Math-Net.Ru

Общероссийский математический портал

А. Ю. Максимовский, О групповых свойствах подстановок, определенных на смежных классах конечной абелевой группы составного порядка по ее подгруппам, *Матем. вопр. криптогр.*, 2016, том 7, выпуск 1, 83–92

DOI: <https://doi.org/10.4213/mvk176>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением

<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.80.73.141

26 апреля 2023 г., 13:24:42

**О групповых свойствах подстановок,
определенных на смежных классах конечной
абелевой группы составного порядка по ее подгруппам**

А. Ю. Максимовский

ООО «Центр сертификационных исследований», Москва

Получено 20.IV.2015

Найдены необходимые и достаточные условия транзитивности и примитивности групп подстановок, образующими элементами которых являются подстановки на смежных классах абелевой группы G . Описано строение этих групп в случаях, когда они примитивны или когда абелева группа G является прямым произведением своих подгрупп. Получены также необходимые и достаточные условия примитивности группы, порожденной правым регулярным представлением группы G и одной из подстановок, определенных на смежных классах группы G .

Работа выполнена при финансовой поддержке Академии криптографии Российской Федерации.

Ключевые слова: абелевы группы, группы подстановок, условия транзитивности, условия примитивности, смежные классы

**On the group properties of substitutions defined on the subgroup
cosets of finite Abelian group of composite order**

A. Yu. Maksimovskiy

Sertification Research Center LLC, Moscow

Abstract. Necessary and sufficient conditions of transitivity and primitivity of substitution groups generated by substitutions on the cosets of the Abelian group G are obtained. The structure of these groups is described for the case of their primitivity and for the case when G is the direct product of its subgroups. Necessary and sufficient conditions of primitivity of the group generated by the right regular representation of the group G and a substitution defined on the cosets of the group G are obtained as well.

Keywords: Abelian groups, substitution groups, transitivity conditions, primitivity conditions, cosets.

Citation: *Mathematical Aspects of Cryptography*, 2016, v. 7, № 1, pp. 83–92 (Russian)

© Академия криптографии Российской Федерации, 2016 г.

Рассмотрим конечную абелеву группу G составного порядка nm , $n < 1$, $m < 1$, с операцией $+$, с нейтральным элементом 0 , которая имеет подгруппы M и N порядков m и n соответственно. Зафиксируем множества $g = \{g(1), g(2), \dots, g(n)\}$ представителей смежных классов группы G по подгруппе M и $t = \{t(1), t(2), \dots, t(m)\}$ представителей смежных классов группы G по подгруппе N . Пусть π — биективное отображение множества g на группу N , $\varphi = (\varphi_1, \varphi_2, \dots, \varphi_n)$ есть фиксированный набор биективных отображений множества M на множество t . Если элемент h группы G лежит в правом смежном классе $M_{g(s)}$ по подгруппе M с представителем $g(s)$, $s \in \{1, 2, \dots, n\}$, то будем использовать представление этого элемента в виде $h = h_M + g(s)$, $h_M \in M$. Определим на группе G отображение $\rho(\pi, \varphi)$, действующее на элемент h из правого смежного класса $M_{g(s)}$ следующим образом:

$$h\rho(\pi, \varphi) = (h_M + g(s))\rho(\pi, \varphi) = (g(s))^\pi + (h_M)\varphi_s. \quad (1)$$

Биективность отображения $\rho(\pi, \varphi)$ очевидна, потому оно является подстановкой группы G . Изучение таких отображений представляет интерес в связи с тем, что их конструкция (1) обобщает понятие регистра сдвига. Действительно, если группа G является k -мерным модулем над некоторым кольцом R с нейтральным по сложению элементом θ , подгруппы M и N таковы, что $M = \{(a, \theta, \dots, \theta), a \in R\}$, $N = \{(a_1, a_2, \dots, a_{k-1}, \theta), a_1, a_2, \dots, a_{k-1} \in R\}$, а отображение π определено по правилу

$$\pi((\theta, c_1, \dots, c_{k-1})) = (c_1, c_2, \dots, c_{k-1}, \theta), \quad c_1, c_2, \dots, c_{k-1} \in R,$$

то подстановка $\rho(\pi, \varphi)$ описывает функционирование регулярного регистра сдвига длины k над кольцом R с функцией обратной связи φ , если положить $\varphi = \varphi(c_1, c_2, \dots, c_k) = \varphi_{c'}(c_1)$, где $c' = (c_2, \dots, c_k)$, $\varphi_{c'}: R \rightarrow R$ есть частичная функция, являющаяся подстановкой кольца R . При этом отображение π «реализует» сдвиг, а регулярность регистра обеспечивается за счет биективности функции обратной связи φ по первому аргументу.

Пусть $\Pi_{M,N}\{g\}$ — множество всех биективных отображений на группу N фиксированного набора $g = \{g(1), g(2), \dots, g(n)\}$ представителей смежных классов группы G по подгруппе M . Очевидно, что $|\Pi_{M,N}\{g\}| = n!$. Пусть $\Phi_{N,M}\{t\}$ — множество всех наборов $\varphi = (\varphi_1, \varphi_2, \dots, \varphi_n)$ биективных отображений $\varphi_s: M \rightarrow t$, $s = 1, 2, \dots, n$, в фиксированный набор $t = \{t(1), t(2), \dots, t(m)\}$ представителей смежных классов группы G по подгруппе N . Очевидно, что $|\Phi_{N,M}\{t\}| = (m!)^n$.

Изучение групповых свойств подстановок вида (1) начнем с группы

$$P_{g,t}(\pi) = \langle \rho(\pi, \varphi), \varphi \in \Phi_{N,M}\{t\} \rangle, \quad \pi \in \Pi_{M,N}\{g\}.$$

Примем обозначение $P(\pi) = P_{g,t}(\pi)$ для фиксированных наборов g и t . Очевидно, $P(\pi)$ является подгруппой группы

$$P = P_{g,t} = \langle \rho(\pi, \varphi), \pi \in \Pi_{M,N}\{g\}, \varphi \in \Phi_{N,M}\{t\} \rangle.$$

Для симметрической группы, действующей на множестве L , будем использовать обозначение $S(L)$.

Утверждение 1. *Группа $P(\pi)$ содержит подгруппы T и Q , являющиеся прямыми произведениями n симметрических групп подстановок степени t . При этом*

$$T = S(\{l_1+t(1), \dots, l_1+t(m)\}) \times \dots \times S(\{l_n+t(1), \dots, l_n+t(m)\}),$$

где $l_s = (g(s))^\pi$, $s \in \{1, 2, \dots, n\}$,

$$Q = S(M+g(1)) \times \dots \times S(M+g(n)),$$

где $M+g(s)$ есть смежный класс по подгруппе M с представителем $g(s)$, $s \in \{1, 2, \dots, n\}$.

Доказательство. Рассмотрим действие произведения $\rho(\pi, \varphi)\rho^{-1}(\pi, \phi)$ для некоторых $\varphi, \phi \in \Phi_{N,M}\{t\}$. Получим цепочку равенств

$$\begin{aligned} ((h_M + g(s))) \rho(\pi, \varphi) \rho^{-1}(\pi, \phi) &= ((g(s))^\pi + (h_M) \varphi_s) \rho^{-1}(\pi, \phi) = \\ &= (h_M) \varphi_s (\phi_s)^{-1} + g(s). \end{aligned}$$

В силу произвольности выбора φ и ϕ отображение $\varphi_s (\phi_s)^{-1}$ является произвольной подстановкой множества $M+g(s)$ для каждого $s \in \{1, 2, \dots, n\}$. Поэтому группа $P(\pi)$ содержит в себе подгруппу $Q = S(M+g(1)) \times \dots \times S(M+g(n))$. Рассматривая аналогичным образом действие произведения подстановок $\rho^{-1}(\pi, \varphi)\rho(\pi, \phi)$ для некоторых $\varphi, \phi \in \Phi_{N,M}\{t\}$, получаем, что $P(\pi)$ содержит в себе подгруппу $T = S(\{m_1+t(1), \dots, m_1+t(m)\}) \times \dots \times S(\{m_n+t(1), \dots, m_n+t(m)\})$. Утверждение доказано. $\square$

Пусть w_q — орбита группы $P(\pi)$, содержащая элемент q группы G .

Утверждение 2. *Группа $P(\pi)$ транзитивна тогда и только тогда, когда группа N содержится в орбите w_0 .*

Доказательство. Необходимость очевидна. Докажем достаточность. Поскольку орбита w_0 содержит в себе группу N , имеет место включение $w_0 \supseteq \{m_1, m_2, \dots, m_n\}$. В то же время по утверждению 1 группа $P(\pi)$ содержит в себе подгруппу T , поэтому $w_0 \supseteq \{m_1+t(1), \dots, m_1+t(m)\} \cup \dots \cup \{m_n+t(1), \dots, m_n+t(m)\} = G$ и группа $P(\pi)$ транзитивна.

Утверждение доказано. $\square$

Следствие 1. Пусть $t = M$ (т.е. G — прямая сумма групп M и N) и отображение π переводит элемент $g(1) \in M$ в нуль группы N . Тогда группа $P(\pi)$ интранзитивна.

Следствие 2. Если группа M содержит группу N , то группа $P(\pi)$ транзитивна.

Рассмотрим случай, когда G — прямая сумма своих подгрупп M и N . В этом случае элемент h группы G можно записать в виде $h = (h_M, h_N)$.

Утверждение 3. Если G — прямая сумма групп M и N , то группа P является сплетением симметрической группы $S(M)$ и симметрической группы $S(N)$, группа $P(\pi)$ является сплетением симметрической группы $S(M)$ и группы $\langle \pi' \rangle$, порожденной подстановкой π' , действие которой на группе N индуцировано отображением π .

Это утверждение вытекает из определения сплетения групп подстановок (см. [1]).

Следствие 3. Если G — прямая сумма групп M и N , то группа P совпадает с множеством подстановок $\{\rho(\pi, \varphi), \pi \in \Pi_{M,N}\{g\}, \varphi \in \Phi_{N,M}\{t\}\}$.

Следствие 4. Если G — прямая сумма групп M и N , то группа P транзитивна и импримитивна, а если, кроме того, группа $\langle \pi' \rangle$ транзитивна, то группа $P(\pi)$ транзитивна и импримитивна.

Замечание 1. Результаты утверждения 3 и следствий из него не зависят от выбора наборов представителей g и t смежных классов группы G по подгруппам M и N .

Всюду далее будем считать, что G не является прямой суммой своих подгрупп M и N .

Утверждение 4. Если группа $P(\pi)$ примитивна, то она совпадает с симметрической группой $S(G)$.

Доказательство. Группа $P(\pi)$, очевидно, содержит в себе транспозицию. Поэтому $P(\pi) = S(G)$ по теореме 5.6.2 из [1]. Утверждение доказано. $\square$

Приведем ряд свойств импримитивной группы $P(\pi)$.

Утверждение 5. Любой нетривиальный блок импримитивности группы $P(\pi)$ является объединением смежных классов по подгруппе M .

Следствие 5. Мощность любого нетривиального блока импримитивности группы $P(\pi)$ делится на m .

Утверждение 6. Если группа M содержит в себе группу N , то $P(\pi) = S(G)$.

Доказательство. Действительно, по следствию 2 группа $P(\pi)$ транзитивна. По условию и утверждению 5 блок импримитивности Δ , содержащий смежный класс M , содержит в себе группу N . Тогда, рассматривая действие подгруппы T на блок импримитивности Δ с учетом утверждения 2, несложно убедиться, что

$$\Delta \supseteq \{l_1+t(1), \dots, l_1+t(m)\} \cup \dots \cup \{l_n+t(1), \dots, l_n+t(m)\} = G.$$

Поэтому группа $P(\pi)$ примитивна. Осталось воспользоваться утверждением 4. $\square$

Условие в утверждении 6 можно ослабить.

Утверждение 7. Если смежный класс $M+g(s)$ группы G по подгруппе M для некоторого $s \in \{1, 2, \dots, n\}$ содержит в себе более половины элементов группы N и группа $P(\pi)$ транзитивна, то $P(\pi) = S(G)$.

Следствие 6. Если для некоторого $j \in \{1, 2, \dots, n\}$ в множестве

$$\{n_j+t(1), n_j+t(2), \dots, n_j+t(m)\}, \quad n_j \in N,$$

содержится не менее $\lfloor \frac{m}{2} \rfloor + 1$ представителей различных смежных классов группы G по подгруппе M и группа $P(\pi)$ транзитивна, то $P(\pi) = S(G)$. Здесь $\lfloor x \rfloor$ — целая часть числа x .

Утверждение 7 и следствие 6 намечают путь, по которому следует двигаться при решении вопроса о примитивности группы $P(\pi)$. Пусть $[M](\rho(\pi, \varphi))^0 = M$ и $[M](\rho(\pi, \varphi))^k$ — объединение всех смежных классов группы G по подгруппе M , которые содержат в себе образы элементов из $[M](\rho(\pi, \varphi))^{k-1}$, $k < 0$, при действии подстановки $\rho(\pi, \varphi)$.

Утверждение 8. 1. Если $|[M](\rho(\pi, \varphi))^k| = nm$ для некоторого k , то $P(\pi) = S(G)$.

2. Если для некоторых целых $k \geq 0$ и $s < 0$

$$[M](\rho(\pi, \varphi))^k = [M](\rho(\pi, \varphi))^{k+s}, \quad \text{причем} \quad |[M](\rho(\pi, \varphi))^k| \leq \frac{nm}{2},$$

то группа $P(\pi)$ интранзитивна или импримитивна.

Опираясь на утверждение 7, можно предложить алгоритм, который позволяет определить, является ли группа $P(\pi)$ примитивной, и при положительном ответе установить совпадение группы $P(\pi)$ с $S(G)$. Этот алгоритм заключается в последовательном построении и проверке свойств множеств $[M](\rho(\pi, \varphi))^k$ для $k < 0$.

Для множества $[M](\rho(\pi, \varphi))^k$, построенного на k -м шаге алгоритма:

$k.1)$ проверяется равенство $|[M](\rho(\pi, \varphi))^k| = nm$. Если оно выполнено, то алгоритм останавливается, и $P(\pi) = S(G)$.

Если оно не выполнено, то:

$k.2)$ проверяется равенство $[M](\rho(\pi, \varphi))^k = [M](\rho(\pi, \varphi))^{k-s}$ для некоторого $s < 0$. Если оно не выполнено, то алгоритм продолжает свою работу, т. е. строится множество $[M](\rho(\pi, \varphi))^{k+1}$. Если выполнено, то алгоритм останавливается, и:

$k.2.1)$ проверяется равенство $s = 1$. Если $s = 1$, то группа $P(\pi)$ интранзитивна и $[M](\rho(\pi, \varphi))^{k-1}$ — ее орбита. Если $s \neq 1$, то

$k.2.2)$ проверяется условие $s|[M](\rho(\pi, \varphi))^k| < nm$. Если оно выполнено, то группа $P(\pi)$ интранзитивна, и ее орбитой служит множество $[M](\rho(\pi, \varphi))^{k-s} \cup \dots \cup [M](\rho(\pi, \varphi))^{k-1}$. Если это условие не выполнено, то группа $P(\pi)$ импримитивна и $[M](\rho(\pi, \varphi))^{k-s}, \dots, [M](\rho(\pi, \varphi))^{k-1}$ — система ее блоков импримитивности.

Число шагов данного алгоритма не превышает $2n$, где n — индекс подгруппы M в группе G .

Замечание 2. При доказательстве утверждений 1–7 коммутативность операции в группе G не использовалась. Следовательно, перечисленные утверждения и следствия из них справедливы для определенного аналогично правилу (1) множества подстановок над произвольной конечной группой G , которая имеет такие подгруппы M и N , что $|G| = |M| \cdot |N|$. Однако в случае неабелевой группы нельзя гарантировать существование таких подгрупп для всего спектра делителей порядка группы G . Это обстоятельство сужает выбор параметров рассматриваемого класса подстановок над конечной группой. Ввиду этого в данной статье мы ограничились рассмотрением случая конечных абелевых групп.

В криптографических приложениях совместно с подстановками вида (1) часто используются подстановки из правого регулярного представления G^* группы G . В связи с этим рассмотрим свойства группы, порожденной группой G^* и подстановкой $\rho(\pi, \varphi)$ при фиксированных отображении π и наборе отображений φ , которую обозначим $GR(\pi, \varphi)$.

Введем обозначения:

$f \equiv h(D)$ — такие подгруппа D и элементы f и h группы G , для которых $(f-h) \in D$;

μ_a — подстановка сдвига группы G на элемент $a \in G$;

$F \# H$ — прямая сумма абелевых групп F и H .

Утверждение 9. *Группа $GR(\pi, \varphi)$ импримитивна тогда и только тогда, когда для некоторой подгруппы D группы G отображения $\pi, \varphi_1, \varphi_2, \dots, \varphi_n$, элементы $g(1), g(2), \dots, g(n)$ и $t(1), t(2), \dots, t(m)$ удовлетворяют следующим условиям:*

1) *если $M \cap D = \{0\}$, $N \cap D = \{0\}$, $|D| = d$, то:*

1.1) *d делит m , и n ,*

1.2) *множество представителей t распадается на $m' = m/d$ подмножеств $T_1, T_2, \dots, T_{m'}$ по d элементов, принадлежащих одному смежному классу группы G по подгруппе $N \# D$,*

1.3) *отображение $(\varphi_s)^{-1} \mu_{a(r)-a(s)} \varphi_r$ переводит каждое из подмножеств $T_1, T_2, \dots, T_{m'}$ в себя, где $s, r, a(s), a(r)$ определяются равенствами*

$$g(s) = a(s) + f(s) + w, \quad g(r) = a(r) + f(r) + w,$$

$a(s), a(r) \in M$, $f(s), f(r) \in D$, w — некоторый элемент группы G , при этом разности вида $(a(r) - a(s) + h) \varphi_r - h \varphi_s$, $h \in M$, лежат в одном смежном классе группы G по подгруппе D с представителем $(g(s))^\pi - (g(r))^\pi$,

1.4) *множество представителей g распадается на $n' = \frac{n}{d}$ подмножеств по d элементов, принадлежащих одному смежному классу группы G по подгруппе $M \# D$;*

2) *если $M \cap D = \{0\}$, $N \cap D \neq \{0\}$, то для всех таких s и j , что $(g(s))^\pi \equiv (g(j))^\pi \pmod{D}$, и любого $i \in \{1, 2, \dots, m\}$*

$$(t(i)(\varphi_s)^{-1} - t(i)(\varphi_j)^{-1}) \equiv (g(j) - g(s)) \pmod{D};$$

3) *если $M \cap D = L \neq \{0\}$, $|L| = m/q$, то:*

3.1) *при $q=1$ группа G есть прямая сумма: $G = M \# N$,*

3.2) *при $q < 1$:*

3.2.1) *множество t разбивается на q подмножеств $U_1, U_2, \dots, U_q$, состоящих из элементов, сравнимых по подгруппе D ,*

3.2.2) *для любого $s \in \{1, 2, \dots, n\}$ отображение φ_s переводит класс элементов, сравнимых по подгруппе L , в некоторое подмножество U_j , множество представителей $g(1), g(2), \dots, g(n)$ распадается на $n'' = n/k$ подмножеств $V_1, V_2, \dots, V_{n''}$ мощности $k = |N \cap L|$, в каждом из которых содержатся элементы, принадлежащие одному и тому же смежному классу группы G по подгруппе D ,*

3.2.3) *каждое множество V_l , $l \in \{1, 2, \dots, n''\}$, подстановка π переводит в смежный класс группы N по подгруппе $N \cap D$.*

Доказательство. Поскольку $G^* \subset GR(\pi, \varphi)$, блоками импримитивности группы $GR(\pi, \varphi)$ могут быть только смежные классы группы G по некоторой ее подгруппе D .

Пусть группа $GR(\pi, \varphi)$ импримитивна, D — подгруппа G , обладающая следующим свойством: для любых таких $a, b \in G$, что $a \equiv b \pmod{D}$, имеет место сравнение $a\rho(\pi, \varphi) \equiv b\rho(\pi, \varphi) \pmod{D}$.

Обозначим через ν индекс $[G : D]$ подгруппы D в группе G .

1) Пусть $M \cap D = \{0\}$ и $N \cap D = \{0\}$. Тогда так как группа G абелева, то, с одной стороны, подгруппа D изоморфна подгруппе фактор-группы G/M , а с другой стороны, подгруппа D изоморфна подгруппе фактор-группы G/N . Поэтому число $d = |D|$ делит и m , и n .

Очевидно, $G < M \# D$, $G < N \# D$. Следовательно, среди представителей $g(1), g(2), \dots, g(n)$ группы G по подгруппе M имеются такие элементы $g(i_2), \dots, g(i_d)$, $\min\{i_2, \dots, i_d\} < 1$, что

$$M \# D = M \cup (M + g(i_2)) \cup \dots \cup (M + g(i_d)).$$

Аналогично, среди представителей $t(1), t(2), \dots, t(m)$ группы G по подгруппе N имеются такие элементы $t(j_2), \dots, t(j_d)$, $\min\{j_2, \dots, j_d\} < 1$, что

$$N \# D = N \cup (N + t(j_2)) \cup \dots \cup (N + t(j_d)).$$

Любой из элементов $g(i_2), \dots, g(i_d)$ может быть однозначно представлен в виде

$$g(i_k) = a(i_k) + f(i_k), \quad a(i_k) \in M, \quad f(i_k) \in D, \quad k = 2, \dots, d.$$

Тогда для любых $h \in M$ и $k \in \{2, \dots, d\}$ справедливы сравнения

$$g(i_k) + h \equiv a(i_k) + h \pmod{D},$$

$$(g(i_k) + h)\rho(\pi, \varphi) \equiv (a(i_k) + h)\rho(\pi, \varphi) \pmod{D}.$$

Так как $a(i_k) + h \in M$,

$$(g(i_k))^\pi + h\varphi_{i_k} \equiv (g(1))^\pi + (a(i_k) + h)\varphi_1 \pmod{D},$$

то справедливо сравнение

$$(g(i_k))^\pi - (g(1))^\pi \equiv (a(i_k) + h)\varphi_1 - h\varphi_{i_k} \pmod{D}.$$

Заметим, что $(g(i_k))^\pi - (g(1))^\pi \notin D$. Поэтому при фиксированном $k \in \{2, \dots, d\}$ разности представителей смежных классов группы G по подгруппе N вида

$(a(i_k) + h)\varphi_1 - h\varphi_{i_k}$, $h \in M$, лежат в одном смежном классе группы G по подгруппе D с представителем $(g(i_k))^\pi - (g(1))^\pi \in N$.

Множество представителей t распадается на m' подмножеств $T_1, T_2, \dots, T_{m'}$ по d элементов, принадлежащих одному смежному классу группы G по подгруппе $N \# D$, причем представители вида $(a(i_k) + h)\varphi_1$ и $h\varphi_{i_k}$ лежат в одном смежном классе группы G по подгруппе $N \# D$. При этом отображение $(\varphi_{i_k})^{-1} \mu_{a(i_k)} \varphi_1$ переводит каждое из подмножеств $T_1, T_2, \dots, T_{m'}$ в себя.

Пусть $(g(s) - g(r)) \in M \# D$. Тогда $g(s)$ и $g(r)$ могут быть представлены в виде

$$g(s) = a(s) + f(s) + w, \quad g(r) = a(r) + f(r) + w,$$

где $a(s), a(r) \in M, f(s), f(r) \in D$, w — некоторый элемент группы G . Тогда $g(s) - a(s) + a(r) \equiv g(r) \pmod{D}$. Следовательно, для любого $h \in M$

$$(g(s))^\pi + h\varphi_s \equiv (g(r))^\pi + (a(r) - a(s) + h)\varphi_r \pmod{D}.$$

Поскольку $(g(s))^\pi - (g(r))^\pi \notin D$, разности представителей смежных классов группы G по подгруппе N вида $(a(r) - a(s) + h)\varphi_r - h\varphi_s$, $h \in M$, лежат в одном смежном классе группы G по подгруппе D с представителем $(g(s))^\pi - (g(r))^\pi \in N$. Следовательно, отображение $(\varphi_s)^{-1} \mu_{a(r)-a(s)} \varphi_r$ переводит каждое из подмножеств $T_1, T_2, \dots, T_{m'}$ в себя. Для каждого $g(s)$ найдутся ровно $d-1$ отличных от него представителей $g(j)$, для которых $g(s) - g(j) \in M \# D$, поскольку в противном случае возникает противоречие с тем, что $M \cap D = \{0\}$.

2) Если $M \cap D = \{0\}$, $N \cap D \neq \{0\}$, то для всех таких $s, j \in \{1, 2, \dots, n\}$, что $(g(s))^\pi \equiv (g(j))^\pi \pmod{D}$, и для любого $i \in \{1, 2, \dots, m\}$ имеет место сравнение

$$(t(i)(\varphi_s)^{-1} - t(i)(\varphi_j)^{-1}) \equiv (g(j) - g(s)) \pmod{D}.$$

3) Если $h \in L = M \cap D$, $h \neq 0$, то для любого $s \in \{1, 2, \dots, n\}$ и любого $h_1 \in M$ справедливо сравнение $h_1 \varphi_s \equiv (h + h_1) \varphi_s \pmod{D}$. Это означает, что все представители $t(1), t(2), \dots, t(m)$ смежных классов по подгруппе N принадлежат $q = [M : L]$ смежным классам группы G по подгруппе D , причем в каждом таком классе находится одинаковое число представителей. Пусть $t = U_1 \cup U_2 \cup \dots \cup U_q$ — разбиение множества t на классы элементов, сравнимых по подгруппе D , а $M = (L + f(1)) \cup \dots \cup (L + f(q))$, $f(1) \in L$, есть разбиение группы на смежные классы по подгруппе L . Тогда для любого $s \in \{1, 2, \dots, n\}$ отображение φ_s переводит класс $L + f(i)$, $i \in \{1, 2, \dots, q\}$, в класс $U_{j(i)}$ для некоторого $j(i) \in \{1, 2, \dots, q\}$.

Далее, если $(g(s))^\pi \equiv (g(j))^\pi (D)$ для некоторых различных $s, j \in \{1, 2, \dots, n\}$, то для любого $i \in \{1, 2, \dots, m\}$ справедливо сравнение

$$t(i)(\varphi_s)^{-1} - t(i)(\varphi_j)^{-1} \equiv g(s) - g(j) (D).$$

Заметим, что $t(i)(\varphi_s)^{-1} - t(i)(\varphi_j)^{-1} \in M$, $g(s) - g(j) \notin M$. Поэтому элемент $g(s) - g(j)$ лежит в смежном классе группы G по подгруппе D с представителем из подгруппы M . Отсюда следует, что если $D \supseteq M$, то $N \cap D = \{0\}$.

Пусть $N \cap D \neq \{0\}$. Тогда группа N распадается на $n'' = n/k$ смежных классов по подгруппе $N \cap D$, причем мощность каждого класса равна $k = |N \cap D|$. Поэтому множество представителей g также распадается на n'' подмножеств $V_1, V_2, \dots, V_{n''}$ мощности k , в каждом из которых содержатся элементы, принадлежащие одному и тому же смежному классу группы G по подгруппе D . При этом подстановка π переводит каждое множество V_l , $l \in \{1, 2, \dots, n''\}$, в смежный класс группы N по подгруппе $N \cap D$.

Наконец, рассмотрим случай $D \supseteq M$. Тогда $N \cap D = \{0\}$ и все представители $t(1), t(2), \dots, t(m)$ смежных классов по подгруппе N принадлежат одному смежному классу группы G по подгруппе D . Если $g(s) \equiv g(j) (D)$ для некоторых s и j , то $(g(s))^\pi \equiv (g(j))^\pi (D)$, поскольку для любого $h \in M$ имеет место сравнение $h\varphi_s \equiv h\varphi_j (D)$. Следовательно, $s = j$. Тогда группа M совпадает с группой D , группа G является прямой суммой своих подгрупп M и N , и все представители $g(1), g(2), \dots, g(n)$ смежных классов по подгруппе M принадлежат одному смежному классу группы G по подгруппе N .

Таким образом, во всех случаях, когда подгруппы M и N группы G имеют тривиальное ($M \cap D = \{0\}$ и $N \cap D = \{0\}$) или нетривиальное ($M \cap D \neq \{0\}$ или $N \cap D \neq \{0\}$) пересечение с подгруппой D , нами получены необходимые условия импримитивности группы $GR(\pi, \varphi)$, которые позволяют с достаточной полнотой охарактеризовать подгруппу D в терминах параметров подстановки $\rho(\pi, \varphi)$ или, наоборот, наложить ограничения на параметры подстановки $\rho(\pi, \varphi)$, исходя из строения подгруппы D .

Достаточность полученных условий устанавливается непосредственной проверкой.

Утверждение доказано. $\square$

Список литературы

- [1] Холл М., *Теория групп*, пер. с англ. Н. В. Дюмина, З. П. Жилинской, / под общ. ред. Л. А. Калужнина, М.: ИИЛ, 1962, 468 с.