Math-Net.Ru

Общероссийский математический портал

Л. С. Казарин, В. М. Сидельников, О группе автоморфизмов p -алгебры Судзуки, *Матем. заметки*, 2006, том 80, выпуск 4, 526–535

DOI: <https://doi.org/10.4213/mzm2845>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 3.91.87.62

26 апреля 2023 г., 03:30:05

УДК 512.54

О ГРУППЕ АВТОМОРФИЗМОВ p -АЛГЕБРЫ СУДЗУКИ

Л. С. Казарин, В. М. Сидельников

В работе дается описание группы автоморфизмов p -алгебры Судзуки и некоторых примарных групп, группа автоморфизмов которых имеет небольшое число орбит.

Библиография: 7 названий.

1. Введение. Известно, что группа невырожденных линейных преобразований линейного векторного пространства V действует транзитивно на множестве ненулевых векторов пространства V . Классификация конечных групп, группа автоморфизмов которых действует транзитивно на множестве элементов простого порядка, получена Э. Шультсом и Г. Хигманом. Основные результаты содержатся в монографии Хуперта и Блекберна [1; гл. 8].

Позднее, решая задачу В. Д. Мазурова, Шахрияри и Шахаби описали строение непримарной нормальной подгруппы H конечной группы G , обладающей тем свойством, что множество элементов H разбивается ровно на три орбиты под действием группы G [2]. Эквивалентным образом получено описание непримарной конечной группы H , группа автоморфизмов которой имеет ровно три орбиты на множестве элементов H . Основной результат статьи [2] состоит в том, что группа H в этом случае является либо группой Фробениуса порядка pq^n , где p делит $q^n - 1$, p и q – простые числа, одно из которых равно 2, либо H – не более чем двухступенно разрешимая p -группа. Строение последней осталось в [2] открытым. Цель работы – найти строение некоторых конечных p -групп с указанным свойством и других групп, группа автоморфизмов которых имеет небольшое число орбит на множестве ее элементов. Полученные результаты представляют интерес для построения последовательностей с длинным периодом, близким по своим свойствам к рекуррентным последовательностям над полем. Другие возможные приложения связаны с близостью умножения в рассматриваемых группах со сложением точек в группе точек эллиптической кривой.

Таким образом, представляет интерес описание конечной неабелевой p -группы, группа автоморфизмов которой имеет небольшое число орбит на множестве элементов P . Для краткости, неабелеву группу P , группа автоморфизмов которой имеет не более k орбит на P , будем называть O_k -группой.

Обозначения, не разъясняющиеся в тексте, общеупотребительны и соответствуют имеющимся в [1].

Работа выполнена при поддержке Российского фонда фундаментальных исследований, проект № 05-01-01018.

2. Группы и алгебры Судзуки. Согласно [1; с. 299–300] неабелева 2-группа, отличная от группы кватернионов, обладающая группой автоморфизмов, транзитивной на множестве элементов простого порядка, называется 2-группой Судзуки. Имеется два типа 2-групп Судзуки класса нильпотентности 2. 2-группа P принадлежит *первому типу*, если $|Z(P)| = q = 2^n$ и $|P| = q^3$. Примерами таких групп служат силовские 2-подгруппы простой группы $U_3(q)$.

2-группы Судзуки *второго типа* (с $|P| = q^2$, $|Z(P)| = q$) исчерпываются, согласно [1; теорема 8.7.9] группами $A(n, \Theta)$, определение которых мы сейчас напомним.

Пусть $F = GF(2^n)$, r – число, делящее n , и Θ – автоморфизм поля F порядка r . Тогда множество матриц вида

$$y = \begin{pmatrix} 1 & \alpha & \beta \\ 0 & 1 & \Theta(\alpha) \\ 0 & 0 & 1 \end{pmatrix}, \quad \alpha, \beta \in F,$$

называется 2-группой Судзуки $A(n, \Theta)$. Она изоморфна силовской 2-подгруппе группы ${}^2B_2(2^n)$, если n – нечетное число.

Определим нечетный аналог 2-групп Судзуки $A_p(n, \Theta) = P$ аналогично тому, как это сделано в работах Ханаки и Сагирова [3], [4]. Пусть $F = GF(p^n)$, $n = mk$ и Θ – автоморфизм F порядка k . Элементы группы P – это упорядоченные пары (a, b) элементов поля F с операцией

$$(a, b)(c, d) = (a + c, b + d + a\Theta(c)).$$

Группу $P = A_p(n, \Theta)$ будем называть p -группой Судзуки. Порядок группы P равен q^2 , где $q = p^n$. Отметим, что 2-группа Судзуки $A(n, \Theta) = A_2(n, \Theta)$.

Множество верхнетреугольных матриц вида

$$y = \begin{pmatrix} \lambda & \beta & \alpha \\ 0 & \lambda & \Theta(\beta) \\ 0 & 0 & \lambda \end{pmatrix},$$

где $\alpha, \beta \in GF(q)$, $q = p^n$, $\lambda \in GF(p)$, Θ – автоморфизм поля $F = GF(q)$, отвечающих p -группе Судзуки, является некоммутативной ассоциативной локальной алгеброй вида $A = 1 \cdot GF(p) \oplus R$, где R – нильпотентная алгебра (состоящая из всех матриц указанного вида с нулевой главной диагональю), аналогичной кольцу Галуа, использовавшемуся ранее для построения рекуррентных последовательностей.

Группа $A_p(n, \Theta)$ является *присоединенной* группой алгебры R , умножение любых элементов x и y в которой задается следующим образом: $x \circ y = x \cdot y + x + y$, где $x \cdot y$ – произведение этих элементов в алгебре R . Тот факт, что $A_p(n, \Theta)$ – присоединенная группа алгебры R , записывается в виде $R^\circ = A_p(n, \Theta)$.

Очевидно, что любой автоморфизм p -алгебры Судзуки R является и автоморфизмом группы $A_p(n, \Theta)$.

Группа автоморфизмов 2-группы Судзуки $A(n, \Theta)$ рассматривалась в работе Брюхановой [5]. Мы получим описание группы автоморфизмов p -алгебры Судзуки R , $p > 2$, в явном виде, не используя тонких соображений, понадобившихся для случая $p = 2$.

Определим следующие подгруппы группы автоморфизмов алгебры R (и группы $P = A_p(n, \Theta) = R^\circ$):

- $A_1 = \{\phi \in \text{Aut}(P) \mid (a, b)^\phi = (a, \psi(a) + b)\}$, где $\psi = \psi_\phi$ – линейное преобразование поля $GF(q)$, рассматриваемого как векторное пространство над $GF(p)$;
- $A_2 = \{\phi \in \text{Aut}(P) \mid (a, b)^\phi = (da, d\Theta(d)b)\}$, где $d = d_\phi$ – ненулевой элемент поля $GF(q) = F$;
- $A_3 = \{\phi \in \text{Aut}(P) \mid (a, b)^\phi = (a^{p^r}, b^{p^r})\}$, где $r = r_\phi \leq n - 1$.

Наш основной результат – это следующая

ТЕОРЕМА 1. Пусть R – p -алгебра Судзуки с $P = A_p(n, \Theta) = R^\circ$ и $G = \text{Aut}(R)$. Тогда $G = A_1 \rtimes A_2 \rtimes A_3$, где A_1, A_2, A_3 определены выше. В частности, $|\text{Aut}(R)| = p^{n^2}(p^n - 1)n$.

3. Доказательство теоремы 1. Мы будем использовать запись элементов алгебры R в виде пар (a, b) , где $a, b \in F$. При этом будут использоваться следующие свойства автоморфизма $\phi \in \text{Aut}(R)$:

$$[(a, b)(c, d)]^\phi = (a, b)^\phi(c, d)^\phi, \quad [(a, b) + (c, d)]^\phi = (a, b)^\phi + (c, d)^\phi$$

для любых двух элементов из R .

Здесь и далее знак умножения используется лишь для групповой операции, в то время как ‘+’ обозначает сложение в алгебре R .

Пусть ϕ – произвольный автоморфизм алгебры R , $(a, b) \in R$. Тогда $(a, b)^\phi = (\lambda(a), \mu(a, b))$, где $\lambda = \lambda_\phi$, $\mu = \mu_\phi$ для некоторых функций λ и μ . Для фиксированного ϕ знак ϕ будет опускаться. При этом

$$\begin{aligned} (a, b)^\phi(c, d)^\phi &= (\lambda(a), \mu(a, b))(\lambda(c), \mu(c, d)) \\ &= (\lambda(a) + \lambda(c), \mu(a, b) + \mu(c, d) + \lambda(a)\Theta(\lambda(c))) \\ &= (\lambda(a + c), \mu(a + c, b + d + a\Theta(c))) = ((a, b)(c, d))^\phi. \end{aligned}$$

Отсюда ясно, что $\lambda: F \rightarrow F$ – линейная функция. Положим $a = 0$. Тогда

$$\mu(0, b + d) = \mu(0, b) + \mu(0, d).$$

С другой стороны, $(a, b) = (a, 0)(0, b)$. Так как $(a, b)^\phi = (a, 0)^\phi(0, b)^\phi$, то получаем следующие соотношения:

$$(\lambda(a), \mu(a, b)) = (\lambda(a), \mu(a, 0))(0, \mu(0, b)) = (\lambda(a), \mu(a, 0) + \mu(0, b)).$$

Следовательно,

$$\mu(a, b) = \mu(a, 0) + \mu(0, b).$$

Обозначим функцию $\mu(*, 0) = \psi_1$, а $\mu(0, *) = \psi_2$. Таким образом, $\mu(a, b) = \psi_1(a) + \psi_2(b)$. Имеем

$$\begin{aligned} [(a, b)(c, d)]^\phi &= (\lambda(a), \psi_1(a) + \psi_2(b))(\lambda(c), \psi_1(c) + \psi_2(d)) \\ &= (\lambda(a) + \lambda(c), \psi_1(a) + \psi_1(c) + \psi_2(b) + \psi_2(d) + \lambda(a)\Theta(\lambda(c))) \\ &= (\lambda(a + c), \psi_1(a + c) + \psi_2(b + d + a\Theta(c))). \end{aligned}$$

Поэтому

$$\psi_1(a) + \psi_1(c) + \psi_2(b) + \psi_2(d) + \lambda(a)\Theta(\lambda(c)) = \psi_1(a + c) + \psi_2(b + d + a\Theta(c)).$$

Положив $a = 0$, заключаем, что

$$\psi_1(0) + \psi_1(c) + \psi_2(b) + \psi_2(d) = \psi_1(c) + \psi_2(b + d).$$

Так как $\mu(0, 0) = \psi_1(0) = \psi_2(0) = 0$, то $\psi_2(b + d) = \psi_2(b) + \psi_2(d)$, т.е. ψ_2 – также линейная функция. Так как ϕ является автоморфизмом алгебры, то он сохраняет сумму элементов:

$$\begin{aligned} ((a, b) + (c, d))^\phi &= (a, b)^\phi + (c, d)^\phi = (\lambda(a), \psi_1(a) + \psi_2(b)) + (\lambda(c), \psi_1(c) + \psi_2(d)) \\ &= (\lambda(a + c), \psi_1(a + c) + \psi_2(b + d)) \\ &= (\lambda(a) + \lambda(c), \psi_1(a) + \psi_1(c) + \psi_2(b) + \psi_2(d)). \end{aligned}$$

Отсюда следует линейность и функции ψ_1 . Далее получаем

$$\psi_2(b + d + c\Theta(a)) = \psi_2(b) + \psi_2(d) + \psi_2(c\Theta(a)) = \psi_2(b) + \psi_2(d) + \lambda(c)\Theta(\lambda(a)),$$

так что

$$\lambda(c)\Theta(\lambda(a)) = \psi_2(c\Theta(a)). \quad (1)$$

Заметим, что ψ_1 – произвольная линейная функция из F в F . Поэтому достаточно изучить автоморфизмы ϕ , для которых

$$(a, b)^\phi = (\lambda(a), \psi(b)),$$

где $\psi = \psi_2$, удовлетворяющие соотношению

$$\psi(a\Theta(c)) = \lambda(a)\Theta(\lambda(c)). \quad (2)$$

Положим $c = 1$. Тогда получаем, что $\psi(a) = \lambda(a)\Theta(\lambda(1))$. В этом случае $\psi(1) = \lambda(1)\Theta(\lambda(1))$. Стало быть, $\Theta(\lambda(1)) = \psi(1)/\lambda(1)$. Отсюда

$$\psi(a) = \lambda(a) \frac{\psi(1)}{\lambda(1)} = d_\lambda \lambda(a).$$

Таким образом, имеем

$$(a, b)^\phi = (\lambda(a), d_\lambda \lambda(b)).$$

Возвращаясь к соотношению (1), получаем

$$\lambda(a)\Theta(\lambda(c)) = d_\lambda \lambda(ca\Theta(c)). \quad (3)$$

Положив $c = a = 1$, получим $\lambda(1)\Theta(\lambda(1)) = d_\lambda \lambda(\Theta(1))$, т.е. $d_\lambda = \Theta(\lambda(1))$, ибо $\lambda(\Theta(1)) = \lambda(1)$. Положив в (3) $a = 1$, получим равенство

$$\Theta(\lambda(1))\lambda(\Theta(c)) = \lambda(1)\Theta(\lambda(ac)),$$

которое можно переписать в виде

$$\Theta(\lambda(b)) = \frac{\Theta(\lambda(1))}{\lambda(1)} \lambda(\Theta(b)). \quad (4)$$

Указанное равенство справедливо для любого $b \in F$ и любого λ , участвующего в определении автоморфизма ϕ .

Пусть функция $\nu = \lambda/\lambda(1)$. Тогда существует автоморфизм $\sigma = \sigma(\nu)$, определенный равенством

$$(a, b)^\sigma = (\nu(a), d_\nu \nu(b)).$$

По предыдущему

$$d_\nu = \Theta(\nu(1)) = \Theta\left(\frac{\lambda(1)}{\lambda(1)}\right) = 1.$$

Поэтому $(a, b)^\sigma = (\nu(a), \nu(b))$. Из формулы (4) получаем, что

$$\Theta(\nu(b)) = \frac{\Theta(1)}{\nu(1)} \nu(\Theta(b)) = \nu(\Theta(b))$$

для любого $b \in F$. При этом $\nu(a)\Theta(\nu(c)) = \nu(a\Theta(c))$. Так как Θ – автоморфизм F , то любой элемент $b \in F$ может быть записан в виде $b = \theta(u)$ для подходящего $u \in F$. Поэтому соотношение

$$\nu(a)\Theta(\nu(c)) = \nu(a\Theta(c)) = \nu(a)\nu(\Theta(c))$$

равносильно тождеству $\nu(bc) = \nu(b)\nu(c)$ для любых $b, c \in F$. Следовательно,

$$\nu(b + c) = \nu(b) + \nu(c), \quad \nu(bc) = \nu(b)\nu(c),$$

откуда ν – автоморфизм поля F . Таким образом, $\nu(a) = a^{p^s}$ для подходящего натурального числа s .

Подведя итог сказанному, мы получили, что любой автоморфизм ϕ алгебры R действует на элементах R следующим образом:

$$(a, b)^\phi = (\lambda(a), \psi_1(a) + \psi_2(b)),$$

где λ , ψ_1 и ψ_2 – линейные (над $GF(p)$) функции. При этом множество автоморфизмов A_1 , состоящее из всех автоморфизмов, для которых $\lambda_\phi = 1 = \psi_2 = \text{id}$, является нормальной подгруппой группы $G = \text{Aut}(R)$. Число всех таких автоморфизмов равно числу всех $GF(p)$ -линейных отображений из F в F , т.е. p^{n^2} . Автоморфизмы ϕ , для которых $\lambda_\phi = d$, где d – произвольный элемент поля $F = GF(p^n)$, отличный от нуля, а $\psi_1 = 0$, также образуют подгруппу группы G . При этом $\psi_2 = d\Theta(d)$ определен однозначно по d . Количество таких автоморфизмов, разумеется, равно $|F^*| = p^n - 1$. При этом $A_1 \cap A_2$ состоит из тождественного автоморфизма, а произведение $A_1 A_2$, как легко убедиться, является нормальной подгруппой G . Наконец, если $\lambda(1) = 1$, $\psi_1 = 0$, то полученный автоморфизм, как показывают приведенные выше рассуждения, есть автоморфизм поля $GF(p^n)$. Таким образом, любой автоморфизм $\phi \in G$ может быть записан в виде

$$\phi = \phi_1 \phi_2 \phi_3, \quad \text{где } \phi_1 \in A_1, \quad \phi_2 \in A_2, \quad \phi_3 \in A_3.$$

Легко проверить оставшиеся свойства. Теорема доказана.

4. Группы автоморфизмов с малым числом орбит. Следующая лемма дает необходимое условие существования O_3 -группы. В силу характеристичности центра группы в нашем случае можно рассматривать лишь двухступенно нильпотентные группы.

ЛЕММА 1. Пусть P – конечная p -группа, являющаяся O_3 -группой,

$$|P| = p^{\alpha+\beta}, \quad \text{где} \quad |Z(P)| = p^\alpha.$$

Тогда P – специальная p -группа (т.е. центр, коммутант и подгруппа Фраттини группы P совпадают и являются элементарными абелевыми p -группами), степень любого неприводимого нелинейного характера группы P равна p^λ , $\lambda > 0$, и выполнено одно из следующих утверждений:

- (i) $\beta = \alpha + \mu = 2\lambda$;
- (ii) $\alpha = \beta = \mu + 2\lambda$.

ДОКАЗАТЕЛЬСТВО. Утверждение о специальности группы P следует из определения O_3 -группы. Пусть $k = k(P)$ – число классов сопряженных элементов группы P . Так как все нецентральные элементы P сопряжены под действием $\text{Aut}(P)$, то размер любого класса сопряженных элементов с представителем $y \in P \setminus Z(P)$ равен

$$h = p^{\beta-\mu}, \quad \text{где} \quad |C_P(y)| = p^{\alpha+\mu}.$$

Поэтому $k = p^\alpha + r$, где r – число классов нецентральных элементов группы P . Так как $|P| = p^\alpha + rp^{\beta-\mu} = p^{\alpha+\beta}$, то

$$r = \frac{p^{\alpha+\beta} - p^\alpha}{p^{\beta-\mu}} = p^{\alpha+\mu} - p^{\alpha+\mu-\beta}.$$

В частности, $\alpha + \mu \geq \beta$. Пусть χ – неприводимый нелинейный характер группы P , так что его степень $\chi(1) = p^\lambda$, где $\lambda > 0$. Так как характер χ^ϕ , определенный на элементах группы P соотношением $\chi^\phi(g) = \chi(g^{\phi^{-1}})$ для любого автоморфизма ϕ группы P , является неприводимым, то из теоремы Брауэра [6; (12.1)] следует сопряженность всех неприводимых нелинейных характеров группы P (число орбит группы $G = \text{Aut}(P)$ на множестве неприводимых характеров группы P то же, что и на множестве элементов группы P). Число линейных характеров, как хорошо известно, равно $|P : P'| = |P : Z(P)| = p^\beta$. Поэтому из равенства

$$\sum_{\chi \in \text{Irr}(P)} \chi(1)^2 = |P|$$

следует, что

$$|P| = p^{\alpha+\beta} = p^\beta + (k(P) - p^\beta)p^{2\lambda} = p^\beta - (p^\alpha + (p^{\alpha+\mu} - p^{\alpha+\mu-\beta}) - p^\beta)p^{2\lambda}.$$

Таким образом, имеем следующее равенство:

$$p^{\alpha+\beta} + p^{\alpha+\mu-\beta+2\lambda} + p^{\beta+2\lambda} = p^\beta + p^{\alpha+2\lambda} + p^{\alpha+\mu+2\lambda}.$$

Нетрудно проверить существование следующих решений:

- (i) $\alpha + \mu = \beta = 2\lambda$,
- (ii) $\alpha = \beta = \mu + 2\lambda$.

Покажем, что другие решения исключены. Действительно, если все числа $\alpha + \beta$, $\alpha + \mu - \beta + 2\lambda$, $\beta + 2\lambda$ различны, то слева и справа – выражения, представляющие p -ичную запись одного и того же числа. Поэтому из неравенств $\alpha + \beta > \beta$ и $\beta + 2\lambda > \beta$ следует, что $\alpha + \mu - \beta + 2\lambda = \beta$. В этом случае имеем

$$p^{\alpha+\beta} + p^{\beta+2\lambda} = p^{\alpha+2\lambda} + p^{\alpha+\mu+2\lambda}.$$

Если $\alpha \leq 2\lambda$, то $\alpha + \beta = \alpha + 2\lambda$ и $\beta = 2\lambda$, а тогда $\alpha + \mu = \beta = 2\lambda$, т.е. имеем решение (i).

Если $\alpha > 2\lambda$, то $\alpha + \beta = \alpha + \mu + 2\lambda$ и $\beta = \mu + 2\lambda$. Но тогда $\alpha = \beta = \mu + 2\lambda$, т.е. получаем соотношения (ii).

Предположим теперь, что $\alpha + \beta = \beta + 2\lambda$, т.е. $\alpha = 2\lambda$. Тогда либо $\beta = \alpha + 2\lambda$, либо $\beta = \alpha + \mu + 2\lambda$. Поэтому либо $\beta = 2\alpha$, либо $\beta = 2\alpha + \mu$. В первом случае

$$2p^{3\alpha} + p^\mu = p^{2\alpha} + p^{2\alpha} + p^{2\alpha+\mu},$$

что очевидно неверно. Во втором – $\beta = 2\alpha + \mu$ противоречит соотношению $\alpha + \mu \geq \beta$.

Допустим, что $\alpha + \beta = \alpha + \mu - \beta + 2\lambda$. Тогда $2\beta = \mu + 2\lambda$ и

$$2p^{\alpha+\beta} + p^{\beta+2\lambda} = p^\beta + p^{\alpha+2\lambda} + p^{\alpha+\beta}.$$

Так как оба слагаемых в левой части делятся на $p^{\beta+1}$, получаем противоречие.

Теперь можно считать, что $\alpha + \mu - \beta + 2\lambda = \beta + 2\lambda$. Отсюда $\alpha + \mu = 2\beta$ и

$$p^{\alpha+\beta} + 2p^{\beta+2\lambda} = p^\beta + p^{\alpha+2\lambda} + p^{2\beta+2\lambda}.$$

В этом случае $\alpha + 2\lambda \geq \beta$. Учитывая, что $\lambda > 0$, получим $\alpha + 2\lambda = 2\beta + 2\lambda$ и $\beta = 2\lambda$, $\alpha = 2\lambda$, т.е.

$$p^{4\lambda} + 2p^{4\lambda} = p^{2\lambda} + 2p^{4\lambda},$$

что приводит к противоречию. Итак, параметры α , β , λ , μ связаны соотношениями (i) или (ii). Лемма доказана.

Отметим, что O_3 -группы, являющиеся 2-группами, допускают почти исчерпывающее описание.

ТЕОРЕМА 2. Пусть P – конечная 2-группа, являющаяся O_3 -группой. Тогда P – специальная 2-группа, на множестве инволюций которой группа $G = \text{Aut}(P)$ действует транзитивно. При этом верно одно из следующих утверждений:

- (i) $|P| = q^3$, где $q = 2^n = |Z(P)| = |P'|$, причем $|C_P(y)| = q^2$ для любого $y \in P \setminus Z(P)$ и степень любого неприводимого характера группы P равна q ;
- (ii) $|P| = q^2$, где $q = 2^n = |Z(P)|$.

ДОКАЗАТЕЛЬСТВО. Пусть P – неабелева 2-группа, группа автоморфизмов G которой имеет три орбиты на P . Если P содержит единственную инволюцию, то по лемме 1 P – группа кватернионов порядка 8, так что выполнено заключение (i), ибо G , разумеется, транзитивна на $P \setminus Z(P)$. Если P имеет нецентральную инволюцию, то все элементы группы P удовлетворяют тождеству $x^2 = 1$ и P – абелева группа. Поэтому все инволюции P лежат в $Z(P)$ и группа G транзитивна на множестве элементов простого порядка из P . При этом P – неабелева группа. По теореме 8.5.5 (d) [1] имеем $|P| = q^2$ или $|P| = q^3$, где $q = 2^n = |Z(P)|$. Если $|P| = q^3$, то из леммы 1 следует, что степень любого нелинейного характера группы P равна q . Теорема доказана.

Теорема 2 дает необходимое условие существования O_3 -групп. Поэтому другая формулировка теоремы 2 такова: конечная O_3 -группа, являющаяся 2-группой, является группой Судзуки или группой кватернионов порядка 8.

Имеется два типа 2-групп Судзуки. Примером групп, принадлежащих первому типу, является силовская 2-подгруппа группы $U_3(q)$, где q четно.

ТЕОРЕМА 3. Пусть P – силовская 2-подгруппа группы $U_3(q)$, где q четно. Тогда P является O_3 -группой.

ДОКАЗАТЕЛЬСТВО. В подходящем базисе элементы группы P записываются матрицами вида

$$y = \begin{pmatrix} 1 & \beta & \alpha \\ 0 & 1 & \widehat{\beta} \\ 0 & 0 & 1 \end{pmatrix},$$

где $\alpha, \beta \in GF(q^2)$ и связаны соотношением $\alpha + \widehat{\alpha} + \beta\widehat{\beta} = 0$. Здесь $\widehat{x} = x^q$, а отображение $x \rightarrow x^q$ есть автоморфизм поля $GF(q^2)$ порядка 2. Непосредственные вычисления в группе $U_3(q)$ показывают, что центр группы P состоит из матриц вида

$$z = \begin{pmatrix} 1 & 0 & \alpha \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

где $\alpha + \widehat{\alpha} = 0$. Таким образом, $|Z(P)| = q$. Центризатор элемента $y \in P \setminus Z(P)$ в обозначениях, введенных выше, состоит из матриц вида

$$z = \begin{pmatrix} 1 & \lambda\beta & \gamma \\ 0 & 1 & \lambda\widehat{\beta} \\ 0 & 0 & 1 \end{pmatrix},$$

где $\lambda \in GF(q) \subset GF(q^2)$ и $\lambda^2\beta\widehat{\beta} + \gamma + \widehat{\gamma} = 0$. Отсюда легко следует, что $C_P(y)$ – абелева группа порядка q^2 , являющаяся гомоциклической группой экспоненты 4 и ранга $n = \log_2 q$. Диагональная группа матриц, состоящая из элементов вида

$$d(\lambda) = \begin{pmatrix} \lambda & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \widehat{\lambda} \end{pmatrix},$$

индуцирует циклическую группу автоморфизмов группы P порядка $q^2 - 1$. При этом

$$y^{d(\lambda)} = \begin{pmatrix} 1 & \lambda\beta & \lambda^{q+1}\alpha \\ 0 & 1 & \widehat{\lambda}\widehat{\beta} \\ 0 & 0 & 1 \end{pmatrix}.$$

Нетрудно видеть, что если λ – примитивный элемент поля $GF(q^2)$, то $y^{d(\lambda)^i} = y$ только при $i \equiv 0 \pmod{q^2 - 1}$. Учитывая, что $|C_P(y)| = q^2$, получаем, что в группе $H = P\langle d(\lambda) \rangle$ все нецентральные элементы сопряжены. Так как $D = \langle d(\lambda) \rangle$ при указанном выборе λ транзитивна на множестве инволюций группы P , получаем, что P является O_3 -группой. Теорема доказана.

Отметим, что силовская 2-подгруппа группы $L_3(q)$ для четного q уже не является O_3 -группой.

ТЕОРЕМА 4. Группа $A(n, \Theta)$ является O_3 -группой, если Θ – нетривиальный автоморфизм нечетного порядка поля F .

ДОКАЗАТЕЛЬСТВО. Пусть порядок автоморфизма Θ равен k , где k – нечетное число. Тогда $n = mk$. По теореме 3.1 из [4] множество степеней неприводимых характеров группы P состоит из чисел 1 и 2^{n-m} . По лемме 2.5 [4] группа P имеет автоморфизм ϕ_λ порядка $2^n - 1$, действующий на P без неподвижных точек, причем длина любой нетривиальной $\Phi_\lambda = \langle \phi_\lambda \rangle$ -орбиты на P равна $2^n - 1$. Кроме того, $P' = Z(P)$ и P – специальная 2-группа. Покажем, что элементы (a, b) и (a, c) группы P сопряжены при помощи некоторого автоморфизма группы P .

Если $a = 0$, то эти элементы сопряжены, ибо подгруппа Φ_λ транзитивна на $Z(P) = \{(0, b) \mid b \in F\}$.

Если $a \neq 0$, то определим автоморфизм ψ группы P следующим образом:

$$(a, b)^\psi = (a, \sigma(a) + b),$$

где σ – линейный оператор над $GF(2)$, действующий на F как на векторном пространстве размерности n . Нетрудно видеть, что так определенное отображение $\psi = \psi(\sigma)$ будет автоморфизмом P при любом выборе линейного оператора σ . В частности, при $\sigma(a) = c - b$ получим, что $(a, b)^\psi = (a, c)$. Но тогда каждый элемент из $P \setminus Z(P)$ имеет $2^n(2^n - 1)$ сопряженных под действием $\text{Aut}(P)$. Учитывая транзитивность $\text{Aut}(P)$ на инволюциях из P и на $P/Z(P)$, получаем заключение теоремы.

Существуют p -группы ($p > 2$), являющиеся O_3 -группами.

ТЕОРЕМА 5. *Экстраспециальная p -группа P порядка p^{2n+1} экспоненты $p > 2$ является O_3 -группой.*

ДОКАЗАТЕЛЬСТВО хорошо известно (фольклор) и потому опускается.

Отметим, что для экстраспециальной p -группы порядка p^{2n+1} степень любого нелинейного неприводимого характера равна p^n , так что в этом случае группа P – типа (i) по классификации леммы 1.

Покажем, что существуют O_4 -группы типа (ii), являющиеся p -группами при $p > 2$.

ТЕОРЕМА 6. *Группа $A_p(n, \Theta)$ является O_4 -группой, если n нечетно.*

ДОКАЗАТЕЛЬСТВО. Группа $S = \langle \sigma_\lambda \rangle$, где λ – примитивный элемент поля F , имеет две орбиты на $Z(P) \setminus \{1\}$ и действует без неподвижных точек на $P/Z(P)$. Пусть $z = (0, c) \in Z(P)$. Покажем, что существует автоморфизм ψ , переводящий элемент $(a, b) \in P \setminus Z(P)$ в элемент $(a, b+c)$. Пусть μ – линейный оператор на F , переводящий элемент a в c . Определим автоморфизм $\psi = \psi(\mu) \in \text{Aut}(P)$ следующим образом: $(a, b)^\psi = (a, \mu(a) + b)$. Тогда для $(a', b') \in P$ имеем $(a', b')^\psi = (a', \mu(a') + b')$. Поэтому

$$\begin{aligned} ((a, b)(a', b'))^\psi &= (a + a', b + b' + a\Theta(a'))^\psi = (a + a', \mu(a + a') + b + b' + a\Theta(a')) \\ &= (a + a', \mu(a) + \mu(a') + b + b' + a\Theta(a')). \end{aligned}$$

С другой стороны,

$$(a, b)^\psi (a', b')^\psi = (a, \mu(a) + b)(a', \mu(a') + b') = (a + a', \mu(a + a') + b + b' + a\Theta(a')).$$

Поэтому $\psi = \psi(\mu)$ – гомоморфизм. Легко убедиться, что его ядро тривиально.

Так как $\mu: F \rightarrow F$ – произвольный линейный оператор над $GF(p)$, то его можно выбрать так, что $\mu(a) = c$, а тогда $(a, b)^\psi = (a, b + c)$. Таким образом, для любых $g \in P \setminus Z(P)$, $z \in P$ существует такой автоморфизм $\psi \in \text{Aut}(P)$, что $g^\psi = gz$. Отсюда следует, что число орбит $\text{Aut}(P)$ на P не превосходит 4. Теорема доказана.

5. Нильпотентные алгебры и их присоединенные группы класса два.

Пусть P – конечная специальная p -группа экспоненты p и класса нильпотентности 2. Следующая конструкция принадлежит Калужнину [7]. Отображение $x \rightarrow x^2$ в группе P является взаимнооднозначным отображением и потому операция извлечения корня квадратного из элементов группы P также определена однозначно. Определим кольцевые операции $+$ и $\cdot$ на P следующим образом:

$$x \cdot y = xyx^{-1}y^{-1} = [x^{-1}, y^{-1}], \quad x + y = xy\sqrt{y \cdot x}.$$

По теореме 1.6.7 из [7] относительно операций $+$, $\cdot$ группа P является нильпотентной алгеброй класса нильпотентности 2 над полем $GF(p)$. Верно и обратное: всякая некоммутативная нильпотентная алгебра R над $GF(p)$, удовлетворяющая соотношению $R^3 = 0$, т.е. класса нильпотентности 2, имеет двухступенно нильпотентную присоединенную группу (т.е. группу с умножением $x \circ y = x + y + x \cdot y$), изоморфную группе экспоненты p . Нетрудно показать, что всякий автоморфизм построенной алгебры является также автоморфизмом присоединенной группы и наоборот. Удивительным образом конструкция Калужнина не дает возможности утверждать, что группа автоморфизмов алгебры R с $R^\circ = A_p(n, \Theta)$ совпадает с группой автоморфизмов группы $R^\circ = A_p(n, \Theta)$. Авторы уверены, что это так, но в настоящий момент не располагают доказательством.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

- [1] B. Huppert, N. Blackburn, *Finite Groups II*, Springer-Verlag, New York, 1982.
- [2] M. Shahryariv, M. A. Shahabi, “Subgroups which are the union of three conjugate classes”, *J. Algebra*, **207** (1998), 326–332.
- [3] A. Hanaki, “A condition on lengths of conjugacy classes and character degrees”, *Osaka J. Math.*, **33** (1996), 207–216.
- [4] И. А. Сагиров, “Степени неприводимых характеров 2-групп Судзуки”, *Матем. заметки*, **66:2** (1999), 258–263.
- [5] Е. Г. Брюханова, “О группах автоморфизмов 2-автоморфных 2-групп”, *Алгебра и логика*, **20:1** (1981), 5–21.
- [6] W. Feit, *Characters of Finite Groups*, W. A. Benjamin Inc., New York, 1967.
- [7] R. L. Kruse, D. T. Price, *Nilpotent Rings*, Gordon & Breach, New York, 1969.

Л. С. Казарин

Ярославский государственный университет им. П. Г. Демидова
E-mail: kazarin@uniyar.ae.ru

Поступило

26.12.2005

В. М. Сидельников

Московский государственный университет
им. М. В. Ломоносова
E-mail: sid@sid.mccme.ru