S©MR ISSN 1813-3304

СИБИРСКИЕ ЭЛЕКТРОННЫЕ
МАТЕМАТИЧЕСКИЕ ИЗВЕСТИЯ

Siberian Electronic Mathematical Reports
http://semr.math.nsc.ru

Том 15, стр. 1332–1343 (2018) УДК 512.54
DOI 10.17377/semi.2018.15.109 MSC 20B05

О РАНГЕ КОММУТАНТА КОНЕЧНОЙ p-ГРУППЫ, ПОРОЖДЕННОЙ ЭЛЕМЕНТАМИ ПОРЯДКА p ПРИ $p > 2$

Б.М. ВЕРЕТЕННИКОВ

Abstract. All groups in the abstract are finite. We define rank $d(G)$ of a p-group G as the minimal number of generators of G, $d(G) = 0$ if $|G| = 1$. Let p be an odd prime number, n, k be integers, $n \geq 1$, $k \geq 1$. By $M(n, k, p)$ we denote the number of sequences $i_1, \ldots, i_k$ in which $1 \leq i_1 \leq \cdots \leq i_k \leq n$, all members i_j are integers and in which any integer from $[1, n]$ may be present at most $(p-1)$ times. In addition we define $M(n, k, p) = 0$ if $n \leq 0$ or $k < 0$ and $M(n, 0, p) = 1$ if $n \geq 1$. By $C(n, k, p)$ we denote $\sum\limits_{1 \leq i_2 \leq n-1} (M(n-i_2+1, k-2, p) - 2M(n-i_2, k-p-1, p) + M(n-i_2-1, k-2p-1, p))(n-i_2)$. By $D(n, p)$ we denote the following sum: $\sum\limits_{k=2}^{n(p-1)} C(n, k, p)$; $D(1, p) = 0$. We prove that for any p-group G generated by n elements of order $p > 2$, $d(G') \leq D(n, p)$ and that the upper bound is attainable. As an intermediate result we prove that the class of nilpotency of such group G with elementary abelian commutator subgroup does not exceed $n(p-1)$ and this upper bound is also attainable.

Keywords: finite p-group generated by elements of order p, minimal number of generators of commutator subgroup, definition of group by means of generators and defining relations.

1. Введение

А.Д. Устюжанинов в [1] представил список конечных 2-групп, порожденных тремя инволюциями, с элементарным абелевым коммутантом. В частности он отметил, что если G — такая группа, то $d(G') \leq 5$. В продолжение этой темы

Veretennikov, B.M., Rank of commutator subgroup of finite p-group generated by elements of order $p > 2$.

Поступила 4 сентября 2018 г., опубликована 31 октября 2018 г.

Б.М. Веретенников в [2] доказал, что если G — конечная 2-группа, порожденная n инволюциями, где $n \geq 2$, то

$$d(G') \leq \binom{n}{2} + 2\binom{n}{3} + \cdots + (n-1)\binom{n}{n},$$

причем верхняя граница достигается.

В предлагаемой статье доказывается аналогичный результат для конечных p-групп, порожденных элементами порядка p при $p > 2$.

В первом разделе статьи доказывается

Теорема 1. *Если G — конечная p-группа, порожденная n элементами $a_1, \dots, a_n$ порядка p, где $n \geq 2$, $d(G) = n$ и G' — элементарная абелева группа, то G' порождается коммутаторами вида $[a_{i_1}, a_{i_2}, a_{i_3}, \dots, a_{i_k}]$, где $k \geq 2$, $i_1 > i_2$, $i_2 \leq i_3 \leq \cdots \leq i_k$, причем среди индексов $i_1, i_2, \dots, i_k$ нет p-кратных повторений.*

Во втором разделе статьи доказывается

Теорема 2. *Если G — конечная p-группа, $d(G) = n \geq 2$ и G порождается n элементами порядка p, то $d(G') \leq D(n,p)$, где*

$$D(n,p) = \sum_{k=2}^{n(p-1)} C(n,k,p),$$

$$C(n,k,p) = \sum_{1 \leq i_2 \leq n-1} (M(n-i_2+1, k-2, p) - 2M(n-i_2, k-p-1, p) + M(n-i_2-1, k-2p-1, p))(n-i_2),$$

а $M(n,k,p)$ для любых $n, k \geq 2$ означает число возрастающих последовательностей $i_1, i_2, \dots, i_k$, составленных из индексов из $[1, n]$, в которых нет p-кратных повторений.

Кроме того, в этом же разделе получена формула для $M(n,k,p)$. Отметим также, что при $n \leq 0$ и $k < 0$ $M(n,k,p)$ полагаем равным нулю, а $M(n,0,p) = 1$ при $n \geq 1$.

В третьем разделе статьи доказывается

Теорема 3. *Для любого нечетного простого p и любого $n \geq 2$ существует конечная p-группа G, порожденная n элементами порядка p с условием $d(G') = D(n,p)$.*

2. Обозначения и предварительные результаты

Используемые в статье обозначения и понятия являются стандартными (см., например, [3, гл. 1]). В частности, $d(G)$ — минимальное число порождающих группы G, метабелевость группы G означает $G'' = 1$, $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ — биноминальный коэффициент.

В вычислениях мы используем основные коммутаторные тождества

$$[ab, c] = [a, c]^b [b, c], [a, bc] = [a, c][a, b]^c$$

и тождество Витта

$$[a, b, c][b, c, a][c, a, b] = 1,$$

справедливое в любой метабелевой группе.

Кроме того, используем коммутаторное тождество $[t,x]^n = [t^n, x]$ выполняемое для любого целого n в любой метабелевой группе G, где $x \in G$, $t \in G'$.

Отметим также два важных утверждения — это леммы 2 и 4 из [2].

Лемма 1. *Если G — метабелева группа, то для любого $x \in G'$ и любых $y_1, \ldots, y_m$ из G значение коммутатора $[x, y_1, \ldots, y_m]$ не меняется при любой перестановке местами элементов $y_1, \ldots, y_m$ в этом коммутаторе.*

Лемма 2. *Пусть H – конечная группа, заданная образующими $b_1, ..., b_n$ и определяющими соотношениями $w_i(b_1, ..., b_n) = 1$, где $1 \leq i \leq s$. Пусть далее k – натуральное число и группа K задана образующими $b_1, ..., b_n$ и b, определяющими соотношениями группы H и добавленными определяющими соотношениями $b_i^b = v_i(b_1, ..., b_n)$, где $1 \leq i \leq n$, а также $b^k = 1$. Пусть, кроме того, выполнены 3 условия для группы H:*

1) $\langle v_1(b_1, ..., b_n), ..., v_n(b_1, ..., b_n) \rangle = H$,

2) b сохраняет все определяющие соотношения группы H в том смысле, что для любого $i = \overline{1, s}$

$$w_i(v_1(b_1, ..., b_n), .., v_n(b_1, ..., b_n)) = 1$$

– верное равенство в группе H,

3) k-я степень автоморфизма ψ группы H, индуцированного отображением

$$b_i \mapsto v_i(b_1, ..., b_n),$$

где $1 \leq i \leq n$, равна id_H.

Тогда $K = H \leftthreetimes \langle b \rangle$, причем $|b| = k$.

3. Доказательство теоремы 1

Лемма 3. *Пусть k — целое число, $k \geq 2$. Тогда при $1 \leq i \leq k-1$ справедливо равенство:*

$$\binom{i}{i} + \binom{i+1}{i} + \cdots + \binom{k-1}{i} = \binom{k}{i+1}.$$

Доказательство. Сразу отметим, что при любом $k \geq 2$ и при $i = k-1$ равенство в лемме 3 очевидно:

$$\binom{k-1}{k-1} = \binom{k}{k}.$$

При $k = 3$ имеем $i = 1$ и

$$\binom{1}{1} + \binom{2}{1} = \binom{3}{2},$$

а это истинное равенство.

Так что в дальнейшем считаем, что $k > 3$. Обозначим

$$A_i = \binom{i}{i} + \binom{i+1}{i} + \cdots + \binom{k-1}{i}.$$

Если $i = 1$, то

$$A_i = \binom{1}{1} + \binom{2}{1} + \cdots + \binom{k-1}{1} =$$

$$1+2+\dots+(k-1)=\frac{k(k-1)}{2}=\binom{k}{2},$$

что и требовалось.

Если $i>1$, рассмотрим $A_{i-1}+A_i$. Имеем:

$$A_{i-1}+A_i=\binom{i-1}{i-1}+\binom{i}{i-1}+\binom{i+1}{i-1}+\dots+\binom{k-1}{i-1}+$$
$$\binom{i}{i}+\binom{i+1}{i}+\dots+\binom{k-1}{i}=$$
$$\binom{i-1}{i-1}+\left(\binom{i}{i-1}+\binom{i}{i}\right)+$$
$$\left(\binom{i+1}{i-1}+\binom{i+1}{i}\right)+\dots+\left(\binom{k-1}{i-1}+\binom{k-1}{i}\right)=$$
$$\binom{i-1}{i-1}+\binom{i+1}{i}+\binom{i+2}{i}+\dots+\binom{k}{i}=$$
$$1+(A_i-1)+\binom{k}{i}=A_i+\binom{k}{i}.$$

Следовательно, $A_{i-1}=\binom{k}{i}$ и лемма доказана при $1\le i\le k-3$. Однако, при $i=k-2$ имеем

$$\binom{i}{i}+\binom{i+1}{i}=\binom{k-2}{k-2}+\binom{k-1}{k-2}=$$
$$1+(k-1)=k=\binom{k}{k-1}$$

и, значит, лемма 3 доказана полностью. □

Лемма 4. *Пусть G — метабелева группа (конечная или бесконечная). Тогда для любых элементов a, b из G и любого натурального m имеет место следующее равенство:*

$$[a,b,b^m]=[a,b,b]^{\binom{m}{1}}[a,b,b,b]^{\binom{m}{2}}\dots[a,\underbrace{b,\dots,b}_{j}]^{\binom{m}{j-1}}\dots$$
$$[a,\underbrace{b,\dots,b}_{m}]^{\binom{m}{m-1}}[a,\underbrace{b,\dots,b}_{m+1}].$$

Доказательство. Используем индукцию по m. При $m=1$ утверждение леммы тривиально. Пусть лемма доказана при фиксированном $m>1$. Тогда имеем:

$$[a,b,b^{m+1}]=[a,b,b][a,b,b^m]^b=[a,b,b]\Big([a,b,b]^{\binom{m}{1}}\times$$
$$[a,b,b,b]^{\binom{m}{2}}\dots[a,\underbrace{b,\dots,b}_{j}]^{\binom{m}{j-1}}\dots[a,\underbrace{b,\dots,b}_{m}]^{\binom{m}{m-1}}[a,\underbrace{b,\dots,b}_{m+1}]\Big)^b=$$

$$[a,b,b]\Big([a,b,b]^{\binom{m}{1}}[a,b,b,b]^{\binom{m}{2}}\times\cdots\times$$

$$[a,\underbrace{b,\ldots,b}_{j}]^{\binom{m}{j-1}}\ldots[a,\underbrace{b,\ldots,b}_{m}]^{\binom{m}{m-1}}[a,\underbrace{b,\ldots,b}_{m+1}]\Big)\times$$

$$\Big([a,b,b,b]^{\binom{m}{1}}[a,b,b,b,b]^{\binom{m}{2}}\times\cdots\times$$

$$[a,\underbrace{b,\ldots,b}_{j+1}]^{\binom{m}{j-1}}\ldots[a,\underbrace{b,\ldots,b}_{m+1}]^{\binom{m}{m-1}}[a,\underbrace{b,\ldots,b}_{m+2}]\Big)=$$

$$[a,b,b]^{\binom{m+1}{1}}[a,b,b,b]^{\binom{m}{2}+\binom{m}{1}}\times\cdots\times$$

$$[a,\underbrace{b,\ldots,b}_{j}]^{\binom{m}{j-1}+\binom{m}{j-2}}\times\cdots\times$$

$$[a,\underbrace{b,\ldots,b}_{m+1}]^{\binom{m+1}{m}}[a,\underbrace{b,\ldots,b}_{m+2}]=$$

$$[a,b,b]^{\binom{m+1}{1}}[a,b,b,b]^{\binom{m+1}{2}}\times\cdots\times$$

$$[a,\underbrace{b,\ldots,b}_{j}]^{\binom{m+1}{j-1}}\ldots[a,\underbrace{b,\ldots,b}_{m+1}]^{\binom{m+1}{m}}[a,\underbrace{b,\ldots,b}_{m+2}].$$

Таким образом, мы получили соответствующую формулу для $[a,b,b^{m+1}]$, и лемма 4 доказана. □

Лемма 5. *Пусть G — группа (конечная или бесконечная), G' — элементарная абелева группа экспоненты p. Тогда, если $a,b\in G$ и $b^p=1$, то $[a,\underbrace{b,\ldots,b}_{p}]=1$.*

Доказательство. Имеем с учетом леммы 4:

$$1=[a,b^p]=[a,b][a,b]^b\ldots[a,b]^{b^{p-1}}=$$

$$[a,b]^p[a,b,b]\ldots[a,b,b^{p-1}]=$$

$$[a,b,b]\times$$

$$[a,b,b]^{\binom{2}{1}}[a,b,b,b]^{\binom{2}{2}}\times$$

$$[a,b,b]^{\binom{3}{1}}[a,b,b,b]^{\binom{3}{2}}[a,b,b,b,b]^{\binom{3}{3}}\times\cdots\times$$

$$[a,b,b]^{\binom{m}{1}}[a,b,b,b]^{\binom{m}{2}}\dots[a,\underbrace{b,\dots,b}_{m+1}]^{\binom{m}{m}}\times\dots\times$$

$$[a,b,b]^{\binom{p-1}{1}}[a,b,b,b]^{\binom{p-1}{2}}\dots[a,\underbrace{b,\dots,b}_{p}]^{\binom{p-1}{p-1}}=$$

$$[a,b,b]^{\binom{1}{1}+\binom{2}{1}+\dots+\binom{p-1}{1}}\times$$

$$[a,b,b,b]^{\binom{2}{2}+\binom{3}{2}+\dots+\binom{p-1}{2}}\times\dots\times$$

$$[a,\underbrace{b,\dots,b}_{i}]^{\binom{i}{i}+\binom{i+1}{i}+\dots+\binom{p-1}{i}}\times\dots\times$$

$$[a,\underbrace{b,\dots,b}_{p-1}]^{\binom{p-2}{p-2}+\binom{p-1}{p-2}}[a,\underbrace{b,\dots,b}_{p}]=$$

$$\left(\prod_{1\le i\le p-2}[a,\underbrace{b,\dots,b}_{i}]^{\binom{p}{i+1}}\right)[a,\underbrace{b,\dots,b}_{p}]=$$

$$[a,\underbrace{b,\dots,b}_{p}]$$

в силу леммы 3 и того, что $\binom{p}{i+1}$ при любом i от 0 до $p-2$ делится на p. Лемма 5 доказана. □

Доказательство. Теперь мы можем доказать теорему 1. В силу лемм 1 и 5 G' порождается коммутаторами вида:

$$x=[a_{i_1},a_{i_2},\dots,a_{i_k}],$$

где $2\le k\le n(p-1)$, $i_1>i_2$, $i_3\le\dots\le i_k$, причем среди индексов $i_1,\dots,i_k$ нет p-кратных повторений. Если $i_2>i_3$, то

$$[a_{i_1},a_{i_2},a_{i_3}][a_{i_2},a_{i_3},a_{i_1}][a_{i_3},a_{i_1},a_{i_2}]=1,$$

откуда

$$[a_{i_1},a_{i_2},a_{i_3}]=[a_{i_2},a_{i_3},a_{i_1}]^{-1}[a_{i_3},a_{i_1},a_{i_2}]^{-1}=$$
$$[a_{i_1},a_{i_3},a_{i_2}][a_{i_2},a_{i_3},a_{i_1}]^{-1}.$$

Следовательно, снова с учетом леммы 1 получим при $i_2>i_3$:

$$x=[a_{i_1},a_{i_2},\dots,a_{i_k}]=[a_{i_1},a_{i_3},a_{j_3},\dots,a_{j_{k-2}}][a_{i_2},a_{i_3},a_{t_3},\dots,a_{t_{k-2}}]^{-1},$$

где $i_3\le j_3\le\dots\le j_{k-2}$ и $i_3\le t_3\le\dots\le t_{k-2}$. Теорема 1 доказана. □

Следствие 1. *Если конечная p-группа G порождается n элементами порядка p и G' — элементарная абелева группа, то класс нильпотентности G' не превосходит $n(p-1)$.*

4. Доказательство теоремы 2

Лемма 6. *Пусть n, k, p — натуральные числа. Тогда число $M(n,k,p)$ возрастающих последовательностей $i_1,\dots,i_k$ из целых индексов из $[1,n]$ без p-кратных повторений равно*

$$\binom{n+k-1}{k}-\binom{n+k-p-1}{k-p}\binom{n}{1}+\binom{n+k-2p-1}{k-2p}\binom{n}{2}-$$

$$\binom{n+k-3p+1}{k-3p}\binom{n}{3}+\cdots+(-1)^n\binom{n+k-np-1}{k-np}\binom{n}{n}.$$

Доказательство. Ясно, что $M(n,k,p)$ — это число решений уравнения $x_1+\cdots+x_n=k$ в целых числах, удовлетворяющих условию $0\le x_i\le(p-1)$ для любого $i=\overline{1,n}$.

Пусть для любого $i_1\in[1,n]$ $N(i_1)$ — число неотрицательных целых решений уравнения $x_1+\cdots+x_n=k$ с условием $x_{i_1}\ge p$.

Далее, пусть для любых $i_1,i_2(i_1<i_2)$ $N(i_1,i_2)$ — число неотрицательных целых решений уравнения $x_1+\cdots+x_n=k$ с условиями $x_{i_1}\ge p$, $x_{i_2}\ge p$.

Вообще, для любого $m\le n$ и любой последовательности индексов $i_1<i_2<\cdots<i_m$ обозначим $N(i_1,\dots,i_m)$ — число неотрицательных целых решений уравнения $x_1+\cdots+x_n=k$ с условиями $x_{i_1}\ge p,\dots,x_{i_m}\ge p$.

Тогда по принципу включения-исключения

$$M(n,k,p)=N-\sum_{i_1=1}^{n}N(i_1)+\sum_{1\le i_1<i_2\le n}N(i_1,i_2)+\cdots+$$

$$(-1)^m\sum_{1\le i_1<\cdots<i_m\le n}N(i_1,\dots,i_m)+\cdots+(-1)^nN(1,2,\dots,n),$$

где N — число неотрицательных целых решений уравнения

$x_1+\cdots+x_n=k$. Известно, что $N=\binom{n+k-1}{k}$. Аналогично, переходя от уравнения $x_1+\cdots+x_n=k$ к уравнению

$$x_1+\cdots+(x_{i_1}-p)+\cdots+x_n=k-p,$$

получим

$$N(i_1)=\binom{n+k-p-1}{k-p}.$$

Далее, $N(i_1,i_2)$ равно числу неотрицательных целых решений уравнения $y_1+\cdots+y_n=k-2p$, и, вообще, для любого $m\le n$ $N(i_1,\dots,i_m)$ равно числу неотрицательных целых решений уравнения $z_1+\cdots+z_n=k-mp$, то есть $\binom{n+k-mp-1}{k-mp}$. Таким образом, лемма доказана.

□

Лемма 7. *Пусть снова $n \geq k \geq 2$. Тогда при фиксированных индексах $i_1 > i_2$, где $i_1 \leq n$, число последовательностей $i_1, i_2, i_3, \dots, i_k$, где $1 \leq i_2 \leq i_3 \leq \dots \leq i_k \leq n$ без p-кратных повторений равно*

$$M(n - i_2 + 1, k - 2, p) - 2M(n - i_2, k - p - 1, p) + M(n - i_2 - 1, k - 2p - 1, p).$$

Доказательство. Рассматриваемое число последовательностей равно числу возрастающих последовательностей $1 \leq i_3 \leq \dots \leq i_k \leq n$, где $i_2 \leq i_3$, без p-кратных повторений, таких, в которых отсутствуют $(p-1)$-кратные повторения индексов i_1, i_2. Без учета последнего условия таких последовательностей $M(n-i_2+1, k-2, p)$ штук. Число таких последовательностей с учетом условия $(p-1)$-кратного повторения индекса i_1 равно

$$M(n - i_2, (k-2) - (p-1), p) = M(n - i_2, k - p - 1, p).$$

Аналогично, число этих же последовательностей с учетом условия $(p-1)$-кратного повторения индекса i_2 равно $M(n - i_2, k - p - 1, p)$. А число рассматриваемых последовательностей с $(p-1)$-кратным повторением и i_1, и i_2 равно

$$M(n - i_2 - 1, k - 2 - 2(p-1), p) = M(n - i_2 - 1, k - 2p - 1, p).$$

Теперь утверждение леммы становится очевидным. $\square$

Теперь завершим доказательство теоремы 2.

Доказательство. Можно считать, что G' — элементарная абелева p-группа. В силу леммы 7 имеем:

$$C(n,k,p) = \sum_{1 \leq i_2 \leq n-1} \Big(M(n - i_2 + 1, k-2, p) - 2M(n - i_2, k - p - 1, p) + M(n - i_2 - 1, k - 2p - 1, p) \Big)(n - i_2) -$$

число коммутаторов $[a_{i_1}, a_{i_2}, \dots, a_{i_k}]$, где $i_1 > i_2$ и $i_2 \leq \dots \leq i_k$ при фиксированном $k \geq 2$.

Тогда из теоремы 1 следует, что

$$d(G') \leq D(n,p) = \sum_{k=2}^{n(p-1)} C(n,k,p).$$

Теорема 2 доказана. $\square$

5. Доказательство теоремы 3

Лемма 8. *Пусть G — метабелева группа, порожденная элементами $a_1, \dots, a_n$, $n \geq 2$. Индексы $i_1, \dots, i_k$ удовлетворяют условиям: $n \geq i_1 > i_2$, $1 \leq i_2 \leq i_3 \leq \dots \leq i_k \leq n$, где $k \geq 2$. Тогда при $i_2 \leq j \leq n$ имеем*

$$[a_{i_1}, a_{i_2}, \dots, a_{i_k}, a_j] = [a_{i_1}, a_{i_2}, a_{j_3}, \dots, a_{j_{k+1}}],$$

где $j_3 \leq \dots \leq j_{k+1} \leq n$ и последовательность $j_3, \dots, j_{k+1}$ состоит из $i_3, \dots, i_k$ и j, а при $i_2 > j \geq 1$ справедливо равенство

$$[a_{i_1}, a_{i_2}, \dots, a_{i_k}, a_j] = [a_{i_1}, a_j, a_{i_2}, \dots, a_{i_k}][a_{i_2}, a_j, a_{j_3}, \dots, a_{j_{k+1}}]^{-1},$$

где $j \leq j_3 \leq \dots \leq j_{k+1} \leq n$ и последовательность $j_3, \dots, j_{k+1}$ состоит из $i_3, \dots, i_k$ и i_1.

Доказательство. В случае, когда $i_2 \le j$, лемма 8 сразу вытекает из леммы 1.

Если же $i_2 > j$, то снова по лемме 1 имеем

$$[a_{i_1}, a_{i_2}, \dots, a_{i_k}, a_j] = [a_{i_1}, a_{i_2}, a_j, a_{i_3}, \dots, a_{i_k}].$$

Далее из тождества Витта

$$[a_{i_1}, a_{i_2}, a_j][a_{i_2}, a_j, a_{i_1}][a_j, a_{i_1}, a_{i_2}] = 1$$

получаем равенство

$$[a_{i_1}, a_{i_2}, a_j] = [a_j, a_{i_1}, a_{i_2}]^{-1}[a_{i_2}, a_j, a_{i_1}]^{-1} =$$
$$[a_{i_1}, a_j, a_{i_2}][a_{i_2}, a_j, a_{i_1}]^{-1}.$$

Окончательно получаем

$$[a_{i_1}, \dots, a_{i_k}, a_j] = \Big[[a_{i_1}, a_j, a_{i_2}][a_{i_2}, a_j, a_{i_1}]^{-1}, a_{i_3}, \dots, a_{i_k}\Big] =$$
$$[a_{i_1}, a_j, a_{i_2}, a_{i_3}, \dots, a_{i_k}][a_{i_2}, a_j, a_{j_3}, \dots, a_{j_{k+1}}]^{-1},$$

где $j \le j_3 \le \dots \le j_{k+1} \le n$ и последовательность $j_3, \dots, j_{k+1}$ состоит из $i_3, \dots, i_k$ и i_1. Лемма 8 доказана. □

Теперь, ориентируясь на равенства в лемме 8, построим для любого $n \ge 2$ и любого нечетного простого p конечную p-группу G, порожденную n элементами порядка p, с элементарным абелевым коммутантом ранга $D(n,p)$.

Рассмотрим всевозможные символы $a_{i_1 i_2 \dots i_k}$, где $n \ge i_1 > i_2$, $1 \le i_2 \le \dots \le i_k \le n$ и среди индексов $i_1, \dots, i_k$ нет p-кратных повторений. Определим по всем таким символам группу

$$H = \prod \langle a_{i_1 i_2 \dots i_k} \rangle$$

— прямое произведение циклических групп порядка p.

В дальнейшем также будем считать, что $a_{i_1 i_2 \dots i_k} = 1$, если среди индексов $i_1, \dots, i_k$ какой-либо индекс повторяется p раз.

Пусть G_1 — группа, порожденная H и элементом a_1 порядка p, причем к определяющим соотношениям группы H добавлены при $i_2 > 1$ соотношения

$$a_{i_1 i_2 \dots i_k}^{a_1} = a_{i_1 i_2 \dots i_k} a_{i_1, 1, i_2, \dots, i_k} a_{i_2, 1, j_3, \dots, j_{k+1}}^{-1}$$

где $1 \le j_3 \le \dots \le j_{k+1} \le n$ и последовательность $j_3, \dots, j_{k+1}$ состоит из $i_3, \dots, i_k$ и i_1, а также соотношения

$$a_{i_1, 1, i_3, \dots i_k}^{a_1} = a_{i_1, 1, i_3, \dots, i_k} a_{i_1, 1, 1, i_3, \dots, i_k}.$$

Непосредственно проверяется, что

$$a_{i_1, 1, i_3, \dots i_k}^{a_1{}^p} = a_{i_1, 1, i_3, \dots, i_k}.$$

Также легко проверить, что при $i_2 > 1$

$$a_{i_1 i_2 \dots i_k}^{a_1{}^p} = a_{i_1 i_2 \dots i_k}.$$

Таким образом, по лемме 2 имеем:

$$G_1 = H \leftthreetimes \langle a_1 \rangle.$$

Предположим теперь, что при $1 \le m \le n-1$ построена группа

$$G_m = H \leftthreetimes \langle a_1 \rangle \leftthreetimes \dots \leftthreetimes \langle a_m \rangle,$$

где $|a_i| = p$, с дополнительными определяющими соотношениями:

a) при $i_2 \le j \le m$

$$[a_{i_1 i_2 \dots i_k}, a_j] = a_{i_1 i_2 j_3 \dots j_{k+1}},$$

где $j_3 \le \dots \le j_{k+1} \le n$ и последовательность $j_3, \dots, j_{k+1}$ состоит из $i_3, \dots, i_k$ и j;

b) при $i_2 > j$, $j \le m$

$$[a_{i_1 i_2 \dots i_k}, a_j] = a_{i_1 j i_2 \dots i_k} a^{-1}_{i_2 j j_3 \dots j_{k+1}},$$

где $j \le j_3 \le \dots \le j_{k+1} \le n$ и последовательность $j_3, \dots, j_{k+1}$ состоит из $i_3, \dots, i_k$ и i_1.

Пусть теперь $G_{m+1} = \langle G_m, a_{m+1} \rangle$, где к определяющим соотношениям группы G_m добавлены соотношения

a) при $i_2 \le m+1$

$$a^{a_{m+1}}_{i_1 i_2 \dots i_k} = a_{i_1 i_2 \dots i_k} a_{i_1 i_2 j_3 \dots j_{k+1}},$$

где $i_2 \le j_3 \le \dots \le j_{k+1} \le n$ и последовательность $j_3, \dots, j_{k+1}$ состоит из $i_3, \dots, i_k$ и $m+1$;

b) при $i_2 > m+1$

$$a^{a_{m+1}}_{i_1 i_2 \dots i_k} = a_{i_1 i_2 \dots i_k} a_{i_1, m+1, i_2, \dots, i_k} a^{-1}_{i_2, m+1, j_3, \dots, j_{k+1}},$$

где $m+1 \le j_3 \le \dots \le j_{k+1} \le n$ и последовательность $j_3, \dots, j_{k+1}$ состоит из $i_3, \dots, i_k$ и i_1;

c) $a^p_{m+1} = 1$;

d) $a_j^{a_{m+1}} = a_j a^{-1}_{m+1,j}$ при $j \le m$.

Как и выше, легко проверяется

$$a^{a^p_{m+1}}_{i_1 i_2 \dots i_k} = a_{i_1 i_2 \dots i_k},$$

и

$$a_j^{a^p_{m+1}} = a_j.$$

Проверим сохранение определяющих соотношений группы G_m под действием a_{m+1}.

Очевидно, что $\left(a^{a_{m+1}}_{i_1 i_2 \dots i_k}\right)^p = 1$ независимо от последовательности $i_1, \dots, i_k$.

Докажем, что

$$\left(a_j a^{-1}_{m+1,j}\right)^p = 1$$

для любого $j \le m$.

Имеем:

$$\left(a_j a^{-1}_{m+1,j}\right)^2 = a_j a^{-1}_{m+1,j} a_j a^{-1}_{m+1,j} = a_j^2 \left(a^{-1}_{m+1,j}\right)^{a_j} a^{-1}_{m+1,j}.$$

Далее:

$$\left(a_j a^{-1}_{m+1,j}\right)^3 = a_j^2 \left(a^{-1}_{m+1,j}\right)^{a_j} a^{-1}_{m+1,j} a_j a^{-1}_{m+1,j} = a_j^3 \left(a^{-1}_{m+1,j}\right)^{{a_j}^2} \left(a^{-1}_{m+1,j}\right)^{a_j} a^{-1}_{m+1,j}$$

и т.д.

В итоге получим:

$$\left(a_j a^{-1}_{m+1,j}\right)^p = a_j^p \left(a^{-1}_{m+1,j}\right)^{{a_j}^{p-1}} \left(a^{-1}_{m+1,j}\right)^{{a_j}^{p-2}} \dots a^{-1}_{m+1,j} =$$

$$a_j^p \left(a_{m+1,j} a^{a_j}_{m+1,j} \dots a^{a_j^{p-1}}_{m+1,j}\right)^{-1}.$$

То, что выражение в скобках равно 1, доказывается так же, как и лемма 5. Таким образом,

$$\left(a_j a_{m+1,j}^{-1}\right)^p = 1,$$

что и требовалось.

Теперь при $i_2 \le j \le m$ проверим сохранение под действием a_{m+1} равенства

$$a_{i_1 i_2 \dots i_k}^{a_j} = a_{i_1 i_2 \dots i_k} a_{i_1 i_2 j_3 \dots j_{k+1}},$$

где $i_1 > i_2$, $i_2 \le \dots \le i_k$, $j_3 \le \dots \le j_{k+1}$ и последовательность индексов $j_3, \dots, j_{k+1}$ состоит из $i_3, \dots, i_k$ и j.

Таким образом, проверяем истинность в G_m при данных условиях равенства

$$\left(a_{i_1 i_2 \dots i_k}^{a_{m+1}}\right)^{a_j^{a_{m+1}}} = a_{i_1 i_2 \dots i_k}^{a_{m+1}} a_{i_1 i_2 j_3 \dots j_{k+1}}^{a_{m+1}}. \tag{1}$$

Заметим прежде всего, что неравенство $i_2 \le j \le m$ влечет неравенство $i_2 < m+1$.

Преобразуем параллельно обе части равенства (1). Имеем:

$$\left(a_{i_1 i_2 \dots i_k} a_{i_1 i_2 p_3 \dots p_{k+1}}\right)^{a_j^{a_{m+1}}} = a_{i_1 i_2 \dots i_k} a_{i_1 i_2 p_3 \dots p_{k+1}} a_{i_1 i_2 j_3 \dots j_{k+1}} a_{i_1 i_2 j_3^{(2)} \dots j_{k+2}^{(2)}}, \tag{2}$$

где $p_3 \le \dots \le p_{k+1}$ и последовательность $p_3, \dots, p_{k+1}$ состоит из $i_3, \dots, i_k$ и $m+1$, $j_3^{(2)} \le \dots \le j_{k+2}^{(2)}$ и последовательность $j_3^{(2)}, \dots, j_{k+2}^{(2)}$ состоит из $i_3, \dots, i_k, j$ и $m+1$,

Преобразуя далее только левую часть равенства (2) получим:

$$a_{i_1 i_2 \dots i_k} a_{i_1 i_2 j_3 \dots j_{k+1}} a_{i_1 i_2 p_3 \dots p_{k+1}} a_{i_1 i_2 p_3^{(2)} \dots p_{k+1}^{(2)}} =$$
$$a_{i_1 i_2 \dots i_k} a_{i_1 i_2 p_3 \dots p_{k+1}} a_{i_1 i_2 j_3 \dots j_{k+1}} a_{i_1 i_2 j_3^{(2)} \dots j_{k+1}^{(2)}}, \tag{3}$$

где $p_3^{(2)} \le \dots \le p_{k+2}^{(2)}$ и последовательность $p_3^{(2)}, \dots, p_{k+2}^{(2)}$ состоит из $p_3, \dots, p_{k+1}$ и j, т.е. из $i_3, \dots, i_k, m+1$ и j.

Следовательно, (1) равносильно истинному равенству (3) в группе G_m, что и требовалось.

Далее, при $i_2 > j$, $j \le m$, $i_2 \le m+1$ под действием a_{m+1} проверим сохранение равенства

$$a_{i_1 i_2 \dots i_k}^{a_j} = a_{i_1 i_2 \dots i_k} a_{i_1, j, i_2, \dots, i_k} a_{i_2, j, j_3, \dots j_{k+1}}^{-1}, \tag{4}$$

где $j_3 \le \dots \le j_{k+1}$ и последовательность $j_3, \dots, j_{k+1}$ состоит из $i_3, \dots, i_k$ и i_1.

Таким образом, при данных условиях нужно доказать справедливость следующего равенства в группе G_m:

$$\left(a_{i_1 i_2 \dots i_k}^{a_{m+1}}\right)^{a_j} = a_{i_1 i_2 \dots i_k}^{a_{m+1}} a_{i_1, j, i_2, \dots, i_k}^{a_{m+1}} \left(a_{i_2, j, j_3, \dots, j_{k+1}^{a_{m+1}}}\right)^{-1}. \tag{5}$$

Левая часть равенства (5) равна

$$\left(a_{i_1 i_2 \dots i_k} a_{i_1 i_2 p_3 \dots p_{k+1}}\right)^{a_j} =$$

$$a_{i_1 i_2 \dots i_k} a_{i_1, j, i_2, \dots, i_k} a_{i_2, j, j_3, \dots, j_{k+1}}^{-1} a_{i_1 i_2 p_3 \dots p_{k+1}} a_{i_1, j, i_2, p_3, \dots, p_{k+1}} a_{i_2, j, p_3^{(2)}, \dots, p_{k+2}^{(2)}}^{-1},$$

где $p_3 \le \dots \le p_{k+1}$ и последовательность $p_3, \dots, p_{k+1}$ состоит из $i_3, \dots, i_k$ и $m+1$, $p_3^{(2)} \le \dots \le p_{k+2}^{(2)}$ и последовательность $p_3^{(2)}, \dots, p_{k+2}^{(2)}$ состоит из $p_3, \dots, p_{k+1}$ и i_1, т.е. из $i_3, \dots, i_k, m+1$ и i_1.

Правая часть равенства (5) равна

$$a_{i_1 i_2 \ldots i_k} a_{i_1 i_2 p_3 \ldots p_{k+1}} a_{i_1, j, i_2, \ldots, i_k} a_{i_1, j, i_2^{(2)}, \ldots, i_{k+1}^{(2)}} a^{-1}_{i_2, j, j_3, \ldots, j_{k+1}} a^{-1}_{i_2, j, j_3^{(2)}, \ldots, j_{k+2}^{(2)}},$$

где $i_2^{(2)} \leq \cdots \leq i_{k+1}^{(2)}$ и последовательность $i_2^{(2)}, \ldots, i_{k+1}^{(2)}$ состоит из $i_2, \ldots, i_k$ и $m+1$, $j_3^{(2)} \leq \cdots \leq j_{k+2}^{(2)}$ и последовательность $j_3^{(2)}, \ldots, j_{k+2}^{(2)}$ состоит из $j_3, \ldots, j_{k+1}$ и $m+1$, т.е. из $i_3, \ldots, i_k, i_1$ и $m+1$.

Таким образом, преобразованные левые и правые части равенства (5) имеют по 6 сомножителей, причем 1-й множитель в левой части равен первому множителю правой части, 2-й множитель левой части равен 3-му множителю правой части, 3-й множитель левой части равен 5-му множителю правой части, 4-й множитель левой части равен 2-му множителю правой части, 5-й множитель левой части равен 4-му множителю правой части и 6-й множитель левой части равен 6-му множителю правой части. Следовательно, равенство (5) является истинным в G_m. Значит, равенство (4) сохраняется под действием a_{m+1} при $i_2 \leq m+1$.

Проверка сохранения равенства (4) под действием a_{m+1} при условии $i_2 > m+1$ осуществляется аналогично.

Теперь по лемме 2

$$G_{m+1} = G_m \leftthreetimes \langle a_{m+1} \rangle.$$

На n-м шаге получим группу

$$G_n = H \leftthreetimes \langle a_1 \rangle \leftthreetimes \cdots \leftthreetimes \langle a_n \rangle,$$

порожденную элементами $a_1, \ldots, a_n$ порядка p с элементарным абелевым коммутантом H ранга $D(n, p)$, что и требовалось.

В заключение заметим, что точную оценку ранга $d(G')$ для конечной 2-порожденной p-группы G, не обязательно порожденной двумя элементами порядка p, получил Н. Блэкберн в [4].

References

[1] A.D. Ustyuzhaninov, *Finite 2-groups generated by exactly three involutions*, In: All-union algebr. symposium (1975) (in Russian), abstracts, part I, Gomel, (1975), 72.

[2] B.M. Veretennikov, *On the commutator subgroups of finite 2-groups generated by involutions*, Trudy Inst. Mat. i Mekh. UrO RAN, **23**:4 (2017), 77–84 (in Russian). MR3758048

[3] M.I. Kargapolov, J.I. Merzljakov *Fundamentals of the Theory of Groups*, New York–Berlin: Springer-Verlag, 1979. MR0551207

[4] N. Blackburn, *On prime-power groups with two generators*, Mathematical Proceedings of the Cambridge Philosophical Society, **54**:3 (1958), 327–337. MR0102557

Boris Michailovich Veretennikov
Ural Federal University,
19 Mira street,
620002 Ekaterinburg, Russia
E-mail address: boris@veretennikov.ru