Сибирский математический журнал
Май—июнь, 2005. Том 46, № 3

УДК 512.542

О СВЯЗИ МЕЖДУ СТРОЕНИЕМ КОНЕЧНОЙ ГРУППЫ И СВОЙСТВАМИ ЕЕ ГРАФА ПРОСТЫХ ЧИСЕЛ

А. В. Васильев

Аннотация: Показано, что условие несмежности числа 2 с хотя бы одним нечетным простым числом в графе Грюнберга — Кегеля конечной группы G является при некоторых естественных дополнительных условиях достаточным для структурного описания группы G, в частности, для доказательства того, что G имеет единственный неабелев композиционный фактор. Рассматриваются также приложения этого результата к вопросу распознаваемости конечных групп по спектру.

Ключевые слова: конечная группа, конечная простая группа, граф простых чисел конечной группы, спектр группы, распознавание по спектру.

Введение

Пусть G — конечная группа, $\pi(G)$ — множество простых делителей ее порядка, $\omega(G)$ — ее спектр, т. е. множество порядков элементов группы G. Граф Грюнберга — Кегеля (или граф простых чисел) $GK(G)$ определяется следующим образом. Множеством вершин этого графа является $\pi(G)$. Простые числа p и q, рассматриваемые как вершины графа $GK(G)$, смежны (т. е. соединены ребром) тогда и только тогда, когда в G найдется элемент порядка pq. Обозначим через $s(G)$ число связных компонент этого графа и через $\pi_i(G)$, $i = 1, \dots, s(G)$, его i-ю компоненту. Если группа G имеет четный порядок, то положим $2 \in \pi_1(G)$. Обозначим через $\omega_i(G)$ множество, состоящее из $n \in \omega(G)$ таких, что каждый простой делитель числа n принадлежит $\pi_i(G)$. Очевидно, что $GK(G)$ однозначно определяется по $\omega(G)$.

Грюнберг и Кегель дали следующее описание конечных групп с несвязным графом простых чисел.

Теорема (Грюнберг — Кегель). *Если конечная группа G имеет несвязный граф $GK(G)$, то выполняется одно из следующих утверждений:*

(а) *$s(G) = 2$ и G — группа Фробениуса;*

(б) *$s(G) = 2$ и G — двойная группа Фробениуса, т. е. $G = ABC$, где A и AB — нормальные подгруппы группы G; AB и BC — группы Фробениуса с ядрами A, B и дополнениями B, C соответственно;*

Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (код проекта 05–01–00797), Совета по грантам президента РФ и государственной поддержке ведущих научных школ (код проекта НШ–2069.2003.1), программы Рособразования «Развитие научного потенциала высшей школы» (код проекта 8294), программы «Университеты России» (код проекта УР.04.01.202), а также Президиума СО РАН (№ 86–197).

(в) *существует неабелева простая группа S такая, что $S \le \overline{G} = G/K \le \mathrm{Aut}(S)$, где K — максимальная нормальная разрешимая подгруппа группы G. Кроме того, K и $\overline{G}/S$ являются $\pi_1(G)$-группами, граф $GK(S)$ несвязен, $s(S) \ge s(G)$, и для любого числа i, $2 \le i \le s(G)$, существует j, $2 \le j \le s(S)$, такое, что $\omega_i(G) = \omega_j(S)$.*

Этот глубокий результат, впервые опубликованный в [1] (мы привели уточненный вариант формулировки этой теоремы из [2]), вместе с полной классификацией конечных простых групп с несвязным графом простых чисел, полученной Уильямсом и А. С. Кондратьевым (см. [1, 3]), имел целый ряд важных следствий (см., например, [1, теоремы 3–6; 3, теоремы 2, 3]. В последние годы эта теорема постоянно используется при доказательстве распознаваемости конечных групп по спектру (подробнее об этом речь пойдет в § 2 настоящей статьи).

Доказательство теоремы Грюнберга — Кегеля существенно использует тот факт, что в группе G найдется элемент простого нечетного порядка, не связанный в $GK(G)$ с простым числом 2. Оказывается, что требование несвязности графа простых чисел в большинстве случаев может быть успешно заменено более слабым требованием несмежности числа 2 с хотя бы одним нечетным простым числом.

Обозначим через $t(G)$ наибольшее число простых делителей порядка группы G, попарно несмежных в $GK(G)$. Другими словами, если $\rho(G)$ — независимое множество с наибольшим числом вершин в $GK(G)$ (множество вершин графа называется *независимым*, если его вершины попарно несмежны), то $t(G) = |\rho(G)|$. В теории графов это число принято называть *числом вершинной независимости* или *неплотностью*. По аналогии мы обозначим через $t(2, G)$ наибольшее число вершин в независимых множествах вершин графа $GK(G)$, содержащих простое число 2. Мы назовем это число 2-*неплотностью*. Основная цель данной статьи — доказать следующее утверждение, которое можно применять для широкого класса конечных групп, в том числе и со связным графом Грюнберга — Кегеля.

Теорема. *Пусть G — конечная группа, удовлетворяющая двум условиям:*

(а) *существует три простых числа из $\pi(G)$, попарно несмежных в $GK(G)$, т. е. $t(G) \ge 3$;*

(б) *существует нечетное простое число из $\pi(G)$, несмежное в $GK(G)$ с числом 2, т. е. $t(2, G) \ge 2$.*

Тогда существует конечная неабелева простая группа S такая, что $S \le \overline{G} = G/K \le \mathrm{Aut}(S)$ для максимальной нормальной разрешимой подгруппы K группы G. Кроме того, $t(S) \ge t(G) - 1$, и выполняется одно из следующих утверждений.

(1) *$S \simeq A_7$ или $L_2(q)$ для некоторого нечетного числа q и $t(S) = t(2, S) = 3$.*

(2) *Для каждого простого числа $p \in \pi(G)$, несмежного с 2 в $GK(G)$, силовская p-подгруппа группы G изоморфна силовской p-подгруппе группы S. В частности, $t(2, S) \ge t(2, G)$.*

Отметим, что условие (а) влечет неразрешимость группы G (см. ниже предложение 1), а следовательно, в силу теоремы Фейта — Томпсона в условии теоремы нет необходимости предполагать, что порядок G четен. Более того, оказывается, что условие (а) можно без ущерба для итогового заключения заменить более слабым условием неразрешимости группы G (см. ниже предложения 2, 3).

Работа разбита на два параграфа. В первом из них изложено доказательство основной теоремы. Во втором — речь идет о приложениях полученного результата к исследованиям вопроса распознаваемости конечных групп по спектру.

§ 1. Доказательство теоремы

Мы начнем с доказательства несложной леммы, которая будет неоднократно использоваться на протяжении этого параграфа.

Лемма 1.1. *Пусть конечная группа G обладает нормальным рядом подгрупп $1 \leq K \leq M \leq G$, а простые числа p, q и r таковы, что p делит $|K|$, q делит $|M/K|$ и r делит $|G/M|$. Тогда числа p, q и r не могут быть попарно несмежны в $GK(G)$.*

Доказательство. Пусть G — минимальный по порядку контрпример к утверждению леммы.

Рассмотрим силовскую p-подгруппу P группы K и ее нормализатор $N = N_G(P)$ в G. В силу аргумента Фраттини $G = KN$ и $N/(N \cap K) \simeq G/K$. Поэтому группа N обладает нормальным рядом подгрупп $1 \leq P \leq N \cap M \leq N$, факторы которого удовлетворяют условиям леммы. Поскольку числа p, q, r попарно несмежны в $GK(G)$, то они попарно несмежны и в $GK(N)$. Так как G — минимальный контрпример, мы можем полагать, что $N = G$ и $P \lhd G$.

Рассмотрим теперь фактор-группу $\overline{G} = G/P$. Пусть $\overline{M} = M/P$, $\overline{Q}$ — силовская q-подгруппа в $\overline{M}$ и $\overline{N} = N_{\overline{G}}(\overline{Q})$ — ее нормализатор в $\overline{G}$. Снова применяя аргумент Фраттини, получаем $\overline{N}/(\overline{N} \cap \overline{M}) \simeq \overline{G}/\overline{M}$, и, следовательно, $|\overline{N}/\overline{Q}|$ делится на r. Обозначим через Q и N полные прообразы подгрупп $\overline{Q}$ и $\overline{N}$ в G. Тогда группа N обладает нормальным рядом подгрупп $1 \leq P \leq Q \leq N$, факторы которого снова удовлетворяют условиям леммы. Значит, $N = G$ и $Q \lhd G$.

Пусть x — элемент порядка r из G. Так как в G нет элементов порядка pr и qr, то x индуцирует регулярный автоморфизм порядка r группы Q. По теореме Томпсона (см. [4]) группа Q нильпотентна. Следовательно, в ней имеется элемент порядка pq; противоречие. Лемма доказана.

Теорема является прямым следствием трех нижеследующих предложений.

Предложение 1. *Пусть G — конечная группа, $t(G) \geq 3$ и K — максимальная нормальная разрешимая подгруппа группы G. Тогда для каждого подмножества ρ простых чисел из $\pi(G)$ такого, что $|\rho| \geq 3$ и все числа из ρ попарно несмежны в $GK(G)$, пересечение $\pi(K) \cap \rho$ содержит не более одного числа. В частности, G неразрешима.*

Доказательство. Пусть p, q, r — три попарно несмежных простых числа из ρ. Предположим, что p и q делят порядок K. Рассмотрим подгруппу R группы G, порожденную подгруппами K и S_r, где S_r — силовская r-подгруппа группы G. Заметим, что не имеет значения, содержится ли S_r в K. В любом случае R — разрешимая группа. Тогда в ней, очевидно, найдется нормальный ряд, факторы которого удовлетворяют условиям леммы 1.1; противоречие. Таким образом, лишь одно простое число из ρ может делить порядок K. В частности, K — собственная подгруппа группы G. Следовательно, G неразрешима. Предложение доказано.

Отметим, что неразрешимость G в условиях предложения 1 несложно получить, используя теорему Грюнберга — Кегеля.

Предложение 2. *Пусть G — конечная неразрешимая группа и $t(2,G) \geq 2$. Тогда существует конечная неабелева простая группа S такая, что $S \leq \overline{G} = G/K \leq \mathrm{Aut}(S)$ для максимальной нормальной разрешимой подгруппы K группы G. Кроме того, выполняется одно из следующих утверждений.*

(1) $S \simeq A_7$ или $L_2(q)$ для некоторого нечетного числа q и $t(S) = t(2,S) = 3$.

(2) Для каждого простого числа $p \in \pi(G)$, несмежного с 2 в $GK(G)$, силовская p-подгруппа группы G изоморфна силовской p-подгруппе группы S. В частности, $t(2,S) \geq t(2,G)$.

Доказательство. Поскольку G неразрешима, ее максимальная нормальная разрешимая подгруппа K не совпадает с G. Пусть p — нечетное простое число, несмежное с числом 2 в $GK(G)$.

Предположим, что p делит порядок подгруппы K. Рассмотрим фактор-группу $\widehat{G} = G/O_{p'}(K)$ и ее подгруппу $\widehat{K} = K/O_{p'}(K)$. Поскольку $O_{p'}(K) \neq K$, подгруппа $O_p(\widehat{K})$ нетривиальна. Кроме того, неразрешимость группы G влечет нетривиальность силовской 2-подгруппы S_2 группы $\widehat{G}$. Так как p несмежно с 2, действие группы S_2 сопряжениями на группе $O_p(\widehat{K})$ является точным и свободным, т. е. каждый нетривиальный элемент S_2 оставляет на месте только единичный элемент группы $O_p(\widehat{K})$. Поэтому подгруппа $\langle O_p(\widehat{K}), S_2\rangle$ группы $\widehat{G}$ является группой Фробениуса с ядром $O_p(\widehat{K})$ и дополнением S_2. Тогда S_2 либо циклическая группа, либо обобщенная группа кватернионов (см., например, [5, теорема 10.3.1(iv)]). Однако группа $\widehat{G}$ неразрешима. Следовательно, S_2 — обобщенная группа кватернионов. Из теоремы Брауэра — Сузуки (см. [6]) следует, что силовская 2-подгруппа группы $\overline{G} = G/K \simeq \widehat{G}/\widehat{K}$ является диэдральной. Все конечные группы с диэдральными силовскими 2-подгруппами были описаны Горенстейном и Уолтером (см. [7, 8]). Из их описания вытекает, что группа $\overline{G}$ содержит единственный неабелев композиционный фактор S, изоморфный A_7 или $L_2(q)$, q нечетно. Несложно проверить, что $t(S) = t(2,S) = 3$. Таким образом, если p делит порядок K, то выполняется утверждение (1) предложения.

Пусть p делит порядок $\overline{G}$, но не делит порядок K. Если мы обозначим через $L = S_1 \times \dots \times S_m$ цоколь группы $\overline{G}$, где S_i — неабелевы простые группы, то $\overline{G} \leq \mathrm{Aut}(L)$.

Предположим, что $m \geq 2$. Если p делит $|L|$, то найдется k такое, что $p \in \omega(S_k)$. С другой стороны, порядок каждой группы S_i, $i = 1, \dots, m$, четен. Поскольку $m \geq 2$, L содержит элемент порядка $2p$; противоречие. Таким образом, мы можем полагать, что p делит порядок $\overline{G}/L$, но не делит порядок L. Пусть $\varphi \in \overline{G}$ — автоморфизм группы L порядка p и $P = S_1^{\varphi}$. Поскольку P проста, любая ее естественная проекция P_i на S_i, $i = 1, \dots, m$, либо тривиальна, либо изоморфна S_1. С другой стороны, так как P нормальна в L, то нормальна и каждая подгруппа P_i, $i = 1, \dots, m$. Значит, $P_i = 1$ или $P_i = S_i$. Следовательно, существует единственное число $j \in \{1, \dots, m\}$ такое, что $S_1^{\varphi} = S_j$. Если $j \neq 1$, то возникает φ-орбита Δ длины p, состоящая из подгрупп, изоморфных S_1. Без потери общности мы можем полагать, что $\Delta = \{S_1, S_2, \dots, S_p\}$. Пусть a_1 — инволюция из S_1 и $a_i = a_1^{\varphi^i}$. Пусть g — элемент из L, чьи проекции g_i на S_i определяются следующим образом: $g_i = a_i$ при $i = 1, \dots, p$ и $g_i = 1$ в остальных случаях. Тогда g — инволюция и элемент $g\varphi \in \overline{G}$ имеет порядок $2p$; противоречие. Таким образом, $S_1^{\varphi} = S_1$, и то же самое верно для каждой S_i, $i = 1, \dots, m$. Поскольку $\varphi \neq 1$, φ действует нетривиально на некоторой S_k. Тогда φ индуцирует внешний автоморфизм группы S_k порядка p.

Следующая лемма, в доказательстве которой мы используем классификацию конечных простых групп, завершает доказательство предложения.

Лемма 1.2. *Пусть G — конечная почти простая группа, т. е. существует неабелева простая группа S такая, что $S \leq G \leq \mathrm{Aut}(S)$. Пусть p — нечетное простое число, несмежное с 2 в $GK(G)$. Тогда p не делит порядок фактор-группы G/S.*

Доказательство леммы. В силу классификационной теоремы S либо спорадическая группа, либо знакопеременная группа, либо группа лиева типа. Если S — спорадическая или знакопеременная группа, то порядок группы $\mathrm{Out}(S)$ не делится на нечетное число. Следовательно, мы можем полагать, что S — группа лиева типа. Из тех же соображений следует, что S не изоморфна группе Титса ${}^2F_4(2)'$.

Обозначим через A группу $\mathrm{Aut}(S)$. Группа A обладает нормальным рядом подгрупп $S \leq \widehat{S} \leq \widehat{A} \leq A$, в котором фактор $\widehat{S}/S$ изоморфен группе диагональных автоморфизмов, фактор $\widehat{A}/\widehat{S}$ изоморфен группе полевых автоморфизмов и фактор $A/\widehat{A}$ изоморфен группе графовых автоморфизмов группы S (см. [9, предложения 3.3–3.6]).

Пусть G — минимальный по порядку контрпример к утверждению леммы. Тогда $|G/S| = p$ и $G = \langle S, \varphi\rangle$. Здесь φ — элемент группы A, не лежащий в S, и порядок его образа $\overline{\varphi}$ в фактор-группе G/S равен p. В силу [9, предложение 3.2] любой автоморфизм конечной простой группы лиева типа раскладывается в произведение внутреннего, диагонального, полевого и графового автоморфизмов. Поэтому без потери общности мы можем полагать, что $\varphi = \delta\theta\gamma$, где δ — диагональный автоморфизм, θ — полевой автоморфизм и γ — графовый автоморфизм группы S.

Предположим, что $G \not\leq \widehat{A}$. Тогда $p = 3$ и S имеет тип D_4. Но группа типа D_4 над любым конечным полем содержит элемент порядка 6; противоречие. Таким образом, $G \leq \widehat{A}$ и $\varphi = \delta\theta$.

Рассмотрим вначале случай, когда $S = A_{n-1}(q) \simeq L_n(q)$ или ${}^2A_{n-1}(q) \simeq U_n(q)$, $q = r^k$ для некоторого простого числа r, $n \geq 3$. Действие δ сопряжениями на S может быть представлено следующим образом. Пусть A — матрица из $SL_n(q)$ ($SU_n(q)$) и a — естественный образ A в $L_n(q)$ ($U_n(q)$). Тогда a^δ — образ матрицы A^D, где

$$D = \begin{pmatrix} E & 0 \\ 0 & \lambda \end{pmatrix},$$

E — единичная матрица размера $(n-1) \times (n-1)$ и λ — элемент порядка $|\delta|$ мультипликативной группы поля.

Пусть

$$T = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & I \end{pmatrix},$$

где I — матрица размера $(n-2) \times (n-2)$, причем I — единичная матрица, когда q четно, и $I = \mathrm{diag}\{1, \dots, 1, -1\}$, когда q нечетно. Матрица T лежит в $SL_n(q)$ ($SU_n(q)$), и ее образ t в $L_n(q)$ ($U_n(q)$) является инволюцией. Очевидно, что матрица D централизует T и, следовательно, δ централизует t. С другой стороны, T лежит в $SL_n(r)$ ($SU_n(r)$), а значит, t лежит в централизаторе любого полевого автоморфизма группы S. Таким образом, $t^\varphi = t^{\delta\theta} = t$, и порядок элемента $t\varphi$ группы G делится на $2p$; противоречие.

Вернемся теперь к общей ситуации. Предположим, что $\delta = 1$. Тогда $\varphi = \theta$ и $|\theta| = p$. Поскольку группа ${}^3D_4(q)$ содержит элемент порядка 6, мы можем полагать, что $p \neq 3$ в случае $S = {}^3D_4(q)$. Пусть группа S над полем порядка q допускает полевой автоморфизм порядка p. Тогда S содержит подгруппу S_0, изоморфную группе того же лиева типа, что и S, над полем порядка q_0, где $q = q_0^p$. Автоморфизм θ централизует S_0 (или подгруппу, сопряженную с ней в S). Следовательно, в G найдется элемент порядка $2p$, что невозможно. Поэтому мы можем полагать, что $\delta \neq 1$.

Если p делит $|\widehat{S}/S|$, то S имеет тип E_6 или ${}^2E_6$ и $p = 3$ (S не может быть линейной или унитарной группой, как показано выше). Поскольку группы типов E_6 и ${}^2E_6$ над любым конечным полем содержат элемент порядка 6, мы приходим к противоречию. Таким образом, можно полагать, что p не делит порядок группы $\widehat{S}/G$ и $|\widehat{A}/\widehat{S}|$ делится на p. Следовательно, φ есть произведение нетривиального диагонального автоморфизма δ и полевого автоморфизма θ порядка p. Группа $\widehat{S}/S$ диагональных автоморфизмов является циклической для любой группы S лиева типа, исключая случай, когда S — группа типа D_n, n четно, q нечетно и $\widehat{S}/S$ — элементарная абелева группа порядка 4 (см. [9, предложение 3.6]). Поскольку при $S = D_n(q)$, $n \geq 4$, группа S содержит элемент порядка 6, мы и в этом случае можем полагать, что $p \neq 3$. В силу того, что подгруппа $\widehat{S}/S$ нормальна в $\widehat{A}/S$, выполняется равенство $\overline{\delta}^{\theta} = \overline{\delta}^{k}$, где $\overline{\delta}$ — образ δ в A/S и k — некоторое натуральное число. Значит, из равенства $|\overline{\varphi}| = |\theta| = p$ и того факта, что порядок δ взаимно прост с p, следует, что p делит $\phi(|\delta|)$, где ϕ — функция Эйлера, сопоставляющая каждому натуральному числу n число обратимых элементов в $\mathbb{Z}_n$. Так как $p \geq 3$, выполняется $|\delta| \geq 5$. Это возможно только в том случае, когда S — группа типа A_n или ${}^2A_n$ и $n \geq 4$; противоречие. Лемма и предложение 2 доказаны.

Предложение 3. *Пусть G — группа, удовлетворяющая условиям предложения 2, и группы K, S, $\overline{G}$ такие, как в заключении предложения 2. Тогда $t(S) \geq t(G) - 1$. Более того, для каждого подмножества ρ простых чисел из $\pi(G)$ такого, что $|\rho| \geq 3$ и все числа из ρ попарно несмежны в $GK(G)$, не более чем одно число из ρ делит произведение $|K| \cdot |\overline{G}/S|$.*

Доказательство. Поскольку группа G удовлетворяет условиям предложения 2, существует конечная неабелева простая группа S такая, что $S \leq \overline{G} = G/K \leq \mathrm{Aut}(S)$, где K — максимальная нормальная разрешимая подгруппа группы G. Заметим, что при $t(G) = 2$ неравенство $t(S) \geq t(G) - 1 = 1$, очевидно, выполняется. Поэтому мы можем полагать, что $t(G) \geq 3$.

Пусть ρ — множество простых делителей порядка группы G, попарно несмежных в $GK(G)$, и $|\rho| \geq 3$. Если мы докажем, что не более чем одно из этих чисел делит $|K| \cdot |\overline{G}/S|$, то получим, что по крайней мере $|\rho| - 1$ чисел из ρ делит порядок S. В частности, это будет означать, что $t(S) \geq t(G) - 1$.

Обозначим через L полный прообраз S в G, а через $\widehat{G}$ фактор-группу $G/L \simeq \overline{G}/S$. Поскольку $\widehat{G} \leq \mathrm{Out}(S)$, группа $\widehat{G}$ разрешима. Следовательно, не более чем два простых числа из ρ могут делить $|\widehat{G}|$. Сначала предположим, что их ровно два. В силу разрешимости группы $\widehat{G}$ в ней найдется нормальная подгруппа $\widehat{M}$ такая, что одно из двух простых чисел, для определенности q, делит $|\widehat{M}|$, а второе r делит $|\widehat{G}/\widehat{M}|$. Так как $|\rho| \geq 3$, в ρ найдется простое число p, делящее порядок группы L и отличное от q и r. Пусть M — полный прообраз группы $\widehat{M}$ в G. Тогда нормальный ряд $1 \leq L \leq M \leq G$ удовлетворяет условиям леммы 1.1; противоречие.

Таким образом, множество простых делителей числа $|\widehat{G}|$ содержит не более одного простого числа из ρ. С другой стороны, предложение 1 показывает, что то же верно и для $\pi(K)$. Следовательно, чтобы завершить доказательство, нам осталось рассмотреть следующую ситуацию: $p, q, r \in \rho$; p делит $|K|$, q делит $|S|$, r делит $|\widehat{G}|$. В этом случае применение леммы 1.1 к нормальному ряду $1 \leq K \leq L \leq G$ снова приводит нас к противоречию. Предложение и теорема доказаны.

§ 2. Приложения

Напомним, что *спектром* $\omega(G)$ конечной группы G называется множество порядков ее элементов, т. е. натуральное число n принадлежит $\omega(G)$ тогда и только тогда, когда в G существует элемент порядка n. Для произвольного подмножества ω множества натуральных чисел обозначим через $h(\omega)$ число попарно неизоморфных конечных групп G таких, что $\omega(G) = \omega$. Мы будем говорить, что для конечной группы G *проблема распознаваемости решена*, если известно значение $h(\omega(G))$ (для краткости $h(G)$). Более точно, группа G называется *распознаваемой по спектру* (кратко, *распознаваемой*), если $h(G) = 1$, *почти распознаваемой*, если $1 < h(G) < \infty$, и *нераспознаваемой*, если $h(G) = \infty$.

Поскольку любая конечная простая группа, содержащая нетривиальную нормальную разрешимую подгруппу, нераспознаваема (см. [10, лемма 1]), каждая распознаваемая или почти распознаваемая группа является расширением прямого произведения M неабелевых простых групп с помощью некоторой подгруппы из $\mathrm{Out}(M)$. Поэтому особый интерес представляет вопрос о распознаваемости простых и почти простых групп. Первые примеры распознаваемых конечных простых групп были указаны Ши в середине 80-х гг. прошлого века (см. [11, 12]). В 1994 г. Ши и Брандл доказали распознаваемость бесконечной серии простых линейных групп $L_2(q)$, $q \neq 9$ (см. [13, 14]). К настоящему времени проблема распознаваемости решена для многих конечных неабелевых простых и почти простых групп, в частности, для всех спорадических групп, для всех простых линейных групп размерности 3, для нескольких серий исключительных групп лиева типа, а также для всех конечных простых групп, простые делители порядков которых не превосходят 13. Последняя по времени попытка дать полный обзор результатов в этой области предпринята в [15]. Однако к настоящему времени список групп, для которых проблема распознаваемости решена, существенно шире, чем приведенный в [15, табл. 1]. Новые результаты см. в [16–20]. Тем не менее полное решение проблемы распознаваемости даже в классе конечных простых групп представляется пока достаточно отдаленным.

Чтобы пояснить, как использовать основную теорему настоящей работы в исследованиях в этой области, остановимся вкратце на схеме доказательства распознаваемости.

Пусть L — конечная неабелева простая группа, а G — произвольная конечная группа, удовлетворяющая условию $\omega(G) = \omega(L)$. Доказательство распознаваемости группы L, как правило, включает в себя три основных этапа.

1. Доказывается, что фактор-группа G/K, где K — максимальная разрешимая нормальная подгруппа группы G, является почти простой. Другими словами, доказывается, что существует неабелева простая группа S такая, что $S \leq \overline{G} = G/K \leq \mathrm{Aut}(S)$.

2. Доказывается, что S изоморфна L.

3. Доказывается, что $\overline{G}/S = 1$ и $K = 1$.

Естественно, в некоторых случаях на одном из этапов может произойти «сбой». Например, в случае, когда $L = L_3(5)$, не удается доказать, что $\overline{G}/S = 1$. Оказывается, что $h(L) = 2$ и группа L имеет тот же спектр, что и ее расширение с помощью графового автоморфизма порядка 2 (см. [21]). А группа $L = L_3(3)$ имеет один и тот же спектр с разрешимой группой Фробениуса (см. [22, предложение 3]) и, следовательно, является нераспознаваемой. Однако, несмотря на исключения, в большинстве работ по распознаваемости реализуется именно указанная выше схема.

Вернемся к первому этапу. Предположим, что L имеет несвязный граф простых чисел. Так как спектр группы G совпадает со спектром L, то и граф простых чисел $GK(G)$ совпадает с графом $GK(L)$, а следовательно, также является несвязным. Поэтому группа G удовлетворяет условиям теоремы Грюнберга — Кегеля. Значит, для нее выполняется одно из трех утверждений этой теоремы. Как показано в [23], случаи (а) и (б) теоремы могут реализоваться только для групп $L_3(3)$, $U_3(3)$ и $S_4(3)$. Таким образом, если L имеет несвязный граф простых чисел и не является одной из трех вышеуказанных групп, то фактор-группа группы G по разрешимому радикалу K является почти простой группой. Тем самым первый этап доказательства распознаваемости L пройден. Отметим, что теорема Грюнберга — Кегеля используется в подавляющем большинстве работ по распознаваемости. В частности, в достаточно обширном списке групп, для которых проблема распознаваемости решена, имеется всего три группы со связным графом простых чисел: группа A_{16} с $h(A_{16}) = 1$ (см. [24]), группа $U_4(5)$ с $h(U_4(5)) = 2$ (см. [20]) и группа A_{10} с $h(A_{10}) = \infty$ (см. [10]). С другой стороны, в наиболее «объемном» классе конечных простых групп — классических простых группах — группы с несвязным графом простых чисел скорее исключение (полный список конечных простых групп с несвязным графом простых чисел см., например, в [15, табл. 2a–2c]). Таким образом, для дальнейших исследований вопроса распознаваемости крайне важным является решение проблемы прохождения первого этапа в случае, когда конечная простая группа имеет связный граф Грюнберга — Кегеля. В недавно опубликованной работе [25, теорема 2] показано, что группа G, спектр которой совпадает со спектром конечной простой группы L, отличной от групп $L_3(3)$, $U_3(3)$, $S_4(3)$ и A_{10}, является неразрешимой. Однако этот результат сложно использовать непосредственно, так как структура группы G остается неопределенной. Из предложений 2 и 3 настоящей работы и указанного результата вытекает

Предложение 4. *Пусть L — конечная простая группа с $t(2, L) \geq 2$, отличная от групп $L_3(3)$, $U_3(3)$, $S_4(3)$ и A_{10}, G — конечная группа, удовлетворяющая условию $\omega(G) = \omega(L)$. Тогда для группы G имеет место заключение теоремы. В частности, группа G обладает единственным неабелевым композиционным фактором.*

Отметим, что условию предложения 4 удовлетворяет очень широкий класс конечных простых групп. В него входят все спорадические группы и все группы лиева типа. Единственный класс конечных простых групп, для которого условие $t(2, G) \geq 2$ выполняется далеко не всегда, это класс знакопеременных групп A_n. А именно, при $n \geq 5$ условие $t(2, A_n) \geq 2$ имеет место только при $n = p, p+1, p+2, p+3$, где p — простое число. Подробное описание групп с $t(2, G) \geq 2$ выходит за рамки данной статьи. Оно будет получено как следствие в статье [26], основным результатом которой является указание для каждой конечной простой группы критерия смежности двух простых делителей ее порядка. В связи с результатом предложения 4 сформулируем следующий вопрос, принадлежащий В. Д. Мазурову.

Вопрос. *Верно ли, что конечная группа, спектр которой совпадает со спектром конечной простой группы, имеет не более одного неабелева композиционного фактора?*

Замечание. Из [25, лемма 9] следует, что любая конечная простая группа со связным графом Грюнберга — Кегеля, исключая группу A_{10}, имеет три попарно несмежных простых делителя. Следовательно, положительный ответ на вопрос Мазурова для любой конечной простой группы L, удовлетворяющей условию $t(2, L) \geq 2$, можно дать, исходя лишь из свойств графа простых чисел группы L. В общей ситуации этого недостаточно, как показывает следующий

Пример. Пусть $L = A_{28}$, а $G = A_5 \times A_n$, где n — любое натуральное число из множества $\{23, \ldots, 28\}$. Тогда $GK(L) = GK(G)$, но $\omega(L) \neq \omega(G)$.

Еще одна причина популярности теоремы Грюнберга — Кегеля среди исследователей, занимающихся вопросом распознаваемости, заключается в том, что свойство несвязности графа простых чисел исходной группы L переносится на неабелев композиционный фактор S группы G, имеющей один и тот же спектр с L. Этот факт, выражаемый неравенством $s(S) \geq s(L)$, является удобным инструментом на втором этапе доказательства распознаваемости, а именно при доказательстве того, что $S \simeq L$. Действительно, если число связных компонент исследуемой группы L равно, скажем, s, то S содержится в списке конечных простых групп, число связных компонент которых не меньше s. Более того, если в группе L есть элемент порядка n и простые делители числа n принадлежат связной компоненте графа $GK(L)$, не содержащей 2, то $n \in \omega(S)$. Этой информации зачастую оказывается достаточно, чтобы элементарными методами установить изоморфизм конечных простых групп S и L, иными словами, доказать *квазираспознаваемость* группы L. Уточним: конечная неабелева простая группа L называется *квазираспознаваемой*, если конечная группа G с тем же спектром, что и L, содержит единственный неабелев композиционный фактор и этот фактор изоморфен L. Это определение восходит к работе [27].

Основная теорема настоящей работы также дает богатую дополнительную информацию о строении спектра неабелева композиционного фактора S группы G. В качестве иллюстрации того, как эта информация может быть использована, мы дадим набросок доказательства квазираспознаваемости групп ${}^2D_n(2^k)$, где n — «достаточно большое» четное число. Нам потребуется следующая

Лемма 2.1 (Жигмонди). *Пусть p — простое число, s — натуральное число, $s \geq 2$. Тогда верно одно из следующих утверждений:*

(а) *существует простое число r такое, что r делит $p^s - 1$ и r не делит $p^t - 1$ при любом натуральном $t < s$;*

(б) $s = 6$ *и* $p = 2$;

(в) $s = 2$ *и* $p = 2^t - 1$ *для некоторого натурального числа* t.

Доказательство см. в [28].

Простое число r, удовлетворяющее п. (а) леммы 2.1, называется *примитивным простым делителем числа* $p^s - 1$.

Предложение 5. *Пусть $L = {}^2D_n(q)$, $q = 2^k$, k, n — натуральные числа, причем n четно и $n \geq 16$. Тогда L квазираспознаваема.*

Набросок доказательства. Имеем

$$|L| = q^{n(n-1)}(q^2-1)(q^4-1)\dots(q^{2n-2}-1)(q^n+1).$$

Если T — максимальный тор в группе L, то порядок T равен

$$|T| = \prod_{j=1}^{t}\left(q^{t_j}-1\right)\prod_{i=1}^{s}\left(q^{s_i}+1\right),$$

где натуральные числа s_i, t_j удовлетворяют соотношению

$$\sum_{j=1}^{t} t_j + \sum_{i=1}^{s} s_i = n,$$

причем число s нечетно (см., например, [18, лемма 2.1]).

Пусть $a_1, \dots, a_l$ — полная система представителей классов сопряженных инволюций в L и $C_i = C_L(a_i)$, $i = 1, \dots, l$, — их централизаторы в L. Тогда (см., например, [3, § 3, п. 5])

$$\pi\left(\prod_{j=1}^{l}|C_i|\right) = \pi\left(2\cdot\prod_{i=1}^{n-2}(q^{2i}-1)\right).$$

Обозначим через r_s некоторый примитивный простой делитель числа $2^{ks}-1$. Заметим, что если $s = 2j$ четно, то r_s является делителем числа $2^{kj}+1$ и не делит $2^{ki}+1$ для любого $i < j$.

Поскольку каждый полупростой элемент из L содержится в некотором максимальном торе группы L, два примитивных делителя r_i и r_j смежны тогда и только тогда, когда в L найдется тор, порядок которого делится на произведение r_ir_j. Зная порядки максимальных торов и множество простых делителей порядков централизаторов инволюций, несложно оценить значения неплотности $t(L)$ и 2-неплотности $t(2, L)$ графа простых чисел группы L. Например, независимое множество с наибольшим числом вершин в $GK({}^2D_{16}(q))$ — это множество простых чисел $\rho = \{r_s \mid s = 9, 11, 13, 15, 16, 18, 20, 22, 24, 26, 28, 30, 32\}$. Поэтому $t({}^2D_{16}(q)) = 13$. Кроме того, при $n \geq 16$ выполняется $t({}^2D_n(q)) \geq t({}^2D_{16}(q))$. Следовательно, $t(L) \geq 13$. Множество вершин $\rho(2, L) = \{2, r_{n-1}, r_{2n-2}, r_{2n}\}$ является независимым в $GK(L)$, и любое другое независимое множество вершин τ графа $GK(L)$, содержащее вершину 2, удовлетворяет условию $|\tau| \leq |\rho(2, L)|$. Значит, $t(2, L) = 4$.

Пусть G — конечная группа, удовлетворяющая условию $\omega(G) = \omega(L)$. Поскольку $GK(G) = GK(L)$, для группы G имеет место заключение теоремы. Пусть S — единственный неабелев композиционный фактор группы G. Если H — простая спорадическая или исключительная группа лиева типа, то $t(H) \leq t(F_1) = 11$ (подробнее см. в [26]). Поскольку $t(S) \geq t(G) - 1 = t(L) - 1 \geq 12$, то S не может быть ни спорадической, ни исключительной группой лиева типа. Следовательно, S либо знакопеременная группа, либо классическая группа лиева типа достаточно большого ранга. В частности, S не может быть группой ${}^2D_{n'}(2^{k'})$, где n' — четное число, меньшее 16, так как неплотность таких групп не превосходит 11. Оказывается, что все указанные группы имеют

2-неплотность, меньшую 4, за исключением случая, когда S сама удовлетворяет условию предложения (см. [26]).

Таким образом, $S \simeq {}^2D_{n'}(2^{k'})$, n' четно и $n' \geq 16$. Осталось доказать, что $n = n'$ и $k = k'$. Поскольку числа r_{2n}, r_{2n-2}, r_{n-1} несмежны с 2 в $GK(G)$, то по п. 2 утверждения теоремы они лежат в $\omega(S)$ и несмежны с 2 в $GK(S)$. Следовательно, они являются примитивными простыми делителями чисел $2^{2n'k'} - 1$, $2^{(2n'-2)k'} - 1$ и $2^{(n'-1)k'} - 1$. Кроме того, так как числа r_{2n}, r_{2n-2}, r_{n-1} попарно несмежны, то никакие два из них не могут делить какую-то одну из указанных разностей. Предположим сначала, что r_{2n} делит $2^{2n'k'} - 1$, r_{2n-2} делит $2^{(2n'-2)k'} - 1$ и r_{n-1} делит $2^{(n'-1)k'} - 1$. Поскольку r_{2n} — примитивный делитель числа $2^{2n'k'} - 1$, то $2n'k'$ — наименьшее натуральное число такое, что $2^{2n'k'} \equiv 1 (\mathrm{mod}\, r_{2nk})$. Но тем же свойством обладает и число $2nk$. Следовательно, $nk = n'k'$. Аналогично $(n-1)k = (n'-1)k'$, откуда $n = n'$ и $k = k'$. Пусть теперь числа r_{2n}, r_{2n-2}, r_{n-1} делят те же разности в другом порядке. Рассмотрим, например, ситуацию, когда r_{2n} — примитивный делитель числа $2^{(2n'-2)k'} - 1$, а r_{2n-2} — примитивный делитель числа $2^{2n'k'} - 1$. Рассуждая, как в предыдущем случае, приходим к равенствам $nk = (n'-1)k'$ и $(n-1)k = n'k'$. Отсюда $k = -k'$, что невозможно. Остальные случаи разбираются аналогично и также приводят к противоречию. Следовательно, возможен только первый случай, и выполняются равенства $n = n'$, $k = k'$, что и требовалось доказать.

Замечание 1. Приведенное выше рассуждение, как уже говорилось, служит лишь иллюстрацией возможностей применения основной теоремы. Его нельзя считать полноценным доказательством предложения 5, так как в нем использовались сведения о величине неплотности и 2-неплотности в конечных простых группах из еще неопубликованной работы [26]. Таким образом, предложение 5 можно будет считать полностью доказанным после выхода указанной статьи.

Замечание 2. Квазираспознаваемость групп ${}^2D_n(2^k)$, $n = 2^m$ (случай, когда $m \geq 4$, — это частный случай предложения 5), была доказана ранее в [18] с использованием теоремы Грюнберга — Кегеля (в этом случае граф простых чисел группы несвязен). Если же n не является степенью двойки, то группа L, удовлетворяющая условиям предложения 5, имеет уже связный граф простых чисел. Тем самым мы впервые получаем бесконечную серию квазираспознаваемых групп со связным графом простых чисел.

ЛИТЕРАТУРА

1. *Williams J. S.* Prime graph components of finite groups // J. Algebra. 1981. V. 69, N 2. P. 487–513.
2. *Мазуров В. Д., Су М. Ч., Чао Х. П.* Распознавание конечных простых групп $L_3(2^m)$ и $U_3(2^m)$ по порядкам их элементов // Алгебра и логика. 2000. Т. 39, № 5. С. 567–585.
3. *Кондратьев А. С.* О компонентах графа простых чисел конечных простых групп // Мат. сб. 1989. Т. 180, № 6. С. 787–797.
4. *Thompson J. G.* Finite groups with fixed-point free automorphisms of prime order // Proc. Nat. Acad. Sci. 1959. V. 45. P. 578–581.
5. *Gorenstein D.* Finite groups. New York: Harper & Row, 1968.
6. *Brauer R., Suzuki M.* On finite groups of even order whose 2-Sylow subgroup is a quaternion group // Proc. Nat. Akad. Sci. 1959. V. 45. P. 1757–1759.
7. *Gorenstein D., Walter J. H.* On finite groups with dihedral Sylow 2-subgroups // Ill. J. Math. 1962. V. 6. P. 553–593.
8. *Gorenstein D., Walter J. H.* The characterization of finite groups with dihedral Sylow 2-subgroups. I, II, III // J. Algebra. 1965. V. 2. P. 85–151, 218–270, 334–393.

9. *Steinberg R.* Automorphisms of finite linear groups // Canad. J. Math. 1960. V. 12, N 4. P. 606–616.

10. *Мазуров В. Д.* Распознавание конечных простых групп по множеству порядков их элементов // Алгебра и логика. 1998. Т. 37, № 6. С. 651–666.

11. *Shi W.* A characteristic property of $PSL_2(7)$ // J. Austral. Math. Soc. Ser. A. 1984. V. 36, N 3. P. 354–356.

12. *Shi W.* A characteristic property of A_5 // J. Southwest-China Teach. Univ. 1986. V. 3. P. 11–14.

13. *Shi W.* A characteristic property of J_1 and $PSL_2(2^n)$ // Adv. Math. 1987. V. 16. P. 397–401.

14. *Brandl R., Shi W.* The characterization of $PSL(2,q)$ by its element orders // J. Algebra. 1994. V. 163, N 1. P. 109–114.

15. *Mazurov V. D.* Characterizations of groups by arithmetic properties // Algebra Colloq. 2004. V. 11, N 1. P. 129–140.

16. *Гречкосеева М. А.* Распознаваемость группы $O^+_{10}(2)$ по ее спектру // Сиб. мат. журн. 2003. Т. 44, № 4. С. 737–741.

17. *Zavarnitsine A. V.* Recognition of the simple groups $L_3(q)$ by element orders // J. Group Theory. 2004. V. 7, N 1. P. 81–97.

18. *Васильев А. В., Гречкосеева М. А.* О распознаваемости конечных простых ортогональных групп размерности $2^m, 2^m+1$ и 2^m+2 над полем характеристики 2 // Сиб. мат. журн. 2004. Т. 45, № 3. С. 510–526.

19. *Васильев А. В., Гречкосеева М. А., Мазуров В. Д., Чао Х. П., Чен Г. Ю., Ши В. Дж.* Распознавание конечных простых групп $F_4(2^m)$ по спектру // Сиб. мат. журн. 2004. Т. 45, № 6. С. 1256–1262.

20. *Васильев А. В.* О распознавании всех конечных неабелевых простых групп, простые делители порядков которых не превосходят 13 // Сиб. мат. журн. 2005. Т. 46, № 2. С. 315–324.

21. *Мазуров В. Д.* О множестве порядков элементов конечной группы // Алгебра и логика. 1994. Т. 33, № 1. С. 81–89.

22. *Мазуров В. Д.* Распознавание конечных простых групп $S_4(q)$ по порядкам их элементов // Алгебра и логика. 2002. Т. 41, № 2. С. 166–198.

23. *Алеева М. Р.* О конечных простых группах с множеством порядков элементов, как у группы Фробениуса или двойной группы Фробениуса // Мат. заметки. 2003. Т. 73, № 3. С. 323–339.

24. *Заварницин А. В.* Распознавание знакопеременных групп степени $r+1$ и $r+2$ для простого r и группы степени 16 по их множествам порядков элементов // Алгебра и логика. 2000. Т. 39, № 6. С. 648–662.

25. *Lucido M. S., Moghaddamfar A. R.* Groups with complete prime graph connected components // J. Group Theory. 2004. V. 7, N 3. P. 373–384.

26. *Васильев А. В., Вдовин Е. П.* Критерий смежности двух вершин в графе простых чисел конечной простой группы. Алгебра и логика (в печати). (См. также Препринт № 152 / СО РАН. Ин-т математики, 2005. 34 с.)

27. *Алексеева О. А., Кондратьев А. С.* О распознаваемости группы $E_8(q)$ по множеству порядков элементов // Укр. мат. журн. 2002. Т. 54, № 7. С. 998–1003.

28. *Zsigmondy K.* Zur Theorie der Potenzreste // Monatsh. Math. Phys. 1892. V. 3. P. 265–284.

Статья поступила 29 ноября 2004 г.

Васильев Андрей Викторович
Институт математики им. С. Л. Соболева СО РАН,
пр. Академика Коптюга, 4, Новосибирск 630090
vdr@gorodok.net