УДК 512.542.5

Большие нильпотентные подгруппы конечных простых групп.

Е. П. Вдовин

В данной работе найдены порядки и строение больших нильпотентных подгрупп во всех конечных простых группах. В частности доказано, что если G — конечная неабелева простая группа, N — ее некоторая нильпотентная подгруппа, то справедливо неравенство $|N|^2 < |G|$.

УДК 512.542.5

Большие нильпотентные подгруппы конечных простых групп.[1]

Е. П. Вдовин

Введение

В данной работе изучаются строение и порядки больших нильпотентных подгрупп в конечных простых группах и конечных группах, близких к простым — конечных группах лиева типа и симметрических группах. Оценки порядков больших нильпотентных подгрупп в конечных простых и близких к простым группам приведены в таблицах 1 и 3. В частности доказано, что если G — некоторая конечная неабелева простая группа, N — ее нильпотентная подгруппа, то $|N|^2 < |G|$ (теорема 1).

Основным иструментом для изучения нильпотентных подгрупп в конечных группах лиева типа является строение централизаторов полупростых элементов, полученное Картером в работах ([1] и [2]). Кроме того, в большинстве конечных простых групп большая нильпотентная подгруппа совпадает с некоторой силовской подгруппой. Поэтому нам потребуются дополнительные сведения о строении силовских подгрупп в конечных простых группах.

Строение силовских подгрупп в симметрических и знакопеременных группах известно довольно давно. Строение силовских подгрупп в конечных группах Шевалле изучалось рядом авторов, см., например, [4], [5] и [6]. Кроме того, Кабанов и Кондратьев в своей обзорной работе [7] указали строение и порядки силовских 2-подгрупп во всех конечных простых группах, кроме спорадических. В недавней работе [8] Зенков и Мазуров доказали, что в каждой конечной простой неабелевой группе для любого простого числа p найдутся две силовские p-подгруппы, имеющие тривиальное пересечение.

Отметим, что порядки и строение больших разрешимых подгрупп в конечных простых и близких к простым группам группах известны. В статье [9] Манн изучил строение и порядки больших разрешимых подгрупп в симметрических и линейных группах, а во всех группах лиева типа порядок и строение больших разрешимых подгрупп получил Сегев [10].

Обозначения и определения, используемые в данной работе можно найти в [11], [12] и [13]. Если G — группа, то запись $H \leqslant G$ означает, что H является подгруппой группы G, $H \trianglelefteq G$ означает, что H является нормальной подгруппой группы G. Через $|G : H|$ обозначается индекс подгруппы H в группе G, $N_G(H)$ — нормализатор подгруппы H в группе G. Если подгруппа H нормальна в G, то через G/H обозначается факторгруппа группы G по H. Если M — подмножество группы G, то через $\langle M\rangle$ обозначается подгруппа, порожденная множеством M, $|M|$ — мощность множества M (или порядок элемента, если вместо множества стоит один элемент). Через $C_G(M)$ обозначается централизатор множества M в группе G, $C_G(G) = \zeta(G)$ — центр группы G. Сопряжение элемента x с помощью элемента y в группе G записывается следующим образом $x^y = y^{-1}xy$. Подгруппа Фиттинга группы G обозначается через $F(G)$, подгруппа Фраттини группы G обозначается через $\Phi(G)$. Если x, y — два элемента группы G, то $[x, y] = x^{-1}y^{-1}xy$ — коммутатор элементов x и y, $[G, G] = G'$ — коммутант группы G. Период группы G обозначается $\exp(G)$. $A \times B$ обозначает прямое произведение групп A и B, $A * B$ — центральное произведение групп A и B.

[1]Работа выполнена при поддержке ФЦП "Интеграция"проект 274, РФФИ, грант 99–01–00550 и международной соросовской программы образования в области точных наук, грант s99-56.

Пусть π — некоторое подмножество множества простых чисел. Тогда для конечной группы G через $O_\pi(G)$ обозначается наибольшая нормальная подгруппа группы G, порядок которой делится только на числа из π, $O^\pi(G)$ — нормальная подгруппа, порожденная элементами, порядок которых не делится на простые числа из π. Под большой нильпотентной подгруппой конечной группы G всегда понимается нильпотентная подгруппа наибольшего порядка.

Если φ — гомоморфизм группы G, g — элемент группы G, то G^φ, g^φ — образы группы G и элемента g относительно гомоморфизма φ, соответственно. Если φ — некоторый автоморфизм группы G, то через G_φ обозначено множество неподвижных точек автоморфизма φ.

Обозначения, связанные с конечными группами лиева типа, выбраны также, как в [12]. Под группой Шевалле, если не оговорено противное, понимается как универсальная группа Шевалле, так и любая ее факторгруппа по подгруппе из центра. При изучении групп Шевалле $GF(q)$ будет обозначать поле порядка q, p — его характеристику, $GF(q)^*$ — мультипликативную группу поля $GF(q)$. Группа Шевалле, соответствующая корневой системе Φ над полем $GF(q)$, обозначается через $\Phi(q)$. Группа Вейля, соответствующая корневой системе Φ, обозначается $W(\Phi)$. Скрученные группы будут обозначаться символами ${}^2A_n(q^2)$, ${}^2D_n(q^2)$, ${}^2E_n(q^2)$, ${}^3D_4(q^3)$, ${}^2B_2(q)$, ${}^2G_2(q)$ и ${}^2F_2(q)$. Φ^+ обозначает множество положительных корней корневой системы Φ, $\Delta = \{r_1, \dots, r_k\}$ — множество фундаментальных корней, причем нумерация выбирается как в [12, (3.4)]. Элемент x из группы Шевалле $\Phi(q)$ называется полупростым, если его порядок взаимно прост с p, и он называется унипотентным, если его порядок является степенью p. Аналогично, полупростая и унипотентная подгруппы группы $\Phi(q)$ определяются как подгруппы, порядок которых взаимно прост с p (p'-подгруппы) и является степенью p, соответственно. Расширенной диаграммой Дынкина группы Шевалле G называется диаграмма, которая получается после добавления к исходной диаграмме Дынкина корня $-r_0$ (здесь r_0 — корень максимального веса) и присоединения его к остальным вершинам по обычному правилу.

Автор выражает искреннюю благодарность Мазурову Виктору Даниловичу за полезные консультации и ценные замечания. Автор также благодарен Васильеву Андрею Викторовичу за чтение и обсуждение рукописи, которое позволило исправить многие ошибки и неточности первоначального варианта.

1 Вспомогательные результаты для алгебраических групп

В этом разделе будут приведены необходимые сведения о строении линейных алгебраических групп (в дальнейшем, для краткости слово «линейных» мы будем опускать), а также будут получены вспомогательные утверждения, которые мы используем для получения оценок порядков нильпотентных подгрупп. Основные определения и результаты о строении и свойствах алгебраических групп можно найти в [13]. Если G — алгебраическая группа, то через G^0 обозначена компонента единицы группы G. Алгебраическая группа называется полупростой, если ее радикал тривиален и алгебраическая группа называется редуктивной, если ее унипотентный радикал тривиален (в обоих случаях не предполагается, что алгебраическая группа связна). Хорошо известно (см., например [13]), что связная полупростая алгебраическая группа — это центральное произведение связных простых алгебраических групп, а связная редуктивная алгебраическая группа G — это произведение тора S и полупростой группы M, причем $S = \zeta(G)^0$, $M = [R, R]$ и группа $S \cap M$ конечна.

Если G — связная редуктивная алгебраическая группа, то пусть T — ее максимальный тор (под тором всегда понимается связная диагонализируемая группа), B — подгруппа Бореля, содержащая тор T. Кроме того, существует такая борелевская подгруппа B^-, что $B \cap B^- = T$. Пусть Φ — корневая система относительно тора T, $\varphi : N_G(T) \to N_G(T)/T = W$ — канонический гомоморфизм на группу Вейля W группы G, X_α — корневые подгруппы относительно тора T (одномерные T-инвариантные унипотентные подгруппы групп B и B^-). Действие группы Вейля W на корневой системе Φ определяется следующим образом ([13, 24.1]). Пусть для каждого элемента w из W взят некоторый его представитель n_w из группы G. Тогда группа Вейля действует на корнях корневой системы Φ по правилу $\alpha^w(t) = \alpha(t^{n_w})$ для всех $\alpha \in \Phi$, $t \in T$. Аналогичным образом группа Вейля действует на весах представления π группы G. Хорошо известно, что $B = TU$, где $U = \langle X_\alpha : \alpha \in \Phi^+ \rangle$ — максимальная унипотентная подгруппа группы G, а $B^- = TU^-$, где через U^- обозначена, группа $\langle X_\alpha : \alpha \in \Phi^- \rangle$. Если на положительных корнях корневой системы Φ задать порядок, то любой элемент из U единственным образом записывается в виде произведения элементов из корневых подгрупп X_α (взятых в заданном порядке).

Пусть G — связная редуктивная группа. Зафиксируем для каждого элемента из группы Вейля W его представителя n_w из группы G. Тогда любой элемент группы G единственным образом представим в виде un_wtv, где $v \in U$, $t \in T$, $u \in U \cap n_wU^-n_w^{-1}$ (см., например, [13, теорема 28.3]). Такое представление элементов группы G называется разложением Брюа. Кроме того, в любой связной редуктивной группе каждый полупростой элемент содержится в некотором максимальном торе, а каждый унипотентный элемент содержится в некоторой максимальной (и связной) унипотентной подгруппе.

Пусть G — связная простая алгебраическая группа, π — ее некоторое рациональное представление, Γ_π — решетка, порожденная весами представления π. Через Γ_{ad} обозначается решетка, порожденная корнями системы Φ, через Γ_{sc} — решетка, порожденная фундаментальными весами. Известно, что справедливы следующие включения $\Gamma_{ad} \leqslant \Gamma_\pi \leqslant \Gamma_{sc}$.

Известно, что для корневой системы данного типа существует несколько различных простых алгебраических групп, которые называются изогениями. Они различаются строением группы Γ_π и порядком конечного центра. В том случае, когда решетка Γ_π совпадает с Γ_{sc}, говорят, что группа G односвязна и она обозначается G_{sc}. Если решетка Γ_π совпадает с Γ_{ad}, то говорят, что группа G имеет присоединенный тип и она обозначается G_{ad}. Любая группа с корневой системой данного типа получается из группы G_{sc} как факторгруппа по подгруппе из центра. Центр группы G_{ad} тривиален и она проста как абстрактная группа.

Пусть c_i — коэффициент, с которым фундаментальный корень r_i входит в разложение корня r_0. Простые числа, делящие коэффициенты c_i, называются *плохими* простыми числами.

Далее напомним несколько фундаментальных результатов о строении алгебраических групп.

Лемма 1.1. *[13, теорема 15.3]. Пусть G — алгебраическая группа. Тогда для любого $x \in G$ существуют такие элементы $s, u \in G$, что $x = su = us$, элемент s полупрост (и называется полупростой частью элемента x, в дальнейшем он будет обозначаться через x_s), элемент u унипотентен (и называется унипотентной частью элемента x, в дальнейшем он будет обозначаться x_u) и такие элементы s и u единственны. Разложение элемента x в виде x_sx_u называется разложением Жордана.*

Лемма 1.2. *[13, теорема 21.3 и теорема 22.2]. Пусть G — связная алгебраическая группа. Тогда все подгруппы Бореля группы G сопряжены. Более того, максимальные торы и максимальные связные унипотентные подгруппы — это в точности максимальные торы* *и максимальные связные унипотентные подгруппы групп Бореля. Кроме того, все максимальные торы и максимальные связные унипотентные группы сопряжены и любой полупростой (унипотентный) элемент лежит в некотором максимальном торе (максимальной связной унипотентной подгруппе).*

Теперь напомним, каким образом связаны конечные группы лиева типа и простые алгебраические группы. Пусть G — простая алгебраическая группа, определенная над алгебраически замкнутым полем характеристики $p > 0$, σ — эндоморфизм группы G такой, что множество его неподвижных точек G_σ конечно. Эндоморфизм σ с таким условием в дальнейшем будет называться автоморфизмом Фробениуса, хотя он может и не совпадать с классическим автоморфизмом Фробениуса. Отметим, что σ является автоморфизмом, если группа G рассматривается как абстрактная группа и σ является эндоморфизмом, если G рассматривается как алгебраическая группа. В общем случае σ имеет вид $q\sigma_0$, где $q = p^\alpha$ — возведение в q-ую степень, а σ_0 — графовый автоморфизм порядка 1, 2 или 3. Тогда $O^{p'}(G_\sigma)$ — группа лиева типа над конечным полем характеристики p и любую группу лиева типа (нормальную или скрученную) можно получить таким образом.

Пусть T — максимальный σ-инвариантный тор связной простой алгебраической группы G. В дальнейшем *максимальным тором* группы G_σ (соответственно $O^{p'}(G_\sigma)$) будем называть группу T_σ (соответственно $T_\sigma \cap O^{p'}(G_\sigma)$).

Далее мы докажем вспомогательный результат, который будет использоваться при изучении нильпотентных подгрупп в конечных группах Шевалле.

Лемма 1.3. *Пусть G — связная редуктивная линейная алгебраическая группа над алгебраически замкнутым полем характеристики p, R — ее редуктивная (не обязательно связная) подгруппа максимального ранга, причем $(|R : R^0|, p) = 1$, $s \in R^0$ — некоторый полупростой элемент, и T — произвольный максимальный тор в R^0, содержащий элемент s. Тогда группа $C_R(s)$ редуктивна (хотя не обязательно связна). Она порождается тором T вместе с теми корневыми подгруппами U_α, для которых $\alpha(s) = 1$, и теми представителями элементов группы Вейля $n_w \in N_R(T)$, которые коммутируют с s. Компонента единицы $C_R(s)^0$ порождается тором T и теми U_α, для которых $\alpha(s) = 1$. В частности, группа $C_R(s)/C_R(s)^0$ изоморфна некоторой секции группы Вейля для G. Более того, все унипотентные элементы из $C_R(s)$ лежат в $C_R(s)^0$.*

Доказательство. Зафиксируем подгруппу Бореля B группы R^0, содержащую T. Ясно, что все указанные в лемме порождающие лежат в $C_R(s)$. Докажем, что $C_R(x)$ порождается указанными в лемме элементами. Покажем сначала, что в группе R (которая не обязательно связна) имеет место разложение Брюа. Пусть x — произвольный элемент из R. Тогда B^x — некоторая подгруппа Бореля группы R^0. В силу леммы 1.2 существует такой элемент $s \in R^0$, что $B^x = B^s$. Тогда элемент xs^{-1} нормализует подгруппу B. Тор $T^{xs^{-1}}$ является максимальным тором группы B. Поскольку все максимальные торы в B сопряжены (лемма 1.2), существует такой элемент g из B, что $T^{xs^{-1}} = T^g$. Поэтому можно считать, что xs^{-1} нормализует тор T. Тогда $xs^{-1} = n_w t$ для некоторого $n_w \in N_R(T)$, $t \in T$. Поскольку t нормализует B и xs^{-1} нормализует B, элемент n_w также нормализует B, значит, он нормализует U — максимальную (связную) унипотентную подгруппу группы B. Поскольку s лежит в R^0, для него существует разложение Брюа, т. е. он представим в виде $u_1 n_{w_1} t_1 v_1$, где $u_1 \in U \cap n_{w_1} U^- n_{w_1}^{-1}$, $n_{w_1} \in N_{R^0}(T)$, $t \in T$ и $v_1 \in U$. Поэтому элемент x представим в виде $x = n_w t u_1 n_{w_1} t_1 v_1$. Поскольку элементы t и n_w нормализуют U, мы получаем представление элемента x в виде $x = u_2 n_{w_2} t_2 v_2$, причем $u_2 \in U \cap n_{w_2} U^- n_{w_2}^{-1}$, $n_{w_2} \in N_R(T)$, $t_2 \in T$ и $v_2 \in U$. Поскольку это разложение Брюа совпадает с разложением Брюа элемента x в группе G, такое разложение единственно.

Если $x \in C_R(s)$, то с помощью разложения Брюа можно записать $x = un_wtv$, где $v \in U$, $t \in T$, $u \in U \cap n_wU^-n_w^{-1}$. Поскольку s нормализует U, $N(T)$, U^- и коммутирует с x единственность разложения влечет, что каждый из u, n_w, v коммутирует с s. Более того, поскольку s нормализует каждую корневую подгруппу U_α, единственность разложения группы U в произведение корневых подгрупп U_α ($\alpha > 0$) влечет, что $\alpha(s) = 1$ как только u или v содержит нетривиальный множитель из U_α. Таким образом, x лежит в группе, порожденной тором T и теми U_α, n_w, которые перестановочны с s.

Поскольку T и все U_α с $\alpha(s) = 1$ связны, то подгруппа H, порожденная ими, замкнута, связна и нормальна в $C_R(s)$. Так как группа Вейля конечна, $|G_R(s) : H| < \infty$, значит, $H = C_R(s)^0$.

Так как корни группы $C_R(s)$ относительно тора T возникают парами (т. е. если $\alpha(s) = 1$, то и $-\alpha(s) = 1$), группа $C_R(s)$ редуктивна. Действительно, если $C_R(s)$ имеет нетривиальный унипотентный радикал V, то он нормализуется тором T, значит, содержит некоторую корневую подгруппу U_α. V нормализуется корневой группой $U_{-\alpha}$, что дает неунипотентный элемент в V, противоречие.

Поскольку $(|R : R^0|, p) = 1$, все унипотентные элементы из группы R лежат в R^0, поэтому все унипотентные элементы из $C_R(s)$ лежат в $C_{R^0}(s)$. Тот факт, что в связной редуктивной группе R^0 любой унипотентный элемент из $C_{R^0}(s)$ лежит в $C_{R^0}(s)^0$ хорошо известен, см. например [14, теорема 2.2]. $\square$

Пусть $x \in G$ — полупростой элемент. Тогда, в силу предыдущей леммы, $C_G^0(x)$ — связная редуктивная подгруппа максимального ранга и $[C_G^0(x), C_G^0(x)]$ — полупростая группа, корневая система которой является аддитивно замкнутой подсистемой корневой системы группы G. Такие подгруппы в дальнейшем будут называться *подсистемными* подгруппами. Поскольку в данной работе изучаются конечные группы, особый интерес представляют элементы простого порядка $r \neq p$. Оказывается, что имеет место следующая лемма.

Лемма 1.4. *[15, 14.1]. Пусть G — простая связная алгебраическая группа и элемент $x \in G$ имеет простой порядок $r \neq p$. Пусть $C' = [C_G^0(x), C_G^0(x)]$ — подсистемная подгруппа. Если Δ — диаграмма Дынкина корневой системы группы C', то справедливо одно из следующих утверждений:*

1. *Δ получается удалением вершин из диаграммы Дынкина группы G;*

2. *Δ получается из расширенной диаграммы Дынкина группы G удалением одной вершины r_i, где $r = c_i$ — коэффициент корня r_i в самом длинном корне r_0.*

В частности, если r не является плохим простым для группы G, то $\dim(\zeta^0(C_G^0(x))) \geqslant 1$.

2 Большие нильпотентные подгруппы

В данном разделе изучаются большие нильпотентные подгруппы в конечных простых группах и группах близких к простым. Данный раздел разбит на четыре части. В первой изучаются большие нильпотентные подгруппы в симметрических и знакопеременных группах. Во второй и третьей изучаются конечные группы лиева типа, в четвертой — спорадические группы. В большинстве случаев большая нильпотентная группа совпадает с некоторой силовской подгруппой. Если G — конечная группа, то через $Syl_p(G)$ обозначается множество силовских p-подгрупп группы G. Через $N(G)$ обозначено множество больших нильпотентных подгрупп конечной группы G, через $n(G)$ — порядок произвольного элемента из $N(G)$.

2.1 Большие нильпотентные подгруппы симметрических и знакопеременных групп

Пусть G — некоторая подгруппа группы S_n. Тогда множество $\{1, \dots, n\}$ относительно действия группы G разбивается на непересекающиеся подмножества (орбиты), на каждом из которых группа G действует транзитивно.

Докажем сначала следующую техническую лемму.

Лемма 2.1. *Пусть N — нильпотентная подгруппа группы S_n и $I_1, I_2, \dots$ — множество орбит центра $\zeta(N)$ группы N на множестве $\{1, \dots, n\}$ Пусть J_1 — набор множеств I_m порядка 1, J_2 — набор множеств I_m порядка 2 и т. д. Пусть $K_1 = \bigcup_{|I_m|=1} I_m$, $K_2 = \bigcup_{|I_m|=2} I_m$ и т. д. Тогда справедливы следующие утверждения.*

1. *Группа $N/\zeta(N)$ переставляет множества одного порядка и, следовательно, $N \leqslant N_1 \times N_2 \times \dots$, где $N_1 \leqslant S_{K_1}$, $N_2 \leqslant S_{K_2}$ и т. д.*
2. *Если k_i — количество орбит относительно действия группы $N/\zeta(N)$ на множестве J_i, то $|\zeta(N) \cap N_i| = i^{k_i}$.*
3. *Если $p_1, \dots, p_s$ — все простые числа, на которые делится i, то порядок группы N_i делится только на простые числа $p_1, \dots, p_s$.*

Доказательство. Пусть σ — некоторый элемент из группы N, который переводит некоторый элемент i из множества I_1 в элемент из некоторого множества I_k. Тогда для любого $\tau \in \zeta(N)$ справедливо $i^{\sigma\tau} = i^{\tau\sigma} \in I_k$. Поскольку $\zeta(N)$ на множестве I_1 действует транзитивно, мы имеем $\{i^\tau : \tau \in \zeta(N)\} = I_1$, следовательно, $I_1^\sigma \subseteq I_k$, т. е. $|I_1| \leqslant |I_k|$. С другой стороны, элемент σ^{-1} переводит некоторый элемент множества I_k в элемент i из множества I_1, следовательно, $I_k^{\sigma^{-1}} \subseteq I_1$, т. е. $|I_k| \leqslant |I_1|$. Объединяя полученные неравенства, получаем, что $|I_1| = |I_k|$. Пункт 1 леммы доказан.

Докажем теперь пункт 2. Можно считать, что $K_i = \{1, \dots, n\}$ и группа $N/\zeta(N)$ действует транзитивно на орбитах (относительно действия центра $\zeta(N)$) множества J_i. Пусть $\{I_1, \dots, I_k\}$ — множество всех орбит множества J_i относительно действия группы $\zeta(N)$. Тогда порядок каждой из них равен i и $i \cdot k = n$. Пусть $l \in I_1$ — некоторый элемент из орбиты I_1. Рассмотрим стабилизатор элемента l в центре $\zeta(N)$ — $St_{\zeta(N)}(l)$ и предположим, что $\tau \in St_{\zeta(N)}(l)$. Пусть $m \in K_i$ — некоторый элемент, лежащий в некоторой орбите I_j. Поскольку группа $N/\zeta(N)$ действует транзитивно на орбитах $I_1, \dots, I_k$, существует такой элемент $\sigma \in N$, что $I_j^\sigma = I_1$. Далее, группа $\zeta(N)$ действует транзитивно на множестве I_1, поэтому существует такой элемент $\varphi \in \zeta(N)$, для которого $(m^\sigma)^\varphi = l$. Тогда $m^\tau = ((l^{\varphi^{-1}})^{\sigma^{-1}})^\tau = ((l^\tau)^{\varphi^{-1}})^{\sigma^{-1}} = m$, следовательно, $\tau = \varepsilon$ и $St_{\zeta(N)}(l) = \{\varepsilon\}$. В силу теоремы Лагранжа $|\zeta(N)| = |\zeta(N) : St_{\zeta(N)}(l)| \cdot |St_{\zeta(N)}(l)| = i$.

Далее, по определению, множество J_i равно $\{I_k : |I_k| = i\}$. Предположим, что существует такое простое число $q \notin \{p_1, \dots, p_s\}$, которое делит порядок группы N_i. Поскольку N_i — нильпотентная группа, существует центральный элемент τ порядка q. Поскольку группа N является прямым произведением групп $N_1, N_2, \dots$, элемент τ лежит в $\zeta(N)$. Из пункта 2 следует, что $|\zeta(N) \cap N_i| = i^k$, где $k \geqslant 1$. Но тогда τ лежит в $\zeta(N) \cap N_i$, но $|\tau|$ не делит $|\zeta(N) \cap N_i|$, противоречие. $\square$

Отметим, что группа N_1, определенная в лемме, тривиальна.

Теперь мы можем определить строение больших нильпотентных подгрупп в симметрических и знакопеременных группах.

Теорема 2.1. *Большая нильпотентная подгруппа в знакопеременной группе сопряжена с одной из следующих групп:*

1. $\langle(1,2,3)\rangle$ *если* $n = 3$.
2. $\langle(1,2,3,4,5)\rangle$ *если* $n = 5$.
3. $\langle(1,2,3)\rangle \times \langle(4,5,6)\rangle$ *если* $n = 6$.
4. $Syl_2(A_n)$ *если* $n \neq 2(2k+1)+1$ *для некоторого натурального* k.
5. $Syl_2(A_{n-3}) \times \langle(n-2, n-1, n)\rangle$ *если* $n = 2(2k+1)+1$, $k \geqslant 1$.

Большая нильпотентная подгруппа в симметрической группе сопряжена с одной из следующих групп.

1. $Syl_2(S_n)$ *если* $n \neq 2(2k+1)+1$ *для некоторого натурального* k.
2. $Syl_2(S_{n-3}) \times \langle(n-2, n-1, n)\rangle$ *если* $n = 2(2k+1)+1$ *для некоторого натурального* k.

Во всех группах большая нильпотентная подгруппа единственна с точностью до сопряжения.

Доказательство. Предположим, что утверждение теоремы неверно и n — минимальное натуральное число, дающее контрпример к утверждению теоремы. Обозначим за P подгруппу группы S_n, строение которой совпадает со строением нильпотентной подгруппы, указанной в лемме и пусть $N \in N(S_n)$ — некоторая большая нильпотентная подгруппа, несопряженная с p

Относительно действия $\zeta(N))$ множество $\{1, \ldots, n\}$ разбивается на орбиты. Возможны следующие два случая.

1. Среди орбит центра $\zeta(N)$ есть подмножества разного порядка. Тогда по лемме 2.1 группа $N(S_n)$ является подгруппой в прямом произведении групп $N_1 \leqslant S_{n_1}$ и $N_2 \leqslant S_{n_2}$, причем $n_1 + n_2 = n$. Поскольку n — минимальное натуральное число, для которого не выполняется утверждение теоремы, группы из $N(S_{n_1})$ и $N(S_{n_2})$ имеют такое строение, как указано в лемме.

Пусть $n_1 \neq 2(2k+1)+1$, тогда $|N_1| \leqslant |S|$, где $S \in Syl_2(S_{n_1})$. В зависимости от того, представимо ли число n_2 в виде $2(2k+1)+1$ или нет, мы получаем следующие оценки порядка группы N_2: $|N_2| \leqslant 3|S_1|$, либо $|N_2| \leqslant |S_2|$, где $S_1 \in Syl_2(S_{n_2-3}$, а $S_2 \in Syl_2(S_{n_2})$. В первом случае мы имеем $|N| \leqslant |N_1| \cdot |N_2| \leqslant |Syl_2(S_{n_1})| \cdot 3|Syl_2(S_{n_2-3})| \leqslant 3|Syl_2(S_{n-3})| \leqslant |P|$, причем равенство может достигаться лишь в том случае, когда $N_1 \in Syl_2(S_{n_1})$, $N_2 = S_1 \times \langle(k_1, k_2, k_3)\rangle$, т. е. когда с точностью до сопряжения выполнено равенство $N = P$. Поскольку n — минимальное число, дающее контрпример, такого быть не может. Аналогично разбирается случай, когда $N_2 \in Syl_2(S_{n_2})$.

Пусть $n_1 = 2(2k_1+1)+1$, $n_2 = 2(2k_2+1)+1$. Тогда $|N(G)| \leqslant 3|S_3| \cdot 3|S_1| < |Syl_2(S_n)| = |P|$, где $S_3 \in Syl_2(S_{n_1-3})$, следовательно, и в этом случае мы приходим к противоречию. Таким образом, первый случай, когда среди орбит существуют подмножества разного порядка невозможен.

2. Все орбиты относительно действия группы $\zeta(N)$ одинакового порядка k. Пусть $I_1, \ldots,$ $I_{\frac{n}{k}}$ — все орбиты множества $\{1, \ldots, n\}$ относительно действия группы $\zeta(N)$. В том случае, когда действие группы $N/\zeta(N)$ на множестве орбит $I_1, \ldots, I_{\frac{n}{k}}$ не является транзитивным, группа N является подгруппой прямого произведения групп N_1 и N_2, каждая из которых является нильпотентной подгруппой в симметрической группе меньшей степени. Также как в первом случае можно доказать, что тогда N не является контрпримером.

Пусть группа N на орбитах $I_1, \ldots, I_{\frac{n}{k}}$ действует транзитивно. В силу леммы 2.1(2) порядок центра $\zeta(N)$ равен k, группу $N/\zeta(N)$ можно рассматривать как нильпотентную подгруппу группы $S_{\frac{n}{k}}$, поэтому $|N| \leqslant k \cdot |N_3|$, где $N_3 \in N(S_{\frac{n}{k}})$. Нетрудно проверить, что в этом случае $|N| \leqslant |Syl_2(S_n)|$, кроме $n = k = 3$. Теорема для симметрических групп доказана.

Рассмотрим теперь знакопеременные группы. Пусть n — минимальное натуральное число, при котором существует контрпример к утверждению теоремы и пусть $N \in N(A_n)$ — этот контрпример. Пусть R обозначает нильпотентную подгруппу группы A_n, которая совпадает с большей нильпотентной группой, указанной в теореме. Как и в случае симметрических групп возможны два случая.

1. Действие группы $N/\zeta(N)$ на множестве орбит центра $\zeta(N)$ не является транзитивным. Тогда либо группа N содержится в прямом произведении нильпотентных групп N_1 и N_2, каждая из которых является нильпотентной подгруппой в знакопеременной группе меньшей размерности, либо она лежит в прямом произведении двух нильпотентных групп N_1 и N_2, каждая из которых является нильпотентной подгруппой в симметрической группе меньшей размерности, но не совпадает с этим прямым произведением. Нетрудно проверить, используя известные порядки больших нильпотентных подгрупп в симметрических группах, что в этом случае N не является контрпримером.

2. Группа $N/\zeta(N)$ на множестве орбит действует транзитивно. Пусть порядок каждой из орбит равен k. Тогда в силу леммы 2.1 $|\zeta(N)| = k$ и группу $N/\zeta(N)$ можно рассматривать как нильпотентную подгруппу группы $S_{\frac{n}{k}}$. Нетрудно проверить, что при $n \geqslant 7$ справедливо неравенство $k|N_4| \leqslant \frac{1}{2}|S| \leqslant |R|$, где $N_4 \in N(A_{\frac{n}{k}})$ и $S \in Syl_2(S_n)$. $\square$

Таблица 1.

Группа G	$n(G)$	Строение
A_3	3	$\langle(1,2,3)\rangle$
A_5	5	$\langle(1,2,3,4,5)\rangle$
A_6	9	$\langle(1,2,3)\rangle \times \langle(4,5,6)\rangle$
A_n, $n \neq 2(2k+1)+1$	$\frac{1}{2}2^{[n/2]+[n/2^2]+\ldots}$	S, где $S \in Syl_2(A_n)$
A_n, $n = 2(2k+1)+1$	$\frac{3}{2}2^{[(n-3)/2]+[(n-3)/2^2]+\ldots}$	$S \times \langle(n-2, n-1, n)\rangle$, $S \in Syl_2(A_{n-3})$
S_n, $n \neq 2(k+1)+1$	$2^{[n/2]+[n/2^2]+\ldots}$	S, $S \in Syl_2(S_n)$
S_n, $n = 2(2k+1)+1$	$3 \cdot 2^{[(n-3)/2]+[(n-3)/2^2]+\ldots}$	$S \times \langle(n-2, n-1, n)\rangle$, $S \in Syl_2(S_{n-3})$

2.2 Общее строение нильпотентных подгрупп в простых алгебраических группах

Лемма 2.2. *Пусть N — замкнутая нильпотентная подгруппа связной простой алгебраической группы G. Тогда существует редуктивная подгруппа R группы G максимального ранга, содержащая группу N. Пусть W_1 — группа Вейля группы R^0. Тогда справедливы следующие утверждения.*

1. *$N = N_s \times N_u$, т. е. группа N представима в виде прямого произведения своих подгрупп, состоящих из полупростых и унипотентных элементов.*
2. *$N_u \leqslant R^0$ и $\zeta(N_s) \cap R^0 \leqslant \zeta(R^0)$.*
3. *Если $N_0 = N \cap R^0$, то тогда N/N_0 изоморфно вкладывается в группу $N_W(W_1)/W_1$.*

Если группа N состоит из σ-неподвижных элементов относительно некоторого автоморфизма Фробениуса σ, то группа R является σ-инвариантной.

Доказательство. Пусть N — некоторая замкнутая нильпотентная подгруппа связной простой алгебраической группы, определенной над алгебраическим замыканием поля $GF(q)$. Тогда группа N состоит из элементов конечного порядка и, в силу ([11, теорема 12.1.1]) представима в виде прямого произведения своих p-подгрупп. В частности, группа N представима в виде $N_s \times N_u$ — прямого произведения своей полупростой и унипотентной частей, соответственно.

Если группа N_s нетривиальна, то тогда ее центр также нетривиален. Ясно, что $\zeta(N_s) = (\zeta(N))_s$. Пусть x — некоторый элемент из $\zeta(N_s)$. Тогда группа N лежит в $C_G(x)$, причем N_u лежит в R^0. Обозначим группу $C_G(x)$ за R. В силу леммы 1.3 R является редуктивной подгруппой группы G максимального ранга. Предположим, что существует элемент s из $\zeta(N_s) \cap R^0$, не лежащий в $\zeta(R^0)$. Тогда рассмотрим группу $C_R(s)$. Ясно, что $N \leqslant C_R(s)$ и $N_u \leqslant R^0$. Кроме того, $C_R(s)$ — редуктивная подгруппа группы G максимального ранга. Поскольку размерность группы R на каждом шаге понижается, данный процесс конечен, так как размерность группы G конечна. Повторяя указанный выше процесс, получим редуктивную подгруппу R группы G максимального ранга, содержащую N. Заметим, что в том случае, когда N состоит из неподвижных точек относительно некоторого автоморфизма Фробениуса σ, группа R σ-инвариантна. Пункты 1 и 2 леммы доказаны.

Докажем пункт 3. Имеем $N/N_0 = NR^0/N_0R^0 \leqslant R/R^0$. Из доказательства леммы 1.3 следует, что любой элемент из R представим в виде nx, где $n \in N_R(T)$ для некоторого максимального тора T группы R^0, а $x \in R^0$. Поскольку R^0 нормальна в R, группа $N_R(T)/T$ содержится в группе $N_W(W_1)$. Отсюда получаем, что $R/R^0 \cong N_R(T)/N_{R^0}(T) \leqslant N_W(W_1)/W_1$ $\square$

Замечание. Из леммы 2.2 следует, что группа $N_0/\zeta(N_0)$ является нильпотентной подгруппой в прямом произведении простых алгебраических групп меньшей размерности — группе $R^0/\zeta(R^0)$. Таким образом, данная лемма обобщает результат [16] о строении полупростых нильпотентных подгрупп в обобщенных линейных группах над конечными полями.

Строение связных редуктивных подгрупп R группы G максимального ранга, а также подгрупп R_σ известно, см. [1], [2] и [3], поэтому для изучения нильпотентных подгрупп в конечных группах лиева типа нам осталось найти порядки больших нильпотентных подгрупп в группах Вейля. Группы Вейля для типов B_n, C_n и D_n являются сплетением 2-группы и симметрической группы S_n. Используя информацию, полученную ранее о строении нильпотентных подгрупп в симметрических группах, можно легко сделать вывод, что большая нильпотентная подгруппа в группе Вейля для этих типов — это в точности силовская 2-группа. В таблице 2 ниже будут указаны оценки порядков больших нильпотентных подгрупп в группах Вейля для всех классических групп и их строение

Таблица 2.

Тип системы Φ	Строение групп $N(W(\Phi))$	Оценка для $n(W(\Phi))$
A_n	см. табл. 1	2^{n+1}
B_n и C_n	лежат в $Syl_2(W)$	2^{2n}
D_n	лежат в $Syl_2(W)$	2^{2n-1}

2.3 Большие нильпотентные подгруппы конечных групп лиева типа

В этой части мы применим общие свойства нильпотентных подгрупп, полученные ранее, к конечным группам лиева типа. В частности будет доказано, что большая нильпотентная подгруппа в большинстве случаев совпадает с максимальной унипотентной подгруппой. Большие нильпотентные подгруппы в конечных группах Шевалле находятся однотипно, поэтому в качестве примера будет разобрана группа $A_n(q)$.

Пусть N — некоторая нильпотентная подгруппа группы $A_n(q)$, покажем, что ее порядок не превосходит порядка наибольшей нильпотентной группы, указанного в таблице 3. Можно считать, что центр группы $A_n(q)$ тривиален. Тогда в силу леммы 2.2 группа N содержится в некоторой собственной редуктивной подгруппе максимального ранга связной простой алгебраической группы типа A_n.

Напомним сначала какое строение имеют редуктивные подгруппы максимального ранга в простой связной алгебраической группе типа A_n и как устроены их неподвижные точки относительно автоморфизма Фробениуса σ (см. [2]). Предположим, что группа G имеет тип A_n. Эндоморфизм σ группы G индуцирует эндоморфизм группы характеров X тора T, также называемый σ, который обладает свойством, что $\sigma = q\sigma_0$, где q — степень числа p и σ_0 — изометрия группы X. σ_0 имеет порядок 1 или 2 в зависимости от того, будет ли группа G_σ нормальной или скрученной. X содержит множество Φ корней и Φ удобно записать в виде $\Phi = \{e_i - e_j : i \neq j, i, j \in \{0, 1 \ldots, n\}\}$, где $e_0, e_1, \ldots, e_n$ образуют ортонормированный базис $(n+1)$-мерного евклидова пространства. Группа Вейля W действует на этом пространстве, переставляя базисные элементы, в соответствии с симметрической группой S_{n+1}. σ_0 действует на корнях либо тождественно, либо как элемент порядка 2.

Корневая система любой σ-инвариантной редуктивной подгруппы группы G эквивалентна относительно W системе Φ_1 следующего типа. Пусть $\lambda = (\lambda_1, \lambda_2, \ldots)$ — разбиение числа $n+1$ и пусть $I_1, I_2, \ldots$ — непересекающиеся подмножества множества $\{0, 1, \ldots, n\}$ с условием $|I_1| = \lambda_1$, $|I_2| = \lambda_2$, ... Пусть $\Phi_1 = \{e_i - e_j \in \Phi : i, j \in I_\alpha$ для некоторого $\alpha\}$. Тогда Φ_1 — подсистема системы Φ типа $A_{\lambda_1-1} \times A_{\lambda_2-1} \times \ldots$, и она будет σ-инвариантной при условии, что, когда σ_0 имеет порядок 2, Φ_1 неподвижна относительно линейного преобразования, определенного правилом $e_i \to -e_{n-i}$.

Лемма 2.3. *[2, предложение 7]. Пусть G — группа типа A_l и пусть эндоморфизм σ таков, что группа G_σ нормального типа. Пусть G_1 — редуктивная подгруппа максимального ранга в G, соответствующая разбиению λ числа $l+1$. Пусть G_1^g — σ-инвариантная подгруппа группы G, получаемая скручиванием группы G_1 посредством элемента $w \in W$, определенного правилом $\pi(g^\sigma g^{-1}) = w$. Предположим, w отображается в τ относительно гомоморфизма $N_W(W_1) \to Aut_W(\Delta_1)$. Пусть n_i — количество частей разбиения λ, равных i, отсюда следует, что $Aut_W(\Delta_1) \cong S_{n_2} \times S_{n_3} \times \ldots$. Предположим, что τ дает разбиения $\mu^{(2)}, \mu^{(3)}, \ldots$ чисел $n_2, n_3, \ldots$, соответственно. Тогда простые компоненты полупростой группы $(M^g)_\sigma$ имеют тип $A_{i-1}(q^{\mu_j^{(i)}})$ в точности с одной компонентой для каждого $i = 2, 3, \ldots$ и каждой части $\mu_j^{(i)}$ разбиения $\mu^{(i)}$.*

Порядок полупростой части $(S^g)_\sigma$ группы $(G_1^g)_\sigma$ дается формулой

$$(q-1)|(S^g)_\sigma| = \prod_{i,j}(q^{\mu_j^{(i)}} - 1).$$

Поскольку центр группы $A_n(q)$ предполагается тривиальным, порядок централизатора, указанный в лемме 2.3, необходимо умножить на дробь $\frac{1}{(n+1,q-1)}$. Действительно, в том случае, когда G не является односвязной группой, конечная группа $O^{p'}(G_\sigma)$ не совпадает с G_σ, поэтому порядок централизатора меньше, чем тот, что указан в лемме. В этом случае $G_\sigma = \hat{H}O^{p'}(G_\sigma)$, причем $|\hat{H} : H| = \frac{d_1}{d}$. Здесь $\hat{H}$ — максимальный тор группы G_σ, H — максимальный тор группы $O^{p'}(G_\sigma)$, d_1 — порядок центра группы $O^{p'}(G_\sigma)$, d — порядок центра группы $(G_{sc})_\sigma$. Поэтому для того, чтобы получить порядок централизатора в группе $O^{p'}(G_\sigma)$, порядок централизатора, указанный в лемме, необходимо умножить на дробь $\frac{d_1}{d}$. Действительно, централизатор любого полупростого элемента содержит некоторый максимальный тор группы Шевалле, и поэтому $(C_G(s)^0)_\sigma = \hat{H}C_{O^{p'}(G_\sigma)}(s)$. Значит, $|(C_G(s)^0)_\sigma : C_{O^{p'}(G_\sigma)}(s)| = \frac{d_1}{d}$, следовательно, $|C_{O^{p'}(G_\sigma)}(s)| = \frac{d_1}{d}|(C_G(s)^0)_\sigma|$. Таким образом, порядок централизатора необходимо умножить на $\frac{d_1}{d}$, но в нашем случае $d_1 = 1$, а $d = (n+1, q-1)$.

В силу леммы 2.3, существует подгруппа N_0 группы N, лежащая в некоторой σ-инвариантной связной редуктивной подгруппе R группы G максимального ранга. Кроме того, $|N : N_0| \leqslant 2^{n+1}$ (см. таблицу 2). Поскольку мы предполагаем, что центр группы $A_n(q)$ тривиален, группа R является собственной подгруппой группы G. Таким образом, группа N_0 представима в виде центрального произведения нильпотентных подгрупп из групп меньшей размерности и группы, которая является подгруппой неподвижных точек некоторого тора. Поэтому порядок группы N оценивается следующим образом

$$(q-1)|N| \leqslant n(S_{n+1})\frac{1}{(n+1,q-1)}\prod_{i,j}(q^{\mu_j^{(i)}} - 1)\prod_{i,j}(i, q^{\mu_j^{(i)}} - 1)n(A_{i-1}(q^{\mu_j^{(i)}})). \tag{1}$$

Здесь в качестве $A_{i-1}(q^{\mu_j^{(i)}})$ рассматривается группа с тривиальным центром.

Используя индукцию по лиеву рангу группы можно показать, что справедливы неравенства

$$(q^k - 1)(i, q^k - 1)n(A_{i-1}(q^k)) \leqslant (q-1)(ik, q-1)n(A_{ik-1}(q)), \tag{2}$$

$$(q-1)(i, q-1)n(A_{i-1}(q))(q-1)(k, q-1)n(A_{k-1}(q)) \leqslant (q-1)(ik, q-1)n(A_{ik-1}(q). \tag{3}$$

С помощью неравенств (2) и (3) правую часть выражения (1) можно привести к виду

$$(q-1)^2 n(S_{n+1})(n_1, q-1)n(A_{n_1-1}(q))(n_2, q-1)n(A_{n_2-1}(q)), \tag{4}$$

где $n_1 + n_2 = n + 1$, либо

$$(q^2-1)n(S_{n+1})((n+1)/2, q^2-1)n(A_{(n+1)/2-1}(q^2)). \tag{5}$$

Нетрудно проверить, что выражения (4) и (5) не превосходят значений, указанных в таблице 3. Остальные конечные группы лиева типа изучаются таким же образом.

В приведенной ниже таблице 3 указано строение больших унипотентных подгрупп в том случае, когда конечная группа G данного типа имеет тривиальный центр. Для групп с произвольным центром большая нильпотентная подгруппа — это прообраз большой нильпотентной подгруппы в группе с тривиальным центром относительно естественного гомоморфизма.

Таблица 3.

Группа G	Строение групп из $N(G)$	$n(G)$
$A_1(2^n)$	циклическая группа	2^n+1
$A_1(q)$, $q-1=2^n$	лежит в $Syl_2(A_1(q))$	2^n
${}^2A_2(2^2)$	лежит в $Syl_3({}^2A_2(2^2))$	27
${}^2A_2(3^2)$	лежит в$Syl_2({}^2A_2(3^2))$	32
для всех остальных групп G	большая унипотентная группа	

2.4 Большие нильпотентные подгруппы спорадических групп

При изучении больших нильпотентных подгрупп будет использоваться [17]. Во всех спорадических группах большая нильпотентная подгруппа — это некоторая силовская подгруппа, поэтому рассуждения, с помощью которых находятся большие нильпотентные группы однотипны. Мы опишем лишь идею.

Если N — нильпотентная подгруппа группы G, $p_1, \ldots, p_k$ — все простые числа, делящие порядок группы N, то в N существует центральный элемент порядка $p_1 \cdot \ldots \cdot p_k$. Изучение порядков централизаторов таких элементов с помощью [17] показывает, что порядок N в этом случае меньше, чем порядок некоторой силовской подгруппы.

В качестве следствия легко получается следующая теорема.

Теорема 1. *Пусть G — неабелева конечная простая группа, N — ее нильпотентная подгруппа. Тогда справедливо неравенство $|N|^2 < |G|$.*

Доказательство. В том случае, когда $N(G)$ совпадает с $Syl_p(G)$ для некоторого простого числа p, утверждение теоремы следует из [8, теорема 2]. В том случае, когда $G = A_n$, $n = 2(2k+1)+1$ для некоторого натурального k легко заметить, что $|N(G)|^2 < 2^{2(n-1)} < |G|$.

Если, наконец, группа G совпадает с $A_1(2^n)$, то группа $N(G)$ абелева и (см. [18]) справедливо неравенство $|N(G)|^2 < |G|$. $\square$

Список литературы

[1] R. W. Carter *Centralizers of semisimple elements in finite groups of Lie type* Proc. London Math. Soc. (3), 37(1978), 3, 491–507.

[2] R. W. Carter *Centralizers of semisimple elements in the finite classical groups* Proc. London Math. Soc. (3), 42(1981), 1, 1–41.

[3] D. Deriziotis *The Brauer complex and its application to the Chevalley groups*, Ph. D. thesis, University of Warwick, 1977.

[4] R. W. Carter, P. Fong *The Sylow 2-subgroups of the finite classical groups*, J. Algebra, 1(1964), 2, 139–151.

[5] A. J. Weir *Sylow p-subgroups of the classical groups over finite fields with characteristic prime to p*, Proc. Amer. Math. Soc., 6(1955), 4, 529–533.

[6] W. J. Wong *Twisted wreath product and Sylow 2-subgroups of classical simple groups*, Math. Z., 97(1967), 5, 406–424.

[7] В. В. Кабанов, А. С. Кондратьев *Силовские 2-подгруппы конечных групп (обзор)*, Свердловск: Ин-т мат. и мех. УНЦ АН СССР, 1979.

[8] В. И. Зенков, В. Д. Мазуров *О пересечении силовских подгрупп в конечных группах*, Алгебра и логика, 35(1996), 4, 424–432.

[9] A. Mann *Soluble subgroups of symmetric and linear groups*, Israel J. Math. 55(1986), 2, 162–172.

[10] Y. Segev Ph. D. thesis, The Hebrew University of Jerusalem, 1985.

[11] D. J. S. Robinson *A Course in the Theory of Groups*, Springer-Verlag New York, 1996.

[12] R. W. Carter *Simple Groups of Lie Type*, Wiley, London, 1972.

[13] Дж. Хамфри *Линейные алгебраические группы* Москва, «Наука», 1980.

[14] J. E. Humphreys *Conjugacy Classes in Semisimple ALgebraic Groups*, American Mathematical Society, Providence, Rhode Island, Mathematical Survey and Monographs, v. 43.

[15] D. Gorenstein, R. Lyons *The local structure of finite groups of characteristic 2 type*, Memoirs Amer. Math. Soc. 276(1983).

[16] Р. Ф. Апатенок, Д. А. Супруненко *О нильпотентных неприводимых линейных группах над конечным полем*, ДАН БССР, 3(1959), 12, 475–478.

[17] J. H. Conway *Atlas of finite groups*, Oxford, Clarendon Press, 1985.

[18] *A. Chermak, A. Delgado A Measuring Argument for Finite Groups*, Proc. Amer. Math. Soc., 107(1989), 4, 907–914.

Адрес автора
Вдовин Евгений Петрович,
630090 Новосибирск,
пр. Коптюга 4
e-mail vdovin@math.nsc.ru