Известия Гомельского государственного университета имени
Ф.Скорины, 3(16) Вопросы алгебры (2000), 125–137
2000 Mathematics Subject Classification: 20D35

Критерий непростоты конечной группы

В.Н.Тютянов

Посвящается профессору В.Гашюцу в связи с его 80-летием

Подгруппы, порожденные элементами класса сопряженности, в большой степени определяют строение конечной группы. Поэтому естественно изучать конечные группы при определенных ограничениях на строение таких подгрупп.

В настоящей статье доказана:

Теорема. *Пусть G — конечная K-группа, в которой имеется элемент x такой, что $< x, x^g >$ — группа нечетного порядка для всякого $g \in G$. Тогда $x \in O(G)$.*

Таким образом, задача 11.1.2 [1], поставленная Л.С.Казариным, решена для K-групп.

Все рассматриваемые группы конечны. Основные обозначения и определения можно найти в [2–4]. Приведем тем не менее некоторые из них для удобства читателя. Под K-группой понимается группа все композиционные факторы которой являются известными простыми группами. Если $x_1, x_2, \dots, x_n \in G$, то $< x_1, x_2, \dots, x_n >$ — группа, порожденная элементами $x_1, x_2, \dots, x_n$. Запись $A * B$ означает центральное произведение групп A и B; $\pi(G)$ — множество всех простых делителей порядка группы G. Через $\mathrm{Syl}_p(G)$ будем обозначать множество всех силовских p-подгрупп группы G. $I(G)$ — множество всех инволюций группы G. Запись $M \subset \cdot\, G$ означает, что подгруппа M максимальна в G. $O(G)$ — наибольшая нормальная подгруппа нечетного порядка группы G, называемая её ядром. $L(G)$ — слой группы G.

Значительная часть доказательства теоремы связана с рассмотрением групп Шевалле, поэтому приведем еще ряд обозначений. Пусть X_l — простая алгебра Ли над полем комплексных чисел, l — ранг этой алгебры и $X = A, B, C, D, E, F$ или G — ее тип. Если $K = GF(q)$ — конечное поле характеристики p, то через $X_l(q)$ обозначается соответствующая группа Шевалле нормального типа; через ${}^rX_l(q)$ обозначается соответствующая группа Шевалле скрученного типа ($r \in \{2, 3\}$). Всюду где речь идет о группах Шевалле $G = X_l(q)$ или ${}^rX_l(q)$ фиксируем следующие обозначения. Φ — система корней евклидова пространства соответствующей размерности и соответствующего типа; Φ^+ — система положительных корней; Σ — система простых корней. Для корня $\alpha \in \Phi$ X_α является соответствующей корневой подгруппой. Отметим также следующие подгруппы: $U = < X_\alpha \mid \alpha \in \Phi^+ > \in \mathrm{Syl}_p(G)$, $N_G(U) \supseteq H$ — подгруппа Картана, $B = UH$ — подгруппа Бореля и $N/H = W$ — группа Вейля, где $N \subseteq N_G(H)$. Любая подгруппа в G, содержащая B, называется параболической.

При доказательстве теоремы мы будем неоднократно использовать теорему о несбалансированных группах:

(U-гипотеза). Пусть X — такая группа, что $Y = F^*(X)$ — простая группа. Если $O(C_X(t)) \neq 1$ для некоторой инволюции $t \in I(X)$, то справедливо одно из следующих утверждений:

(1) $Y \in Chev(p)$ *для некоторого нечетного простого числа* p;

(2) $Y \cong A_n$, *n нечетно;*

(3) $Y \cong L_3(4)$ *или группе Хельда.*

План изложения следующий. В §1 приведен ряд вспомогательных результатов. В §2 получены ограничения на строение минимального контрпримера к теореме. При этом устанавливается, что минимальный контрпример — либо простая неабелева группа, либо группа вида $M \leftthreetimes <x>$, где M — простая неабелева группа. Доказательство теоремы завершается в §§3–6 рассмотрением каждого из перечисленных выше случаев. Ссылаясь на лемму i из (другого) j-го параграфа, мы обозначаем ее так: лемма $(j.i)$, или просто $(j.i)$. Внутри параграфа обозначение обычное: лемма i.

§1. Вспомогательные результаты

В этом параграфе мы приведем утверждения, которые неоднократно будут использоваться в работе.

Лемма 1 (теорема Бэра). *Если D — сопряженный класс элементов простого порядка p в группе G, причем $< x, y >$ является p-группой для любой пары элементов $x, y \in D$, то $D \subseteq O_p(G)$.*

Доказательство. См. 2.66 [2].

Лемма 2. *Пусть X — группа Шевалле нечетной характеристики, не изоморфная $PSL_2(q)$, $t \in I(X)$ и $Y = O(C_X(t)) \neq 1$. Тогда $L(X)$ не может быть группой следующих типов: ${}^3D_4(q), E_8(q), F_4(q), G_2(q), {}^2G_2(q)$.*

Доказательство. Лемма на стр. 345 [5].

Лемма 3. *Пусть p — простое число и G — группа с циклической силовской p-подгруппой. Тогда G p-разрешима тогда и только тогда, когда любые два ее элемента порядка p порождают p-разрешимую группу.*

Доказательство. [6].

Лемма 4. *Пусть $\Sigma = \{r_1, r_2, \ldots, r_n\}$ — система простых корней конечной группы Шевалле G, $I \subseteq \{1, 2, \ldots, n\}$, $Q_I =< X_r \mid r \in \Phi^+$ и $r = \sum_{j=1}^{n} m_j r_j$ с $m_i > 0$ для некоторого $i \in I >$ и $L_I =< X_{r_i}, X_{-r_i} \mid i \notin I >$. Тогда:*

1. Параболические подгруппы группы G, содержащие ее подгруппу Бореля B, исчерпываются группами $G_I =< B, X_{-r_j} \mid j \notin I >$.

2. (a) $G_I = Q_I L_I H$ и H нормализует L_I;

(b) $Q_I = O_p(G_I)$ и $Q_I \bigcap L_I H = 1$;

(c) $N_G(Q_I) = G_I$;

(d) если $n \geq 2$, то L_I — центральное произведение групп Шевалле, каждая из которых находится по связной компоненте диаграммы Дынкина группы G, полученной отбрасыванием вершин, входящих в I.

Доказательство. См. (2.1), (2.2) [7].

Разложение G_I в полупрямое произведение Q_I и $L_I H$ называется разложением Леви, а подгруппа $L_I H$ и ее сопряженные в Q_I называются дополнениями Леви.

Лемма 5. *Пусть G — конечная группа Шевалле нормального типа. Пусть $x \in U$, $x \neq 1$. Тогда x сопряжен в G с элементом $x' = \prod_{\beta > 0} x_\beta(t_\beta)$, где $t_\beta \neq 0$ для некоторого $\beta \in \Sigma$.*

Доказательство. Лемма 1 [8].

Лемма 6. *Пусть G — конечная группа Шевалле нормального типа и $r \in \Sigma$. Тогда w_r переводит r в $-r$, а любой положительный корень в положительный.*

Доказательство. Лемма 2.1.5 [9].

§2. Минимальный контрпример

Всюду далее будем считать, что группа G — минимальный контрпример к теореме. Без ограничения общности можно считать, что $|x|$ является простым числом. Дальше в работе это будет использоваться без дополнительных оговорок.

Лемма 1. $O(G) = 1$

Доказательство. Пусть $O(G) \neq 1$. Обозначим $\overline{G} = G/O(G)$. Ясно, что $x \notin O(G)$, поэтому $\overline{x} \neq 1$. Так как G — минимальный контрпример, то $\overline{x} \in O(\overline{G})$ и $O(\overline{G}) \neq 1$. Последнее, очевидно, невозможно.

Лемма 2. $O_2(G) = 1$

Доказательство. Пусть $O_2(G) \neq 1$. Рассмотрим подгруппу $O_2(G) < x >$. Если $G = O_2(G) < x >$, то так как $< x, x^g >$ — группа нечетного порядка для любого $g \in G$ получим, что $< x, x^g >=< x >$. Отсюда следует, что $< x > \lhd G$. Получили противоречие с леммой 1. Таким образом, $O_2(G) < x >\neq G$. Поэтому $x \in O(O_2(G) < x >)$ и $O_2(G) < x >= O_2(G) \times < x >$. Следовательно, $x \in C_G(O_2(G)) \trianglelefteq G$. Если $C_G(O_2(G)) \neq G$, то $x \in O(C_G(O_2(G)))$. Отсюда заключаем, что $O(G) \neq 1$. Противоречие с леммой 1. Следовательно, $C_G(O_2(G)) = G$. Рассмотрим фактор-группу $\overline{G} = G/O_2(G)$. Ясно, что $1 \neq \overline{x} \in O(\overline{G})$. Пусть L — полный прообраз группы $O(\overline{G})$ в G. Поскольку $C_G(O_2(G)) = G$, то $L = O_2(L) \times O(L)$ и $O(L) \neq 1$, так как $O(\overline{G}) \neq 1$. Таким образом, $1 \neq O(L) \subseteq O(G)$. Противоречие с леммой 1.

Лемма 3. *Группа G является либо простой неабелевой группой, либо имеет вид $G = N \leftthreetimes < x >$, где N — простая неабелева группа.*

Доказательство. Пусть N — собственная минимальная нормальная подгруппа в G. Из леммы 1 и леммы 2 следует, что $N = N_1 \times N_2 \times \ldots \times N_f$, где N_i — простые неабелевы группы. Если $x \in N$, то $x \in O(N)$, так как N — собственная подгруппа в G. Но так как $O(N) = 1$, то это невозможно. Следовательно, $x \notin N$. Рассмотрим группу $N < x >$.

(a) $N < x >\neq G$.

В этом случае $x \in O(N < x >)$ и $O(N < x >) =< x > (N \bigcap O(N < x >))$. Так как $N \bigcap O(N < x >) = 1$, то $O(N < x >) =< x >$ и $x \in C_G(N)$. Если $C_G(N) \neq G$, то $x \in O(C_G(N))$, а поэтому $1 \neq x \in O(C_G(N)) \subseteq O(G)$. Противоречие с леммой 1. Таким образом, $C_G(N) = G$. Так как N является неабелевой группой, то последнее невозможно.

(b) $N < x >= G$.

Так как $< x >\cong Z_p$, то $G = N \leftthreetimes < x >$. Группа $< x >$ действует транзитивно на множестве $\{N_1, N_2, \ldots, N_f\}$, поэтому $f \in \{1, p\}$. Если $f = 1$, то $N = N_1$ — простая неабелева группа и лемма 3 доказана. Следовательно, $f = p$. Группа $< x >$ действует транзитивно на $\{N_1, N_2 \ldots, N_p\}$, поэтому при подходящей нумерации получим: $N_{i+1} = N_1^{x^i}$, где $i = 0, 1, \ldots, p-1$. Таким образом, $N = N_1 \times N_1^x \times \ldots \times N_1^{x^{p-1}}$. Пусть t — инволюция из N_1. Тогда t не централизует x. Группа $< x, x^t >$ имеет нечетный порядок. Рассмотрим элемент $x^{-1}x^t \in< x, x^t >$. Очевидно, что $1 \neq (x^{-1}tx)t \in N_1^x \times N_1$ и поэтому $x^{-1}x^t$ является инволюцией. Последнее невозможно, так как порядок группы $< x, x^t >$ — нечетное число. Лемма 3 доказана.

Лемма 4. *Ядра подгрупп, содержащих элемент x и отличных от G, нетривиальны.*

Доказательство. Очевидно.

Лемма 5. *В группе G существует максимальная подгруппа четного порядка, содержащая элемент x.*

Доказательство. Очевидно, существует цепь $1 \subset < x, t > = < x, x^t > \leftthreetimes < t > \subseteq M \subset\cdot G$, где $t \in I(G)$, а M является максимальной подгруппой в G. Это доказывает лемму 5.

Лемма 6. *Пусть $t \in I(G)$ и $[t, x] = 1$. Тогда G удовлетворяет условиям U-гипотезы.*

Доказательство. Из леммы 3 следует, что $F^*(G)$ — простая неабелева группа. Так как $x \in C_G(t)$, то $1 \neq x \in O(C_G(t))$. Условия U-гипотезы выполнены.

§3. G — спорадическая группа

В этом параграфе будет показано, что минимальный контрпример к теореме не может быть спорадической группой.

1. $G \in \{M_{22}, M_{24}\}$. Из [3] следует, что ядра всех максимальных подгрупп в G единичные. Это противоречит утверждению (2.4).

2. $G \cong M_{23}$. Из [3] и (2.4) следует, что единственной (с точностью до изоморфизма) максимальной подгруппой в группе G, содержащей x, может быть группа Фробениуса $23 : 11$. Получили противоречие с (2.5).

3. $G \cong J_1$. Из [3] и (2.4) следует, что максимальная подгруппа M, содержащая элемент x, может быть только одного из следующих типов: $19 : 6$, $11 : 10$, $D_6 \times D_{10}$, $7 : 6$.

(a) $M \cong 19 : 6$. В этом случае $|x| \in \{3, 19\}$. Пусть сначала $|x| = 19$. Рассмотрим группу нечетного порядка $< x, x^g >$, где g — произвольный элемент группы G. Эта группа содержится в максимальной подгруппе типа $19 : 6$, имеющей единственную подгруппу порядка 19. Следовательно, $< x, x^g >$ — 19-группа для всех $g \in G$. По теореме Бэра (лемма 1.1) $x \in O_{19}(G)$, что невозможно в силу утверждения (2.1). Пусть теперь $|x| = 3$. Из [3] следует, что в группе G имеется один класс сопряженных элементов порядка 3, централизаторы которых имеют порядок 30. Таким образом, согласно (2.6), группа G удовлетворяет условиям U-гипотезы. Последнее невозможно.

(b) $M \cong 11 : 10$. Доказательство проводится также как в случае (a).

(c) $M \cong D_6 \times D_{10}$. Так как $|x| \in \{3, 5\}$, то из [3] следует, что найдется $t \in I(G)$ для которой $[t, x] = 1$. Следовательно, в силу (2.6), группа G удовлетворяет условиям U-гипотезы, что невозможно.

(d) $M \cong 7 : 6$. Этот случай рассматривается также как (a).

4. $G \cong HS$. Из [3] и (2.4) следует, что максимальными подгруппами в G, содержащими элемент x, могут быть только подгруппы следующего типа: $5 : 4 \times A_5$. Поэтому $|x| = 5$. Группа HS содержит максимальную подгруппу типа $U_3(5) : 2$ индекс которой взаимно прост с 5. Следовательно, для некоторого $g \in G$ $x^g \in U_3(5) : 2$ и $O(U_3(5) : 2) \neq 1$. Последнее невозможно.

5. $G \cong M^cL$. Из [3] и (2.4) следует, что максимальными в G подгруппами, содержащими x, могут быть только подгруппы следующих типов: $3_+^{1+4} : 2S_5$, $3^4 : M_{10}$, $5_+^{1+2} : 2 : 8$. Наличие в группе M^cL максимальных подгрупп $U_4(3)$ и $U_3(5)$ с тривиальными ядрами и индексами $(|M^cL : U_4(3)|, 3) = 1 = (|M^cL : U_3(5)|, 5)$ исключает все названные случаи.

6. $G \cong He$. Из [3] и (2.4) следует, что максимальными подгруппами в G, содержащими x, могут быть только группы следующих типов: $7^2 : 2L_2(7)$, $3.S_7$, $7_+^{1+2} : (S_3 \times 3)$, $7 : 3 \times L_3(2)$, $5^2 : 4A_4$. Группа Хельда содержит подгруппу $S_4(4) : 2$ индекса $2 \cdot 3 \cdot 7^3$, что исключает подгруппу $5^2 : 4A_4$. Случай, когда $|x| = 3$, исключается наличием подгруппы $2^2 \cdot L_3(4) \cdot S_3$ индекса $2 \cdot 5 \cdot 7^2 \cdot 17$. Согласно строению максимальных подгрупп, оставшихся в списке, заключаем, что $|x| = 7$. Группа нечетного порядка $< x, x^g >$ содержится в одной из следующих групп: $7^2 : L_2(7)$, $7_+^{1+2} : (S_3 \times 3)$, $7 : 3 \times L_3(2)$. В первом

случае $< x, x^g >\subseteq O(7^2 : L_2(7)) = 7^2$ и является 7-группой. Во втором случае, так как 7-силовская подгруппа единственная, то снова $< x, x^g >$ — 7-группа. В третьем случае $< x, x^g >\subseteq O(7 : 3 \times L_3(2)) = 7 : 3$ и $< x, x^g >$ является 7-группой. Таким образом, для всех $g \in G$ $< x, x^g >$ — 7-группа. По теореме Бэра $x \in O_7(G)$. Получили противоречие с (2.1).

7. $G \cong Ru$. Из [3] и (2.4) следует, что максимальными в G подгруппами, содержащими x, могут быть только группы следующих типов: $5^2 : 4S_5$, $3{\cdot}A_6{\cdot}2^2$, $5_+^{1+2} : [2^5]$, $5 : 4 \times A_5$. Группа Рудвалиса содержит подгруппу $U_3(5) : 2$ индекса 579072 с тривиальным ядром. Это исключает случаи $5^2 : 4S_5$, $5_+^{1+2} : [2^5]$ и $5 : 4 \times A_5$. Наконец, группа $3{\cdot}A_6{\cdot}2^2$ исключается существованием подгруппы $(2^6 : U_3(3)) : 2$ индекса 188500.

8. $G \in \{M_{11}, M_{12}, J_3, O'N, Co_3, Fi_{22}, Suz, Fi_{23}, J_2, F_5, Co_1\}$. Если G изоморфна одной из первых восьми групп списка, то из [3] и (2.4) следует, что $|x| = 3$. Когда $G \in \{J_2, F_5\}$, то из [3] и (2.4) заключаем, что $|x| \in \{3, 5\}$. Если же $G \cong Co_1$, то $x \in \{3, 5, 7\}$. Из таблиц характеров [3] следует, что во всех названных случаях $|C_G(x)|$ является четным числом, а группа G удовлетворяет условиям U-гипотезы. Последнее невозможно.

9. $G \cong Co_2$. Из [3] и (2.4) следует, что максимальными в G подгруппами, содержащими x, могут быть только группы следующих типов: $3_+^{1+4} : 2_-^{1+4}.S_5$, $5_+^{1+2} : 4S_4$. Группа Co_2 содержит подгруппу $U_6(2) : 2$ индекса 2300 с тривиальным ядром. Ее существование исключает группы первого типа. Группы второго типа исключаются наличием у G подгруппы M^cL индекса 47104.

10. $G \cong Ly$. Из [3] и (2.4) заключаем, что максимальными в G подгруппами, содержащими x, могут быть группы следующих типов: $3.M^cL : 2$, $5^{3{\cdot}}L_3(5)$, $5_+^{1+4} : 4S_6$, $3^5 : (2 \times M_{11})$, $3^{2+4} : 2A_5.D_8$, $67 : 22$, $37 : 18$. Отсюда следует, что $|x| \in \{3, 5, 11, 37, 67\}$. В первых трех случаях $|C_G(x)|$ — четное число и группа G, согласно (2.6), удовлетворяет условиям U-гипотезы, что невозможно. Случай, когда $|x| \in \{37, 67\}$ рассматривается аналогично случаю (а) для группы J_1.

11. $G \cong Th$. Из [3] и (2.4) следует, что x содержится в одной из подгрупп следующих типов:

(1) 3-*локальные подгруппы:* $(3 \times G_2(3)) : 2$, $[3^9].2S_4$, $3^2.[3^7].2S_4$, $3^5 : 2S_6$.

(2) 5-*локальные подгруппы:* $5_+^{1+2} : 4S_4$; $5^2 : GL_2(5)$.

(3) 7-*локальные подгруппы:* $7^2 : (3 \times 2S_4)$.

(4) 31-*локальные подгруппы:* $31 : 15$.

Отсюда следует, что $|x| \in \{3, 5, 7, 31\}$. В первых трех случаях $|C_G(x)|$ — четное число и группа G удовлетворяет условиям U-гипотезы, что невозможно. Последний случай исключается с помощью (2.5).

12. $G \cong J_4$. Из [3] и (2.4) следует, что x содержится в одной из подгрупп следующих типов: $11_+^{1+2} : (5 \times 2S_4)$, $29 : 28$, $43 : 14$, $37 : 12$. Если $|x| \in \{5, 11\}$, то $|C_G(x)|$ — четное число и группа G удовлетворяет условиям U-гипотезы, что невозможно. Оставшиеся три случая рассматриваются аналогично случаю (а) для группы J_1.

13. $G \cong Fi'_{24}$. Из [3] и (2.4) следует, что x содержится в одной из подгрупп следующих типов: $(3 \times O_8^+(3) : 3) : 2$, $3^{7{\cdot}}O_7(3)$, $3_+^{1+10} : U_5(2)$, $3^2.3^4.3^6.(A_5 \times 2A_4).2$, $(3^2 : 2 \times G_2(3)).2$, $7 : 6 \times A_7$, $29 : 14$, $3^3.[3^{10}].GL_3(3)$. Отсюда следует, что $|x| \in \{3, 7, 29\}$. Если $|x| \in \{3, 7\}$, то $|C_G(x)|$ является четным числом и группа G удовлетворяет условиям U-гипотезы, что невозможно. Случай, когда $|x| = 29$ рассматривается аналогично случаю (а) для группы J_1.

14. $G \cong B = F_{2+}$. Из [3] и (2.4) следует, что $|x| \in \{3, 5, 7, 11, 13, 17, 19, 23, 31, 47\}$. В первых восьми случаях $|C_G(x)|$ — четное число и группа G удовлетворяет условиям

U-гипотезы, что невозможно. Случаи $|x| \in \{31, 47\}$ $(31 : 15, 47 : 23)$ исключаются с помощью (2.5).

15. $G \cong F_1$. Из [3] и (2.4) следует, что $|x| \in \{3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 41, 47, 59, 71\}$. При $|x| \in \{3, 5, 7, 11, 13, 17, 19, 23, 31, 47\}$ $|C_G(x)|$ является четным числом и группа G удовлетворяет условиям U-гипотезы, что невозможно. Случаи, когда $|x| \in \{29, 41, 59, 71\}$ $[(29 : 14 \times 3)\cdot 2, 41 : 40, 59 : 29, 71 : 35]$ исключаются либо с помощью приема, использованного в п. (a) для группы J_1, либо с помощью (2.5).

§4. G — знакопеременная группа

В этом параграфе будет показано, что минимальный контрпример к теореме не может быть знакопеременной группой A_n $(n \geq 5)$.

Лемма 1. *Пусть A_p — знакопеременная группа для простого числа $p > 3$. Если $f = (1, 2, \ldots, p-1, p)$, то найдется элемент $g \in A_p$ такой, что группа $< f, f^g >$ имеет четный порядок.*

Доказательство. Положим $y = (1, 2, \ldots, p-2, p, p-1)$. По теореме Силова найдется $g \in A_p$, для которого $f^g = y^m$, где $1 \leq m < p$. Поэтому $< f, f^g > = < f, y >$. Отсюда следует, что $< f, f^g > \ni fy = (1, 3, \ldots, p-4, p-2)(2, 4, \ldots, p-3, p)(p-1)$. Если $(p-1)/2$ — четное число, то $|fy|$ также четное число. Следовательно, в этом случае группа $< f, f^g >$ имеет четный порядок. Таким образом, $(p-1)/2 = 2k+1$. Рассмотрим $z = (1, 2, 3, \ldots, p-5, p-4, p, p-1, p-2, p-3)$. По теореме Силова найдется $h \in A_p$ для которого $f^h = z^m$, где $1 \leq m < p$. Следовательно, $< f, f^h > = < f, z >$. Отсюда заключаем, что $< f, f^h > \ni fz = (1, 3, \ldots, p-6, p-4)(2, 4, \ldots, p-5, p)(p-3)(p-1)(p-2)$. Так как $(p-3)/2 = 2k$, то $|fz|$, а вместе с ним и $| < f, f^h > |$ будут четными числами. Это доказывает лемму 1.

Лемма 2. *Пусть A_n — знакопеременная группа для $n \geq 5$ и $p \in \pi(A_n) \setminus \{2, 3\}$. Тогда всякий элемент $f \in A_n$ порядка p содержится в группе $< f, f^g >$ четного порядка для некоторого $g \in A_n$.*

Доказательство. Если $p = n$, то утверждение следует из леммы 1, поэтому $3 < p < n$. Рассмотрим произвольный элемент $f = (1, 2, \ldots, p) \ldots (pk+1, \ldots, p(k+1))(p(k+1)+1) \ldots (n) \in A_n$ порядка p. Если $(p-1)/2$ — четное число, то рассмотрим $g \in A_n$ для которого $(1, 2, \ldots, p-2, p-1, p)^g = (1, 2, \ldots, p-2, p, p-1)^j$, где $1 \leq j \leq p-1$. Тогда $< f, f^g > = < (1, 2, \ldots, p-2, p-1, p)f_1, (1, 2, \ldots, p-2, p, p-1)^j f_2 >$, где f_1 и f_2 — ограничения f и f^g на оставшиеся $n-p$ символов. Найдется число l, для которого $(1, 2, \ldots, p-2, p, p-1)^{jl} = (1, 2, \ldots, p-2, p, p-1)$. Поэтому, как в лемме 1, $< f, f^g > \ni f(f^g)^l$ — элемент четного порядка. Случай, когда $(p-1)/2$ — нечетное число рассматривается аналогично. В качестве $g \in A_p$ достаточно взять элемент для которого $(1, 2, \ldots, p-2, p-1, p)^g = (1, 2, \ldots, p-5, p-4, p, p-1, p-2, p-3)^j$ при некотором $1 < j < p$. Лемма 2 доказана.

Лемма 3. *Пусть A_n — знакопеременная группа для $n \geq 5$ и $p = 3$. Тогда всякий элемент $f \in A_n$ порядка 3 содержится в группе четного порядка $< f, f^g >$ для некоторого $g \in A_n$.*

Доказательство. Если $f = (1, 2, 3)(4) \ldots (n)$, то положим $g = (1, 2)(3, 4)\ (5) \ldots (n) \in A_n$. Тогда $< f, f^g > \ni f f^g f^{-1} (f^g)^{-1}$ — элемент четного порядка. Если число тройных циклов в записи элемента f больше одного и $f = (1, 2, 3)(4, 5, 6)f_1$, где f_1 — перестановка на символах $\{7, 8, \dots, n\}$, то положим $g = (1,4,2)(3,6,5)(7)\dots(n)$. Непосредственный подсчет показывает, что $g^{-1}f^{-1}gf \in < f, f^g >$ имеет четный порядок. Лемма 3 доказана.

Пусть $G \cong A_n$, $n \geq 5$. Так как $|x|$ — нечетное простое число, то из лемм 2 и 3 заключаем, что x содержится в группе четного порядка $< x, x^g >$ для некоторого $g \in G$, что невозможно. Таким образом, минимальный контрпример G не может быть знакопеременной группой A_n $(n \geq 5)$.

§5. G — простая группа лиевского типа

При рассмотрении групп лиевского типа над полем характеристики p, будем выделять две ситуации: x — унипотентный элемент порядка p и x — полупростой элемент простого порядка r.

(i) *x — унипотентный элемент порядка p.*

Пусть сначала G — группа Шевалле нормального типа. По теореме Силова, без ограничения общности, можно считать, что $x \in U =< X_\varepsilon \mid \varepsilon \in \Phi^+ >$. Рассмотрим собственную параболическую подгруппу L в группе G и покажем, что из включения $x^g \in L$ следует включение $x^g \in O_p(L)$ для всех $g \in G$. Для подгруппы L имеет место разложение Леви $L = O_p(L)(L_I H)$ (см. лемму 1.4). Так как $|x| = p$, то $x^g \in O_p(L)L_I$. Отсюда следует, что $x^g \in O(O_p(L)L_I) = O_p(L)O(L_I)$. Поскольку L_I — центральное произведение групп лиевского типа над полем характеристики p, то $O(L_I) = O(Z(L_I))$ и $x^g \in O_p(L)O(Z(L_I))$. Из абелевости группы $O(Z(L_I))$ заключаем, что $x^g \in O_p(L)$.

В силу леммы 1.5, элемент x имеет разложение: $x = x_{\beta_1}(t_1)x_{\beta_2}(t_2)\dots x_{\beta_{k-1}}(t_{k-1})$ $x_{\alpha_k}(t_k)x_{\beta_{k+1}}(t_{k+1})\dots x_{\beta_N}(t_N)$, где $\beta_i \in \Phi^+$, $\alpha_k \in \Sigma$ и $t_k \neq 0$. Подействуем на x элементом группы Вейля $w = w_{\alpha_k}$. Из леммы 1.6 следует, что $x^w = x_{\gamma_1}(r_1)x_{\gamma_2}(r_2)\dots x_{\gamma_{k-1}}(r_{k-1})x_{-\alpha_k}(\pm t_k)x_{\gamma_{k+1}}(r_{k+1})\dots x_{\gamma_N}(r_N)$, где $\gamma_i \in \Phi^+$ и элемент x^w содержится в параболической подгруппе $< B, X_{-\alpha_k} >$, где B — подгруппа Бореля. Если G не является группой типа A_1, то $< B, X_{-\alpha_k} > \neq G$, поэтому $x^w \in O_p(< B, X_{-\alpha_k} >) \subseteq U$. Отсюда следует, что $x_{-\alpha_k}(\pm t_k) \subseteq U =< X_\varepsilon \mid \varepsilon \in \Phi^+ >$. Последнее невозможно.

Таким образом, $G \cong L_2(p^n)$ для подходящего значения параметра n. Без ограничения общности можно считать, что x является образом матрицы $X = \begin{bmatrix} 1 & \beta \\ 0 & 1 \end{bmatrix}$ из группы $SL_2(p^n)$, где $o \neq \beta \in GF(p^n)$. Рассмотрим матрицу $T = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \in SL_2(p)$. Имеют место соотношения: $X^T = \begin{bmatrix} 1 & 0 \\ -\beta & 1 \end{bmatrix}$ и $< X, X^T > \cong SL_2(p)$. Противоречие с тем, что $< x, x^t >$ является группой нечетного порядка (здесь t — образ матрицы T в $L_2(p^n)$). Случай, когда G — группа Шевалле нормального типа, полностью рассмотрен.

Пусть G — группа Шевалле скрученного типа. Если лиевский ранг у G больше единицы, то, согласно теореме 32 [10], рассуждения для групп нормального типа переносятся почти автоматически. Поэтому доказательство этого случая мы опускаем. Следовательно, $G \in \{^2B_2(q), {}^2G_2(q), {}^2A_2(q)\}$.

(a) $G \cong {}^2B_2(q)$.

Группа $^2B_2(q)$ определена над полем характеристики 2. Так как $|x|$ совпадает с характеристикой поля и является нечетным числом, то этот случай невозможен.

(b) $G \cong {}^2G_2(q) \cong {}^2G_2(3^{2n+1})$.

Согласно теореме C [11] и (2.4), максимальные подгруппы в ${}^2G_2(q)$, содержащие элемент x порядка 3, могут иметь только следующее строение $\mathbb{Z}_{q\pm\sqrt{3q}+1} : \mathbb{Z}_6$, $2^2 \times D_{\frac{1}{2}(q+1)} : 3$, $[q^6] : (q-1)$.

(1) $x \in \mathbb{Z}_{q\pm\sqrt{3q}+1} : \mathbb{Z}_6$.

В этом случае $[x,t] = 1$ для некоторой инволюции $t \in I(G)$. Так как $C_G(t) = < t > \times PSL_2(q)$ и $x \in O(C_G(t))$, то $O(PSL_2(q)) \neq 1$. Последнее, очевидно, невозможно.

(2) $x \in (2^2 \times D_{\frac{1}{2}(q+1)}) : 3$ — *нормализатор в G четверной подгруппы.*

Так как элемент x нормализует четверную подгруппу, то по условию теоремы он будет ее централизовать. Снова $[x,t] = 1$ для некоторой $t \in I(G)$, что невозможно по (1.2) и (2.6).

(3) $x \in [q^6] : (q-1)$.

Рассмотрим группу $< x, x^g >$ для некоторого $g \in G$. Эта группа, очевидно, содержится в группе типа $[q^6] : (q-1)$, иначе выполняется либо случай (1), либо случай (2). Поэтому $< x, x^g >$ — 3-группа для всех $g \in G$ и по теореме Бэра $x \in O_3(G)$. Противоречие с (2.1).

(c) $G \cong PSU_3(q^2)$.

Прообраз элемента x в группе $SU_3(q^2)$ с точностью до сопряженности имеет вид:

$$X = \begin{bmatrix} 1 & 1 & b \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{bmatrix}, \quad X = \begin{bmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

или

$$X = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{bmatrix}, \text{ где } b \in GF(q^2).$$

Обозначим $T = \begin{bmatrix} 0 & 0 & 1 \\ 0 & -1 & 0 \\ 1 & 0 & 0 \end{bmatrix} \in SU_3(q^2)$. Пусть t является образом T в группе $PSU_3(q^2)$. Тогда $< x, t > = < x, x^t > \leftthreetimes < t >$, причем $| < x, x^t > |$ — нечетное число. По теореме 7.1 [12] группа $< x, t >$ содержится в борелевской подгруппе группы $PSU_3(q^2)$. Поэтому группа $< X, T >$ также содержится в борелевской подгруппе группы $SU_3(q^2)$. Однако по построению группа $< X, T >$ заведомо не может содержаться в борелевской подгруппе.

(ii) x — *полупростой элемент простого порядка r.*

Пусть x содержится в некоторой собственной параболической подгруппе L группы G. Согласно лемме 1.4 для L имеет место разложение Леви: $L = O_p(L)(L_I H)$. Ясно, что $x \in O(L)$. Так как x полупростой элемент, то заключаем, что $x \in O(Z(L_I)H)$. Поэтому x нормализует унипотентную подгруппу U, а следовательно, $x \in H$. Если лиевский ранг группы G больше единицы, то x нормализует собственную подгруппу $< X_\varepsilon, X_{-\varepsilon} >$ в группе G для всех $\varepsilon \in \Phi^+$. Следовательно, $x \in O(< X_\varepsilon, X_{-\varepsilon} >< x >) = < x >$. Таким образом, $[x, U] = 1$. Последнее невозможно.

Поэтому лиевский ранг группы G равен единице и $G \in \{A_1(q); {}^2A_2(q); {}^2G_2(q); {}^2B_2(q)\}$.

Если $G \cong PSL_2(q)$, то x содержится в циклической силовской q-подгруппе. Противоречие с результатом Глаубермана (1.1). Если $G \cong PSU_3(q^2)$, то так как $x \in H$ получим, что x централизует некоторую инволюцию $t \in H$. Рассмотрим $C = C_G(t)$. Ясно, что $x \in O(C)$. По теореме 4.247 [2] найдется инволюция $u \in C$ и субнормальная подгруппа L в $C_G(u)$ такие, что $L \cong SL_2(q)$ и $< O(C), t >$ нормализует L, причем $C_{<O(C),t>}(L) = 1$. Так как $x \in < O(C), t >$, то $x \in N_G(L)$ и, следовательно, $[x, L] = 1$. Противоречие с тем, что $C_{<O(C),t>}(L) = 1$.

Пусть $G \cong {}^2G_2(q)$. Так как $x \in H$, то $[x, t] = 1$ для некоторой $t \in I(G)$. Имеем: $C_G(t) = < t > \times PSL_2(q)$ и $x \in O(C_G(t))$, что невозможно.

Наконец рассмотрим случай $G \cong {}^2B_2(q)$. Так как x содержится в H, то x будет также содержаться в некоторой борелевской подгруппе и $[x, U] = 1$, где U — унипотентная подгруппа в G. Последнее невозможно.

По лемме (1.3) силовские r-подгруппы в G не являются циклическими. Поэтому найдется элемент $y \in G$ порядка r для которого $S = < x, y > \cong \mathbb{Z}_r \times \mathbb{Z}_r$. Обозначим через T максимальный в G тор, содержащий подгруппу S. Рассмотрим произвольный $z \in S^{\#}$ и покажем, что $C_G(z) \leq N_G(T)$. Из (2.9) [14] следует, что $C_G(z) \trianglerighteq Y = Y_0T$ и $Y_0 = D_1 * D_2 * \ldots * D_k * F$, где D_i — группы лиевского типа над полем характеристики p, а $F \leq T$. Предположим, что не все $D_i = 1$. Элемент x нормализует всякую подгруппу D_i и $x \in O(C_G(z))$. Поэтому для некоторой инволюции $v \in I(C_G(z))$ элемент $x \in O(C_G(v))$. Если группа G определена над полем характеристики 2, то ядра централизаторов инволюций тривиальны. Следовательно, G определена над полем нечетной характеристики. Если $G \in \{A_1(q), {}^2G_2(q)\}$, то силовские r-подгруппы в G являются циклическими, что невозможно. Поэтому $G \notin \{A_1(q), {}^2G_2(q)\}$. Тогда по теореме 4.247 [2] найдется инволюция $u \in C_G(v)$ и субнормальная подгруппа L в $C_G(u)$ такие, что $L \cong SL_2(q)$ и $M = < O(C_G(v), v) >$ нормализует L, причем $C_M(L) = 1$. Так как $x \in M$, то $x \in N_G(L)$ и, следовательно, $[x, L] = 1$. Противоречие с тем, что $C_M(L) = 1$.

Таким образом, все $D_i = 1$. Но тогда $Y = T \trianglelefteq C_G(z)$ и $C_G(z) \leq N_G(T)$. Из [13] следует, что возможен один из следующих случаев:

(i) $G \cong {}^2F_4(2)'$, $r = 5$.

В этом случае G содержит подгруппу $S \cong L_2(25)$ и $(|G : S|, 5) = 1$. Поэтому $O(S) \neq 1$, что невозможно.

(ii) $G \in \{PSp(n, 2), \Omega_n^{\pm}(2), F_4(2), F_4(4), {}^2F_4(2)', E_6(2), E_7(2), E_8(2), E_8(4)\}$, $r = 3$.

Централизаторы элементов порядка 3 в группах лиевского типа характеристики 2 были описаны Бургонем (стр. 425–431 [4]). Из этого описания следует, что ни один из данных случаев реализоваться не может.

§6. $G = M \leftthreetimes < x >$, где M — простая неабелева группа

Если M изоморфна знакопеременной или спорадической группе, то $\mathrm{Out}(G)$ является 2-группой, что противоречит нечетности $|x|$. Поэтому M — группа лиевского типа.

(i) $M \in Chev(p)$, $|x| = p$.

Без ограничения общности можно считать, что $x \in N_G(U)$. Положим $G^* = Inndiag(M)$, $B^* = N_{G^*}(U)$. Тогда $B^* = UH^*$, где $H^* \supseteq H$ и H^* нормализует каждую корневую подгруппу X_ε $(\varepsilon \in \Phi)$. Следовательно, если $x \in G^*$, то можно считать, что $x \in H^*$, так как $x \in N_G(U)$. Можно считать, что группа H^* есть расширение H с помощью группы диагональных автоморфизмов, поэтому $(|H^*|, p) = 1$, что противоречит включению $x \in H^*$.

Таким образом, $x \notin Inndiag(M)$. Согласно лемме 7.3 [4], возможна одна из следующих ситуаций:

1. *x индуцирует на M полевой автоморфизм, автоморфизм графа или графо-полевой автоморфизм.*

Пусть $GF(p^m)$ — конечное поле, над которым определена группа лиева типа M. Найдется $\gamma \in \mathrm{Aut}(GF(p^m))$, для которого отображение корневых подгрупп: $X_\varepsilon(t) \to X_\varepsilon(t^\gamma)$ (для всех $\varepsilon \in \Sigma$) продолжается до полевого автоморфизма x группы M. Поэтому x нормализует каждую корневую подгруппу $X_{\pm\varepsilon}$, где $\varepsilon \in \Sigma$. Если лиевский ранг группы M больше единицы, то так как G — минимальный контрпример к теореме, x будет централизовать группу $< X_\varepsilon, X_{-\varepsilon} >$ для всех $\varepsilon \in \Sigma$. Следовательно, $[x, X_{\pm\varepsilon}] = 1$ для всех $\varepsilon \in \Sigma$. Отсюда следует, что $[x, M] = 1$. Последнее невозможно. Поэтому лиевский ранг группы M равен единице.

(a) *$M \cong PSL_2(p^m)$, где $m = ap$.*

Пусть t — инволюция, не коммутирующая с x. Тогда $tt^x \in < x, t > = < x, x^t > \leftthreetimes < t > = (M_1 \leftthreetimes < x >) \leftthreetimes < t > = (M_1 \leftthreetimes < t >) \leftthreetimes < x >$, где $M_1 = M \bigcap < x, x^g >$ — x-допустимая группа. Согласно теореме Диксона ([14], теорема 8.27), M_1 — абелева группа нечетного порядка. Положим $tt^x = u \in M_1$. Так как M_1 является абелевой, допустимой относительно x группой, то $uu^x = u^x u$. Поэтому $tt^x t^x t^{x^2} = t^x t^{x^2} tt^x$, или $t^x tt^{x^2} = t^{x^2} tt^x$.

Рассмотрим матрицу $T = \begin{bmatrix} \alpha & 1 \\ -1-\alpha^2 & -\alpha \end{bmatrix}$, где α — произвольный элемент поля $GF(p^m)$, а инволюция t ее образ в $PSL_2(p^m)$. Через X обозначим матрицу соответствующую элементу x. Условие $t^x tt^{x^2} = t^{x^2} tt^x$ влечет, что $T^X TT^{X^2} = \pm T^{X^2} TT^X$, где

$$T^X = \begin{bmatrix} \overline{\alpha} & 1 \\ -1-\overline{\alpha}^2 & -\overline{\alpha} \end{bmatrix}, \qquad T^{X^2} = \begin{bmatrix} \overline{\overline{\alpha}} & 1 \\ -1-\overline{\overline{\alpha}}^2 & -\overline{\overline{\alpha}} \end{bmatrix}.$$

Черта означает действие автоморфизма Фробениуса на элемент поля $GF(p^m)$. Матрица T^{X^2} получается из матрицы T^X заменой $\overline{\alpha}$ на $\overline{\overline{\alpha}}$. Поэтому матрицы $T^X TT^{X^2}$ и $T^{X^2} TT^X$ получаются друг из друга перестановкой $\overline{\alpha}$ и $\overline{\overline{\alpha}}$. Пусть сначала $T^X TT^{X^2} = T^{X^2} TT^X$. Тогда имеет место равенство:

$$-\alpha - \alpha\overline{\alpha}^2 + \overline{\alpha} + \alpha^2\overline{\alpha} + \overline{\overline{\alpha}} + \overline{\alpha}^2\overline{\overline{\alpha}} - \alpha\overline{\alpha}\,\overline{\overline{\alpha}} = -\alpha - \alpha\overline{\overline{\alpha}}^2 + \overline{\overline{\alpha}} + \alpha^2\overline{\overline{\alpha}} + \overline{\alpha} + \overline{\overline{\alpha}}^2\overline{\alpha} - \alpha\overline{\alpha}\,\overline{\overline{\alpha}}.$$

Положим $\overline{\alpha} = \alpha^{p^a}$, тогда $\overline{\overline{\alpha}} = \alpha^{p^{2a}}$. Подставив значения $\overline{\alpha}$ и $\overline{\overline{\alpha}}$ в предыдущее равенство, получим:

$$\alpha^{2p^{2a}+p^a} - \alpha^{2p^{2a}+1} - \alpha^{p^{2a}+2p^a} + \alpha^{p^{2a}+2} + \alpha^{2p^a+1} - \alpha^{p^a+2} = 0.$$

Таким образом, пришли к полиномиальному уравнению:

$$p(z) = z^{2p^{2a}+p^a} - z^{2p^{2a}+1} - z^{p^{2a}+2p^a} + z^{p^{2a}+2} + z^{2p^a+1} - z^{p^a+2} = 0$$

степени $2p^{2a} + p^a$.

Равенство $T^X TT^{X^2} = -T^{X^2} TT^X$ также приводит к полиномиальному уравнению степени $2p^{2a} + p^a$. Так как всякий элемент поля $GF(p^{ap})$ должен удовлетворять одному из этих уравнений, то должно выполняться неравенство: $2(2p^{2a} + p^a) \geq p^{ap}$, где $p \geq 3$. Легко видеть, что данное неравенство может выполняться лишь при $p = 3$ и $a = 1$. В этом случае $p(z) = z^{21} - z^{19} - z^{15} + z^{11} + z^7 - z^5$. Разложим этот многочлен на множители: $p(z) = z^5(z-1)^5(z+1)^5(z^2+1)(z^4+1)$. Из этого разложения следует, что этот многочлен имеет не более 9 корней в поле $GF(3^3)$. Случаю $T^X T T^{X^2} = -T^{X^2} T T^X$ соответствует многочлен $g(z) = z(z^{20} - z^{18} + z^{14} + z^{12} + z^{10} - z^8 - z^6 + z^4 - z^2 + 1)$. Рассмотрим левую циркулянтную матрицу (см. стр. 330 [15]) для многочлена, стоящего в круглых скобках. Ранг квадратной матрицы 10×10, находящейся в левом верхнем углу левой циркулянтной матрицы равен 9. По теореме Кенига-Радоша (теорема 6.1 [15]) число ненулевых решений уравнения, стоящего в круглых скобках, в поле $GF(3^3)$ не более $26 - 9 = 17$. Поэтому обоим уравнениям удовлетворяет не более 26 элементов поля $GF(3^3)$. Следовательно, найдется элемент поля $GF(3^3)$, который не удовлетворяет ни одному из двух многочленов $p(z)$ и $g(z)$, что невозможно.

(b) $M \cong PSU_3(p^{2k})$.

Рассмотрим группу $SU_3(p^{2k})$. Пусть X — полевой автоморфизм группы $SU_3(p^{2k})$, соответствующий элементу x. Рассмотрим подгруппы

$$Y = \left\langle \begin{bmatrix} 1 & 0 & \alpha \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \middle| \alpha \in GF(p^{2k}) \text{ и } tr\alpha = 0 \right\rangle,$$

$$Z = \left\langle \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ \alpha & 0 & 1 \end{bmatrix} \middle| \alpha \in GF(p^{2k}) \text{ и } tr\alpha = 0 \right\rangle,$$

порядков p^k. Очевидно, что $Y^X = Y$ и $Z^X = Z$.

Следовательно, $< Y, Z >=< Y^X, Z^X >=< Y, Z >^X$ и X нормализует группу $< Y, Z >$. Рассмотрев фактор-группу группы $SU_3(p^{2k}) < X >$ по ее центру, получим, что $[x, < \overline{Y}, \overline{Z} >] = 1$, где $\overline{Y}$ и $\overline{Z}$ образы X и Y в $PSU_3(p^{2k})$, а $< \overline{Y}, \overline{Z} >$ является группой $A_1(p^k)$. Таким образом, x централизует некоторую инволюцию $t \in I(M)$. Рассмотрим $C = C_G(t)$. Так как $x \in C$, то $x \in O(C) \neq 1$. По теореме 4.247 [2] найдется инволюция $u \in C$ и субнормальная подгруппа L в $C_G(u)$ такие, что $L \cong SL_2(q)$, где q — нечетное число и $< O(C), t >$ нормализует L, причем $C_{<O(C),t>}(L) = 1$. Так как $x \in < O(C), t >$, то $x \in N_G(L)$ и, следовательно, $[x, L] = 1$. Противоречие с тем, что $C_{<O(C),t>}(L) = 1$.

(c) $M \cong {}^2G_2(q)$.

В этом случае $C_M(x) \cong {}^2G_2(q_0)$, где $q_0^\alpha = q$. Следовательно, $[x, t] = 1$ для некоторой инволюции $t \in I(M)$ и $x \in C_G(t)$. Так как G — минимальный контрпример к теореме, то $x \in O(C_G(t)) \neq 1$. Противоречие с леммой 1.2.

2. $p = 3$, $M \cong D_4(3^n)$ и x индуцирует либо автоморфизм графа, либо графо-полевой автоморфизм.

Пусть сначала x индуцирует автоморфизм графа. Занумеруем схему Дынкина группы $D_4(3^n)$, обозначив ее вершины цифрами $1, 2, 3, 4$, где вершина 2 соединена со всеми остальными вершинами.

Рассмотрим группу $R =< X_{\varepsilon_2}, X_{-\varepsilon_2} >\cong A_1(3^n)$. Ясно, что x нормализует R, а поэтому $[x, R] = 1$. Таким образом, найдется $t \in I(M)$ для которой $[t, x] = 1$. Теперь, рассуждая как в пункте (b), прийдем к противоречию.

Случай, когда x индуцирует графо-полевой автоморфизм рассматривается аналогично.

(ii) $|x| = r \neq p$.

Пусть сначала $x \notin Inndiag(M)$. Так как $|x| \neq p$, то по лемме 7.3 [4] x индуцирует полевой автоморфизм. Данный случай рассматривается так же как (i) (a)–(c). Поэтому будем считать, что $x \in Inndiag(M)$. Если x содержится в максимальном минизотропном торе, то рассуждения из (ii) §5 переносятся на этот случай почти автоматически, что приводит к противоречию. Таким образом, можно считать, что x содержится в некоторой собственной параболической подгруппе группы G. Легко показать, что $x \in H^*$. Если лиевский ранг группы M больше единицы, то $[x, X_\varepsilon] = 1$ для всех $\varepsilon \in \Phi$. Поэтому $[x, M] = 1$, что невозможно. Следовательно лиевский ранг у M равен единице. Учитывая, что x — нечетное простое число и $x \in Inndiag(M)$ получим, что $M \cong U_3(p^{2k})$. Рассмотрим группу $SU_3(p^{2k})$ и положим, что X — внутренне-диагональный автоморфизм, соответствующий элементу x. Так как $X \in H^*$, то X нормализует унипотентную подгруппу: $U = \left\langle \begin{bmatrix} 1 & a^\tau & b \\ 0 & 1 & -a^\tau \\ 0 & 0 & 1 \end{bmatrix}, \text{ где } Tr(b) + N(a) = 0, a^\tau = a^{p^k}, a, b \in GF \right\rangle$ центром которой является группа

$$Z = \left\langle \begin{bmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \middle| \; b \in GF(p^{2k}), tr(b) = 0 \right\rangle.$$

Из того, что $Z char U$ следует, что X нормализует Z. Точно также можно показать, что X нормализует группу:

$$\tilde{Z} = \left\langle \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ b & 0 & 1 \end{bmatrix} \middle| \; b \in GF(p^{2k}), tr(b) = 0 \right\rangle.$$

Теперь, рассуждая как в пункте (i) (b), прийдем к последнему противоречию. Теорема полностью доказана.

Автор выражает признательность профессору Л.С.Казарину за постоянное внимание к данной работе, а также доктору физико-математических наук И.Д.Супруненко, сделавшей ряд полезных замечаний.

Abstract. It is proved that if G is a finite K-group with an elemnt x such that $\langle x, x^g \rangle$ is of odd order for every $g \in G$, then $x \in O(G)$.

Литература

[1] Л.С.Казарин, *Группы с факторизацией*, Ярославль, 1981. 78 с. ДЕП. ВИНИТИ. № 3900.

[2] Д.Горенстейн, *Конечные простые группы. Введение в их классификацию*, М.: Мир, 1985.

[3] J.H.Conway, R.T.Curtis, S.P.Norton, R.A.Parker, R.A.Wilson, *Atlas of finite groups,* Oxford.: Clarendon Press, 1985.

[4] D.Gorenstein, R.Lyons, *The lokal structure of finite groups of characteristic 2 type,* Mem. Amer. Math. Soc., 276, 1983.

[5] N.Burgoyne, *Finite groups with Chewalley-type components,* Pacific Journal of Math., 72:2 (1977), 341–388.

[6] G.Glauberman, *A characterization of the Suzuki groups,* Ill. J. Math., 12 (1968), 76–98.

[7] А.С.Кондратьев, *Подгруппы конечных групп Шевалле,* Успехи математических наук, 41:1(247) (1986), 57–96.

[8] I.D.Suprunenko, A.A.Premet, *Quadratic modules for Chevalley groups over fields of odd characterisaties,* Math. Nachr., 110:4 (1983), 65–96.

[9] R.W.Carter, *Simple groups of Lie type,* London: Wiley. 1972.

[10] Р.Стейнберг, *Лекции о группах Шевалле,* М.: Мир. 1975.

[11] P.Kleidman, *The maximal subgroups of the Chevalley groups $G_2(q)$ with q odd, the Ree groups ${}^2G_2(q)$, and their automorphism groups,* J. Algebra, 117 (1988), 30–71.

[12] D.M.Bloom, *The subgroups of $PSL(3,q)$ for odd q,* Trans. Amer. Math. Soc., 127:1 (1967), 150–178.

[13] G.M.Seitz, *Generation of finite groups of Lie type,* Trans. Amer. Math. Soc., 271:2 (1982), 351–407.

[14] B.Huppert, *Endliche Gruppen,* B erlin.: Springer–Verlag. 1967.

[15] Р.Лидл, Г.Нидеррайтер, *Конечные поля,* М.: Мир. 1988.

Поступило 6.06.2000

Гомельский государственный университет
им.Ф.Скорины
246019 Гомель, Беларусь