L. S. Kazarin, V. M. Sidel'nikov, An automorphism group of Suzuki p-group,
Tr. Diskr. Mat., 2007, Volume 10, 87–96

Труды по дискретной математике
Том 10, с. 87–96
М.: ФИЗМАТЛИТ, 2007

ГРУППА АВТОМОРФИЗМОВ p-ГРУППЫ СУДЗУКИ

Л. С. КАЗАРИН, В. М. СИДЕЛЬНИКОВ

В работе, являющейся продолжением исследований авторов, дается описание группы автоморфизмов p-группы Судзуки $A_p(n, \Theta)$. Это описание будет полезно в предполагаемых приложениях указанных групп, например при описании связанных с ними ассоциативных схем и рекуррентных последовательностей.

§ 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. Шультом и Г. Хигманом. Основные результаты содержатся в монографии Б. Хупперта и Н. Блекберна [1, гл. VIII].

Неабелевы 2-группы, имеющие более одной инволюции, группа автоморфизмов которых транзитивна на множестве инволюций, называются 2-группами Судзуки. Разрешимость группы автоморфизмов 2-группы Судзуки доказана Е. Брюхановой в [5]. В этом случае строение группы хорошо известно. Имеется два типа таких групп класса нильпотентности два, одна из которых напоминает силовскую 2-подгруппу группы $U_3(q)$, q — степень двойки, а вторая — силовскую 2-подгруппу простой группы Судзуки. Ханаки и Сагиров (см. [3, 4]) исследовали обобщения 2-групп Судзуки $A(n, \Theta)$, названные нами p-группами Судзуки $A_p(n, \Theta)$ (см. [7]), определение которых мы сейчас напомним.

Пусть $F = \mathbf{GF}(p^n)$, m — число, делящее n, и Θ — автоморфизм поля F порядка $m > 1$. 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 p-группой Судзуки $P = A_p(n, \Theta)$.

Можно дать более простое определение. Пусть $F = \mathbf{GF}(p^n)$, $n = mk$ и Θ — автоморфизм F порядка $m > 1$. Элементы группы P — это упорядоченные пары (a, b) элементов поля F с операцией

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

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

Определим следующие подгруппы группы автоморфизмов группы $P = A_p(n, \Theta)$:

$A_1 = \{\varphi \in \mathrm{Aut}(P) \mid (a, b)^\varphi = (a, \mu(a) + b)\}$, где $\mu = \mu_\varphi$ — линейное преобразование поля $\mathbf{GF}(q)$, рассматриваемого как векторное пространство над $\mathbf{GF}(p)$;

$A_2 = \{\varphi \in \mathrm{Aut}(P) \mid (a, b)^\varphi = (ea, e\Theta(e)b)\}$, где $e = e_\varphi$ — ненулевой элемент поля $\mathbf{GF}(q) = F$;

$A_3 = \{\varphi \in \mathrm{Aut}(P) \mid (a, b)^\varphi = (a^{p^l}, b^{p^l})\}$, где $l = l_\varphi \leqslant n - 1$.

Сформулируем наш основной результат.

Теорема 1. *Пусть P — p-группа Судзуки ($P = A_p(n, \Theta)$) и $G = \mathrm{Aut}(P)$, причем порядок Θ — нечетное число m, делящее n и взаимно простое с p. Тогда $G = (A_1 \rtimes A_2) \rtimes A_3$, где A_1, A_2, A_3 определены выше. В частности, $|\mathrm{Aut}(R)| = p^{n^2}(p^n - 1)n$.*

§ 2. ВСПОМОГАТЕЛЬНЫЕ РЕЗУЛЬТАТЫ

Зафиксируем введенные в теореме 1 обозначения до конца статьи. Автоморфизм Θ везде нечетного порядка.

С группой P связана нильпотентная алгебра R над $\mathbf{GF}(p)$, элементы которой также будут записываться в виде упорядоченных пар (a, b), где $a, b \in F = \mathbf{GF}(q)$ и характеристика поля F равна p. Таким образом, P и R совпадают как множества, но операции в R задаются следующим образом:

$$(a, b) + (c, d) = (a + c, b + d); \quad (a, b) * (c, d) = (0, a\Theta(c)).$$

При этом групповая операция на P связана с кольцевыми следующим образом:

$$(a, b)(c, d) = (a, b) * (c, d) + (a, b) + (c, d).$$

Группа P является присоединенной группой R° алгебры R. Легко проверить, что любой автоморфизм алгебры R индуцирует автоморфизм присоединенной группы. Вообще говоря, $H = \mathrm{Aut}(R) \leqslant \mathrm{Aut}(P) = G$. Однако группы A_i ($i = 1, 2, 3$) являются группами автоморфизмов и алгебры R.

Поэтому из теоремы следует совпадение группы автоморфизмов алгебры R и группы P, являющейся присоединенной группой алгебры R.

Лемма 1. *Пусть F — поле характеристики p и Θ — его нетривиальный автоморфизм порядка, взаимно простого с p. Тогда $F = K \oplus L$, где $L = (1 - \Theta)F$, $K = C_F(\Theta)$. В частности, Θ действует на L без неподвижных точек.*

Доказательство. Следует из теоремы 5.2.3 в [2]. Заметим, что, согласно принятой в теории групп терминологии, автоморфизм называется действующим без неподвижных точек, если он оставляет на месте только нейтральный элемент группы (см. [2, с. 333]).

Лемма 2. *Пусть φ — произвольный автоморфизм группы P. Тогда существуют такие отображения $\lambda = \lambda_\varphi$, $\mu = \mu_\varphi$, $\psi = \psi_\varphi$ из F в F, что $(a, b)^\varphi = (\lambda(a), \mu(a) + \psi(b))$, причем λ и ψ — $\mathbf{GF}(p)$-линейные и невырожденные, $\mu(0) = 0$ и для любых $a, c \in F$ выполнено $\mu(a + c) = \mu(a) + \mu(c) + \lambda(a)\Theta(\lambda(c)) - \psi(a\Theta(c))$.*

Доказательство. Пусть φ — произвольный автоморфизм группы P, $(a, b) \in P$. Отметим, что центр $Z(P)$ группы P состоит из элементов вида $(0, b)$, где $b \in F$, а элементы группы $P/Z(P)$ параметризуются первой координатой элементов $(a, b) \in P$. Тогда $(a, b)^\varphi = (\lambda(a), \sigma(a, b))$, где $\lambda = \lambda_\varphi$, $\sigma = \sigma_\varphi$ для некоторых отображений $\lambda\colon F \to F$ и $\sigma\colon F \times F \to F$. Для фиксированного φ индекс φ в обозначениях ассоциированных с ним отображений будет опускаться. При этом

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

Отсюда ясно, что $\lambda\colon F \to F$ — $\mathbf{GF}(p)$-линейная функция. Положим $a = 0$. Тогда

$$\sigma(0, b + d) = \sigma(0, b) + \sigma(0, d). \qquad (*)$$

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

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

Следовательно,

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

Пусть $\sigma(\cdot, 0) = \mu$, а $\sigma(0, \cdot) = \psi$. Таким образом, $\sigma(a, b) = \mu(a) + \psi(b)$, причем ψ $\mathbf{GF}(p)$-линейна (см. $(*)$). Имеем

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

Поэтому

$$\mu(a)+\mu(c)+\psi(b)+\psi(d)+\lambda(a)\Theta(\lambda(c))=\mu(a+c)+\psi(b+d+a\Theta(c)).$$

В силу линейности ψ имеем

$$\mu(a+c)=\mu(a)+\mu(c)+\lambda(a)\Theta(\lambda(c))-\psi(a\Theta(c)).$$

Положив $a=0=c$ и воспользовавшись линейностью ψ и λ, заключаем, что $\mu(0)=0$.

Наконец, невырожденность λ и ψ следует из существования обратного к φ отображения. Для λ это очевидно, а биективность ψ следует из биективности ограничения φ на $Z(P)$.

Отсюда следует заключение леммы.

Лемма 3. *Пусть φ — автоморфизм группы P и λ,μ,ψ — ассоциированные с ним функции. Тогда выполнены следующие утверждения:*

i) $\lambda(a)\Theta(\lambda(c))-\lambda(c)\Theta(\lambda(a))=\psi(a\Theta(c)-c\Theta(a))$;

ii) *μ является $\mathbf{GF}(p)$-линейной тогда и только тогда, когда φ является автоморфизмом алгебры R;*

iii) *множество автоморфизмов группы P, индуцирующих тождественный автоморфизм на $P/Z(P)$, совпадает с $A_1\leqslant \mathrm{Aut}(R)$.*

Доказательство. (i) следует из леммы 2.

(ii) Заметим, что автоморфизм φ группы P является автоморфизмом алгебры R тогда и только тогда, когда он сохраняет сумму и произведение элементов:

$$((a,b)+(c,d))^{\varphi}=(a,b)^{\varphi}+(c,d)^{\varphi}=(\lambda(a),\mu(a)+\psi(b))+(\lambda(c),\mu(c)+\psi(d))=$$
$$=(\lambda(a+c),\mu(a+c)+\psi(b+d))=(\lambda(a)+\lambda(c),\mu(a)+\mu(c)+\psi(b)+\psi(d)).$$

Отсюда следует линейность функции μ. Далее получаем

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

так что

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

Поэтому для кольцевого умножения имеем

$$((a,b)*(c,d))^{\varphi}=(0,a\Theta(c))^{\varphi}=(0,\psi(a\Theta(c)))=(0,\lambda(a)\Theta(\lambda(c)))=$$
$$=(\lambda(a),\mu(a)+\psi(b))*(\lambda(c),\mu(c)+\psi(d))=(a,b)^{\varphi}*(c,d)^{\varphi}.$$

Отсюда следует (ii).

(iii) Пусть $\varphi\in\mathrm{Aut}(P)$ индуцирует тождественный автоморфизм на $P/Z(P)$. Из свойств групп $A_p(n,\Theta)$ и нечетности порядка Θ (см. [4]) следует, что $Z(P)=[P,P]=\Phi(P)$. По лемме о трех подгруппах $[P,\langle\varphi\rangle,P]=$

$= [\langle\varphi\rangle, P, P] = 1$ влечет $[Z(P), \langle\varphi\rangle] = [P, P, \langle\varphi\rangle] = 1$. Поэтому для любого элемента $(a, b) \in P$ имеем: $(a, b)^\varphi = (a, 0)^\varphi (0, b)^\varphi = (a, \mu(a))(0, b) = (a, \mu(a) + b)$. Из леммы 2 и (ii) следует, что $\varphi \in A_1 \leqslant \mathrm{Aut}(R)$. Лемма доказана.

Лемма 4. *Пусть G_1 — множество всех таких автоморфизмов φ группы P, что им ассоциированные функции λ_φ обладают свойством $\lambda(1) = 1$. Тогда G_1 — подгруппа G. При этом $G = A_2 G_1$.*

Доказательство. Предположим, что φ_1 и φ_2 таковы, что ассоциированные им функции λ_1 и λ_2 обладают свойством $\lambda_1(1) = \lambda_2(1) = 1$. Тогда для автоморфизма $\varphi_1\varphi_2 = \varphi_3$, имеющего ассоциированную функцию λ_3, и элемента $(1, b) \in P$ имеем: $(1, b)^{\varphi_1\varphi_2} = (\lambda_2(\lambda_1(1)), v) = (1, v)$ для некоторого $v \in F$. Легко видеть, что $\lambda_3 = \lambda_2\lambda_1$ и потому $\varphi_3 \in G_1$.

Пусть теперь φ — произвольный автоморфизм группы P и $\lambda(1) = u$ для некоторого $u \in F$. По лемме 2 элемент u отличен от нуля. Поэтому существует такой элемент $y \in F$, что $yu = 1$. Рассмотрим такой автоморфизм $\varphi_1 \in A_2$, что $(a, b)^{\varphi_1} = (ya, y\Theta(y)b)$. Очевидно, что $\varphi\varphi_1 = \varphi'$ переводит $(1, b) \in P$ в элемент $(1, b')$ для подходящего $b' \in F$. Поэтому любой элемент из $G = \mathrm{Aut}(P)$ представляется в виде произведения элементов из G_1 и из A_2, т. е. $G = G_1 A_2 = A_2 G_1$. Лемма доказана.

Лемма 5. *Пусть Θ — нетривиальный автоморфизм нечетного порядка поля $F = \mathbf{GF}(p^n)$. Тогда множество элементов вида $a\Theta(b) - b\Theta(a)$ порождает поле F, рассматриваемое как векторное пространство над $\mathbf{GF}(p)$.*

Доказательство. В [4] имеется доказательство утверждения $[P, P] = Z(P)$, равносильного заключению леммы.

Дадим более короткое доказательство. Рассмотрим выражение $a\Theta(b) - b\Theta(a)$ при $b = ac$. Тогда его можно переписать в виде $a\Theta(a)\Theta(c) - ac\Theta(a) = a\Theta(a)(\Theta(c) - c)$. Выберем такой элемент c поля F, что $d = \Theta(c) - c \neq 0$. Нам достаточно доказать, что элементы вида $a\Theta(a)$ порождают F как векторное пространство над $\mathbf{GF}(p)$.

В самом деле, множество элементов из F вида fd, где $f \in F$, есть ненулевой идеал поля F и потому совпадает с F.

Обозначим через M множество элементов поля F, имеющих вид $x\Theta(x)$, где $x \in F$. Пусть порядок Θ равен m, а $n = km$. Выберем a примитивным элементом поля F. Тогда

$$a\Theta(a) = a^{p^{ik}+1} = z,$$

где $(i, m) = 1$. Очевидно, что $z^j = (a\Theta(a))^j = a^j\Theta(a^j) \in M$. Так как порядок мультипликативной группы F равен $p^{km} - 1$, то порядок элемента z равен $(p^{km} - 1)/s$, где s — наибольший общий делитель чисел $p^{ik} + 1$ и $p^{km} - 1$. Очевидно, что s делит

$$(p^{2ik} - 1, p^{km} - 1) = p^{(2ik, mk)} - 1 = p^k - 1.$$

Следовательно, $(p^k - 1, p^{ik} + 1) = s$. Тогда

$$p^{ik} + 1 \equiv 2 \pmod{s} \equiv 0 \pmod{s},$$

откуда $s = 1$ при $p = 2$ и $s = 2$ при $p > 2$. Поэтому $M = F$ при $p = 2$ и $|F^* : M| \leqslant 2$ при $p > 2$. В первом случае мы получили желаемое. В случае $p > 2$ из того, что $|F|/|M| < 3$, заключаем, что подпространство F, натянутое на M, также совпадает с F. Лемма доказана.

Лемма 6. *Пусть $\varphi \in G_1 \leqslant G = \mathrm{Aut}(P)$, где G_1 — подгруппа G, определенная в лемме 4, и λ, ψ — ассоциированные с φ отображения. Тогда $\lambda(a) - \Theta(\lambda(a)) = \psi(a - \Theta(a))$ для любого $a \in F$. В частности, $\Theta(a) = a$ тогда и только тогда, когда $\Theta(\lambda(a)) = \lambda(a)$.*

Доказательство. Так как $\lambda(1) = 1$, то, применяя лемму 3 (i) и подставляя $c = 1$, получаем: $\lambda(a) - \Theta(\lambda(a)) = \psi(a - \Theta(a))$. Из невырожденности ψ (лемма 2) следует нужное нам заключение.

Лемма 7. *Пусть $G = \mathrm{Aut}(P)$ и $A = A_1$ — группа автоморфизмов P, индуцирующих тождественный автоморфизм на $P/Z(P)$. Тогда G/A содержит нормальную подгруппу, изоморфную группе $\mathbf{GL}_{n/r}(p^r)$ (вложенную в $\mathbf{GL}_n(p)$ естественным образом) для некоторого делителя r числа n.*

Доказательство. Как уже было отмечено выше, группа $Z(P)$ совпадает с подгруппой Фраттини $\Phi(P)$ группы P. По лемме 2 ассоциированные с автоморфизмом φ отображения λ и ψ могут интерпретироваться как элементы группы $\mathbf{GL}_n(p)$. При этом те автоморфизмы P, которые индуцируют тождественный автоморфизм на $P/Z(P)$, образуют подгруппу A группы G (лемма 3 (iii)). Группа A, очевидно, является нормальной подгруппой G. Заметим, что по лемме 3 (iii) $A = A_1$, где A_1 определена во введении. При этом для $\lambda = id_F$, $\psi = id_F$ отображение μ линейно (лемма 3 (iii)). Согласно лемме 3 (iii), группа G/A является подгруппой группы $\mathbf{GL}_n(p)$. При этом действие G/A на $P/Z(P)$ описывается оператором λ.

Так как среди автоморфизмов P имеется автоморфизм $\varphi_\alpha \in A_2$, для которого $\lambda_\alpha(a) = \alpha \cdot a$, где α — примитивный элемент поля F, то G/A содержит цикл Зингера — циклическую подгруппу, действующую транзитивно на множестве ненулевых элементов F.

Для удобства читателя напомним, что по теореме Кантора [6] подгруппа группы $\mathbf{GL}_n(q)$, содержащая цикл Зингера, имеет нормальную подгруппу, изоморфную $\mathbf{GL}_{n/r}(q^r)$ для некоторого r, делящего n, причем $\mathbf{GL}_{n/r}(q^r)$ вложена в $\mathbf{GL}_n(q)$ естественным образом.

В нашем частном случае $\mathbf{GL}_1(p)n \simeq A_2 \rtimes A_3 \leqslant G/A$ содержит нормализатор цикла Зингера в $\mathbf{GL}_n(p)$. Поэтому по теореме Кантора, цитированной выше, заключаем, что G/A содержит нормальную подгруппу $\mathbf{GL}_{n/r}(p^r)$ (вло-

женную в $\mathbf{GL}_n(p)$ естественным образом) для некоторого делителя r числа n. Лемма доказана.

Отметим, что в нашем случае можно утверждать больше: группа G содержит подгруппу, изоморфную $\mathbf{GL}_{n/r}(p^r)r$. При $(n,p) \neq (6,2)$ (очевидно, что $n \geqslant 3$) эта подгруппа максимальна в $\mathbf{GL}_n(p)$.

§ 3. ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 1

Начиная с этого момента мы зафиксируем параметр $r = n/s$ и подполе $F_0 = \mathbf{GF}(p^r)$, фигурирующие в лемме 7. Через $\widehat{G}$ будет обозначаться подгруппа G/A, изоморфная $\mathbf{GL}_s(p^r)r$.

Поле $F = F_0 \oplus F_0 e_2 \oplus \ldots \oplus F_0 e_s$ для некоторых элементов $e_1 = 1, e_2, e_3, \ldots$ $\ldots, e_s \in F$, $rs = n$. Наша цель — доказать, что $s = 1$.

Как следует из леммы 7, действие автоморфизма $\varphi \in G$ на $P/Z(P)$ описывается оператором $\lambda = \lambda_\varphi$, ассоциированным с φ. Для доказательства теоремы 1 достаточно установить, что некоторые из автоморфизмов, содержащихся в $\mathbf{GL}_s(p^r)$, не могут быть реализованы в качестве преобразования λ, ассоциированного с автоморфизмом φ группы P.

Напомним, что через G_1 нами обозначена подгруппа группы G, состоящая из всех автоморфизмов группы P, для которых $\lambda(1) = 1$. Очевидно, что F_0 инвариантно относительно любого отображения λ, ассоциированного с автоморфизмом $\varphi \in G_1$. Пусть $\varphi \in G_1$ — такой автоморфизм P, что его образ при эпиморфизме $G \to \widehat{G}$ лежит в $\mathbf{GL}_s(F_0)$, и λ и ψ — ассоциированные с ним отображения. Тогда для $c \in F_0$ выполнено: $\lambda(c) = c$. С другой стороны, если $c \in K = C_F(\Theta)$, то $\lambda(c) \in K$ по лемме 6. Так как это свойство должно выполняться для любого отображения λ_φ с φ из G_1, то необходимо $K \leqslant F_0$.

Действительно, $G_1 A/A$ содержит подгруппу H, изоморфную $\mathbf{GL}_{s-1}(F_0)$, действующую транзитивно на множестве ненулевых элементов из $T = F_0 e_2 \oplus \ldots \oplus F_0 e_s$. Допустим, что K содержит элемент $y = c + u$, где $c \in F_0$ и u — ненулевой элемент из T. Так как $\lambda(c) = c$ для любого вектора $c \in F_0$, где $\lambda = \lambda_\varphi$ для $\varphi \in G_1$, то $\lambda(c+u) = c + \lambda(u) \in K$. Отсюда $\lambda(u) - u$ содержится в $K \cap T$. При этом можно выбрать $\varphi \in G_1$ так, что $\lambda_\varphi(u) \neq u$ для u, отличного от нуля. Так как $H \leqslant G_1 A/A$ действует транзитивно на множестве ненулевых векторов из T, то $T \subseteq K$. Отсюда легко следует, что $F = K$, противоречие.

Покажем, что при $K \neq F_0$ для $x \in F_0$ и $\varphi \in G_1$ выполнено: $\psi_\varphi(x) = x$. В самом деле, для указанного φ и ассоциированных с ним отображений λ и ψ имеем: в силу леммы 3 (i) $a\Theta(c) - c\Theta(a) = \psi(a\Theta(c) - c\Theta(a))$ при $a, c \in$ $\in F_0$. По лемме 5 множество элементов поля F_0, определенных выражением слева, содержит базис поля F_0 как векторного пространства над $\mathbf{GF}(p)$, что и требовалось. Итак, $\psi(x) = x$ для любого $x \in F_0$ при $\varphi \in G_1$.

Из леммы 3 (i) следует, что в общем случае выполнено следующее соотношение:

$$\psi(e_i\Theta(e_j) - e_j\Theta(e_i)) = \lambda(e_i)\Theta(\lambda(e_j)) - \lambda(e_j)\Theta(\lambda(e_i)) \tag{1}$$

для любых $1 \leqslant i, j \leqslant s$. В частности,

$$\psi(e_i - \Theta(e_i)) = \lambda(e_i) - \Theta(\lambda(e_i)) \tag{2}$$

при $j = 1$, когда $e_1 = 1$.

При $a = fe_2$, $c = ge_2 \in F_0 = F_0e_1$ получаем

$$a\Theta(c) - c\Theta(a) = fe_2\Theta(ge_2) - ge_2\Theta(fe_2) = (f\Theta(g) - g\Theta(f))e_2\Theta(e_2).$$

По лемме 3 (i) имеем

$$\psi((f\Theta(g) - g\Theta(f))e_2\Theta(e_2)) = \psi(fe_2\Theta(ge_2) - ge_2\Theta(fe_2)) = \\ = \lambda(fe_2)\Theta(\lambda(ge_2)) - \lambda(ge_2)\Theta(\lambda(fe_2)).$$

Учитывая F_0-линейность отображения λ, получаем, что

$$\lambda(fe_2)\Theta(\lambda(ge_2)) - \lambda(ge_2)\Theta(\lambda(fe_2)) = (f\Theta(g) - g\Theta(f))\lambda(e_2)\Theta(\lambda(e_2)).$$

Таким образом,

$$\psi((f\Theta(g) - g\Theta(f))e_2\Theta(e_2)) = (f\Theta(g) - g\Theta(f))\lambda(e_2)\Theta(\lambda(e_2)).$$

По лемме 5 множество элементов вида $a\Theta(c) - c\Theta(a)$ для $a, c \in F_0$ содержит базис поля F_0 (при условии $F_0 \neq K$) как векторного пространства над $\mathbf{GF}(p)$. В силу линейности ψ над $\mathbf{GF}(p)$ получаем, что

$$\psi(e_2\Theta(e_2)) = \lambda(e_2)\Theta(\lambda(e_2)). \tag{3}$$

Но тогда оказывается, что при $F_0 \neq K$ для любого $\gamma \in F_0$

$$\psi(\gamma e_2\Theta(e_2)) = \gamma\lambda(e_2)\Theta(\lambda(e_2)).$$

Рассмотрим теперь автоморфизм $\varphi \in G_1$, для которого ассоциированное с φ отображение λ имеет вид $\lambda(1) = 1$ и $\lambda(e_i) = de_i$ для некоторого $d \in \in K \setminus \{0, 1\}$ и для всех $i \geqslant 2$. Если $K = \{0, 1\}$, то автоморфизм Θ имеет нечетный порядок $n/2$, а поле F — характеристику 2. По теореме из [5] получаем противоречие. Поэтому можно считать, что $K \neq \{0, 1\}$.

Так как F_0 инвариантно относительно автоморфизма Θ и порядок Θ взаимно прост с p, то по теореме Машке $F = F_0 \oplus F_1$, где F_1 — также инвариантное подпространство относительно Θ. Заметим, что K содержится в F_0 и потому F_1 содержится в $(1 - \Theta)F$. Без ограничения общности можно считать, что $e_2, e_3, \ldots, e_s \in F_1$.

Допустим, что $F_0 \neq K$. Тогда для отображения ψ, ассоциированного с автоморфизмом φ, выполнено: $\psi(x) = x$ для любого $x \in F_0$. При $x \in F_1$ выполнено: $\lambda(x) = dx$. Согласно полученным выше соотношениям (3),

$$\psi(e_2\Theta(e_2)) = \lambda(e_2)\Theta(\lambda(e_2)) = d^2e_2\Theta(e_2).$$

С другой стороны, по (2)

$$\psi(e_2 - \Theta(e_2)) = \lambda(e_2) - \Theta(\lambda(e_2)) = d(e_2 - \Theta(e_2)). \tag{4}$$

Заметим, что $(1 - \Theta)$ — K-линейный оператор на F_1, не имеющий отличных от нуля неподвижных точек (по лемме 1). В частности, $e_2 - \Theta(e_2), e_3 - \Theta(e_3), \ldots, e_s - \Theta(e_s)$ — базис F_1. Используя (4) и $\mathbf{GF}(p)$-линейность ψ, нетрудно убедиться, что ограничение ψ на F_1 является K-линейным отображением. При этом $\psi(1 - \Theta) = (1 - \Theta)\lambda$ ввиду (2). Ограничение ψ на F_1 также есть умножение на d. Таким образом, если $y \in F$, то $y = u + v$, где $u \in F_0$, $v \in F_1$, так что $\psi(y) = u + dv$. Для элемента $y = e_2\Theta(e_2)$ имеем: $\psi(y) = d^2y = d^2u + d^2v$, где $u \in F_0$, $v \in F_1$. Отсюда следует, что $d = 1$ или $d = 0$ вопреки его выбору.

Итак, в дальнейшем можно считать, что $F_0 = K$. Будем рассматривать элемент $\varphi \in G_1$ с ассоциированными функциями λ и ψ, причем $\lambda(a) = a$ для $a \in K$ и $\lambda(x) = dx$ для $x \in F_1 = (1 - \Theta)F$. При этом из (1) и (2) легко следует K-линейность ограничения отображения ψ, ассоциированного с $\varphi \in G_1$, на F_1. Если $a, b \in F_1 \setminus \{0\}$, то $z = a\Theta(b) - b\Theta(a) = \alpha + u$ для некоторых $\alpha \in K$ и $u \in F_1$. Выберем элемент $c \in F_1 \setminus \{0\}$ так, чтобы $g = c\Theta(b) - b\Theta(c) = \beta + v$, где $\beta \in K$, $v \in F_1$. Нетрудно показать, что можно выбрать элемент $c \in F_1$ так, чтобы u и v были линейно независимы.

Тогда

$$w = (\beta a - \alpha c)\Theta(b) - b\Theta(\beta a - \alpha c) = \beta u - \alpha v \neq 0.$$

Понятно, что

$$\psi(w) = \lambda(\beta a - \alpha c)\Theta\lambda(b) - \lambda(b)\Theta\lambda(\beta a - \alpha c) = d^2w.$$

В случае, когда $\alpha = 0$, положим $w = z$, а когда $\beta = 0$, положим $w = g$. В любом из этих случаев имеем: $w \in F_1$ и $\psi(w) = d^2w$. Здесь мы воспользовались тем обстоятельством, что K-линейная комбинация элементов из F_1 также является элементом из F_1, а отображение $\psi(a\Theta(b) - b\Theta(a))$ билинейно относительно аргументов a и b над полем K. Так как $\psi(1 - \Theta) = (1 - \Theta)\lambda$, то $\psi(w) = dw$ для любого w из F_1. Отсюда $d^2 = d$, что приводит к противоречию. Таким образом, и в случае $F_0 = K$ рассматриваемый автоморфизм φ не может быть реализован при $s > 1$. Если $s = 1$, то G — разрешимая группа, содержащая цикл Зингера, и результат легко следует из леммы 7. Теорема доказана.

Авторы выражают признательность Ф. М. Малышеву, внимательно прочитавшему первоначальную версию статьи и сделавшему много полезных замечаний.

СПИСОК ЛИТЕРАТУРЫ

1. *Huppert B., Blackburn N.* Finite groups II. — New York: Springer-Verlag, 1982.
2. *Gorenstein D.* Finite groups. — New York: Harper and Row, 1968.
3. *Hanaki A.* A condition on lengths of conjugacy classes and character degrees. — Osaka J. Math., 1996, № 33, p. 207–216.
4. *Сагиров И.А.* Степени неприводимых характеров 2-групп Судзуки. — Матем. заметки, 1999, т. 66, № 2, с. 258–263.
5. *Брюханова Е.Г.* О группах автоморфизмов 2-автоморфных 2-групп. — Алгебра и логика, 1981, т. 20, № 1, с. 5–21.
6. *Kantor W.M.* Linear groups containing a Singer cycle. — J. Algebra, 1980, v. 62, p. 232–234.
7. *Казарин Л.С., Сидельников В.М.* О группе автоморфизмов p-алгебры Судзуки (в печати).