Известия Гомельского государственного университета
имени Ф.Скорины, 3(36), 2006

УДК 512.54

Зависимость порядков конечной простой группы и пересечения централизатора и класса сопряженных элементов инволюции

О. В. Голованова[1], В. М. Левчук[2]

Введение

Как обычно, централизатор элемента τ в группе G обозначаем через $C_G(\tau)$, а класс сопряженных элементов с представителем τ – через τ^G. По известной теореме Р. Брауэра число конечных простых групп с заданным централизатором инволюции конечно. Разрабатывая с 90-х годов обобщение этой теоремы, В.П. Шунков ввел (см., например, [1]) понятие *параметра вложения инволюции:*

$$t(G,\tau) = \max_{g\in G} |gC_G(\tau) \cap (\tau^G\tau^G)|.$$

В 2001-м году он анонсировал теорему [2]: *Существует только конечное число периодических простых групп с инволюцией и с заданным конечным параметром вложения этой инволюции, причем все они конечны.*

В основе теоремы Шункова лежит предположение: *Существует только конечное число конечных простых групп с заданным конечным параметром вложения инволюции.* Доказательство теоремы к настоящему времени не опубликовано и авторы исследуют его с 2003 года. О. В. Голованова (Листова) [3] установила неограниченность параметров вложения инволюции $\tau = (1\,2)(3\,4)$ в бесконечных семействах знакопеременных групп A_n. (Компьютерные вычисления параметров вложения инволюций знакопеременных групп малых степеней и некоторых спорадических групп см. [4] и [5].) См. также [6] и § 3 ниже.

Ясно, что $t(G,\tau) \geq |C_G(\tau) \cap \tau^G|$ и поэтому вызывает интерес

Гипотеза 1. *Для любого натурального числа m существует только конечное число конечных простых неабелевых групп G, имеющих инволюцию τ с условием $|C_G(\tau) \cap \tau^G| \leq m$.*

Конечно, гипотезу 1 достаточно (по модулю ККПГ) подтвердить для бесконечных семейств знакопеременных групп A_n и групп лиева типа. Симметрическую группу степени n обозначаем через S_n. К основным результатам статьи относится

Теорема 2. *Пусть $G = S_n$ или A_n и M – произвольное натуральное число. Тогда для любой инволюции τ из G при достаточно большом $|G|$ имеем $|C_G(\tau) \cap \tau^G| > M$.*

Случай групп $PSL_n(q)$ рассматривает теорема 2.1. В § 3 гипотеза 1 подтверждается для групп лиева типа ранга 1 (теорема 3.1). См. там же замечание в начале параграфа.

§ 1. Симметрические и знакопеременные группы

Основным результатом параграфа является

---

[1]Автор поддержан РФФИ (грант № 05-01-00576-а)
[2]Автор поддержан РФФИ (грант № 06-01-00824)

Теорема 1.1. *Пусть $G = S_n$ или A_n, и пусть N – произвольное натуральное число. Если порядок $|G|$ группы G достаточно большой, то для любой инволюции τ из G имеем $|C_G(\tau) \cap \tau^G| > N$.*

Описание классов сопряженных элементов в S_n и A_n дает известная

Лемма 1.2. *Если $\beta = (a_{11} \dots a_{1r})(a_{21} \dots a_{2s}) \dots (a_{m1} \dots a_{mt})$ и*

$$\alpha = \begin{pmatrix} a_{11} & \dots & a_{1r} & a_{21} & \dots & a_{2s} & \dots & a_{m1} & \dots & a_{mt} \\ b_{11} & \dots & b_{1r} & b_{21} & \dots & b_{2s} & \dots & b_{m1} & \dots & b_{mt} \end{pmatrix},$$

то

$$\alpha^{-1}\beta\alpha = (b_{11} \dots b_{1r})(b_{21} \dots b_{2s}) \dots (b_{m1} \dots b_{mt}).$$

Следствие 1.3. *Две подстановки сопряжены в симметрической группе тогда и только тогда, когда они имеют одинаковое число циклов каждой длины.*

Доказательство леммы и ее следствия см. [7, лемма 5.1.1 и теорема 5.1.3].

Следствие 1.3 позволяет перечислить инволюции в группах S_n и A_n.

Лемма 1.4. *Симметрическая группа S_n имеет, в точности, $\left[\frac{n}{2}\right]$ классов сопряженных инволюций и их представителями являются*

$$\sigma_k = (1\,2)(3\,4)\dots(2k-1\;\,2k), \quad 1 \le k \le \left[\frac{n}{2}\right].$$

Порядок централизатора инволюции σ_k равен

$$|C_{S_n}(\sigma_k)| = 2^k \cdot (k)! \cdot (n-2k)!.$$

Лемма 1.5. *Если две инволюции из A_n сопряжены в S_n, то они сопряжены и в A_n. Знакопеременная группа A_n имеет, в точности, $\left[\frac{n}{4}\right]$ классов сопряженных инволюций и их представителями являются*

$$\tau_k = (1\,2)(3\,4)(5\,6)(7\,8)\dots(4k-3\;\,4k-2)(4k-1\;\,4k), \quad 1 \le k \le \left[\frac{n}{4}\right].$$

Порядок централизатора инволюции τ_k равен

$$|C_{A_n}(\tau_k)| = 2^{2k-1} \cdot (2k)! \cdot (n-4k)!$$

Доказательство. Докажем лемму 1.5; доказательство леммы 1.4 проводится аналогично.

Произвольная инволюция из A_n есть произведение четного числа $2k$ независимых циклов длины 2 и имеет вид $(a_1\ a_2)(a_3\ a_4)\dots(a_{4k-1}\ a_{4k})$. По лемме 1.2 она сопряжена подходящим элементом $\alpha \in S_n$ с элементом τ_k. Поскольку подстановка τ_k не изменяется при замене цикла $(1\ 2)$ на $(2\ 1)$, то можем считать, что $\alpha \in A_n$. В силу следствия 1.3, подстановки τ_k попарно не сопряжены в S_n и, тем более, в A_n. Отсюда вытекает, что A_n имеет точно $\left[\frac{n}{4}\right]$ классов сопряженных инволюций.

По лемме 1.2, для произвольной подстановки $\pi \in S_n$ получаем:

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & 4k-1 & 4k & \dots & n \\ j_1 & j_2 & j_3 & j_4 & \dots & j_{4k-1} & j_{4k} & \dots & j_n \end{pmatrix},$$

$$\pi^{-1}\tau_k\pi = (j_1\,j_2)(j_3\,j_4)\dots(j_{4k-1}\;j_{4k}).$$

Для всех подстановок $\pi \in C_{S_n}(\tau_k)$ элементы $j_{4k+1}, j_{4k+2}, \dots, j_n$ пробегают множество $\{4k+1, 4k+2, \dots, n\}$ и их можно выбрать $(n-4k)!$ различными способами. С другой стороны, множество $\{j_1, j_2\}$ для подстановки π можно выбрать $2k$ различными способами: $\{1, 2\}$, $\{3, 4\}$, $\ldots, \{4k-1, 4k\}$. Тогда множество $\{j_3, j_4\}$ можно выбрать $2k-1$ различными способами. Продолжая далее, получаем $(2k)!$ различных способов выбора набора множеств $\{j_1, j_2\}$, $\{j_3, j_4\}$, ..., $\{j_{4k-1}, j_{4k}\}$ для подстановки π. Учитывая равенства $(j_1 j_2) = (j_2 j_1)$, $\ldots$, $(j_{4k-1}\ j_{4k}) = (j_{4k}\ j_{4k-1})$, получаем $2^{2k} \cdot (2k)!$ различных способов выбора символов $j_1, j_2, \ldots, j_{4k}$ подстановки $\pi \in C_{S_n}(\tau_k)$. Включение $\pi \in A_n$ выполняется, очевидно, лишь в половине этих случаев. Таким образом, централизатор $C_{A_n}(\tau_k)$ состоит из $2^{2k-1} \cdot (2k)! \cdot (n-4k)!$ подстановок. Лемма доказана.

Доказательство теоремы 1.1. Пусть $G = S_n$ или A_n и τ – произвольная инволюция из G. Оценим количество инволюций, лежащих в пересечении

$$D = C_G(\tau) \cap \tau^G.$$

Нам нужно показать, что порядок $|D|$ растет вместе с порядком $|G|$.

Число символов в носителе инволюции τ, то есть число действительно перемещаемых ею символов, есть четное число $2m$. Число $2m$-элементных подмножеств M во множестве из $n-2m$ элементов, не лежащих в носителе, равно $\binom{n-2m}{2m}$. При ограниченном m это число растет вместе с возрастанием n. С другой стороны, каждое подмножество M есть носитель хотя-бы одной инволюции из D. Различным подмножествам M соответствуют различные инволюции из D, откуда

$$|D| > \binom{n-2m}{2m}.$$

С точностью до сопряжения в G, можем считать, что инволюция τ совпадает с подстановкой $\sigma_k = (1\,2)(3\,4)(5\,6)\ldots(2m-1\ \ 2m)$. Произведения ее независимых циклов

$$(j_1\, j_2)(j_3\, j_4), \quad (j_1\, j_3)(j_2\, j_4), \quad (j_1\, j_4)(j_2\, j_3)$$

всегда попарно перестановочны. (Вместе с единичной подстановкой они дают силовскую 2-подгруппу знакопеременной группы степени 4.) В частности, это позволяет выбрать две инволюции в D, отличные от τ и получающиеся из нее заменой произведения $(1\ 2)(i\ \ i+1)$ независимых циклов на произведение $(1\ \ i)(2\ \ i+1)$ или $(1\ \ i+1)(2\ \ i)$. Всего инволюций в D находим таким способом, по крайней мере, $2 \cdot \binom{m}{2} + 1$.

Таким образом, для произвольной инволюции $\tau \in G$ с носителем порядка $2m$ во всех случаях выполняется неравенство

$$|C_G(\tau) \cap \tau^G| > \max\left\{\binom{n-2m}{2m}, m(m-1)\right\}.$$

Заметим, что когда порядок группы G достаточно большой, то и число n достаточно большое, а следовательно достаточно большим будет либо число $m(m-1)$, либо число $\binom{n-2m}{2m}$. Поэтому, в силу предыдущего неравенства, для выбранных групп G достаточно большого порядка при любом выборе инволюции $\tau \in G$ порядок пересечения $|C_G(\tau) \cap \tau^G|$ будет больше любого наперед заданного числа N. Теорема доказана.

§ 2. Группа $PSL_n(q)$

Теорема 2.1. *Пусть $G = PSL_n(q)$ и M – произвольное натуральное число. Если порядок $|G|$ группы G достаточно большой, то для любой инволюции τ из G, с* *условием диагонализируемости в G при нечетном q, имеем $|C_G(\tau) \cap \tau^G| > M$.*

Доказательство. Ясно, что если порядок $|G|$ группы $G = PSL_n(q)$ возрастает, то растет либо n, либо q и нам потребуется рассматривать обе возможности. Случай $n = 2$ рассмотрен в [6] и далее считаем $n > 2$.

Выберем инволюцию τ группы $G = PSL_n(q)$ как в теореме. Все характеристические корни матрицы, соответствующей τ в $SL_n(q)$, равны ± 1. Отсюда легко следует, что τ приводится к жордановой форме J сопряжением в группе G. Когда q – нечетное число, J является диагональной матрицей с элементами ± 1 по главной диагонали.

Нам потребуется

Лемма 2.2. *Инволюция $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ $SL_2(q)$-сопряжена при четном или нечетном q соответственно с матрицей*

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \quad diag\ (-1, 1).$$

Доказательство. При четном q указанные матрицы сопряжены даже в группе $SL_2(2) \cong S_3$. Сравнивая характеристические многочлены указанных матриц при нечетном q, получаем их сопряженность по теореме Жордана в $GL_2(q)$; в силу диагональности одной из матриц и ее централизатора, матрицы также $SL_2(q)$-сопряжены.

В случае нечетного q инволюция τ из теоремы сопряжена в группе G с диагональной матрицей

$$\tau_k = diag(-E_{2k}, E_{n-2k}) = diag(-1, \ldots, -1, 1, \ldots, 1), \quad 1 < 2k < n,$$

(E_m — единичная $m \times m$ матрица) имеющей централизатор

$$C_G(\tau_k) = \left\{ \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} \mid A \in GL_{2k}(q),\ B \in GL_{n-2k}(q),\ |A| \cdot |B| = 1 \right\}.$$

Инволюция τ_k сопряжена с инволюцией

$$diag(-1, 1, \ldots, -1, 1, Q),$$

где Q при $2k < n - 2k$ есть единичная матрица E, $Q = -E$ при $2k > n - 2k$ и $Q = \emptyset$ при $2k = n - 2k$. В силу леммы 2.2, τ_k сопряжена также с инволюцией

$$diag\left(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \ldots, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, Q \right) = \sigma.$$

Матрица σ лежит в централизаторе $C_G(\tau_k)$ инволюции τ_k, поскольку число элементов -1 по главной диагонали τ_k четно. Поэтому централизатор $C_G(\tau_k)$ содержит как диагональную подгруппу H группы G, так и множество σ^H инволюций. Пользуясь включениями

$$diag\ (t_1, t_1^{-1}, t_2, t_2^{-1}, \ldots) \in H,$$

$$diag\left(\begin{pmatrix} 0 & t_1^2 \\ t_1^{-2} & 0 \end{pmatrix}, \begin{pmatrix} 0 & t_2^2 \\ t_2^{-2} & 0 \end{pmatrix}, \ldots \right) \in \sigma^H \quad (t_1, t_2 \in GF^*(q)),$$

и полагая $L = \min\{2k, n - 2k\}$, находим неравенства

$$|C_G(\tau_k) \cap \tau_k^G| \geq |\sigma^H| \geq \left(\frac{q-1}{2}\right)^L.$$

Отсюда вытекает, что порядок $|C_G(\tau_k) \cap \tau_k^G|$ пересечения растет, если q возрастает.

Оказывается, порядок пересечения возрастает также и в случаях, когда растет степень n матриц. Действительно, централизатор $C_G(\tau_k)$ содержит диагональную подгруппу H группы G. Диагональная инволюция из H сопряжена в G с τ_k тогда и только тогда, когда число элементов -1 на ее главной диагонали равно $2k$. Поскольку $1 < 2k < n$, то число

$$\begin{pmatrix} n \\ 2k \end{pmatrix} = \frac{n!}{(2k)!(n-2k)!}$$

таких инволюций всегда растет с возрастанием n.

Пусть сейчас q — четное число. Тогда жорданова форма произвольной инволюции имеет $k \geq 1$ клеток вида $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ и $n - 2k$ клеток (1) размерности 1. Поэтому группа $G = PSL_n(q)$ (аналогично $SL_n(q)$) имеет, в точности, $[\frac{n}{2}]$ классов сопряженных инволюций, как и в [8, §4]. Представителями классов можно взять инволюции

$$\eta_k = diag\left(\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \ldots, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, 1, \ldots, 1\right)$$

с k клетками размерности 2, $1 \leq k \leq [\frac{n}{2}]$. Для централизатора инволюции η_k в G выполняется включение

$$C_G(\eta_k) \supset \{diag\,(UT_2(q), \ldots, UT_2(q), 1, \ldots, 1)\}\,.$$

В частности, централизатор содержит $(q-1)^k$ сопряженных с η_k инволюций

$$diag\left(\begin{pmatrix} 1 & 0 \\ s_1 & 1 \end{pmatrix}, \ldots, \begin{pmatrix} 1 & 0 \\ s_k & 1 \end{pmatrix}, 1, \ldots, 1\right), \quad s_1, \ \ldots, \ s_k \in GF^*(q).$$

Отсюда вновь вытекает, что порядок $|C_G(\eta_k) \cap \eta_k^G|$ возрастает, если порядок q основного поля четный и растет.

Допустим, что возрастает степень n матриц. По доказанному выше, произвольная инволюция группы $G = PSL_n(q)$ сопряжена в ней с инволюцией η_k и, в силу леммы 2.2, с инволюцией

$$diag\left(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \ldots, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, 1, 1, \ldots, 1\right) = \sigma_k,$$

где число клеток размерности 2 равно k. Таким образом, доказано, что всякая инволюция группы G сопряжена с одной из мономиальных инволюций σ_k, $1 \leq k \leq [\frac{n}{2}]$.

С другой стороны, мономиальная подгруппа $N(q)$ в G является расщепляемым расширением диагональной подгруппы $D(q)$. Более того,

$$N(q) = D(q)\lambda N(2), \quad N(2) \cong S_n.$$

Поэтому, элементы из $N(2)$ можем записывать, как подстановки, в частности,

$$\sigma_k = (1\ 2)(3\ 4)\ldots(2k-1\ 2k), \quad 1 \leq k \leq \left[\frac{n}{2}\right].$$

Отсюда

$$|C_G(\sigma_k) \cap \sigma_k^G| > |C_{S_n}(\sigma_k) \cap \sigma_k^{S_n}|,$$

поскольку для подгруппы H произвольной группы G и инволюции τ из H всегда имеем

$$|C_G(\tau) \cap \tau^G| > |C_H(\tau) \cap \tau^H|.$$

Остается применить теорему 1.1. Теорема полностью доказана.

§ 3. Группы лиева типа

Методы доказательства теоремы 2.1 позволяют подтвердить гипотезу 1 и для других классических групп. Известно (в частности, [9], [10]), что представляя такую группу группой Шевалле $G(q)$, в ее группе Вейля $W = W(G)$ всегда имеем подгруппу, изоморфную симметрической группе достаточно большой степени, если лиев ранг $G(q)$ достаточно большой. Например,

$$W(B_n) \cong W(C_n) \cong W(^2D_{n+1}) \cong S_n \lambda (Z/2Z)^n.$$

Отдельных рассмотрений требуют группы исключительных лиевых типов. Далее в этом параграфе доказывается

Теорема 3.1. *Пусть M –натуральное число и $G = G(q)$ — группа лиева типа ранга 1 над полем порядка q. Тогда при достаточно большом q имеем $|C_G(\tau) \cap \tau^G| > M$ для любой инволюции τ из G.*

Доказательство. В простой группе лиева типа ранга 1 инволюции образуют один класс сопряженных элементов. Возрастание вместе с q параметров вложения инволюций в группах $PSL_2(q)$, Ри $^2G_2(q)$ и Сузуки $^2B_2(q)$ доказано в [6]. Теорема 3.1 для этих групп, по существу, доказана там же. Остается доказать теорему для унитарных групп.

Унитарная группа $G = PSU_3(q^2)$ над полем $F = GF(q^2)$ в представлении [9, § 13.7] порождается матрицами

$$(t,u) = \begin{pmatrix} 1 & 0 & 0 \\ t & 1 & 0 \\ u & \bar{t} & 1 \end{pmatrix} \quad (u,\ t \in F,\ \bar{t} = t^q,\ u + \bar{u} = t\bar{t}),$$

$$\tau = \begin{pmatrix} 0 & 0 & 1 \\ 0 & -1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \quad \delta(t) = \begin{pmatrix} t & 0 & 0 \\ 0 & t^{-1}\bar{t} & 0 \\ 0 & 0 & \bar{t}^{\,-1} \end{pmatrix},\ t \in F^* = F \setminus \{0\}.$$

Матрицы (t,u) образуют унипотентную подгруппу U, центр которой имеет порядок q и совпадает с подгруппой

$$Z(U) = \{(0,u) \mid u \in F,\ \bar{u} = -u\}.$$

Элементы $\delta(t)$ образуют диагональную подгруппу H и действуют сопряжениями на $Z(U)$ по правилу:

$$\delta(t)^{-1}\ (0,u)\ \delta(t) = (0, ut\bar{t}).$$

Поскольку $\frac{q^2-1}{q+1} = q-1$, то элементы $t\bar{t} = t^{q+1}$ при $t \in F^*$ пробегают мультипликативную группу ненулевых элементов подполя порядка q в F. Поэтому H-сопряжения действуют транзитивно на множестве нееденичных элементов из $Z(U)$. Если σ – любой из этих элеменов, то

$$|C_G(\sigma) \cap \sigma^G| \geq q - 1.$$

Это доказывает теорему для четных q, поскольку в этих случаях все нееденичные элементы из $Z(U)$ являются инволюциями.

Пусть q — нечетно. Централизатор в G инволюции

$$\delta(-1) = diag\ (-1, 1, -1) = \pi$$

содержит инволюцию τ и подгруппу $Z(U)\lambda H$. Более точно,

$$C_G(\pi) = \left\{ \begin{pmatrix} a_{11} & 0 & a_{12} \\ 0 & |A|^{-1} & 0 \\ a_{21} & 0 & a_{22} \end{pmatrix} |A = ||a_{ij}|| \in U_2(q^2) \right\} \cong U_2(q^2).$$

В частности, $q-1$ сопряженных в G инволюций

$$\delta(t)\tau\delta^{-1}(t) = \begin{pmatrix} 0 & 0 & t\bar{t} \\ 0 & -1 & 0 \\ (\bar{t}t)^{-1} & 0 & 0 \end{pmatrix}, \quad t \in F^*,$$

лежат в централизаторе $C_G(\pi)$ и поэтому

$$|C_G(\pi) \cap \pi^G| > q-1.$$

Теорема доказана.

Abstract. Let $G = S_n$, A_n or $PSL_n(q)$, and M is a natutal number.Then for every involution τ of G for sufficiently big $|G|$ we have $|C_G(\tau) \cap \tau^G| > M$.

Литература

1. Рябинина Н.А., Сучков Н.М., Шунков В.П. Об особых подгруппах конечных групп с инволюциями, Алгебраические системы (сборник научных трудов). Красноярск: Препринт ВЦ СО РАН, № 10 (1995), 3–11.

2. Шунков В.П. Группы с инволюциями, Международный семинар по теории групп (Екатеринбург, 17–21 декабря 2001г.), тезисы докл. — Екатеринбург: Ин-т мат. и мех. УрО РАН, изд-во Урал. ун-та, 2001, 245–246.

3. Голованова (Листова) О.В. Параметры вложения инволюций знакопеременных групп, Algebra and Model Theory. Collection of papers. Edited by A.G. Pinus and K.N. Ponomarev. Novosibirsk State Technical University, 2003, 62–68.

4. Листова О.В. О группе Матье M_{12}, Международный семинар по теории групп (Екатеринбург, 17-21 декабря 2001г.), тезисы докл., Екатеринбург: Ин-т мат. и мех. УрО РАН; Изд-во Урл. ун-та, 2001, 135.

5. Листова О.В. Параметры вложения инволюций некоторых групп, Материалы Конференции молодых ученых Института вычислительного моделирования СО РАН. Красноярск: ИВМ СО РАН, 2003, 30–35.

6. Голованова О.В. Параметры вложения инволюций конечных простых групп лиева типа ранга 1: Сб. статей “IV Всесибирский конгресс женщин-математиков”, Красноярск: КрасГУ, 2006.

7. Холл М. Теория групп, Под ред. Л.А. Калужнина, Москва, Издательство иностранной литературы, 1962.

8. Aschbacher M. and Seitz G.M. Involutions in chevalley groups over fields of even order, Nagoya Math. J., **63** (1976), 1–91.

9. Carter R.W., Simple groups of Lie type, New York, Wiley and Sons, 1972.

10. Бурбаки Н. Группы и алгебры Ли, Москва, Мир, 1972.

Красноярский государственный университет

Поступило 11.04.06