ИЗВЕСТИЯ ВЫСШИХ УЧЕБНЫХ ЗАВЕДЕНИЙ

2003 МАТЕМАТИКА № 10 (497)

УДК 512.542

И.А. САГИРОВ

ОБОБЩЕНИЕ 2-ГРУПП СУДЗУКИ $A(m,\theta)$

2-группы Судзуки $A(m,\theta)$ введены Хигманом, а наиболее полно исследованы в ([1], гл. VIII). Напомним, как они определяются. Рассмотрим конечное поле $GF(q)$, $q=2^m$, $m>1$, и его автоморфизм θ порядка k для некоторого делителя $k>1$ числа m. 2-группа Судзуки $A(m,\theta)$ — это множество упорядоченных пар элементов из $GF(q)$ с операцией $(a,b)(c,d)=(a+c,b+d+c\theta(a))$ для любых $a,b,c,d\in GF(q)$. Степени неприводимых характеров 2-групп Судзуки в случае автоморфизма θ нечетного порядка найдены в [2]. Позже автором было получено описание степеней неприводимых характеров групп $A(m,\theta)$ для произвольного автоморфизма θ [3]. Заменяя в определении 2-групп Судзуки поле $GF(2^m)$ на произвольное конечное поле $\mathbb{F}=GF(p^m)$, получим естественное обобщение этих групп. Обозначим полученные группы через $A_p(m,\theta)$. В продолжение [3] в данной работе получено полное описание степеней неприводимых характеров групп $A_p(m,\theta)$.

Ниже будут использоваться следующие обозначения: $\mathrm{Irr}(G)$ — множество всех неприводимых характеров, $\mathrm{Lin}(G)$ и $\mathrm{Irr}_1(G)$ – множества соответственно всех линейных и нелинейных неприводимых характеров, $\mathrm{cd}(G)$ — множество степеней неприводимых характеров, $\mathrm{Cl}(G)$ — множество классов сопряженных элементов группы G, $k(G)=|\mathrm{Cl}(G)|$.

Основная теорема. *Если $G=A_p(m,\theta)$ — p-группа порядка q^2, где $m>1$ целое, $q=p^m$, θ — автоморфизм порядка $k>1$, $n=m/k$, поля $GF(q)$, то выполнены следующие утверждения*:

(i) *если k нечетно, то* $\mathrm{cd}(G)=\{1,p^{\frac{m-n}{2}}\}$;

(ii) *если $k=2$, то* $\mathrm{cd}(G)=\{1,p^{\frac{m}{2}}\}$;

(iii) *если k четно и $k\neq 2$, то* $\mathrm{cd}(G)=\{1,p^{\frac{m}{2}},p^{\frac{m}{2}-n}\}$, *причем G имеет $\frac{p^m-1}{p^n+1}p^n$ характеров степени $p^{\frac{m}{2}}$ и $\frac{p^m-1}{p^n+1}p^{2n}$ характеров степени $p^{\frac{m}{2}-n}$.*

Как уже отмечалось, случай $p=2$ исследован в [3]. Поэтому в дальнейшем будем считать, что p — нечетное простое число и G обозначает группу $A_p(m,\theta)$, θ — автоморфизм порядка k поля $\mathbb{F}=GF(q)$, $q=p^m$ и $n=m/k$.

Лемма 1. *Для группы G выполняются следующие утверждения*:

(i) $Z(G)=\{(0,b)\mid b\in\mathbb{F}\}$, $|Z(G)|=p^m$;

(ii) $k(G)=p^{m+n}+p^m-p^n$;

(iii) $|G'|\geq p^{m-n}$.

Доказательство. (i) Из определения группы G следует, что если $(a,b)\in G$, то $(a,b)^p=(pa,pb+\frac{p(p-1)}{2}a\theta(a))$, а т. к. p — нечетное простое число, то $(a,b)^p=(0,0)$ и G — группа экспоненты p. Далее, $(a,b)^{-1}=(-a,-b+a\theta(a))$, и два элемента (a,b) и (c,d) коммутируют тогда и только тогда, когда $c\theta(a)=a\theta(c)$, что при $c\neq 0$ эквивалентно равенству $ac^{-1}=\theta(ac^{-1})$. Отсюда, в частности, следует $Z(G)=\{(0,b)\mid b\in\mathbb{F}\}$ и $|Z(G)|=p^m$.

(ii) Из доказательства п. (i) получаем, что централизатор любого нецентрального элемента G имеет порядок p^{m+n}. Но тогда число элементов, сопряженных с произвольным элементом из

$G\backslash Z(G)$, равно p^{m-n}. Пусть r — число нецентральных G-классов. Тогда $rp^{m-n}+p^m=p^{2m}=|G|$. Отсюда $r=p^{m+n}-p^n$ и

$$k(G)=p^{m+n}+p^m-p^n.$$

(iii) Так как $|C_G(g)|=p^{m+n}$ для любого элемента $g\in G\backslash Z(G)$, то $|G'|\geq p^{m-n}$.

Лемма 2. *Отображение ϕ_λ, заданное условием $\phi_\lambda(a,b)=(\lambda a,\lambda\theta(\lambda)b)$ $((a,b)\in G)$, является автоморфизмом группы G для любого $\lambda\in\mathbb{F}^*$.*

Доказательство аналогично доказательству леммы 2.3 из [4].

Так как θ — автоморфизм порядка k поля $\mathbb{F}$, то для любого $x\in\mathbb{F}$ имеем $\theta(x)=x^{p^{nv}}$ при v таком, что $(v,k)=1$. Зафиксируем такое v.

Лемма 3. (i) *Пусть $m=nk$ и $(v,k)=1$. Тогда*

$$(p^m-1,p^{nv}+1)=\begin{cases}2, & \text{если } k \text{ нечетно};\\ p^n+1, & \text{если } k \text{ четно}.\end{cases}$$

(ii) *Если m четно, а n — некоторое натуральное число, то*

$$(p^m-1,p^n+1)=\begin{cases}2, & \text{если } \frac{n}{(\frac{m}{2},n)} \text{ четно};\\ p^{(\frac{m}{2},n)}+1, & \text{если } \frac{n}{(\frac{m}{2},n)} \text{ нечетно}.\end{cases}$$

Доказательство. (i) Так как $(k,v)=1$, то $d=(p^m-1,p^{nv}+1)\mid(p^m-1,p^{2nv}-1)=(p^m-1,p^{2n}-1)$. Имеем

$$(p^m-1,p^{2n}-1)=\begin{cases}p^n-1, & \text{если } k \text{ нечетно};\\ p^{2n}-1, & \text{если } k \text{ четно}.\end{cases}$$

Пусть k нечетно. Найдем $(p^{nv}+1,p^n-1)$. Если $r>2$ простое и $r\mid(p^{nv}+1,p^n-1)$, то $p^n\equiv 1\pmod r$, а значит, $p^{nv}+1\equiv 2\pmod r$ — противоречие. Если $r=4$, то рассуждения аналогичны. Таким образом, при нечетном k имеем $(p^{nv}+1,p^n-1)=2$, откуда $d=2$.

Если k четно, то $p^n+1\mid p^m-1$ и $p^n+1\mid p^{nv}+1$, откуда $p^n+1\mid d$. Кроме того, $p^{nv}+1=(p^n+1)(p^{n(v-1)}-p^{n(v-2)}+\cdots+p^{2n}-p^n+1)$, $p^m-1=(p^n+1)(p^{n(k-1)}-p^{n(k-2)}+\cdots+p^n-1)$. Обозначим вторые множители в этих произведениях соответственно через A и B. Так как v нечетно, то A также нечетно, а в силу четности k число B четно. Отсюда следует, что $2\nmid\frac{d}{p^n+1}$. Поскольку $p^{2n}-1=(p^n+1)(p^n-1)$ и $(p^{nv}+1,p^n-1)=2$, получаем $d=p^n+1$.

(ii) Очевидно, $d=(p^m-1,p^n+1)\mid(p^m-1,p^{2n}-1)=p^{(m,2n)}-1=p^{2(\frac{m}{2},n)}-1=(p^{(\frac{m}{2},n)}-1)(p^{(\frac{m}{2},n)}+1)$. Далее, по аналогии с рассуждениями п. (i) $(p^{(\frac{m}{2},n)}-1,p^n+1)=2$,

$$(p^{(\frac{m}{2},n)}+1,p^n+1)=\begin{cases}2, & \text{если } \frac{n}{(\frac{m}{2},n)} \text{ четно};\\ p^{(\frac{m}{2},n)}+1, & \text{если } \frac{n}{(\frac{m}{2},n)} \text{ нечетно}.\end{cases}$$

Пусть сначала $\frac{n}{(\frac{m}{2},n)}$ четно. Тогда $d\in\{2,4\}$. В силу четности n при $p\equiv 1\pmod 4$ имеем $p^n+1\equiv 2\pmod 4$, а при $p\equiv 3\pmod 4$ $p^2\equiv 1\pmod 4$ и $p^n+1\equiv(p^2)^{\frac{n}{2}}+1\equiv 2\pmod 4$. Поэтому $4\nmid p^n+1$ и $d=2$.

Если $\frac{n}{(\frac{m}{2},n)}$ нечетно, то положим $\frac{n}{(\frac{m}{2},n)}=s$, $(\frac{m}{2},n)=t$. Тогда $p^{ts}+1=(p^t+1)(p^{t(s-1)}-p^{t(s-2)}+\cdots+p^{2t}-p^t+1)$, откуда $\frac{p^n+1}{p^t+1}$ нечетно.

Лемма 4. *Пусть λ — примитивный элемент поля $\mathbb{F}$. Длина орбиты ϕ_λ на $G\backslash Z(G)$ равна p^m-1. Длина орбиты ϕ_λ на $Z(G)^\#$ равна $\frac{p^m-1}{2}$ при нечетном k и $\frac{p^m-1}{p^n+1}$ при четном k.*

Доказательство. По определению $\phi_\lambda^i(a,b)=(\lambda^i a,(\lambda\theta(\lambda))^i b)$. Если $a\neq 0$, то утверждение следует из примитивности λ. Если $a=0$, то $\phi_\lambda^i(0,b)=(0,(\lambda\theta(\lambda))^i b)=(0,b)$ только при $(\lambda\theta(\lambda))^i=1$. Так как $\theta(\lambda)=\lambda^{p^{nv}}$, последнее выполнено при $\lambda^{(p^{nv}+1)i}=1$. Отсюда $p^m-1\mid(p^{nv}+1)i$ и утверждение леммы следует из леммы 3.

Лемма 5. *Пусть* $\chi \in \mathrm{Irr}_1(G)$, $\chi(1) = p^\alpha$, $Z_0 = Z(G) \cap \operatorname{Ker}\chi$. *Тогда* $|Z(G) : Z_0| = p$, $G' \not\leq Z_0$, $\mathrm{cd}(G/Z_0) = \{1, p^\alpha\}$, $|\mathrm{Irr}_1(G/Z_0)| = (p-1)p^{m-2\alpha}$. *Кроме того, любой нелинейный неприводимый характер* G *является характером ровно одной группы* G/Z, *где* $|Z(G) : Z| = p$ *и* $G' \not\leq Z$.

Доказательство. Так как группа $Z(G/\operatorname{Ker}\chi)$ циклическая, а $Z(G)$ элементарная абелева, то $|Z(G) : Z_0| = p$. Рассмотрим фактор-группу G/Z_0. Так как χ нелинейный, то $G'Z_0 = Z(G)$. Кроме того, $|(G/Z_0)'| = p$ и G/Z_0 — группа экспоненты p. Отсюда следует, что $G/Z_0 = G_1 \times Z_1$, где $Z_1 \leq Z(G/Z_0)$, а G_1 экстраспециальная. Теперь оставшиеся утверждения леммы следуют из описания степеней неприводимых характеров экстраспециальных групп ([4], теорема 5.5.5).

Теорема 1. *Если* $G = A_p(m, \theta)$ *и* θ *— автоморфизм нечетного порядка* $k > 1$ *поля* $\mathbb{F}$, *то* $G' = Z(G)$ *и* $\mathrm{cd}(G) = \{1, p^{\frac{m-n}{2}}\}$.

Доказательство. Пусть λ — примитивный элемент поля $\mathbb{F}$. В этом случае имеются две ϕ_λ-орбиты длины $\frac{p^m-1}{2}$ на $Z(G)^\#$. Если $g \in G'$, то и вся ϕ_λ-орбита элемента g также лежит в G'. Отсюда $|G'| \geq \frac{p^m-1}{2}$, а т. к. $|G'| \,|\, p^m$, то $|G'| = p^m$ и $G' = Z(G)$. Очевидно, имеется не более двух ϕ_λ-орбит на множестве подгрупп порядка p в $Z(G)$. Но поскольку $(p, |\phi_\lambda|) = 1$, то по теореме Машке имеется также не более двух ϕ_λ-орбит на множестве подгрупп индекса p в $Z(G)$. Так как $G/Z_0 \cong G/Z_0^{\phi_\lambda}$ для любой подгруппы Z_0 индекса p в $Z(G)$, а $|\mathrm{cd}(G/Z_0)| = 2$ по лемме 5, то группа G имеет не более двух степеней неприводимых нелинейных характеров.

Допустим, что $\mathrm{cd}(G) = \{1, p^\alpha, p^\beta\}$. Это означает, что имеются две ϕ_λ-орбиты на множестве подгрупп индекса p в $Z(G)$, причем длины этих орбит равны $\frac{p^m-1}{2(p-1)}$. Тогда характеров степени p^α имеется $\frac{p^m-1}{2(p-1)}(p-1)p^{m-2\alpha}$, а характеров степени p^β имеется $\frac{p^m-1}{2(p-1)}(p-1)p^{m-2\beta}$. Так как $k(G) = p^{m+n} + p^m - p^n$, то $p^{m+n} + p^m - p^n = p^m + \frac{p^m-1}{2}p^{m-2\alpha} + \frac{p^m-1}{2}p^{m-2\beta}$. Отсюда, $p^n = \frac{1}{2}(p^{m-2\alpha} + p^{m-2\beta})$, что возможно лишь при $\alpha = \beta$. Таким образом, $\mathrm{cd}(G) = \{1, p^\alpha\}$, откуда $\alpha = \frac{m-n}{2}$. □

В дальнейшем будем считать, что k четно.

Лемма 6. *Пусть* λ *— примитивный элемент поля* $\mathbb{F}$ *и* k *четно. Тогда*

(i) *если* $m \neq 2n$, *то* $G' = Z(G)$ *и* $(G')^\#$ *имеет* $p^n + 1$ ϕ_λ*-орбит длины* $\frac{p^m-1}{p^n+1}$;

(ii) *если* $m = 2n$, *то либо* $G' = Z(G)$ *и* $(G')^\#$ *имеет* $p^n + 1$ ϕ_λ*-орбит длины* $\frac{p^m-1}{p^n+1} = p^n - 1$, *либо* $|G'| = p^{\frac{m}{2}}$ *и все элементы* $(G')^\#$ *сопряжены под действием автоморфизма* ϕ_λ.

Доказательство аналогично доказательству леммы 3.2 из [3].

До конца доказательства теоремы 2 будем считать, что $G' = Z(G)$, т. е. элементы $(G')^\#$ разбиваются под действием ϕ_λ на $p^n + 1$ орбит длины $\frac{p^m-1}{p^n+1}$.

Лемма 7. *Пусть* λ *— примитивный элемент поля* $\mathbb{F}$. *Тогда под действием автоморфизма* ϕ_λ *неглавные неприводимые характеры* G *разбиваются на* p^n *орбит длины* $p^m - 1$ *и* $p^n + 1$ *орбит длины* $\frac{p^m-1}{p^n+1}$.

Доказательство аналогично доказательству п. 2 леммы 3.2 из [3].

Лемма 8. *Пусть* λ *— примитивный элемент поля* $\mathbb{F}$. *Тогда множество всех подгрупп индекса* p *группы* $Z(G)$ *под действием* ϕ_λ *разбивается либо на* $p^n + 1$ *орбит длины* $\frac{p^m-1}{(p^n+1)(p-1)}$, *либо на* $\frac{p^n+1}{2}$ *орбит длины* $\frac{2(p^m-1)}{(p^n+1)(p-1)}$.

Доказательство. Рассмотрим подгруппу $P \leq Z(G)$ порядка p. Пусть $P = \langle (0,x) \rangle = \{1, (0,x), \ldots, (0,x)^{p-1}\}$, а s — наименьшее число такое, что $\phi_\lambda^s(0,x) \in P$. Так как $\left|\phi_\lambda\,|_{Z(G)}\right| = \frac{p^m-1}{p^n+1}$ согласно лемме 4, то $s \,\big|\, \frac{p^m-1}{p^n+1}$ и $P^\#$ разбивается на $\frac{p-1}{t}$ ϕ_λ-орбит длины t, $st = \frac{p^m-1}{p^n+1}$. Но тогда длина ϕ_λ-орбиты, содержащей подгруппу P, равна s. Пусть $P_1 = \langle (0,y) \rangle$ — другая подгруппа порядка p из $Z(G)$. Так как $Z(G) = \{(0,b) \mid b \in \mathbb{F}\}$, а λ — примитивный элемент поля $\mathbb{F}$, то $(0,y) = (0, \lambda^f x)$. Кроме того, т. к. $\phi_\lambda^s(0,x) \in P$, то $\phi_\lambda^s(0,x) = (0, (\lambda\theta(\lambda))^s x) = (0,x)^r = (0, rx)$. Тогда $\phi_\lambda^s(0,y) = (0, (\lambda\theta(\lambda))^s y) = (0, (\lambda\theta(\lambda))^s \lambda^f x) = (0, \lambda^f(\lambda\theta(\lambda))^s x) = (0, r\lambda^f x) = (0,y)^r$. Это означает, что длина ϕ_λ-орбиты, содержащей подгруппу P_1, также равна s. Таким образом, длины

всех ϕ_λ-орбит на множестве подгрупп порядка p в $Z(G)$ равны s. Так как всего подгрупп порядка p имеется $\frac{p^m-1}{p-1}$, то число ϕ_λ-орбит равно $\frac{p^m-1}{s(p-1)} = \frac{t(p^n+1)}{p-1}$. Поскольку $(p^n+1, p-1) = 2$, то $t \in \{p-1, \frac{p-1}{2}\}$. Значит, множество всех подгрупп порядка p группы $Z(G)$ под действием ϕ_λ разбивается либо на p^n+1 орбит длины $\frac{p^m-1}{(p^n+1)(p-1)}$, либо на $\frac{p^n+1}{2}$ орбит длины $\frac{2(p^m-1)}{(p^n+1)(p-1)}$.

Пусть теперь $Q \le Z(G)$ и $|Z(G) : Q| = p$. Так как $Q = P_1 \times \cdots \times P_{m-1}$, где $|P_i| = p$, то $\phi_\lambda^s(Q) = Q$. Если же для некоторого $s_1 < s$ имеет место $\phi_\lambda^{s_1}(Q) = Q$, то по теореме Машке $Z(G) = Q \times P$, где $|P| = p$ и $\phi_\lambda^{s_1}(P) = P$, что противоречиво. Теперь заключение леммы следует из доказанного в предыдущем абзаце. $\square$

Лемма 9. *Пусть $\chi \in \mathrm{Irr}_1(G)$, $\chi(1) = p^\alpha$. Тогда $\alpha \le \frac{m}{2}$; $\alpha \ge \frac{m}{2} - n$, если число ϕ_λ-орбит на множестве подгрупп индекса p в $Z(G)$ равно p^n+1, и $\alpha > \frac{m}{2} - n$, если число ϕ_λ-орбит равно $\frac{p^n+1}{2}$.*

Доказательство. Из леммы 5 следует, что $\chi \in \mathrm{Irr}_1(G/Z_0)$, где $Z_0 \le Z(G)$, $|Z(G) : Z_0| = p$ и $|\mathrm{Irr}_1(G/Z_0)| = (p-1)p^{m-2\alpha}$. Последнее означает, что $m - 2\alpha \ge 0$ и $\alpha \le \frac{m}{2}$.

Пусть $Z_1, \ldots, Z_u$ — множество представителей ϕ_λ-орбит на множестве подгрупп индекса p в $Z(G)$. Тогда $\mathrm{cd}(G/Z_i) = \{1, p^{\alpha_i}\}$, $|\mathrm{Irr}_1(G/Z_i)| = (p-1)p^{m-2\alpha_i}$. Кроме того, любые две подгруппы индекса p в $Z(G)$, принадлежащие одной ϕ_λ-орбите, изоморфны. Так как $|\mathrm{Irr}_1(G)| = p^{m+n} - p^n$, то

$$p^{m+n} - p^n = \frac{p^m - 1}{u(p-1)} \sum_{i=1}^{u} (p-1)p^{m-2\alpha_i},$$

откуда $up^n = \sum\limits_{i=1}^{u} p^{m-2\alpha_i}$.

Пусть $u = p^n + 1$. Если для некоторого i выполняется $m - 2\alpha_i > 2n$, то $p^{m-2\alpha_i} \ge p^{2n+1} > p^n(p^n+1) = up^n$ — противоречие. Значит, $m - 2\alpha_i \le 2n$ и $\alpha_i \ge \frac{m}{2} - n$ для всех i.

Пусть $u = \frac{p^n+1}{2}$. Если для некоторого i выполняется $m - 2\alpha_i \ge 2n$, то $p^{m-2\alpha_i} \ge p^{2n} > \frac{1}{2}p^n(p^n+1) = up^n$ — противоречие. Значит, $\alpha_i > \frac{m}{2} - n$ для всех i.

Теорема 2. *Если $G' = Z(G)$ и k четно, то $\mathrm{cd}(G) = \{1, p^{\frac{m}{2}-n}, p^{\frac{m}{2}}\}$, причем группа G имеет $\frac{p^m-1}{p^n+1}p^{2n}$ неприводимых характеров степени $p^{\frac{m}{2}-n}$ и $\frac{p^m-1}{p^n+1}p^n$ неприводимых характеров степени $p^{\frac{m}{2}}$.*

Доказательство. Согласно лемме 7 множество $\mathrm{Irr}(G)\backslash\{1_G\}$ под действием ϕ_λ разбивается на p^n орбит длины $p^m - 1$ и $p^n + 1$ орбит длины $\frac{p^m-1}{p^n+1}$. В силу того что $\mathrm{Lin}(G) \cong G/G'$, неглавные линейные характеры G образуют одну ϕ_λ-орбиту длины $p^m - 1$. Поэтому на $\mathrm{Irr}_1(G)$ имеется $p^n - 1$ ϕ_λ-орбит длины $p^m - 1$. По лемме 5 каждый нелинейный неприводимый характер G является характером ровно одной группы G/Z_0, где $Z_0 \le Z(G)$ и $|Z(G) : Z_0| = p$, а по лемме 8 множество $\mathfrak{M}$ всех подгрупп индекса p группы $Z(G)$ под действием ϕ_λ разбивается либо на p^n+1 орбит длины $\frac{p^m-1}{(p^n+1)(p-1)}$, либо на $\frac{p^n+1}{2}$ орбит длины $\frac{2(p^m-1)}{(p^n+1)(p-1)}$.

Пусть сначала число ϕ_λ-орбит в $\mathfrak{M}$ равно p^n+1. Рассмотрим характер $\chi \in \mathrm{Irr}_1(G/Z_0)$, $Z_0 \in \mathfrak{M}$. Если длина ϕ_λ-орбиты χ равна $p^m - 1$, то в $\mathrm{Irr}_1(G/Z_0)$ содержатся $(p-1)(p^n+1)$ характеров из ϕ_λ-орбиты χ. Если же длина ϕ_λ-орбиты χ равна $\frac{p^m-1}{p^n+1}$, то в $\mathrm{Irr}_1(G/Z_0)$ содержатся $p-1$ характеров из ϕ_λ-орбиты χ. Отметим, что если для некоторой подгруппы $Z_0 \in \mathfrak{M}$ в $\mathrm{Irr}_1(G/Z_0)$ нет характеров, длина ϕ_λ-орбиты которых равна $\frac{p^m-1}{p^n+1}$, то $\mathrm{Irr}_1(G/Z_0)$ разбивается на орбиты длины $(p-1)(p^n+1)$. Так как $|\mathrm{Irr}_1(G/Z_0)| = (p-1)p^{m-2\alpha}$, где $p^\alpha \in \mathrm{cd}(G/Z_0)$, то $p^n + 1 | p^{m-2\alpha}$ — противоречие. Значит, в каждой группе G/Z_0 имеются по крайней мере $p-1$ характеров, длина ϕ_λ-орбиты которых равна $\frac{p^m-1}{p^n+1}$. Так как всего таких характеров $p^m - 1$, а $|\mathfrak{M}| = \frac{p^m-1}{p-1}$, то в каждой группе G/Z_0 имеется ровно $p-1$ характеров, длина ϕ_λ-орбиты которых равна $\frac{p^m-1}{p^n+1}$.

Пусть $\mathrm{cd}(G/Z_0) = \{1, p^\alpha\}$ и в G/Z_0 содержатся $t(p-1)(p^n+1)$ характеров с ϕ_λ-орбитой длины $p^m - 1$. Тогда $|\mathrm{Irr}_1(G/Z_0)| = (p-1)p^{m-2\alpha} = (p-1) + t(p-1)(p^n+1)$. Отсюда $p^{m-2\alpha} - 1 = t(p^n+1)$ и $p^n + 1 \mid p^{m-2\alpha} - 1$. Следовательно, $n \mid m - 2\alpha$ и $\frac{m-2\alpha}{n}$ четно. По лемме 9 имеем $\frac{1}{2}m - n \le \alpha \le \frac{1}{2}m$,

откуда $0 \le \frac{m-2\alpha}{n} \le 2$. Пусть $t > 0$. Тогда $|\operatorname{Irr}_1(G/Z_0)| > p-1$, а потому $m-2\alpha \ne 0$. Значит, $\frac{m-2\alpha}{n}=2$ и $\alpha = \frac{1}{2}m - n$, $|\operatorname{Irr}_1(G/Z_0)| = (p-1)p^{2n}$, $t = p^n - 1$. Так как $t = p^n - 1$, то в $\operatorname{Irr}_1(G/Z_0)$ содержатся представители всех ϕ_λ-орбит длины $p^m - 1$ из $\operatorname{Irr}_1(G)$. Поэтому все характеры с ϕ_λ-орбитой длины $p^m - 1$ содержатся в одной ϕ_λ-орбите из $\mathfrak{M}$. Тогда в G имеются $(p-1)p^{2n}\frac{p^m-1}{(p-1)(p^n+1)} = p^{2n}\frac{p^m-1}{p^n+1}$ характеров степени $p^{\frac{1}{2}m-n}$. Сумма квадратов их степеней равна $p^m\frac{p^m-1}{p^n+1}$. Количество оставшихся неприводимых нелинейных характеров G равно $t_1 = p^n(p^m-1) - p^{2n}\frac{p^m-1}{p^n+1} = p^n\frac{p^m-1}{p^n+1}$, а сумма квадратов их степеней равна $\Sigma = p^m(p^m-1) - p^m\frac{p^m-1}{p^n+1} = p^m\frac{p^n(p^m-1)}{p^n+1}$. Если $\chi \in \operatorname{Irr}_1(G)$, то $\chi(1)^2 \le |G : Z(G)| = p^m$. Так как $\Sigma = t_1 p^m$, то все оставшиеся нелинейные характеры G имеют степень $p^{\frac{1}{2}m}$.

Пусть теперь число ϕ_λ-орбит в $\mathfrak{M}$ равно $\frac{p^n+1}{2}$. Напомним, что длина этих ϕ_λ-орбит равна $\frac{2(p^m-1)}{(p-1)(p^n+1)}$. Если в $\operatorname{Irr}_1(G/Z_0)$ ($Z_0 \in \mathfrak{M}$) содержится характер χ, длина ϕ_λ-орбиты которого равна $p^m - 1$, то в $\operatorname{Irr}_1(G/Z_0)$ содержатся также $(p-1)\frac{p^n+1}{2}$ сопряженных с χ. Аналогично, если в $\operatorname{Irr}_1(G/Z_0)$ имеется характер, длина ϕ_λ-орбиты которого равна $\frac{p^m-1}{p^n+1}$, то в $\operatorname{Irr}_1(G/Z_0)$ имеются также $\frac{p-1}{2}$ ему сопряженных. По аналогии с предыдущим случаем можно показать, что в каждой группе G/Z_0 ($Z_0 \in \mathfrak{M}$) имеются характеры с ϕ_λ-орбитой длины $\frac{p^m-1}{p^n+1}$.

Допустим, в некоторой группе G/Z_0 имеются ровно $\frac{p-1}{2}$ характеров с ϕ_λ-орбитой длины $\frac{p^m-1}{p^n+1}$. Тогда $|\operatorname{Irr}_1(G/Z_0)| = (p-1)p^{m-2\alpha} = \frac{p-1}{2} + t(p-1)\frac{p^n+1}{2}$, $t \ge 0$. Отсюда $2p^{m-2\alpha} = 1 + t(p^n+1)$ невозможно, т. к. $2p^{m-2\alpha}$ и $p^n + 1$ четны. Значит, в каждой группе G/Z_0 имеется по крайней мере $p-1$ характеров, длина ϕ_λ-орбиты которых равна $\frac{p^m-1}{p^n+1}$. Так как $|\mathfrak{M}| = \frac{p^m-1}{p-1}$, а количество указанных характеров $p^m - 1$, то в каждой группе G/Z_0 имеются ровно $p-1$ характеров с ϕ_λ-орбитой длины $\frac{p^m-1}{p^n+1}$ (причем эти характеры принадлежат двум разным ϕ_λ-орбитам).

Пусть теперь G/Z_0 содержит характеры с ϕ_λ-орбитой длины $p^m - 1$. Тогда по доказанному $|\operatorname{Irr}_1(G/Z_0)| = (p-1)p^{m-2\alpha} = (p-1) + t(p-1)\frac{p^n+1}{2}$. Отсюда $2(p^{m-2\alpha}-1) = t(p^n+1)$. Так как m четно, то $m - 2\alpha$ также четно, поэтому, используя лемму 3 (ii), нетрудно показать, что либо $n \mid \frac{m-2\alpha}{2}$, $p^n + 1 \mid p^{m-2\alpha} - 1$ и $t = 2\frac{p^{m-2\alpha}-1}{p^n+1}$, либо $p = 3$, $n = 1$ и $t = \frac{3^{m-2\alpha}-1}{2}$. Однако по условию $n \ne 1$ и второй случай невозможен. В первом же случае получаем, что либо $2n \le m - 2\alpha$, $\alpha \le \frac{m}{2} - n$, что противоречит лемме 9, либо $m - 2\alpha = 0$, $\alpha = \frac{m}{2}$, $t = 0$, противоречиво.

Таким образом, случай, когда в $\mathfrak{M}$ имеются $\frac{p^n+1}{2}$ ϕ_λ-орбит, невозможен.

Следствие. Если $m = 2n$, то $|G'| = p^{\frac{m}{2}}$.

Доказательство. Предположим, что $G' = Z(G)$. Тогда по теореме 2 $\operatorname{cd}(G) = \{1, p^{\frac{m}{2}-n}, p^{\frac{m}{2}}\}$, что невозможно в силу равенства $\frac{m}{2} - n = 0$.

Теорема 3. *Если $m = 2n$, то* $\operatorname{cd}(G) = \{1, p^{\frac{m}{2}}\}$.

Доказательство. Согласно лемме 6 (ii) и следствию теоремы 2 имеем $|G'| = p^{\frac{1}{2}m}$, $|G : G'| = p^{m+\frac{1}{2}m} = p^{m+n} = |\operatorname{Lin}(G)|$, откуда $|\operatorname{Irr}_1(G)| = p^m - p^n = p^{\frac{1}{2}m}(p^{\frac{1}{2}m} - 1)$. Каждый неприводимый нелинейный характер группы G содержится ровно в одной группе G/Z_0, где Z_0 — подгруппа индекса p в $Z(G)$ и $G' \not\le Z_0$. Число таких подгрупп равно $\frac{p^m-1}{p-1} - \frac{p^{\frac{1}{2}m}-1}{p-1} = \frac{p^{\frac{1}{2}m}-1}{p-1}p^{\frac{1}{2}m}$, причем в каждой группе G/Z_0 имеются не менее $p-1$ неприводимых нелинейных характеров. Сравнивая число нелинейных неприводимых характеров группы G и число подгрупп индекса p в $Z(G)$, не содержащих G', получаем, что в любой группе G/Z_0 имеются ровно $p-1$ нелинейных неприводимых характеров. Пусть $\operatorname{cd}(G/Z_0) = \{1, p^\alpha\}$. Тогда $p - 1 = |\operatorname{Irr}_1(G/Z_0)| = (p-1)p^{m-2\alpha}$. Отсюда $\alpha = \frac{1}{2}m$.

Доказательство основной теоремы. В случае нечетного k доказательство основной теоремы следует из теоремы 1. При четном k оно получается непосредственно из леммы 6, теоремы 2, следствия к ней и теоремы 3.

Литература

1. Huppert B., Blackburn N. *Finite Groups.* II. – Berlin–Heidelberg–New York: Springer, 1982. – 454 p.
2. Hanaki A. *A condition on lengths of conjugacy classes and character degrees* // Osaka J. Math. – 1996. – № 33. – P. 207–216.
3. Сагиров И.А. *Степени неприводимых характеров 2-групп Судзуки* // Матем. заметки. – 1999. – Т. 66. – № 2. – С. 258–263.
4. Gorenstein D. *Finite groups.* – New York: Harper and Row, 1968. – 527 p.

Ярославский государственный университет

Поступили
первый вариант 18.01.2001
окончательный вариант 08.11.2001