d четырехугольник не пересекает четырехугольника $(1,2;1,2)$ и имеет с последним по крайней мере одну общую прямую. Пусть сначала четырехугольники d и $(1,2;1,2)$ имеют ровно две общие прямые. Без ограничения общности будем считать, что вершина d совпадает с $(3,4;1,2)$. По определению, $\Delta(x) = [x \cap [d] \cap \langle\langle [x,a] \rangle\rangle$. Покажем, что графы $\Delta(x)$ и Σ изоморфны.

Прежде всего заметим, что $\Delta(x)$ содержит вершины из $(3,4;1,2)$, а остальные вершины из $\Delta(x)$ являются четырехугольниками, которые, с одной стороны, смежны с $(3,4;1,2)$, а с другой — пересекают или смежны с $(1,2;1,2)$. Очевидно, не существует четырехугольников, изолированных и от $(1,2;1,2)$, и от $(3,4;1,2)$. Четырехугольников, которые были бы изолированы от одного из четырехугольников $(1,2;1,2)$ и $(3,4;1,2)$ и пересекали другой, тоже не существует. Остаются четырехугольники $(1,3;1,2)$, $(2,3;1,2)$, $(1,4;1,2)$ и $(2,4;1,2)$. Таким образом, граф $\Delta(x)$ содержит ровно 8 вершин. Следовательно, по лемме 2.3 граф $\Delta(x)$ изоморфен Σ.

Пусть теперь четырехугольники d и $(1,2;1,2)$ имеют точно одну общую прямую. Тогда с точностью до выбора координат на $[x,b]$ можно считать, что d — четырехугольник $(3,4;1,3)$. По аналогии с предыдущим абзацем находим, что $\Delta(x)$ содержит вершины из $(3,4;1,3)$ и следующие четырехугольники: $(1,3;1,3)$, $(1,4;1,3)$, $(2,3;1,3)$, $(2,4;1,3)$, $(3,4;3,4)$, $(3,4;3,5)$. Таким образом, граф $\Delta(x)$ содержит по крайней мере 10 вершин и, следовательно, по лемме 2.3 изоморфен T. □

Скажем, что вершина x из Δ имеет тип Σ (соответственно, тип T), если подграф $\Delta(x)$ изоморфен подграфу Σ (соответственно, T) из леммы 1.3.

Лемма 2.5. *Пусть x — вершина типа Σ. Тогда выполняются следующие утверждения*:

(1) *$\{x\} \cup \Delta(x)$ содержится в подграфе $R = R_x$ из Δ, изоморфном $T(6)$*;

(2) *если R содержит вершину типа T, то x — единственная вершина из R, имеющая тип Σ*;

(3) *если R не содержит вершин типа T, то $R = \Delta$.*

Д о к а з а т е л ь с т в о. Имеется биекция между вершинами октаэдра $[a] \cap [x]$ и четырехугольниками подграфа $\Delta(x)$, при которой вершине $b \in [a] \cap [x]$ соответствует четырехугольник $[b] \cap [x] \cap [d]$. Поэтому каждый четырехугольник из $\Delta(x)$ вкладывается в октаэдр, лежащий в $[d]$. В результате получим подграф R, содержащий x, $\Delta(x)$ и 6-вершинный подграф (соответствующий четырехугольникам из $\Delta(x)$. Подграф R изоморфен $T(6)$. Утверждение (1) доказано.

Допустим, что $\Delta(x)$ содержит вершину y типа T. Тогда $R(y)$ содержит (2×3)-подрешетку, состоящую из вершин типа T. Значит, любая 5-клика из R, содержащая вершину типа Σ, либо состоит из вершин типа Σ, либо содержит единственную вершину типа Σ. В первом случае вершины из R, имеющие тип T, индуцируют треугольный подграф, изоморфный $T(5)$, а во втором случае каждая вершина из $R - \{x\}$ имеет тип T.

Покажем, что первый случай невозможен. В противном случае для вершины y типа T из R подграф $\Delta(y)$ является объединением двух непересекающихся (2×4)-решеток. Без ограничения общности можно считать, что первая решетка содержит клики $\{a_1, ..., a_4\}$, $\{b_1, ..., b_4\}$, а вторая решетка содержит клики $\{c_2, ..., c_5\}$, $\{d_2, ..., d_5\}$, причем вершины, имеющие заданный индекс, образуют клику. Ребра $\{a_1, b_1\}$, $\{c_5, d_5\}$ назовем концевыми. Теперь 5-клика графа $\Delta(y)$, состоящая из вершин типа Σ, содержит концевое ребро и 3 вершины f_1, f_2, f_3, отвечающие четырехугольникам (2×4)-решетки, содержащим указанное концевое ребро. Если вершины g_1, g_2, g_3 отвечают четырехугольникам второй (2×4)-решетки из $\Delta(y)$, содержащим другое концевое ребро, то $\{f_1, ..., f_3, g_1, ..., g_3\}$ является октаэдром. Противоречие с тем, что $\Delta(f_i)$ содержится в R. Утверждение (2) доказано.

Допустим, что каждая вершина из R имеет тип Σ. Тогда R является связной компонентой графа Δ. Так как в $\bar{J}(10,5)$ нет вершин, изолированных от подграфов, изоморфных $T(6)$, то $\Delta = R$. □

Если некоторая вершина графа Γ смежна с 3 вершинами грани октаэдра $[a]\cap[x]$, то будем говорить, что она лежит на этой грани. Раскрасим грани октаэдра в "шахматном порядке", так что из двух соседних граней одна будет белого, а другая — черного цвета.

Лемма 2.6. *Выполняются следующие утверждения*:

(1) *для любой вершины $x \in \Gamma_2(a)$ найдется такая 6-клика $L = L_x$ в $\Gamma_3(a)\cap[x]$, что для $d \in L$ вершина x имеет тип Σ в графе $\Gamma_2(a)\cap[d]$, а для любой вершины $e \in \Gamma_3(a)\cap[x]-L$ вершина x имеет тип T в графе $\Gamma_2(a)\cap[e]$;*

(2) *клика L является объединением двух треугольников L^h, L^v таких, что $\Gamma_2(a)\cap[x]$ содержит две изолированные (3×4)-решетки Ψ_h, Ψ_v, причем $\Gamma_2(a)\cap[x]\cap[d] \subset \Psi_y$, если $d \in L^y$, $y \in \{v, h\}$;*

(3) *вершины решетки Ψ_h лежат на гранях октаэдра одного цвета (по 3 вершины на грани), а вершины решетки Ψ_v лежат на гранях другого цвета.*

Доказательство. Пусть $x \in \Gamma_2(a)$. Тогда $K_0([a]\cap[x]) = [x]\cap\Gamma_3(a)$. Зафиксируем вершину $b \in [a]\cap[x]$ и представим $[x]$ как объединение $\{b\}\cup([b]\cap[x])$ с множеством вершин, отвечающих четырехугольникам решетки $[b]\cap[x]$. Октаэдр $[a]\cap[x]$ содержит вершину b, четырехугольник Φ из $[b]\cap[x]$ и вершину, отвечающую Φ, а $K_0([a]\cap[x])$ состоит из вершин, отвечающих четырехугольникам, не пересекающим Φ. По лемме 2.4 вершина x имеет тип Σ в графе $\Gamma_2(a)\cap[d]$ тогда и только тогда, когда четырехугольник, отвечающий d, не пересекает Φ и имеет две общих прямых с Φ; вершина x имеет тип T в графе $\Gamma_2(a)\cap[e]$ тогда и только тогда, когда четырехугольник, отвечающий e, не пересекает Φ и имеет единственную общую прямую с Φ.

Вершины, отвечающие четырехугольникам, не пересекающим Φ и имеющим две общие горизонтальные (вертикальные) прямые с Φ, образуют 3-клику, которую назовем горизонтальной (вертикальной). Так как четырехугольники, отвечающие вершинам горизонтальной и вертикальной клик, изолированы в решетке $[b]\cap[x]$, то каждая вершина горизонтальной клики смежна с каждой вершиной вертикальной клики. Утверждение (1) доказано.

Если $\{d_1, d_2, d_3\}$ — горизонтальная 3-клика из L, то подграфы $\Gamma_2(a)\cap[x]\cap[d_i]$ являются (2×4)-решетками, попарно пересекающимися по разным 4-кликам. Таким образом, объединение трех указанных решеток является (3×4)-решеткой Ψ_h из $\Gamma_2(a)\cap[x]$. Симметрично, вертикальной 3-клике из L отвечает (3×4)-решетка Ψ_v, причем решетки Ψ_h и Ψ_v изолированы. Утверждение (2) доказано.

Если x — вершина типа Σ в графе $\Gamma_2(a)\cap[d]$, то ввиду леммы 2.4 столбцы решетки Ψ_h содержатся в грани октаэдра $[a]\cap[x]$ одного цвета, а столбцы решетки Ψ_v — в грани другого цвета. Утверждение (3) доказано. □

Лемма 2.7. *Пусть $d \in \Gamma_3(a)$ и $d \in L_x \cap L_y$ для различных вершин $x, y \in \Gamma_2(a)\cap[d]$. Тогда выполняются следующие утверждения*:

(1) *если x, y смежны, то $L_x \cap L_y = \{d, e\}$ для некоторой вершины $e \neq d$ и все вершины из $[d]\cap[e]\cap[x]$ имеют тип Σ относительно d и относительно e;*

(2) *если x, y несмежны и $L_x \cap L_y$ содержит не менее двух вершин, то либо*

(i) $L_x \cap L_y = \{d, e\}$, $[x] \cap [y]$ *содержит вершину* f *из* $L_x - L_y$ *и вершину* g *из* $L_y - L_x$, *либо*

(ii) $L_x \cap L_y$ *является треугольником из* L_x *и из* L_y *и* $[x] \cap [y]$ *содержит* 3*-клику из* $\Gamma_2(a)$, *либо*

(iii) $L_x \cap L_y = \{d, e, h\}$, *при этом одна из точек* d, e, h *лежит в одном треугольнике из* L_x, *а остальные две — в другом, и* $[x] \cap [y]$ *содержит не менее* 5 *вершин из* $\Gamma_3(a)$.

Д о к а з а т е л ь с т в о. Пусть $d \in \Gamma_3(a)$ и $d \in L_x \cap L_y$ для различных вершин $x, y \in \Gamma_2(a) \cap [d]$. Если x, y смежны, то $\Gamma_2(a) \cap [d]$ — треугольный граф, изоморфный $T(6)$, $[y] \cap L_x = \{d, e\}$ и относительно некоторой вершины e все вершины из $[d] \cap [e] \cap [x]$ имеют либо тип Σ, либо тип T. В первом случае решетка $[d] \cap [e]$ содержит 5-клику Φ из $\Gamma_2(a)$, и для любой вершины u из этой клики L_u содержит d, e и $M - \{u\}$, где M является 5-кликой из $[d] \cap [e]$, пересекающей Φ по $\{u\}$. Во втором случае пересечение подграфа $[d] \cap \Gamma_2(a)$ с решеткой $[e] \cap [y]$ является объединением 4-клики из Φ и 2-клики, содержащей концевые вершины не пересекающей Φ (2×4)-решетки из $[e] \cap [y]$. Противоречие с тем, что $\Gamma_2(a) \cap [d]$ изоморфен $T(6)$. Утверждение (1) доказано.

Пусть вершины x, y несмежны. Если $L_x \cap L_y$ содержит 2 вершины d, e, то d, e лежат либо в разных треугольниках L_x^v и L_x^h, либо в одном. Во втором случае $[d] \cap [e]$ содержит 5-клику из $x^\perp \cap \Gamma_2(a)$, а d, e лежат в общем треугольнике из L_y, $|L_x \cap L_y| = 3$. В первом случае d, e лежат в разных треугольниках из L_x. Тогда они лежат в разных треугольниках из L_y и либо $|L_x \cap L_y| = 3$, либо $L_x - \{d, e\}$ и $l_y - \{d, e\}$ лежат на параллельных прямых решетки $[d] \cap [e]$. Таким образом, либо (a) $L_x \cap L_y = \{d, e\}$, $[x] \cap [y]$ содержит вершину f из $L_x - L_y$ и вершину g из $L_y - L_x$, либо (b) $L_x \cap L_y$ является треугольником из L_x и из L_y и $[x] \cap [y]$ содержит треугольник из $\Gamma_2(a)$, либо (c) $L_x \cap L_y = \{d, e, h\}$, при этом одна из точек d, e, h лежит в одном треугольнике из L_x, а остальные две — в другом, и $[x] \cap [y]$ содержит не менее 5 вершин из $\Gamma_3(a)$. $\square$

Лемма 2.8. *Пусть* x, y *— смежные вершины из* $\Gamma_2(a)$ *и* $L_x \cap L_y = \{d, e\}$. *Тогда выполняются следующие утверждения*:

(1) *вершины* d, e *лежат в единственной* 7*-клике* K *из* $\Gamma_3(a)$ *такой, что для любой вершины* $u \in K$ *подграф* $[u] \cap \Gamma_2(a)$ *является треугольным графом, изоморфным* $T(6)$, *пересекающим окрестности других вершин из* K *по различным* 5*-кликам*;

(2) *подграф* Ω, *индуцированный объединением подграфов* $[u] \cap \Gamma_2(a)$, *где* u *пробегает* K, *изоморфен графу Джонсона* $J(7, 3)$, *и для любой вершины* $z \in \Omega$ *клика* K *пересекает* L_z *по треугольнику.*

Д о к а з а т е л ь с т в о. Пусть $\{d, e, f\}$ — треугольник из L_x, отвечающий (3×4)-решетке Ψ из $[x] \cap \Gamma_2(a)$. Тогда 4-клики $\{y_1, ..., y_4\}$, $\{z_1, ..., z_4\}$ и $\{u_1, ..., u_4\}$ из Ψ попадают в пересечения окрестностей пар вершин $\{d, e\}$, $\{d, f\}$ и $\{e, f\}$.

По лемме 2.7 имеем $L_{y_i} \cap L_{z_i} = \{d, g_i\}$. Решетка $[d] \cap [y_1]$ содержит 5-клики $\{x, y_2, ..., y_4, e\}$, $\{z_1, ..., g_1\}$, поэтому e смежна с g_i. Симметрично, f смежна с g_i и $K = \{d, e, f, g_1, ..., g_4\}$ является 7-кликой. Далее, $[d] \cap [w] \cap \Gamma_2(a)$ является 5-кликой для любой вершины $w \in K - \{d\}$, причем каждая вершина этой 5-клики является вершиной типа Σ относительно w. Теперь роль d может играть любая вершина из K. Утверждение (1) доказано.

Так как каждая вершина $x \in \Omega$ смежна точно с 3 вершинами из K, то Ω является локально (3×4)-графом с $\mu = 4$. По теореме 1 из [3] граф Ω изоморфен $J(7, 3)$. По лемме 2.6 клика K пересекает L_z по треугольнику для любой вершины $z \in \Omega$. $\square$

Лемма 2.9. *Если* Δ *содержит вершину* x *типа* Σ, *то каждая вершина из* $\Delta(x)$ *имеет тип* Σ.

Доказательство. Пусть $y \in \Delta(x)$ и y — вершина типа T. Обозначим через L_1, L_2 непересекающиеся 5-клики из $[d,x]$ такие, что $\Delta(x) \subset L_1 \cup L_2$, а через L_3, L_4, L_5 — различные 5-клики из $[d,x]$, не пересекающие $L_1 \cup L_2$. Без ограничения общности $y \in L_1$. Через y' обозначим смежную с y вершину из L_1. По лемме 2.5 $\{x\} \cup \Delta(x)$ содержится в подграфе $R = R_x$ из Δ, изоморфном $T(6)$. Тогда $\Delta(y) \cap R$ является (2×4)-решеткой, причем $\{x, y'\}$ — максимальная клика из $\Delta(y)$. Далее, $\Delta(y) - R$ также является (2×4)-решеткой, причем ее вершины отвечают четырехугольникам решетки $[x,d]$, содержащим y и пересекающим по ребру одну из клик L_3, L_4, L_5. Поэтому указанные четырехугольники пересекают точно две из указанных клик, скажем L_3, L_4.

Поскольку для любой вершины $z \in \Delta(x) \cap L_2$ найдутся точно две вершины из Δ, отвечающие четырехугольникам решетки $[d,x]$, содержащим y, z, то все вершины из $L_2 \cap \Delta(x)$ имеют тип T и $\Delta(z) - R$ является (2×4)-решеткой, причем ее вершины отвечают четырехугольникам решетки $[x,d]$, содержащим z и пересекающим по ребру одну из клик L_3, L_4. Таким образом, подграф Δ содержит все вершины, отвечающие четырехугольникам решетки $[x,d]$, лежащим в $L_3 \cup L_4 \cup L_5$.

Обозначим через L 5-клику решетки $[d,x]$, не пересекающую $\Delta(x)$, и рассмотрим вершину w, отвечающую четырехугольнику из $L_2 \cup L_3$, пересекающему L по ребру $\{w_2, w_3\}$, $w_i \in L_i$. Решетка $[d,w]$ содержит 5-клику, состоящую из вершин w_2, w_3 и вершин, отвечающих трем четырехугольникам из $L_2 \cup L_3$, имеющим общее ребро $\{w_2, w_3\}$ с четырехугольником, отвечающим вершине w. Так как $w_1, w_2 \notin \Delta$, то $\Delta(w)$ содержит максимальную 3-клику. Противоречие с тем, что любая максимальная клика в графах типа Σ или типа T содержит точно 2 или 4 вершины. □

Завершим доказательство теоремы. Через Σ обозначим множество всех вершин d из $\Gamma_3(a)$ таких, что $\Delta = [d] \cap \Gamma_2(a)$ является треугольным графом, изоморфным $T(6)$. Зафиксируем вершину d из Σ. По лемме 2.8 подграф $K = \{d\} \cup K_5(\Delta)$ является 7-кликой из Σ. Выберем вершину $z \in K - \{d\}$. Тогда $[d] \cap [z]$ является (5×5)-решеткой, содержащей 5-клику L из Δ и 5-клику $K' = K - \{d, z\}$, не пересекающую Δ. Каждая вершина из $\Delta - L$ смежна с двумя вершинами из L и с двумя вершинами из $K_5(\Delta)$, поэтому каждая вершина из $\Delta - L$ отвечает четырехугольнику решетки $[d] \cap [z]$, пересекающему K' и L по двум вершинам. Теперь вершины из $[d] \cap [z] - (K' \cup L)$ принадлежат $K_1(\Delta)$ и попадают в Σ. Вершины, отвечающие четырехугольникам решетки $[d] \cap [z]$, не пересекающим L и пересекающим K', принадлежат $K_1(\Delta)$ и попадают в Σ. Наконец, вершины, отвечающие четырехугольникам решетки $[d] \cap [z]$, не пересекающим K', принадлежат $K_3(\Delta)$ и не попадают в Σ.

Пусть $y \in K_1(\Delta) - z^{\perp}$. Тогда y отвечает четырехугольнику решетки $[d] \cap [z]$, содержащему ребро $\{u_1, u_2\}$ из K' и ребро $\{w_1, w_2\}$ (u_i смежна с w_i). Далее, подграф $\Sigma(d) \cap [y]$ содержит: вершины u_1, u_2, w_1, w_2; 6 вершин, отвечающих четырехугольникам, взятым в (2×5)-подрешетке из $[d] \cap [z]$ и содержащим ребро $\{u_1, w_1\}$ или $\{u_2, w_2\}$; пару вершин, отвечающих четырехугольникам, содержащим u_1, u_2 и не пересекающим $L \cup \{w_1, w_2\}$. Итак, подграф $\Sigma(d) \cap [y]$ содержит две вершины u_1, u_2 степени 7, восемь вершин степени 5 и две вершины степени 3. Повторив рассуждения для y в роли d, заключаем, что 7-клика $K_y = \{y\} \cup K_5([y] \cap \Gamma_2(a))$ пересекает K по крайней мере по двум вершинам. Противоречие с леммой 2.8. Теорема доказана. □

Поступила 8.11.2006

СПИСОК ЛИТЕРАТУРЫ

1. **Makhnev A.A.** On the graphs with μ-subgraphs isomorphic to $K_{u\times 2}$ // Proc. Steklov Inst. Math. Suppl. 2. 2001. P. 169–178.
2. **Кабанов В.В., Махнев А.А., Падучих Д.В.** Локальное строение графов без 3-корон с реберно регулярными μ-подграфами // Алгебра и ее приложения: Тез. докл. междунар. конф. Красноярск: изд-во Красноярск. гос. ун-та, 2002. С. 55–56.
3. **Blokhuis A., Brouwer A.E.** On locally 4-by-4 grid graphs // J. Graph Theory. 1989. V. 13, no. 2. P. 229–244.

Том 13 № 1 2007

УДК 517.977

СВОЙСТВО D_π КОНЕЧНЫХ ГРУПП В СЛУЧАЕ $2 \notin \pi$ [1]

Д. О. Ревин

В работе завершено описание конечных простых групп со свойством D_π для любого множества π нечетных простых чисел. Поскольку ранее было доказано, что конечная группа обладает свойством D_π тогда и только тогда, когда каждый ее композиционный фактор обладает этим свойством, результаты работы означают исчерпывающую характеризацию свойства D_π для всех конечных групп с известными композиционными факторами в случае, когда $2 \notin \pi$.

Введение

Пусть G — конечная группа, π — некоторое множество простых чисел. Через π' обозначим множество всех простых чисел, не лежащих в π, через $\pi(n)$ — множество простых делителей натурального числа n, а через $\pi(G)$ — множество $\pi(|G|)$. Группа с условием $\pi(G) \subseteq \pi$ называется π-группой. Подгруппа H группы G называется *холловой π-подгруппой*, если $\pi(H) \subseteq \pi$ и $\pi(|G : H|) \subseteq \pi'$. В соответствии с [1] будем говорить, что группа G *обладает свойством* E_π, если в G имеется холлова π-подгруппа. Если при этом любые две холловы π-подгруппы сопряжены, то будем говорить, что группа G *обладает свойством* C_π. Если к тому же любая π-подгруппа группы G содержится в некоторой холловой π-подгруппе, то будем говорить, что G *обладает свойством* D_π. Группу со свойством E_π (C_π, D_π) будем называть также E_π-(соответственно, C_π-, D_π-) *группой.*

Используя классификацию конечных простых групп, Ф. Гросс [2,3] доказал, что для любого множества π нечетных простых чисел свойства E_π и C_π эквивалентны. Простым следствием этого утверждения является тот факт, что если $2 \notin \pi$, то любая конечная группа обладает свойством C_π тогда и только тогда, когда каждый ее композиционный фактор является E_π группой. В [2,4,5] получено описание холловых подгрупп нечетного порядка во всех конечных простых группах, и тем самым для любого множества π нечетных простых чисел и любой конечной группы с известными композиционными факторами можно сказать, обладает она свойствами E_π и C_π или нет. В [5] для любого множества простых чисел π, не содержащего 2, с помощью классификации конечных простых групп доказано, что конечная группа обладает свойством D_π тогда и только тогда, когда каждый ее композиционный фактор является D_π-группой. Таким образом, если $2 \notin \pi$, для получения исчерпывающей характеризации свойства D_π в классе всех конечных групп достаточно описать неабелевы простые группы с этим свойством.

Далее всюду предполагается, что π не содержит 2. Из [1,6] следует, что знакопеременная группа A_n обладает свойством D_π тогда и только тогда, когда $|\pi \cap \pi(n!)| \leqslant 1$. Спорадические группы со свойством D_π описаны в [2]. Простые группы лиева типа со свойством D_π при условии, что характеристика основного поля лежит в π, описаны в [2,7].

Цель настоящей статьи — описать простые D_π-группы лиева типа над полем характеристики p при условии, что $2, p \notin \pi$. Это описание приведено ниже в теоремах 1–3. Несколько слов

[1]Работа выполнена при поддержке РФФИ (проект 05-01-00797), Совета по грантам Президента РФ для поддержки молодых ученых и ведущих научных школ (проект МК-1730.2005.1) и СО РАН (грант № 29 для молодых ученых и интеграционный проект 2006.1.2).

об используемых в формулировках теорем обозначениях. Если r — нечетное простое число и q — целое число, не делящееся на r, то через $e(q,r)$ обозначено наименьшее натуральное число n такое, что $q^n \equiv 1 \pmod r$.

Теорема 1. *Пусть G — конечная группа лиева типа над полем $\mathrm{GF}(q)$ характеристики p, отличная от групп Судзуки и Ри; π — множество простых чисел такое, что $2, p \notin \pi$; $r = \min \pi \cap \pi(G)$, $\tau = (\pi \cap \pi(G)) \setminus \{r\} \neq \varnothing$. Допустим, что существует $t \in \tau$, для которого $e(q,r) \neq e(q,t)$, и положим $a = e(q,r)$, $b = e(q,t)$. Тогда группа G обладает свойством D_π, если и только если выполнено одно из следующих условий:*

(1) $G = A_{n-1}(q)$, $a = r-1$, $b = r$, $(q^{r-1}-1)_r = r$, $\left[\dfrac{n}{r-1}\right] = \left[\dfrac{n}{r}\right]$ *и для любого* $s \in \tau$ *справедливы соотношения* $e(q,s) = b$, $n < bs$;

(2) $G = A_{n-1}(q)$, $a = r-1$, $b = r$, $(q^{r-1}-1)_r = r$, $\left[\dfrac{n}{r-1}\right] = \left[\dfrac{n}{r}\right] + 1$, $n \equiv -1 \pmod r$ *и для любого* $s \in \tau$ *справедливы соотношения* $e(q,s) = b$, $n < bs$;

(3) $G = {}^2A_{n-1}(q)$, $r \equiv 1 \pmod 4$, $a = r-1$, $b = 2r$, $(q^n-1)_r = r$, $\left[\dfrac{n}{r-1}\right] = \left[\dfrac{n}{r}\right]$ *и для любого* $s \in \tau$ *выполнено равенство* $e(q,s) = b$;

(4) $G = {}^2A_{n-1}(q)$, $r \equiv 3 \pmod 4$, $a = \dfrac{r-1}{2}$, $b = 2r$, $(q^n-1)_r = r$, $\left[\dfrac{n}{r-1}\right] = \left[\dfrac{n}{r}\right]$ *и для любого* $s \in \tau$ *выполнено равенство* $e(q,s) = b$;

(5) $G = {}^2A_{n-1}(q)$, $r \equiv 1 \pmod 4$, $a = r-1$, $b = 2r$, $(q^n-1)_r = r$, $\left[\dfrac{n}{r-1}\right] = \left[\dfrac{n}{r}\right] + 1$, $n \equiv -1 \pmod r$ *и для любого* $s \in \tau$ *выполнено равенство* $e(q,s) = b$;

(6) $G = {}^2A_{n-1}(q)$, $r \equiv 3 \pmod 4$, $a = \dfrac{r-1}{2}$, $b = 2r$, $(q^n-1)_r = r$, $\left[\dfrac{n}{r-1}\right] = \left[\dfrac{n}{r}\right] + 1$, $n \equiv -1 \pmod r$ *и для любого* $s \in \tau$ *выполнено равенство* $e(q,s) = b$;

(7) $G = {}^2D_n(q)$, $a \equiv 1 \pmod 2$, $n = b = 2a$ *и для любого* $s \in \tau$ *либо* $e(q,s) = a$, *либо* $e(q,s) = b$;

(8) $G = {}^2D_n(q)$, $b \equiv 1 \pmod 2$, $n = a = 2b$ *и для любого* $s \in \tau$ *либо* $e(q,s) = a$, *либо* $e(q,s) = b$.

При этом холлова π-подгруппа группы G является абелевой.

Теорема 2. *Пусть G — группа лиева типа над полем $GF(q)$ характеристики p, отличная от групп Судзуки и Ри; π — множество простых чисел такое, что $2, p \notin \pi$; $r = \min \pi \cap \pi(G)$, $\tau = (\pi \cap \pi(G)) \setminus \{r\} \neq \varnothing$. Допустим, что для всех $t \in \tau$ имеет место равенство $e(q,r) = e(q,t)$, и положим $c = e(q,r)$. Тогда группа G обладает свойством D_π, если и только если выполнено одно из следующих условий:*

(1) $G = A_{n-1}(q)$ *и для любого* $s \in \tau$ *справедливо* $n < cs$;

(2) $G = {}^2A_{n-1}(q)$, $c \equiv 0 \pmod 4$ *и для любого* $s \in \tau$ *справедливо* $n < cs$;

(3) $G = {}^2A_{n-1}(q)$, $c \equiv 2 \pmod 4$ *и для любого* $s \in \tau$ *справедливо* $2n < cs$;

(4) $G = {}^2A_{n-1}(q)$, $c \equiv 1 \pmod 2$ *и для любого* $s \in \tau$ *справедливо* $n < 2cs$;

(5) G *— одна из групп* $B_n(q)$, $C_n(q)$ *или* ${}^2D_n(q)$, c *четно и для любого* $s \in \tau$ *справедливо* $2n < cs$;

(6) G *— одна из групп* $B_n(q)$, $C_n(q)$ *или* $D_n(q)$, c *нечетно и* $n < cs$ *для любого* $s \in \tau$;

(7) $G = D_n(q)$, *c четно и* $2n \leqslant cs$ *для любого* $s \in \tau$;

(8) $G = {}^2D_n(q)$, *c нечетно и* $n \leqslant cs$ *для любого* $s \in \tau$;

(9) $G = {}^3D_4(q)$;

(10) $G = E_6(q)$ *и если* $r = 3$ *и* $c = 1$, *то* $5, 13 \notin \tau$;

(11) $G = {}^2E_6(q)$ *и если* $r = 3$ *и* $c = 2$, *то* $5, 13 \notin \tau$;

(12) $G = E_7(q)$ *и если* $r = 3$ *и* $c \in \{1, 2\}$, *то* $5, 7, 13 \notin \tau$, *а если* $r = 5$ *и* $c \in \{1, 2\}$, *то* $7 \notin \tau$;

(13) $G = E_8(q)$ *и если* $r = 3$ *и* $c \in \{1, 2\}$, *то* $5, 7, 13 \notin \tau$, *а если* $r = 5$ *и* $c \in \{1, 2\}$, *то* $7, 31 \notin \tau$;

(14) $G = G_2(q)$;

(15) $G = F_4(q)$ *и если* $r = 3$ *и* $c = 1$, *то* $13 \notin \tau$.

Теорема 3. *Пусть G — одна из групп ${}^2B_2(2^{2m+1})$, ${}^2G_2(3^{2m+1})$, ${}^2F_4(2^{2m+1})$. Пусть π — множество простых чисел такое, что $2 \notin \pi$, а если $G = {}^2G_2(3^{2m+1})$, то и $3 \notin \pi$. Группа G обладает свойством D_π тогда и только тогда, когда выполнено одно из следующих условий*:

(1) $G = {}^2B_2(2^{2m+1})$, $\pi \cap \pi(G)$ *содержится в одном из множеств* $\pi(2^{2m+1} - 1)$, $\pi(2^{2m+1} \pm 2^{m+1} + 1)$;

(2) $G = {}^2G_2(3^{2m+1})$, $\pi \cap \pi(G)$ *содержится в одном из множеств* $\pi(3^{2m+1} - 1)$, $\pi(3^{2m+1} \pm 3^{m+1} + 1)$;

(1) $G = {}^2F_4(2^{2m+1})$, $\pi \cap \pi(G)$ *содержится в одном из множеств* $\pi(2^{2(2m+1)} \pm 1)$, $\pi(2^{2m+1} \pm 2^{m+1} + 1)$, $\pi(2^{2(2m+1)} \pm 2^{3m+2} \mp 2^{m+1} - 1)$, $\pi(2^{2(2m+1)} \pm 2^{3m+2} + 2^{2m+1} \pm 2^{m+1} - 1)$.

Таким образом, для любого множества π нечетных простых чисел все конечные простые группы со свойством D_π описаны, и тем самым получена исчерпывающая характеризация этого свойства в классе всех конечных групп.

Автор выражает глубокую признательность Е.П. Вдовину, многие идеи которого легли в основу данной работы.

1. Предварительные сведения и результаты

Используемые в работе обозначения и терминология стандартны. Под известными простыми группами понимаются группы, которые упоминаются в классификационной теореме [13]. Если G — конечная группа, H — ее подгруппа, $x \in G$, p — простое число и π — некоторое множество простых чисел, то через $G^\#$, $Z(G)$, $N_G(H)$, $C_G(H)$, $C_G(x)$, $O^{p'}(G)$ и $O_\pi(G)$ обозначаются множество неединичных элементов группы G, центр группы G, нормализатор в G подгруппы H, централизатор в G подгруппы H, централизатор в G элемента x, подгруппа, порожденная всеми p-элементами группы G, и наибольшая нормальная π-подгруппа группы G соответственно.

Всюду в статье через p и r обозначаются некоторые простые числа, а через q — некоторая натуральная степень числа p. При этом для любого натурального числа e *примитивными простыми делителями числа* $q^e - 1$ называются простые числа, которые делят $q^e - 1$, но не делят ни одно из чисел $q^d - 1$, где $d < e$. *Примитивными простыми делителями числа* $q^e + 1$ называются примитивные простые делители числа $q^{2e} - 1$. Если не оговорено специально, через η обозначается число 1 или -1.

Необходимые сведения о системах корней, группах лиева типа и линейных алгебраических группах могут быть найдены в [8–10]. Если Φ — корневая система, то через $W(\Phi)$ обозначается ее группа Вейля. В обозначениях скрученных групп лиева типа, отличных от групп Судзуки и Ри, мы будем следовать [8], считая, что $\mathrm{GF}(q)$ — подполе неподвижных точек относительно действия соответствующего полевого автоморфизма основного поля. В остальных случаях поле определения совпадает с основным. Группы ${}^2A_n(q)$, ${}^2D_n(q)$ и ${}^2E_6(q)$ будут иногда обозначаться соответственно через $A_n^-(q)$, $D_n^-(q)$ и $E_6^-(q)$, а группы $A_n(q)$, $D_n(q)$ и $E_6(q)$ — соответственно через $A_n^+(q)$, $D_n^+(q)$ и $E_6^+(q)$. Будем также вместо знака "$\pm$" в этих случаях иногда писать "±1".

Если $\overline{G}$ — связная простая линейная алгебраическая группа, то для любого эндоморфизма σ этой группы через $\overline{G}_\sigma$ будем обозначать множество элементов $\overline{G}$, неподвижных относительно σ. Хорошо известно, что любая группа лиева типа G может быть вложена в подходящую простую линейную алгебраическую группу $\overline{G}$ как подгруппа, совпадающая с $O^{p'}(\overline{G}_\sigma)$ для некоторого сюръективного эндоморфизма σ алгебраической группы $\overline{G}$, причем если G универсальна, а $\overline{G}$ односвязна, то $G = \overline{G}_\sigma$.

Необходимые сведения о классических группах и о классах Ашбахера можно найти в [23]. Группу $\mathrm{GU}_n(q)$ будем обозначать символом $\mathrm{GL}^-(q)$, а группу $\mathrm{GL}(q)$ — символом $\mathrm{GL}^+(q)$. Будем также вместо знака "$\pm$" в этих обозначениях иногда писать "±1". Если V — векторное пространство с квадратичной формой, то символом $\eta(V)$ будем обозначать знак этой формы. Если группа G действует на векторном пространстве V линейными преобразованиями, то для любого $g \in G$ обозначим через $[V,g]$ множество линейных комбинаций векторов вида $vg - v$, $v \in V$, а через $[V,G]$ — подпространство $\sum\limits_{g\in G}[V,g]$.

В следующей лемме собраны известные утверждения о свойствах E_π, C_π и D_π.

Лемма 1. *Пусть G — конечная группа, A — ее нормальная подгруппа. Тогда справедливы следующие утверждения:*

(1) *Если H — холлова π-подгруппа группы G, то $H \cap A$ является холловой π-подгруппой в A, а факторгруппа HA/A является холловой π-подгруппой в G/A.*

(2) *Если G — E_π- или D_π-группа, то факторгруппа G/A обладает свойством E_π или D_π соответственно.*

(4) *Если A и G/A обладают свойством C_π, то группа G обладает свойством C_π.*

(5) *Если группа A разрешима, то факторгруппа G/A обладает свойством D_π тогда и только тогда, когда группа G обладает свойством D_π. В частности, группа G обладает свойством D_π тогда и только тогда, когда любое центральное расширение группы G обладает свойством D_π.*

(6) *Если группа G является центральным произведением групп G_i, $i = 1, 2, ..., n$, то группа G обладает свойством E_π, C_π или D_π тогда и только тогда, когда каждая из групп G_i, $i = 1, 2, ..., n$, обладает этим свойством.*

(7) *Если G — E_π-группа, и ее холлова π-подгруппа нильпотентна, то G обладает свойством D_π* [25].

(8) *Если A — E_π-группа и ее холлова π-подгруппа нильпотентна, а G/A обладает свойством D_π, то G обладает свойством D_π* [1, теорема D5], [27, теорема 1].

Лемма 2 ([5], теорема 2). *Пусть G — конечная группа, A — ее нормальная подгруппа, все композиционные факторы которой являются известными простыми группами. Тогда если A и G/A обладают свойством D_π для некоторого множества π нечетных простых чисел, то G обладает свойством D_π.*

Лемма 3. *Пусть G — группа из списка $W(E_6)$, $W(E_7)$, $W(E_8)$, $W(F_4)$, $W(G_2)$, $\mathrm{SL}_2(5)$, $\mathrm{SL}_3(2)$, $\mathrm{SL}_3(3)$, $\mathrm{SL}_3(5)$, $\mathrm{SL}_4(2)$, S_8. Пусть $\pi \subseteq \pi(G) \setminus \{2\}$, $|\pi| \geqslant 2$, $r = \min \pi$, $\tau = \pi \setminus \{r\}$. Тогда для любой π-подгруппы H группы G либо H является r-группой, либо $O_\tau(H) \neq 1$.*

Доказательство. Поскольку $W(F_4)$ и $W(G_4)$ являются $\{2,3\}$-группами, эти случаи можно не рассматривать. Пусть G — одна из оставшихся групп. Согласно информации из [21] о группах $\mathrm{PSp}_4(3) \simeq \mathrm{U}_4(2)$, $\mathrm{PSp}_6(2)$ и $\mathrm{P}\Omega_8^+(2)$, имеют место изоморфизмы $W(E_6) \simeq \mathrm{Sp}_4(3).2$, $W(E_7) \simeq 2 \times \mathrm{PSp}_6(2)$ и $W(E_8) \simeq 2.\mathrm{P}\Omega_8^+(2).2$. Таким образом, во всех рассматриваемых случаях в группе G имеется нормальный ряд $G \geqslant G_1 \geqslant G_2 \geqslant 1$ такой, что G/G_1 и G_2 — 2-группы (возможно, тривиальные), а $L = G_1/G_2$ — простая группа из списка $\mathrm{PSp}_4(3) \simeq \mathrm{U}_4(2)$, $\mathrm{PSp}_6(2)$, $\mathrm{P}\Omega_8^+(2)$, $\mathrm{L}_2(4) \simeq A_5$, $\mathrm{L}_3(2) \simeq \mathrm{L}_2(7)$, $\mathrm{SL}_3(3)$, $\mathrm{SL}_3(5)$, $\mathrm{SL}_4(2) \simeq A_8 \simeq \mathrm{P}\Omega_6^+(2)$. Все эти группы являются группами лиева типа. Можно считать, что H является подгруппой группы L.

Будем считать, что $O_\tau(H) = 1$. Группа H разрешима согласно [22], поэтому $R = O_r(H) \neq 1$. Если $r > 3$ и r отлично от характеристики, то r не делит порядок группы Вейля соответствующей группы, и силовская r-подгруппа группы L содержится в некотором торе. Если $\overline{L}$ — такая простая алгебраическая группа, что $L = O^{p'}(\overline{L}_\sigma)$ (здесь p — характеристика группы L) для подходящего эндоморфизма σ, то группа $N_{\overline{L}}(R)/C_{\overline{L}}(R)$ изоморфна секции группы Вейля, и, следовательно, ее порядок не делится на простые числа, бóльшие r. Отсюда легко вытекает, что H является r-группой. Если r является характеристикой, то H содержится в некоторой собственной параболической подгруппе по теореме Бореля-Титса [11], и нетрудно показать, что порядок фактора Леви этой параболической подгруппы не делится на простые числа, бóльшие r. Пусть теперь $r = 3 \neq p$. Допустим, $L \neq \mathrm{P}\Omega_8^+(2)$. Тогда порядок силовской 3-подгруппы S группы L не превосходит 3^4, причем равенство будет иметь место только для группы $\mathrm{PSp}_6(2)$, в которой силовская 3-подгруппа неабелева. Из разрешимости H следует, что $C_H(R) \leqslant R$. Секционный ранг группы R не превосходит 3, поэтому $N_L(R)/C_L(R) \leqslant \mathrm{GL}_3(3)$. Таким образом, единственное простое число, отличное от 3, на которое может делиться $|H|$, — это 13. Но легко проверить, что $|L|$ в рассматриваемых случаях не делится на 13. Остался случай, когда $L = \mathrm{P}\Omega_8^+(2)$ и $r = 3$. В силу разрешимости H, эта подгруппа должна содержаться в элементе одного из классов Ашбахера $\mathcal{C}_1$–$\mathcal{C}_8$ [23, теорема 1.2.1]. Анализ этих случаев не составляет труда и сводится к уже рассмотренным. □

2. Радикальные r-подгруппы и r-суперлокалы симметрических и классических групп

Пусть r — простое число и G — конечная группа. Радикальной r-подгруппой группы G будем называть r-подгруппу R (возможно, тривиальную) такую, что $R = O_r(N_G(R))$, а нормализатор такой подгруппы будем называть r-суперлокалом.

Следуя [15,16], зафиксируем обозначения. Пусть r — простое число. Для любого натурального числа c пусть A_c — элементарная абелева r-группа порядка r^c. Эта группа однозначно, с точностью до сопряженности, вкладывается как транзитивная подгруппа в симметрическую группу S_{r^c}. При этом $C_{S_{r^c}}(A_c) = A_c$ и $N_{S_{r^c}}(A_c)/A_c \simeq \mathrm{GL}_c(r)$ [14, 15]. Для любой конечной последовательности $\mathfrak{c} = (c_1, c_2, \ldots, c_t)$ натуральных чисел обозначим через $A_\mathfrak{c}$ подстановочное сплетение $A_{c_1} \wr A_{c_2} \wr \cdots \wr A_{c_t}$, вложенное естественным образом как транзитивная подгруппа в группу S_{r^d}, где $d = c_1 + c_2 + \cdots + c_t$. Это вложение однозначно с точностью до сопряженности.

Лемма 4. *Во введенных обозначениях $N_{S_{r^d}}(A_\mathfrak{c})/A_\mathfrak{c} \simeq \mathrm{GL}_{c_1}(r) \times \mathrm{GL}_{c_2}(r) \times \cdots \times \mathrm{GL}_{c_t}(r)$.*

Доказательство. См. [14, лемма 12] и [15, (2.1)]. □

Подгруппу $A_\mathfrak{c}$ будем называть *базисной подгруппой* группы S_{r^d}.

Лемма 5. *Пусть Ω — конечное множество и R — радикальная r-подгруппа группы $S(\Omega)$. Тогда существуют соответствующие друг другу разложения*

$$\Omega = \Omega_0 \cup \Omega_1 \cup \cdots \cup \Omega_s,\ R = R_0 \times R_1 \times \cdots \times R_s,$$

где $\Omega_i \cap \Omega_j = \varnothing$ при $i \neq j$, такие, что R_0 — тривиальная подгруппа группы $S(\Omega_0)$, а R_i — базисная подгруппа группы $S(\Omega_i)$ при $i \geqslant 1$.

Доказательство. См. [14, теоремы 1 и 2] и [15, (2A)]. □

Пусть множество Ω и подгруппа R группы $S(\Omega)$ выбраны, как в условии леммы 5 и $\Omega = \Omega_0 \cup \Omega_1 \cup \cdots \cup \Omega_s$, $R = R_0 \times R_1 \times \cdots \times R_s$ — разложения, о которых идет речь в этой лемме. Для любой конечной последовательности натуральных чисел $\mathfrak{c} = (c_1, c_2, \ldots, c_t)$ пусть $R(\mathfrak{c})$ — произведение тех R_i, для которых $R_i = A_\mathfrak{c}$, $\Omega(\mathfrak{c})$ — объединение соответствующих им Ω_i, а $u(\mathfrak{c})$ — их количество. Пусть также $S_\mathfrak{c} = S_{r^d}$, где $d = c_1 + c_2 + \cdots + c_t$.

Лемма 6. *Во введенных обозначениях*

$$N_{S(\Omega)}(R) = S(\Omega_0) \times \prod_\mathfrak{c} N_{S(\Omega(\mathfrak{c}))}(R(\mathfrak{c})),$$

$$N_{S(\Omega)}(R)/R = S(\Omega_0) \times \prod_\mathfrak{c} N_{S(\Omega(\mathfrak{c}))}(R(\mathfrak{c}))/R(\mathfrak{c}),$$

$$N_{S(\Omega(\mathfrak{c}))}(R(\mathfrak{c})) = N_{S_\mathfrak{c}}(A_\mathfrak{c}) \wr S_{u(\mathfrak{c})},$$

$$N_{S(\Omega(\mathfrak{c}))}(R(\mathfrak{c}))/R(\mathfrak{c}) = N_{S_\mathfrak{c}}(A_\mathfrak{c})/A_\mathfrak{c} \wr S_{u(\mathfrak{c})}.$$

Доказательство. См. [14, теоремы 1 и 2] и [15, (2B)] (в последней работе лемма доказана при некотором дополнительном предположении). □

Пусть теперь r — нечетное простое число, n — натуральное число, q — нетривиальная степень простого числа p, отличного от r. Пусть G — одна из групп $\mathrm{GL}_n^\eta(q)$, $\mathrm{Sp}_{2n}(q)$, $\mathrm{O}_{2n+1}(q)$, $\mathrm{O}_{2n}^\eta(q)$, причем в последних трех случаях q предполагается нечетным. Поскольку в ортогональном случае q нечетно, всегда можно считать, что группа G совпадает с группой $I(U)$ изометрий некоторого векторного пространства U с соответствующей билинейной или унитарной формой, которое мы будем называть естественным модулем для G. Пусть $e = e(\eta q, r)$, если $G = \mathrm{GL}_n^\eta(q)$, и $e = e(q^2, r)$ в остальных случаях. Пусть число a определяется равенством $(q^{2e} - 1)_r = r^a$. Пусть $\varepsilon \in \{\pm 1\}$, причем если $G = \mathrm{GL}_n^\eta(q)$, то $\varepsilon = \eta^e$, а в остальных случаях знак ε выбирается таким образом, чтобы r^a делило $q^e - \varepsilon$. Пусть γ — неотрицательное целое число и E_γ — экстраспециальная группа экспоненты r и порядка $r^{2\gamma+1}$ (если $\gamma = 0$, то E_γ — циклическая группа порядка r). Пусть α — неотрицательное целое число и Z_α — циклическая группа порядка $r^{a+\alpha}$. Пусть $R_{\alpha,\gamma}$ — центральное произведение групп E_γ и Z_α такое, что $Z(E_\gamma) = \Omega_1(Z_\alpha)$. Известно [15–17], что группа автоморфизмов группы $R_{\alpha,\gamma}$, оставляющих неподвижными элементы из $Z(E_\gamma)$, изоморфна $\mathrm{Sp}_{2\gamma}(r)$, и естественное полупрямое произведение $L_{\alpha,\gamma}$ групп $R_{\alpha,\gamma}$ и $\mathrm{Sp}_{2\gamma}(r)$ вкладывается в группу $\mathrm{GL}_{r^\gamma}^\varepsilon(q^{er^\alpha})$. В свою очередь [23, таблицы 3.5.C, 3.5.E и 3.5.F] группа $\mathrm{GL}_{r^\gamma}^\varepsilon(q^{er^\alpha})$, расширенная элементом порядка er^α, вкладывается в группу $\mathrm{GL}_{er^{\alpha+\gamma}}^\eta(q)$, а расширенная элементом порядка $2er^\alpha$ — в группу $I(V_{\alpha,\gamma})$, где $V_{\alpha,\gamma}$ — симплектическое или ортогональное пространство над полем $\mathrm{GF}(q)$ размерности $2er^{\alpha+\gamma}$, причем $\eta(V_{\alpha,\gamma}) = \varepsilon$, если $V_{\alpha,\gamma}$ — ортогональное пространство. Обозначим через b число er^α, если $G = \mathrm{GL}_n^\eta(q)$, и число $2er^\alpha$ в остальных случаях. Далее, каждую из групп $\mathrm{GL}_{er^{\alpha+\gamma}}^\eta(q)$ и $I(V_{\alpha,\gamma})$ посредством вложения

$$g \mapsto \begin{pmatrix} g & & \\ & \ddots & \\ & & g \end{pmatrix}$$

можно вложить в группу $G_{m,\alpha,\gamma}$, равную соответственно $\mathrm{GL}^{\eta}_{mer^{\alpha+\gamma}}(q)$ и $I(V_{m,\alpha,\gamma})$, где

$$V_{m,\alpha,\gamma} = \underbrace{V_{\alpha,\gamma} \perp \dots \perp V_{\alpha,\gamma}}_{m \text{ раз}},$$

причем в ортогональном случае $\eta(V_{m,\alpha,\gamma}) = \varepsilon^m$. Обозначим через $R_{m,\alpha,\gamma}$ и $L_{m,\alpha,\gamma}$ образы в $G_{m,\alpha,\gamma}$ групп $R_{\alpha,\gamma}$ и $L_{\alpha,\gamma}$ относительно этих вложений. Положим также $C_{m,\alpha,\gamma} = C_{G_{m,\alpha,\gamma}}(R_{m,\alpha,\gamma})$, $N_{m,\alpha,\gamma} = N_{G_{m,\alpha,\gamma}}(R_{m,\alpha,\gamma})$ и $N^0_{m,\alpha,\gamma} = \{g \in N_{m,\alpha,\gamma} | [g, Z(R_{m,\alpha,\gamma})] = 1\}$.

Лемма 7. *Во введенных обозначениях*

$$C_{m,\alpha,\gamma} \simeq \mathrm{GL}^{\varepsilon}_m(q^{er^\alpha}) \otimes I_\gamma,$$

где I_γ — единичная матрица размера r^γ, а через $\otimes$ обозначено кронекерово произведение матриц:

$N^0_{m,\alpha,\gamma}$ совпадает с центральным произведением групп $L_{m,\alpha,\gamma}C_{m,\alpha,\gamma}$;

факторгруппа $N_{m,\alpha,\gamma}/N^0_{m,\alpha,\gamma}$ является циклической группой порядка b.

Д о к а з а т е л ь с т в о. См. [15, 3C и п. 4] и [16, п. 2]. □

Далее, пусть $\mathfrak{c} = (c_1, c_2, \dots, c_l)$, где $c_1, c_2, \dots, c_l$ — натуральные числа. Пусть A_{c_i} — элементарная абелева группа порядка r^{c_i} для любого $i = 1, \dots, l$ и $A_{\mathfrak{c}}$ — подстановочное сплетение $A_{c_1} \wr A_{c_2} \wr \dots \wr A_{c_l}$. Пусть также $u = r^{c_1+c_2+\dots+c_l}$, $d = mer^{\alpha+\gamma}u$. Группу $A_{\mathfrak{c}}$ можно естественным образом отождествить с подгруппой из S_u. Кроме того, положим $G_{m,\alpha,\gamma,\mathfrak{c}} = \mathrm{GL}^{\eta}_d(q)$ в случае, когда $G = \mathrm{GL}^{\eta}_n(q)$, а в остальных случаях $G_{m,\alpha,\gamma,\mathfrak{c}} = I(V_{m,\alpha,\gamma,\mathfrak{c}})$, где

$$V_{m,\alpha,\gamma,\mathfrak{c}} = \underbrace{V_{m,\alpha,\gamma} \perp \dots \perp V_{m,\alpha,\gamma}}_{u \text{ раз}},$$

причем в ортогональном случае $\eta(V_{m,\alpha,\gamma,\mathfrak{c}}) = \varepsilon^m$. Согласно [15, п. 4] и [16, п. 2] группа $R_{m,\alpha,\gamma,\mathfrak{c}} = R_{m,\alpha,\gamma} \wr A_{\mathfrak{c}}$ естественным образом вкладывается в группу $G_{m,\alpha,\gamma,\mathfrak{c}}$, определяется в ней однозначно с точностью до сопряжения и называется ее *базисной подгруппой*.

Лемма 8. *Пусть числа q, n, r и группа G те же, что и ранее. Пусть во введенных обозначениях $H = G_{m,\alpha,\gamma,\mathfrak{c}}$ и $R = R_{m,\alpha,\gamma,\mathfrak{c}}$. Из определения группы R следует, что R является полупрямым произведением группы $R_1 \times \dots \times R_u$, где $u = r^{c_1+\dots+c_l}$ и каждая из групп R_i является группой $R_{m,\alpha,\gamma}$, и группы $A_{\mathfrak{c}}$. Пусть V — естественный модуль группы H и $V_i = [V, R_i]$ — подпространство, которое можно отождествить с естественным модулем группы R_i. Тогда справедливы следующие утверждения*:

(1) *$C_H(R) \simeq C_{m,\alpha,\gamma} \otimes I_{\mathfrak{c}}$, где $I_{\mathfrak{c}}$ — единичная матрица размера u.*

(2) *$N_H(R) = (N_{m,\alpha,\gamma}/R_{m,\alpha,\gamma}) \otimes N_{S_u}(A_{\mathfrak{c}})$, $N_H(R)/R \simeq (N_{m,\alpha,\gamma}/R_{m,\alpha,\gamma}) \times \mathrm{GL}_{c_1}(r) \times \dots \times \mathrm{GL}_{c_l}(r)$.*

(3) *Если $A(R)$ — пересечение всех максимальных абелевых подгрупп группы R, $\mathcal{E} = \{[V, g] | g \in A(R)^\#\}$ и W — минимальный по включению элемент $\mathcal{E}$, то W совпадает с одним из подпространств $V_1, \dots, V_u$, причем $\dim W = mer^{\alpha+\gamma}$ в случае, когда $G = \mathrm{GL}^{\eta}_n(q)$, и $\dim W = 2mer^{\alpha+\gamma}$ в остальных случаях.*

(4) *Группа R действует естественным образом на множестве $\{V_1, \dots, V_u\}$. При этом подгруппа $R_1 \times \dots \times R_u$ совпадает с ядром этого действия, а подгруппа $A_{\mathfrak{c}}$ действует как подгруппа из S_u.*

Д о к а з а т е л ь с т в о. См. [15, (1.4), (4.1) с доказательством] и [16, (2.1), (2.2), доказательство (2C), (2.4), (2.5) и доказательство (2E)]. □

Лемма 9. *Пусть числа q, n, r и группа G те же, что и ранее, и для подходящих m, α, γ, $\mathfrak{c}$, m', α', γ' и $\mathfrak{c}'$ подгруппа $R = R_{m,\alpha,\gamma,\mathfrak{c}} = R_{m',\alpha',\gamma',\mathfrak{c}'}$ является базисной в некоторой группе $H = G_{m,\alpha,\gamma,\mathfrak{c}} = G_{m',\alpha',\gamma',\mathfrak{c}'}$. Тогда $m = m'$, $\alpha = \alpha'$, $\gamma = \gamma'$ и $\mathfrak{c} = \mathfrak{c}'$.*

Доказательство. Из утверждения (1) леммы 8 и леммы 7 следует изоморфизм $C_H(R) \simeq \mathrm{GL}_m^\varepsilon(q^{er^\alpha})$. Числа m, α, γ и последовательность $\mathfrak{c}$ определяются однозначно: m и α по известным q, r, e, ε; число γ — в силу утверждения (3) леммы 8; последовательность $\mathfrak{c}$ — ввиду утверждения (4) леммы 8 и [14, лемма 12 (3)]. □

Лемма 10. *Пусть группа G та же, что и ранее, и V — естественный модуль для G, снабженный соответствующей формой. Пусть R — радикальная r-подгруппа группы G. Тогда существуют соответствующие друг другу разложения*

$$V = V_0 \perp V_1 \perp \dots \perp V_t, \quad R = R_0 \times R_1 \times \dots \times R_t$$

такие, что R_0 — тривиальная подгруппа $I(V_0)$ и R_i — базисная подгруппа группы $I(V_i)$ при $i \geqslant 1$.

Доказательство. См. [15, (4A)] и [16, (2B) и (2D)]. □

Пусть теперь в прежних обозначениях R — радикальная r-подгруппа группы G, V — естественный модуль для G и

$$V = V_0 \perp V_1 \perp \dots \perp V_t, \quad R = R_0 \times R_1 \times \dots \times R_t \text{ —}$$

разложения, о которых идет речь в лемме 10. Пусть $R(m,\alpha,\gamma,\mathfrak{c})$ — произведение тех из подгрупп R_i, для которых $R_i = R_{m,\alpha,\gamma,\mathfrak{c}}$, $V(m,\alpha,\gamma,\mathfrak{c})$ — сумма соответствующих этим R_i подпространств V_i, а $u(m,\alpha,\gamma,\mathfrak{c})$ — число таких R_i. Пусть также $G(m,\alpha,\gamma,\mathfrak{c}) = I(V(m,\alpha,\gamma,\mathfrak{c}))$ — соответствующая группа изометрий, отождествляемая с соответствующей подгруппой в G.

Следующая лемма описывает строение суперлокалов в группе G.

Лемма 11. *Во введенных обозначениях*

$$N_G(R) = I(V_0) \times \prod_{m,\alpha,\gamma,\mathfrak{c}} N_{G(m,\alpha,\gamma,\mathfrak{c})}(R(m,\alpha,\gamma,\mathfrak{c})),$$

$$N_G(R)/R = I(V_0) \times \prod_{m,\alpha,\gamma,\mathfrak{c}} N_{G(m,\alpha,\gamma,\mathfrak{c})}(R(m,\alpha,\gamma,\mathfrak{c}))/R(m,\alpha,\gamma,\mathfrak{c}),$$

$$N_{G(m,\alpha,\gamma,\mathfrak{c})}(R(m,\alpha,\gamma,\mathfrak{c})) = N_{G_{m,\alpha,\gamma,\mathfrak{c}}}(R_{m,\alpha,\gamma,\mathfrak{c}}) \wr S_{u(m,\alpha,\gamma,\mathfrak{c})},$$

$$N_{G(m,\alpha,\gamma,\mathfrak{c})}(R(m,\alpha,\gamma,\mathfrak{c}))/R(m,\alpha,\gamma,\mathfrak{c}) = (N_{G_{m,\alpha,\gamma,\mathfrak{c}}}(R_{m,\alpha,\gamma,\mathfrak{c}})/R_{m,\alpha,\gamma,\mathfrak{c}}) \wr S_{u(m,\alpha,\gamma,\mathfrak{c})}.$$

Доказательство. Эта лемма доказана в [15, (4B)] и [16, (2C) и (2E)] в предположении, что существует неприводимый комплексный характер φ группы $N_G(R)$ такой, что $R \leqslant \ker\varphi$, и φ, рассматриваемый как характер группы $N_G(R)/R$, принадлежит r-блоку дефекта 0. Существование такого характера используется только для того, чтобы показать, что если некоторый сомножитель $R_i = R_{m,\alpha,\gamma,\mathfrak{c}}$ в разложении группы R сопряжен с сомножителем $R_{i'} = R_{m',\alpha',\gamma',\mathfrak{c}'}$, то $m = m'$, $\alpha = \alpha'$, $\gamma = \gamma'$ и $\mathfrak{c} = \mathfrak{c}'$. Однако в силу леммы 9 эти равенства имеют место и без предположения о существовании такого характера φ. □

В предыдущих обозначениях для любого $i = 0, 1, \dots, t$ положим $G_i = I(V_i)$, причем G_i отождествляется с соответствующей подгруппой из G, если считать, что G_i тождественно действует на всех V_j при $i \neq j$. Пусть $C_i = C_{G_i}(R_i)$. Таким образом, в силу лемм 7 и 8, если $i = 0$, то $C_i = G_i$, и если $i \geqslant 1$ и $R_i = R_{m,\alpha,\gamma,\mathfrak{c}}$, то $C_i \simeq \mathrm{GL}_m^\varepsilon(q^{er^\alpha})$. В частности, $|C_i|$ всегда делится на $q^e - \varepsilon$.

Лемма 12. *Пусть при введенных обозначениях R — нецентральная радикальная подгруппа группы G. Тогда $C_G(R) = C_0 \times C_1 \times \dots \times C_t$. Кроме того, имеет место одно из следующих утверждений*:

(1) $|C_G(R)/Z(G)|$ *делится на все нечетные примитивные простые делители числа* $q^e - \varepsilon$.

(2) $G = \mathrm{GL}_n^\eta(q)$, $t = 1$, $e \in \{1, 2\}$, $G_0 = 1$, $G = G_1$, $R = R_1$ *и для некоторых* α, γ *и* $\mathfrak{c}$ *имеет место равенство* $R_1 = R_{1,\alpha,\gamma,\mathfrak{c}}$. *При этом*

(2.1) $C_G(R)$ — *циклическая группа порядка* $q^{er^\alpha} - \varepsilon$;

(2.2) $N_G(R)/N_G^0(R)$ — *циклическая группа порядка* $b = er^\alpha$, *где через* $N_G^0(R)$ *обозначена группа* $C_{N_G(R)}(Z(R))$;

(2.3) $N_G^0(R)/(RC_G(R)) \simeq \mathrm{Sp}_{2\gamma}(r) \times \mathrm{GL}_{c_1}(r) \times \dots \times \mathrm{GL}_{c_l}(r)$;

(2.4) *число* n, *с помощью которого определяется степень группы* G, *равно числу* $r^{\alpha+\gamma+c_1+\dots+c_l}$;

(2.5) *любой отличный от* r *примитивный нечетный простой делитель числа* $q^e - \varepsilon$ *не делит* $|C_G(R)/Z(G)|$;

(2.6) *если* $e = 1$, *то* $\varepsilon = \eta$, *а если* $e = 2$, *то* $\eta = -1$ *и* $\varepsilon = 1$.

Д о к а з а т е л ь с т в о. Утверждение о строении группы $C_G(R)$ следует из леммы 11.

Если группа G является ортогональной или симплектической, то $Z(G)$ — 2-группа, и поэтому имеет место утверждение (1). Пусть $G = \mathrm{GL}_n^\eta(q)$ и для краткости $C = C_G(R)$. При этом $|Z(G)| = q - \eta$. Ясно, что $t \geqslant 1$. Можно считать, что $|C/Z(G)|$ не делится на $q^e - \varepsilon$. Поскольку $Z(G)$ — циклическая группа, из сделанного выше замечания о порядке групп C_i при $i \geqslant 1$ следует, что $t = 1$. Если $G_0 \neq 1$, то $|G_0|$ делится на $q - \eta = |Z(G)|$ и тогда $|C/Z(G)|$ делится на $|C_1|$. Поэтому $G_0 = 1$, $G = G_1$, $R = R_1$ и $R_1 = R_{m,\alpha,\gamma,\mathfrak{c}}$ для некоторых m, α, γ и $\mathfrak{c}$. Если $m > 1$, то $|C/Z(G)|$ делится на $q^e - \varepsilon$. Поэтому $m = 1$. Таким образом, C — циклическая подгруппа порядка $q^{er^\alpha} - \varepsilon$. Утверждения о строении групп $N_G(R)/N_G^0(R)$ и $N_G^0(R)/(RC_G(R))$, а также выражение для числа n вытекают из лемм 7 и 8 и определения группы $R_{m,\alpha,\gamma,\mathfrak{c}}$. Осталось доказать: если число $(q^{er^\alpha} - \varepsilon)/(q - \eta)$ не делится на некоторый примитивный нечетный простой делитель числа $q^e - \varepsilon$, то (a) оно не делится ни на один из таких делителей, кроме, может быть, числа r; (b) $e = 1$ и $\varepsilon = \eta$ или $e = 2$ и $\eta = -1$, $\varepsilon = 1$.

Напомним, что в рассматриваемом случае $\varepsilon = \eta^e$. Имеем

$$\frac{q^{er^\alpha} - \varepsilon}{q - \eta} = \frac{q^{er^\alpha} - \varepsilon}{q^e - \varepsilon} \cdot \frac{q^e - \varepsilon}{q - \eta},$$

$$\frac{q^{er^\alpha} - \varepsilon}{q^e - \varepsilon} = q^{e(r^\alpha - 1)} + \varepsilon q^{e(r^\alpha - 2)} + \varepsilon^2 q^{e(r^\alpha - 3)} + \dots + \varepsilon^{r^\alpha - 1}.$$

Поэтому если t — простой делитель числа $q^e - \varepsilon$, то $q^e \equiv \varepsilon \pmod t$ и

$$\frac{q^{er^\alpha} - \varepsilon}{q^e - \varepsilon} \equiv r^\alpha \varepsilon^{r^\alpha - 1} \pmod t.$$

Следовательно, любой отличный от r примитивный нечетный простой делитель числа $q^e - \varepsilon$, делящий $|C/Z(G)|$, должен делить число

$$x = \frac{q^e - \varepsilon}{q - \eta} = \frac{q^e - \eta^e}{q - \eta}.$$

Пусть x не делится на некоторый примитивный нечетный простой делитель числа $q^e - \varepsilon$. Тогда либо $e = 1$, $\varepsilon = \eta$ и, следовательно, $x = 1$, либо $e = 2$, $\eta = -1$, $\varepsilon = 1$ и, следовательно, $x = q - 1$ и $q^e - \varepsilon = q^2 - 1$. В любом случае x не делится на примитивные простые делители числа $q^e - \varepsilon$. Лемма доказана. $\square$

3. Доказательство основных результатов

Теорема 1 доказана в [5, доказательство теоремы 4]. Доказательства теорем 2 и 3 начнем с того, что введем некоторые обозначения и эквивалентным образом переформулируем теоремы.

Пусть L — конечная группа лиева типа над полем $\mathrm{GF}(q)$ характеристики p или полная классическая группа (т. е. одна из групп $\mathrm{GL}_n^\eta(q)$,$\mathrm{O}_{2n+1}(q)$, $\mathrm{Sp}_{2n}(q)$, $\mathrm{O}_{2n}^\eta(q)$), π — некоторое множество нечетных простых чисел. Будем говорить, что пара (L,π) *удовлетворяет условию* $(*)$, если $p \notin \pi$, группа L обладает свойством E_π, $|\pi \cap \pi(L)| \geqslant 2$ и, если L отлична от групп Судзуки и Ри, то для любых двух элементов $s,t \in \pi \cap \pi(L)$ имеет место равенство $e(q,s) = e(q,t)$.

Лемма 13. *Пусть $L = O^{p'}(\overline{L}_\sigma)$ — конечная группа лиева типа и пара (L,π) удовлетворяет условию $(*)$. Пусть S — σ-инвариантная полупростая связная подгруппа группы $\overline{L}$ (необязательно максимального ранга) и $O^{p'}(S) = L_1 * \dots * L_k$, где $L_1,\dots,L_k$ — конечные группы лиева типа. Тогда для любой группы L_i пара (L_i,π) удовлетворяет условию $(*)$. Кроме того, если $r = \min(\pi \cap \pi(L))$, $c = e(q,r)$ и число r делит $|L_i|$, то $|L_i|$ делится на все примитивные простые делители числа $q^c - 1$ и, в частности, на все числа из $\pi \cap \pi(L)$.*

Д о к а з а т е л ь с т в о. Если L_i отлична от групп вида ${}^3D_4(q^\alpha)$ или $L_i = {}^3D_4(q^\alpha)$ и $c \neq 4\beta$, где β делит α, то все следует из [5, лемма 15]. Допустим, $L_i = {}^3D_4(q^\alpha)$ и $c = 4\beta$, $\beta|\alpha$. Тогда $q^{2\beta} \equiv -1 \pmod r$. Если r делит, а числа из τ не делят $|L_i|$, то $q^{4\alpha} - q^{2\alpha} + 1$ делится на r. Тогда $r = 3$ и, следовательно, одно из чисел $q-1$, q или $q+1$ делится на r. Так как $r \neq p$, отсюда вытекает, что $c = e(q,r) \in \{1,2\}$. Противоречие. □

Далее, для пары (L,π), удовлетворяющей условию $(*)$, всегда будем обозначать символом r число $\min(\pi \cap \pi(L))$, символом τ — множество $\pi \cap \pi(L) \setminus \{r\}$ и символом c — число $e(q,t)$ для любого $t \in \tau$ (при этом c не зависит от t).

Будем говорить, что пара (L,π) *удовлетворяет условию* $(**)$, если она удовлетворяет условию $(*)$ и справедливы следующие утверждения:

(1) если $G = E_6(q)$, $r = 3$ и $c = 1$, то $13 \notin \tau$;

(2) если $G = {}^2E_6(q)$, $r = 3$ и $c = 2$, то $13 \notin \tau$;

(3) если $G = E_7(q)$, $r = 3$ и $c \in \{1,2\}$, то $13 \notin \tau$;

(4) если $G = E_8(q)$, $r = 3$ и $c \in \{1,2\}$, то $13 \notin \tau$;

(5) если $G = E_8(q)$, $r = 5$ и $c = 1$, то $31 \notin \tau$;

(6) если $G = F_4(q)$, $r = 3$ и $c \in \{1,2\}$, то $13 \notin \tau$.

З а м е ч а н и е. Для классических групп и групп Судзуки и Ри условия $(*)$ и $(**)$ эквивалентны.

Лемма 14. *Пусть $L = O^{p'}(\overline{L}_\sigma)$ — конечная группа лиева типа и пара (L,π) удовлетворяет условию $(**)$. Пусть $\overline{S}$ — σ-инвариантная полупростая связная подгруппа группы $\overline{L}$ (необязательно максимального ранга) и $O^{p'}(\overline{S}_\sigma) = L_1 * \dots * L_k$, где $L_1,\dots,L_k$ — конечные группы лиева типа. Тогда для любой группы L_i пара (L_i,π) удовлетворяет условию $(**)$.*

Д о к а з а т е л ь с т в о. Лемма немедленно вытекает из леммы 13. □

Заметим, что, с учетом результатов [3, 5], теоремы 2 и 3 можно эквивалентным образом объединить в одно утверждение.

Теорема 4. *Пусть L — группа лиева типа и пара (L,π) удовлетворяет условию $(*)$. Группа L обладает свойством D_π тогда и только тогда, когда пара (L,π) удовлетворяет условию $(**)$.*

Доказательство. *Необходимость.* Докажем утверждения (1), (2) и (6). Пусть $G = E_6^\eta(q)$ или $G = F_4(q)$, $r = 3$. Пусть $c = 1$, если $G = F_4(q)$, или $\eta = 1$ в остальных случаях, и пусть $c = 2$, если $\eta = -1$. Допустим, $13 \in \tau$. В соответствии с [20, теорема 1], если $p \geqslant 5$, то в группе G имеется элементарная абелева подгруппа E порядка 3^3 такая, что $N_G(E)/C_G(E) \simeq \mathrm{SL}_3(3)$. Если же $p = 2$, то G содержит подгруппу $E_6^\eta(2)$ или $F_4(2)$, и, согласно [21], имеют место вложения $3^3 : \mathrm{SL}_3(3) < \mathrm{L}_4(3) < F_4(2) < E_6^\eta(2)$. Поскольку $|\mathrm{SL}_3(3)|$ делится на 13, в этих случаях G всегда содержит π-подгруппу, не обладающую нормальной холловой τ-подгруппой.

Докажем утверждения (3) и (4). Пусть $G = E_7(q)$ или $G = E_8(q)$, $r = 3$, $c \in \{1,2\}$. Допустим, $13 \in \tau$. В силу вложений каждой из групп $E_6^\eta(q)$, $\eta = \pm 1$, в группу G [9, таблица 2], по доказанному G не обладает свойством D_π.

Докажем утверждение (5). Пусть $G = E_8(q)$, $r = 5$ и $c \in \{1,2\}$. Допустим, что $31 \in \tau$. Условия $c \in \{1,2\}$ и $r = 5$ означают, что при $p \equiv \pm 2 \pmod 5$ число q является четной степенью числа p. Тогда из [20, теорема 1] следует, что при $p \neq 2, 5$ в группе G имеется элементарная абелева подгруппа E порядка 5^3 такая, что $N_G(E)/C_G(E) \simeq \mathrm{SL}_3(5)$. При $p = 2$, согласно [20, теорема 5.1], в G есть подгруппа $\mathrm{L}_4(5)$. Далее, в обоих случаях рассуждения, аналогичные приведенным в доказательстве необходимости утверждений (1), (2) и (6), показывают, что G не обладает свойством D_π.

Достаточность. Можно считать, что группа L универсальна. Допустим, доказываемое неверно, и L — группа лиева типа наименьшего порядка такая, что пара (L,π) удовлетворяет условию $(**)$, но L не обладает свойством D_π. Тогда в группе L существует максимальная π-подгруппа M, не являющаяся холловой. Доказательство несуществования группы L разобьем на серию вспомогательных лемм.

Лемма 15. *Пусть M нормализует некоторую собственную подгруппу F группы L такую, что $F = L_1 * \dots * L_k$, где $L_1,\dots,L_k$ — группы лиева типа, для каждой из которых пара (L_i,π) удовлетворяет условию $(**)$. Тогда $M \cap F$ и $M \cap L_i$ — холловы π-подгруппы групп F и L_i соответственно.*

Доказательство. В силу минимальности L, каждая из групп $L_1,\dots,L_k$ обладает свойством D_π, поэтому, согласно [5, теорема 2], группа FM обладает этим свойством, и, следовательно, M — холлова π-подгруппа группы FM. Теперь по лемме 1 п. (1) утверждение доказано. $\square$

Лемма 16. *Во введенных обозначениях $O_\tau(M) \leqslant Z(L)$.*

Доказательство. Можно считать, что L универсальна. Пусть $L = \overline{L}_\sigma$. Так как группа L обладает абелевой холловой τ-подгруппой T, группа L обладает свойством D_τ. Таким образом, можно считать, что $O_\tau(M)$ содержится в T. Известно [5, теорема 4], что T содержится в некотором σ-инвариантном максимальном торе $\overline{S}$ группы $\overline{L}$ таком, что $N_L(S)$ содержит силовскую r-подгруппу группы L, где $S = \overline{S}_\sigma$. Допустим, $X = O_\tau(M) \nleqslant Z(L)$. Так как $X \leqslant \overline{S}$, то $\overline{C} = C_{\overline{L}}(X)^0$ — связная редуктивная σ-инвариантная подгруппа максимального ранга группы $\overline{L}$ меньшей размерности. Следовательно, $\overline{C} = \overline{H}\overline{L}_1 * \dots * \overline{L}_k$, где $\overline{H}$ — некоторый максимальный тор группы $\overline{C}$, а $\overline{L}_1,\dots,\overline{L}_k$ — нормальные в $\overline{C}$ простые связные σ-инвариантные подгруппы. Пусть $C = \overline{C}_\sigma$, $L_i = (\overline{L}_i)_\sigma$ и $H = \overline{H}_\sigma$. Из леммы 14 и минимальности порядка контрпримера L следует, что группа C обладает свойством D_π, причем ее холлова π-подгруппа содержит нормальную холлову τ-подгруппу, которая, в силу включений $\overline{S} \leqslant \overline{C}$ и $S \leqslant C$, является холловой τ-подгруппой группы L. Так как X — нормальная подгруппа группы M, подгруппа C является M-инвариантной. Поэтому группа CM обладает свойством D_π, и, следовательно, M

— холлова π-подгруппа группы CM. Но тогда $C \cap M$ — холлова π-подгруппа групп C и L, и кроме того, $T \leqslant C \cap M$. Имеют место включения

$$T \leqslant O_\tau(C \cap M) \leqslant O_\tau(M) = X.$$

Таким образом, $X = T$. Теперь, в силу максимальности M, M/T — силовская r-подгруппа группы $N_L(T)/T$, а поскольку $N_L(T)$ содержит силовскую r-подгруппу группы L, M — холлова π-подгруппа группы L. Противоречие. □

Лемма 17. *Пусть M нормализует некоторую собственную подгруппу F группы L такую, что $F = L_1 * \dots * L_k$, где $L_1, \dots, L_k$ — неразрешимые группы лиева типа, для каждой из которых пара (L_i, π) удовлетворяет условию $(**)$. Тогда все группы L_i, $i = 1, 2, \dots, k$, являются π'-группами.*

Доказательство. В силу минимальности L холлова π-подгруппа каждой из подгрупп L_i обладает нормальной холловой τ-подгруппой. То же верно и для F. Теперь $M \cap F$ — холлова π-подгруппа группы F и $O_\tau(M \cap F) \leqslant O_\tau(M) \leqslant Z(L)$ и, следовательно, $O_\tau(M \cap F) \leqslant Z(F)$. Это означает, что каждая из групп $L_i/Z(L_i)$ является τ'-группой. Поскольку $|L_i/Z(L_i)|$ всегда делится на $|Z(L_i)|$, отсюда вытекает, что все L_i являются τ'-группами. Применение леммы 13 завершает доказательство. □

Лемма 18. *Группа L не совпадает ни с одной из групп вида $A^\eta_{n-1}(q)$, а при нечетных q — ни с одной из групп вида $B_n(q)$, $C_n(q)$ или $D^\eta_n(q)$.*

Доказательство. Допустим, L — одна из групп, перечисленных в условии леммы. Положим $G = \mathrm{GL}^\eta_n(q)$, если $L = A^\eta_{n-1}(q)$, $G = \mathrm{O}_{2n+1}(q)$, если $L = B_n(q)$, $G = \mathrm{Sp}_{2n}(q)$, если $L = C_n(q)$, и $G = \mathrm{O}^\eta_{2n}(q)$, если $L = D^\eta_n(q)$. Очевидно, что G обладает свойством D_π тогда и только тогда, когда L обладает этим свойством. Пусть N — максимальная π-подгруппа группы G, не являющаяся холловой π-подгруппой. Из леммы 16 следует, что $O_\tau(N) \leqslant Z(G)$. Пусть $R = O_r(N)$. Так как $N \nleqslant Z(G)$ и в силу разрешимости N (см. [22]), $R \nleqslant Z(G)$. Максимальность N влечет включение $O_r(N_G(R)) \leqslant O_r(N) = R$, поэтому R — радикальная r-подгруппа группы G. Пусть все обозначения из § 2 для данной группы G имеют место. Тогда числа из множества τ и число r — примитивные простые делители числа $q^e - \varepsilon$. Пусть $C = C_G(R)$. Учитывая строение C (см. лемму 12), из леммы 17 заключаем, что имеет место утверждение (2) леммы 12. Покажем, что $|N_G(R)/Z(G)|$ не делится на числа из τ. Поскольку $N \leqslant N_G(R)$, отсюда будет следовать, что образ N в факторгруппе $G/Z(G)$ является r-группой, что приведет нас к противоречию, так как любая силовская r-подгруппа группы G нормализует некоторую холлову τ-подгруппу. Из утверждения (2) леммы 12 следует, что если $|N_G(R)/Z(G)|$ делится на некоторое число $t \in \tau$, то t должно делить в обозначениях этой леммы либо число $|\,\mathrm{Sp}_{2\gamma}(r)|$, либо одно из чисел $|\,\mathrm{GL}_{c_i}(r)|$, $i \in \{1, \dots, l\}$. Значит, t либо делит $r^{2j} - 1$, где $j \leqslant \gamma$, либо делит $r^k - 1$, где $k \leqslant c_i$. Так как в силу леммы 12 п. (2) $G = \mathrm{GL}^\eta_n(q)$, то G обладает холловой $\{r, t\}$-подгруппой и $e(q, r) = e(q, t) = c$. В силу [3, теоремы 4.1 и 4.3] получаем $n < ct$, а если $\eta = -1$ и $c \equiv 2 \pmod 4$, то $2n < ct$. Поскольку в нашем случае $\varepsilon = 1$ при $e = 2$, имеем $c \in \{1, 2\}$. Из леммы 12 вытекает, что если $c = 2$, то $\eta = -1$, поэтому в нашем случае всегда $n < t$. Допустим, t делит $r^f \pm 1$, где $f = j$ или $f = k$. Тогда t делит $(r^f \pm 1)/2$. Но

$$\frac{r^f \pm 1}{2} \leqslant r^f - 1 < r^{\alpha + \gamma + c_1 + \dots + c_l} = n < t.$$

Противоречие. Лемма доказана. □

Лемма 19. *Группа L не совпадает ни с одной из групп вида $B_n(q) \simeq C_n(q)$ или $D^\eta_n(q)$, где q — степень числа 2.*

Доказательство. Допустим, L — одна из групп, перечисленных в условии леммы. Положим $G = \mathrm{Sp}_{2n}(q)$, если $L = B_n(q)$ или $L = C_n(q)$, и $G = \mathrm{O}_{2n}^{\eta}(q)$, если $L = D_n^{\eta}(q)$. При этом $Z(G) = 1$. Как и в предыдущей лемме, L обладает свойством D_π тогда и только тогда, когда G обладает этим свойством, поэтому в G имеется максимальная π-подгруппа N, не являющаяся холловой π-подгруппой. Так как $(|N|, 2) = 1$, то в силу [22] N разрешима. Согласно [23, теорема 1.2.1], подгруппа N содержится в элементе H_0 одного из классов Ашбахера $\mathcal{C}_1$, $\mathcal{C}_2$, $\mathcal{C}_3$, $\mathcal{C}_4$, $\mathcal{C}_5$, $\mathcal{C}_7$ и $\mathcal{C}_8$ и не содержится в элементе $\mathcal{C}_6$, поскольку q — степень 2 [23, таблицы 3.5.C, 3.5.E и 3.5.F].

Можно считать, что $H_0 \notin \mathcal{C}_5$. Действительно, допустим, что $H_0 \in \mathcal{C}_5$. Тогда H_0 — ортогональная или симплектическая группа той же размерности, что и G, но над меньшим полем. Пусть G_1 — минимальная по включению подгруппа группы G вида $\mathrm{Sp}_{2n}(q_1)$ или $\mathrm{O}_{2n}^{\pm}(q_1)$, где $q = q_1^s$, содержащая N. Поскольку N имеет нечетный порядок, $N \neq G_1$. Поэтому N содержится в элементе одного из классов $\mathcal{C}_1$, $\mathcal{C}_2$, $\mathcal{C}_3$, $\mathcal{C}_4$, $\mathcal{C}_7$ и $\mathcal{C}_8$ группы G_1. Но тогда N содержится в элементе такого же класса группы G.

Допустим, $H_0 \notin \mathcal{C}_2 \cup \mathcal{C}_7$. Если $H_0 \in \mathcal{C}_1$ — параболическая подгруппа группы G, то, так как $(|N|, 2) = 1$, подгруппа N содержится в факторе Леви H подгруппы H_0. В остальных случаях положим $H = H_0$. Тогда H — либо некоторая классическая группа G_1, либо центральное произведение двух классических групп $G_1 * G_2$ (возможно, единичной размерности). Как и в [5, лемма 15] и леммах 13 и 14, легко показывается, что если число $|G_i|$ делится на r, то оно делится и на все числа из τ, и тогда пара (G_i, π) удовлетворяет условию $(**)$. Следовательно, каждая из групп G_i обладает свойством D_π и их холловы π-подгруппы обладают нормальными холловыми τ-подгруппами. Как и в доказательстве леммы 16, легко показывается, что $N \cap G_i$ — холлова π-подгруппа группы G_i для любого i, причем ясно, что хотя бы одно из этих пересечений нетривиально. Для этого пересечения $O_\tau(N \cap G_i)$ — нетривиальная нормальная τ-подгруппа группы N, существование которой невозможно по лемме 16.

Таким образом, $H_0 \in \mathcal{C}_2 \cup \mathcal{C}_7$. С учетом того, что q — степень 2, из [23, таблицы 3.5.C, 3.5.E и 3.5.F, предложения 4.2.10, 4.2.11 и 4.7.5] следует, что имеет место один из следующих случаев:

(1) $G = \mathrm{Sp}_{2n}(q)$, $H_0 \in \mathcal{C}_2$ — группа типа $\mathrm{Sp}_{2m}(q) \wr S_l$, $n = lm$, $l \geqslant 2$;

(2) $G = \mathrm{O}_{2n}^{+}(q)$, $H_0 \in \mathcal{C}_2$ — группа типа $\mathrm{O}_{2m}^{\varepsilon}(q) \wr S_l$, $n = lm$, $l \geqslant 2$, $\varepsilon^l = +1$;

(3) $G = \mathrm{O}_{2n}^{+}(q)$, $H_0 \in \mathcal{C}_7$ — группа типа $\mathrm{Sp}_{2m}(q) \wr S_l$, $2n = (2m)^l$, $l \geqslant 2$, число m четно при $l = 2$ и $m \neq 1$ при $q = 2$;

(4) $G = \mathrm{O}_{2n}^{-}(q)$, $H_0 \in \mathcal{C}_2$ — группа типа $\mathrm{O}_{2m}^{-}(q) \wr S_l$, $n = lm$, $l \geqslant 3$ нечетно;

(5) $G = \mathrm{O}_{2n}^{+}(q)$, $H_0 \in \mathcal{C}_2$ — группа типа $\mathrm{GL}_n(q).2$;

(6) $G = \mathrm{O}_{2n}^{+}(q)$, $H_0 \in \mathcal{C}_7$ — группа типа $\mathrm{Sp}_{2m}(q) \wr S_2$, $2n = (2m)^2$, m нечетно, при $q = 2$ $m \neq 1$.

В случае (6), согласно [23, предложение 4.7.5], $H_0 = \mathrm{Sp}_{2m}(q) \times \mathrm{Sp}_{2m}(q)$. Случаи (5) и (6) рассматриваются аналогично случаю, когда $H_0 \notin \mathcal{C}_2 \cup \mathcal{C}_7$. В остальных случаях заметим, что $l \leqslant n$. В силу [23, предложения 4.2.10, 4.2.11 и 4.7.5] группа H_0 равна $G_1 \wr S_l$, где G_1 — классическая группа, причем, как и ранее, либо G_1 — π'-группа, либо $|G_1|$ делится на r и на все числа из τ, G_1 обладает свойством D_π и холлова π-подгруппа группы G_1 обладает нормальной холловой τ-подгруппой. Как и ранее, если G_1 не является π'-группой, то $N \cap H$ — холлова π-подгруппа базы H сплетения $H_0 = G_1 \wr S_l$, и N обладает нетривиальной нормальной τ-подгруппой $O_\tau(N \cap H)$, что невозможно. Значит, G_1 — π'-группа, и можно считать, что $N \leqslant S_l$.

Пусть $R = O_r(N)$. Из максимальности N вытекает, что R — радикальная r-подгруппа группы S_l. Покажем, что $|N_{S_l}(R)|$ не делится на числа из τ. Тем самым мы придем к противоречию, поскольку включение $N \leqslant N_{S_l}(R)$ будет означать, что N является r-группой вопреки предположению о максимальности N как π-подгруппы.

Пусть $S_l = S(\Omega)$ для некоторого множества Ω. Используем обозначения § 2 и лемм 4, 5 и 6. Пусть $\Omega = \Omega_0 \cup \Omega_1 \cup \dots \cup \Omega_s$, $R = R_0 \times R_1 \times \dots \times R_s$ — разложения из леммы 5. Заметим, что $S(\Omega_0)$ является π'-группой. Действительно, по лемме 6 подгруппа N содержится в произведении $S(\Omega_0) \times S(\Omega_1 \cup \dots \cup \Omega_s)$. В силу максимальности N, $N \cap S(\Omega_0)$ совпадает с проекцией N на $S(\Omega_0)$ и является максимальной π-подгруппой группы $S(\Omega_0)$. Поскольку $O_r(N \cap S(\Omega_0)) = R_0 = 1$ и $O_\tau(N \cap S(\Omega_0)) \leqslant O_\tau(N) = 1$, то $N \cap S(\Omega_0) = 1$, что в силу максимальности π-подгруппы $N \cap S(\Omega_0)$ в $S(\Omega_0)$ дает требуемое. Допустим, существует число $x \in \tau$, которое делит $|N_{S(\Omega)}(R)|$. Тогда по лемме 6 существует подгруппа R_i, $i \geqslant 1$, такая, что $R_i = A_\mathfrak{c}$ для некоторой последовательности $\mathfrak{c} = (c_1, c_2, \dots, c_t)$, и x делит $|N_{S_\mathfrak{c}}(A_\mathfrak{c}) \wr S_{u(\mathfrak{c})}|$ в обозначениях этой леммы. Тогда, согласно [3, теоремы 4.4 и 4.5], $n \leqslant cx$. Кроме того, по лемме 4 число x делит $|\operatorname{GL}_{c_j}(r)|$ для некоторого $j \leqslant t$ или x делит $|S_{u(\mathfrak{c})}|$. Рассмотрим первый случай. Из Малой теоремы Ферма следует, что $c \leqslant r-1$. Допустим, x делит число $r^f - 1$ для некоторого $f \leqslant \max\{c_1, \dots, c_t\}$. Так как $x > r$, для некоторого натурального y справедливо равенство $r^{f-1} + r^{f-2} + \dots + 1 = xy$. Имеем

$$(r-1)x \leqslant (r-1)xy = r^f - 1 < r^f \leqslant r^{c_1+c_2+\dots+c_t} \leqslant l \leqslant n \leqslant cx \leqslant (r-1)x.$$

Противоречие. Допустим, $x \leqslant u(\mathfrak{c})$. Так как $R \neq 1$ и $l \geqslant r^{c_1+c_2+\dots+c_t} u(\mathfrak{c})$, справедливо неравенство $u(\mathfrak{c}) \leqslant l/r$. Поэтому

$$x \leqslant u(\mathfrak{c}) \leqslant \frac{l}{r} \leqslant \frac{n}{r} \leqslant \frac{cx}{r} \leqslant \frac{r-1}{r}x < x.$$

Противоречие. Лемма доказана. □

Лемма 20. *Группа L не совпадает ни с одной из групп вида $E_6(q)$, ${}^2E_6(q)$, $E_7(q)$, $E_8(q)$, $F_4(q)$, $G_2(q)$, ${}^3D_4(q)$.*

Доказательство. Допустим, L — одна из групп, перечисленных в условии леммы. Можно считать при этом, что L проста. Заметим, что в этом случае $c \in \{1, 2\}$ и $\{r\} \cup \tau \subseteq \pi(q \pm 1)$, поскольку в противном случае L обладает абелевой холловой π-подгруппой [5, леммы 7–13] и, следовательно, является D_π-группой, согласно [25]. Пусть G и $\overline{G}$ соответственно — группа лиева типа и простая односвязная алгебраическая группа, для которых $G = \overline{G}_\sigma$ и $L = O^{p'}(G)$. Как и в доказательствах двух предыдущих лемм, свойства D_π для групп L и G равносильны. Пусть через N обозначена некоторая максимальная π-подгруппа группы L, не являющаяся холловой π-подгруппой. Так как согласно [22] N разрешима, из [18] следует, что справедливо одно из следующих утверждений:

(I) N нормализует некоторую собственную σ-инвариантную связную подгруппу $\overline{F}$ группы $\overline{G}$;

(II) N содержится в нормализаторе некоторой жордановой подгруппы группы G.

Рассмотрим случай, когда справедливо утверждение (I). Разобьем наши рассуждения на три подслучая.

(I.1) $R_u(\overline{F}) \neq 1$. Согласно [24, лемма 3.9] можно считать, что $\overline{F}$ — параболическая подгруппа группы $\overline{G}$. В этом случае $N_{\overline{G}}(\overline{F}) = \overline{F}$, поэтому $N \leqslant F = \overline{F}_\sigma$. Поскольку F — параболическая подгруппа группы G и $(|N|, p) = 1$, подгруппа N содержится в некотором факторе Леви F_L подгруппы F. Если H — подгруппа Картана группы G, содержащаяся в F_L, то $F_L = HL_1 * \dots * L_k$ для некоторых групп лиева типа $L_1, \dots, L_k$, отличных от групп Судзуки или Ри. При этом все подгруппы $L_1, \dots, L_k$ нормальны в F_L. Как и в доказательстве предыдущей леммы, с учетом минимальности L нетрудно заметить, что F_L обладает свойством D_π, поэтому N — холлова π-подгруппа группы F_L. Поскольку очевидно, что N не содержится в H, хотя бы одна из групп $L_i/Z(L_i)$ нетривиальна, ее порядок делится на $q \pm 1$, и, значит, он делится на все числа из τ. Таким образом, $O_\tau(N\cap L_i)$ — нормальная τ-подгруппа группы N, не лежащая в $Z(G)$. Противоречие.

(I.2) $\overline{F}$ — связная редуктивная подгруппа максимального ранга. В этом случае $F=\overline{F}_\sigma=\overline{T}_\sigma L_1*\dots*L_k$, где $\overline{T}$ — максимальный σ-инвариантный тор группы $\overline{G}$, а $L_1,\dots,L_k$ — группы лиева типа над некоторым расширением основного поля. Согласно [12], среди L_i нет групп Судзуки или Ри. Лемма 15 и тот факт, что порядок каждой из групп $L_1,\dots,L_k$ делится на $q\pm1$ и, следовательно, на все числа из τ, доказывают, что $k=0$. Поэтому $\overline{F}$ — максимальный тор и $|F|$ не делится на числа из τ. Значит, NF/F вкладывается в группу $W=N_{\overline{G}}(\overline{F})/\overline{F}$ — группу Вейля группы $\overline{G}$. Согласно [5, леммы 9, 10, 11, 13], либо число r — единственное число из π, которое может делить $|W|$, либо $L=E_6^\eta(q)$, $\{r\}\cup\tau\subseteq\pi(q+\eta)$, $r=3$, $5\in\tau$. В первом случае N является r-группой, что противоречит ее максимальности. Во втором случае порядок тора F делится на 3, так как в противном случае F является π'-группой и N вкладывается в $W=W(E_6)$ вопреки лемме 3. Поэтому, как следует из [5, таблица 1] и [26, предложение 3.3.5], тор F должен соответствовать элементу w из группы Вейля, для которого характеристический многочлен $f_{\rho w}(t)$ элемента ρw делится на многочлен вида $t^{2d}-(-\eta t)^d+1$ (здесь ρ — изометрия евклидова пространства, порожденного корневой системой типа E_6, индуцированная эндоморфизмом σ, как описано в [26, 2.9]). Отсюда следует, что $|\rho w|$ делится на 3. Поскольку $N\leqslant N(G,F)$ и, согласно [26, предложение 3.3.6], $N(G,F)/F\simeq C_{W,\sigma}(w)=C_W(\rho w)$, число $|C_W(\rho w)|$ делится на 5. Таким образом, группа $\langle W,\rho\rangle$ должна содержать элемент порядка 15. Но, так как W — нормальная подгруппа индекса 1 или 2 в $\langle W,\rho\rangle$, это означает, что группа Вейля корневой системы типа E_6, а вместе с ней и группа $\mathrm{Sp}_4(3)$ должны содержать элемент порядка 15, что неверно [21].

(I.3) $\overline{F}$ — связная редуктивная подгруппа немаксимального ранга. Можно считать, что $Z(\overline{F})=Z(\overline{G})$ и, в частности, $\overline{F}$ не является тором, поскольку в противном случае $\overline{F}$ можно заменить связной N-инвариантной и σ-инвариантной подгруппой максимального ранга $C_{\overline{G}}(Z(\overline{F}))$. Таким образом, $\overline{F}=\overline{G}_1*\overline{G}_2*\dots*\overline{G}_k$, где $\overline{G}_1,\overline{G}_2,\dots,\overline{G}_k$ — простые алгебраические подгруппы группы $\overline{G}$. Пусть $G_i=(\overline{G}_i)_\sigma$, $i=1,2,\dots,k$. Тогда $F=\overline{F}_\sigma=G_1*G_2*\dots*G_k$. Если порядок хотя бы одной из групп G_i делится на r, то с помощью леммы 13, как и ранее, несложно доказывается, что подгруппа $O_\tau(N\cap(G_{i_1}*\dots*G_{i_s}))$, где $G_{i_1},\dots,G_{i_s}$ — орбита G_i относительно действия N сопряжениями на сомножителях группы F, является нетривиальной нормальной τ-подгруппой группы N. В противном случае все G_i должны быть группами Судзуки, поскольку порядки всех остальных групп, которыми могут быть G_i, делятся на $q-1$ и $q+1$. Пусть $G_1={}^2B_2(2^{2m+1})$. Поскольку в оставшемся случае F является π'-группой, $N_1=N_N(G_1)$ индуцирует на G_1 некоторую группу внешних автоморфизмов. Поскольку эти автоморфизмы должны быть полевыми, элементы некоторой подгруппы H_1 группы G_1, изоморфной ${}^2B_2(2)\simeq 5:4$, централизуются группой N_1. Пусть x_1 — элемент порядка 5 из H_1. Пусть $t_1,\dots,t_s$ — полная система представителей правых смежных классов группы N по подгруппе N_1. Можно, не уменьшая общности, считать, что $G_1,\dots,G_s$ — орбита относительно действия группы N на множестве групп G_i и что $G_i=G_1^{t_i}$, $i=1,\dots,s$. Положим $x_i=x_1^{t_i}$ для всех $i\leqslant s$ и $x=x_1\dots x_s$. Поскольку x — полупростой элемент, $C_{\overline{G}}(x)^0$ — собственная связная редуктивная σ-инвариантная подгруппа максимального ранга группы $\overline{G}$, нормализуемая подгруппой N, и, значит, имеет место случай (I.2).

Теперь предположим, что справедливо утверждение (II). Тогда в соответствии с [19] имеет место один из следующих случаев:

(II.1) $\overline{G}$ — группа типа D_4 и $N\leqslant 2^3.\,\mathrm{O}_6^+(2)$ или $N\leqslant 2^3.S_8$;

(II.2) $\overline{G}$ — группа типа E_6 и $N\leqslant 3^3.3^3.\,\mathrm{SL}_3(3)$;

(II.3) $\overline{G}$ — группа типа E_8 и $N\leqslant 2^5.2^{10}.\,\mathrm{SL}_2(5)$;

(II.4) $\overline{G}$ — группа типа E_8 и $N \leqslant 5^3.\,\mathrm{SL}_3(5)$;

(II.5) $\overline{G}$ — группа типа F_4 и $N \leqslant 3^3.\,\mathrm{SL}_3(3)$;

(II.6) $\overline{G}$ — группа типа G_2 и $N \leqslant 2^3.\,\mathrm{SL}_3(2)$.

Случаи (II.1), (II.3) и (II.6) исключаются в силу леммы 3. Из этой же леммы следует, что жорданова подгруппа, в нормализаторе которой содержится N, должна быть r-группой. Таким образом, в случаях (II.2) и (II.5) единственным простым числом из τ может быть 13, а в случае (II.4) — 31. К тому же, поскольку прообраз нормализатора жордановой подгруппы должен содержаться в группе G, из [20, теорема 1] вытекает, что если $L = E_6^{\eta}(q)$, то $q \equiv \eta \pmod 3$, что противоречит условию $(**)$. Лемма доказана. □

Лемма 21. *Группа L не совпадает ни с одной из групп вида ${}^2B_2(2^{2m+1})$, ${}^2F_4(2^{2m+1})$, ${}^2G_2(3^{2m+1})$.*

Доказательство. Для ${}^2G_2(3^{2m+1})$ утверждение было доказано в [27]. Для групп ${}^2B_2(2^{2m+1})$ и ${}^2F_4(2^{2m+1})$ доказываемое вытекает из списка максимальных подгрупп в этих группах [28, 29] и минимальности L. □

Теперь теорема 4 прямо следует из лемм 18–21. Тем самым, теоремы 2 и 3 доказаны. □

Поступила 21.11.2006

СПИСОК ЛИТЕРАТУРЫ

1. **Hall P.** Theorems like Sylow‘s // Proc. London Math. Soc. 1956. V. 6, no. 22. P. 286–304.
2. **Gross F.** On a conjecture of Philip Hall // Proc. London Math. Soc. Ser. III. 1986. V. 52, no. 3. P. 464–494.
3. **Gross F.** Odd order Hall subgroups of the classical linear groups // Math. Z. 1995. V. 220, no. 3. P. 317–336.
4. **Gross F.** Conjugacy of odd order Hall subgroups // Bull. London Math. Soc. 1987. V. 19, no. 4. P. 311–319.
5. **Вдовин Е. П., Ревин Д. О.** Холловы подгруппы нечетного порядка конечных групп // Алгебра и логика. 2002. Т. 41, № 1. С. 15–56.
6. **Thompson J. G.** Hall subgroups of the symmetric groups // J. Comb. Th. Ser. A. 1966. No. 1. P. 271—279.
7. **Ревин Д. О.** Свойство D_π в одном классе конечных групп // Алгебра и логика. 2002. Т. 41, № 3. С. 335–370.
8. **Carter R. W.** Simple groups of Lie type. London: Wiley, 1972.
9. **Кондратьев А. С.** Подгруппы конечных групп Шевалле // Успехи мат. наук. 1986. Т. 41, №1. С. 57–96.
10. **Humphreys J. E.** Linear algebraic groups. New York: Springer-Verlag, 1972.
11. **Borel A., Tits J.** Eléments unipotents et sousgroupes paraboliques de groupes réductifs, I // Invent. Math. 1971. V. 12, no. 2. P. 95–104.
12. **Borel A., de Siebental J.** Les-sous-groupes fermés de rang maximum des groupes de Lie clos // Comment. Math. Helv. 1946. V. 23. P 200–221.
13. **Горенстейн Д.** Конечные простые группы: введение в их классификацию. М.: Мир, 1985.
14. **Ревин Д. О.** Суперлокалы в симметрических и знакопеременных группах // Алгебра и логика. 2003. Т. 42, № 3. С. 338–365.
15. **Alperin J. L., Fong P.** Weights for symmetric and general linear groups // J. Algebra. 1990. V. 131, no. 1. P. 2–22.
16. **An J.** Weights for classical groups // Trans. Amer. Math. Soc. 1994. V. 342, no. 1. P. 1–42.

17. **Griess R.** Automorphisms of extra special groups and nonvanishing degree 2 cohomology // Pacif. J. Math. 1973. V. 48. P. 403–411.
18. **Borovik A. V.** The structure of finite subgroups of simple algebraic groups // Algebra and Logic. 1989. V. 28, no 3. P. 163–183.
19. **Borovik A. V.** The structure of Jordan subgroups of simple algebraic groups // Algebra and Logic. 1989. V. 28, no. 2. P. 97–108.
20. **Cohen A. M., Liebeck M. W., Saxl J., Seitz G. M.** The local maximal subgroups of exceptional groups of Lie type, finite and algebraic // Proc. London Math. Soc., Ser. III. 1992. V. 64, no. 1. P. 21–48.
21. **Conway J. H., Curtis R. T., Norton S. P., Parker R. A., Wilson R. A.** Atlas of Finite Groups. Oxford: Clarendon Press, 1985.
22. **Feit W., Thompson J.** Solvability of groups of odd order // Pacif. J. Math. 1963. V. 13, no. 3. P. 775–1029.
23. **Kleidman P. B., Liebeck M.** The subgroup structure of finite classical groups. Cambridge: Cambridge Univ. Press, 1990.
24. **Revin D. O., Vdovin E. P.** Hall subgroups of finite groups // Ischia Group Theory 2004: Proceedings of a Conference in Honour of Marcel Herzog. Contemporary Mathematics. 2006. V. 402. P. 229–265.
25. **Wielandt H.** Zum Satz von Sylow // Math. Z. 1954. V. 60, no. 4. P. 407–408.
26. **Carter R. W.** Finite groups of Lie type, conjugacy classes and complex characters// London: Wiley, 1985.
27. **Мазуров В. Д., Ревин Д. О.** О холловом D_π-свойстве для конечных групп // Сиб. мат. журн. 1997. Т. 38, № 1. С. 106–113.
28. **Suzuki M.** On a class of doubly transitive groups // Ann. Math. 1962. V. 75, no. 1. P. 105–145.
29. **Malle G.** The maximal subgroups of ${}^2F_4(q^2)$ // J. Algebra. 1991. V. 139, no. 1. P. 52–69.

Том 13 № 1 2007

УДК 512.544

О ГРУППАХ С ПОЧТИ СОВЕРШЕННОЙ ИНВОЛЮЦИЕЙ

А. И. Созутов

Работа посвящена обобщениям теорем Жордана, Фробениуса, М. Холла, Брауэра — Судзуки — Уолла, Шункова, Мазурова, Беляева.

1. Точно дважды транзитивные группы

Пусть G — произвольная группа, H — ее собственная подгруппа и $F^{\#} = G \setminus \cup_{x\in G} H^x$, $F = F^{\#} \cup \{1\}$. Множество F инвариантно в G и замкнуто относительно взятия обратного элемента. Если $H \cap H^g = 1$ для любого $g \in G \setminus H$, то подгруппа H называется *обособленной в* G, а (G, H) — *парой Фробениуса* [1]. В подстановочном представлении группа G есть транзитивная группа подстановок с неединичным стабилизатором точки H, в которой лишь единичная подстановка оставляет на месте две точки, а множество $F^{\#}$ состоит из регулярных подстановок. Если G конечна, то по известной теореме Фробениуса F есть подгруппа и $G = F \leftthreetimes H$. Частный случай этой теоремы доказал еще К. Жордан, предполагая группу G дважды транзитивной. Такие группы сейчас называются *точно дважды транзитивными* [2]. Они тесно связаны с теорией почти-полей и почти-областей [3]. М. Холл доказывает теорему Жордана и для бесконечных групп, у которых в каждом смежном классе по подгруппе H содержится точно одна регулярная подстановка ([4], теорема 20.7.1, п. 3). На самом деле этого условия достаточно для доказательства теоремы Фробениуса ([1], лемма 2.6), а теорема Жордана — Холла верна в более сильной формулировке.

Теорема 1 ([5], теорема 1). *Пусть G — точно дважды транзитивная группа подстановок, H — ее стабилизатор точки. Если некоторый смежный класс $Hg \neq H$ содержит не более одной регулярной подстановки, то все регулярные подстановки группы G вместе с единичной подстановкой составляют регулярную абелеву нормальную подгруппу F и $G = F \leftthreetimes H$.*

В случае, когда стабилизатор точки содержит инволюцию, заключение теоремы 1 остается верным и при более слабом условии на количество регулярных подстановок в смежном классе по стабилизатору точки.

Теорема 2 ([5], теорема 2). *Пусть G — точно дважды транзитивная группа подстановок, H — ее стабилизатор точки и в H есть инволюция. Если некоторый смежный класс $Hg \neq H$ содержит конечное множество регулярных подстановок, то все регулярные подстановки группы G вместе с единичной подстановкой составляют регулярную абелеву нормальную подгруппу F и $G = F \leftthreetimes H$.*

2. Некоторые обобщения теоремы Фробениуса

В [6] В.П. Шунков получил следующее обобщение теоремы Фробениуса.

Теорема 3. *Периодическая группа с конечной обособленной подгруппой четного порядка является локально конечной группой Фробениуса.*

Далее нам нужны новые понятия. Инволюция j бесконечной группы G называется *конечной*, если $|jj^g| < \infty$ для каждого элемента $g \in G$ [1, 14]. Следующие две теоремы из [1] обобщают результаты В.П. Шункова из [7].

Теорема 4. *Пусть множество инволюций J группы G содержит конечную инволюцию, а группа G — обособленную подгруппу H с инволюцией, причем для некоторого смежного класса $Hg \neq H$ пересечение $J^2 \cap Hg$ конечно. Тогда все инволюции в G сопряжены, инволюция в H единственна, $\langle J \rangle$ — локально конечная группа Фробениуса с абелевым ядром F и дополнением порядка 2, а $G = F \leftthreetimes H$.*

Теорема 5. *Пусть G — периодическая группа, (G, H) — пара Фробениуса, H содержит инволюцию и J — множество инволюций из G. Группа G тогда и только тогда является группой Фробениуса с дополнением H, когда для некоторого смежного класса $Hg \neq H$ пересечение $J^2 \cap Hg$ конечно.*

Инволюция j называется *совершенной* в G, если любые две неперестановочные инволюции из j^G сопряжены при помощи инволюции из этого же класса [5]. Инволюцию $j \in G$ назовем *почти совершенной*, если любые две инволюции из j^G, произведение которых имеет бесконечный порядок, сопряжены при помощи некоторой инволюции из G (в отличие от определения из [15], в котором сопрягающая инволюция выбиралась из j^G). Среди конечных инволюций совершенными являются: изолированная инволюция, 3-транспозиции Фишера, нечетные транспозиции Ашбахера, инволюции в группах $L_2(Q)$, $Sz(Q)$, $U_3(Q)$ над локально конечным полем Q характеристики 2, инволюция из обособленной подгруппы. Определение конечной инволюции есть (j, j)-условие конечности, часто используемое в работах В.П. Шункова и его учеников. Определения совершенной и почти совершенной инволюции носят другой характер. В точно дважды транзитивной группе инволюция из стабилизатора точки совершенна, при этом произведение двух инволюций может иметь бесконечный порядок. В аксиоматике геометрий, принадлежащей Бахману, большую роль играют два множества инволюций: симметрии относительно гиперплоскостей и точек. Например, для евклидовой плоскости это два разных класса сопряженных инволюций, и оба состоят из совершенных инволюций. Понятие почти совершенной инволюции еще раз расширяет класс смешанных групп, на которые переносятся затронутые в данной статье результаты.

В [5] получено такое обобщение теоремы 3.

Теорема 6. *Пусть (G, H) — пара Фробениуса, H конечна и содержит совершенную в G инволюцию. Тогда инволюция в H единственна, все инволюции в G сопряжены, $G = F \leftthreetimes H$ и F — абелева 2-полная группа.*

В § 6 статьи доказана следующая теорема.

Теорема 7. *Пусть группа G содержит конечную обособленную подгруппу H с почти совершенной инволюцией j. Тогда инволюция j в H единственна, $G = F \leftthreetimes H$, F — абелева группа, а j инвертирует F.*

3. Обобщения теоремы Брауэра — Судзуки — Уолла

В данном разделе речь пойдет об обобщении известных результатов о строении конечных групп с абелевыми централизаторами инволюций [9, 10]. Группы с конечной инволюцией, в которых централизатор каждой инволюции есть абелева 2-группа, изучены В.Д. Мазуровым (теорема 2, [11]), за исключением случая квазициклических силовских 2-подгрупп. Доказательство этого результата по существу опирается на следующую теорему (следствие теоремы 1 из [11]).

Теорема 8. *Пусть G — трижды транзитивная группа, в которой стабилизатор двух точек коммутативен и не содержит инволюций. Тогда существует поле P характеристики 2 такое, что группа G подобна проективной линейной группе $PGL_2(P)$ в ее естественном действии на проективной прямой $P \cup \{\infty\}$.*

В [12] с помощью приведенной теоремы 8 Мазурова доказана следующая теорема, обобщающая результаты из [9, 11].

Теорема 9. *Пусть группа G содержит почти совершенную инволюцию i и централизатор каждой инволюции из G является элементарной абелевой группой. Тогда выполняется одно из следующих утверждений:*

1. *G — расширение элементарной абелевой 2-группы $U = C_G(i)$ с помощью группы без инволюций, при этом каждый элемент из $G \setminus U$ действует на U регулярно.*

2. *$G = F \leftthreetimes \langle i \rangle$ — группа Фробениуса с 2-полным абелевым ядром F и дополнением $\langle i \rangle$.*

3. *G изоморфна группе $PGL_2(Q)$, где Q — подходящее квадратично замкнутое поле характеристики 2.*

Для периодических групп с абелевыми централизаторами инволюций Н.М. Сучковым [13] получен аналог известной теоремы Судзуки [10] и тем самым доказана локальная конечность таких групп, за исключением случая, когда силовские 2-подгруппы группы являются квазициклическими. Естественно возникает задача об обобщении результатов Мазурова и Сучкова на группы с (почти) совершенной инволюцией. Условие почти совершенности инволюции существенно ослабляет условия периодичности и конечности инволюции, поскольку во всех трех пунктах теоремы 9 группа G не обязана быть периодической. В качестве примера, иллюстрирующего необходимость данного условия, можно привести свободное произведение $G = A * B$ произвольной группы A с абелевыми централизаторами инволюций на произвольную группу B без инволюций. Понятно, что для такой группы G теорема 9 уже неверна.

4. Группы с почти регулярной инволюцией

Напомним, что инволюция j бесконечной группы G с конечным централизатором $C_G(j)$ называется *почти регулярной*. Группа G, содержащая разрешимую нормальную подгруппу конечного индекса, называется *почти разрешимой*. В 1972 г. В.П. Шунков [8] доказал следующий фундаментальный результат.

Теорема 10. *Периодическая группа с почти регулярной инволюцией локально конечна, почти разрешима и все ее квазициклические 2-подгруппы порождают нормальную черниковскую подгруппу.*

В.В. Беляев [14] получил более общий результат для групп с конечной инволюцией:

Теорема 11. *Пусть группа G содержит конечную почти регулярную инволюцию j. Тогда справедливы следующие утверждения.*

1. *G — локально конечная группа.*

2. *$[j, G]$ содержится в FC-радикале группы G и $|G : [j, G]| \leq |C_G(j)|$.*

3. *Коммутант FC-радикала группы G конечен.*

Из этой теоремы легко вывести теорему 10. В статье [15] теорема 11 была обобщена на более широкий класс групп.

Теорема 12. *Пусть группа G содержит почти регулярную инволюцию j и любые две инволюции из j^G, порядок произведения которых бесконечен, сопряжены при помощи подходящей инволюции из j^G. Тогда справедливы следующие утверждения.*

1. *$[j, G]$ содержится в FC-радикале группы G и $|G : [j, G]| \leq |C_G(j)|$.*
2. *Коммутант FC-радикала группы G конечен.*
3. *$FC(G)$ содержит нормальную в G нильпотентную класса 2 подгруппу конечного индекса.*

В [15] инволюция из формулировки теоремы 12 называлась почти совершенной. Позднее было замечено, что это определение можно ослабить до существования сопрягающей инволюции в группе, а не в классе j^G. Именно такая инволюция в следующей теореме называется *почти совершенной.*

Теорема 13. *Пусть группа G содержит почти совершенную инволюцию j и $|C_G(j)| < \infty$. Тогда* (1) *G почти разрешима и* (2) *все ее квазициклические 2-подгруппы порождают нормальную черниковскую подгруппу.*

Теорема 13 доказывается в § 7.

5. Обозначения и известные результаты

Используемые в статье обозначения стандартны. Пусть G — произвольная группа, тогда $\langle X\rangle$ — подгруппа, порожденная множеством $X \subseteq G$, в частности, $\langle x\rangle$ — циклическая подгруппа (в отличие от обозначений из [14]), порожденная элементом x; $x^G = \{\, x^y = y^{-1}xy \mid y \in G \,\}$ — класс сопряженных с x элементов группы G; $[x, y] = x^{-1}y^{-1}xy$ — коммутатор элементов $x, y \in G$; $[X, Y] = \langle [x, y] \mid x \in X, y \in Y\rangle$ для любых подмножеств X, Y из G.

Если $x, y \in G$ и $|G : C_G(x)| < \infty$, $|G : C_G(y)| < \infty$, то по теореме Пуанкаре [17, 18] индекс $|G : C_G(xy)|$ также конечен, и, значит, множество

$$FC(G) = \{x \mid x \in G,\, |G : C_G(x)| < \infty\}$$

является подгруппой, называемой *FC-радикалом* группы G. По лемме Дицмана [16, 18] конечное инвариантное множество элементов конечного порядка в произвольной группе порождает конечную нормальную подгруппу, и в силу теоремы Шмидта [16, 17] FC-радикал обладает локально конечной периодической частью, при этом каждое ее конечное множество элементов содержится в конечной нормальной подгруппе группы.

Если группа G обладает конечным покрытием смежными классами по некоторым подгруппам, то по лемме Неймана (доказательство см., например, в [1], лемма 2.11) хотя бы одна из этих подгрупп имеет в G конечный индекс. С помощью этой леммы в [14] доказано следующее предложение.

Предложение 1. *Если X — конечное подмножество произвольной группы G и $X \cap X^g \neq \varnothing$ для любого $g \in G$, то пересечение $X \cap FC(G)$ не пусто.*

Нам понадобится еще одна лемма из [14].

Предложение 2. *Пусть H — конечная нормальная подгруппа произвольной группы G, j — инволюция из G и $|C_G(j)| = n < \infty$. Тогда $|C_{G/H}(jH)| \leq |C_G(j)|$, и если $|C_{G/H}(jH)| = |C_G(j)|$, то $h^j = h^{-1}$ для любого $h \in H$ и $H \leq Z([j, G])$.*

Следующие свойства групп диэдра хорошо известны.

Предложение 3. *Пусть $D = \langle i, j\rangle$, где i и j — инволюции.*

1. *Если в $\langle ij\rangle$ есть инволюция z, то $z \in Z(D)$ и инволюции i, j не сопряжены в D.*

2. *Если порядок элемента ij конечен и нечетен, то i^D — единственный класс сопряженных инволюций группы D, $i = j^c$, где $c \in \langle ij\rangle$, $c^2 = ij$, и для инволюции $k = ic$ имеем $i^k = j$, $j^k = i$.*

3. *Если порядок элемента ij бесконечен, то в D имеется точно два класса сопряженных инволюций i^D и j^D.*

Предложение 4. *Пусть j — почти совершенная инволюция группы G. Если $T \lhd G$ и $j \notin T$, то инволюция $\overline{j}$ почти совершенна в факторгруппе $\overline{G} = G/T$.*

Д о к а з а т е л ь с т в о. Действительно, если $|\overline{j} \cdot \overline{j}^{\overline{g}}| = \infty$, то для любого прообраза g элемента $\overline{g}$ порядок $|jj^g|$ также бесконечен и для некоторой инволюции $v \in G$ имеем $j^v = j^g$. Но тогда $\overline{j}^{\overline{v}} = \overline{j}^{\overline{g}}$ и предложение доказано.

6. Доказательство теоремы 7

В леммах 1 и 2 группа G и ее инволюция j удовлетворяют условиям более общей теоремы 13. Будем использовать индукцию по $|C_G(j)|$, основание индукции — лемма 1. Обозначим через J множество инволюций группы G.

Лемма 1. *Пусть $C_G(j) = \langle j\rangle$. Тогда $G = F \leftthreetimes \langle j\rangle$, F — абелева группа без инволюций, а j инвертирует F.*

Д о к а з а т е л ь с т в о. Пусть $F = G \setminus J$, f — произвольный элемент из F и $v = j^f$. По определению почти совершенной инволюции найдется инволюция $k \in J$ такая, что $v^k = j$. Ввиду условий леммы $fk \in \langle j\rangle$. Поскольку $f \neq k$, то $f = jk$ и $f^j = f^{-1}$. Таким образом, $J = jF$, $F = jJ$. Множество F инвариантно в G, поэтому любая инволюция из j^G инвертирует каждый элемент из F. Отсюда выводим, что $\langle j^G\rangle = A \leftthreetimes \langle j\rangle$, $A \subseteq F$ и $A \leq C_G(F)$, в частности A — абелева нормальная в G подгруппа.

Пусть k — произвольная инволюция из J. Тогда $f = jk \in F$ и k инвертирует каждый элемент из A. Поэтому $\langle J\rangle = C_G(A) \leftthreetimes \langle j\rangle$. Понятно, что $C_G(A) = F$ и для любых $b, c \in F$ выполняется $bc = (c^{-1}b^{-1})^{-1} = (c^{-1}b^{-1})^j = cb$. Лемма доказана.

Пусть G — минимальный относительно $|C_G(j)|$ контрпример к теореме 7. Ключ к доказательству, как и в [14], дает следующая лемма.

Лемма 2. *Справедливо хотя бы одно из следующих утверждений*:

1. $G = C_G(j) \cdot FC(G)$.

2. *$FC(G)$ содержит инволюцию.*

Д о к а з а т е л ь с т в о. Следуя [14], для любого $b \in G$ через $J(b)$ обозначим множество инволюций из $C_G(b)$. Пусть $g \in G$, $j^g \neq j$ и

$$X_g = J(j) \cup J(j^g) \cup \{(rg)^s, (rg)^{-1} \mid r, s \in C_G(j)\}.$$

Ввиду условий теоремы 7 множество X_g конечно и, поскольку $j \neq j^g$, то $1 \notin X_g$. Пусть x — произвольный элемент из G. Докажем, что пересечение $X_g^x \cap X_g$ непусто. Допустим, что

$J(j^x) \cap (J(j) \cup J(j^g)) = \varnothing$. Тогда порядки произведений $j^x j$ и $j^x j^g$ не являются четными (утверждение 1 предложения 3). Согласно утверждению 2 предложения 3 и определению почти совершенной инволюции, найдутся инволюции $v, t \in G$, для которых $j^{gv} = j^x$ и $j^{xt} = j$. Отсюда выводим соотношения $gvt = r^{-1} \in C_G(j)$, $tv = rg$ и $xt = s^{-1} \in C_G(j)$, $sx = t$, а также $(rg)^{sx} = (tv)^t = (rg)^{-1}$ и

$$(s^{-1}rgs)^x = (rg)^{-1}. \tag{6.1}$$

Следовательно, $X_g \cap X_g^x \neq \varnothing$. В силу предложения 1 некоторый элемент из X_g содержится в $FC(G)$. Если для некоторого g пересечение $X_g \cap FC(G)$ содержится в $J(j) \cup J(j^g)$, то имеет место утверждение 2 леммы. В остальных случаях для каждого $g \in G$ найдется такой элемент $r \in C_G(j)$, что $rg \in FC(G)$. Но тогда $G = C_G(j)FC(G)$, и лемма доказана.

Покажем, что теорема 7 верна. Когда G — конечная группа, ее утверждения легко следуют из известных теорем Фробениуса и Бернсайда. Пусть группа G бесконечна. Поскольку H конечна, обособлена в G и содержит инволюцию j, то $H \cap FC(G) = 1$ и ввиду леммы Дицмана и теорем Силова в $FC(G)$ нет инволюций. По лемме 2 $G = C_G(j)FC(G)$, и мы заключаем, что $C_G(j) = H$, $G = FC(G) \leftthreetimes H$.

Докажем, что в группе $B = FC(G) \leftthreetimes \langle j \rangle$ инволюция j почти совершенна. Если в $FC(G)$ периодическая часть $T(G)$ нетривиальна, то $T(G) \leftthreetimes H$ — локально конечная группа Фробениуса и в силу теоремы Бернсайда инволюция j единственна в H. Но тогда $J \subset B$ и почти совершенность j в B следует из ее определения. Пусть $FC(G)$ — группа без кручения. Тогда по известной теореме Шура [18] $FC(G)$ — абелева группа. Допустим, что $t \in j^G \setminus j^B$, $k \in J$ и $j^k = t$. Тогда $b = jkjk \in FC(G)$, $|G : C_G(b)| < |H|$ и $H \cap C_G(b) \neq 1$. Противоречие. Следовательно, j почти совершенна в B и в этом случае.

По лемме 1, примененной к B, группа $FC(G)$ абелева и j инвертирует каждый элемент из $FC(G)$. Наконец, каждая инволюция из H инвертирует подходящий неединичный элемент из $FC(G)$ и поскольку H обособлена в G, то инволюция j единственна в H. Теорема доказана.

7. Доказательство теоремы 13

Пусть группа G — минимальный относительно $|C_G(j)|$ контрпример к теореме 13.

Лемма 3. *Пусть V — конечная нормальная подгруппа группы G. Тогда для факторгруппы $\overline{G} = G/V$ и инволюции $\overline{j}$ выполняются все условия теоремы* 13, *полный прообраз подгруппы $FC(\overline{G})$ в группе G совпадает с $FC(G)$ и, если теорема* 13 *верна для $\overline{G}$, то она верна и для группы G.*

Д о к а з а т е л ь с т в о. По предложениям 2 и 4, $|C_{\overline{G}}(\overline{j})| \leq |C_G(j)|$ и инволюция $\overline{j}$ почти совершенна в факторгруппе $\overline{G}$. Следовательно, для пары $(\overline{G}, \overline{j})$ условия теоремы 13 верны. Элемент $\overline{g}$ принадлежит $FC(\overline{G})$ в том и только том случае, если $|\overline{g}^{\overline{G}}| < \infty$. Так как для любого прообраза g элемента $\overline{g}$ имеет место неравенство $|g^G| \leq |V| \cdot |\overline{g}^{\overline{G}}|$, то $g \in FC(G)$ и полный прообраз подгруппы $FC(\overline{G})$ в группе G совпадает с $FC(G)$.

Далее, пусть для пары $(\overline{G}, \overline{j})$ теорема 13 верна. Поскольку в каждом смежном классе по $[jV, gV]$ содержится элемент $[j, g]$, то полный прообраз подгруппы $[\overline{j}, \overline{G}]$ в G содержит подгруппу $[j, G]$ и $[j, G] \leq FC(G)$. На основании леммы 2 заключаем, что $G = FC(G)C_G(j)$. Таким образом, утверждение (1) теоремы 13 справедливо и для группы G.

Докажем утверждение (2) теоремы 13. Пусть $\overline{R}$ — разрешимая ступени n нормальная в $\overline{G}$ подгруппа конечного индекса, R — ее полный прообраз и $C = C_R(V)$. Тогда C нормальна в G, имеет в ней конечный индекс и разрешима ступени не выше $n + 1$. Лемма доказана.

Каждая максимальная 2-подгруппа группы называется ее силовской 2-подгруппой. Пусть Q — некоторая силовская 2-подгруппа из $FC(G)$.

Лемма 4. *Если Q конечна, теорема* 13 *верна.*

Д о к а з а т е л ь с т в о. По условиям множество $Q \cup (C_G(j) \cap FC(G))$ конечно, состоит из элементов конечного порядка и в силу леммы Дицмана его нормальное замыкание T в G конечно. Обозначим $\overline{G} = G/T$. Если $|C_{\overline{G}}(\overline{j})| < |C_G(j)|$, то в силу индуктивного предположения и леммы 3 теорема 13 верна. Пусть $|C_{\overline{G}}(\overline{j})| = |C_G(j)|$. Тогда ввиду предложения 2 подгруппа T абелева, инвертируется каждой инволюцией из j^G и содержится в $Z([j, G])$. Как и в лемме 3, докажем, что $FC(\overline{G}) = FC(G)/T$. Понятно, что $FC(\overline{G}) \cap C_{\overline{G}}(\overline{j}) = \overline{1}$. По лемме 2 $\overline{G} = C_{\overline{G}}(\overline{j})FC(\overline{G})$, и поскольку $|C_{\overline{G}}(\overline{j})| = |C_G(j)|$, то $G = C_G(j)\ FC(G)$, $[j, G] \leq FC(G)$, и утверждение (1) теоремы 13 доказано.

Как вытекает из леммы Дицмана, элементы конечного порядка в $FC(\overline{G})$ составляют характеристическую подгруппу $\overline{B}$. Поскольку $C_{\overline{B}}(\overline{j}) = \overline{1}$, то $\overline{B}$ — абелева группа. По теореме Шура [18] факторгруппа $\overline{G}/\overline{B}$ — абелева группа без кручения. Итак, в этом случае FC-радикал группы $\overline{G}$ разрешим ступени 2, а $FC(G)$ — ступени 3. Поскольку $[G : FC(G)] < |C_G(j)|$, утверждение (2) теоремы 13 также верно. Лемма доказана.

Лемма 5. *Если подгруппа Q бесконечна, то верны следующие утверждения.*

1. *Q — черниковская группа с полной частью $\widetilde{Q}$, $Q \leq Z(FC(G))$ и Q совпадает с полной частью каждой силовской 2-подгруппы из $FC(G)$.*

2. *Подгруппа $\widetilde{Q}$ нормальна в G и $|C_{G/\widetilde{Q}}(j\widetilde{Q})| < |C_G(j)|$, в частности, для факторгруппы $G/\widetilde{Q}$ и ее инволюции $j\widetilde{Q}$ теорема* 13 *верна.*

3. *Силовские 2-подгруппы факторгруппы $G/\widetilde{Q}$ конечны.*

Д о к а з а т е л ь с т в о. 1. В силу леммы Дицмана $FC(G)$ обладает локально конечной периодической частью T. По теореме Шмидта группа $B = T \leftthreetimes \langle j \rangle$ локально конечна и инволюция j обязана содержаться в некоторой бесконечной силовской 2-подгруппе S группы B. По известной теореме Блэкберна S — черниковская группа, и поскольку в ее полной части $\widetilde{S}$ нет подгрупп конечного индекса, то $\widetilde{S}$ содержится в центре группы $FC(G)$, инвертируется инволюцией j и, очевидно, совпадает с полной частью каждой силовской 2-подгруппы из $FC(G)$. Утверждение 1 доказано.

2. Из утверждения 1 леммы выводим, что $\widetilde{Q} \triangleleft G$, $j^{\widetilde{Q}} = j\widetilde{Q}$, $C_{G/\widetilde{Q}}(j\widetilde{Q}) = C_G(j)\widetilde{Q}/\widetilde{Q}$ и $|C_{G/\widetilde{Q}}(j\widetilde{Q})| < |C_G(j)|$. Утверждение 2 леммы доказано.

3. В силу предложения 4 и индуктивного предположения для факторгруппы $G/\widetilde{Q}$ и ее инволюции $j\widetilde{Q}$ теорема верна. Пусть $\overline{A}$ — максимальная полная абелева 2-подгруппа факторгруппы $G/\widetilde{Q}$. Тогда $\overline{A}$ нормальна в $\overline{G}$ и инвертируется инволюцией $\overline{j}$. Следовательно, полный прообраз A группы $\overline{A}$ есть нормальная в G полная абелева 2-подгруппа, инвертируемая инволюцией j. По теореме Блэкберна A — черниковская группа, и поскольку она нормальна в G, то $A \leq FC(G)$ и $A = \widetilde{Q}$. Значит, силовские 2-подгруппы факторгруппы $G/\widetilde{Q}$ конечны. Утверждение 3 леммы доказано.

Завершим доказательство теоремы 13. В силу лемм 4, 5 считаем, что силовская 2-подгруппа $Q = \widetilde{Q}$ в $FC(G)$ является черниковской полной абелевой подгруппой. Согласно индуктивному предположению и лемме 5 силовские 2-подгруппы в $\overline{G} = G/\widetilde{Q}$ конечны и теорема для факторгруппы $\overline{G} = G/\widetilde{Q}$ и инволюции $j\widetilde{Q}$ верна. Отсюда заключаем, что объединение всех квазициклических 2-подгрупп в G порождает нормальную подгруппу $\widetilde{Q}$ и $\overline{G}$ обладает разрешимой нормальной подгруппой $\overline{B}$. Полный прообраз B группы $\overline{B}$ будет искомой разрешимой нормальной в G подгруппой конечного индекса, и теорема доказана.

Поступила 15.08.2006

СПИСОК ЛИТЕРАТУРЫ

1. **Попов А.М., Созутов А.И., Шунков В.П.** Группы с системами фробениусовых подгрупп. Красноярск: ИПЦ КГТУ, 2004.
2. **Мазуров В.Д.** О точно дважды транзитивных группах // Вопросы алгебры и логики: Тр. Ин-та математики СО РАН. Новосибирск. 1996. Т. 30. С. 114–118.
3. **Wähling H.** Theorie der Fastkörper. Essen: Thalen Verlag, 1987.
4. **Холл М.** Теория групп. М.: ИЛ, 1962.
5. **Созутов А.И.** О парах Фробениуса с совершенными инволюциями // Алгебра и логика. 2005. Т. 44, № 6. С. 751–762.
6. **Шунков В.П.** О некотором обобщении теоремы Фробениуса на периодические группы // Алгебра и логика. 1967. Т. 6, № 3. С. 113–124.
7. **Шунков В.П.** Группы с конечной вложенной инволюцией // Алгебра и логика. 1990. Т. 29, № 1. С. 102–123.
8. **Шунков В.П.** О периодических группах с почти регулярной инволюцией // Алгебра и логика. 1972. Т. 11, № 4. С. 470–494.
9. **Brauer R., Suzuki M., Wall G.E.** A characterization of the one-dimensional unimodular projective groups over finite fields // Ill. J. Math. 1958. V. 2, no. 3. P. 718–742.
10. **Suzuki M.** On characterizations of linear groups // Trans. Amer. Math. Soc. 1959. V. 92, no. 2. P. 191–219.
11. **Мазуров В.Д.** О бесконечных группах с абелевыми централизаторами инволюций // Алгебра и логика. 2000. Т. 39, № 1. С. 74–86.
12. **Созутов А.И., Крюковский А.С.** О группах с элементарными абелевыми централизаторами инволюций // Алгебра и логика, в печати.
13. **Сучков Н.М.** О периодических группах с абелевыми централизаторами инволюций // Мат. сборник. 2002. Т. 193, № 2. С. 153–160.
14. **Беляев В.В.** Группы с почти регулярной инволюцией // Алгебра и логика // 1987. Т. 26, № 5. С. 531–535.
15. **Созутов А.И.** О группах с почти регулярной инволюцией // Алгебра и логика, в печати.
16. **Курош А.Г.** Теория групп. М.: Наука, 1967.
17. **Каргаполов М.И., Мерзляков Ю.И.** Основы теории групп. М.: Наука, 1982.
18. **Горчаков Ю.М.** Группы с конечными классами сопряженных элементов. М.: Наука, 1978.

ТРУДЫ ИНСТИТУТА МАТЕМАТИКИ И МЕХАНИКИ УрО РАН

Том 13 № 1 2007

THE INFLUENCE OF s-SEMIPERMUTABLE SUBGROUPS ON THE STRUCTURE OF FINITE GROUPS[1]

Na Tang, Wenbin Guo, V. V. Kabanov

A subgroup H of a group G is called s-semipermutable in G if H is permutable with every Sylow p-subgroup of G with $(p, |H|) = 1$. In this paper, we use s-semipermutable subgroups to determine the structure of finite groups. Some of the previous results are generalized.

1. Introduction

The influence of minimal subgroups on the structure of finite groups is of considerable interest to many scholars. N. Ito [8] proved that, for an odd prime p, a group G is p-nilpotent if all elements of G of order p lie in the center of G, and that G is 2-nilpotent if all elements of G of order 2 or 4 lie in the center of G. J. Buckley [2] proved that if G is a group of odd order and all minimal subgroups of G are normal in G, then G is supersoluble. Later, W.E. Deskins, M. Asaad, P. Csorgo, etc. used s-quasinormal subgroups to study the structure of finite groups [1, 4]. Recall that a subgroup H is called s-quasinormal in G if H is permutable with every Sylow subgroup Q of G, that is, $QH = HQ$ [9]. Chongmu Chen [3] gave the definition of s-semipermutable (or s-seminormal) subgroup: a subgroup H is called *s-semipermutable* in G if $HP = PH$ for every Sylow p-subgroup P of G with $(p, |H|) = 1$. Recently, Qinhai Zhang and Lifang Wang [17] proved that $G \in \mathfrak{F}$ if and only if there exists a normal subgroup N such that $G/N \in \mathfrak{F}$ and all minimal subgroups and all subgroups of order 4 of N are s-semipermutable in G, where $\mathfrak{F}$ is a saturated formation containing all supersoluble groups. At the same time, they also found that $G \in \mathfrak{F}$ if and only if there exists a normal subgroup N such that $G/N \in \mathfrak{F}$ and every maximal subgroup of a Sylow subgroup is s-semipermutable in G, where $\mathfrak{F}$ is a saturated formation containing all the class of supersoluble groups.

As a development of the above results, in this paper we use s-semipermutable subgroups to study the structure of finite groups. In particular, some new criteria for supersoluble groups, p-nilpotent groups and, more than that, for groups in a given saturated formation are obtained, and some known results were generalized.

All the groups considered in this paper are finite. All unexplained notation and terminology are standard and can be found in Guo [6] and Shemetkov [12].

2. Elementary properties

A class $\mathfrak{F}$ of groups is called a *formation* if $\mathfrak{F}$ satisfies the following two conditions:

(1) if $G \in \mathfrak{F}$ and $N \trianglelefteq G$, then $G/N \in \mathfrak{F}$;

(2) if $G/N \in \mathfrak{F}$ and $G/M \in \mathfrak{F}$, then $G/(M \cap N) \in \mathfrak{F}$.

[1]Research of the authors are supported by NNSF Grant of China (project no. 10471118) and the International Joint Research Fund between NSFC and RFBR (project no. 05-01-39000).

It is clear that in a nonempty formation $\mathfrak{F}$ every group G has the smallest normal subgroup N (denoted by $G^{\mathfrak{F}}$) such that the quotient group G/N belongs to $\mathfrak{F}$. The normal subgroup $G^{\mathfrak{F}}$ is called the $\mathfrak{F}$-residual of G. A formation $\mathfrak{F}$ is said to be a saturated formation if $G \in \mathfrak{F}$ whenever $G/\Phi(G) \in \mathfrak{F}$. It is well known that the class $\mathfrak{N}$ of all nilpotent groups and the class $\mathfrak{U}$ of all supersoluble groups are both saturated formations.

For a formation $\mathfrak{F}$, we set $\pi(\mathfrak{F}) = \bigcup_{G\in\mathfrak{F}} \pi(G)$ and call it the *characteristic* of $\mathfrak{F}$. A normal factor H/K of a group G is said to be $\mathfrak{F}$-central in G if $[H/K](G/C_G(H/K)) \in \mathfrak{F}$. A normal subgroup N of a group is said to be $\mathfrak{F}$-hypercenter in G if every G-chief factor of N is $\mathfrak{F}$-central in G. It is easy to check that the product of any two $\mathfrak{F}$-hypercentral normal subgroups of a group G is again an $\mathfrak{F}$-hypercentral normal subgroup of G. We denote by $Z_\infty^{\mathfrak{F}}(G)$ the product of all nonidentity $\mathfrak{F}$-hypercentral normal subgroups of a group G; $Z_\infty^{\mathfrak{F}}(G)$ is called the $\mathfrak{F}$-hypercenter of G.

The product of all nilpotent normal subgroups of a group G is also a nilpotent normal subgroup, denoted by $F(G)$, which is called the Fitting subgroup of G. Let $C = C_G(F(G))$, $Z = Z(F(G))$, and $M/Z = \mathrm{Soc}\ (C/Z)$. We call $F^*(G) = MF(G)$ the generalized Fitting subgroup of G (cf. [16]). It is well known that if G is a soluble group, then $F^*(G) = F(G)$.

A subgroup H of G is called a semipermutable subgroup if $HK = KH$ for every subgroup K such that $(|H|, |K|) = 1$. A subgroup H of G is called an s-semipermutable subgroup of G if $HP = PH$ for every Sylow p-subgroup P of G such that $(p, |H|) = 1$ (cf. [3]).

A group G is called a CLT-group if there exists a subgroup of order m, for an arbitrary m, such that $m \mid |G|$. If every quotient group of G is a CLT-group, then G is called a QCLT-group (cf. [3]).

For convenience, we list here some of the known results which will be useful in the sequel.

Lemma 2.1 ([17]). *Let H be an s-semipermutable subgroup of G.*

(1) *If $H \le T \le G$, then H is s-semipermutable in T.*

(2) *If H is a p-subgroup and $H \trianglelefteq G$, then HK/K is s-semipermutable in G/K.*

Lemma 2.2 (cf. [7, Lemma 5]**).** *Let $\mathfrak{F}$ be an S-closed local formation and H be a subgroup of G. Then $H \cap Z_\infty^{\mathfrak{F}}(G) \subseteq Z_\infty^{\mathfrak{F}}(H)$.*

Recall that a group G is said to be an outer-supersoluble if every proper quotient of G is supersoluble but G is not supersoluble.

Lemma 2.3 ([15, Lemma 2.3]). *If G is an outer-supersoluble group and a QCLT-group, then $\Phi(G) = 1$ and*

(1) *$F(G)$ is a unique minimal normal subgroup of G and $C_G(F(G)) = F(G)$;*

(2) *$G = AF(G)$ and $A \cap F(G) = 1$ for some maximal supersoluble subgroup A of G;*

(3) *$F(G)$ is an acyclic elementary Abelian 2-subgroup, $2^2 \le |F(G)| < |G_2|$, and $O_2(A) = 1$, where G_2 is a Sylow 2-subgroup of G;*

(4) *$[A_2, A_2] = 1$, $A' \le A_{2'}$, where A_2 is a Sylow 2-subgroup of A and $A_{2'}$ is a Hall $2'$-subgroup of A;*

(5) *$G' = A'F(G)$, and $F(G)$ is a Sylow 2-subgroup of G';*

(6) *If $|F(G)| = 4$, then $G \backsimeq S_4$.*

Lemma 2.4 ([15, Theorem 3.1]). *Let G be a QCLT-group and let one of the following conditions hold*:

(1) *the commutator subgroup G_2' of G_2 is normal in G, where G_2 is a Sylow 2-subgroup of G;*

(2) *G has a normal 2-complement.*

Then G is a supersoluble group.

Lemma 2.5 ([14, Theorem 3.2]). *Suppose that H is a normal subgroup of a group G such that G/H is nilpotent. Let every cyclic subgroup of order 4 of $F^*(H)$ be s-semipermutable in G. Then G is nilpotent if and only if every element of prime order of $F^*(H)$ is contained in $Z_\infty(G)$.*

Lemma 2.6. *If $\mathfrak{F}$ is a saturated formation, then $\mathfrak{N}_{\pi(\mathfrak{F})} \subseteq \mathfrak{F}$ and $Z_\infty(G) \subseteq Z_\infty^{\mathfrak{F}}(G)$.*

Proof. Since a saturated formation is a local formation, there exists a formation function f such that $\mathfrak{F} = LF(f) = \{G \mid G/C_G(G_i/G_{i-1}) \in f(p)$ for every chief factor G_i/G_{i-1} of G and every $p \in \pi(G_i/G_{i-1})\}$ (cf. [6, Theorem 3.1.11]). Now let $G \in \mathfrak{N}_{\pi(\mathfrak{F})}$. Then for every chief factor G_i/G_{i-1} of G and $p \mid |G_i/G_{i-1}|$, we have $G/C_G(G_i/G_{i-1}) = 1 \in f(p)$. Hence $G \in \mathfrak{F}$. The second statement is obvious.

Lemma 2.7. *Let G be a group. If every cyclic subgroup of order 4 of G is s-semipermutable in G and every minimal subgroup of G is contained in $Z_\infty(G)$, then G is nilpotent.*

Proof. Assume that the assertion is false and choose G to be a counterexample of minimal order.

Let K be a proper subgroup of G. Since every cyclic subgroup of K of order 4 is s-semipermutable in G, by Lemma 2.1 every cyclic subgroup of K of order 4 is s-semipermutable in K.

Every minimal subgroup of K, being a minimal subgroup of G, by assumption is contained in $Z_\infty(G)$ and hence in $K \cap Z_\infty(G)$ and then by Lemma 2.2 in $Z_\infty(K)$.

Thus, K is a nilpotent group by the choice of G. This means that G is a Schmidt group. By [6, Theorem 3.4.11], G has the following properties:

- G is a soluble biprime group (i.e., $|\pi(G)| = 2$);
- $G^{\mathfrak{N}}$ is a Sylow q-subgroup of G for some $q \in \pi(G)$;
- $G/G^{\mathfrak{N}}$ is a cyclic p-subgroup, where $p \in \pi(G) \setminus \{q\}$;
- if $G^{\mathfrak{N}}$ is an Abelian group, then $G^{\mathfrak{N}}$ is an elementary Abelian group;
- if $q > 2$, then the exponent of $G^{\mathfrak{N}}$ is q; if $q = 2$, then the exponent of $G^{\mathfrak{N}}$ does not exceed 4.

Assume that $\exp(G^{\mathfrak{N}}) = q$; then $G^{\mathfrak{N}} \subseteq Z_\infty(G)$ and, consequently, G is nilpotent, a contradiction. If there exists an element x of order 4 in $G^{\mathfrak{N}} \setminus \Phi(G^{\mathfrak{N}})$, then by the s-semipermutability of $\langle x\rangle$ we have $\langle x\rangle G_p = G_p\langle x\rangle$ for any $G_p \in \mathrm{Syl}_p(G)$ and $p \neq 2$. Assume that $G = \langle x\rangle G_p$; then $G^{\mathfrak{N}} = \langle x\rangle$ is an Abelian group and consequently is an elementary Abelian group by (3), which is impossible. Hence, $\langle x\rangle G_p < G$ and so $\langle x\rangle G_p$ is nilpotent. It follows that $\langle x\rangle \trianglelefteq \langle x\rangle G_p$. Therefore, $G_p \leq N_G(\langle x\rangle)$. Since G_p is arbitrary, it follows that $O^2(G) \leq N_G(\langle x\rangle)$. If $N_G(\langle x\rangle) = G$, then $\langle x\rangle \trianglelefteq G$ and so $\langle x\rangle\Phi(G^{\mathfrak{N}})/\Phi(G^{\mathfrak{N}}) = G^{\mathfrak{N}}/\Phi(G^{\mathfrak{N}})$. This induces that $G^{\mathfrak{N}} = \langle x\rangle$, again a contradiction. Thus, $N_G(\langle x\rangle) < G$. Since $G/O^2(G) = G^{\mathfrak{N}}O^2(G)/O^2(G) \simeq G^{\mathfrak{N}}/G^{\mathfrak{N}} \cap O^2(G) \in \mathfrak{N}$, we have $G^{\mathfrak{N}} \subseteq O^2(G)$. Thus, $G = G^{\mathfrak{N}}O^2(G) = O^2(G) \leq N_G(\langle x\rangle) < G$. The final contradiction completes the proof.

3. Main Results

Theorem 3.1. *Let $\mathfrak{F}$ be a saturated formation such that $\pi(\mathfrak{F})=\mathbb{P}$. Then a group G belongs to $\mathfrak{F}$ if and only if there exists a normal subgroup N of G such that $G/N \in \mathfrak{F}$, any minimal subgroup of N is contained in the $\mathfrak{F}$-hypercenter $Z_\infty^{\mathfrak{F}}(G)$ of G, and any cyclic subgroup of N of order 4 is s-semipermutable in G.*

Proof. The necessity is obvious, we only need to prove the sufficiency. Assume it is false and choose G to be a counterexample of minimal order.

Let x be an element of prime order of $G^{\mathfrak{F}}$. Since, obviously, $G^{\mathfrak{F}} \subseteq N$, we have $x \in Z_{\infty}^{\mathfrak{F}}(G) \cap G^{\mathfrak{F}} \subseteq Z(G^{\mathfrak{F}})$ by [5, IV, 6.10]. Then, by Lemma 2.7, $G^{\mathfrak{F}}$ is nilpotent.

Since $\mathfrak{F}$ is a saturated formation, $G^{\mathfrak{F}} \nsubseteq \Phi(G)$. Let M be an arbitrary maximal subgroup M of G such that $G = MG^{\mathfrak{F}} = MF(G)$. We prove that $M \in \mathfrak{F}$. We first claim that $G^{\mathfrak{F}} \cap M \trianglelefteq G$. In fact, we may consider a minimal normal subgroup T of G with $T \leq G^{\mathfrak{F}}$. If $T \leq M$, then $G^{\mathfrak{F}}/T \cdot M/T = G/T$. By induction, we find that $(G^{\mathfrak{F}}/T) \cap (M/T) \trianglelefteq G/T$. Thus, $G^{\mathfrak{F}} \cap M \trianglelefteq G$. If $T \nleq M$, then $G = MT$. Since $G^{\mathfrak{F}} \cap M \leq G^{\mathfrak{F}} \leq F(G) \leq C_G(T)$, we also have $G^{\mathfrak{F}} \cap M \trianglelefteq G$.

Now, we prove that $Z_{\infty}^{\mathfrak{F}}(G) \leq M$. Assume that $G^{\mathfrak{F}} \cap M \neq 1$. Since $(G/M \cap G^{\mathfrak{F}})/(M/M \cap G^{\mathfrak{F}})_{(G/M\cap G^{\mathfrak{F}})} = (G/M \cap G^{\mathfrak{F}})/(M_G/M \cap G^{\mathfrak{F}}) \simeq G/M_G \notin \mathfrak{F}$, we can find, by induction, that $Z_{\infty}^{\mathfrak{F}}(G/M \cap G^{\mathfrak{F}}) \leq M/M \cap G^{\mathfrak{F}}$. In view of $Z_{\infty}^{\mathfrak{F}}(G)(M \cap G^{\mathfrak{F}})/(M \cap G^{\mathfrak{F}}) \leq Z_{\infty}^{\mathfrak{F}}(G/(M \cap G^{\mathfrak{F}}))$, we have $Z_{\infty}^{\mathfrak{F}}(G) \leq M$. If $M \cap G^{\mathfrak{F}} = 1$, then $G = [G^{\mathfrak{F}}]M$. Moreover, $M \simeq G/G^{\mathfrak{F}} \in \mathfrak{F}$. In this case, we have $Z_{\infty}^{\mathfrak{F}}(G) \leq M$. (If not, then $G = Z_{\infty}^{\mathfrak{F}}(G)M$. Since $G/Z_{\infty}^{\mathfrak{F}}(G) = MZ_{\infty}^{\mathfrak{F}}(G)/Z_{\infty}^{\mathfrak{F}}(G) \simeq M/(M \cap Z_{\infty}^{\mathfrak{F}}(G)) \in \mathfrak{F}$, we obtain that $G \in \mathfrak{F}$, a contradiction.) Then, since $[G^{\mathfrak{F}}, Z_{\infty}^{\mathfrak{F}}(G))] = 1$ by [5, IV, 6.10], we see that every G-chief factor A/B below $Z_{\infty}^{\mathfrak{F}}(G)$ is actually an M-chief factor. Since $F(G) \leq C_G(A/B)$, we have $MC_G(A/B)/C_G(A/B) = G/C_G(A/B) \simeq M/C_M(A/B)$. It follows that $Z_{\infty}^{\mathfrak{F}}(G) \leq Z_{\infty}^{\mathfrak{F}}(M)$. Whence, using Lemma 2.1, we conclude that M satisfies the hypotheses of the theorem. The minimal choice of G implies that $M \in \mathfrak{F}$. Therefore, by [6, Theorem 3.4.2], the following conditions hold:

- $G^{\mathfrak{F}}$ is a p-group for some prime p;
- $G^{\mathfrak{F}}/\Phi(G^{\mathfrak{F}})$ is a chief factor of G;
- if $G^{\mathfrak{F}}$ is an Abelian group, then $G^{\mathfrak{N}}$ is an elementary Abelian group;
- if $p > 2$, then the exponent of $G^{\mathfrak{N}}$ is p; if $p = 2$, then the exponent of $G^{\mathfrak{N}}$ is 2 or 4.

If $G^{\mathfrak{F}}$ is an elementary Abelian group, then $G^{\mathfrak{F}} \leq Z_{\infty}^{\mathfrak{F}}(G)$ by the hypotheses; this implies $G \in \mathfrak{F}$, a contradiction. So we may assume that the exponent of $G^{\mathfrak{N}}$ is 4. Let $x \in G^{\mathfrak{F}} \setminus \Phi(G^{\mathfrak{F}})$ be such that $|x| = 2$. Let $K = \langle x \rangle^G$. Then $K \trianglelefteq G$ and $K \leq \Omega_1(G^{\mathfrak{F}}) \leq Z_{\infty}^{\mathfrak{F}}(G)$. On the other hand, $G^{\mathfrak{F}} = K\Phi(G^{\mathfrak{F}}) = K$ as $G^{\mathfrak{F}}/\Phi(G^{\mathfrak{F}})$ is a chief factor of G. It follows that $G^{\mathfrak{F}} \subseteq Z_{\infty}^{\mathfrak{F}}(G)$, a contradiction. This shows that $|x|$=4 for any $x \in G^{\mathfrak{F}} \setminus \Phi(G^{\mathfrak{F}})$. Because $G^{\mathfrak{F}} \nsubseteq \Phi(G)$, there exists a maximal subgroup of G such that $G = G^{\mathfrak{F}}M$. Since $\langle x \rangle$ is s-semipermutable in G by the hypotheses, $\langle x \rangle M_q = M_q\langle x \rangle$, where $M_q = G_q$ is a Sylow q-subgroup of M, for any $q \neq 2$. Since $\langle x \rangle$ is subnormal in $G^{\mathfrak{F}}$, $\langle x \rangle$ is subnormal in G. Hence $\langle x \rangle$ is subnormal in $\langle x \rangle M_q$, and consequently $M_q \leq N_G(\langle x \rangle)$. In other words, M_q may be regarded as an action group of $\langle x \rangle$ by conjugation. But the automorphism group of a cyclic group of order 4 is a cyclic group of order 2, so M_q acts trivially on $\langle x \rangle$. This shows that $\langle x \rangle$ is centralized by $O^2(M)$, which implies that $G^{\mathfrak{F}}$ is centralized by $O^2(M)$. Hence $O^2(M) \trianglelefteq G$, as $G = MG^{\mathfrak{F}}$. It follows that G/M_G is a 2-group. Since $\pi(\mathfrak{F}) = \mathbb{P}$, we have $\mathfrak{N} \subseteq \mathfrak{F}$ by Lemma 2.6. This induces that $G/M_G \in \mathfrak{F}$, and consequently, $G = G^{\mathfrak{F}}M = M$. The final contradiction completes the proof.

Theorem 3.1 immediately implies the following corollary.

Corollary 3.1.1. *Let $\mathfrak{F}$ be a saturated formation with $\pi(\mathfrak{F}) = \mathbb{P}$. Then $G \in \mathfrak{F}$ if and only if every element of prime order of $G^{\mathfrak{F}}$ is contained in $Z_{\infty}^{\mathfrak{F}}(G)$ and every cyclic subgroup of order 4 of $G^{\mathfrak{F}}$ are s-semipermutable in G.*

Since the class of all p-nilpotent groups and the class of all nilpotent groups are saturated formations with characteristic $\mathbb{P}$ and an s-quasinormal subgroup of G is s-semipermutable in G, by Theorem 3.1 we also can directly obtain the following results in [11].

Corollary 3.1.2 ([11, Theorem 4.3]). *Let N be a normal subgroup of a group G such that G/N is p-nilpotent, where p is a fixed prime. Suppose every element of prime order of N is contained in $Z_\infty(G)$ and every cyclic subgroup of order 4 of N is s-quasinormal in G. Then G is p-nilpotent.*

Corollary 3.1.3 ([11, Theorem 4.4]). *Let N be a normal subgroup of a group G such that G/N is nilpotent. Suppose every element of prime order of N is contained in $Z_\infty(G)$ and every cyclic subgroup of order 4 of N is s-quasinormal in G. Then G is nilpotent.*

Corollary 3.1.4 ([11, Theorem 4.2]). *Suppose G is a group. If every cyclic subgroup of order 4 is s-quasinormal in G and every minimal subgroup is contained in $Z_\infty(G)$, then G is nilpotent.*

Theorem 3.2. *Let $\mathfrak{F}$ be a saturated formation with $\pi(\mathfrak{F}) = \mathbb{P}$ and G be a group such that every cyclic subgroup of $F^*(G^{\mathfrak{F}})$ of order 4 is s-semipermutable in G. Then $G \in \mathfrak{F}$ if and only if every element of prime order of $F^*(G^{\mathfrak{F}})$ is contained in $Z_\infty^{\mathfrak{F}}(G)$.*

Proof. If $G \in \mathfrak{F}$, then $Z_\infty^{\mathfrak{F}}(G) = G$. Thus the necessity is obvious, we only need to prove the sufficiency.

By the hypotheses and [5, IV,6.10], for all subgroups P of prime order of $F^*(G^{\mathfrak{F}})$, we have $P \leqslant Z_\infty^{\mathfrak{F}}(G) \cap G^{\mathfrak{F}} \leqslant Z(G^{\mathfrak{F}}) \leqslant Z_\infty(G^{\mathfrak{F}})$. By Lemma 2.1 every cyclic subgroup of order 4 of $F^*(G^{\mathfrak{F}})$ is s-semipermutable in $G^{\mathfrak{F}}$. It follows from Lemma 2.5 that $G^{\mathfrak{F}}$ is nilpotent. Therefore, $F^*(G^{\mathfrak{F}}) = F(G^{\mathfrak{F}}) = G^{\mathfrak{F}}$. By the hypotheses, every element of prime order of $G^{\mathfrak{F}}$ is contained in $Z_\infty^{\mathfrak{F}}(G)$ and every subgroup of order 4 of $G^{\mathfrak{F}}$ is s-semipermutable in G, hence, by Corollary 3.1.1, we get $G \in \mathfrak{F}$. This contradiction completes the proof.

Since s-quasinormal subgroups are s-semipermutable subgroups and $\mathfrak{N} \subseteq \mathfrak{F}$ implies that $\pi(\mathfrak{F}) = \mathbb{P}$, by our Theorem 3.2, we also obtain Theorem 4.7 in [11].

Corollary 3.2.1 ([11, Theorem 4.7]). *Let $\mathfrak{F}$ be a saturated formation such that $\mathfrak{N} \subseteq \mathfrak{F}$. Let G be a group such that every cyclic subgroup of $F^*(G^{\mathfrak{F}})$ of order 4 is s-quasinormal in G. Then $G \in \mathfrak{F}$ if and only if every element of prime order of $F^*(G^{\mathfrak{F}})$ is contained in $Z_\infty^{\mathfrak{F}}(G)$.*

Theorem 3.3. *Let G is a QCLT-group. If the derived subgroup G_2' of a Sylow 2-subgroup G_2 of G is s-semipermutable in G, then G is a supersoluble group.*

Proof. Assume that the claim is false and let G be a counterexample of minimal order. By Lemma 2.1, we easily see that the quotient groups of G satisfy the hypotheses. The choice of G implies that G is an outer-supersoluble group. By Lemma 2.3, it follows that $G = AF(G)$ with $A \cap F(G) = 1$ and $F(G)$ is a 2-group. Then $G_2 = G_2 \cap AF(G) = (A \cap G_2)F(G)$, and by Lemma 2.3(2), we have $G_2/F(G) \simeq A \cap G_2$. Moreover, by Lemma 2.3(4), we have $G_2' \leq F(G)$.

(1) If $G_2' = 1$ or $G_2' = F(G)$, then by Lemma 2.4, G is supersoluble, a contradiction.

(2) Now assume that $1 < G_2' < F(G)$. Since $F(G)$ is a 2-group, for every $q \neq 2$, every Sylow q-subgroup of A is also a Sylow q-subgroup of G. Let $A_{p_1}, A_{p_2}, \cdots, A_{p_m}$ be a Sylow basis of A. In view of s-semipermutability of G_2' in G, we obtain $G_2'A_{p_i} = A_{p_i}G_2'$ for all odd p_i, $i = 1, 2, \cdots, m$. Moreover, $G_2' \trianglelefteq G_2$, we have $G_2'A \leq G$. This shows that $A < G_2'A < G$, which contradicts the maximality of A. The proof is complete.

Recall that a subgroup H of G is seminormal [13] in G if there exists a subgroup K such that $HK = G$ and $HK_1 < G$ for an arbitrary proper subgroup K_1. By [10], a seminormal subgroup is a semipermutable subgroup. Thus, our Theorem 3.3 implies Theorem 3.4 in [15].

Corollary 3.3.1 ([15, Theorem 3.4]). *Let G be a QCLT-group. If the commutative subgroup G_2' of a Sylow 2-subgroup G_2 of G is seminormal in G, then G is supersoluble.*

Received November 8, 2006

BIBLIOGRAPHY

1. **Assad M., Csorgo P.** The Influence of Minimal Subgroups on the Structure of Finite Groups // Arch. Math. 1999. V. 72. P. 401–404.
2. **Buckley J.** Finite Group Whose Minimal Subgroups Are Normal // Math. Z. 1970. V. 116. P. 15–17.
3. **Chen Chongmu.** Inner-outer Σ-groups and Minimal non-Σ-groups. Chongqing: Southwest Normal University Press, 1988.
4. **Deskins W.E.** On Quasinormal Subgroups of Finite Groups // Math. Z. 1963. V. 82. P. 125–132.
5. **Doek K., Hawkes T.** Finite Soluble Groups. Berlin—New York: Walter de Gruyter, 1992.
6. **Guo Wenbin.** The Theory of Classes of Groups. Beijing: Science Press; New York and etc.: Kluwer Academic Publishers, 2000.
7. **Guo Wenbin.** The Influence of Minimal Subgroups on the Structure of Finite Groups // Southeast Asian Bull. Math. 1998. V. 22. P. 287–290.
8. **Ito N.** Über eine zur Frattini-Gruppe duale Bildung // Nagoya Math. J. 1955. V. 9. P. 123–127.
9. **Kegel O.H.** Sylow-Gruppen and Subnormalteiler Endlicher Gruppen // Math. Z. 1962. V. 78. P. 205–221.
10. **Li Q.** Minimal Subgroups and Supersolvablity // J. Math. 1996. V. 16 (2). P. 129–132.
11. **Li Yangming, Wang Yanming.** On π-Quasinormally Embedded Subgroups of Finite Groups // J. Algebra. 2004. V. 281. P. 109–123.
12. **Shemetkov L.A.** Formations of Finite Groups // Moscow: Nauka, 1978.
13. **Su X.** s-Seminormal Subgroups of Finite Groups // J. Math. 1988. V. 8 (1). P. 5–9.
14. **Tang Na, Guo Wenbin.** On s-Semipermutable Subgroups // Proceeding of the F. Scorina Gomel State University. 2006. No. 3 (36). P. 88-91.
15. **Wang P., Lu Z., Bian P.** On the Supersolvability of QCLT-Groups // Northeast. Math. 1996. V. 12 (1). P. 41–45.
16. **Xu M.** An Introduction to Finite Groups. Beijing: Science Press, 1999.
17. **Zhang Qinhai, Wang Lifang.** The Influence of s-Semipermutable Subgroups on the Structure of Finite Groups // J. Math. 2005. V. 48 (1). P. 81–88.

V. A. Antonov and S. G. Chekanov. **Double Frobenius Groups.** Trudy Inst. Mat. i Mekh. UrO RAN. 2007. Vol. 13, no. 1. P. 3–10.

Double Frobenius groups are studied. Some properties of a minimal counterexample to V.D. Mazurov's conjecture about these groups are obtained. Under some additional restrictions the conjecture is confirmed.

V. A. Belonogov. **Certain Pairs of Irreducible Characters of the Groups S_n and A_n.** Trudy Inst. Mat. i Mekh. UrO RAN. 2007. Vol. 13, no. 1. P. 11–43.

Investigation of pairs of semiproportional irreducible characters of finite groups is continued. The interest in these investigations is maintained by the discovered earlier connection between the presence or absence of such a pair in a group and the local structure of this group. In the paper, the question of the presence of such pairs in the alternating groups A_n is investigated. A more general problem of description of pairs of irreducible characters of the symmetric group S_n having the same set of roots in one of the sets A_n and $S_n \setminus A_n$ is also considered. All such pairs of irreducible characters of the symmetric group S_n have been found in the case when the main diagonal lengths of the Young diagrams corresponding to these characters do not exceed 2.

I. N. Belousov and A. A. Makhnev. **A Distance-Regular Graph with the Intersection Array** $\{8,7,5;1,1,4\}$
and Its Automorphisms. Trudy Inst. Mat. i Mekh. UrO RAN. 2007. Vol. 13, no. 1. P. 44–56.

Possible orders and subgraphs of the fixed points of a distance-regular graph with the intersection array $\{8,7,5;1,1,4\}$ are found. It is shown that such a graph is not vertex-transitive.

V. V. Bludov and B. V. Gusev. **Geometric Equivalence of Groups.** Trudy Inst. Mat. i Mekh. UrO RAN. 2007. Vol. 13, no. 1. P. 57–78.

Based on the notion of geometric equivalence of groups, new classes of groups, namely, geometric varieties of groups, are defined. Some properties of such classes, including their relation to quasi-varieties and prevarieties of groups, are studied. Examples of torsion free nilpotent groups that are geometrically nonequivalent to their minimal completions, as well as an example of centrally metabelian groups that are geometrically nonequivalent but generate equal quasi-varieties, are given.

A. P. Il'inykh[†]*.* **Quasifields Associated with an Automorphism of the Additive Group of a Finite Field.** Trudy Inst. Mat. i Mekh. UrO RAN. 2007. Vol. 13, no. 1. P. 99–101.

We propose a construction of finite quasifields based on using of special automorphisms of the additive groups of finite fields.

L. S. Kazarin. **Nilpotent Algebras and Their Applications.** Trudy Inst. Mat. i Mekh. UrO RAN. 2007. Vol. 13, no. 1. P. 102–114.

The work is devoted to the structure of finite nilpotent algebras and their applications, first of all, to the structure of products of groups. Some questions concerning the application of nilpotent algebras (and related structures) to the construction of recurrent sequences are touched upon.

A. V. Konygin. **Sets with Trivial Global Stabilizers for Prime Permutation Groups Which Are not Almost Simple.** Trudy Inst. Mat. i Mekh. UrO RAN. 2007. Vol. 13, no. 1. P. 115–131.

Let G be a primitive permutation group on a finite set X such that the global stabilizer of any subset of the set X in the group G is nontrivial. The description of G is obtained in the case when G is not almost simple.

K. V. Kostousov. **Cayley Graphs of the Group $\mathbb{Z}^4$ That Are Limits of Minimal Vertex-Primitive Graphs of Type HA.** Trudy Inst. Mat. i Mekh. UrO RAN. 2007. Vol. 13, no. 1. P. 132–147.

In the joint paper by Giudici, Li, Praeger, Seress, and Trofimov, it is proved that any graph that is a limit of vertex-primitive graphs of type HA is isomorphic to a Cayley graph of the group $\mathbb{Z}^d$. Earlier, the author proved that for $d \leq 3$ the number of pairwise nonisomorphic Cayley graphs of the group $\mathbb{Z}^d$, which are limits of minimal vertex-primitive graphs of type HA, is finite (and obtained their explicit description). The present paper includes the construction of a countable family of such graphs for the case $d = 4$; moreover, up to isomorphism there are only finitely many Cayley graphs of such a type outside this family.

A. A. Makhnev and M. S. Nirova. **Uniform Extensions of Partial Geometries.** Trudy Inst. Mat. i Mekh. UrO RAN. 2007. Vol. 13, no. 1. P. 148–157.

A geometry of rank 2 is an incidence system $(P, \mathcal{B})$, where P is a set of points and $\mathcal{B}$ is a set of subsets from P, called blocks. Two points are called collinear if they lie in a common block. A pair (a, B) from $(P, \mathcal{B})$ is called a flag if its point belongs to the block, and an antiflag otherwise. A geometry is called φ-uniform (φ is a natural number) if for any antiflag (a, B) the number of points in the block B collinear to the point a equals 0 or φ, and strongly φ-uniform if this number equals φ. In this paper, we study φ-uniform extensions of partial geometries $pG_\alpha(s, t)$ with $\varphi = s$ and strongly φ-uniform geometries with $\varphi = s - 1$. In particular, the results on extensions of generalized quadrangles, obtained earlier by Cameron and Fisher, are extended to the case of partial geometries.

V. D. Mazurov and A. V. Zavarnitsine. **On Element Orders in Coverings of the Simple Groups $L_n(q)$ and $U_n(q)$.** Trudy Inst. Mat. i Mekh. UrO RAN. 2007. Vol. 13, no. 1. P. 89–98.

We prove that if a finite simple linear or unitary group defined over a field of characteristic p and having dimension sufficiently large as compared with p acts on a finite-dimensional vector space over some field of the same characteristic p, then the corresponding semidirect product contains an element whose order is distinct from any element order of the simple group.

D. V. Paduchikh. **The Nonexistence of Locally $\bar{J}(10, 5)$-Graphs.** Trudy Inst. Mat. i Mekh. UrO RAN. 2007. Vol. 13, no. 1. P. 158–167.

In the paper, the nonexistence of graphs is proved for which the neighborhood of every vertex is isomorphic to the graph $\bar{J}(10, 5)$.

D. O. Revin. **The D_π Property of Finite Groups in the Case $2 \notin \pi$.** Trudy Inst. Mat. i Mekh. UrO RAN. 2007. Vol. 13, no. 1. P. 166–182.

The characterization of finite simple groups with the D_π property for any set π of odd prime numbers is completed. It was proved earlier that a finite group has the D_π property if and only if each of its composition factors has this property, hence the results of the paper provide an exhaustive characterization of the D_π property for all finite groups with known composition factors in the case $2 \notin \pi$.

A. I. Sozutov. **On Groups with Almost Perfect Involution.** Trudy Inst. Mat. i Mekh. UrO RAN. 2007. Vol. 13, no. 1. P. 183–190.

The theorems of Jordan, Frobenius, M. Hall, Brauer–Suzuki–Wall, Shunkov, Mazurov, and Belyaev are generalized.

Na Tang, Wenbin Guo, and V. V. Kabanov. **The Influence of s-Semipermutable Subgroups on the Structure of Finite Groups.** Trudy Inst. Mat. i Mekh. UrO RAN. 2007. Vol. 13, no. 1. P. 191–196.

A subgroup H of a group G is called s-semipermutable in G if H is permutable with every Sylow p-subgroup of G with $(p, |H|) = 1$. In this paper, we use s-semipermutable subgroups to determine the structure of finite groups. Some of the previous results are generalized.

E. P. Vdovin. **On the Existence of Carter Subgroups.** Trudy Inst. Mat. i Mekh. UrO RAN. 2007. Vol. 13, no. 1. P. 79–88.

In terms of normal series of a finite group, the existence criterion of a Carter subgroup is obtained. An example showing that the criterion cannot be reformulated in terms of composition factors is given. In conclusion, Carter subgroups in almost simple groups are classified.

Научное издание

ТРУДЫ
ИНСТИТУТА МАТЕМАТИКИ И МЕХАНИКИ УрО РАН

Сборник научных трудов

Рекомендовано к изданию Ученым советом
Института математики и механики
и НИСО Уральского отделения Российской академии наук

ЛР № 020764 от 24.04.98

Ответственные за выпуск: А. С. Кондратьев, С. И. Тарасова.
Литературный редактор: Е. Г. Понизовкина.
Технический редактор: Н. Н. Моргунова.

Оригинал-макет подготовлен в ИММ УрО РАН.

НИСО УрО РАН № 63(07).
Подписано в печать 7.06.2007. Формат $60 \times 84^1/_8$. Печать офсетная.
Усл. печ. л. 24,5. Уч.-изд. л. 19,25. Тираж 200 экз. Заказ 2390.

Институт математики и механики УрО РАН
620219 г. Екатеринбург, ГСП-384, ул. С. Ковалевской, 16

Отпечатано с готовых диапозитивов в типографии
ООО “Издательство Учебно-Методический центр — УПИ”
620002 г. Екатеринбург, ул. Мира, д.17, офис 226.