Е. И. Хухро, Конечные p-группы, близкие к группам простого периода, *Алгебра и логика*, 1986, том 25, номер 2, 227–240

Алгебра и логика, 25, № 2 (1986),227-240

УДК 519.44

КОНЕЧНЫЕ p-ГРУППЫ, БЛИЗКИЕ К ГРУППАМ ПРОСТОГО ПЕРИОДА

Е.И.ХУХРО

В настоящей работе дается ответ на вопрос Блэкберна и Эспуэласа [1] о степенном строении конечных p-групп, близких к группам периода p. В качестве следствия опровергается гипотеза об индексе обобщенной подгруппы Хьюза $H_{p^2}(G)$ для непримарных групп G (см. [2]).

Недавно Блэкберн и Эспуэлас (см. [1]) доказали, что если в метабелевой p-группе P подгруппа $\mho_1(P)=\langle x^p \mid x\in P\rangle$ имеет порядок p, то индекс подгруппы $\Omega_1(P)=\langle x\in P \mid x^p=1\rangle$ не превосходит p^p. На основе этого результата о p-группах Эспуэлас [2] доказал, что если в конечной группе G силовская p-подгруппа метабелева и не совпадает с G, то индекс подгруппы $H_{p^2}(G)=\langle x\in G \mid x^{p^2}\neq 1\rangle$ не превосходит p^p. Авторы работы [1] поставили вопрос, не будет ли для любой конечной p-группы P с $|\mho_1(P)|=p$ выполняться неравенство $|P:\Omega_1(P)|\leqslant p^p$. Кроме того, в работе [2] отмечается гипотеза: для любой конечной группы G, не являющейся p-группой, при $p>2$ выполняется неравенство $|G:H_{p^2}(G)|\leqslant p^p$. (Для $p=2,3$ первое предположение справедливо [1]; второе для $p=3$ доказано Дэффи [3].)

В настоящей работе опровергаются оба предположения.

Теорема. *Предположим, что для каждого $k=1,2,\dots,r$ полилинейные тождества степени $1+k(p-1)$, выполняющиеся в присоединенном кольце Ли свободной группы простого периода p, не являются следствием его полилинейных тождеств меньшей степени. Тогда существует конечная $(1+r(p-1))$-ступенно нильпотентная p-группа P, в которой $|\mho_1(P)|=p$ и $|P:\Omega_1(P)|\geqslant p^{1+r(p-1)}$, причем $\Omega_1(P)=\Phi(P)$.*

Пока лишь для тождеств степени $2p-1$ и $p=5, 7, 11$ известно [4], что условие теоремы действительно выполняется.

Следствие 1. *При* $p=5, 7, 11$ *существует конечная* $(2p-1)$*-ступенно нильпотентная* p*-группа* P, *для которой* $|\mho_1(P)|=p$ *и* $|P:\Omega_1(P)|\geqslant p^{2p-1}$, *причем* $\Omega_1(P)=\Phi(P)$.

Томпсон и Хьюз [5] доказали, что $|G:H_p(G)|\leqslant p$ для любой конечной непримарной группы G. Для периода p^2 ситуация оказалась иной.

Следствие 2. *В условиях теоремы существует конечная группа* G, *не являющаяся* p*-группой, для которой*

$$|G:H_{p^2}(G)|\geqslant p^{1+r(p-1)}.$$

Следствие 3. *Для* $p=5, 7, 11$ *существует конечная группа* G, *не являющаяся* p*-группой, для которой*

$$|G:H_{p^2}(G)|\geqslant p^{2p-1}.$$

Все полилинейные тождества кольца Ли свободной группы простого периода p нашел Воон-Ли [6]. Уолл [7] доказал, что из них только тождества степени $1+k(p-1)$ могут оказаться действительно новыми. При том же предположении, что и в нашей теореме, Уолл [7] построил примеры p-групп Q с $|Q:H_p(Q)|=p^r$. (Для степени $3p-2$ аналогичные результаты получены в [8].) Ранее Уолл [4, 9] рассмотрел компоненты степени $2p-1$ и $3p-3$.

Группы из заключения теоремы являются также скрытными p-группами в терминологии из [10, 11]. Они имеют бо́льший ранг, чем построенные ранее Уоллом в [11]. Как и в [11], в доказательстве основного результата используется невырожденная n-форма над полем из p элементов, т.е. однородный степени n многочлен от s переменных $\lambda_1, \lambda_2, \ldots, \lambda_s$, равный нулю только при $\lambda_1=\lambda_2=\ldots=\lambda_s=0$. (В работе [11] степень формы была связана с периодом группы. По теореме Шевалле [12] над полем $GF(p)$ не существует невырожденных n-форм от s переменных при $n<s$. Это обстоятельство могло наводить на мысль о невозможности существования групп из заключения теоремы.)

В настоящей работе слагаемые n-формы возникают как коэффициенты при некоторых элементах Ли степени $1+k(p-1)$, $k=1, 2, \ldots, r$. При этом используется техника, развитая Уоллом в [7].

В § 1 мы приводим необходимые в дальнейшем результаты и определения из [7], в § 2 строится невырожденная n-форма, обладающая некоторыми дополнительными свойствами, в § 3 завершается доказательство теоремы, а в § 4 доказываются следствия 2 и 3.

§ 1. Тождества присоединенного кольца Ли свободной группы простого периода

В этом параграфе приводятся необходимые в дальнейшем определения и результаты из [7].

Пусть p и r - числа из формулировки теоремы. Для краткости положим $N=1+r(p-1)$ и зафиксируем это значение N для дальнейшего.

Через A будем обозначать ассоциативную алгебру с 1 над кольцом p-целых рациональных чисел с порождающими $x_1, x_2, \ldots, x_N$, в которой равен 0 любой моном степени $\geq p$ по какой-либо из переменных x_i, а также равен 0 любой моном степени $\geq N+1$. Через $\mathcal{L}$ будем обозначать подалгебру Ли, порожденную элементами $x_1, x_2, \ldots, x_N$ относительно операции $[a, b] = ab - ba$.

Через $\zeta_s(y_1, y_2, \ldots, y_s)$ обозначается полилинейная однородная степени s компонента многочлена

$$((1+y_1)\cdot(1+y_2)\cdot \ldots \cdot(1+y_s))^p,$$

где y_i - любые некоммутирующие переменные; в частности, $\zeta_1(y) = py$.

Для удобства введено обозначение

$$\zeta(y_1^{a_1} y_2^{a_2} \ldots y_N^{a_N}) = \zeta_{\Sigma a_i}(\underbrace{y_1, \ldots, y_1}_{a_1}, \ldots, \underbrace{y_N, \ldots, y_N}_{a_N}).$$

Здесь числа a_i могут быть равны 0, - тогда соответствующая переменная x_i пропущена.

Положим
$$e(y) = \sum_{m=0}^{p-1} \frac{y^m}{m!}.$$

Тогда в кольце A справедливо равенство

$$e(x_i)^n = e(nx_i)$$

для любых $i=1,2,\ldots,N$ и $n \in \mathbb{Z}$. Имеет место равенство

$$\left(e(x_1)^{n_1}\cdot\ldots\cdot e(x_N)^{n_N}\right)^p=\sum\frac{n_1^{a_1}\cdot\ldots\cdot n_N^{a_N}}{a_1!\cdot\ldots\cdot a_N!}\cdot\zeta\left(x_1^{a_1}\ldots x_N^{a_N}\right),\tag{1}$$

где под знаком суммы числа a_i независимо изменяются от 0 до $p-1$, при этом, по определению, $\zeta_0=1$.

В алгебре A определяется последовательность идеалов

$$I_1\subseteq I_2\subseteq\ldots$$

Идеал I_s порожден элементами $\zeta_i(l_1,\ldots,l_i)$ для всех $i=1,2,\ldots,s$ и для всевозможных однородных элементов $l_j\in\mathcal{L}$. Как доказано в [7], условие теоремы эквивалентно тому, что

$$\zeta_{1+k(p-1)}(x_1,x_2,\ldots,x_{1+k(p-1)})\notin I_{k(p-1)}\tag{2}$$

для всех $k=1,2,\ldots,r$. Там же (и в [6]) показано, что для любого m многочлен $\zeta_{m+1}(y_1,y_2,\ldots,y_{m+1})$ является симметрической функцией по модулю I_m. Поэтому обычные рассуждения типа линеаризации показывают, что (2) эквивалентно любому из утверждений

$$\zeta_{1+k(p-1)}(x_1^{a_1}\ldots x_N^{a_N})\notin I_{k(p-1)}\tag{3}$$

при $a_1+a_2+\ldots+a_N=1+k(p-1)$ и $0\leqslant a_i\leqslant p-1$ для всех $i=1,2,\ldots,N$.

В [7] также доказано, что $I_m=I_{m+1}$, если только $m\neq k(p-1)$ ни для какого k.

Через F обозначается мультипликативная группа из A, порожденная элементами $e(x_1),\ldots,e(x_N)$. Эта группа нильпотентна ступени N. Пусть $V_1=e(x_1),\ldots,V_N=e(x_N)$, $V_{N+1},\ldots,V_T$ - базисные коммутаторы группы F, упорядоченные обычным образом. Тогда каждый элемент из F имеет вид

$$V_1^{m_1}\cdot V_2^{m_2}\cdot\ldots\cdot V_T^{m_T},\quad m_i\in\mathbb{Z}.$$

По формуле Бейкера-Кэмпбелла-Хаусдорфа имеем $V_i=e(v_i)$ для некоторого $v_i\in\mathcal{L}$. Поясним это утверждение подробнее. Пусть $exp(y)$ обозначает сумму $\sum_{m=0}^{N}\frac{y^m}{m!}$. Рассмотрим групповой коммутатор C от элементов $exp(x_i)=e(x_i)$. Используя формулу Бейкера-Кэмпбелла-Хаусдорфа, несложно показать, что $C=exp(c+\ldots)$, где c - кольцевой коммутатор от x_i с такой же расстановкой скобок, как у C, а точки обозначают сумму однородных элементов Ли, степень каждого из которых по каждой из переменных x_i не меньше чем у C. Следовательно, $(C+\ldots)^p=0$, и $C=e(C+\ldots)$, как и утверждалось.

Итак, каждый из определенных выше элементов v_i имеет вид $C+\ldots$ с указанным выше свойством. Это свойство гарантирует, что любой моном от элементов v_i равен 0, как только он имеет степень $\geqslant p$ по какой-то из переменных v_i. Следовательно, согласно (1), p-я степень произвольного элемента из F имеет вид

$$\left(V_1^{m_1}\cdot\ldots\cdot V_T^{m_T}\right)^p=\sum\frac{m_1^{a_1}\cdot\ldots\cdot m_T^{a_T}}{a_1!\cdot\ldots\cdot a_T!}\cdot\zeta\left(v_1^{a_1}\ldots v_T^{a_T}\right). \quad (4)$$

§ 2. Невырожденная N-форма

Введем обозначение для коэффициентов однородного степени N многочлена F от N переменных $\lambda_1,\lambda_2,\ldots,\lambda_N$. Положим

$$F(\lambda_1,\ldots,\lambda_N)=\sum f\begin{pmatrix}a_i & a_{i+1}\ldots a_N\\ i & i+1\ldots N\end{pmatrix}\cdot\lambda_i^{a_i}\cdot\lambda_{i+1}^{a_{i+1}}\cdot\ldots\cdot\lambda_N^{a_N},$$

где $a_i+a_{i+1}+\ldots+a_N=N$ и первым в верхней строке в скобках всегда будет стоять первый ненулевой показатель в мономе $\lambda_i^{a_i}\cdot\lambda_{i+1}^{a_{i+1}}\cdot\ldots\cdot\lambda_N^{a_N}=$ $=\lambda_1^0\cdot\lambda_2^0\cdot\ldots\cdot\lambda_{i-1}^0\cdot\lambda_i^{a_i}\cdot\lambda_{i+1}^{a_{i+1}}\cdot\ldots\cdot\lambda_N^{a_N}$. Числа $a_i,a_{i+1},\ldots$ будем называть показателями коэффициента $f\begin{pmatrix}a_i & a_{i+1}\ldots\\ i & i+1\ldots\end{pmatrix}$.

Известно, что существует невырожденная N-форма над $GF(p)$, т.е. такой многочлен F, что $F(\lambda_1,\ldots,\lambda_N)=0$ тогда и только тогда, когда $\lambda_1=\lambda_2=\ldots=\lambda_N=0$. Достаточно выбрать некоторую базу $e_1,\ldots,e_N$ конечного поля $GF(p^N)$, состоящего из p^N элементов и рассматриваемого как базисное пространство над простым подполем $GF(p)$. Тогда умножение в поле $GF(p^N)$ на любой элемент $\sum_1^N\lambda_i e_i$ является линейным преобразованием над $GF(p)$. Определитель его матрицы в заданной базе – норма элемента $\sum_1^N\lambda_i e_i$ – выражается как полилинейный однородный многочлен от переменных $\lambda_1,\ldots,\lambda_N$. Он и является невырожденной N-формой.

Нам потребуется далее, чтобы выполнялось одно дополнительное свойство.

Лемма 1. *Существует такая невырожденная N-форма от N переменных над $GF(p)$*

$$F=\sum f\begin{pmatrix} a_i & a_{i+1}\cdots \\ i & i+1\ \ldots \end{pmatrix}\cdot\lambda_i^{a_i}\cdot\lambda_{i+1}^{a_{i+1}}\cdot\ \ldots,$$

что если среди показателей какого-либо коэффициента есть больше или равные p, то либо этот коэффициент равен 0, либо такой показатель только один и стоит первым из ненулевых.

Доказательство. Мы построим новую форму, удовлетворяющую лемме 1, исходя из некоторой невырожденной N-формы. Воспользуемся тем, что в поле $GF(p)$ при $i_1\neq 0$ и $i_2\neq 0$, очевидно, выполняется тождество

$$\lambda_{j_1}^{i_1+p-1}\cdot\lambda_{j_2}^{i_2}=\lambda_{j_1}^{i_1}\cdot\lambda_{j_2}^{i_2+p-1}\quad \text{для любых } \lambda_{j_1},\lambda_{j_2}\in GF(p).$$

Поэтому можно привести подобные в имеющейся какой-то невырожденной N-форме

$$G(\lambda_1,\ldots,\lambda_N)=\sum g\begin{pmatrix} a_i & a_{i+1}\cdots \\ i & i+1\ \ldots \end{pmatrix}\cdot\lambda_i^{a_i}\cdot\lambda_{l+1}^{a_{i+1}}\ldots$$

А именно, каждому моному однозначно соответствует набор тех индексов переменных λ_ℓ, показатели степени у которых ненулевые:

$$\lambda_i^{a_i}\cdot\lambda_j^{a_j}\cdot\lambda_k^{a_k}\cdot\ldots\longrightarrow(i,j,k,\ldots),$$

где $a_i\neq 0,\ a_j\neq 0,\ a_k\neq 0,\ldots$

Каждому набору показателей при этом однозначно ставится в соответствие набор их остатков $(\bar a_i,\bar a_j,\ldots)$ при делении на $p-1$, причем вместо остатка 0 будем писать $p-1$. Справедливо равенство

$$\lambda_i^{a_i}\cdot\lambda_j^{a_j}\cdot\lambda_k^{a_k}\cdot\ldots=\lambda_i^{\bar a_i+m(p-1)}\cdot\lambda_j^{\bar a_j}\cdot\lambda_k^{\bar a_k}\cdot\ldots,$$

где $m(p-1)+\bar a_i+\bar a_j+\ldots=a_i+a_j+\ldots=N$.

Следовательно,

$$\sum g\begin{pmatrix} a_i\ldots a_j\ldots a_k\ldots \\ i\ \ldots\ j\ \ldots\ k\ \ldots \end{pmatrix}\cdot\lambda_i^{a_i}\cdot\lambda_j^{a_j}\cdot\lambda_k^{a_k}\cdot\ \ldots=$$

$$=\left[\sum g\begin{pmatrix} a_i\ldots a_j\ldots a_k\ldots \\ i\ \ldots\ j\ \ldots\ k\ \ldots \end{pmatrix}\right]\cdot\lambda_i^{\bar a_i+m(p-1)}\cdot\lambda_j^{\bar a_j}\cdot\lambda_k^{\bar a_k}\cdot\ldots,$$

где суммирование ведется по всем мономам, соответствующим данному набору остатков $(\bar{a}_i, \bar{a}_j, \bar{a}_k, \dots)$ (и данному набору индексов $(i, j, k, \dots)$).

Остается положить равными нулю все коэффициенты новой формы при мономах, соответствующих данному набору остатков $(\bar{a}_i, \bar{a}_j, \dots)$, кроме одного:

$$f\begin{pmatrix} \bar{a}_i + m(p-1) \dots \bar{a}_j \dots \bar{a}_k \dots \\ i \quad\quad\quad \dots j \dots k \dots \end{pmatrix} = \sum g \begin{pmatrix} a_i \dots a_j \dots a_k \dots \\ i \dots j \dots k \dots \end{pmatrix}.$$

Значения новой формы совпадают со значениями старой при всех значениях аргументов, и поэтому эта новая форма также невырожденна. Она и является искомой.

Лемма 1 доказана.

Далее мы будем считать, что невырожденная N-форма F удовлетворяет лемме 1.

Отметим еще два свойства коэффициентов невырожденной формы F.

Лемма 2. *а) Среди коэффициентов, все показатели которых не превосходят* $p-1$ *, имеются не равные* 0.

б) Для каждого $j=1,2,\dots,N$ *имеет место* $f\begin{pmatrix} N & 0 & \dots & 0 \\ j & j+1 & \dots & N \end{pmatrix} \neq 0.$

Доказательство. Предположим, что утверждение а) не выполняется. Для любых $\lambda_i, \lambda_{i+1}, \dots$ из $GF(p)$ при $a_i \geqslant p$ выполняется тождество

$$\lambda_i^{a_i} \cdot \lambda_{i+1}^{a_{i+1}} \cdot \dots = \lambda_i^{a_i-(p-1)} \cdot \lambda_{i+1}^{a_{i+1}} \cdot \dots$$

Поэтому форма F при всех значениях аргументов равна форме

$$F' = \sum f\begin{pmatrix} a_i & a_{i+1} & \dots \\ i & i+1 & \dots \end{pmatrix} \cdot \lambda_i^{a_i-(p-1)} \cdot \lambda_{i+1}^{a_{i+1}} \cdot \dots$$

степени $N-(p-1)$ от N аргументов. Следовательно, форма F' также невырожденна. Это противоречит теореме Шевалле [12], утверждающей, что над $GF(p)$ не существует невырожденных q-форм от n переменных при $q < n$.

Для доказательства п. б) при заданном j положим $\lambda_i = 0$, если $i \neq j$, а $\lambda_j = 1$. При этих значениях аргументов значение формы F равно $f\begin{pmatrix} N & 0 & \dots & 0 \\ j & j+1 & \dots & N \end{pmatrix}$ и не может равняться нулю в силу невырожденности F.

§ 3. Доказательство теоремы

Группа P, удовлетворяющая заключению теоремы, есть канонический образ группы F из § 1 в фактор-кольце A/Q кольца A по некоторому идеалу Q. Идеал Q задается порождающими элементами, в записи которых участвуют коэффициенты невырожденной N-формы F из § 2. В этом параграфе каждый коэффициент формы F будем считать одним из целых чисел $0,1,2,\dots,p-1$, в соответствии с образом этого числа в $\mathbb{Z}/p\mathbb{Z}\cong GF(p)$. Обозначаться коэффициенты будут теми же буквами.

Идеал Q порождают следующие элементы:

а) все элементы вида $\zeta_m(\ell_1,\ell_2,\dots,\ell_m)$, где ℓ_i - однородные элементы из $\mathcal{L}$, кроме элементов

$$\zeta_{1+k(p-1)}(x_1^{a_1}\dots x_N^{a_N}),\quad \sum a_i=1+k(p-1),\quad k=0,1,\dots,r;$$

б) элементы $\zeta_{1+k(p-1)}(x_1^{a_1}\dots x_N^{a_N})$ при условии, что $f\begin{pmatrix}a_i+m(p-1) & a_{i+1}\dots\\ i & i+1\dots\end{pmatrix}=0$, где a_i - первое ненулевое число среди чисел $a_1,a_2,\dots,a_N$ (здесь $m(p-1)+\sum a_i=1+r(p-1)$);

в) элементы

$$-\frac{px_i}{f\begin{pmatrix}N & 0 & \dots & 0\\ i & i+1 & \dots & N\end{pmatrix}}+\frac{1}{a_j!\cdot a_{j+1}!\cdot\dots}\cdot\frac{1}{f\begin{pmatrix}a_j+m(p-1) & a_{j+1}\dots\\ j & j+1\dots\end{pmatrix}}\cdot\zeta(x_j^{a_j}x_{j+1}^{a_{j+1}}\dots),$$

где индекс i независимо пробегает все числа $1,2,\dots,N$, а числа a_ℓ независимо изменяются от 0 до $p-1$ так, что $a_j>0$, $m(p-1)+\sum a_\ell=N$ при $m<r$ и

$$f\begin{pmatrix}a_j+m(p-1) & a_{j+1} & \dots\\ j & j+1 & \dots\end{pmatrix}\neq 0.$$

Удовлетворяющие условиям п. в) наборы $(a_j a_{j+1}\dots)$ будем называть допустимыми. Отметим, что для допустимого набора $(a_j,a_{j+1},\dots)$, очевидно, $\sum a_i=1+k(p-1)$ для некоторого $k=1,2,\dots,r$.

Сразу отметим некоторые свойства группы P- образа группы F в фактор-кольце A/Q. Так как $\zeta_1(C)=pC$, то по п. а) идеал Q содержит все элементы $p\ell$ для $\ell\in\mathcal{L}^2$. Следовательно, для любого элемента из коммутанта $e(C)\in F'$ справедливо сравнение

$$e(c)^p = e(pc) \equiv 1 \,(mod\, Q).$$

Это означает, что коммутант группы P имеет период p.

С учетом порождающих идеала Q вида в) по лемме 2 получаем, что

$$e(x_i)^p \equiv 1 + c \,(mod\, Q), \quad \text{где} \quad c \in \mathcal{L}^N,$$

для каждого $i = 1, 2, \ldots, N$. Отсюда следует, что группа P/P' - также периода p. Из определения Q ясно, что элементы $x_1, x_2, \ldots$ $\ldots, x_N$ линейно-независимы над $\mathbb{Z}/p\mathbb{Z}$ по модулю $Q + p\mathcal{L}$. Отсюда вытекает, что $|P/P'| = p^N$. Кроме того, ясно, что образ произвольного элемента из F

$$e(x_1)^{\lambda_1} \cdot \ldots \cdot e(x_N)^{\lambda_N} \cdot V_{N+1}^{\lambda_{N+1}} \cdot \ldots \cdot V_T^{\lambda_T} \tag{5}$$

лежит в $\Phi(P) = P'$ тогда и только тогда, когда

$$\lambda_1 \equiv \lambda_2 \equiv \ldots \equiv \lambda_N \equiv 0 \,(mod\, p).$$

Для доказательства теоремы нужно доказать, во-первых, что p-е степени всех элементов из $P \setminus \Phi(P)$ не равны 1 и, во-вторых, что все они лежат в одной и той же подгруппе порядка p.

Предположим, что образ p-й степени некоторого элемента (5) из F равен 1 по модулю Q. Согласно (4) это означает, что

$$\sum \frac{\lambda_1^{a_1} \cdot \ldots \cdot \lambda_T^{a_T}}{a_1! \cdot \ldots \cdot a_T!} \cdot \zeta\left(x_1^{a_1} \ldots x_N^{a_N} v_{N+1}^{a_{N+1}} \ldots v_T^{a_T}\right) = 1 + \sum u v w,$$

где в правой части в каждом слагаемом $u, w \in A$, а v - элемент из пп. а), б) или в). Ввиду п. а) из определения идеала Q, слева можно оставить только те слагаемые, что не лежат в Q:

$$\sum_{k=0}^{r} \sum \frac{\lambda_1^{a_1} \cdot \ldots \cdot \lambda_N^{a_N}}{a_1! \cdot \ldots \cdot a_N!} \cdot \zeta_{1+k(p-1)}\left(x_1^{a_1} \ldots x_N^{a_N}\right) = \sum u v w \tag{6}$$

(здесь учтено также, что $\zeta_0 = 1$).

Идея дальнейших рассуждений состоит в том, чтобы по частям собрать значение невырожденной N-формы F от $\lambda_1, \lambda_2, \ldots, \lambda_N$ и приравнять его нулю по модулю p. Для этого подсчитываются мультиоднородные компоненты суммарной степени $1 + k(p-1)$ для каждого $k = 0, 1, \ldots, r$

в обеих частях равенства (6). Вычисления упрощаются благодаря тому, что подсчет компонент суммарной степени $1+k(p-1)$ ведется по модулю идеала $I_{k(p-1)}$.

Пусть после приведения подобных в правой части (6) через $\alpha(i;a_j,a_{j+1},\dots)$ обозначен (единственный) скалярный коэффициент при элементе $-\dfrac{px_i}{f\binom{N\ \ 0\ \ \dots\ 0}{i\ \ i+1\ \ N}}+\dfrac{1}{a_j!\cdot a_{j+1}!\cdots}\cdot\dfrac{1}{f\binom{a_j+m(p-1)\ \ a_{j+1}\dots}{j\qquad j+1\dots}}\cdot\zeta(x_j^{a_j}x_{j+1}^{a_{j+1}}\dots)$ типа в).

Подсчитаем сначала однородную компоненту степени 1, т.е. рассмотрим случай $k=0$. Для фиксированного j в левой части однородная компонента равна $\lambda_j\cdot\zeta_1(x_j)=\lambda_j px_j$. В правой части в эту компоненту дают вклад только слагаемые вида uvw для v из п. в), причем и u и w должны быть скалярны. Поэтому справедливо равенство

$$p\lambda_j x_j=-\frac{px_j}{f\binom{N\ \ 0\ \ \dots\ 0}{j\ \ j+1\dots N}}\cdot\sum\alpha(j;a_i,a_{i+1},\dots),$$

где справа суммирование ведется по всем допустимым наборам $(a_i, a_{i+1},\dots)$. Отсюда

$$f\binom{N\ \ 0\ \ \dots\ 0}{j\ \ j+1\dots N}\lambda_j=-\sum\alpha(j;a_i,a_{i+1},\dots),$$

а так как $\lambda_j^N=\lambda_j^{1+r(p-1)}\equiv\lambda_j\,(mod\,p)$, то получаем:

$$f\binom{N\ \ 0\ \ \dots\ 0}{j\ \ j+1\dots N}\lambda_j^N\equiv-\sum\alpha(j;a_i,a_{i+1},\dots)(mod\,p).$$

Суммируя теперь по j, получаем слева фрагмент N-формы

$$\sum_j f\binom{N\ \ 0\ \ \dots\ 0}{j\ \ j+1\dots N}\lambda_j^N\equiv-\sum_j\sum\alpha(j;a_i,a_{i+1},\dots)(mod\,p),\tag{7}$$

где справа суммируются коэффициенты $\alpha(j;a_i,a_{i+1},\dots)$ по всем $j=1,2,\dots,N$ и всем допустимым наборам $(a_i,a_{i+1},\dots)$.

Пусть теперь k - любое число из $1,2,\dots,r$, а $(a_j,a_{j+1},\dots)$ - любой допустимый набор, причем $a_j+a_{j+1}+\dots=1+k(p-1)$. Рассмотрим мультиоднородную компоненту правой части равенства (6), отвечающую в левой части слагаемому

$$\frac{\lambda_j^{a_j}\cdot\lambda_{j+1}^{a_{j+1}}\cdots}{a_j!\cdot a_{j+1}!\cdots}\cdot\zeta_{1+k(p-1)}(x_j^{a_j}x_{j+1}^{a_{j+1}}\ldots).$$

Эту компоненту в правой части подсчитаем по модулю идеала $I_{k(p-1)}$. Ясно, что слагаемые $u v w$ для v из п. б) либо лежат в $I_{k(p-1)}$, либо не могут быть той же мультистепени в силу допустимости набора $(a_j, a_{j+1},\ldots)$. Слагаемые $u v w$ для v из п. а), имеющие ту же мультистепень, очевидно, лежат в $I_{k(p-1)}$. Слагаемые $u v w$ для v из п. в) той же мультистепени также лежат в $I_{k(p-1)}$, если только u и w не скалярны. Следовательно, имеет место сравнение

$$\frac{\lambda_j^{a_j}\cdot\lambda_{j+1}^{a_{j+1}}\cdots}{a_j!\cdot a_{j+1}!\cdots}\cdot\zeta_{1+k(p-1)}(x_j^{a_j}x_{j+1}^{a_{j+1}}\ldots)\equiv$$

$$\equiv\frac{1}{a_j!\cdot a_{j+1}!\cdots}\cdot\frac{1}{f\begin{pmatrix}a_j+m(p-1) & a_{j+1}\ldots\\ j & j+1\ldots\end{pmatrix}}\cdot\zeta(x_j^{a_j}x_{j+1}^{a_{j+1}}\ldots)\times$$

$$\times\sum_i\alpha(i;a_j,a_{j+1},\ldots)\ (\mathrm{mod}\ I_{k(p-1)}).$$

Отсюда

$$\left[f\begin{pmatrix}a_j+m(p-1) & a_{j+1}\ldots\\ j & j+1\ldots\end{pmatrix}\lambda_j^{a_j}\lambda_{j+1}^{a_{j+1}}\ldots-\sum_i\alpha(i;a_j,a_{j+1},\ldots)\right]\times$$

$$\times\zeta_{1+k(p-1)}(x_j^{a_j}x_{j+1}^{a_{j+1}}\ldots)\equiv 0\ (\mathrm{mod}\ I_{k(p-1)}).$$

Так как все целые числа, кроме делящихся на p, обратимы в A, то, в силу (3), получаем:

$$f\begin{pmatrix}a_j+m(p-1) & a_{j+1}\ldots\\ j & j+1\ldots\end{pmatrix}\cdot\lambda_j^{a_j}\cdot\lambda_{j+1}^{a_{j+1}}\cdots\equiv\sum_i\alpha(i;a_j,a_{j+1},\ldots)(\mathrm{mod}\,p).$$

С учетом сравнения $\lambda_j^{a_j}\equiv\lambda_j^{a_j+m(p-1)}\ (\mathrm{mod}\,p)$ перепишем в виде

$$f\begin{pmatrix}a_j+m(p-1) & a_{j+1}\ldots\\ j & j+1\ldots\end{pmatrix}\cdot\lambda_j^{a_j+m(p-1)}\cdot\lambda_{j+1}^{a_{j+1}}\cdots\equiv\sum_i\alpha(i;a_j,a_{j+1},\ldots)(\mathrm{mod}\,p).$$

Снова в левой части стоит одно из слагаемых, составляющих значение N-формы $F(\lambda_1,\ldots,\lambda_N)$. Просуммировав последнее сравнение по всем допустимым наборам $(a_j, a_{j+1},\ldots)$, получим справа сумму всех коэффициентов $\alpha(i; a_j, a_{j+1},\ldots)$. Слева же, согласно лемме 1, возникнут, причем ровно по одному разу, все слагаемые N-формы, кроме уже учтенных в (7). Складывая полученное сравнение с (7), получаем

$$F(\lambda_1, \lambda_2, \ldots, \lambda_N) \equiv 0 \pmod p.$$

Ввиду невырожденности формы F отсюда следует, что $\lambda_1 \equiv \lambda_2 \equiv \ldots \ldots \equiv \lambda_N \equiv 0 \pmod p$. Как отмечено выше, это и означает, что любой элемент порядка p из P обязательно лежит в $\Phi(P)=P'=\Omega_1(P)$.

Покажем теперь, что p-е степени всех элементов из P лежат в одной циклической подгруппе порядка p, содержащейся в $Z(P)\cap\Phi(P)$. Напомним, что p-я степень произвольного элемента из F по модулю Q имеет вид

$$1+\sum_{k=0}^{r}\sum \frac{\lambda_1^{a_1}\cdot\ldots\cdot\lambda_N^{a_N}}{a_1!\cdot\ldots\cdot a_N!}\cdot \zeta_{1+k(p-1)}\left(x_1^{a_1}\ldots x_N^{a_N}\right).$$

Элементы типа в) из определения идеала Q позволяют отождествить по модулю Q все элементы вида

$$\zeta_{1+k(p-1)}\left(x_j^{a_j}\ldots x_N^{a_N}\right) \text{ при всех } k=0,1,\ldots,r$$

и всевозможных допустимых наборах $(a_j,\ldots,a_N)$. Для не допустимых наборов $(a_j,\ldots,a_N)$ такие элементы лежат в Q по п. б) определения. Поэтому p-я степень любого элемента из F по модулю Q сравнима с элементом

$$1+\alpha\zeta_N\left(x_j^{a_j}\ldots x_N^{a_N}\right), \quad \sum a_i = N,$$

где α - некоторый скалярный множитель и $(a_j, a_{j+1}\ldots)$ - некоторый фиксированный допустимый набор. Образы всех таких элементов составляют подгруппу порядка p, лежащую в $\gamma_N(P)\cap Z(P)\cap\Phi(P)$.

§ 4. Обобщенная подгруппа Хьюза

Напомним, что, по определению, $H_{p^2}(G)=\langle x\in G \mid x^{p^2}\neq 1\rangle$. В этом параграфе мы докажем следствие 2, т.е. в условиях теоремы построим конечную непримарную группу G, в которой $|G:H_{p^2}(G)| \geq$ $\geq p^{1+\tau(p-1)}$.

Пусть P - конечная p-группа, удовлетворяющая заключению теоремы. Все элементы из $P \setminus \Phi(P)$ имеют нетривиальные p-е степени, лежащие в одной центральной подгруппе Z_1 порядка p. Группа P обладает представлением над конечным полем характеристики, взаимно-простой с p, при котором каждый элемент из $Z_1 \setminus \{1\}$ действует без нетривиальных неподвижных точек. Пусть W - соответствующее векторное пространство. Естественное полупрямое произведение $W \leftthreetimes P$ и является искомой группой G.

Докажем, что все элементы из $WP \setminus W\Phi(P)$ имеют порядок p^2. Тогда, очевидно, получим $H_{p^2}(G) \leq W\Phi(P)$, и

$$|G:H_{p^2}(G)| \geq |WP : W\Phi(P)| \geq p^{1+\tau(p-1)}.$$

Любой элемент $g \in P \setminus \Phi(P)$ действует на W также без нетривиальных неподвижных точек, так как этим свойством обладает g^p.

Поэтому справедливо равенство

$$W = \{w^{-1} \cdot w^g \mid w \in W\}.$$

(Множество в правой части имеет порядок $|W| : |C_W(g)| = |W| : 1$.)

Следовательно, для любых $u \in W$, $g \in P \setminus \Phi(P)$ имеем: $u = w^{-1} w^{-g}$, откуда

$$(ug^{-1})^{p^2} = u \cdot u^g \cdot u^{g^2} \cdot \ldots \cdot u^{g^{p^2-1}} \cdot g^{-p^2} =$$

$$= (w^{-1} w^g) \cdot (w^{-1} w^g)^g \cdot \ldots \cdot (w^{-1} w^g)^{g^{p^2-1}} = 1.$$

Следствие 2 доказано.

Литература

1. N.BLACKBURN, A.ESPUELAS, The power structure of metabelian p-groups, Proc. Amer. Math. Soc., 92, N 4 (1984), 478-484.

2. A.ESPUELAS, On the Hughes problem for exponent p^2, Arch. Math., 43, N 5 (1984), 388-390.

3. T.LAFFEY, The Hughes problem for exponent nine, Math. Proc. Cambridge Phil.Soc., 87 (1980), 393-399.

4. G.E.WALL, On the Lie ring of a group of prime exponent, Proc. Second Int. Conf. Theory Groups, Canberra, 1973, Lect.Notes Math. N 372, Berlin, 1974, 667-690.

5. D.R.HUGHES, J.G.THOMPSON, The H_p-problem and the structure of H_p-groups, Pacif. J. Math., 9 (1959), 1097-1101.

6. M.R.VAUGHAN-LEE, The restricted Burnside problem, Bull. London Math., Soc., 17 (1985), 113-133.

7. G.E.WALL, On the multilinear identities which hold in the Lie ring of a group of prime-power exponent, Preprint, Univ.Sydney, 1985.

8. Е.И.ХУХРО, Новое тождество в кольце Ли свободной группы простого периода, Тезисы 18-й Всесоюзн. алгебраич. конф., часть 2, Кишинёв, 1985, 257.

9. G.E.WALL, On the Lie ring of a group of prime exponent. II, Bull. Austral. Math. Soc., 19, N 1 (1978), 11-28.

10. L.G.KOVÁCS, J.NEUBÜSER, B.H.NEUMANN, On finite groups with «hidden» primes, J.Austral. Math. Soc., 12 (1971), 287-300.

11. G.E.WALL, Secretive prime-power groups of large rank, Bull. Austral. Math. Soc., 12, N 3 (1975), 363-370.

12. C.CHEVALLEY, Démonstration d'une hypothése de M.Artin,, Abh. Math. Sem. Univ. Hamburg, 11 (1936), 73-75.

Поступило 11 октября 1985 г.