О строго вещественных элементах конечных групп

А. В. ТИМОФЕЕНКО
Красноярский государственный педагогический университет
e-mail: A.V.Timofeenko62@mail.ru

УДК 512.54

Ключевые слова: расширенный централизатор, строго вещественный элемент, группа, инволюция.

Аннотация

Если G — группа, $x \in G$ и в группе G найдётся такая инволюция i, что $x^i = x^{-1}$, то элемент x называют *строго вещественным*, как и группу, состоящую только из таких элементов. В настоящей работе расположение строго вещественных элементов в конечной группе и существование в ней элементов, которые строго вещественными не являются, изучаются в связи с вопросами 14.69 и 14.82 из «Коуровской тетради». Для доказательства теорем созданы и реализованы в системе компьютерной алгебры GAP4r3 алгоритмы, которые можно применять и для некоторых других конечных групп.

Abstract

A. V. Timofeenko, On strongly real elements of finite groups, Fundamentalnaya i prikladnaya matematika, vol. 11 (2005), no. 2, pp. 209—218.

Let G be a group and $x \in G$. If x is inverted by an involution i of G, i.e., $x^i = x^{-1}$, then the element x is called *strongly real*. A group consisting of only strongly real elements is called *strongly real*. In this paper, we study the disposition of strongly real elements in a finite group and the existence of elements that are not strongly real in connection with problems 14.69 and 14.82 from "The Kourovka Notebook." For the proofs of the theorems, algorithms are created and implemented in the computer algebra system GAP4r3. They can also be applied for some other finite groups.

Если G — группа, $x \in G$ и в группе G найдётся такая инволюция i, что $x^i = x^{-1}$, то элемент x называют *строго вещественным*, как и группу, состоящую только из таких элементов. Ясно, что элемент x является произведением инволюций xi и i при $x \neq i$. В самом общем плане, без предположения конечности группы, вопросы расположения строго вещественных и близких им элементов освещены в работах В. П. Шункова (см., например, [5]). В [3] доказано, что если числа t и m фиксированы, то среди конечных групп G с инволюцией i, параметр вложения которой в G не превосходит t, строго i-вещественную подгруппу порядка больше m содержат те группы, для которых порядок $|i^G|$ достаточно велик. Строго i-вещественной называется такая подгруппа H группы G, что каждый элемент из H инвертируется инволюцией i, а параметром вложения инволюции i в группе G называется число $\max\limits_{g \in G}\{|gC_G(i) \cap i^G i^G|\}$.

Фундаментальная и прикладная математика, 2005, том 11, № 2, с. 209—218.

В настоящей работе расположение строго вещественных элементов в конечной группе и существование в ней элементов, которые строго вещественными не являются, изучаются в связи с вопросами 14.69 (Я. Н. Нужин), 14.82 (А. И. Созутов записал как известный) из «Коуровской тетради» [2].

Теорема 1. *Строго вещественными спорадическими конечными простыми группами являются только группы Янко J_1 и J_2, причём $J_1 = CC_1$ для класса C сопряжённых в J_1 инволюций и некоторого его подмножества C_1 мощности не больше 867, а множество элементов группы J_2 нельзя представить ни как произведение двух её классов сопряжённых инволюций, ни как квадрат каждого из них, но если A — класс сопряжённых инволюций группы J_2, то каждый её элемент равен произведению трёх инволюций из A.*

Доказательство. Ответ на вопрос о строгой вещественности конечных простых спорадических групп найден С. Г. Колесниковым и Я. Н. Нужиным [6]. Элементы, не являющиеся строго вещественными, они нашли по таблице характеров каждой спорадической группы, кроме групп J_1 и J_2. Изложенное ниже рассуждение позволяет для каждого элемента группы либо доказать, что он не является строго вещественным, либо указать в этой группе все элементы, которые сопряжением переводят данный элемент в обратный.

Пусть G — группа, $x \in G$ и $\mathrm{Invert}(G,x) = \{i \in G \mid |i| = 2,\ x^i = x^{-1}\}$. Тогда если множество $\mathrm{Invert}(G,x)$ пустое, то элемент x не является строго вещественным. Опишем алгоритм построения множества $\mathrm{Invert}(G,x)$. Подробнее изложены те его части, которые не были запрограммированы в системе компьютерной алгебры GAP4r3.

Напомним, что *расширенным централизатором* $C_G^*(x)$ элемента x группы G называется множество $\{g \in G \mid g^{-1}xg \in \{x, x^{-1}\}\}$. Если централизатор $C_G(i)$ — собственная подгруппа расширенного централизатора, то индекс $|C_G^*(x) : C_G(x)|$ равен 2. Действительно, если $g_1, g_2 \in C_G^*(x) \setminus C_G(x)$, то $x^{g_2} = x^{g_1}$, $x^{g_2 g_1^{-1}} = x$, т. е. $g_2 g_1^{-1} \in C_G(x)$. Поэтому $g_2 \in C_G(x)g_1$ и $C_G^*(x) = C_G(x) \cup C_G(x)g_2$. Элементы множества $\mathrm{Invert}(G,x)$ будем обозначать буквой u. Разберём отдельные случаи.

1. $|x| = 1$. Тогда u пробегает множество всех инволюций группы G. Если известны представители не каждого класса сопряжённых в G инволюций, то строится силовская 2-подгруппа группы G. Затем из этой подгруппы выбираются все инволюции. Те из них, которые попарно не сопряжены в G, и являются представителями классов, объединение которых есть множество всех инволюций группы G.

2. x — инволюция. Тогда из $x^u = x^{-1} = x$ следует $u \in C_G(x)$. Следовательно, u пробегает множество инволюций подгруппы $C_G(x)$.

3. $|x| > 2$. Из $uxu = x^{-1}$ следует $u \in C_G^*(x) \setminus C_G(x)$. При отрицательном ответе на вопрос о сопряжённости в G элементов x^{-1} и x получаем, что элемент x не является строго вещественным. Если же $x^g = x^{-1}$ для некоторого $g \in G$, то ввиду $C_G^*(x) = C_G(x) \cup C_G(x)g$ каждая интересующая нас инволюция u

лежит в смежном классе $C_G(x)g$. Сначала строим расширенный централизатор $C_G^*(x) = \text{гр}(C_G(x), g)$. Затем из множества всех инволюций подгруппы $C_G^*(x)$ удаляем инволюции централизатора $C_G(x)$, остаются все обращающие элемент x инволюции группы G. Если множество $C_G^*(x) \setminus C_G(x)$ инволюций не содержит, то элемент x не является строго вещественным.

Пусть x пробегает множество представителей всех классов сопряжённых элементов группы G. Если для каждого такого x множество $\mathrm{Invert}(G, x)$ непусто, то G — строго вещественная группа. Если же в группе G найдётся такой y, что $\mathrm{Invert}(G, y) = \varnothing$, то каждый элемент класса y^G не является строго вещественным и группа G тоже.

Для групп Янко J_1 и J_2 множество представителей их классов сопряжённых элементов автор взял из [7]. Проверка строгой вещественности каждого из них по реализованному в системе ГАП (GAP) алгоритму построения множества Invert заняла несколько секунд. Строгая вещественность групп J_1 и J_2 доказана.

Пусть C — множество всех сопряжённых в G инволюций. Если в памяти компьютера умещается список L всех элементов группы, то на вопрос о верхней границе мощности множества C_1 из теоремы 1 можно ответить так.

Для каждого $j \in C$ удаляем из L его подмножество $L \cap jC$ и полученное множество снова обозначаем буквой L. Параллельно подсчитываем количество таких $j \in C$, что $L \cap jC = \varnothing$. Вычисления останавливаются, когда либо $L = \varnothing$, либо рассмотрены все элементы $j \in C$.

В группе J_1 все инволюции сопряжены, и множество L становится пустым после того, как из него 867 раз удалены пересечения $L \cap jC$. Другими словами, мощность подмножества C_1 равна 867, а мощность C равна 1463.

Число классов сопряжённых элементов группы J_2 равно двум. Обозначим их буквами A и B. Вычисления, аналогичные проведённым для группы J_1, приводят к неравенствам $J_2 \neq A^2$, $J_2 \neq B^2$, $J_2 \neq AB$ и равенству $J_2 = A^2 \cup B^2 \cup AB$.

Если G — группа, $I \subseteq G$ и множество I содержит только инволюции, то множество элементов группы G называется *строго I-вещественным*, когда каждый его элемент инвертируется сопряжением некоторой инволюцией из I.

Лемма 1. *Пусть G — группа, i — её инволюция, j — не сопряжённая с i в G инволюция, если такая существует. Тогда для группы $G \in \{J_1, J_2, M_{11}, M_{12}\}$ явно указано множество её строго i^G-вещественных и строго j^G-вещественных элементов, а также множество таких элементов группы G, что каждый из них является произведением инволюции из i^G и элемента из j^G. Кроме того, если A и B — множества элементов классов сопряжённых инволюций группы G, то явно указаны подмножества $A_1, A_2 \subset A$ и $B_1, B_2 \subset B$, такие что $A^2 = AA_1$, $B^2 = BB_1$, $AB = AB_2 = A_2B$.*

Доказательство. Опишем алгоритмы, приводящие для каждой группы G с инволюцией i к построению строго i^G-вещественной части группы G.

Наиболее прозрачным является алгоритм прямого перебора инволюций, сопряжённых с элементом i. Его применение ограничено сегодня группами порядков до нескольких миллионов с подстановочными представлениями степеней до 10^4.

Прежде всего необходимо выбрать по возможности наименьшее подстановочное представление группы G. Затем мы строим класс i^G сопряжённых в G с i инволюций и множество его элементов обозначаем буквой C. Пусть L — пустое множество и $k = 0$. Для каждой инволюции i из C принимаем значение параметра m равным 0 и для каждого $j \in C$ рассматриваем произведение ij. Если $ij \in L$, то увеличиваем число m на единицу, иначе пополняем множество L элементом ij. Если ни для одного $j \in C$ множество L пополнить не удалось (т. е. $m = |C|$), то увеличиваем на единицу число k. В результате, рассмотрев уже все элементы i из C, получаем множество CC_1 элементов группы G, представимых произведением двух инволюций из i^G, причём $|C_1| = |i^G| - k$.

Заметим, что по описанному выше алгоритму можно явно указать не только множество L строго i^G-вещественных элементов группы G, но и для каждого элемента из L указать, произведением каких инволюций он является.

Гипотеза. Наименьшее по мощности из подмножеств множества C инволюций группы J_1 множество C_1 со свойством $J_1 = CC_1$ состоит из 867 инволюций.

Пусть теперь в группе G инволюции i и j не сопряжены, а множества сопряжённых с ними в G инволюций обозначены как A и B соответственно. Без ограничения общности рассуждения будем считать, что $|A| \leqslant |B|$. Как и выше, строим множества L_A и L_B строго i^G- и строго j^G-вещественных элементов группы G. Пусть L_{AB} — множество таких (строго вещественных) элементов g группы G, что $g = ab$, $a \in A$, $b \in B$. Алгоритм построения множества L_{AB} отличается от изложенного выше тем, что, фиксируя инволюцию i из меньшего множества A, мы рассматриваем произведения ij, где j пробегает множество B.

Описанные алгоритмы реализованы в системе GAP4r3 (пример для группы Матье M_{12} см. в приложении). Лемма 1 доказана.

Лемма 2. *Множество элементов группы J_2 является кубом любого из её классов сопряжённых инволюций.*

Доказательство. Поскольку для каждой инволюции i группы J_2 построено множество S её строго i^{J_2}-вещественных элементов, то достаточно построить объединение $\bigcup\limits_{i \in i^{J_2}} Si$. Оказалось, что оно совпадает с множеством элементов группы J_2. Лемма 2 доказана.

Теорема 1 доказана.

Теорема 2. *За исключением групп Матье M_{11}, M_{22}, M_{23} и группы Маклафлина* McL, *для каждой конечной простой спорадической группы число 5 — минимум числа таких порождающих её инволюций, что их произведение равно единице, а для указанных четырёх групп это число равно 6.*

Доказательство. Меньше пяти указанное в теореме число быть не может. Действительно, если инволюции i_1, i_2, i_3, i_4 порождают группу G и

$$i_1 i_2 i_3 i_4 = 1, \tag{1}$$

то $G = \text{гр}(i_1, i_2, i_3)$ и $(i_1 i_2)^i = i_2 i_1$ при $i \in \{i_1, i_2, i_3\}$, т. е. циклическая подгруппа $\text{гр}(i_1 i_2)$ нормальна в G, что противоречит простоте группы G. Если число сомножителей в равенстве (1) равно трём, то G — группа диэдра.

Как известно [1], для каждых трёх инволюций, порождающих спорадическую группу, любые две инволюции неперестановочны только в четырёх группах теоремы 2. Поэтому в любой другой спорадической группе G требуемую пятёрку будут составлять инволюции xy, z, z, y, x, где $yx = xy$, $\text{гр}(x, y, z) = G$.

Пусть $G \in \{M_{11}, M_{22}, M_{23}, \text{McL}\}$. Поскольку все инволюции в группе G сопряжены, то, зафиксировав одну из инволюций (обозначим её a) и проверив для каждой тройки инволюций w, x, y группы G с условием $|awxy| = 2$, что $\text{гр}(a, w, x, y) \neq G$, можно доказать теорему. В [4] это сделано для $G \in \{M_{11}, M_{22}, M_{23}\}$.

Чтобы получить такой результат для группы Маклафлина за реальное машинное время (несколько десятков часов), автор изменил алгоритм. Во-первых, осуществлён перебор уже не троек, а всех пар инволюций w, x группы G. Для инволюций w, x найдены все такие пары инволюций $y, z \in G$, что $awxyz = 1$. Поскольку инволюция a выбрана из двуэлементного порождающего группу G множества [7], то остаётся проверить, что в подгруппе $\text{гр}(a, w, x, y)$ нет другого элемента этого множества. Во-вторых, перебор инволюций (в группе McL их 22275) распараллелен на мультипроцессорном компьютере (для группы McL — на 275 сопроцессоров по 81 инволюции).

Приложение

К доказательству леммы 1

Ниже размещена программа для системы компьютерной алгебры GAP4r3, в которой реализован алгоритм из доказательства леммы 1. После программы напечатан текст выводимых ею на экран результатов.

```
G := MathieuGroup(12); b := GeneratorsOfGroup(G)[2]^2;
a := GeneratorsOfGroup(G)[3]; n := Size(G);
Print("|G|=",n,"\n");

d1 := Elements(ConjugacyClass(G,b));
d2 := Elements(ConjugacyClass(G,a));
nc:=Length(d1); cc:=[]; k:=0;
Print("|i^G|=",nc,"\n"); nn := Length(d2);
for i in d1 do m := 0;
  for j in d2 do ij := i * j;
    if ij in cc then m := m + 1; else Add(cc,ij);
      if Length(cc) = n then break; fi;
    fi;
```

```
  od;
  if Length(cc) = n then break; fi;
  if m = nn then k := k + 1; fi;
od;
Print("|c2|=",Position(d1,i)-k);
Print(", |sr|=",Length(cc),", k=",k,"\n");

for d in [a,b] do c := Elements(ConjugacyClass(G,d));
  nc := Length(c); cc := []; k := 0;
  Print("|i^G|=",nc,"\n");
  for i in c do m := 0;
    for j in c do ij := i * j;
      if ij in cc then m := m + 1; else Add(cc,ij);
        if Length(cc) = n then break; fi;
      fi;
    od;
    if Length(cc) = n then break; fi;
    if m = nc then k := k + 1; fi;
  od;
  Print("|c1|=",Position(c,i)-k);
  Print(", |sr|=",Length(cc),", k=",k,"\n");
od;

gap> Read("M12.txt");time;
|G|=95040
|i^G|=495
|c2|=351, |sr|=47520, k=144
|i^G|=396
|c1|=348, |sr|=26896, k=48
|i^G|=495
|c1|=165, |sr|=36180, k=330
747926
```

К доказательству теоремы 1

```
#########################################################
##
#F  InvRep( <group> )
##  Построение списка представителей классов
##  сопряжённых инволюций группы group
##

InvRep := function(g)
  local s0,s1,z,a,m,b,l;
```

```
  if IsInt(Size(g) / 2) then
    z  := SylowSubgroup(g,2);
    s1 := Filtered(Elements(z), u -> u <>() and u^2 = ());
    s0 := [];
    Add(s0,s1[1]);
    a := 1;
    m := Length(s1);
    if m > 1 then
      for z in s1{[2..m]} do
        b := 0;
        for l in [1..a] do
          if z in ConjugacyClass(g,s0[l]) then
            b := b + 1; fi;
        od;
        if b = 0 then Add(s0,z); fi;
        a := Length(s0);
      od;
    fi;
  else
    s0 := [];
  fi;
  return s0;
end;

########################################################
##
#F  Inv( <group> )
##  Построение списка инволюций группы group
##

Inv := function(g)
  local s0,s1,z,m;

  if IsInt(Size(g) / 2) then
    z  := SylowSubgroup(g,2);
    s1 := Filtered(Elements(z), u -> u <>() and u^2=());
    s0 := Elements(ConjugacyClass(g,s1[1]));
    m  := Length(s1);
    if m > 1 then
      for z in s1{[2..m]} do
        if not(z in s0) then
          s0 := Concatenation(s0,
            Elements(ConjugacyClass(g,z)));
```

```
        fi;
      od;
    fi;
  else
    s0 := [];
  fi;
  return s0;
end;

########################################################
##
#F  InvOd( <group> )
##  Построение (упорядоченного) множества инволюций
##  группы group
##

InvOd := function(g)
  local s0,s1,z,m;

  if IsInt(Size(g) / 2) then
    z  := SylowSubgroup(g,2);
    s1 := Filtered(Elements(z), u -> u <>() and u^2=());
    s0 := Elements(ConjugacyClass(g,s1[1]));
    m  := Length(s1);
    if m > 1 then
      for z in s1{[2..m]} do
        if not(z in s0) then
          s0 := Concatenation(s0,
            Elements(ConjugacyClass(g,z)));
        fi;
      od;
    fi;
  else
    s0 := [];
  fi;
  return Set(s0);
end;

######################################################
##
#F  ECentralizer( <group>, <element> )
##  Построение расширенного централизатора элемента
##  element группы group
##
```

```
##BIND_GLOBAL( "ECentralizer", function ( arg )

##  if Length(arg) = 2 then
##    return ExtendedCentralizer( arg[1], arg[2] );
##  fi;
##  Error( "usage: ECentalizer( <Group>,  <element> ");

##end );

##DeclareSynonym( "EC", ECentalizer );

ExtendedCentralizer := function(g, x)
  local n,k,C;

  n := Order(x);
  if n = 1 then
    C := g;
  elif n = 2 then
    C := Centralizer(g,x);
  else
    k := x^-1;
    if IsConjugate(g,x,k) then
      k := RepresentativeAction(g,x,k);
      C := Centralizer(g,x);
      C := ClosureGroup(C,k);
    else
      C := Centralizer(g,x);
    fi;
  fi;
  return C;
end;

#####################################################
##
#F  Invert( <group>, <element> )
##  Построение (упорядоченного) множества таких
##  инволюций группы group, что, сопрягая ими элемент
##  element, получаем ему обратный
##

Invert := function(g, x)
  local n, I;

  n := Order(x);
```

```
  if ( n = 1 ) then
    I := Inv(g);
  elif ( n = 2 ) then
    I := Inv(Centralizer(g,x));
  else
    n := Inv(Centralizer(g,x));
    I := Filtered(Inv(ExtendedCentralizer(g,x)),
      u -> not (u in n) );
  fi;
  return I;
end;
```

Работа выполнена при финансовой поддержке РФФИ (проект № 05-01-00576-а) и КГПУ (проект № 19-04-1/ФП).

Литература

[1] Мазуров В. Д. О порождении спорадических простых групп тремя инволюциями, две из которых перестановочны // Сиб. мат. журн. — 2003. — Т. 44, № 1. — С. 193—198.

[2] Нерешённые вопросы теории групп. Коуровская тетрадь. — Новосибирск: Новосибирский гос. ун-т, 2002.

[3] Рябинина Н. А., Сучков Н. М., Шунков В. П. Об особых подгруппах конечных групп с инволюциями. — Препринт ВЦ СО РАН, № 10. — Красноярск, 1995. — С. 3—11.

[4] Шмидт В. А. О порождающих множествах инволюций знакопеременных и спорадических групп // Материалы XXXIV научной студенческой конференции: сборник статей. — Красноярск: Изд-во Красноярского гос. ун-та, 2001. — С. 139—144.

[5] Шунков В. П. M_p-группы. — М.: Наука, 1990.

[6] Kolesnikov S. G., Nuzhin Ja. N. On strong reality of finite simple groups // Acta Appl. Math. — 2005. — Vol. 85. — P. 195—203.

[7] Wilson R. ATLAS of Group Representations. — http://web.mat.bham.ac.uk/atlas/v2.0.