УДК 512.543

Р.В. Скуратовський

ТВІРНІ І СПІВВІДНОШЕННЯ ДЛЯ СИЛОВСЬКИХ *p*-ПІДГРУП ГРУПИ S_n

In this article, we investigate generators and relations of syllows subgroups of some symmetric group. It will enable studying syllows subgroups of other groups since every finite subgroup is isomorphicaly embedded in the syllows subgroup of some symmetric group. We find a set of relations for a fixed system of generators and prove that this set of relations is minimal between sets of relations. Research methods are the method of Shreier's canonical words and rewriting process. In addition, we prove that such subgroups have a finite presentation, notably it has finite number of generators and relation. We prove the existence of close connection of such subgroups with the iterated wreath product of cyclic subgroups with prime order – C_p. Therefore, it became the research subject. Also, we investigate the iterated wreath product, related to automaton group and transformations. Furthermore, the structure properties of symmetryc group S_{p^k} were previously studied, while we describe all other properties left. Specifically, we study commutants and corresponding verbal subgroups. We find the presentation for syllows p-subgroups of S_{p^k} and S_n.

Вступ

Силовські *p*-підгрупи скінченної симетричної групи підстановок відіграють у класі скінченних *p*-груп настільки ж важливу роль, як і симетричні групи в класі всіх скінченних груп. Доволі важливим зображенням цих груп є їх козображення. Вінцевий добуток [1] – одна із найбільш уживаних конструкцій у сучасній теорії груп. Дослідженням будови вінцевих добутків присвячено численні публікації таких відомих фахівців з теорії груп, як В.І. Сущанський [2] , Л.А. Калужнін [2], А. Воріна [3], Г. Бомслаг [2], А.Л. Шмелькін [4], В.Г. Мікаелян [5], П. Нейман, Х. Нейман [2] та ін. В [1, 6] досліджено структурні властивості силовських *p*-підгруп симетричної групи степеня p^k, тобто S_{p^k}.

Серед вінцевих добутків конкретних груп найбільш вивченими є вінцеві добутки циклічних, елементарних абелевих, симетричних і знакозмінних груп (Л.А. Калужнін [2], К. Бузаші [2], В.І. Сущанський [2], Ю.В. Боднарчук [7], Ю.В. Дмитрук [4] та ін.). В дисертації [8] охарактеризовано вербальні підгрупи групи фінітарних автоморфізмів 2-адичного дерева. Зроблено оцінку ширини членів нижнього центрального ряду, ряду комутантів і степеневих підгруп групи фінітарних автоморфізмів 2-адичного дерева. Але співвідношення для силовських *p*-підгруп все ще не знайдені, більше того, вони дещо інші, ніж для 2-підгруп.

Постановка задачі

Козображення і різноманітні властивості цієї півгрупи майже не розглядалися ніким. Отже, метою є знаходження твірних і співвідношень цих підгруп в ітерованому вінцевому добутку симетричних груп.

Основні поняття

Маємо дві групи підстановок: (G,M) та (H,N). Надалі розглянемо вінцевий добуток груп $(G,M)\wr H$, визначимо дію $(G,M)\wr H$ на $M\times N$:

$$\{[f_1;f_2(x)] \| f_1\in G,\ f_2: M\to H,$$
$$(m,n)^{[f_1;f_2(x)]}\to(m^{g_1},n^{h_2(m)})\}.$$

Правило множення в групі $G\wr H$ у загальному вигляді запишеться як

$$[f_1;\ f_2(x)]\cdot[g_1;\ g_2(x)]=[f_1g_1;\ f_2(x)g_2(x^{f_1})],$$

де $[f_1;\ f_2(x)]$, $[g_1;\ g_2(x)]$ – елементи групи $G\wr H$.

У цьому випадку $G=C_p=M$ та $H=N==C_p$, тобто обидві групи діють самі на собі. Необхідно лише задати дію, нехай це будуть ліві зсуви.

Розв'язання задачі

Як відомо, кожна силовська підгрупа довільної групи, ізоморфна певній силовській *p*-підгрупі P симетричної групи степеня n, яка ізоморфна прямому добутку

$$P = P_1^{a_1} \times P_2^{a_2} \times \ldots \times P_m^{a_m},$$

де P_k – силовська p-підгрупа групи S_{p^k}. Кожна така P_k є ізоморфною [2] до k-кратного вінцевого добутку регулярних циклічних груп степеня p:

$$P_k \cong \wr_{i=1}^{k} C_i.$$

Якщо $R(T_k)$ – козображення для P_k, то відповідним козображенням для P є силовська p-підгрупа в S_n:

$$P \simeq \left\langle \begin{array}{c} t_{ikz} \mid R(T_k),\ t_{ikz}t_{jks} = t_{jks}t_{ikz},\ 0 \le i, j < k \le m, \\ 1 \le z,\ s \le \alpha_k,\ t_{lkz}t_{jvs} = t_{jvs}t_{lkz},\ 1 \le z \le \alpha_k, \\ 1 \le s \le \alpha_v,\ 1 \le k, v \le m \end{array} \right\rangle,$$

де t_{ikz} – i-й твірний підгрупи P_z, спряженої з P_k; T_k – твірні підгрупи P_k, $1 \le k \le m$. Підкреслимо, що P є нільпотентною, як p-група. Знайдемо козображення для силовської p-підгрупи групи S_{p^k}. Зрозуміло, що вона є максимальною нільпотентною транзитивною підгрупою в S_{p^k}.

Подамо елементи групи $C_p \wr C_p$ у вигляді таких таблиць:

$$u_1 u_2 = [g;\ h_1, \ldots, h_p] \cdot [g;\ h_1', \ldots, h_p'] =$$
$$= [gg;\ h_1 h_{g(1)}',\ h_2 h_{g(2)}',\ \ldots, h_p h_{g(p)}'].$$

Лема 1. Елементи $x_1 = [a; e, e, \ldots, e]$, $x_2 = [e; a, e, \ldots, e]$ є системою твірних в $C_p \wr C_p$, де x_1, x_2 – активний і пасивний елементи, а системою твірних для $P_n \cong \wr_{i=1}^{n} C_i$ є

$$\begin{aligned} x_{n,1} &= [[[[[a; e, e, \ldots, e]e, e, \ldots, e]e, e, \ldots, e]\ldots]e, e, \ldots, e] = \\ &= [[[[[x_{2,1}]e, e, \ldots, e]e, e, \ldots, e]\ldots]e, e, \ldots, e], \\ x_{n,2} &= [[.[[[e; a,\ e, \ldots, e]e, e, \ldots, e]e, e, \ldots, e]\ldots]e, e, \ldots, e] = \\ &= [[.[[[x_{2,2}]e, e, \ldots, e]e, e, \ldots, e] \underbrace{\ldots}_{n-4}]e, e, \ldots, e], \end{aligned} \tag{1}$$

$$x_{n,n-1} = [[x_{n-1,n-1}]e, e, \ldots, e]$$

і

$$x_{n,n} = [[e]a, e, \ldots, e]$$

або

$$x_{n,n} = [[[[[e; e, e, \ldots, e]e, e, \ldots, e]e, e, \ldots\ldots, e]\ldots]a, e, \ldots, e].$$

Доведемо це індукцією за кількістю множників. Так, для $C_p \wr C_p$

$$x_1 \cdot x_2 = [a; e, e, \ldots, e][e; a, e, \ldots, e] =$$
$$= [a \cdot e; e \cdot e, e \cdot e, \ldots, e \cdot a].$$

Якщо подіяти зліва елементом x_1^{-i} на x_2, то він зсуває елементи таблиці, які є елементами підгрупи, що виступає базою вінцевого добутку, тобто підгрупи H, вліво на i позицій. Тоді

$$x_1^{-1} x_2 x_1 = [a^{-1}; e,\ e, \ldots, e] \cdot [e; a,\ e, \ldots, e] \times$$
$$\times [a; e,\ e, \ldots, e] = [e; a,\ e, \ldots, e].$$

Таким чином, можна "переставляти" елемент a в таблиці $u = [e; a, \ldots, e, e] = x_2$ на будь-яку позицію з H.

Нехай $[u]_i$ – та координата (елемент) таблиці u, де $i \in \overline{0, \ldots, p-1}$.

Перемноживши $\underbrace{x_2 \cdot x_2 \cdot \ldots \cdot x_2}_{i \text{ разів}} = [e; a^i, e, e]$, $i \in \overline{0, \ldots, p-1}$, аналогічним чином можна переставляти елемент a^i на будь-яку з позицій, які відповідають елементам з бази H, тобто це $[u]_j$, $j \in \{1, \ldots, p\}$.

Надалі очевидно, що елементи у вигляді $[e; h_1, h_2, \ldots, h_p]\,[e; h_1', h_2', \ldots, h_p']$ перемножуються прямо, тобто поелементно, тому можна отримати будь-який елемент вигляду $[e; a_1^{i_0}, a^{i_2}, \ldots, a^{i_{p-1}}] = WT$, де $i_j \in \{0, 1, \ldots, p-1\}$. Звідси випливає, що $x_1^{-i} x_2 x_1^i x_2 = x_2 x_1^{-i} x_2 x_1^i$, $i \in \{1, \ldots, p-1\}$.

***Означення* 1.** Назвемо елементами k-го рівня L_k елементи, утворені при спряженні твірного з k-го множника групи $P_n \cong \wr_{i=1}^{n} C_i$.

На n-му кроці індукції маємо групу $P_n = G = (\ldots((C_p \wr C_p) \wr C_p)\ldots) \wr C_p$, де C_p – підгрупа групи підстановок. Завдяки асоціативності вінцевого добутку груп підстановок на класі всіх груп підстановок [1] маємо $G = C_p \wr (...(C_p \wr (C_p \wr C_p))...)$.

Тут елементи групи, яку помножили на добуток, отриманий на останній ітерації, належать до L_n. Вони виступають пасивними елементами найбільшої таблиці. Елементи, утворені на n-й ітерації, позначимо $x_{n,m}$, m — номер твірного, зокрема, $x_{n,n}$ — твірний з L_n. Зрозуміло, що елементи з L_n множаться прямо. Елементи з усіх попередніх рівнів діють лівим зсувом на елементах з L_n та зсувають твірний з L_n по всіх позиціях пасивної частини твірного $x_{n,n}$. Отже, твірними для G є елементи (1).

Легко переконатися, що $x_{m-1,1}^{-i} x_{m,1} x_{m-1,1}^{i} x_{n,1} = x_{n,1} x_{m-1,1}^{-i} x_{m,1} x_{m-1,1}^{i}$, $i \in \{0, 1, ..., p-1\}$, де x_m — твірний m-го рівня; x_{m-1}, x_n — твірні з L_{n-1}, L_n.

Ітеруючи операцію вінцевого добутку, отримаємо на n-й ітерації таку конструкцію: таблиці попереднього рівня вкладені в таблиці наступного рівня та є їх активними елементами. Завдяки зміні порядку множення елемент першої групи є повністю активним і діє на інших елементах. Він міститься в першій таблиці, яка має глибокий рівень вкладення. Крім того, p пасивних елементів цієї таблиці діють на відповідних сегментах пасивної частини другої таблиці, яка безпосередньо містить згадану вище таблицю як активну, а саме перший пасивний елемент h_1 першої таблиці діє на перших p пасивних елементах $h_{1,i}$ $i = 1, ..., p$, другої таблиці. Аналогічним чином перший пасивний елемент h_2 другої таблиці діє на наступних p пасивних елементах $h_{2,i}$, $i = 1, ..., p$, третьої таблиці тощо. Таким чином, друга таблиця містить p^2 пасивних елементів. Третя таблиця містить p^3 пасивних елементів, які також поділені на сегменти дії пасивних елементів з попередньої таблиці.

Надалі означимо твірний елемент з L_k як $x_{n,k,1}$ для $k \in (1, ..., n)$.

Лема 2. Виконуються співвідношення $x_{n,n,1} x_{n,k,l} = x_{n,k,l} x_{n,n,1}$, $l \neq 1 (mod\ p)$, $x_{n,n,m} x_{n,k,1} = x_{n,k,1} x_{n,n,m}$, де $x_{n,n,m}$ — m-й елемент з L_n, $k \leq n$, $m > p^{n-k}$, для n-кратного вінцевого добутку.

Доведемо індуктивно правильність співвідношень у групі G. Базу індукції доведено раніше. Припустимо, що для добутку n–1-груп співвідношення виконуються. Далі помножимо отриманий добуток на групу C_p і доведемо справедливість співвідношень для елементів з новоутвореного рівня L_n. Спрягаючи твірні з L_n, отримуємо всі елементи з L_n. У новій таблиці u ці елементи породжують циклічні підгрупи C_{p^n} і утворюють нормальну підгрупу H_n, яка є прямим добутком цих підгруп дійсно, $\forall x \in L_n$, $\forall g \in G$ маємо

$$g^{-1} x_i g = \left[[...[a^{-j} e a^j; e, ..., e]...]; h_1 x_{n(g^{-1})} h_1^{-1}{}_{(g^{-1} x_n)}, ... \right] =$$

$$= \left[[...[e; e, ..., e]...]; h_1 x_{n(g^{-1})} h_1^{-1}{}_{(g^{-1} x_n)}, ... \right] \in H,$$

звідси $H \lhd G$.

Елементи $x_{n,n-1,l}^{-k} x_{n,n,m} x_{n,n-1,l}^{k}$, $k \in \{0, 1, ..., p-1\}$, $1 \leq l \leq p^{n-1}$, $x_{n,n,m} \in L_n$, $lp \leq m \leq (l+1)p$ породжують підгрупи $\langle x_{n,n,l} \rangle \simeq C_p$ в $H_n \lhd G$, які дають прямий розклад, де H_n — база вінцевого добутку.

Дійсно, $\langle x_{n,n,I} \rangle \cap \langle x_{n,n,j} \rangle = e$ при $i \neq j$, $\forall h \in H_n$: $h = \langle x_{n,n,1} \rangle \times \langle x_{n,n,2} \rangle \times ... \times \langle x_{n,n,p^n} \rangle$ однозначно записується у вигляді $h = x_{n,n,1}^{i_1} x_{n,n,2}^{i_2} ... x_{n,n,p^n}^{i_{p-1}}$, звідси $H_n = \langle x_{n,n,1}, ..., x_{n,n,p^n} \rangle$. Крім того, $\forall x_{n,i} \in H_n$, $\forall g \in G$, маємо

$$g^{-1} x_{n,i} g =$$

$$= [[...[e; e, ..., e]...]; ..., h_1 x_{n,i(g^{-1})} h_1^{-1}{}_{(g^{-1} x_{n,i})}, ...] \in \langle x_i \rangle,$$

тобто $\langle x_i \rangle \lhd H_n$. Детальніше $H_n = \langle x_{n,n,1} \rangle \times \langle x_{n,n,2} \rangle \times ... \times \langle x_{n,n,p^n} \rangle$ та $\langle x_{n,n,m} \rangle \rhd H_n$, оскільки $x_{n,n-1,j}^{-k} x_{n,n,m} x_{n,n-1,j}^{k} = \langle x_{n,n,m} \rangle$, $k \in \{0, 1, ..., p-1\}$, $1 \leq j \leq p^{n-1}$, $x_{n,n,m} \in L_n$.

Тому, згідно з другим визначенням внутрішнього прямого добутку [1], маємо $x_{n,n,i} x_{n,n,j} = x_{n,n,j} x_{n,n,i}$. Тоді в силу того, що твірний елемент $x_{n,k,1}$ діє тільки на перші p^{n-k} елементів з L_n і не діє на інші його елементи, варто $x_{n,n,m} x_{n,k,1} = x_{n,k,1} x_{n,n,m}$ при $k \leq n$, $p^{n-k} < m < p^n$, при цьому третій індекс змінюється від 1 до n. Аналогічно маємо $x_{n,n,1}x_{n,k,l} = x_{n,k,l}x_{n,n,1}$, оскільки $x_{n,k,l}$, $l \neq 1(\bmod p)$, не діє на перші елементи з L_n. Виконання співвідношення $x_i^p = e$ очевидне.

Нехай $F(t_0, t_1, ..., t_n)$ – вільна група. Введемо відстань між елементами F. Усі елементи, які отримані з t_m спряженням і сам t_m, мають відстань до t_0, рівну m, $m > 0$, $m \in \mathbb{N}$, будемо називати їх елементами m-го рангу; t_0 – твірний рангу 0; t_i – твірний рангу i; $u_{i_0 i_1 i_2 ... i_{m-1}} = t_0^{-i_0} t_1^{-i_1} ... t_{m-1}^{-i_{m-1}} t_m t_{m-1}^{i_{m-1}} ... t_1^{i_1} t_0^{i_0}$ – елемент рангу m.

***Означення* 2.** Індексною структурою елемента $u_{i_0 i_1 i_2 ... i_{m-1}} = t_0^{-i_0} t_1^{-i_1} ... t_{m-1}^{-i_{m-1}} t_m t_{m-1}^{i_{m-1}} ... t_1^{i_1} t_0^{i_0}$ називається вектор $\delta(u_{i_0, i_1 ... i_{m-1}}) = (i_0, i_1, i_2 ... i_{m-1}) = \delta(u_m)$, де $u_m = u_{i_0 i_1 i_2 ... i_{m-1}}$, який складається зі степенів усіх елементів $t_j^{i_j} \in L_j$, $j < n$, $j < m$, $j \in \mathbb{N}$, $i_j \in \overline{0, ..., p-1}$, які спрягають t_m у $u_{i_0 i_1 i_2 ... i_{m-1}}$. Наприклад, $u_{ijk0}^s = t_0^{-i} t_1^{-j} t_2^{-k} t_4^s t_2^k t_1^j t_0^i$, $\delta(u_{0123}) = (i, j, k, 0)$, t_m назвемо базовим елементом з $u_{i_0 i_1 i_2 ... i_{m-1}}$, через $\delta_{01...r-1}(u) = i_0 ... i_{r-1}$ позначимо перші координати індексу зсуву для $u_{i_0 i_1 i_2 ... i_{n-1}}$.

Легко переконатися, що елементи $u_{i_0 i_1 i_2 ... i_{n-1}}$ утворюють систему твірних.

Теорема 1. Група $G = (...((C_p \wr C_p) \wr C_p)...) \wr C_p$ – силовська p-підгрупа групи $S_{p^{n+1}}$ має козображення

$$\langle t_j \;\; j \in \{0, ..., n\} \mid t_j^p = e, [t_k^{-i} t_m t_k^i, t_l] = e,$$
$$1 \le i \le p-1, \;\; n \ge l \ge m > k \ge 0 \rangle.$$

Д о в е д е н н я. Кількість основних співвідношень становить

$$\sum_{j=1}^{n} (j(j+1):2)(p-1) + (n+1) - (n(n+1):2)(p-1):2,$$
$$n \ge m \ge l > k \ge 0.$$

Дійсно, кількість співвідношень комутації $[t_k^{-i} t_m t_k^i, t_l] = e$, $n \ge m \ge l > k \ge 0$ визначається так:

$$\sum_{l=0}^{n} \sum_{m=0}^{l} \sum_{k=0}^{m-1} 1 = \sum_{l=0}^{n} \sum_{m=0}^{l} m = \sum_{l=0}^{n} l(l+1) : 2 =$$
$$= \sum_{j=1}^{n} j(j+1) : 2,$$

оскільки доданок $l = 0$ можна не враховувати. Зазначимо, що $\frac{p-1}{2}$ – достатнє число ступенів i, при яких співвідношення вигляду $[t_k^{-i} t_l t_k^i, t_l] = e$ породжують усі інші співвідношення вигляду

$$[t_0^{i_0} t_1^{i_1} \cdot ... \cdot t_k^{-i} \cdot ... \cdot t_{l-1}^{-i_{m-1}} t_l t_{l-1}^{i_{m-1}} \cdot ... \cdot t_k^i \cdot ... \cdot t_1^{i_1} t_0^{i_0},$$
$$t_0^{-i_0} t_1^{-i_1} \cdot ... \cdot t_{k-1}^{-i_{k-1}} t_l t_{k-1}^{i_{k-1}} \cdot ... \cdot t_1^{i_1} t_1^{i_0}] = e,$$
$$[t_0^{-i_0} t_1^{-i_1} \cdot ... \cdot t_k^{-j_k} t_l t_k^{j_k} \cdot ... \cdot t_1^{i_1} t_0^{i_0},$$
$$t_0^{-i_0} t_1^{-i_1} \cdot ... \cdot t_{k-1}^{-i_{k-1}} t_k^{-s_k} \cdot ... \cdot t_l \cdot ... \cdot t_k^{s_k} t_{k-1}^{i_{k-1}} \cdot ... \cdot t_1^{i_1} t_1^{i_0}] = e.$$

Дійсно, при виведенні співвідношень з однаковими базовими елементами маємо

$$t_k^{-p+1} \left| t_k^{-1} t_l t_k t_l = t_l t_k^{-1} t_l t_k \right| t_k^{p-1} \Rightarrow$$
$$\Rightarrow t_l t_k^{-p+1} t_l t_k^{p-1} = t_k^{-p+1} t_l t_k^{p-1} t_l,$$

тому достатньо $\frac{p-1}{2}$ значень i. При різних базових елементах t_m, t_l у співвідношенні $t_k^{-1} t_l t_k t_m = t_m t_k^{-1} t_l t_k$ – необхідні p–1 значень $i \in \overline{0, ..., p-1}$ для такого породження. Тому враховуємо, що для співвідношень $t_k^{-i} t_l t_k^i t_l = t_l t_k^{-i} t_l t_k^i$ достатньо лише $\frac{p-1}{2}$ значень ступеня i.

Нехай N – нормальне замикання співвідношень R в групі $F(t_0, t_1, ..., t_n)$. Отже, маємо епіморфізм $F / N \to G$, заданий на твірних $t_i \mapsto x_{i+1}$ $(i = 0, ..., n)$. Тому $|F / N| \ge |G|$. Доведемо, що такий епіморфізм є ізоморфізмом. Для цього доведемо далі нерівність

$$|F / N| \le |(...((C_p \wr C_p) \wr C_p)...) \wr C_p| = p^{p^n + ... + p + 1}.$$

***Означення* 3.** Індексною структурою елемента $t_m^{i_k}$, де k – номер позиції t_m у $W = t_{j_0}^{i_0} t_{j_1}^{i_1} ... t_m^{i_k} ... t_{j_l}^{i_l}$ (в цьому слові $k = m$), є вектор, що складається із сумарних індексів зсуву, наведених по модулю p, які задаються попередніми елементами, які є елементами менших рангів і діють на цей елемент $t_m^{i_k}$, тобто це $\delta_{01...n-1}(t_m^{i_k}) = (s_0, s_1, ..., s_{m-1})$. Тут s_l – сума, взята по модулю p, степенів усіх елементів t_l, які діють на $t_m^{i_k}$, $l < m$. Позначимо $i_l(k) = \delta_l(t_m^{i_k})$, l-ю координату індексу зсуву елемента $t_m^{i_k}$ в слові W.

Доведемо, що із співвідношень

$$t_j^p = e, \quad [t_k^{-i} t_m t_k^i, t_l] = e, \; 1 < i \le p-1,$$

$$n \ge m, \;\; l \ge k \ge 0, \;\; j \in Z_{n+1},$$

виводяться інші:

$$[t_{i_0}^{-s_0} t_{i_1}^{-s_1} t_{i_2}^{-s_2} \ldots t_{i_{n-1}}^{-s_{n-1}} t_m^{s_n} t_{i_{n-1}}^{s_{n-1}} \ldots t_{i_2}^{s_2} t_{i_1}^{s_1} t_{i_0}^{s_0},$$

$$t_{j_0}^{-z_0} t_{j_1}^{-z_1} \ldots t_l^h \ldots t_{j_1}^{z_1} t_{j_0}^{z_0}] = e, \qquad (2)$$

а також співвідношення вигляду

$$v_{i_0 i_1 i_2 \ldots i_r}^{-s} u_{j_0 j_1 j_2 \ldots j_r \ldots j_{n-1}} = u_{j_0 j_1 j_2 \ldots j_{r+s} \ldots j_{n-1}} v_{i_0 i_1 i_2 \ldots i_r}^{-s}.$$

Дійсно, співвідношення, що залишилися, виводяться з цих:

$$t_k^{-i_k} t_l^{-i_l} t_k^{i_k} \mid t_k^{-i_k} t_b t_k^{i_k} t_m \mid t_k^{-i_k} t_l^{i_l} t_k^{i_k} =$$

$$= t_k^{-i_k} t_l^{i_l} t_k^{i_k} \mid t_m t_k^{-i_k} t_b t_k^{i_k} \mid t_k^{-i_k} t_l^{i_l} t_k^{i_k}, \; k < l < b < m,$$

$$t_k^{-i_k} t_l^{-i_l} t_b t_l^{i_l} t_k^{i_k} t_m = t_m t_k^{-i_k} t_l^{-i_l} t_b t_l^{i_l} t_k^{i_k},$$

тому $[t_k^{-i_k} t_l^{i_l} t_b t_l^{i_l} t_k^{i_k}, t_m] = e$, оскільки $t_k^{-i_k} t_l^{-i_l} t_k^{i_k} t_m = t_m t_k^{-i_k} t_l^{-i_l} t_k^{i_k}$,

$$t_l^{-i_l} \mid t_k^{-i} t_n t_k^i t_m \mid t_l^{i_l} = t_l^{-i_l} \mid t_m t_k^{-i} t_n t_k^i \mid t_l^{i_l}, \; k > l,$$

$$t_l^{-i_l} t_k^{-i} t_n t_k^i t_l^{i_l} t_l^{-i_l} t_m t_l^{i_l} = t_l^{-i_l} t_m t_l^{i_l} t_l^{-i_l} t_k^{-i} t_n t_k^i t_l^{i_l} \Rightarrow$$

$$\Rightarrow [t_l^{-i_l} t_k^{-i} t_n t_k^i t_l^{i_l}, t_l^{-i_l} t_m t_l^{i_l}] = e.$$

У випадку $k < l$ отримуємо можливість незалежного прирощення l-ї координати $\delta_{01\ldots b-1}(u_b)$, тому можемо нарощувати степінь кожного твірного, який має індекс більше k.

Далі аналогічними перетвореннями одержуємо довільний вираз вигляду (2).

При цьому істотною при виведенні співвідношень з $t_k^{-i} t_b t_k^i t_m = t_m t_k^{-i} t_b t_k^i$ є можливість лише паралельного нарощування ступенів – t_k^{i+j} і t_l, $l < k$.

Дійсно, $t_k^{-j} \mid t_k^{-i} t_l t_k^i t_k^{-s} t_m t_k^s = t_k^{-s} t_m t_k^s t_k^{-i} t_l t_k^i \mid t_k^j$, звідси $t_k^{-i-j} t_l t_k^{i+j} t_k^{-s-j} t_m t_k^{s+j} = t_k^{-s-j} t_m t_k^{s+j} t_k^{-i-j} t_l t_k^{i+j}$.

Таким чином, степені спряжених елементів змінилися на однакову величину. Тому, маючи співвідношення з різними величинами $\min\{|s-i|, p-|s-i|\}$, можна вивести всі співвідношення, тому достатньо взяти $1 \le i \le \frac{p-1}{2}$, $s = 0$.

Нехай на m-й ітерації перетворення маємо $u_{i_0 i_1 i_2 \ldots i_n} u_{j_0 j_1 \ldots j_n} = u_{j_0 j_1 \ldots j_n} u_{i_0 i_1 i_2 \ldots i_n}$, тобто індекси зсуву різні, тоді можливе незалежне нарощування індексу зсуву незалежно в кожному зі співмножників $u_{i_0 i_1 i_2 \ldots i_n}$, $u_{j_0 j_1 \ldots j_n}$.

Лема 3. Із співвідношення $u_{i_l i_{l+1} i_{l+2} \ldots i_b} u_{j_k j_{k+1} \ldots j_m} = u_{j_k j_{k+1} \ldots j_m} u_{i_l i_{l+1} i_{l+2} \ldots i_b}$, де $\delta(u_{m+1}) = j_k j_{k+1} \ldots j_m$, $\delta(u_{b+1}) = i_l i_{l+1} \ldots i_b$, випливають співвідношення, що мають елементи з довільними індексними структурами, крім індексу з найменшим номером в індексній структурі елементів цього співвідношення, тобто $\{j_k, j_{k+1}, \ldots, j_m; i_l, i_{l+1}, \ldots, i_b\}$, $k < l$, який нарощується одночасно в обох частинах.

Спочатку доведемо для часткового випадку. Перетворимо ліву частину рівності $u_{i_0 i_1 i_2 \ldots i_n} u_{j_0 j_1 \ldots j_b} = u_{j_0 j_1 \ldots j_b} u_{i_0 i_1 i_2 \ldots i_n}$, права частина перетвориться аналогічно:

$$t_0^{-i_0} t_1^{-i_1} \ldots t_{k-1}^{-i_{k-1}} t_k^{-m} t_{k-1}^{i_{k-1}} \ldots t_1^{i_1} t_0^{i_0} \mid u_{i_0 i_1 i_2 \ldots i_n} u_{j_0 j_1 \ldots j_b} =$$

$$= u_{j_0 j_1 \ldots j_b} u_{i_0 i_1 i_2 \ldots i_n} \mid t_0^{-i_0} t_1^{-i_1} \ldots t_k^m \ldots t_1^{i_1} t_0^{i_0}.$$

Розглянемо зміну в результаті спряження:

$$u_{i_0 i_1 i_2 \ldots i_n} u_{j_0 j_1 \ldots j_b} : (t_0^{-i_0} t_1^{-i_1} \ldots t_{k-1}^{-i_{k-1}} t_k^{-m} t_{k-1}^{i_{k-1}} \ldots t_1^{i_1} t_0^{i_0}) \times$$

$$\times t_0^{-i_0} t_1^{-i_1} \ldots t_k^{-i_k} \ldots t_n \ldots t_k^{i_k} \ldots t_1^{i_1} t_0^{i_0} \times$$

$$\times \underbrace{(t_0^{-i_0} \ldots t_{k-1}^{i_{k-1}} t_k^m t_{k-1}^{i_{k-1}} \ldots t_0^{i_0} \cdot t_0^{-i_0} \ldots t_k^{-m} \ldots t_0^{i_0})}_{e} \times$$

$$\times t_0^{-j_0} t_1^{-j_1} \ldots t_b^{j_n} \ldots t_1^{j_1} t_0^{j_0} (u_{i_0 \ldots i_{k-1}}^m u_{i_0 \ldots i_{k-1}}^{-m}) =$$

$$= u_{i_0 \ldots i_{k-1}}^{-m} u_{i_0 i \ldots i_n} (u_{i_0 \ldots i_{k-1}}^m u_{i_0 \ldots i_{k-1}}^{-m}) u_{j_0 \ldots j_b} u_{i_0 \ldots i_{k-1}}^m =$$

$$= t_0^{-i_0} t_1^{-i_1} \ldots t_k^{-m} t_k^{-i_k} \ldots t_n \ldots t_k^{i_k} t_k^m \ldots t_1^{i_1} t_0^{i_0} \times$$

$$\times t_0^{-j_0} t_1^{-j_1} \ldots t_b^{j_n} \ldots t_1^{j_1} t_0^{j_0} = u_{i_0 i_1 \ldots, k+m, \ldots n} u_{j_0 j_1 \ldots j_b}.$$

Тут змінилась k-та координата індексу зсуву елемента $u_{i_0 i_1 \ldots i_n}$ внаслідок спряження його елементом рангу k, який має відповідний індекс зсуву $\delta(u_k) = i_0 i_1 \ldots i_{k-1}$, тобто елементом $u_{i_0 \ldots i_{k-1}}^m$.

Аналогічні перетворення для решти n індексів, крім 0. Так можна вивести співвідношення з будь-якими індексами зсуву, крім найменшої координати, яка нарощується паралельно. Аналогічно для рівності

$$u_{i_l i_{l+1}\dots i_b} u_{j_k j_{k+1}\dots j_m} = u_{j_k j_{k+1}\dots j_m} u_{i_l i_{l+1}\dots i_b}$$

$$t_k^{-m} \mid u_{i_0 i_1 i_2 \dots i_n} u_{j_0 j_1 \dots j_b} = u_{j_0 j_1 \dots j_b} u_{i_0 i_1 i_2 \dots i_n} \mid t_k^m \Rightarrow$$

$$\Rightarrow t_k^{-i_k - m} t_{k+1}^{-i_{k+1}} \dots t_n \dots t_{k+1}^{i_{k+1}} t_k^{i_k + m}\ t_k^{-m} t_l^{-i_l} t_{l+1}^{-i_{l+1}} \dots t_m \dots t_{l+1}^{i_{l+1}} t_l^{i_l} t_k^m =$$

$$= t_k^{-m} t_l^{-i_l} t_{l+1}^{-i_{l+1}} \dots t_m \dots t_{l+1}^{i_{l+1}} t_l^{i_l} t_k^m\ t_k^{-i_k - m} t_{k+1}^{-i_{k+1}} \dots t_n \dots t_{k+1}^{i_{k+1}} t_k^{i_k + m},$$

у результаті отримаємо $u_{s_k i_l i_{l+1} \dots i_b} u_{j_k + s_k j_{k+1} \dots j_m} = u_{j_k + s_k, j_{k+1} \dots j_m} u_{s_k i_l i_{l+1} \dots i_b}$.

Лема 4. За умови $\delta(u_{i_0 \dots i_{n-1}}) = i_0 i_1 \dots i_k j_{k+1} \dots j_{n-1}$, $\delta(u_{i_0 \dots i_{b-1}}) = i_0 i_1 \dots i_k i_{k+1} \dots i_b$ маємо можливість лише паралельного нарощування для 0-го, ..., k-го індексів $u_{i_0 i_1 \dots i_n} u_{i_0 \dots i_k j_{k+1} \dots j_b} = u_{i_0 \dots i_k j_{k+1} \dots j_b} u_{i_0 i_1 \dots i_n}$.

Доведемо це для k-го, для решти k–1-індексів аналогічно:

$$u_{i_0 i_1 i_2 . i_{k-1} .. i_n} u_{i_0 i_1 .. i_{k-1} j_k .. j_b} = u_{i_0 i_1 .. i_{k-1} j_k .. j_b} u_{i_0 i_1 i_2 \dots i_n} \Rightarrow$$

$$\Rightarrow u_{i_0 i_1 \dots, i_k + m, \dots n} u_{i_0 i_1 \dots, j_k + m, \dots j_b} = u_{i_0 i_1 \dots, j_k + m, \dots n} u_{j_0 j_1 \dots, i_k + m, \dots j_b}.$$

Для доведення леми перетворимо ліву частину рівності, в правій частині робимо аналогічні перетворення:

$$t_0^{-i_0} t_1^{-i_1} \dots t_{k-1}^{-i_{k-1}} t_k^{-m} t_{k-1}^{i_{k-1}} \dots t_1^{i_1} t_0^{i_0} \mid u_{i_0 i_1 i_2 \dots i_n} u_{i_0 i_1 . i_k .. j_b} =$$

$$= u_{i_0 i_1 \dots j_b} u_{i_0 i_1 i_2 \dots i_n} \mid t_0^{-i_0} t_1^{-i_1} \dots t_k^m \dots t_1^{i_1} t_0^{i_0} \Rightarrow$$

$$= (t_0^{-i_0} t_1^{-i_1} \dots t_{k-1}^{-i_{k-1}} t_k^{-m} t_{k-1}^{i_{k-1}} \dots t_1^{i_1} t_0^{i_0}) t_0^{-i_0} t_1^{-i_1} \dots t_k^{-i_k} \dots t_n \dots t_k^{i_k} \times$$

$$\times \dots t_1^{i_1} t_0^{i_0} (t_0^{-i_0} \dots t_{k-1}^{i_{k-1}} t_k^m t_{k-1}^{i_{k-1}} \dots t_0^{i_0} \cdot t_0^{-i_0} \dots t_k^{-m} \dots t_0^{i_0}) \times$$

$$\times t_0^{-i_0} t_1^{-i_1} .. t_k^{-j_k} . t_b^{j_n} . t_k^{j_k} .. t_2^{i_1} t_0^{i_0} (t_0^{-i_0} t_1^{-i_1} \dots t_k^m \dots t_1^{i_1} t_0^{i_0}) =$$

$$= u_{i_0 \dots i_{k-1}}^{-m} u_{i_0 \dots i_n} (u_{i_0 \dots i_{k-1}}^m u_{i_0 \dots i_{k-1}}^{-m}) u_{i_0 \dots j_b} u_{i_0 \dots i_{k-1}}^m =$$

$$= t_0^{-i_0} t_1^{-i_1} \dots t_k^{-m} t_k^{-i_k} \dots t_n \dots t_k^{i_k} t_k^m \dots t_1^{i_1} t_0^{i_0} \times$$

$$\times t_0^{-j_0} t_1^{-j_1} .. t_k^{-m} t_k^{-j_k} . t_b^{j_n} .. t_k^m t_k^{-j_k} . t_2^{j_1} t_0^{j_0} =$$

$$= u_{i_0 i_1 \dots, i_k + m, \dots n} u_{j_0 j_1 .., j_k + m, \dots j_b}.$$

Тут змінилась k-та координата індексу зсуву всіх елементів при спряженні їх елементом рангу k, оскільки $t_k^{-i_k}$ має такий самий індекс зсуву $\delta(u) = i_0 i_1 \dots i_{k-1}$ і діє на всі елементи більшого рангу в $u_{i_0 i_1 i_2 \dots i_n} u_{i_0 i_1 . i_k .. j_b}$. Для індексів $0 \dots k-1$ міркування аналогічні.

Зазначимо, що при $\delta_{12\dots r-1}(u_r) = \delta_{12\dots r-1}(v_n)$ для $u_{i_0 i_1 .. i_{r-1}} \in L_r$ і $v_{i_0 i_1 .. i_{n-1}} \in L_n$, $r < n$, маємо $v_{i_0 i_1 i_2 \dots i_r}^{-s} u_{i_0 i_1 i_2 \dots i_r \dots j_{n-1}} = u_{i_0 i_1 i_2 \dots, i_r + s, j_{r+1}, \dots j_{n-1}} v_{i_0 i_1 i_2 \dots i_r}^{-s}$.

Дійсно, при такому збігу індексів зсуву для елементів t_r із $v_{i_0 i_1 i_2 \dots i_{r-1}}^{-s}$ і $u_{i_0 i_1 i_2 \dots i_r \dots j_{n-1}}$ елемент $v_{i_0 i_1 i_2 \dots i_{r-1}}^{-s}$ після переміщення до елемента $t_r \in u_{i_0 i_1 i_2 \dots i_r \dots j_{n-1}}$ буде мати індекс зсуву такий самий, як і елемент $t_r^{i_r}$ з $u_{i_0 i_1 i_2 \dots i_r \dots j_{n-1}}$, тому $v_{i_0 i_1 i_2 \dots i_{r-1}}^{-s}$ діє на всі наступні елементи (тобто на елементи, що мають ранг R_m, $n \ge m > r$) лівим зсувом.

Іншими словами,

$$v_{i_0 i_1 i_2 \dots i_{r-1}}^{-s} u_{i_0 i_1 i_2 \dots i_r \dots i_{n-1}} = t_0^{-i_0} t_1^{-i_1} t_2^{-i_2} \dots t_r^{-s} \dots t_2^{i_2} t_1^{i_1} t_0^{i_0} \times$$

$$\times t_0^{-i_0} t_1^{-i_1} t_2^{-i_2} \dots t_{n-1}^{-i_{n-1}} t_n t_{n-1}^{i_{n-1}} \dots t_2^{i_2} t_1^{i_1} t_0^{i_0} =$$

$$= t_0^{-i_0} t_1^{-i_1} t_2^{-i_2} \dots t_r^{-s} \dots t_2^{i_2} t_1^{i_1} t_1^{-i_1} e t_2^{-i_2} \dots t_{n-1}^{-i_{n-1}} t_n t_{n-1}^{i_{n-1}} \dots t_2^{i_2} t_1^{i_1} t_0^{i_0} =$$

$$= t_0^{-i_0} t_1^{-i_1} t_2^{-i_2} \dots t_r^{-s-i_r} t_{r+1}^{-i_{r+1}} \dots t_{n-1}^{-i_{n-1}} t_n t_{n-1}^{i_{n-1}} \dots t_2^{i_2} t_1^{i_1} t_0^{i_0} \cdot e =$$

$$= t_0^{-i_0} t_1^{-i_1} \dots t_r^{-s-i_r} t_{r+1}^{i_{r+1}} \dots t_{n-1}^{-i_{n-1}} t_n t_{n-1}^{i_{n-1}} \dots t_{r+1}^{i_{r+1}} t_r^{s+i_r} \dots t_2^{i_2} t_1^{i_1} t_0^{i_0} \times$$

$$\times t_0^{-i_0} t_1^{-i_1} t_2^{-i_2} \dots t_r^{s} \dots t_2^{i_2} t_1^{i_1} t_0^{i_0} t_0^{-i_0} t_1^{-i_1} t_2^{-i_2} \dots t_r^{-s} \dots t_2^{i_2} t_1^{i_1} t_0^{i_0} =$$

$$= t_0^{-i_0} t_1^{-i_1} \dots t_r^{-s-i_r} t_{r+1}^{i_{r+1}} \dots t_{n-1}^{-i_{n-1}} t_n t_{n-1}^{i_{n-1}} \dots t_{r+1}^{i_{r+1}} t_r^{s+i_r} \times$$

$$\times \dots t_2^{i_2} t_1^{i_1} t_0^{i_0} \cdot t_0^{-i_0} t_1^{-i_1} t_2^{-i_2} \dots t_r^{-s} \dots t_2^{i_2} t_1^{i_1} t_0^{i_0} =$$

$$= u_{i_0 i_1 i_2 \dots i_r + s \dots i_{n-1}} v_{i_0 i_1 i_2 \dots i_{r-1}}^{-s}.$$

Таким чином, рівність виведена.

***Означення* 4.** Канонічним словом – W_c – цього класу еквівалентних слів називається найкоротше слово, що складається з елементів $u_{i_0 i_1 i_2 \dots i_{m-1}} = t_0^{-i_0} t_1^{-i_1} \dots t_{m-1}^{-i_{m-1}} t_m t_{m-1}^{i_{m-1}} \dots t_1^{i_1} t_0^{i_0}$, $m \le n$, $i_j \in \overline{0, \dots, p-1}$, причому їх добуток упорядкований по спаданню номерів рангів, тобто на початку слова стоять елементи n-го рангу, потім n–1-го і так далі до елемента 0-го рангу – $u_{00\dots 0}$. Між собою елементи кожного рангу впорядковані по зростанню індексу зсуву.

Лема 5. Покажемо, що в кожному фактор-класі групи F/N є представник, який є словом вигляду W_c.

Будь-який елемент групи F/N, тобто слово довільної довжини, можна подати у вигляді добутку множників $u_{i_0 i_1 i_2 \dots i_{m-1}}$, використовуючи вказані у теоремі 1 співвідношення, а також співвідношення

$$v_{i_0, i_1 \dots i_r}^{-s} u_{i_0, i_1 \dots i_r \dots j_{n-1}} = u_{i_0, i_1, i_2 \dots, i_r + s, j_{r+1}, \dots j_{n-1}} v_{i_0, i_1 \dots i_r}^{-s}$$

і наступний переписуючий процес:

а) рухаючись по елементах слова, знаходимо перший елемент, індекс зсуву якого менший від попереднього;

б) знайдений елемент групи відмінюємо всіма попередніми і, взявши його в дужки, виносимо отриманий добуток на початок слова, залишивши дублікат усіх елементів, крім знайденого, на тому самому місці;

в) починаючи з місця інверсії, повторюємо процес, але спрягаючи всіма попередніми елементами, що мають індекс, менший за індекс елемента, який дав наступну інверсію порядку індексів. Таким чином, елементи з R_i можуть спрягатися лише елементами $t_0, t_1, \ldots, t_{i-1}$:

$$W = t_0^{-i_0} t_1^{-i_1} \mathrm{t}_2^{-i_2} t_1^{-i_3} t_k^{-i_4} t_n^{i_5} t_{i_5}^{-i_5} \ldots t_{i_l}^{i_h} =$$

$$= (t_0^{-i_0} t_1^{-i_1} t_2^{-i_2} t_1^{i_1} t_0^{i_0}) t_0^{-i_0} t_1^{-i_1} \cdot t_1^{-i_3} t_k^{-i_k} t_1^{i_3} t_1^{i_1} t_0^{i_0} \ldots =$$

$$= (t_0^{-i_0} t_1^{-i_1} t_2^{-i_2} t_1^{i_1} t_0^{i_0})(t_0^{-i_0} t_1^{-i_1} t_1^{-i_3} t_k^{-i_k} t_1^{i_3} t_2^{i_2} t_1^{i_1} t_0^{i_0}) \ldots =$$

$$= (t_0^{-i_0} t_1^{-i_1} t_2^{-i_2} t_1^{i_1} t_0^{i_0})(t_0^{-i_0} t_1^{-i_1 - i_3} t_k^{-i_k} t_1^{i_1 + i_3} t_0^{i_0}) =$$

$$= (t_0^{-s_0} t_1^{-s_1} t_2^{-s_2} t_1^{s_1} t_0^{s_0})(t_0^{-s_0} t_1^{-s_3} t_k^{-s_k} t_1^{s_3} t_0^{s_0}) \ldots,$$

$$s_3 = i_1 + i_3,\ s_1 = i_1,\ s_2 = i_2,\ s_k = i_k.$$

Елемент $t_2^{-s_2}$ у других дужках другої рівності пропущений, оскільки він діє лівим зсувом на базовий елемент $t_k^{-i_k}$, що надав наступну інверсію порядку індексів, перебуваючи зліва від нього в перших дужках, де $| s_i |$ належить наведеній системі лишків по модулю *p*. Далі, застосовуючи співвідношення, справедливі в цій групі, упорядковуємо так:

$$W = (t_{j_0}^{-s_{j0}} t_{j_1}^{-s_{j1}} t_{j_2}^{-s_{j2}} t_{j_3}^{-s_{j3}} t_{j_4}^{-s_4} t_n^{j_1} t_{j_4}^{s_{j4}} t_{j_3}^{s_{j3}} t_{j_2}^{s_{j2}} t_{j_1}^{s_{j1}} t_{j_0}^{s_{j0}}) \cdot \ldots$$

$$\ldots \cdot (t_{i_0}^{-s_{i0}} t_{i_1}^{-s_{i1}} t_{i_2}^{-s_{i2}} t_{i_3}^{-s_{i3}} t_{i_4}^{-s_{i4}} t_{i_5}^{-s_{i5}} t_{i_6}^{-s_{i6}} \times$$

$$\times t_{i_7}^{-s_{i6}} t_n^{j_2} t_{i_7}^{s_{i7}} t_{i_6}^{s_{i6}} t_{i_5}^{s_{i5}} t_{i_4}^{s_{i4}} t_{i_3}^{s_{i3}} t_{i_2}^{s_{i2}} t_{i_1}^{s_{i1}} t_{i_6}^{s_{i0}}) \cdot \ldots$$

$$\ldots \cdot (t_{z_0}^{-s_{z0}} t_{z_1}^{-s_{z1}} \ldots t_{z_l}^{-s_{zl}} t_n^{s_b} t_{z_l}^{s_{zl}} \ldots t_{z_1}^{s_{z1}} t_{i_0}^{s_{z0}}) \cdot \ldots$$

$$\ldots \cdot (t_1^{-s_w} t_2^{-s_e} t_1^{-s_w}) t_n^{z_n} \cdot \ldots \cdot t_3^{z_3} t_2^{z_2} t_1^{z_1} t_0^{-z_0},$$

$i_0 \le j_0$, якщо $i_0 = j_0$, то $s_{j_0} < s_{i_0}$ ..., де в дужках стоять елементи $u_{i_0 i_1 \ldots i_{k-1}}$, $0 \le k \le n$, базовий елемент яких сполучається серією елементів менших рангів, що розміщені перед ним, але поза дужками в процесі переписування, застосованого до слова *W*. Тепер перепишемо *W* у твірних $u_{i_0 i_1 \ldots i_n}$ і, використовуючи співвідношення та їх наслідки вигляду $u_{ijk}^s u_{i,j,k,k+1,\ldots,l} = u_{i,j,k,k+1+s,\ldots,l} u_{ijk}^s$, зводимо до W_c. Для цього упорядковуємо елементи $u_{i_0 i_1 \ldots i_k}$ за спаданням рангів базових елементів, при збігу рангів упорядковуємо у зворотному лексикографічному порядку індексів зсуву. Далі у виразах $u_{i_0 i_1 \ldots i_n}$ *n*-го рангу в початок слова ставимо елемент з найменшим вектором індексу зсуву. Згідно з координатним порядком, це $i_0, \ldots, i_{n-1}$. Аналогічно впорядковуємо елементи n–1-го рангу. В кінці слова дописуємо елемент t_0^k, де $k_0 = \deg(\prod t_0^{s_i}) \bmod p$.

***Означення* 5.** Відповідність результуючих степенів елементів з усіма індексами зсуву з *W*, записаним у вигляді таблиці, елементами якої є ці степені, впорядковані у зворотному лексикографічному порядку по $\delta_{0,\ldots,m-1}(t_m^{i_k}) = (i_0, i_1, i_2 \ldots i_{m-1})$ цих елементів з *W*, називається степеневою структурою елемента $t_m^{i_k}$.

Легко перевірити, що слова з рівними степеневими структурами — еквівалентні. Зрозуміло, що елементи є базовими в $u_{i_0 i_1 \ldots i_n}$, із W_c мали інші позиції в *W*, але їх індекси зрушень не змінилися. Результуючі ступені для елементів зі всілякими індексами зсуву також не змінилися, тому не змінилася і степенева структура вихідного слова. Дійсно, *j*-та координата індексу зсуву для базового елемента в $u_{i_0 i_1 i_2 \ldots i_{n-1}}^{s_k}$ з W_c дорівнює *j*-й координаті індексу зсуву для елемента $t_n^{i_m} \in W$, тобто $\delta_j(t_n^{i_m}) = i_j(m)$, де m — номери місць елементів t_n^m:

$$\delta(u_{i_0, i_1 \ldots i_{m-1}}) = (i_0, i_1, i_2 \ldots i_{m-1}) =$$

$$= \delta_{01 \ldots n-1}(t_n^{i_m}) = (i_0, i_1, i_2 \ldots i_{n-1}),$$

оскільки послідовність активних щодо $t_n^{i_k}$ елементів в слові W, які стоять перед ним і діють на ньому, збігається із спрягаючою послідовністю для цього елемента в $u_{i_0 i_1 i_2 \ldots i_{n-1}}^{s_j}$ згідно з побудовою переписуючого процесу слів. Отримуємо $W_c = u_{i_0 i_1 i_2 \ldots i_n} \cdot \ldots \cdot u_{j_0 j_1 \ldots j_n} \cdot u_{k_0 k_1 \ldots k-1} \ldots u_{l_0 \ldots l_{n-1}} \cdot \ldots \cdot u_{i_0} t_0^{z_0}$, s_k — результуючий степінь елементів з індексом зсуву, рівним $\delta_{01 \ldots n-1}(t_n^{i_k}) = (i_0, i_1, i_2 \ldots i_{n-1})$.

Звідси випливає, що $|F / N| \le p^{p^n+\ldots+p+1}$, оскільки деякі канонічні слова теоретично можуть виявитися рівними. Однак переконаємося в тому, що всі канонічні слова різні. Для елементів $n+1$-го рангу кількість різних $\delta(u_{i_0 i_1 \ldots i_n})$ дорівнює p^n, тому кількість різних елементів $n+1$-го рангу — p^{p^n}, аналогічно кількість елементів n-1-го рангу — $p^{p^{n-1}}$, ... , 1-го рангу — p, 0-го рангу – 1, тому всього їх $p^{p^n+\ldots+p+1}$.

Оскільки маємо також нерівність $|F / N| \ge$ $\ge p^{p^n+\ldots+p+1}$, отриману з епіморфізму і, з огляду на наведену вище нерівність зі зворотним знаком, зрозуміло, що вона вироджується в рівність

$$|F / N| = |(\ldots((C_p \wr C_p) \wr C_p)\ldots) \wr C_p| = p^{p^n+\ldots+p+1},$$

тому маємо ізоморфізм. Отже, козображення правильне. Властивості конормальності твірні з G не мають, бо C_p — проста група, тому ознака мінімальності системи твірних з [1] до G незастосовна. Тому мінімальність доведемо окремо.

Теорема 2. Описана система твірних є зведеною, тобто жоден з твірних не можна виразити через інші, і має мінімальне число співвідношень.

Доведення подамо трьома кроками:

1. Легко переконатися, що k-кратний добуток регулярних циклічних груп має мінімум k твірних такого виду. Очевидно, якщо відкинути співвідношення $t_i^p = e$, то отримаємо групу нескінченного порядку. Далі, використовуючи індукцію по змінних, база якої t_1, t_2 в $C_p \wr C_p$.

Означення 6. Глибиною зсуву твірного t_2 у співвідношенні $t_1^{-i} t_2 t_1^i t_1^{-j} t_2 t_1^j = t_1^{-j} t_2 t_1^j t_1^{-i} t_2 t_1^i$ називається $hzt_1(per) := \min\{|j-i|,\ p-|j-i|\}$. Наприклад, для $t_1^{-p+2} t_2 t_1^{p-2} t_2 = t_2 t_1^{-p+2} t_2 t_1^{p-2}$ маємо $hzt_1(per) = 2$, позначеним

$$r_1 = t_1^{-1} t_2 t_1 t_2 t_1^{-1} t_2^{-1} t_1 t_2^{-1} = e. \quad (3)$$

Покажемо, що всілякі спряження співвідношень не змінюють їх величину $hzper(u_k u_0)$. Покажемо це для $X = \{t_1^m, t_2^n\}$ як бази індукції, а всі інші слова виражаються через них, тому теж не змінять $hzper(u_k u_0) = k$. Розглянемо

$$r_k = t_1^{-k} t_2^j t_1^k t_2^z \ t_1^{-k} t_2^{-j} t_1^k t_2^{-z} = e.$$

Представимо його через степені

$$t_1^k,\ hzt_1(u_k u_0) = k = |k-0|,\ m, z, j \in \{0, 1, \ldots, p-1\},$$

$$k < \frac{p-1}{2};$$

$$t_1^{-m}(t_1^{-k} t_2^j t_1^k t_2^z t_1^{-k} t_2^{-j} t_1^k t_2^{-z})\ t_1^m =$$

$$= t_1^{-k-m} t_2^j t_1^{k+m} t_1^{-m} t_2^z (t_1^m t_1^{-m}) t_1^{-k} t_2^{-j} t_1^k (t_1^m t_1^{-m}) t_2^{-z} t_1^m =$$

$$= t_1^{-k-m} t_2^j t_1^{k+m} t_1^{-m} t_2^z t_1^m \ t_1^{-k-m} t_2^{-j} t_1^{k+m} t_1^{-m} t_2^{-z} t_1^m =$$

$$= t_1^{-m} \mid r_k \mid t_1^m = e \Rightarrow t_1^{-k-m} t_2^j t_1^{k+m} \ t_1^{-m} t_2^z t_1^m =$$

$$= t_1^{-m} t_2^z t_1^m \ t_1^{-k-m} t_2^j t_1^{k+m},\ hzt_1(u_m u_{k+m}) = k =$$

$$= |k+m-m|,\ k < \frac{p-1}{2};.$$

Спрягли вирази r_k з елементом t_1^m і знову знайшли величину $hzt_1(per)$, очевидно, що вона не змінилась.

Легко перевірити, що $hzt_1(per)$ не зміниться і при спряженні елементом t_2^m, оскільки t_2^m не діє ні на один елемент. Покажемо це:

$$t_2^{-m}\ (t_1^{-k} t_2^j t_1^k t_2^z) t_2^m = t_2^{-m} (t_2^z t_1^{-k} t_2^j t_1^k)\ t_2^m \Leftrightarrow$$

$$\Leftrightarrow t_2^{-m} t_1^{-k} t_2^j t_1^k t_2^m t_2^z t_2^m = t_2^{-m} t_2^z t_2^{-m} t_1^{-k} t_2^j t_1^k t_2^m \Leftrightarrow$$

$$\Leftrightarrow t_1^{-k} t_2^j t_{p-k+1}^{-m} t_1^k t_2^m t_2^z = t_2^z t_2^{-m} t_1^{-k} t_{k+2}^m t_2^j t_1^k =$$

$$= t_1^{-k} t_2^j t_1^k (t_2^{-m} t_2^m) t_2^z = t_2^z (t_2^{-m} t_2^m) t_1^{-k} t_2^j t_1^k \sim u_k^j u_0^z = u_0^z u_k^j.$$

Таким чином, спряження не змінює значення $hzt_1(per)$, але нарощує індекси на однакову величину при спряженні елементом t_1^m і не змінює величини $hzt_1(per)$ при спряженні елементом t_2^m. Звідси випливає, що спряження довільною комбінацією елементів $t_1^m t_2^n t_1^l t_2^k t_1^j t_2^i \ldots$ не змінить глибини зсуву $hzt_1(per)$, тобто не дасть нового співвідношення.

2. Проаналізуємо нормальне замикання множини

$$R = \left\{ r_2, r_3, \ldots, r_m,\ m = \frac{p-1}{2} \right\},$$

де r_i — твірні нормального замикання, які є співвідношеннями з глибиною зсуву *i*.

***Означення* 7.** Глибиною зсуву $hzt_k(w, t_n^{i_m}, t_n^{i_k})$ елементів $t_n^{i_m}$, $t_n^{i_k}$ для довільного слова $w \in N(R)$ називається модуль різниці їх *k*-х координат індексу зсуву $\delta_k(t_n^{i_m}) = i_k(m)$ і $\delta_k(t_n^{i_l}) = i_k(l)$, де $i_k(m)$ *k*-та координата індексу зсуву елемента $t_n^{i_m}$ в слові *W*, тобто сума степенів усіх елементів t_k, що діють на $t_n^{i_m}$.

Глибиною зсуву $hzt_k(r, t_n^{i_m})$ елемента $t_n^{i_m}$ у співвідношенні *r* для довільного співвідношення називається *k*-та координата індексу зсуву $i_l(k) = \delta_l(t_m^{i_k})$.

Лема 6. Вставка слів, що рівні *e*, в слова вигляду $t_{i_1}^{-j} \ldots t_{i_{n-1}}^{-l_{n-1}} t_n t_{i_{n-1}}^{l_{n-1}} \ldots t_1^j t_n t_{i_1}^{-j} \ldots t_{i_{n-1}}^{-l_{n-1}} t_n^{-1} t_{i_{n-1}}^{l_{n-1}} \ldots t_1^j t_n^{-1} = e$, наприклад, $v = r_j = t_1^{-j} t_2 t_1^j t_2 t_1^{-j} t_2^{-1} t_1^j t_2^{-1}$, де $hzt_1(per) = hzt_1(r, t_2) = j$, а також заміни типу

$$\begin{aligned} t_2 t_1^{-1} &= t_1^{-1} t_1 t_2 t_1^{-1}, \\ t_{l_k} t_1^{-1} &= t_1^{-1} t_1 t_{l_k} t_1^{-1} \end{aligned} \tag{4}$$

не змінять $hzt_1(r_j, t_2^{i_m}, t_2^{i_k})$, тобто $hzt_1(per) = j = hzt_1(r_j', t_2^{i_m}, t_2^{i_k})$, де r_j' — слово r_j після перетворення, аналогічно $hzt_1(r_j', t_{l_k}^{i_k}, t_{l_m}^{i_m})$ і для $hzt_{l_s}(r_j', t_{l_k}^{i_k}, t_{l_m}^{i_m}), 1 \le l_s < l_k \le n.$

Доведення. Вставка слів, рівних *e,* не змінить індексів зсуву $\delta_1(t_2^{i_m}) = i_1(m)$ і $\delta_1(t_2^{i_k}) = i_1(k)$. Підрахуємо зміну цих самих індексів зсуву внаслідок застосування перетворення (4). Очевидно, що це перетворення не змінить сумарних індексів зсуву, що задані сумами степенів попередніх елементів t_1.

***Означення* 8.** Визначимо для довільного слова $w \in N(R)$ величину $lz(t_1, k, t_2, \upsilon, w) = \sum_{i=0}^{l} \deg(t_1^{s_{j_i}})$, l — число елементів t_1 перед t_2 з $w\upsilon$, k — номер елемента t_2 в підслові υ, $k \in \overline{0, n}$, до якого зроблено перетворення.

У загальному випадку $\wr_1^n C_p$ буде мати

$$lz(t_p, k, t_q, \upsilon, w) = \sum_{i=0}^{l} \deg(t_p^{s_i}),$$

де l — число елементів t_p перед t_q, $p < q$, з $w\upsilon$, k — номер елемента t_q в підслові υ, $k \in \overline{0, n}$, до якого зроблено перетворення, а величина $\deg(t_i^{s_i}) := \begin{cases} s_i, & t_i = t_p, \\ 0, & t_i \ne t_p. \end{cases}$

Властивість. Перетворення вставки, закреслення слів, еквівалентних *e* у слові w_0, а також перетворення типу (3) слова w_0 на слово w_1 залишають величину $lz(t_1, k_1, t_2, v, w_1)$ рівною $lz(t_1, k_0, t_2, v, w_0)$. Тобто ця величина є інваріантною відносно цих перетворень, де w_0 і w_1 — еквівалентні слова, а k_0 і k_1 — місця елемента t_2 (в загальному випадку t_q) до і після перетворення.

Зауваження. Необхідною умовою виведення співвідношення з $hzt_1(per) = 1$ із співвідношень з $hzt_1(\mathrm{per}) \ne 1$ є зміна величини $lz(t_1, k, t_2, v, w)$.

Зрозуміло, що для випадку $C_p \wr C_p$ при такому виведенні степені *i* та *j* мають стати $\min\{|j - i|, \ p - |j - i|\} = 1$ у якомусь зі слів вигляду $t_1^{-i} t_2^m t_1^i t_1^{-j} t_2^z t_1^j \cdot t_1^{-i} t_2^{-m} t_1^i t_1^{-j} t_2^{-z} t_1^j = e.$

Доведення. Застосуємо перетворення (4), яке є елементарним перетворенням, а не співвідношенням, яке не змінює $lz(t_1, k, t_2, v, w)$ для всіх t_2, і аналогічні перетворення. Тому досягти за допомогою таких перетворень зміни $hzt_1(per)$ з довільного *i* на одиницю неможливо. Залишаються лише елементарні перетворення — вставка і закреслення *e*:

- для вставки послідовностей, де скрізь стоять $t_1^{-i} t_1^i, t_2 t_2^{-1}, \ldots,$ можна застосовувати перетворення типу (4) і елементарні перетворення. Співвідношення тут відсутні, в результаті виводимо

$$t_1^i t_1^{-i} t_2 t_2^{-1}\, e = t_1^i t_1^{-i} t_2 t_1^i t_1^{-i} t_2^{-1} (t_1^i t_1^{-i}) =$$

$$t_1^i (t_1^{-i} t_2 t_1^i t_1^{-i} t_2^{-1} t_1^i) t_1^{-i} = t_1^i (t_1^{-i} t_2 t_1^i t_1^{-i} t_2^{-1} t_1^i\ (t_2^{-1} t_2)) t_1^{-i},$$

але, як сказано вище, зі слів у дужках не виводяться потрібні співвідношення, оскільки немає співвідношень, які переставлять t_2 на потрібне місце з метою виведення (2). Іншими словами, зроблені перетворення не змінили $lz(t_1, k, t_2, v, w)$ для всіх k;

- вставка одиничних слів одне в інше: $uv = ut_1^i t_1^{-i} v = ut_1^{-i} t_2 t_2^{-1} t_1^i v = ut_1^{-i} t_2 t_1^i t_1^{-i} t_2^{-1} t_1^i v$ — дає підслово, отримане в а).

Проаналізуємо, що дає застосування перестановок, які визначаються співвідношеннями з R.

Покажемо невивідність співвідношень (2) з $hzt_1(per) = 1$ множенням r_j на $r_k^{\pm 1}: j - k = 1$, де $j, k \in \mathbb{N}$.

Нехай виключено $r_1 = t_1^{-1} t_2 t_1 t_2 \cdot t_1^{-1} t_2^{-1} t_1 t_2^{-1}$, а разом з тим усі з $hzt_1(per) = 1$:

$$r_1 = t_1^{-k} t_2 t_1^k t_1^{-k-1} t_2 t_1^{k+1} \; t_1^{-k} t_2^{-1} t_1^k t_1^{-k-1} t_2^{-1} t_1^{k+1} =$$
$$= u_k u_{k+1} u_k^{-1} u_{k+1}^{-1}.$$

Зазначимо, що інваріантом для r_1 є чергування індексів зсуву, різниця яких рівна 1, крім того, сума всіх степенів елементів t_1, t_2 для всіх r_k рівна 0.

Доведемо, що вираз із глибиною зсуву $hzt_1(per) = 1$ не можна отримати, перемножуючи $r_3^{\pm 1}$, $r_2^{\pm 1}$. Аналогічно для інших k_i, у яких $|k_1 - k_2| = 1$,

$$r_2 r_3 = t_1^{-2} t_2 t_1^2 t_2 \; t_1^{-2} t_2^{-1} t_1^2 t_2^{-1} \; t_1^{-3} t_2 t_1^3 t_2 \; t_1^{-3} t_2^{-1} t_1^3 t_2^{-1}.$$

Прокомутувавши виділені доданки, можна скоротити елементи $t_2^{\pm 1}$ (які відповідають елементам $u_0^{\pm 1}$ і відсутні в (2)), а також прокомутувати $t_1^{-3} t_2 t_1^3 t_1^{-3} t_2^{-1} t_1^3 = t_1^{-3} t_2^{-1} t_1^3 t_1^{-3} t_2 t_1^3$ і отримати

$$t_1^{-2} t_2 t_1^2 [t_1^{-2} t_2^{-1} t_1^2 \; t_1^{-3} t_2 t_1^3] t_1^{-3} t_2^{-1} t_1^3 \neq r_2 r_3.$$

Однак отримати вираз вигляду (2), користуючись співвідношеннями з R, неможливо, бо перестановка між u_k^i і u_m^j, де $|k - m| = 1$, $|i, j| \le p - 1$, серед цих перетворень відсутня. Тому вираз, де поряд стоять u_2 і u_3, а далі u_2^{-1} і u_3^{-1}, отримати неможливо. Якщо ж почати скорочувати елементи t_1^i, $i \in \{\pm 2, \pm 3\}$, які стоять поряд, то отримаємо

$$t_1^{-2} t_2 t_1^2 t_1^{-2} t_2^{-1} t_1^2 \; t_1^{-3} t_2 t_1^3 t_1^{-2} t_2^{-1} t_1^3 =$$
$$= t_1^{-2} \; t_2 t_2^{-1} \; t_1^{-1} \; t_2 t_2^{-1} \; t_1^3 = t_1^{-3} t_1^3,$$

вираз без t_2. При частковому скороченні цих елементів отримаємо

$$t_1^{-2} t_2 t_1^2 t_1^{-2} t_2^{-1} t_1^2 \; t_1^{-3} t_2 t_1^3 t_1^{-3} t_2^{-1} t_1^3 =$$
$$= t_1^{-2} t_2 t_1 t_1^{-1} t_2^{-1} \; t_1^{-1} t_2 t_1 t_1^{-1} t_2^{-1} t_1^3,$$

де знову в правій частині не буде чергування $\delta_1(t_2^{i_m})$, як у r_1. Тому вираз вигляду (2) отримати неможливо. Значить, для його утворення необхідне відкинуте співвідношення з $hzt_1(per) = 1$.

Зрозуміло, що внаслідок множення r_k r_m: $|k - m| \neq 1$ вирази типу (1) не отримати неможна, тому що

$$t_1^{-2} t_2 t_1^2 t_1^{-2} t_2^{-1} t_1^2 \; t_1^{-5} t_2 t_1^5 t_1^{-5} t_2^{-1} t_1^5 =$$
$$= t_1^{-2} t_2 t_1^2 t_1^{-5} t_2 t_1^5 t_1^{-2} t_2^{-1} t_1^2 t_1^{-5} t_2^{-1} t_1^5 =$$
$$= t_1^{-2} \; \underbrace{t_2 t_1^{-3} t_2 t_1^3 \; t_2^{-1} t_1^{-3} t_2^{-1} t_1^3}_{r_3} \; t_1^2, \; hz(per) = 3.$$

Таким чином, отримали тільки $lz(t_1, k, t_2, v, w) \in \{-2, -5\}$, однак слова з $lz(t_1, k, t_2, v, w) = -1$ цими перетвореннями не виводяться.

Аналогічно для степенів $\forall i, j: |i - j| \neq 1$.

3. Далі, скориставшись методом математичної індукції, покладаємо, що для t_{n-1} не буде вивідності. Доведемо це для t_n. Візьмемо довільне

$$r_{m,n}^{k,1} = t_k^{-1} t_m t_k t_n \; t_k^{-1} t_m^{-1} t_k t_n^{-1} = 1, \; k > m > n, \qquad (5)$$

і покажемо, що це співвідношення не вивідне: у $N\left(\dfrac{\{t_i^p = e, r_{1,2}^{0,h}, r_{1,3}^{0,h}, .. r_{l,m}^{k,h}, \ldots, r_{n-1,n}^{n-2,h}\}}{r_{n,m}^{k,1}} \right)$ $1 \le h \le \dfrac{p-1}{2}$,

де $r_{m,n}^{k,1}$ — це співвідношення (5) з глибиною зсуву по твірному t_k: $hzt_k(per) = 1$. Як показано, раніше спряженням елементами t_k^{-i} співвідношення $r_{m,n}^{k,r} = t_k^{-r} t_n t_k^r t_m \; t_k^{-r} t_n^{-1} t_k^r t_m^{-1} = e$ з глибиною зсуву $hzt_k(per) = r$ змінити $hzt_k(per)$ не вдалося. Інші твірні не змінюють цієї глибини зсуву, оскільки не змінюють степінь спрягаючих елементів t_k. Всі міркування про елементарні перетворення, як це показано раніше, не змінюють величини $lz(t_k, k, t_n, v, w)$, тому (5) так не виводиться.

Разом з (5) з нормального замикання виключаємо всі слова вигляду $X^{-1} r_{m,n}^{k,1} X$ $X \in F$ як безпосередні наслідки з $r_{m,n}^{k,1}$. Тому неможна скористатись комутацією $X^{-1}r_{m,n}^{k,1}X$ з іншими $r_{t,n}^{l,x}$ без доведення. Аналогічно міркуємо для інших твірних N і елементів, що спряжені з ними. Слова вигляду

$$(t_k^{-1}Z^{-1}t_mZt_k)t_n(t_k^{-1}Z^{-1}t_m^{-1}Zt_k)t_n^{-1} = e, \qquad (6)$$

де всі елементи t_i, $i > k$, з Z впорядковані за зростанням, є безпосереднім наслідком зі співвідношення (4), що показано в теоремі 1, тому слова вигляду (5) не застосовуються без доведення їх вивідності. В добутку вигляду

$$Y^{-1}t_nY\ X^{-1}t_k^{-1}Z^{-1}t_mZt_kX \times$$
$$\times Y^{-1}t_n^{-1}YX^{-1}t_k^{-1}Z^{-1}t_m^{-1}Zt_kX \times$$
$$\times W^{-1}t_nW\ V^{-1}t_k^{-1}H^{-1}t_mHt_kH \times$$
$$\times W^{-1}t_n^{-1}WV^{-1}t_k^{-1}H^{-1}t_m^{-1}Ht_kV \qquad (7)$$

підслова X, V є послідовностями: $t_0^{i_0}t_1^{i_1}...t_{k-1}^{i_{k-1}}$, де $\exists\ i_s \neq 0$ і $X \neq V$. Тому t_m, t_n мають різні спрягаючі слова X, Y, W, H, які, зрозуміло, не скорочуються, а при спряженні добутку (6) різними словами, які описані в лемі 3, неможливо одночасно скоротити елементи з найменшими індексами зсуву, які є різними за побудовою. Тому підслово $r_{m,n}^{k,1}$ не виводиться. Тому з добутку

$$Y^{-1}t_nY\ t_k^{-1}X^{-1}t_mXt_k\ Y^{-1}t_n^{-1}Yt_k^{-1}X^{-1}t_m^{-1}Xt_k \times$$
$$\times W^{-1}t_nW\ t_k^{-1}H^{-1}t_mHt_k\ W^{-1}t_n^{-1}Wt_k^{-1}H^{-1}t_m^{-1}Ht_k$$

не виводиться (5). Якщо перемножувати слова $r_{m,n}^{k,i}$ і $r_{m,n}^{k,j}$, де $\min\{|j-i|,\ p-|j-i|\} = l$, а $r_{m,n}^{k,1}$ відсутня, то отримаємо $hz(per)$ $\|i-j|+l-1| = 1$ чи $p-\|i-j|+l-1| = 1$:

$$t_k^{-i}t_nt_k^it_k^{-j}t_mt_k^j\ t_k^{-i}t_n^{-1}t_k^it_k^{-j}t_m^{-1}t_k^j \times$$
$$\times t_k^{-i+l-1}t_nt_k^{i-l+1}t_k^{-j+l-1}t_mt_k^{j-l+1} \times$$
$$\times t_k^{-i+l-1}t_n^{-1}t_k^{i-l+1}t_k^{-j+l-1}t_m^{-1}t_k^{j-l+1},$$

де $[t_k^{-i}t_n^{-1}t_k^i, t_k^{-j-l+1}t_mt_k^{j+l-1}] \neq e$, оскільки $\|i-j| + l - 1| = 1$, наприклад,

$$t_k^{-2}t_nt_k^2t_k^{-4}t_mt_k^4t_k^{-2}t_n^{-1}t_k^2t_k^{-4}t_m^{-1}t_k^4 \times$$
$$\times t_k^{-1}t_nt_kt_k^{-3}t_mt_k^3t_k^{-1}t_n^{-1}t_kt_k^{-3}t_m^{-1}t_k^3,$$

підслово $t_k^{-3}t_mt_k^3$ можна переставити лише до підслова $t_k^{-4}t_m^{-1}t_k^4$, бо ці підслова не комутують, інакше було б використано співвідношення $r_{m,m}^{k,1} = e$, яке ми виключили.

Якщо перемножити $r_{m,n}^{k,i}$ і $r_{m,n}^{k,j}$, де $\min\{|j-i|,\ p-|j-i|\} = 1$, то отримаємо ситуацію, розглянуту на другому кроці. Розглядати $r_{m,r}^{k,i}$ $r_{m,l}^{k,j}$ $r \neq n$, де хоча б один ранг базового елемента з $r_{m,r}^{k,i}$ $r_{m,l}^{k,j}$ не з множини тих, що з (4), немає сенсу, бо серед них відсутні необхідні елементи, які не утворюються спряженням і елементарними перетвореннями.

Наслідок. Козображення силовської підгрупи P групи S_n:

$$P \simeq \left\langle \begin{array}{c} t_{lkz} \left| t_{lkz}^p = e,\ [t_{lkz}^{-i}t_{jkz}t_{lkz}^i, t_{bkz}] = e,\ t_{lkz}t_{jks} = t_{jks}t_{lkz}, \right. \\ 1 \le z, s \le \alpha_k,\ 0 \le l < j \le b < k,\ t_{lkz}t_{jvs} = t_{jvs}t_{lkz}, \\ 1 \le z \le \alpha_k,\ 1 \le s \le \alpha_v,\ 1 \le k, v \le m \end{array} \right\rangle,$$

де t_{ikz} — i-й твірний підгрупи P_z, спряженої з P_k; T_k — система твірних підгрупи P_k, $1 \le k \le m$, $P_k \cong \wr_{i=1}^{k} C_p$, $1 \le k \le m$.

Доведення. Це випливає з теореми 1 і структури силовської підгрупи симетричної групи. При цьому існує таке p-розбиття множини X на підмножини X_i, де діє P підстановками, так, що породжувальні елементи силовських підгруп P_l діють на X_i, не можуть бути редуковані при побудові прямого добутку $P = P_1^{a_1} \times P_2^{a_2} \times ... \times P_m^{a_m}$, оскільки вони не цикличні. Хоча якщо використати для спряження елементи $g \notin P$, $g \in S_n$, то породжувальні підгруп, спряжених до P_k, можна редукувати, тобто третій індекс можна не використовувати.

Нагадаємо, що сферична функція росту виражає залежність між кількістю слів і довжиною слова в цій системі твірних S, тобто це кількість слів, які записані в цій системі твірних S, цієї довжини l:

$$\delta_S(l) = \{g \in G \,|\, \|g\|_S = l\};$$

$$\delta_S(2) = |p|^{p+1},\quad \delta_S(3) = |p|^{p^2+p+1},$$

$$\delta_S(4) = |p|^{p^3+p^2+p+1},$$

$$\delta_S(l) = |p|^{p^{l-1}+p^{l-2}+\ldots+p^2+p+1},\ l \in \mathbb{N}.$$

Отже, маємо експоненційну сферичну функцію росту.

Висновки

Таким чином, досліджено козображення силовських підгруп групи підстановок – ним виявився вінцевий добуток циклічних груп C_p, доведено їх скінченнозаданість. Також вдалось довести мінімальність такого зображення для цієї системи твірних.

У статті побудовано сферичну функцію росту для силовських підгруп групи S_{p^k}. Знайдено коефіцієнти сферичного ряду росту, який є генератрисою для сферичної функції росту. Вивчено властивості ітерованого вінцевого добутку циклічних груп простого порядку.

Метою подальших досліджень є пошук козображення цих самих підгруп, які мають властивість мінімальності системи твірних серед усіляких систем твірних, а також мінімальної системи співвідношень для шуканої системи твірних. Також актуальним є дослідження діаметрів таких груп і таке зображення для вінцевого добутку знакозмінних груп.

1. *Дрозд Ю.А., Скуратовський Р.В.* Твірні та співвідношення для вінцевих добутків // Укр. матем. журн. – **60**, № 7. – 2008. – С. 997–999.
2. *Сущанський В.І., Сікора В.С.* Операції на групах підстановок. – Чернівці: Рута, 2003. – 256 с.
3. *A. Woryna,* “On Generation of Wreath Products of Cyclic Groups by Two State Time Varying Mealy Automata”, Int. J. Algebra Comput., vol. 16(2), pp. 397–415, 2006.
4. *Шмелькин Л.А.* Сплетения и многообразия групп // Изв. АН СССР. Сер. Матем. – 1965. – **29**, 1. – С. 149–170.
5. *Микаелян В.Г.* Вербальные вложения и сплетения групп: Автореф. дис. ... док. физ.-мат. наук. МГУ им. М. Ломоносова. – М., 2011. – С. 27.
6. *A.J. Weir,* “Sylow p-Subgroups of the Classical Groups Over Finite Fields”, Proc. of the American Math. Soc. Aug., vol. 6, no. 4, pp. 529–537, 1955.
7. *Yu. Bodnarchuk*, “On Generators of the Tame Invertible Polynomial Maps Group”, Int. J. Algebra Comput., vol. 15, no. 5, pp. 851–867, October 2005.
8. *Одрібець С.П.* Амальгамовані об’єднання graток і гратки нормальних дільників у вінцевих добутках: Автореф. дис. ... канд. фіз.-мат. наук: 01.01.06. – Київ. нац. ун-т ім. Т.Шевченка. – К., 2001. – 16 с.

Рекомендована Радою
фізико-математичного факультету
НТУУ “КПІ”

Надійшла до редакції
7 лютого 2013 року