О полных множествах силовских подгрупп счетной симметрической группы

И. Д. Иванюта

Симметрическая группа S (M)* счетного множества M не является S-полной [1]. В настоящей заметке найдены необходимые и достаточные условия, при которых полное множество силовских подгрупп группы S (M) ее порождает.

Определение 1. Множество подгрупп

$$P^{(p_1)},\ P^{(p_2)}, \ldots,\ P^{p_k}, \ldots \tag{1}$$

произвольной группы G называется полным силовским, если выполняются следующие условия:

1) $P^{(p_i)}$ — силовская p_i-подгруппа группы G, где p_i — простое число ($i = 1, 2, \ldots$);

2) $p_i \neq p_j$, $i \neq j$;

---

* $S(M)$ — группа всех таких взаимно однозначных отображений множества M на себя, каждое из которых действительно перемещает лишь конечное число символов.

3) каково бы ни было простое число p, входящее в порядки элементов группы G, множество (1) содержит некоторую силовскую p-подгруппу группы G.

Определение 2. Периодическая группа G называется S-полной, если она порождается любым ее полным множеством силовских подгрупп.

Теорема 1. *Полное множество*

$$P^{(p_1)},\ P^{(p_2)}, \ldots, P^{(p_k)}, \ldots (P)$$

силовских подгрупп группы S (M) *тогда и только тогда ее порождает, когда никакое непустое подмножество множества* M *не является областью транзитивности одновременно для всех подгрупп множества* (P).

Лемма 1. *Пусть* $\mathrm{A} = \langle \alpha_1, \alpha_2, \ldots, \alpha_k \rangle$, $\mathrm{B} = \langle \beta_1, \beta_2, \ldots, \beta_q \rangle$ — *конечные множества, пересечение которых непусто,* $k > 1$, $q > 1$, $b = (\beta_1, \beta_2, \ldots, \beta_q)$ — *циклическая подстановка. Тогда*

1) *если* $\mathrm{A} \subset \mathrm{B}$, q — *простое число, то* $S(\mathrm{A})$ *и* b *порождают* $S(\mathrm{B})$: $\{S(\mathrm{A}), b\} = S(\mathrm{B})$;

2) *если* $\mathrm{A} \not\subset \mathrm{B}$, *то при произвольном конечном* q $S(\mathrm{A})$ *и* b *порождают* $S(\mathrm{A} \cup \mathrm{B})$.

Доказательство. (1) Для некоторого m, $1 \leqslant m < q$, $b^m = (\alpha_1, \alpha_2, \beta_{i_3}, \ldots)$, где $\alpha_1, \alpha_2 \in \mathrm{A}$. Тогда подстановки $a = (\alpha_1, \alpha_2) \in S(\mathrm{A})$ и b^m, как известно, порождают $S(\mathrm{B})$.

(2) Предположим $\beta_1 \in \mathrm{A} \cap \mathrm{B}$, и пусть $a = (\alpha_{j_1}, \alpha_{i_2}, \ldots, \alpha_{j_l}, \beta_1) \in S(\mathrm{A})$, где $\alpha_{j_1}, \alpha_{j_2}, \ldots, \alpha_{j_l}$ — все элементы из A, не принадлежащие $\mathrm{A} \cap \mathrm{B}$. Тогда подстановки $c = ab$ и $d = (\beta_1, \alpha_{j_1}) \in S(\mathrm{A})$ порождают $S(\mathrm{A} \cup \mathrm{B})$.

Лемма 2. *Если силовская p-подгруппа* Q *группы* S (M) *переводит* α *в* β, $\alpha, \beta \in$ M, *то* Q *содержит цикл длины* p^n, *для некоторого* $n = 1, 2, \ldots$, *переводящий* α *в* β.

Доказательство. Из строения силовских p-подгрупп группы S (M) (см. [2]) следует, что если группа Q переводит α в β, то она содержит подгруппу P_n, подобную сплетению n циклических групп порядка p, которая также переводит α в β. Поэтому достаточно доказать лемму для P_n. Доказательство будем вести полной индукцией по n. Для группы P_1, порожденной циклом длины p, справедливость утверждения очевидна.

Группа P_n содержит нормальный делитель D, подобный прямому произведению p экземпляров группы P_{n-1}, т. е. $D = \prod\limits_{i=0}^{p-1} P_{n-1}^{(i)}$. Обозначим через Γ_i множество элементов, которые перемещает подгруппа $P_{n-1}^{(i)}$, $i = 0, 1, \ldots, p-1$.

Предположим $\alpha \in \Gamma_i$, $\beta \in \Gamma_j$. Группа P_n содержит цикл a длины p^n, перемещающий все символы множества $\Gamma = \bigcup\limits_{i=0}^{p-1} \Gamma_i$: $a = (\gamma_1^{(1)}, \gamma_2^{(1)}, \ldots, \gamma_p^{(1)}, \gamma_1^{(2)}, \gamma_2^{(2)}, \ldots)$, где $\gamma_i^{(s)} \in \Gamma_i$. Тогда для некоторого k, $1 \leqslant k < p$, $a^k = (\alpha, \gamma_j^{(l)}, \ldots)$. По предположению индукции $P_{n-1}^{(i)}$ содержит цикл $b = (\gamma_i^{(l)}, \beta_1, \ldots)$, а тогда $b^{-1}ab = (\alpha, \beta, \ldots)$ цикл длины p^n, переводящий α в β.

Лемма 3. *Пусть силовская p-подгруппа* Q *группы* S (M) *содержит цикл* $a = (\alpha_1, \alpha_2, \ldots, \alpha_{p^n})$,

$$a^p = (\alpha_1, \alpha_{p+1}, \alpha_{2p+1}, \ldots)(\alpha_2, \alpha_{p+2}, \ldots) \ldots (\alpha_p, \alpha_{2p}, \ldots, \alpha_{p^n}).$$

Тогда Q *содержит элементы* $a_i = (\alpha_i, \alpha_{p+i}, \ldots)$, $i = 1, 2, \ldots, p$.

Доказательство. Элемент a принадлежит некоторой подгруппе группы Q, подобной P_n [2]. Тогда $a^p \in D = \prod_{i=0}^{p-1} P_{n-1}^{(i)}$, a_i — проекция a^p на $P_{n-1}^{(i-1)}$.

Очевидно $a_i \in P_{n-1}^{(i-1)} \subset Q$.

Доказательство теоремы 1. Необходимость очевидна. Достаточность. Пусть α_1 — произвольный элемент множества M. В силу условий теоремы, существует группа $P^{(p_i)}$ множества (P), которая не оставляет α_1 на месте. Из леммы 3 следует, что $P^{(p_i)}$ содержит цикл $a = (\alpha_1, \alpha_2, \ldots, \alpha_{p_i})$; пусть $\Lambda_1 = \langle \alpha_1, \alpha_2, \ldots, \alpha_{p_i} \rangle$. Рассмотрим два случая:

1) $p_i > 2$. Как следует из [2], группа $P^{(2)}$ множества (P) может оставлять на месте не более одного символа множества M. Следовательно, $P^{(2)}$ содержит цикл $b = (\beta_1, \beta_2)$, перемещающий по крайней мере один символ множества Λ_1; пусть $\Lambda_2 = \langle \beta_1, \beta_2 \rangle$. Тогда в силу леммы 1 $\{a, b\} = S(\Lambda_1 \cup \Lambda_2)$.

2) $p_i = 2$, $a = (\alpha_1, \alpha_2)$.

а) Пусть некоторая группа $P^{(p_j)}$ из (P), $p_j \neq 2$, перемещает α_1 или α_2. Тогда $P^{(p_j)}$ содержит цикл $b = (\beta_1, \beta_2, \ldots, \beta_{p_j})$, перемещающий α_1 или α_2, и $\{a, b\} = S(\Lambda_1 \cup \Lambda_2)$, где $\Lambda_1 = \langle \alpha_1, \alpha_2 \rangle$, $\Lambda_2 = \langle \beta_1, \beta_2, \ldots, \beta_{p_j} \rangle$.

б) Пусть все группы $P^{(p_j)}$, $p_j \neq 2$, из (P) оставляют α_1 и α_2 на месте. Тогда $P^{(2)}$ содержит цикл $c = (\alpha_1, \gamma_1, \alpha_2, \gamma_2)$ перемещающий α_1 и α_2, так как в противном случае множество $\langle \alpha_1, \alpha_2 \rangle$ было бы областью транзитивности всех групп множества (P). В силу леммы 3 $P^{(2)}$ содержит цикл $d = (\gamma_1, \gamma_2)$; пусть $\Lambda_3 = \langle \gamma_1, \gamma_2 \rangle$. Группа $P^{(3)}$ из (P) может оставлять на месте не более двух элементов. Следовательно, она содержит цикл $b = (\beta_1, \beta_2, \beta_3)$, который перемещает по крайней мере один символ множества $\Lambda_4 = \langle \alpha_1, \alpha_2, \gamma_1, \gamma_2 \rangle$; пусть $\Lambda_2 = (\beta_1, \beta_2, \beta_3\rangle$. Тогда по лемме 1 $\{b, d\} = S(\Lambda_2 \cup \Lambda_3)$ и $\{b, d, c\} = S(\Lambda_2 \cup \Lambda_4)$.

Пусть уже имеем $S(\Gamma_1)$ для некоторого конечного множества $\Gamma_1 = \langle \alpha_1, \alpha_2, \ldots, \alpha_m \rangle$, содержащего α_1. Возможны следующие случаи.

1) Множество (P) содержит группу $P^{(p_\mu)}$, элемент $b = (\beta_1, \beta_2, \ldots, \beta_{p_\mu^n})$ которой перемещает часть символов множества Γ_1, и некоторые символы множества M, не принадлежащие Γ_1. Тогда по лемме 1 $\{S(\Gamma_1), b\} = S(\Gamma_1 \cup \Gamma_2)$, где $\Gamma_2 = \langle \beta_1, \beta_2, \ldots, \beta_{p_\mu^n} \rangle$.

2) Множество (P) содержит группу $P^{(p_\nu)}$, элемент $b = (\beta_1, \beta_2, \ldots, \beta_{p_\nu^k})$ которой перемещает все символы множества Γ_1, и некоторые символы, не лежащие в Γ_1, т. е. $m < p_\nu^k$.

Если $k = 1$, то по лемме 1 $\{S(\Gamma_1), b\} = S(\Gamma_1 \cup \Gamma_2)$, где $\Gamma_2 = \langle \beta_1, \beta_2, \ldots, \beta_{p_\nu^k} \rangle$.

Пусть $k > 1$. Очевидно, $b^{p_\nu} = (\beta_1, \beta_{p_\nu+1}, \ldots)(\beta_2, \beta_{p_\nu+2}, \ldots) \ldots (\beta_{p_\nu}, \beta_{2p_\nu}, \ldots, \beta_{p_\nu^k})$ и по лемме 3 группа $P^{(p_\nu)}$ содержит элементы $b_{i-1} = (\beta_i, \beta_{p_\nu+i}, \ldots)$, $i = 1, 2, \ldots, p_\nu$; пусть $\mathrm{B}_{i-1} = \langle \beta_i, \beta_{p_\nu+i}, \ldots \rangle$, $\mathrm{B} = \langle \beta_1, \beta_2, \ldots, \beta_{p_\nu^k} \rangle$.

Может быть, что один из элементов b_i тоже перемещает все символы множества Γ_1 и $m < p_\nu^{k-1}$. Тогда вместо элемента b можно рассматривать b_i. Выберем k так, чтобы $p_\nu^{k-1} \leqslant m < p_\nu^k$.

Рассмотрим возможные случаи.

a) $m \neq ep_\nu^{k-1}$. Тогда один из элементов b_i перемещает некоторые символы из Γ_1 и некоторые символы из M, не лежащие в Γ_1, и по лемме 1 $\{S(\Gamma_1), b_i\} = S(\Gamma_1 \cup B_i)$.

b) $m = ep_\nu^{k-1}$ и один из элементов b_i перемещает некоторые символы из Γ_1 и символы, не лежащие в Γ_1. Тогда $\{S(\Gamma_1), b_i\} = S(\Gamma_1 \cup B_i)$.

c) $m = ep_\nu^{k-1}$ и подстановки $b_{s_1}, \ldots, b_{s_r}$ перемещают только символы из Γ_1, а подстановки $b_{s_{r+1}}, \ldots, b_{s_{p_\nu}}$ — только символы, не принадлежащие Γ_1.

Пусть $r > 1$. Тогда для некоторого h, $1 \leqslant h < p_\nu$, $b^h = (\beta_{s_1}, \beta_{s_2}, \ldots)$, где $\beta_{s_1} \in B_{s_1}, \beta_{s_2} \in B_{s_2}$, и подстановки b^h и $d = (\beta_{s_1}, \beta_{s_2}) \in S(\Gamma_1)$ порождают $S(\Gamma_1 \cup B) = S(B)$.

Пусть $r = 1$, т. е. $\Gamma = B_{s_1}$. Очевидно, $b^{-j} S(B_i) b^j = S(B_{(i+j) \bmod p_\nu})$, $j = 1, 2, \ldots, p_\nu$, и $S(B_{s_1})$ и b порождают группу, подобную сплетению $S(B_{s_1}) wr C$ (C — циклическая группа порядка p_ν), с основанием $D = \prod_{i=0}^{p_\nu - 1} S(B_i)$.

Между p_ν^{k-1} и p_ν^k существует по крайней мере одно простое число t. Группа $P^{(t)}$ из (P) содержит элемент $g = (\gamma_1, \gamma_2, \ldots, \gamma_t)$, который перемещает хотя бы один символ множества B, поскольку $t < p_\nu^k$; пусть $\Delta = \langle \gamma_1, \gamma_2, \ldots, \gamma_t \rangle$.

Предположим $\Delta \not\subset B$ и $\Delta \cap B_i \neq \varnothing$. Тогда по лемме 1 $\{S(B_i), g\} = S(\Delta \cup B_i)$, $\{S(\Delta \cup B_i), b\} = S(\Delta \cup B)$.

Пусть $\Delta \subset B$. Поскольку $p_\nu^{k-1} < t$, то $\Delta \cap B_i \neq \varnothing$ и $\Delta \cap B_j \neq \varnothing$, $i \neq j$, и $S(B_i)$, $S(B_j)$, g порождают группу $S(\Delta \cup B_i \cup B_j)$, которая вместе с элементом b порождает $S(B)$.

Итак, для произвольного элемента $\alpha \in M$ можно построить бесконечную возрастающую последовательность конечных симметрических групп $S(\Gamma_1) \subset S(\Gamma_2) \subset \ldots$, которые перемещают α. Пусть $S^\alpha(\Gamma) = \bigcup_{i=1}^{\infty} S(\Gamma_i)$, G — группа, порожденная группами множества (P). Предположим $G \neq S(M)$. Если $S^\alpha(\Gamma)$ и $S^\beta(\Lambda)$ такие, что $\Gamma \cap \Lambda \neq \varnothing$, то $S^\alpha(\Gamma)$, $S^\beta(\Lambda)$ порождают, очевидно, $S(\Gamma \cup \Lambda)$. Поэтому $G \neq S(M)$ только тогда, когда для некоторых α и β $S^\alpha(\Gamma)$ и $S^\beta(\Lambda)$ такие, что $\Gamma \cap \Lambda = \varnothing$. Но тогда множества Γ и Λ являются областями транзитивности групп множества (P), что противоречит условию теоремы.

Теорема доказана.

ЛИТЕРАТУРА

1. П. А. Гольберг, S-радикал и силовские базы бесконечных групп, Матем. сб., т. 50 (92), № 1, 1960, 25—42.
2. И. Д. Иванюта, Силовские p-подгруппы счетной симметрической группы, УМЖ, т. XV, № 3, 1963, 240—248.

Поступила 16.XI 1965 г.
Киев