

О структуре сплетения двух циклических групп порядков степеней простого числа.

П. Лакатош (Дебрецен*)

§ 1. Введение.

Уже в работе Г. Поя [6] (1937) встречается понятие сплетения, однако, на значимость этого понятия для теории групп впервые указал Л. Калужин. В работе [3] он доказал, что силовские p -подгруппы симметрической группы p^n -ой (p -простое число) степени являются сплетением n -циклических групп простого порядка p . Он же описал [4] характеристические подгруппы этих групп, а А. Вейр [5] — их абелевы нормальные делители. К. Бузаши, развивая направление изучения этих структур, в [2] определил нормальные делители упомянутых групп (1969).

Настоящая работа продолжает структурные исследования Л. Калужнина, А. Вейра и К. Бузаши и использует их методы.

Факт медленного рождения предшествующих результатов указывает на сложность темы; даже такой простой случай, каким занимаемся мы в этой работе, до сих пор не рассматривался в литературе, несмотря на многочисленные статьи о сплетениях, которые появляются каждый год.

Напомним интересные для нас результаты о нильпотентных сплетениях. Х. Либек [7] определил класс нильпотентности сплетения группы A с показателем p^n (p -простое) с конечной абелевой p -группой. В случае, когда A циклическая p -группа, а B конечная абелева p -группа, А. Мельдрум решил вопрос о принадлежности выбранного элемента базиса их сплетения некоторому члену верхнего центрального ряда сплетения.

В предлагаемой работе рассматривается сплетение циклической группы A порядка p^n с циклической группой B порядка p^m , где p -простое число, n и m -произвольные натуральные числа.

Во втором параграфе статьи дается анализ общих свойств рассматриваемой группы W . Определяется центр группы, дается один удобный для дальнейших исследований базис для коммутанта группы. Описываются некоммутативные члены верхнего центрального ряда группы, причем, как следствие, получается длина центрального ряда.

*) Piroska Lakatos (Debrecen).

В третьем параграфе сначала рассматривается случай $n=1$. Оказывается, что верхний и нижний центральные ряды в этом случае совпадают. В этом случае, и позже, в случае $m=1$, определяются все члены нижнего и верхнего центральных рядов и удобный базис в них.

§ 2

1. Сначала напомним некоторые известные свойства сплетения.

Пусть $A = \{a\}$ и $B = \{b\}$ циклические группы, порожденные элементами a и b , порядка p^n и p^m (в дальнейшем число p везде произвольное фиксированное простое, а n и m произвольные натуральные числа).

Пусть далее A_i ($i=1, 2, \dots, p^m$)-группы, изоморфные с A (с изоморфизмом $a \rightarrow a(b^i) = a_i$).

Обозначим

$$(2.1) \quad K = \bigcup_{b^i \in B} A_i.$$

Сплетением W группы A с группой B назовем расщепляющееся расширение группы K при помощи B , в котором элементы из B индуцируют автоморфизмы в K по закону

$$(2.2) \quad b^{-1}a_i b = a_{i+1} \quad (i+1 \text{ приводится по модулю } p^m).$$

Очевидно, группа K является максимальным нормальным делителем в группе W и порядок W равен $p^{n \cdot p^m + m}$.

Сплетение группы A с B будем обозначать через $A \text{ wt } B = W$. В дальнейшем буквы A, A_i, B, K, W, a, b, n и m везде обозначают определенные тут группы, элементы и числа. Коммутатор двух элементов x и y будем обозначать символом $[x, y]$, k -тый член нижнего центрального ряда группы W как W_k , а для k -го члена верхнего центрального ряда зафиксируем обозначение Z_k . Порядок произвольной группы G обозначим $|G|$. Напомним полезные соотношения коммутаторов в группе W , проверяемые непосредственно:

пусть $k, k' \in K, \omega \in W$ произвольные элементы, тогда

$$(2.3) \quad [k, \omega k'] = [k, \omega],$$

$$(2.4) \quad [\omega, k \cdot k'] = [\omega, k][\omega, k'],$$

$$(2.5) \quad [b^i, a_i] = a_{i+1}^{-1} \cdot a_i = [a_i^{-1}, b^i],$$

$$(2.6) \quad [b^i, a_i] = [b, a_i][b, a_{i+1}] \cdot \dots \cdot [b, a_{i+i-1}],$$

$$(2.7) \quad [k, b^i, b^i] = [k, b^i, b^i],$$

(где индексы элементов a_j приводятся по модулю p^m).

Часто будем пользоваться следующими полезными двойственными свойствами (см. [2]).

В обозначениях $\alpha_1 = a_1$, $\alpha_j = [b, \alpha_{j-1}]$, ($j=2, \dots, p^m$)

$$(2.8) \quad \alpha_i = \prod_{v=1}^i a_v^{(-1)^{v-1} C_{i-1}^{v-1}}, \quad i = 1, 2, \dots, p^m$$

$$(2.9) \quad a_i = \prod_{v=1}^i \alpha_v^{(-1)^{v-1} C_{i-1}^{v-1}},$$

где C_{i-1}^{v-1} -биномиальные коэффициенты.

2. Легко доказать с помощью соотношений (2.3); (2.4) и (2.5) следующие важные теоремы:

Теорема 2.1. Группа $W_1 = [b, K] \subseteq K$.

Теорема 2.2. Центр Z_1 группы W является циклической группой, порожденной элементом $z = a_1 \cdot a_2 \cdot \dots \cdot a_{p^m}$ порядка p^n .

Лемма 2.3. Пусть φ такое отображение группы K на себя, что $\varphi(k) = [b, k]$ для любого $k \in K$.

Тогда φ является эндоморфизмом группы K , ядром которого является центр группы W .

Доказательство. По (2.4) для каждого $k, k' \in K$

$$\varphi(k \cdot k') = [b, k \cdot k'] = [b, k][b, k'] = \varphi(k) \cdot \varphi(k'),$$

причем для элемента $k \in K$ ядра ψ выполняется $[b, k] = e$, поэтому $k \in Z_1$, и $\varphi^{-1}(e) = Z_1$.

Теорема 2.4. Система элементов $[b, a_i] = \beta_i$, ($i=1, 2, \dots, p^m-1$) образует базис группы W_1 , откуда $|W/W_1| = p^{n+m}$.

Доказательство. Взаимный коммутант $W_1 = [b, K]$ порождается взаимными коммутаторами порождающих элементов группы W , поэтому группа $[b, K]$ порождается системой элементов

$$\beta_i = [b, a_i] = a_{i+1}^{-1} \cdot a_i \quad (i = 1, 2, \dots, p^m; i+1 \text{ приводится по модулю } p^m).$$

Однако

$$\beta_1 \cdot \beta_2 \cdot \dots \cdot \beta_{p^m-1} = \beta_{p^m}^{-1},$$

поэтому элементы $\beta_1, \beta_2, \dots, \beta_{p^m-1}$ уже порождают группу W_1 . Порядок группы $[b, K] = \varphi(K)$, согласно лемме 2.3, равен $p^{n(p^m-1)}$ (так как порядок ядра эндоморфизма, по теореме 2.2, равен p^n), и значит элементы $\beta_1, \beta_2, \dots, \beta_{p^m-1}$ определяют минимальную «линейно независимую» систему образующих в группе W_1 .

Лемма 2.5. Пусть элементы $\beta_v = a_{v+1}^{-1} \cdot a_v$ ($v=1, 2, \dots, p^m-1$), $\alpha_1 = a_1$, $\alpha_i = [b, \alpha_{i-1}]$ ($i=2, 3, \dots, p^m$). Тогда α_i и β_v могут быть представлены в виде

$$(2.10) \quad \alpha_i = \prod_{v=1}^{i-1} \beta_v^{(-1)^{v-1} C_{i-2}^{v-1}}, \quad (i=2, 3, \dots, p^m)$$

$$(2.11) \quad \beta_v = \prod_{i=1}^{v+1} \alpha_i^{(-1)^i C_{v-1}^{i-2}}, \quad (v=1, 2, \dots, p^m-1).$$

Доказательство. Согласно формуле (2.9)

$$\begin{aligned} \beta_v &= a_{v+1}^{-1} \cdot a_v = \prod_{i=1}^{v+1} \alpha_i^{(-1)^i C_v^{i-1}} \cdot \prod_{i=1}^v \alpha_i^{(-1)^{v-1} C_{v-1}^{i-1}} = \prod_{i=1}^v \alpha_i^{(-1)^i (C_v^{i-1} - C_{v-1}^{i-1})} \cdot \alpha_{v+1}^{(-1)^{v+1} \cdot C_v^v} = \\ &= \prod_{i=2}^v \alpha_i^{(-1)^i C_{v-1}^{i-2}} \cdot \alpha_{v+1}^{(-1)^{v+1} C_{v-1}^{v-1}} = \prod_{i=2}^{v+1} \alpha_i^{(-1)^i \cdot C_{v-1}^{i-2}}. \end{aligned}$$

Мы получили соотношение (2.11). Также по формуле (2.8)

$$\begin{aligned} \alpha_i &= \prod_{v=1}^i a_v^{(-1)^{v-1} C_{i-1}^{v-1}} = a_1 \prod_{v=2}^i a_v^{(-1)^{v-1} (C_{i-2}^{v-2} + C_{i-2}^{v-1})} = \\ &= a_1 \cdot a_2^{-1} \cdot \prod_{v=2}^{i-1} a_v^{(-1)^{v-1} C_{i-2}^{v-1}} \cdot \prod_{v=2}^{i-1} a_{v+1}^{(-1)^v C_{i-2}^{v-1}} = \prod_{v=1}^{i-1} \beta_v^{(-1)^{v-1} C_{i-2}^{v-1}}. \end{aligned}$$

Замечание. Символы β_v и α_i будут обозначать в дальнейшем элементы, введенные в предыдущей лемме.

Теорема 2.6. Элементы $\alpha_2, \alpha_3, \dots, \alpha_{p^m}$ образуют базис группы W_1 .

Доказательство. Согласно теореме 2.4 элементы β_v ($v=1, 2, \dots, p^m-1$) образуют базис группы W_1 . Эти элементы можно выразить по соотношению (2.11) с помощью элементов α_i ($i=2, 3, \dots, p^m$). Таким образом теорема доказана.

Лемма 2.7. Пусть p простое и k целое число, которое записывается в виде

$$k = k_1 \cdot p^{l-1} + k_2 \cdot p^{l-2} + \dots + k_{l-1} \cdot p + k_l, \quad (k_i < p; i=1, 2, \dots, l).$$

Если $p^s \parallel k$, но $p^{s+1} \nparallel k$ для некоторого s , то $p^{l-s} \parallel C_{p^l}^k$, но $p^{l-s+1} \nparallel C_{p^l}^k$.

Доказательство. Очевидно в этом случае

$$* \quad C_{p^l}^k = \frac{p^l \cdot (p^l - 1) \cdot \dots \cdot (p^l - (k-1))}{k \cdot 1 \cdot \dots \cdot k-1} \quad \text{и} \quad k \equiv p^l.$$

Для любого числа $1 \leq \alpha \leq k-1$ и j $p^j \parallel d$ тогда и только тогда, если $p^j \parallel p^l - d$, что доказывает лемму.

Лемма 2.8. Для элемента $z = a_1 \cdot a_2 \cdot \dots \cdot a_{p^m}$ центра Z_1

$$(2.12) \quad z = \prod_{v=1}^{p^m} \alpha_v^{(-1)^{v-1} C_{p^m}^v}.$$

Доказательство. Легко проверяется, что

$$a_1^{p^m-1} \cdot a_2^{-1} \cdot a_3^{-1} \cdot \dots \cdot a_{p^m}^{-1} = \beta_1^{p^m-1} \cdot \beta_2^{p^m-2} \cdot \dots \cdot \beta_{p^m-2}^2 \cdot \beta_{p^m-1} = z^{-1} \cdot \alpha_1^{p^m}.$$

Отсюда, используя соотношение (2.11) и свойства биномиальных коэффициентов,

$$\begin{aligned} z^{-1} \cdot \alpha_1^{p^m} &= \alpha_2^{p^m-1} \cdot \alpha_2^{\binom{1}{0}(p^m-2)} \cdot \alpha_3^{-\binom{1}{1}(p^m-2)} \cdot \alpha_2^{\binom{2}{0}(p^m-3)} \cdot \alpha_3^{-\binom{2}{1}(p^m-3)} \cdot \\ &\quad \cdot \alpha_4^{\binom{2}{2}(p^m-3)} \cdot \dots \cdot \alpha_2^{\binom{p^m-2}{0}} \cdot \alpha_3^{-\binom{p^m-2}{1}} \cdot \dots \cdot \alpha_{p^m-1}^{-\binom{p^m-2}{p^m-3}} \cdot \alpha_{p^m}^{\binom{p^m-2}{p^m-2}} = \\ &= \alpha_2^{\sum_{i=0}^{p^m-2} \binom{i}{0} + \sum_{i=0}^{p^m-3} \binom{i}{1} + \dots + \sum_{i=0}^1 \binom{i}{0} + \binom{0}{0}} \cdot \alpha_3^{-\left(\sum_{i=1}^{p^m-2} \binom{i}{1} + \sum_{i=1}^{p^m-3} \binom{i}{2} + \dots + \sum_{i=1}^2 \binom{i}{1} + \binom{1}{1}\right)} \cdot \\ &\quad \cdot \dots \cdot \alpha_{p^m-1}^{\sum_{i=p^m-3}^{p^m-2} \binom{i}{p^m-3} + \binom{p^m-3}{p^m-3}} \cdot \alpha_{p^m}^{-\binom{p^m-2}{p^m-2}} = \alpha_2^{\sum_{i=1}^{p^m-1} \binom{i}{1}} \cdot \alpha_3^{-\sum_{i=2}^{p^m-2} \binom{i}{2}} \cdot \dots \cdot \alpha_{p^m-1}^{\sum_{i=p^m-2}^{p^m-1} \binom{i}{p^m-2}} \cdot \\ &\quad \cdot \alpha_{p^m}^{-\binom{p^m}{p^m}} = \alpha_2^{\binom{p^m}{2}} \cdot \alpha_3^{-\binom{p^m}{3}} \cdot \dots \cdot \alpha_{p^m-1}^{\binom{p^m}{p^m-1}} \cdot \alpha_{p^m}^{-\binom{p^m}{p^m}} = \prod_{v=2}^{p^m} \alpha_v^{(-1)^v \cdot C_{p^m}^v}. \end{aligned}$$

Отсюда следует

$$z = \prod_{v=1}^{p^m} \alpha_v^{(-1)^{v-1} C_{p^m}^v},$$

что и требовалось доказать.

Лемма 2.9. Для фиксированного целого числа $0 \leq k \leq m$ обозначим через $\bar{A}_k$ подгруппу W , порожденную элементами

$$a_i \cdot a_{p^k+i}^{-1} \quad (i = 1, 2, \dots, p^m - p^k; \quad 0 \leq k \leq m-1).$$

Элемент вида

$$(*) \quad c = a_1^{\gamma_1} \cdot a_2^{\gamma_2} \cdot \dots \cdot a_{p^m}^{\gamma_{p^m}}, \quad c \in K$$

тогда и только тогда содержится в $\bar{A}_k$, когда

$$\gamma_i + \gamma_{p^k+i} + \dots + \gamma_{p^m-p^k+i} \equiv 0 \pmod{p^n}$$

для всех $1 \leq i \leq p^k$.

(Это свойство элемента $c \in K$ в дальнейшем будем называть T_k -свойством.)

Доказательство. Покажем сначала для $k=0$, что такие и только такие элементы содержатся в группе $\bar{A}_0 = W_1$, для которых $\sum_{i=1}^{p^m} \gamma_i \equiv 0 \pmod{p^n}$. Очевидно (по теореме 2.4), что при представлении $(*)$ элементов группы W_1 сумма показателей делится на p^n .

По предыдущему в группе K по крайней мере $p^{n(p^m-1)}$ элементов (каков порядок группы W_1) обладает свойством T_0 . Пусть далее c и c' — произвольные различные элементы группы K вида

$$c = a_1^{\gamma_1} \cdot a_2^{\gamma_2} \cdot \dots \cdot a_{p^m}^{\gamma_{p^m}} \quad \text{и} \quad c' = a_1^{\gamma'_1} \cdot a_2^{\gamma'_2} \cdot \dots \cdot a_{p^m}^{\gamma'_{p^m}},$$

где $\sum_{i=1}^{p^m} \gamma_i$ и $\sum_{i=1}^{p^m} \gamma'_i$ делятся на p^n .

Будем прибавлять к показателям γ_1 и γ'_1 по порядку число $1 \leq i < p^n$. Так полученные элементы обозначим через c_1^i и $c_1'^i$. Очевидно, суммы показателей степеней c_1^i и $c_1'^i$ сравнимы с числом i по модулю p^n .

Если $c \neq c'$, тогда $c_1^i \neq c_1'^i$, в противном случае $\gamma_{1-i} \equiv \gamma'_1 + i$ и $\gamma_j \equiv \gamma'_j \pmod{p^n}$ были бы справедливы для $j=2, 3, \dots, p^n$ и $1 \leq i < p^n$, в противоречии с нашими условиями $c \neq c'$. Таким образом элементы группы K , распадаются на p^n классов, причем содержание класса зависит от того, какое число $1 \leq i \equiv p^n$ прибавили мы к показателям γ_1 и γ'_1 .

Отсюда, используя, что $|K| = p^{n \cdot p^m}$, получим, что точно $p^{n(p^m-1)}$ элементов обладает свойством T_0 .

Аналогичным образом доказывается утверждение при $k \neq 0$ (с помощью выбора подходящего сплетения $\text{Awg}\{b^{p^{n-k}}\}$). Лемма доказана.

Лемма 2.10. $z^{p^{n-i}} \in \bar{A}_{m-i}$, причем $z^{p^{n-i-1}} \notin \bar{A}_{m-i}$ ($i=1, 2, \dots, m$), где группы $\bar{A}_{m-1}$ введены в лемме 2.9.

Доказательство. Легко проверяется, что элемент $z^{p^{n-i}} = \prod_{j=1}^{p^n} a_j^{p^{n-i}}$ обладает свойством T_{m-i} , и элемент $z^{p^{n-i-1}}$ не обладает этим свойством.

Лемма 2.11. Пусть $\bar{A}_{m-1} = {}^0\bar{A}_{m-1}$ и пусть

$$[W, {}^0\bar{A}_{m-1}] = {}^1\bar{A}_{m-1}, \quad [W, {}^{i-1}\bar{A}_{m-1}] = {}^i\bar{A}_{m-1}.$$

Тогда ${}^{s-1}\bar{A}_{m-1} \neq \{e\}$, причем ${}^s\bar{A}_{m-1} = \{e\}$, где $s = n(p^m - p^{m-1})$.

Доказательство. Легко проверяется (по соотношениям (2.3) и (2.4)), что

$${}^i\bar{A}_{m-1} = \varphi({}^{i-1}\bar{A}_{m-1}),$$

где отображение φ является эндоморфизмом группы K (по лемме 2.3).

Ядро этого эндоморфизма группы ${}^{i-1}\bar{A}_{m-1}$ по лемме 2.10 содержит подгруппу порядка p для всех $i=1, 2, \dots, s-1$, где $s = n(p^m - p^{m-1})$. Так как $|\bar{A}_{m-1}| = p^{n(p^m - p^{m-1})} = p^s$, то $|{}^{s-1}\bar{A}_{m-1}| = p$, а $|{}^s\bar{A}_{m-1}| = 1$. Лемма доказана.

Так как по предыдущей лемме для всех элементов $\bar{a}_{m-1} \in \bar{A}_{m-1} \subset K$ каждый s -ый коммутатор с элементом b равен единице, верно.

Следствие 2.12.

$$\bar{A}_{m-1} \subseteq Z_{n(p^m - p^{m-1})}.$$

Лемма 2.13. Пусть *A_k группа, порожденная элементами

$${}^*a_i^{(k)} = a_i \cdot a_{p^k+i} \cdot \dots \cdot a_{p^m-p^k+i} \quad (i = 1, 2, \dots, p^k; 0 \leq k \leq m-1)$$

и

$${}^*A_k = {}^*_0A_k, \quad {}^*_1A_k = [W, {}^*_0A_k], \quad {}^*_iA_k = [W, {}^*_{i-1}A_k].$$

Тогда

$${}^*A_k \subseteq Z_{n \cdot p^k}.$$

Доказательство. Очевидно, что элементы ${}^*a_i^{(k)}$, $(i=1, 2, \dots, p^k)$, образуют базис группы, введенной в лемме. То по выбору чисел k , $|{}^*A_k| = p^k \cdot p^n$. Аналогично доказательству леммы 2.11 рассмотрим взаимные коммутанты

$$[W, {}^*A_k] = {}^*_1A_k, \quad [W, {}^*_{i-1}A_k] = {}^*_iA_k.$$

При помощи эндоморфизма φ группы K (${}^*A_k \subset K$) можно получить, что $\varphi^{k \cdot p^n}({}^*A_k) = \{e\}$, и таким же образом

$${}^*A_k \subseteq Z_{n \cdot p^k},$$

ведь группы *_iA_k содержат подгруппу центра, по крайней мере порядка p .

Теорема 2.14.

$$\{b^{p^k}\} \subset Z_{s+p^{m-1}-p^k+1},$$

причем

$$\{b^{p^k}\} \not\subseteq Z_{s+p^{m-1}-p^k}, \quad \text{где } 0 \leq k < m, \quad s = n(p^m - p^{m-1}).$$

Доказательство. По следствию 2.12 и лемме 2.13 легко видеть, что ${}^*A_{m-1} \cdot \bar{A}_{m-1} \subseteq Z_s$, ведь $n(p^m - p^{m-1}) \equiv n \cdot p^{m-1}$.

Тогда $\alpha_1^p \in {}^*A_{m-1} \cdot \bar{A}_{m-1}$, потому что при обозначениях $\bar{a}_j = a_j \cdot a_{p^{m-1}+j}^{-1}$ элемент

$$a_1 \cdot a_{p^{m-1}+1} \cdot \dots \cdot a_{p^m-p^{m-1}+1} \cdot \bar{a}_{p^m-2p^{m-1}+1} \cdot \bar{a}_{p^m-3p^{m-1}+2} \cdot \dots \cdot \bar{a}_{p^m-p^{m-1}+1} = \alpha_1^p$$

содержится в подгруппе ${}^*A_{m-1} \cdot \bar{A}_{m-1} \subseteq Z_s$.

С помощью формулы (2.8)

$$\alpha_{p^{m-1}+1} = a_1^{\binom{p^{m-1}}{0}} \cdot a_2^{-\binom{p^{m-1}}{1}} \cdot \dots \cdot a_{p^{m-1}}^{\binom{p^{m-1}-1}{p^{m-1}-1}} \cdot a_{p^{m-1}+1}^{-\binom{p^{m-1}}{p^{m-1}-1}} = \prod_{v=1}^{p^{m-1}+1} a_v^{(-1)^{v-1} C_{p^{m-1}}^{v-1}}$$

и леммы 2.7 $C_{p^{m-1}}^i \equiv 0 \pmod{p}$, где $i=1, 2, \dots, p^{m-1}$, получим, что

$$\alpha_{p^{m-1}+1} \in {}^*A_{m-1} \cdot \bar{A}_{m-1}.$$

Так же $\alpha_{p^{m-1}} \in {}^*A_{m-1} \cdot \bar{A}_{m-1}$, иначе элемент

$$a_1 \cdot a_2 \cdot \dots \cdot a_{p^{m-1}} = \prod_{v=1}^{p^{m-1}} \alpha_v^{(-1)^{v-1} C_{p^{m-1}}^v}$$

содержался бы в ${}^*A_{m-1} \cdot \bar{A}_{m-1}$, поэтому что $C_{p^{m-1}}^v \equiv 0 \pmod{p}$, если $v=1, 2, \dots, p^{m-1}$. Поэтому из-за

$$[b, a_1 \cdot a_2 \cdot \dots \cdot a_{p^{m-1}}] = a_1 \cdot a_{p^{m-1}+1}^{-1} \in \bar{A}_{m-1}$$

в подгруппе ${}^*A_{m-1} \cdot \bar{A}_{m-1}$ существовал бы такой элемент $a_1 \cdot a_2 \cdot \dots \cdot a_{p^{m-1}}$, для которого s -ый коммутатор с элементом b не был бы равен единице, что противоречит условию $\bar{A}_{m-1} \subseteq Z_s$. Тогда

$$\{\alpha_1^p, \alpha_2^p, \dots, \alpha_{p^{m-1}}^p, \alpha_{p^{m-1}+1}, \dots, \alpha_{p^m}\} \subseteq {}^*A_{m-1} \cdot \bar{A}_{m-1} \subseteq Z_s.$$

По определению верхнего центрального ряда легко видеть, что

$$\alpha_{p^{m-1}} \in Z_{s+1}, \alpha_{p^{m-1}-1} \in Z_{s+2}, \dots, \alpha_1 \in Z_{s+p^{m-1}},$$

и значит $\alpha_2 \in Z_{s+p^{m-1}-1}$, следовательно $W = Z_s$. Если $Z_{s+p^{m-1}-k} = W$, но $Z_{s+p^{m-1}-k-1} \neq W$ (при $k \geq 0$), тогда $\alpha_2 \in Z_{s+p^{m-1}-k-1}$, но $\alpha_2 \notin Z_{s+p^{m-1}-k-2}$, иначе

$$W_1 \subseteq Z_{s-k-2+p^{m-1}}, \text{ т. е. } Z_{s+p^{m-1}-k-1} = W.$$

Тогда

$$\alpha_{p^{m-1}+1} \in Z_{s+p^{m-1}-k-p^{m-1}},$$

причем

$$(2.13) \quad \alpha_{p^{m-1}+1} \notin Z_{s+p^{m-1}-k-p^{m-1}-1}.$$

По предыдущему $\alpha_{p^{m-1}+1} \in Z_s$, поэтому ясно, что $s+p^{m-1}-k-p^{m-1} \geq s$. Отсюда $k \leq 0$, и значит $k=0$, ведь мы предполагали $k \geq 0$ и

$$(2.14) \quad Z_{s+p^{m-1}} = W, \text{ причем } Z_{s+p^{m-1}-1} \neq W.$$

Переходим к утверждению: если $\{b^{p^k}\} \subset Z_l$, то $[b^{p^k}, c] \in Z_{l-1}$ для всяких $c \in K$. Если $c = a_i$, то $[b^{p^k}, a_i] = a_{i+p^k}^{-1} \cdot a_i \in Z_{l-1}$, поэтому

$$l-1 \geq s+p^{m-1}-p^k, \text{ и } l \geq s+p^{m-1}-p^k+1,$$

ведь из (2.13) легко видеть что

$$\alpha_{p^k+1} \in Z_{s+p^{m-1}-p^k}, \quad \alpha_{p^k+1} \notin Z_{s+p^{m-1}-p^k+1}.$$

Теорема доказана.

Из доказательства теоремы 2.14 следует:

Следствие 2.14. Класс нильпотентности группы W равен

$$n(p^m - p^{m-1}) + p^{m-1}.$$

По теореме 2.14 при $k=m-1$ мы получили, что $\{b^{p^{m-1}}\} \subset Z_{s+1}$, но $\{b^{p^{m-1}}\} \not\subseteq Z_s$. Таким же образом, по доказательству теоремы 2.14 имеет место.

Теорема 2.15. Последний коммутативный член верхнего центрального ряда группы W имеет вид

$$Z_{n(p^m - p^{m-1})} = \{\alpha_1^p, \alpha_2^p, \dots, \alpha_{p^{m-1}}^p, \alpha_{p^{m-1}+1}, \dots, \alpha_{p^m}\}$$

и

$$Z_{n(p^m - p^{m-1}) + p^{m-1} - p^k + l} = \{b^{p^k}\} \{\alpha_1^p, \alpha_2^p, \dots, \alpha_{p^k+l}^p, \alpha_{p^k+l+1}, \dots, \alpha_{p^m}\},$$

где

$$1 \leq l \leq p^{k+1} - p^k \text{ и } m-1 \geq k \geq 0.$$

§ 3

Обозначим через C_l циклическую группу порядка l , и далее также будем пользоваться обозначениями предыдущего параграфа.

1. Пусть $\bar{W} = C_p \text{ wr } C_{p^m}$. При $n=1$, согласно результатам предыдущего параграфа, $|\bar{W}| = p^{p^m+m}$, и класс нильпотентности группы $\bar{W}$ равен p^m .

По теореме 2.6

$$\bar{W}_1 = \{\alpha_2, \alpha_3, \dots, \alpha_{p^m}\},$$

и элементы α_j , заданные в лемме 2.5, выполняют $\alpha_j \in \bar{W}_{j-1}$ ($j=2, 3, \dots$), а центр группы $\bar{W}$ является циклической группой порядка p , порожденной элементом $\alpha_1 \cdot \alpha_2 \cdot \dots \cdot \alpha_{p^m}$.

Из упомянутых результатов, с использованием эндоморфизма, введенного в лемме 2.3, следует.

Теорема 3.1. В нижнем центральном ряде группы $\bar{W}$:

$$\bar{W}_0 = \bar{W}, \quad \bar{W}_k = \{\alpha_{k+1}, \alpha_{k+2}, \dots, \alpha_{p^m}\} \quad (k = 1, 2, \dots, p^m - 1), \quad \bar{W}_{p^m} = \{e\}.$$

Согласно теореме 2.15 очевидна

Теорема 3.2. В верхнем центральном ряде группы $\bar{W}$:

$$Z_0 = \{e\},$$

$$Z_s = \{\alpha_{p^m-s+1}, \alpha_{p^m-s+2}, \dots, \alpha_{p^m}\} = \bar{W}_{p^m-s}, \quad \text{где } 1 \leq s \leq p^m - p^{m-1},$$

$$Z_{p^m-p^k+l} = \{b^{p^k}\} \{\alpha_{p^k-l+1}, \alpha_{p^k-l+2}, \dots, \alpha_{p^m}\} = \{b^{p^k}\} \bar{W}_{p^k-l},$$

где $0 < k < m; \quad 1 \leq l \leq p^k - p^{k-1},$

$$Z_{p^m} = \bar{W}.$$

2. Пусть $W' = C_{p^n} \text{ wr } C_p$. При $m=1$ справедливы результаты предыдущего параграфа. Значит $|W'| = p^{n \cdot p+1}$, класс нильпотентности группы W' равен $n(p-1)+1$. Нашей целью опять является описание нижнего и верхнего центральных рядов сплетения.

По теореме 2.6 $W'_1 = \{\alpha_2, \alpha_3, \dots, \alpha_p\}$, и $|W'_1| = p^{n \cdot (p-1)}$, значит порядок каждой факторгруппы нижнего центрального ряда (кроме первого) равен p .

Лемма 3.3. В нижнем центральном ряде группы W'

$$W'_{i(p-1)+1} = \{\alpha_2^{p^i}, \alpha_3^{p^i}, \dots, \alpha_p^{p^i}\},$$

$$W'_{i(p-1)+2} = \{\alpha_2^{p^{i+1}}, \alpha_3^{p^i}, \dots, \alpha_p^{p^i}\}.$$

$$(i = 1, 2, \dots, n-1)$$

Доказательство. По выбору элемента α_{p+1} ясно, что $\alpha_{p+1} = [b, \alpha_p] \in W'_p$, и по соотношению (2.12)

$$\alpha_p = z \cdot \prod_{v=1}^{p-1} \alpha_v^{(-1)^v \cdot C_p^v}.$$

Это значит, что

$$[b, \alpha_p] = \prod_{v=1}^{p-1} \alpha_{v+1}^{(-1)^v \cdot C_p^v} \in W'_p$$

и

$$[b, [b, \alpha_p]] = \alpha_{p+1} = \prod_{v=1}^{p-2} \alpha_{v+1}^{(-1)^v \cdot C_p^v} \cdot [b, \alpha_p]^p \in W'_{p+1} \subset W'_p.$$

Очевидно, $\alpha_{p+1}^p \in W'_p$, поэтому $\prod_{i=2}^{p-2} \alpha_{v+1}^{(-1)^v \cdot C_p^v} \in W'_p$. По лемме 2.7 $C_p^v \equiv 0 \pmod{p}$, но $C_p^v \equiv 0 \pmod{p^2}$, где $v=1, 2, \dots, p-1$, поэтому

$$\prod_{v=1}^{p-2} \alpha_{v+2}^{(-1)^v \cdot C_p^v} = \alpha_2^{k_1 \cdot p} \cdot \alpha_3^{k_2 \cdot p} \cdot \dots \cdot \alpha_p^{k_{p-2} \cdot p}$$

для подходящих целых чисел k_j , где $p \nmid k_j$, $j=1, 2, \dots, p$. Легко проверяется, что элементы $\alpha_3^{k_1 \cdot p} \cdot \alpha_4^{k_2 \cdot p} \cdot \dots \cdot \alpha_{p-2}^{k_{p-2} \cdot p}$, $\alpha_4^{k_1 \cdot p} \cdot \alpha_5^{k_2 \cdot p} \cdot \dots \cdot \alpha_{p-3}^{k_{p-3} \cdot p}$, ..., $\alpha_{p-1}^{k_1 \cdot p} \cdot \alpha_p^{k_2 \cdot p}$, $\alpha_p^{k_1 \cdot p}$ также содержатся в подгруппе W'_p , поэтому соответствующее произведение их степеней, именно элементы $\alpha_2^p, \alpha_3^p, \dots, \alpha_p^p$, также содержатся в W'_p . По теореме 2.6 легко видеть, что порядок группы W'_p не более чем $p^{(n-1)p-1}$ и значит

$$W'_p = \{\alpha_2^p, \alpha_3^p, \dots, \alpha_p^p\},$$

$\alpha_2^p \in W'_{p+1}$, иначе $W'_p = W'_{p+1}$, но из-за $\alpha_2^p \in W'_p$ ясно, что $\alpha_3^p \in W'_{p+1}$.

Из рассуждений подобных предыдущим, следует, что из-за $\alpha_2^p \in W'_p$, имеет место $\alpha_p^p \in W'_{2(p-1)}$ и с помощью соотношения (2.12) получим что

$$\prod_{v=1}^{p-2} \alpha_{v+1}^{(-1)^v \cdot C_p^v \cdot p} \in W'_{2p-1} \quad (v=1, 2, \dots, p-1),$$

наконец,

$$W'_{2(p-1)+2} = \{\alpha_2^{p^2}, \alpha_3^{p^2}, \dots, \alpha_p^{p^2}\}.$$

Тогда $\alpha_2^{p^2} \in W'_{p+1}$, и отсюда следует

$$W'_{p+1} = \{\alpha_2^{p^2}, \alpha_3^{p^2}, \dots, \alpha_p^{p^2}\}.$$

Значит при $i=1$ утверждение верно.

Предположим, что оно доказано для всех натуральных чисел $1 \leq i < n$, то есть

$$W'_{(i-1)(p-1)+1} = \{\alpha_2^{p^{i-1}}, \alpha_3^{p^{i-1}}, \dots, \alpha_p^{p^{i-1}}\},$$

$$W'_{(i-1)(p-1)+2} = \{\alpha_2^{p^i}, \alpha_3^{p^i}, \dots, \alpha_p^{p^i}\}.$$

Так как, по предположению

$$\alpha_2^{p^{i-1}} \in W'_{(i-1)(p-1)+1}, \quad \text{то} \quad \alpha_p^{p^{i-1}} \in W'_{i(p-1)},$$

и т. д. Аналогичным образом получим

$$\{\alpha_2^{p^i}, \alpha_3^{p^i}, \dots, \alpha_p^{p^i}\} = W'_{i(p-1)+1}.$$

$\alpha_2^{p^i} \in W'_{i(p-1)+2}$, иначе было бы $W'_{i(p-1)+2} = W'_{i(p-1)+1}$, и подобно предыдущему, продолжая доказательство,

$$\alpha_2^{p^{i+1}} \in W'_{i(p-1)+1}.$$

Но порядок группы $W'_{i(p-1)+2}$ не более чем $p^{(n-i)(p-1)-1}$, поэтому

$$W'_{i(p-1)+2} = \{\alpha_2^{p^{i+1}}, \alpha_2^{p^i}, \dots, \alpha_p^{p^i}\} \quad 1 \leq i \leq n,$$

что и требовалось доказать.

Теорема 3.4. В нижнем центральном ряде группы W'

$$а) W'_0 = W' = \{b\}\{\alpha_1, \alpha_2, \dots, \alpha_p\},$$

$$б) W'_{k(p-1)+1} = \{\alpha_2^{p^k}, \alpha_3^{p^k}, \dots, \alpha_p^{p^k}\}, \quad k = 0, 1, 2, \dots, n,$$

$$в) W'_{k(p-1)+2} = \{\alpha_2^{p^{k+1}}, \alpha_3^{p^k}, \dots, \alpha_p^{p^k}\},$$

$$г) W'_{k(p-1)+l} = \{\alpha_2^{p^{k+1}}, \alpha_3^{p^{k+1}}, \dots, \alpha_l^{p^{k+1}}, \alpha_{l+1}^{p^k}, \dots, \alpha_p^{p^k}\},$$

где, в случае в) и г), $k=0, 1, 2, \dots, n-1$; $l=3, 4, \dots, p-1$.

Доказательство. Утверждение б) и в) верны по лемме 3.3, а утверждение а) очевидно по определению сплетения.

Так как $W'_{k(p-1)+l} \subset K$, и

$$[W', W'_{k(p-1)+l}] = [b, W'_{k(p-1)+l}] = W'_{k(p-1)+l+1},$$

то по теореме 2.6 группу $W'_{k(p-1)+l+1}$ порождают элементы вида $[b, \alpha_i^k]$, где $\alpha_i^k \in W'_{k(p-1)+l}$ и $2 \leq i < p-1$. Таким образом, утверждение г) тоже легко проверяется.

Лемма 3.5. В верхнем центральном ряде группы

$$|Z_1/Z_0| = p^n, \quad |Z_{n(p-1)+1}/Z_{n(p-1)}| = p^2,$$

а порядок остальных факторгрупп в центральном ряде равен p .

Доказательство. $|Z_1/Z_0| = p^n$ очевидно по теореме 2.2.

Если была бы по крайней мере одна факторгруппа в верхнем центральном ряде порядка p^3 , тогда класс нильпотентности группы W' был бы не более чем $n(p-1)$.

По лемме 2.13, элемент b , содержится в группе $Z_{n(p-1)+1}$, но не содержится в $Z_{n(p-1)}$. По теореме 2.15 $\alpha_1 \in Z_{n(p-1)+1}$, но $\alpha_1 \notin Z_{n(p-1)}$, и легко проверяется что $b^i \alpha_1^j \notin Z_{n(p-1)}$, где $p \nmid i$ и $p \nmid j$ (i и j натуральные), то возможно только

$$|Z_{n(p-1)+1}/Z_{n(p-1)}| = p^2.$$

Лемма доказана.

Теорема 3.6. В верхнем центральном ряде группы W'

а) $Z_1 = \{z\}$,

б) $Z_{k(p-1)+1} = \{z, \alpha_2^{p^{n-k}}, \dots, \alpha_{p-1}^{p^{n-k}}, \alpha_p^{p^{n-k}}\} \quad k = 0, 1, \dots, n-1,$

в) $Z_{k(p-1)+l} = \{z, \alpha_2^{p^{n-k}}, \dots, \alpha_{p-l}^{p^{n-k}}, \alpha_{p-l+1}^{p^{n-k-1}}, \dots, \alpha_{p-1}^{p^{n-k-1}}, \alpha_p^{p^{n-k-1}}\},$

где $k = 0, 1, \dots, n-1$; $l = 2, 3, \dots, p-1$,

г) $Z_{n(p-1)+1} = W'$.

Доказательство. Утверждение а) (по теореме 2.2) и г) очевидно. По связи верхнего и нижнего центрального ряда конечных нильпотентных групп и по теореме 3.4

$$Z_{k(p-1)+1} \supseteq W'_{(n-k)(p-1)} = W'_{(n-k-1)(p-1)+p-1} = \{\alpha_2^{p^{n-k}}, \dots, \alpha_{p-1}^{p^{n-k}}, \alpha_p^{p^{n-k-1}}\}.$$

Так же очевидно, что

$$Z_1 \subset Z_{k(p-1)+1},$$

т. е. группа

$$R = \{z, \alpha_2^{p^{n-k}}, \alpha_3^{p^{n-k}}, \dots, \alpha_{p-1}^{p^{n-k}}, \alpha_p^{p^{n-k-1}}\} \subseteq Z_{k(p-1)+1}.$$

По лемме 2.8

$$z = \prod_{i=1}^p \alpha_i^{(-1)^i \cdot C_p^i},$$

и значит

$$z \in \{\alpha_1^p, \alpha_2^p, \dots, \alpha_{p-1}^p, \alpha_p^p\}, \quad \text{причем} \quad z \notin \{\alpha_1^p, \alpha_2^p, \dots, \alpha_{p-1}^p, \alpha_p^p\}.$$

Тогда

$$z^{p^i} \in \{\alpha_1^{p^{i+1}}, \alpha_2^{p^{i+1}}, \dots, \alpha_{p-1}^{p^{i+1}}, \alpha_p^{p^i}\},$$

причем

$$z^{p^i} \notin \{\alpha_1^{p^{i+1}}, \alpha_2^{p^{i+1}}, \dots, \alpha_{p-1}^{p^{i+1}}, \alpha_p^{p^{i+1}}\}.$$

С помощью леммы 2.8 можно убедиться, что элемент z^i , $i \not\equiv 0 \pmod{p^n}$, не может быть записан в виде произведения степеней элементов

$$\alpha_1^{p^{n-k}}, \alpha_2^{p^{n-k}}, \dots, \alpha_{p-1}^{p^{n-k}}, \alpha_p^{p^{n-k-1}}, \quad \text{где} \quad i = 1, 2, \dots, p^{n-2}.$$

Так же верно, что

$$|R| = p^{n-1} \cdot p^{k(p-1)} \cdot p^{k+1} = p^{k(p-1)+1}.$$

По лемме 2.3 имеем, что

$$|Z_{k(p-1)+1}| = |R|,$$

т. е.

$$|Z_{k(p-1)+1}| = \{z, \alpha_2^{p^{n-k}}, \dots, \alpha_{p-l}^{p^{n-k}}, \alpha_{p-l+1}^{p^{n-k-1}}, \dots, \alpha_p^{p^{n-k-1}}\} \subseteq Z_{k(p-1)+l},$$

значит утверждение б) верно.

Если

$$\bar{R} = \{z, \alpha_2^{p^{n-k}}, \dots, \alpha_{p-l}^{p^{n-k}}, \alpha_{p-l+1}^{p^{n-k-1}}, \dots, \alpha_p^{p^{n-k-1}}\},$$

то

$$|\bar{R}| = p^{n-k(p-1)-l+1},$$

и значит

$$Z_{k(p-1)+l} = \bar{R} \quad (k = 0, 1, \dots, n-1; l = 2, 3, \dots, p-1).$$

Теорема доказана.

Литература

- [1] К. Бузаши, Ядра неприводимых представлений силовской p -подгруппы S_n симметрической группы S_{p^3} . *Publ. Math.* **14** (1967), 285—310.
- [2] К. Бузаши, Ядра неприводимых представлений силовской p -подгруппы S_n симметрической группы S_{p^n} . *Publ. Math.* **16** (1969), 199—227.
- [3] L. KALOUJNINE, Sur les p -groupes de Sylow du groupe symetrique du degree p^m . *C. R. Acad. Sci. Paris* **221** (1945), 222—224.
- [4] L. KALOUJNINE, La structure du p -groupe de Sylow du groupe symetrique du degree p^k . *C. R. Acad. Sci. Paris* **222** (1946), 1424—1425.
- [5] A. I. WEIR, The Sylow subgroups of the symmetric groups. *Proc. Amer. Math. Soc.* **6** (1955), 534—541.
- [6] GY. PÓLYA, Kombinatorische Anzahlbestimmungen für Gruppen, Graphen und Chemische Verbindungen. *Acta Math.* **68** (1937), 145—254.
- [7] H. LIEBECK, Concerning nilpotent wreath products. *Proc. Cambridge Philos. Soc.* **58** (1962), 443—453.
- [8] I. D. P. MELDRUM, Central series in wreath products. *Proc. Cambridge Philos. Soc.* **6** (1967), 551—567.

(Поступила: 8. I. 1974)