Сибирский математический журнал
Март—апрель, 2013. Том 54, № 2

УДК 512.542.52

ФУНКЦИИ ЭЙЛЕРА — ХОЛЛА НА ГРУППАХ РИ

Д. В. Левчук, Ю. Ю. Ушаков

Аннотация. Исследуется вопрос Сыскина о вычислении значений второй функции Эйлера — Холла на простых конечных группах. Решение вопроса завершается для трех из четырех серий групп лиева типа ранга 1 (кроме унитарных).

Ключевые слова: конечная простая группа, группа лиева типа, функция Эйлера — Холла.

Введение

В 60-70-е гг. была установлена порождаемость двумя элементами любой известной конечной простой группы. По модулю классификации двупорожденной будет и любая конечная простая группа. Отсюда и из работы Холла [1, § 1.6] сразу следует существование для любого натурального числа $n \geq 2$ и конечной простой неабелевой группы G наибольшего числа $d = d_n(G)$ такого, что прямая степень G^d порождается n элементами.

Вопрос о нахождении чисел $d_2(G)$ записал С. А. Сыскин в «Коуровской тетради» [2, вопрос 12.86]: *для каждой известной простой конечной группы G найти максимальное число d такое, что прямое произведение d экземпляров группы G порождается двумя элементами.*

Гипотезу о естественной оценке числа $d_2(G)$ высказали в 1995 г. Эрфаниан и Уайголд [3] и записал Уайголд [2, вопрос 17.116]: *если G — конечная простая неабелева группа, то $d_2(G) \geq \sqrt{|G|}$.*

Для некоторых классических групп гипотеза подтверждена в [4–6]. Для простых групп G лиева типа ранга 1, кроме унитарных, Ю. Ю. Ушаков [7] доказал более общее неравенство:

$$d_m(G) \geq |G|^{m-\frac{3}{2}} \quad (m \geq 2).$$

Конечно, для чисел $d_2(G)$ единообразную формулу можно ожидать лишь для отдельных классов групп. Н. М. Сучков и Д. М. Приходько [8] нашли их рекуррентное описание для групп Сузуки $Sz(q)$ и $PSL_2(q)$ с четными q. Для нечетных q числа $d_2(PSL_2(q))$ исследовал Д. М. Приходько (см. [9] и замечание 1 в § 1); для простых q они вычислены в [1].

В настоящей статье решение вопроса для групп Ри лиева типа ${}^2G_2$ дает

Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (код проекта 12–01–00968–а).

Теорема 1. *Пусть $Re(q)$ ($q = 3^n$, $n > 1$) — конечная простая группа Ри типа ${}^2G_2$. Тогда для простых чисел n имеем $d_2(Re(q)) = (1/n) \cdot \rho(q)$, где*

$$\rho(q) = (q-3)(q^6 + 2q^5 + 6q^4 + 18q^3 + 53q^2 + 160q + 464).$$

Если число n составное, то

$$d_2(Re(q)) = \frac{1}{n}\Big[\rho(q) - \sum_{t|n,\, n>t>1} t \cdot d_2(Re(3^t))\Big].$$

Таким образом, вопрос Сыскина получает решение для групп лиева типа ранга 1, за исключением унитарного случая. Наряду со значениями функции d_2 вычисляются значения обобщенной функции Эйлера из [1].

Ю. Ю. Ушаков написал § 3, остальные результаты получены обоими авторами совместно.

§ 1. Холловская и рекуррентная редукции

Холл [1] называет *m-базой группы G* упорядоченный набор из m элементов группы G, порождающих эту группу. Количество m-баз группы G Холл обозначает через $\varphi_m(G)$ и называет *m-й функцией Эйлера.* Очевидно, значение функции φ_1 на циклической группе G совпадает со значением теоретико-числовой функции Эйлера на порядке $|G|$. Холл редуцировал вычисление значения $d_m(G)$ на произвольной конечной простой неабелевой группе G к вычислению значения $\varphi_m(G)$, доказав в [1] соотношение

$$\varphi_m(G) = d_m(G) \cdot |\operatorname{Aut} G| \quad (m > 1). \tag{1}$$

Группа $G(q)$ лиева типа ранга 1, определенная над конечным полем порядка q, является простой при $q > 3$. Для нее возможны всего 4 типа: $PSL_2(q)$, $Sz(q)$, $q = 2^n$, $n = 2k+1$ (группа Сузуки), $Re(q) = {}^2G_2(q)$, $q = 3^n$ (группа Ри) и $PSU_3(q)$ (унитарная группа).

Группу $G(q)$ в стандартном линейном представлении порождают антидиагональная инволюция τ с коэффициентами из простого подполя $GF(p) \subseteq GF(q)$ и силовская p-подгруппа U — нижняя (или верхняя) унитреугольная подгруппа в $G(q)$. Выделяют также диагональную подгруппу H, подгруппу Бореля $B = U \leftthreetimes H$ — нормализатор подгруппы U и мономиальную подгруппу $N = H \leftthreetimes \langle\tau\rangle$. Кроме унитарного случая, N есть диэдральная группа, и в соответствии с выбором $G(q)$ будет (см. [10, 11]) $|U|$ равно q, q^2 или q^3; $|H| = (q-1)/d$; d равно НОД$(2, q-1)$, 1 или 1. Разложение Брюа $G(q) = B\langle\tau\rangle B$ ($= B\langle\tau\rangle U$) и известные описания автоморфизмов дают следующую лемму и формулы порядков:

$$|G(q)| = |H| \cdot |U| \cdot (1 + |U|), \quad |\operatorname{Aut} G(q)| = d \cdot n \cdot |G(q)| \quad (q = p^n).$$

Лемма 1. *Группа $G(q)$ действует сопряжениями на множестве сопряженных с U подгрупп как дважды транзитивная группа подстановок. Различные сопряженные с U подгруппы пересекаются по единице. Если два элемента из U сопряжены в $G(q)$, то они сопряжены и в B.*

Нам потребуются известные (см. [10–14]) свойства группы Ри над конечным полем $F = GF(q)$ порядка $q = 3^n$ с нечетным n. Как обычно, $C_G(S)$ и $N_G(S)$ или кратко $C(S)$ и $N(S)$ обозначают соответственно централизатор и нормализатор подмножества S в группе G. Также положим $\theta := 3^k$, где $n = 2k+1$.

(А) Унипотентная подгруппа U группы $Re(q)$ представляется элементами $\alpha(u)\beta(v)\gamma(w) = (u, v, w)$ $(u, v, w \in F)$ с умножением (см. [10, 13.6.4]):

$$(u, v, w)(x, y, z) = (u + x, +y - ux^{3\theta}, w + z - vx + ux^{3\theta+1} - u^2x^{3\theta}).$$

(Б) Силовская 2-подгруппа в $Re(q)$ есть элементарная абелева 2-группа порядка 8, и все 2-подгруппы равного порядка в $Re(q)$ сопряжены.

(В) Централизатором диагональной инволюции η в $Re(q)$ является

$$C(\eta) = \langle\eta\rangle \times L(q), \quad L(q) := \langle\tau, \beta(F)\rangle \simeq PSL_2(q),$$

и $A_0 := H \cap L(q)$ — циклическая холлова подгруппа порядка $(q-1)/2$.

(Г) Подгруппа, содержащая диагональный элемент порядка > 2, либо лежит в B, B^τ или $C(\eta)$, либо H-сопряжена с подгруппой группы Ри над подполем поля F.

(Д) В $Re(q)$ существуют циклические холловы подгруппы нечетных порядков $(q+1)/4$, $q + 1 - \sqrt{3q}$ и $q + 1 + \sqrt{3q}$, соответственно $A_1 \subset L(q)$ и самоцентрализуемые подгруппы A_2 и A_3, причем

$$|Re(q)| = 8q^3 \cdot |A_0| \cdot |A_1| \cdot |A_2| \cdot |A_3| = q^3(q^3 + 1)(q - 1).$$

(Е) Для любого $i = 0, 1, 2, 3$ нормализатор подгруппы A_i содержит нормализатор всякой ее неединичной подгруппы, числа $|A_i|$ попарно взаимно просты и существуют элемент t порядка 6 и четверная подгруппа T такие, что при $q > 3$ нормализатор $N(A_i)$ есть группа Фробениуса $A_i \leftthreetimes \langle t\rangle$ с ядром A_i, если $i = 2, 3$, а также

$$C(A_1) = T \times A_1, \quad N(A_1) = N(T) = T \leftthreetimes (A_1 \leftthreetimes \langle t\rangle).$$

(Ж) Максимальная подгруппа группы $Re(q)$ при $q > 3$ сопряжена с подгруппой B, $C(\eta)$, $N(A_i)$ $(i = 1, 2, 3)$ или с $Re(m)$, когда в F существует максимальное подполе порядка m.

Разрешимый радикал произвольной группы по определению есть ее наибольшая разрешимая нормальная подгруппа. Описание в группах Ри подгрупп с неединичным разрешимым радикалом с учетом (Ж) завершает

Лемма 2. *Собственная подгруппа группы $Re(3)$ совпадает с $Re(3)'$ или сопряжена либо с нормализатором $P_2 \leftthreetimes (A_3 \leftthreetimes \langle t^2\rangle)$ силовской 2-подгруппы P_2, либо с $P_2 \leftthreetimes A_3$, либо с подгруппой одной из подгрупп B, $C(\eta)$ и $N(A_3)$.*

Доказательство. Известно, что $Re(3) \simeq \mathrm{Aut}\, SL_2(8)$ и $Re(3)' \simeq SL_2(8)$; остальные подгруппы в $Re(3)$ разрешимы. Кроме того, в группе $Re(3)$ подгруппа A_3 порядка 7 силовская, $|N(A_3))| = 42$ и $A_0 = A_1 = A_2 = 1$.

Как показывает подгрупповое описание группы $SL_2(8)$, максимальными в $Re(3)$, помимо $Re(3)'$ и B, являются подгруппы $N(P_2)$ и $N(A_3)$. В пересечении с $Re(3)'$ они дают подгруппы $P_2 \leftthreetimes A_3$ и $A_3 \leftthreetimes \langle t^3\rangle$, которые в $SL_2(8)$ являются соответственно подгруппой Бореля (группа Фробениуса) и мономиальной подгруппой. Поэтому если подгруппа в $Re(3)$ разрешима и не сопряжена с подгруппой из B, $C(\eta)$ или $N(A_3)$, то она лежит в разрешимой подгруппе $N(P_2)$.

Группа $N(P_2)$ порядка 168 имеет холловы максимальные подгруппы порядков 21, 24 и 56. Согласно обобщенной силовской теореме [15, теорема 20.1.1] если в конечной разрешимой группе порядок какой-либо подгруппы M делит порядок холловой подгруппы M_1, то M лежит в сопряженной с M_1 подгруппе. Сопряжение элементом порядка 7 в $N(P_2)$ циклически переставляет инволюции, поэтому подгруппа порядка, кратного 14, содержит подгруппу $P_2 \leftthreetimes A_3$ порядка 56. Остается заметить, что подгруппа порядка 24 в $N(P_2)$ централизует одну из лежащих в ней инволюций. □

Множество всех упорядоченных пар элементов группы G, лежащих в подгруппах с неединичным разрешимым радикалом, обозначается через $W(G)$ или кратко W. Известна [16] следующая редукция к W.

Лемма 3. *Если $G(q)$ — простая группа Ри $Re(q)$, то*

$$\varphi_2(G(q)) = |G(q)|^2 - |W| - \sum_{G(k)<G(q)} \frac{|G(q)|}{|G(k)|}\varphi_2(G(k)) - \frac{|G(q)|}{|G(3)|}\varphi_2(G(3)'). \qquad (2)$$

Для простых групп $G(q) = Sz(q)$ и $SL_2(q)$ с четным q также выполняется (2), *если в правой части равенства опустить последнее слагаемое.*

Согласно Н. М. Сучкову и Д. М. Приходько [8, теоремы 1, 2] имеем

$$d_2(SL_2(2^n)) = \frac{1}{n}\phi(2^n), \quad \phi(q) := (q-2)(q^2+q-1),$$

$$d_2(Sz(2^n)) = \frac{1}{n}\psi(2^n), \quad \psi(q) := (q-2)(q^4+q^3+2q^2+4q-1)$$

для простого числа n, а если n — составное число, то

$$d_2(SL_2(2^n)) = \frac{1}{n}\Big[\phi(2^n) - \sum_{k|n,\, n>k>1} kd_2(SL_2(2^k))\Big],$$

$$d_2(Sz(2^n)) = \frac{1}{n}\Big[\psi(2^n) - \sum_{k|n,\, n>k>1} kd_2(Sz(2^k))\Big].$$

Замечание 1. Д. М. Приходько исследовал функцию φ_2 также на группах $PSL_2(q)$ с нечетным $q = p^n > 3$ (p — простое число), используя равенства $\varphi_2(PSL_2(3)) = 96$, $\varphi_2(PGL_2(3)) = 216$ и функции

$$\chi(q) := q(q^2-1)(q-3)(q^2+2q+3)/4,$$

$$\eta(q) := \begin{cases} 9q(q^2-1) & \text{при } q \equiv 1,7 \pmod 8, \\ 0 & \text{при } q \equiv 3,5 \pmod 8, \end{cases}$$

$$\mu(q) := \begin{cases} 9q(q^2-1) & \text{при } q \equiv 1,7 \pmod 8,\ q \not\equiv 1,9 \pmod{10}, \\ 38q(q^2-1) & \text{при } q \equiv 3,5 \pmod 8,\ q \equiv 1,9 \pmod{10}, \\ 47q(q^2-1) & \text{при } q \equiv 1,7 \pmod 8,\ q \equiv 1,9 \pmod{10}, \\ 0 & \text{при } q \equiv 3,5 \pmod 8,\ q \not\equiv 1,9 \pmod{10}. \end{cases}$$

Он устанавливает равенства

$$\varphi_2(PSL_2(q)) = \chi(q) - \mu(q) - q(q^2-1) \times \Bigg(\sum_{t|n,\, q>p^t\geq 5} \frac{\varphi_2(PSL_2(p^t))}{p^t(p^{2t}-1)} + \sum_{2t|n,\, q>p^t\geq 5} \frac{\varphi_2(PGL_2(p^t))}{p^t(p^{2t}-1)}\Bigg),$$

$$\varphi_2(PGL_2(q)) = 3\chi(q) + \eta(q) - q(q^2-1) \sum_{t|n,\, q>p^t\geq 5} \frac{\varphi_2(PGL_2(p^t))}{p^t(p^{2t}-1)}.$$

Отметим, что простые группы Ри обладают неразрешимой подгруппой с неединичным разрешимым радикалом в отличие от групп $Sz(q)$ и $PSL_2(q)$.

§ 2. Редукция к парам с первым $\{2,3\}$-элементом

Подмножество пар в W элементов из подгрупп, сопряженных с

$$B, \quad N(A_i) \ \ (i=1,2,3) \quad \text{или} \quad C(\eta), \tag{3}$$

обозначаем через W'. В этом параграфе устанавливается

Лемма 4. *Число* $|\{(x,y)\in W' : |x| \nmid 8q^3\}|$ *равно* $q(q^3-2q^2-4q+5)|Re(q)|$.

Из описаний подгрупп и $\{2,3\}$-элементов групп $Re(q)$ и $SL_2(8)$ вытекает

Лемма 5. *Либо всякий элемент* $x \neq 1$ *группы* $Re(q)$ *с точностью до сопряжения есть* $\{2,3\}$*-элемент* η, $\alpha(1)$, $\gamma(1)$, $\beta(\pm 1)$ *или* $\beta(\pm 1)\eta$, *либо* $\langle x\rangle \cap A_i \neq \{1\}$ *при единственном* $i=0,1,2,3$.

Лемма 6. *Число пар* $(x,y)\in W'$ *с* НОД$(|x|,|A_2|\cdot|A_3|)>1$ *равно* $2q|Re(q)|$.

Доказательство. Неединичные элементы из пересечения любых двух подгрупп, сопряженных с $N(A_i)$, $i=2,3$, являются $\{2,3\}$-элементами. Поэтому фиксированный элемент x, порядок которого не взаимно прост с $q^2-q+1 = |A_2|\cdot|A_3|$, лежит ровно в одной подгруппе, сопряженной с $N(A_i)$, $i=2,3$, и число требуемых пар из W с первым элементом x равно $|N(A_i)|$. Так как группа $N(A_i)$ $(i=2,3)$ есть группа Фробениуса с ядром A_i, все ее не $\{2,3\}$-элементы лежат в A_i, а число элементов группы $Re(q)$, порядок которых не взаимно прост с $|A_i|$, равно $(|A_i|-1)|Re(q):N(A_i)|$.

Отсюда число пар элементов x,y, лежащих в подгруппах, сопряженных с $N(A_i)$, для которых порядок $|x|$ не взаимно прост с $|A_i|$, равно

$$(|A_i|-1)|Re(q):N(A_i)||N(A_i)| = |Re(q)|(|A_i|-1).$$

Суммирование по $i=2,3$ этих чисел дает утверждение леммы. □

Лемма 7. *Число пар* $(x,y)\in W'$ *с условием* НОД$(|x|,|A_1|)>1$ *равно* $|Re(q)|\cdot\frac{1}{2}q(q-1)(q-3)$.

Доказательство. Пусть $x\in Re(q)$ и НОД$(|x|,|A_1|)>1$. Тогда с точностью до сопряжения пересечение $\langle x\rangle\cap A_i$ неединично и его централизатор совпадает с $C(A_1)=\langle T\rangle\times A_1$, где $T=\langle i,j\rangle$ — четверная группа. Максимальные подгруппы, содержащие x и сопряженные с (3), исчерпываются централизаторами инволюций из T и подгруппой $N(A_1)=N(T)$, причем

$$N(T)\cap C(i) = N(T)\cap C(ij) = N(T)\cap C(j) = C(T).$$

Легко найти мощность объединения этих максимальных подгрупп:

$$|N(A_1)\cup C(i)\cup C(j)\cup C(ij)| = |N(A_1)| + 3|C(i)| - 3|C(T)| = 3q(q^2-1).$$

Число элементов группы $Re(q)$, порядок которых не взаимно прост с $|A_1|$, равно $4(|A_1|-1)|Re(q):N(A_1)|$. Следовательно, число пар из W, порядок первого элемента которых не взаимно прост с $|A_1|$, равно

$$3q(q^2-1)(q-3)|Re(q):N(A_1)| = \frac{1}{2}q(q-1)(q-3)|Re(q)|. \quad \square$$

Лемма 8. *Число пар* $(x, y) \in W'$, *для которых порядок* $|x|$ *не взаимно прост с* $(q-1)/2$, *равно* $\frac{1}{2}|Re(q)|q(q-3)(2q^2+q-1)$.

Доказательство. Пусть x — первый элемент такой пары. Тогда с точностью до сопряженности можно считать, что x — диагональный элемент. Найдем число пар из W с первым элементом x. По [14, теорема 2] подгруппы, сопряженные (3) и содержащие x, исчерпываются $C(\eta)$, B, B^τ. Найдем объединение этих подгрупп. Имеем

$$|C(\eta) \cap B| = |C(\eta) \cap B^\tau| = |\beta(F) \rtimes H|, \quad B \cap B^\tau = B \cap B^\tau \cap C(\eta) = H.$$

Тогда число пар из W' с фиксированным первым элементом x равно

$$|B \cup B^\tau \cup C(\eta)| = |B| + |B^\tau| + |C(\eta)| - |B \cap B^\tau| - |B \cap C(\eta)| \\ - |B^\tau \cap C(\eta)| + |B \cap B^\tau \cap C(\eta)| = q(q-1)(2q^2+q-1).$$

Число диагональных элементов, порядок которых не взаимно прост с $|A_0|$, равно $|H| - 2 = q - 3$. Число подгрупп, сопряженных с $N(A_0)$, равно $|Re(q) : N(H)|$. Тогда число пар из W', порядок первого элемента которых не взаимно прост с $|A_0|$, равно

$$\frac{|Re(q)|}{|N(H)|}(q-3)q(q-1)(2q^2+q-1) = \frac{1}{2}|Re(q)|q(q-3)(2q^2+q-1). \quad \square$$

Утверждение леммы 4 получается суммированием числа пар в W', вычисленных в леммах 6–8.

§ 3. Перечисление пар с первым $\{2,3\}$-элементом

Согласно лемме 5 каждый $\{2,3\}$-элемент группы $Re(q)$ с точностью до сопряженности либо не централизует ни одной инволюции в $Re(q)$, либо сопряжен с $\beta(\pm 1)$, $\beta(\pm 1)\eta$ или η. Разделим множество пар из W' с первым $\{2,3\}$-элементом на непересекающиеся подмножества в зависимости от того, в какой класс сопряженности входит первый элемент пары.

Лемма 9. *Количество пар* $(x, y) \in W$ *с 3-элементом* x, *не централизующим ни одной инволюции, равно* $(q^2+1)(q-1)|Re(q)|$.

Доказательство. 3-Элемент, не централизующий ни одной инволюции, сопряжен с $\gamma(1)$ порядка 3 или $\alpha(1)$ порядка 9. Число таких элементом в B равно $(q^3-q^2)+(q-1) = (q-1)(q^2+1)$, а в $Re(q)$ их число равно $(q-1)(q^2+1)|Re(q) : B|$. Каждый такой элемент с точностью до сопряженности лежит в максимальных подгруппах $Re(k)$ и B. Поэтому количество пар $(x, y) \in W'$, в которых первый элемент является 3-элементом и не централизует ни одной инволюции, равно

$$(q^2+1)(q-1)|Re(q) : B| \cdot |B| = (q^2+1)(q-1)|Re(q)|. \quad \square$$

Все $\{2,3\}$-элементы группы Ри, за исключением перечисленных в лемме 9, сопряжены с элементами порядков 2, 3 или 6 из $N(A_1) = (T \times A_1) \rtimes \langle t \rangle$. Найдем число элементов 2-, 3- и 6-го порядков в нормализаторе $N(A_1)$, вычислив централизаторы в нем основных элементов:

$$C_{N(A_1)}(t^3) = T \rtimes \langle t \rangle, \quad C_{N(A_1)}(t^2) = C_{N(A_1)}(t) = \langle t \rangle.$$

Элемент t^2 сопряжен в $Re(q)$ с элементом $\beta(\pm 1)$ и не сопряжен с $t^4 = t^{-2}$ в силу леммы 1. Поэтому элементы t и t^{-1} также не сопряжены, и верна

Лемма 10. *Множество $N(A_1)\backslash C(A_1)$ состоит из двух классов сопряженности в $Re(q)$ по $4|A_1|$ элементов порядка 3 с представителями $\beta(1)$ и $\beta(-1)$, двух классов по $4|A_1|$ элементов 6-го порядка и одного класса из $4|A_1|$ инволюций.*

Лемма 11. *Количество пар $(x, y) \in W'$ с первым элементом порядка 3, централизующим какую-либо инволюцию, равно $|Re(q)|(2q^2 + 4q - 6)$.*

Доказательство. Пусть $z \in Re(q)$ и $\beta(1) \in C(\eta)^z := z^{-1}C(\eta)z$. Тогда $\beta(1)$ и $z\beta(1)z^{-1}$ сопряжены в $C(\eta) = \langle\eta\rangle \times L(q)$, т. е. $cz\beta(1)z^{-1}c^{-1} = \beta(1)$ для некоторого $c \in C(\eta)$. Отсюда $cz \in C(\beta(1)) = \langle\eta\rangle\beta(F)\gamma(F)$ и $z \in C(\eta)\gamma(F)$. Поэтому $\beta(F) \subseteq C(\eta) \cap C(\eta)^z$ и можно считать, что $z = \gamma(s)$.

Пользуясь разложением Брюа для группы $L(q)$, получаем разложение $C(\eta) \cap C(\eta)^z = \beta(F)M\beta(F)$ для некоторой подгруппы M в мономиальной подгруппе $N = H \leftthreetimes \langle\tau\rangle$. Предположим, что диагональный элемент h лежит в пересечении подгрупп $C(\eta)$ и $C(\eta)^{\gamma(s)}$. В силу свойства (Г) $|h| \leq 2$. Случай $h = \eta$ возможен лишь при $s = 0$, и потому $M \cap H = 1$, поскольку

$$1 = [\eta, \gamma(s)^{-1}\eta\gamma(s)] = ((\gamma(s)^{-1})^\eta\gamma(s))^2 = \gamma(s)^4.$$

Но и случай $M \nsubseteq H$ невозможен, так как иначе $|H \cap \langle\beta(F), M\rangle| > 1$. Отсюда

$$C(\eta) \cap z^{-1}C(\eta)z = \beta(F), \quad z = \gamma(s) \ (s \in F). \tag{4}$$

Обозначим через C объединение всех подгрупп, сопряженных с $C(\eta)$ и содержащих элемент $\beta(1)$. Получаем

$$|C| = \Big|\bigcup_{s\in F} C(\eta)^{\gamma(s)}\Big| = q|C(\eta)| - (q-1)|\beta(F)| = q(q-1)(q^2+q-1).$$

С учетом леммы 1 подгруппа Бореля B — единственная из сопряженных с ней подгрупп, содержащих $\beta(1)$. Очевидно, что пересечение $B \cap C(\eta)^{\gamma(s)}$ равно $\beta(F) \leftthreetimes H^{\gamma(s)}$, причем $(\beta(F) \leftthreetimes H^{\gamma(s_1)}) \cap (\beta(F) \leftthreetimes H^{\gamma(s_2)}) = \beta(F)$. Отсюда

$$|B \cap C| = \Big|\bigcup_{x\in F} \beta(F) \leftthreetimes H^{\gamma(x)}\Big| = q\cdot q(q-1) - (q-1)\cdot q = q(q-1)^2,$$

$$|B \cup C| = |B| + |C| - |B \cap C| = |B| + |C| - q(q-1)^2 = 2q^3(q-1).$$

Выберем t так, что $t^2 = \beta(1)$. Положим $D_1 = T \leftthreetimes \langle t\rangle$ и $D_i = \langle t\rangle$ для $i = 2, 3$. Для каждого $i = 1, 2, 3$ найдем мощность множества N_i пар $(\beta(1), y) \in W'$ элементов, лежащих в одной из сопряженных с $N(A_i) = A_i \leftthreetimes D_i$ подгрупп, не лежащих в подгруппах, сопряженных с B и $C(\eta)$. С учетом (Д) и леммы 10 нетрудно убедиться, что число вхождений элементов, сопряженных с $\beta(\pm 1)$, в подгруппы, сопряженные с $N(A_i)$, равно $\frac{|D_i|}{3}|Re(q) : N(A_i)| = \frac{1}{3}|Re(q)|$ и совпадает с $r \cdot q(q-1)(q^3+1)$, где r — число сопряженных с $N(A_i)$ подгрупп, содержащих $\beta(1)$; действительно, число элементов, сопряженных с $\beta(\pm 1)$ в группе $Re(q)$, равно $q(q-1)(q^3+1)$. Отсюда

$$r = \frac{|Re(q)|}{3(q^3+1)(q^2-q)} = \frac{q^2}{3}.$$

Если $y \in D_i$, то подгруппа $\langle\beta(1), y\rangle$ централизует инволюцию t^3 и, следовательно, $(\beta(1), y) \notin N_i$. Когда $y \notin D_i$, покажем, что $(\beta(1), y) \in N_i$, причем $\langle\beta(1), y\rangle$ лежит в единственной подгруппе, сопряженной с $N(A_i)$. Достаточно показать, что число $|\langle\beta(1), y\rangle|$ не делит $|D_i|$. Предположим противное, т. е.

$|\langle\beta(1), y\rangle|$ делит $|D_i|$. Тогда подгруппа $\langle\beta(1), y\rangle$ является a-сопряженной с некоторой подгруппой $D' \subseteq D_i$ при $a \in A_i$. Учитывая включение $\beta(1) \in a^{-1}D'a$, находим $a^{-1}D'a = D'$, поэтому $y \in D_i$ вопреки выбору элемента y. Таким образом, приходим к равенству

$$|N_i| = \frac{q^2}{3}|N(A_i) \setminus D_i| = \frac{q^2}{3}|D_i|(|A_1| - 1).$$

Число всех элементов порядка 3 в группе $Re(q)$, каждый из которых централизует какую-либо инволюцию, равно $q(q-1)(q^3+1)$, так как в подгруппе Бореля B такие элементы образуют подмножество $\beta(F^*)\gamma(F)$. Умножив найденное число на $|B \cup C| + |N_1| + |N_2| + |N_3|$, получаем утверждение леммы. □

Лемма 12. *Количество пар* $(t, x) \in W'$ *с первым элементом порядка* 6 *равно* $|Re(q)|(q^3 + 5q - 6)$.

Доказательство. Каждый элемент 6-го порядка группы $Re(q)$ сопряжен с элементом $\beta(\pm 1)\eta$. Найдем мощность объединения максимальных подгрупп, сопряженных с (3) и содержащих элемент $t = \beta(1)\eta$. Элемент t лежит только в тех подгруппах, в которых лежат одновременно элементы η и $\beta(1)$. В силу (4) подгруппы B и $C(\eta)$ исчерпывают все сопряженные с ними подгруппы, содержащие элемент $t = \beta(1)\eta$, а следовательно, и инволюцию t^3. Учитывая равенство $B \cap C(\eta) = \beta(F) \rightthreetimes H$, находим

$$|B \cup C(\eta)| = q^3(q-1) + q(q-1)(q+1) - q(q-1) = q^4 - q^2.$$

Нетрудно видеть, что для каждого $i = 1, 2, 3$ число подгрупп, сопряженных с $N(A_i)$ и содержащих $\beta(\pm 1)\eta$, равно $q/3$. Попарные пересечения указанных подгрупп имеют порядок, делящий число 24. Поэтому все пары $(t, x) \in W'$ элементов этих пересечений лежат в подгруппе $C(\eta)$. Пары $(\beta(1)\eta, x)$, порождающие подгруппу с НОД$(|\langle\beta(1)\eta, x\rangle|, |A_i|) > 1$ при каком-либо $i = 1, 2, 3$, лежат в единственной подгруппе, сопряженной с $N(A_i)$. Следовательно, число таких пар (t, x) равно $(8q(|A_1| - 1) + 2q(|A_2| + |A_3| - 2)) = 6(q^2 - q)$.

Элементы $t = \beta(1)\eta$ и $t^{-1} = \beta(-1)\eta$ не сопряжены в группе $Re(q)$, причем централизатор в B элемента $\beta(1)\eta$ совпадает с $\beta(F) \rightthreetimes \langle\eta\rangle$. Поэтому число элементов 6-го порядка в B равно $q^3 - q^2$. Следовательно, число всех пар из W' с первым элементом порядка 6 равно

$$|Re(q) : B|(q^3 - q^2)(q^4 - q^2 + 6q(q-1)) = |Re(q)|(q^3 + 5q - 6). \quad \square$$

Лемма 13. *Число пар* $(x, y) \in W'$ *с инволюцией* x *равно* $(2q^2 + q - 2)|Re(q)|$.

Доказательство. Для каждого элемента $y \in Re(q)$ вычислим мощность множества W_y пар (x, y) элементов группы $Re(q)$ с условиями $|x| = 2$ и $(x, y) \in W'$. Очевидно, такие множества не пересекаются, а их объединение для всех $y \in Re(q)$ даст требуемое в лемме подмножество в W'.

В силу леммы 5 достаточно найти $|W_y|$ для $y = \beta(1)$, $\gamma(1)$, $\alpha(1)$, $\beta(1)\eta$, η, a_0, a_1, a_2, a_3, где a_0 — диагональный элемент порядка > 2, а a_i при $i = 1, 2, 3$ — элементы такие, что НОД$(|a_i|, |A_i|) > 1$. Для каждого из указанных элементов при доказательстве лемм 6–12 найдено число сопряженных с ним элементов и перечислены содержащие его подгруппы, сопряженные с (3). Тогда число $|W_y|$ равно числу инволюций в объединении сопряженных с (3) подгрупп, содержащих y.

Поскольку число инволюций в $N(A_i)$, $i = 2, 3$, равно $|A_i|$, то

$$|W_{a_3}| = |A_3|, \quad |W_{a_2}| = |A_2|.$$

Нормализатор $N(A_1) = N(T)$, где T — четверная подгруппа, и централизаторы инволюций из T исчерпывают все максимальные подгруппы, сопряженные с (3) и содержащие a_1. Попарные пересечения этих подгрупп, вычисленные в доказательстве леммы 7, совпадают с $C(T)$ и содержат $4|A_1| + 3$ инволюций. Централизатор инволюции содержит $q(q-1)+1$ инволюций, а число инволюций в $N(A_1)$ равно $4|A_1| + 3$. Отсюда

$$|W_{a_1}| = 4|A_1| + 3 + 3 \cdot (q(q-1)+1) - 3 \cdot (4|A_1| - 3) = 3q^2 - 5q - 5.$$

Максимальные подгруппы, сопряженные с (3) и содержащие a_0, исчерпываются подгруппами B, B^τ и $C(\eta)$. Число инволюций в B равно q^2. Пересечения $B \cap C(\eta) = \beta(F) \leftthreetimes H$, $B^\tau \cap C(\eta) = \beta(F)^\tau \leftthreetimes H$ и $B \cap B^\tau = H$ содержат по одной инволюции. Поэтому

$$|W_{a_0}| = 2q^2 + q(q-1) + 1 - 2 - 1 + 1 \cap C(\eta)| = 3q^2 - q - 1.$$

Итак, число пар $(x, y) \in W'$ с условиями $|x| = 2$ и $|y| \nmid 8q^3$ равно

$$\frac{1}{6}(|W_{a_3}| + |W_{a_2}|) \cdot |Re(q)| + |W_{a_1}| \cdot (q-3) \cdot |Re(q) : N(A_1)| \\ + |W_{a_0}| \cdot (q-3) \cdot |Re(q) : N(H)|. \quad (5)$$

Если пара $(x, \beta(1))$ лежит в $W_{\beta(1)}$ и не порождает подгруппу в B или $C(\eta)^{\gamma(x)}$, $x \in F$, то с точностью до сопряженности $x, \beta(1) \in N(A_i) = A_i \leftthreetimes D_i$ для некоторого $i = 1, 2, 3$, причем $x \in N(A_i) \setminus D_i$. Число инволюций в подгруппах B, $C(\eta)^{\gamma(s)}$ и $C(\eta)^{\gamma(s)} \cap B = \beta(F) \leftthreetimes H^{\gamma(s)}$ равно q^2, $q(q-1)+1$ и 1 соответственно. Кроме того, $C(\eta)^{\gamma(s_1)} \cap C(\eta)^{\gamma(s_2)} = \beta(F)$. Поэтому объединение подгруппы B и подгрупп, сопряженных с $C(\eta)$ и содержащих $\beta(1)$, содержит $q^2 + q \cdot (q(q-1)+1) - q = q^3$ инволюций. Следовательно,

$$|W_{\beta(1)}| = q^3 + \frac{q^2}{3}(4|A_1| + |A_2| + |A_3| - 6) = 2q^3 - q^2,$$

$$|W_{\beta(1)\eta}| = q^2 + (q(q-1)+1) - 1 + \frac{q}{3}(4|A_1| + |A_2| + |A_3| - 6)) = q(3q-2).$$

Все пары (x, y), для которых $x^2 = y^2 = 1$, лежат в W'. Элемент $\gamma(1)$ или $\alpha(1)$ лежит в единственной максимальной подгруппе B, содержащей q^2 инволюций. Поэтому имеем

$$|W_\eta| = |Re(q) : C(\eta)|, \quad |W_1| = |Re(q)|, \quad |W_{\gamma(1)}| = |W_{\alpha(1)}| = q^2.$$

Порядки классов сопряженных элементов с представителями $\beta(\pm 1)$, $\beta(\pm 1)\eta$, $\alpha(1)$, $\gamma(1)$ и η известны из свойств (A), (B) и из доказательств лемм 11 и 12. Поэтому в терминах найденных чисел $|W_{\beta(1)}|$, $|W_{\beta(1)\eta}|$, $|W_{\alpha(1)}|$, $|W_{\gamma(1)}|$ и $|W_\eta|$ число пар $(x, y) \in W'$ с инволюцией x и $\{2, 3\}$-элементом y равно

$$|Re(q) : B| \cdot (|W_{\beta(1)}| \cdot q(q-1) + |W_{\beta(1)\eta}| \cdot (q^3 - q^2) \cdot |Re(q) : B| \\ + |W_{\alpha(1)}|(q^3 - q^2) + |W_{\gamma(1)}|q) + |W_\eta| \cdot |Re(q) : C(\eta)| + |W_1|. \quad (6)$$

Наконец, складывая (5) и (6), получаем требуемое в лемме число. □

Замечание 2. В [14] указано 7-мерное представление группы Шевалле $G_2(K)$ над произвольным полем K (см. также [17]) и, на его основе, когда K есть совершенное поле характеристики 3, представление группы Ри в $SL_7(K)$. В [18] для построения 7-мерного представления группы $G_2(F)$ над алгебраически замкнутым полем характеристики 3 и вместе с тем представления группы Ри ${}^2G_2(q) = \langle U, \tau\rangle$ в $SL_7(q)$ применяется подход с использованием системы компьютерной алгебры.

§ 4. Доказательство основной теоремы

Завершим доказательство теоремы 1.

Подгруппы в $Re(q)$, не лежащие в подгруппах, сопряженных с B, $C(\eta)$ или $N(A_i)$ $(i = 1, 2, 3)$, в силу (Ж) и леммы 2 исчерпываются подгруппами порядков 56 и 168, т. е. сопряженными с $P_2 \leftthreetimes A_3$ или $N(P_2)$. Непосредственно или с помощью GAP находим значения на них функции φ_2:

$$\varphi_2(P_2 \leftthreetimes A_3) = 2688, \quad \varphi_2(N(P_2)) = 18816.$$

Число сопряженных в $Re(q)$ с каждой из них равно $|Re(q) : N(P_2)|$, так что

$$|W \setminus W'| = (18816 + 2688) \cdot |Re(q) : N(P_2)| = 128|Re(q)|.$$

Вместе с леммами 4, 9, 11–13 это дает

$$|W| = (q^4 - q^2 + 16q - 114)|Re(q)|.$$

Положим

$$\rho(q) = \left(|Re(q)| - \frac{|W|}{|Re(q)|} - \frac{\varphi_2(Re(3)') - \varphi_2(Re(3))}{|Re(3)|}\right) \quad (q = 3^n > 3).$$

Непосредственно или с помощью GAP несложно устанавливаются равенства $\varphi_2(Re(3)) = 1717632$ и $\varphi_2(Re(3)') = 214704$. Поэтому

$$\rho(q) = (q-3)(q^6 + 2q^5 + 6q^4 + 18q^3 + 53q^2 + 160q + 464).$$

Тогда соотношения (2) и (1) дают

$$\varphi_2(Re(q)) = |Re(q)|\left(\rho(q) - \sum_{t|n,\, n>t>1} \frac{\varphi_2(Re(3^t))}{|Re(3^t)|}\right) = n|Re(q)| \cdot d_2(Re(q)).$$

Поскольку $\varphi_2(Re(3^t)) = |\operatorname{Aut} Re(3^t)| \cdot d_2(Re(3^t)) = t|Re(3^t)| \cdot d_2(Re(3^t))$, то

$$d_2(Re(q)) = \frac{1}{n}\Big[\rho(q) - \sum_{t|n,\, n>t>1} t \cdot d_2(Re(3^t))\Big].$$

Это завершает доказательство основной теоремы 1.

Замечание 3. С учетом замечания 1 вопрос Сыскина получает решение для всех групп лиева типа ранга 1, за исключением унитарного случая.

ЛИТЕРАТУРА

1. *Hall Ph.* The Eulerian functions of a group // Quart. J. Math. 1936. V. 7. P. 134–151.
2. *Коуровская тетрадь.* Нерешенные вопросы теории групп. 15-е изд. Новосибирск: Ин-т математики СО РАН, 2002.
3. *Erfanian A., Wiegold J.* A note on growth sequence for finite simple groups // Bull. Austral. Math. Soc. 1995. V. 51. P. 495–499.
4. *Erfanian A., Rezaei R.* On the growth sequence of $PSp(2m, q)$ // Int. J. Algebra. 2007. V. 1, N 2. P. 51–62.
5. *Erfanian A.* A note on growth sequences of alternating groups // Arch. Math. 2002. V. 78, N 4. P. 257–262.
6. *Erfanian A.* A note on growth sequences of PSL(m,q) // Southeast Asian Bull. Math. 2005. V. 29, N 4. P. 697–713.
7. *Ушаков Ю. Ю.* Оценка функций Ф. Холла на группах лиева типа ранга 1 // Владикавк. мат. журн. 2012. Т. 15, № 2. С. 50–56.
8. *Сучков Н. М., Приходько Д. М.* О числе пар порождающих групп $L_2(2^m)$ и $Sz(2^{2k+1})$ // Сиб. мат. журн. 2001. Т. 42, № 5. С. 1162–1167.
9. *Приходько Д. М.* О числе пар порождающих простой конечной группы // V Междунар. конф. «Алгебра и теория чисел: современные проблемы и приложения». Тула: ТГПУ, 2003. С. 185–186.
10. *Carter R. W.* Simple groups of Lie type. London: John Wiley & Sons, 1972.
11. *Стейнберг Р.* Лекции о группах Шевалле. М.: Мир, 1975.
12. *Ward H. N.* On Ree's series of simple groups // Trans. Amer. Math. Soc. 1966. V. 121, N 1. P. 62–89.
13. *Janko Z., Thompson J. C.* On a class of finite simple groups of Ree // J. Algebra. 1966. V. 4, N 2. P. 274–292.
14. *Левчук В. М., Нужин Я. Н.* О строении групп Ри // Алгебра и логика. 1985. Т. 24, № 1. С. 26–41.
15. *Каргаполов М. И., Мерзляков Ю. И.* Основы теории групп. М.: Наука, 1996.
16. *Левчук Д. В.* Функции Ф. Холла на группах лиева типа ранга 1 // Владикавк. мат. журн. 2008. Т. 10, № 1. С. 37–39.
17. *Hurrelbrink J., Rehmann U.* Eine endliche Presentation der Gruppe $G_2(Z)$ // Math. Z. 1975. Bd 141, Heft 3. S. 243–251 .
18. *Kemper G., Lübeck F., Magaard K.* Matrix generators for the Ree groups ${}^2G_2(q)$ // Comm. Algebra. 2001. V. 29, N 1. P. 407–413.

Статья поступила 16 января 2012 г.

Ушаков Юрий Юрьевич, Левчук Денис Владимирович
Сибирский федеральный университет, кафедра алгебры и математической логики,
пр. Свободный, 79, Красноярск 660041
yuron@akadem.ru, dlevchuk82@mail.ru