Math-Net.Ru

Общероссийский математический портал

Ф. М. Малышев, Теорема Поста–Глускина–Хоссу для конечных n -квазигрупп и самоинвариантные семейства подстановок, *Матем. сб.*, 2016, том 207, номер 2, 81–92

DOI: <https://doi.org/10.4213/sm8447>

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: 35.173.219.12

26 апреля 2023 г., 08:55:48

УДК 512.548.74

Ф. М. Малышев

Теорема Поста–Глускина–Хоссу для конечных n -квазигрупп и самоинвариантные семейства подстановок

Исследуются конечные n -квазигруппы ($n \geq 3$) со следующим свойством дополнительной обратимости. Если на каких-то двух наборах из n аргументов с одинаковыми первыми компонентами квазигрупповая операция дает одинаковые результаты, то наборы из остальных $n-1$ компонент осуществляют одинаковые левые сдвиги. Для таких n -квазигрупп доказывается аналог теоремы Поста–Глускина–Хоссу, которая ранее доказывалась только в ассоциативном случае. Теорема сводит операцию n -квазигруппы к групповой. Основным средством для доказательства выступает вводимое и исследуемое в работе двухпараметрическое самоинвариантное семейство подстановок на произвольном конечном множестве.

Библиография: 13 названий.

Ключевые слова: n -квазигруппа, ассоциативность, n -арная группа, автоморфизм, латинский гиперкуб.

DOI: 10.4213/sm8447

§ 1. Введение

Напомним, что n -квазигрупповой операцией на множестве G называется отображение $A: G^n \rightarrow G$, являющееся биекцией (взаимно обратимым отображением) по каждому из n аргументов при любой фиксации остальных $n-1$ аргументов (см. [1; § 8]). Для $A(x_1, \dots, x_n)$ будем использовать обозначение $[x_1, \dots, x_n]$, $x_i \in G$, $i = 1, \dots, n$. Через

$$R_{(x_{i+1}, \dots, x_n)}: G^i \rightarrow G, \quad L_{(x_1, \dots, x_{n-i})}: G^i \rightarrow G, \quad i = 1, \dots, n-1,$$

обозначаем соответственно правые и левые сдвиги:

$$R_{(x_{i+1}, \dots, x_n)}(x_1, \dots, x_i) = [x_1, \dots, x_n] = L_{(x_1, \dots, x_{n-i})}(x_{n-i+1}, \dots, x_n).$$

Ассоциативная n -квазигруппа называется n -арной группой (см. [2; гл. I], [3]). Условие ассоциативности задается тождествами

$$[x_1, \dots, x_n], x_{n+1}, \dots, x_{2n-1} = [x_1, \dots, x_i, [x_{i+1}, \dots, x_{i+n}], x_{i+n+1}, \dots, x_{2n-1}], \quad i = 1, \dots, n-1. \quad (1.1)$$

Теорема Поста–Глускина–Хоссу (см. [4]–[6]) утверждает, что ассоциативная операция n -квазигруппы на множестве G может быть представлена в виде

$$[x_1, \dots, x_n] = x_1 \cdot \theta(x_2) \cdots \theta^{n-2}(x_{n-1}) \cdot \theta^{n-1}(x_n) \cdot c \quad (1.2)$$

для некоторых: групповой операции “ $\cdot$ ” на множестве G , автоморфизма $\theta \in \text{Aut}(G, \cdot)$, элемента $c \in G$, удовлетворяющих условиям

$$\theta^{n-1}(x) = c \cdot x \cdot c^{-1}, \quad x \in G, \quad \theta(c) = c. \quad (1.3)$$

До недавнего времени (см. [2; гл. II, п. 2.5]) эта теорема была известна как теорема Глускина–Хоссу или теорема Хоссу–Глускина. Изучение работ В. Дернте [7] и Э. Поста [4], проведенное в статье [8], убедительно показало, что включение фамилии Поста в название теоремы не должно вызывать возражений, этим восстанавливается историческая справедливость.

Обобщения и уточнения этой теоремы для более слабых условий ассоциативности имеются в работе Ф. Н. Сохацкого [9]. Методы доказательств работы [9] напоминают рассуждения наиболее изящного доказательства теоремы Поста–Глускина–Хоссу, принадлежащего Е. И. Соколову [10]. Вплоть до настоящего времени данная теорема остается актуальной для специалистов по n -группоидам (см., например, [11]).

В настоящей работе требование ассоциативности (1.1) в этой теореме ослабляется настолько, что исчезает условие (1.3), а правый сдвиг на элемент c в (1.2) заменяется на произвольную подстановку множества G .

ОПРЕДЕЛЕНИЕ 1. Будем говорить, что n -квазигруппа G является *1-слабо обратимой справа*, если для любых $\bar{b}_1, \bar{b}_2 \in G$ из равенства $[a, \bar{b}_1] = [a, \bar{b}_2]$ при некотором $a \in G$ следует равенство $[\bar{b}_1, x] = [\bar{b}_2, x]$ для всех $x \in G$.

Применяя тождество (1.1) при $i = 1$ к обеим частям равенства

$$[[a, \bar{b}_1], x_{n+1}, \dots, x_{2n-1}] = [[a, \bar{b}_2], x_{n+1}, \dots, x_{2n-1}],$$

убеждаемся, что для n -квазигрупп из ассоциативности следует *1-слабая обратимость справа*. Но из 1-слабой обратимости справа, как показывается ниже, ассоциативность не следует.

Нетрудно еще видеть, что если условие 1-слабой обратимости справа справедливо для n -квазигруппы G с операцией $A: G^n \rightarrow G$, то оно будет справедливо также для n -квазигрупп с операциями

$$\tilde{A}: G^n \rightarrow G, \quad \tilde{A}(x_1, \dots, x_n) = (\sigma A)(x_1, \dots, x_n) = \sigma(A(x_1, \dots, x_n)),$$

где подстановка σ на G , $\sigma \in S_G$, может быть любой. Это позволяет далее переходить при необходимости к n -квазигруппам, для которых при некотором заданном элементе $e \in G$ справедливо тождество $[e, \dots, e, x] = x$, $x \in G$.

В § 2 работы доказываемся следующая теорема.

ТЕОРЕМА 1. Пусть имеется конечная n -квазигруппа G со свойством 1-слабой обратимости справа. Тогда для некоторых: подстановки $\sigma \in S_G$, групповой операции “ $\cdot$ ” на множестве G и автоморфизма $\varphi \in \text{Aut}(G, \cdot)$ справедливо тождество

$$\sigma([x_1, \dots, x_n]) = x_1 \cdot \varphi(x_2) \cdots \varphi^{n-2}(x_{n-1}) \cdot \varphi^{n-1}(x_n), \quad x_i \in G, \quad i = 1, \dots, n.$$

Утверждаемое в этой теореме будет справедливо и для n -квазигрупп $A: G^n \rightarrow G$ с аналогично определяемой 1-слабой обратимостью слева. Для доказательства достаточно теорему 1 применить к n -квазигруппе G с 1-слабо обратимой справа операций $[x_1, \dots, x_n] = A(x_n, \dots, x_1)$ и затем обратиться к групповой операции $a \circ b = b \cdot a$.

Теорему 1 можно применять к n -группам. Пусть при этом e – единица группы $(G, \cdot)$. Из теоремы 1 и тождества (1.1) при $i = 1$ и $x_2 = \dots = x_{n+1} = e$ следует равенство $\sigma^{-1}(x_1) = x_1 \cdot c$, $x_1 \in G$, $c = \varphi(\sigma^{-1}(e))$. Таким образом, выполнено тождество (1.2). Далее, из тождеств (1.2) и (1.1) при $i = 1$ следуют условия (1.3). В результате получаем новое доказательство исходной теоремы Поста–Глускина–Хоссу для конечных n -арных групп.

Как видим, n -группы составляют малую долю в классе n -квазигрупп со свойством 1-слабой обратимости справа. Ясно, что n -квазигруппа из теоремы 1 не будет n -группой, если не будет выполнена совокупность следующих требований:

- i) $\sigma^{-1}(x) = xc$, $c = \varphi(\sigma^{-1}(e))$, $x \in G$ – любое;
- ii) $\varphi(c) = c$;
- iii) $\varphi^{n-1}(x) = cxc^{-1}$, $x \in G$ – любое.

Например, если n четно, G – циклическая группа 3-го порядка, $\varphi \in \text{Aut}G \setminus \{\text{id}_G\}$, $\sigma = \text{id}_G$, то $c = e$, а $\varphi^{n-1} = \varphi \neq \text{id}_G$, поэтому соответствующая n -квазигруппа не будет n -группой.

Эквивалентный и более традиционный для теории n -квазигрупп способ выделения 1-слабо обратимых справа n -квазигрупп предоставляет приводимое ниже предложение¹ 1. Это предложение имеет дело с одним специальным функциональным уравнением общей ассоциативности (см. [2; гл. IV]):

$$f(x, h(\bar{y}, z)) = g(h(x, \bar{y}), z). \quad (1.4)$$

В этом уравнении неизвестными являются $(n-1)$ -квазигруппа h и 2-квазигруппы f, g . Через $x, \bar{y}, z$ в уравнении (1.4) обозначаются независимые переменные со значениями из G, G^{n-2}, G соответственно.

ПРЕДЛОЖЕНИЕ 1. *Тогда и только тогда n -квазигруппа $A: G^n \rightarrow G$ является 1-слабо обратимой справа, когда*

$$A(x, \bar{y}, z) = f(x, h(\bar{y}, z)) = g(h(x, \bar{y}), z),$$

где тройка квазигрупп $(f, g, h): f: G^2 \rightarrow G, g: G^2 \rightarrow G, h: G^{n-1} \rightarrow G$ является решением функционального уравнения (1.4).

ДОКАЗАТЕЛЬСТВО. Свойство 1-слабой обратимости справа для n -квазигруппы $A(x, \bar{y}, z)$ вида (1.4) легко проверяется непосредственно. Обратно, пусть n -квазигруппа $A: G^n \rightarrow G$ является 1-слабо обратимой справа. Выберем некоторый элемент $a \in G$. Пару элементов $\bar{v}, \bar{v}' \in G^{n-1}$ отнесем к одному классу эквивалентности, если $A(a, \bar{v}) = A(a, \bar{v}')$. Имеем ровно $|G|$ классов эквивалентности, поскольку операция A является n -квазигруппой. Разбиение G^{n-1} на

¹На это обстоятельство автору указал рецензент.

классы эквивалентности, отвечающие другому элементу $a' \in G$, $a' \neq a$, останутся прежним. Иначе, при заданном $d \in G$ из определения 1 получили бы противоречие: $|\{A(\bar{v}, d), \bar{v} \in G^{n-1}\}| < |G|$. Рассмотрим отображение $h: G^{n-1} \rightarrow G$ с одинаковыми значениями на каждом классе эквивалентности, но с различными значениями на разных классах эквивалентности. Отображение h задает $(n-1)$ -квазигруппу на G . Квазигруппы f и g определим соответственно тождествами $A(x, \bar{u}) = f(x, h(\bar{u}))$ и $A(\bar{u}, z) = g(h(\bar{u}), z)$, в которых $\bar{u}$ независимая от x переменная со значениями в G^{n-1} . Предложение 1 доказано.

В работе [12] рассматривалось более общее функциональное уравнение:

$$f(\bar{x}, h_1(\bar{y}, \bar{z})) = g(h_2(\bar{x}, \bar{y}), \bar{z}),$$

где $\bar{x}, \bar{y}, \bar{z}$ – независимые переменные со значениями в декартовых степенях G^l, G^m, G^k соответственно. Там, в частности, доказано (см. также [2; гл. 4, п. 4.2]), что если четверка квазигрупп $f: G^{l+1} \rightarrow G$, $g: G^{k+1} \rightarrow G$, $h_1: G^{m+k} \rightarrow G$, $h_2: G^{l+m} \rightarrow G$ является решением этого уравнения, то для некоторой групповой операции “ $\circ$ ” на G и квазигрупп $L: G^l \rightarrow G$, $M: G^m \rightarrow G$, $K: G^k \rightarrow G$ справедливо

$$f(\bar{x}, h_1(\bar{y}, \bar{z})) = g(h_2(\bar{x}, \bar{y}), \bar{z}) = L(\bar{x}) \circ M(\bar{y}) \circ K(\bar{z}).$$

В случае уравнения (1.4) $l = k = 1$, $m = n - 2$, L и K будут подстановками на G , причем условие $h_1 = h_2$ в (1.4) позволяет доказать, что $(n-2)$ -квазигруппа M тоже будет 1-слабо обратимой справа. Это позволяет надеяться получить на этом пути другое доказательство теоремы 1, отличное от предлагаемого в настоящей работе.

Основным средством для доказательства теоремы 1 в § 2 будут так называемые *двупараметрические самоинвариантные семейства подстановок* на множестве G .

ОПРЕДЕЛЕНИЕ 2. Семейство подстановок на множестве G $\pi_{x,y} \in S_G$, $x, y \in G$, назовем *самоинвариантным*, если для всех $x, y, z, u, v \in G$:

- а) $\pi_{y,z}\pi_{x,y} = \pi_{x,z}$,
- б) $\pi_{\pi_{x,y}(u), \pi_{x,y}(v)} = \pi_{u,v}$.

Доказательство теоремы 1 основано на следующем результате о строении *самоинвариантных* семейств подстановок.

ТЕОРЕМА 2. Пусть на конечном множестве G имеется самоинвариантное семейство подстановок $\pi_{x,y} \in G$, $x, y \in G$, для которого группа $H = \langle \pi_{x,y} \mid x, y \in G \rangle$ транзитивна на G . Тогда для некоторой групповой операции “ $\cdot$ ” на множестве G и автоморфизма $\varphi \in \text{Aut}(G, \cdot)$ будем иметь $\pi_{x,y} = L_{\varphi(y^{-1} \cdot x)}$, $x, y \in G$, где $L_z(u) = z \cdot u$, $z, u \in G$.

Теорема 2 доказывается в § 3. В § 4 доказывается теорема 3 о строении *самоинвариантных* семейств подстановок на множестве G , для которых множество G разбивается на несколько орбит под действием группы H .

§ 2. Задание n -квазигрупп со свойством слабой обратимости через групповую операцию (доказательство теоремы 1)

Далее предполагаем, что на конечном множестве G задана n -квазигрупповая операция $[x_1, \dots, x_n]$, обладающая свойством из определения 1, которое для краткости называем слабой обратимостью.

“Таблица” Кэли n -квазигруппы образует латинский гиперкуб, у которого на позиции с номером $(x_1, \dots, x_n) \in G^n$ располагается значение $[x_1, \dots, x_n] \in G$. Сечение этого куба путем фиксации любых $n - 2$ компонент будет латинским квадратом.

Как обычно, диагональю считаем множество из $|G|$ позиций латинского квадрата, в которых находится один и тот же элемент. На диагонали нет двух позиций в одной строке или в одном столбце. Совокупность всех диагоналей латинского квадрата образует разбиение множества его позиций [13].

ПРЕДЛОЖЕНИЕ 2. Пусть имеются конечная n -квазигруппа G со свойством слабой обратимости и отвечающий ей латинский гиперкуб. Разбиение на диагонали позиций латинских квадратов на всех сечениях $x_1 = a_1, \dots, x_{n-2} = a_{n-2}$ одно и то же, не зависит от конкретного $\bar{a} = (a_1, \dots, a_{n-2}) \in G^{n-2}$.

ДОКАЗАТЕЛЬСТВО. Предположим противное: существуют диагонали с парами позиций $(\bar{a}, i, j)$, $(\bar{a}, i_1, j_1)$ для квадрата в сечении $(a_1, \dots, a_{n-2}) = \bar{a} \in G^{n-2}$ и $(\bar{b}, i, j)$, $(\bar{b}, i_1, j_2)$ для квадрата в сечении $(b_1, \dots, b_{n-2}) = \bar{b} \in G^{n-2}$, в которых $j_1 \neq j_2$. Это означает, что $[\bar{a}, i_1, j_1] = [\bar{a}, i, j]$ и $[\bar{b}, i, j] = [\bar{b}, i_1, j_2]$. Пусть $\bar{a} = (a_1, \bar{a}_2) \in G \times G^{n-3}$, $\bar{b} = (b_1, \bar{b}_2) \in G \times G^{n-3}$. Применяя по одному разу свойство слабой обратимости, получаем $[\bar{a}_2, i_1, j_1, u_1] = [\bar{a}_2, i, j, u_1]$, $[\bar{b}_2, i, j, u_1] = [\bar{b}_2, i_1, j_2, u_1]$ для любого $u_1 \in G$. Применяя свойство слабой обратимости еще по $n - 3$ раза, получаем $[i_1, j_1, \bar{u}] = [i, j, \bar{u}] = [i_1, j_2, \bar{u}]$, $\bar{u} \in G^{n-2}$, поэтому $j_1 = j_2$. Полученное противоречие доказывает предложение 2.

Для каждого $\bar{a} \in G^{n-2}$ определим семейство подстановок $\pi_{i,j}^{\bar{a}} \in S_G$, $i, j \in G$, полагая $\pi_{i,j}^{\bar{a}}(\alpha) = \beta$, если $[\bar{a}, i, \alpha] = [\bar{a}, j, \beta]$. Очевидно, $\pi_{j,k}^{\bar{a}} \pi_{i,j}^{\bar{a}} = \pi_{i,k}^{\bar{a}}$, в частности, $\pi_{i,i}^{\bar{a}} = \text{id}_G$. Эти же подстановки задаются требованием принадлежности позиций $(\bar{a}, i, \alpha)$, $(\bar{a}, j, \beta)$ одной и той же диагонали латинского квадрата в сечении $(x_1, \dots, x_{n-2}) = \bar{a}$. При таком задании из предложения 2 следует, что $\pi_{i,j}^{\bar{a}} = \pi_{i,j}^{\bar{b}}$ для всех $\bar{a} \neq \bar{b}$. Другими словами,

$$[\bar{a}, i, \alpha] = [\bar{a}, j, \beta] \iff [\bar{b}, i, \alpha] = [\bar{b}, j, \beta].$$

Далее индекс $\bar{a}$ в обозначении введенных подстановок не указываем.

ПРЕДЛОЖЕНИЕ 3. Семейство подстановок $\pi_{i,j} \in S_G$, $i, j \in G$, является самоинвариантным.

ДОКАЗАТЕЛЬСТВО. Необходимо убедиться, что из равенства $\pi_{i,j}(\alpha) = \beta$ следует $\pi_{i',j'}(\alpha) = \beta$, где $i' = \pi_{a,b}(i)$, $j' = \pi_{a,b}(j)$. Зафиксируем некоторый элемент $e \in G$. Обозначим $c = (e, \dots, e) \in G^{n-2}$, $c' = (e, \dots, e) \in G^{n-3}$. По свойству слабой обратимости из равенств $[c', a, i, \alpha] = [c', a, j, \beta]$, $[c, a, i] = [c, b, i']$,

$[c, a, j] = [c, b, j']$ получаем

$$[c', b, i', \alpha] = [c', a, i, \alpha] = [c', a, j, \beta] = [c', b, j', \beta],$$

поэтому $\pi_{i', j'}(\alpha) = \beta$. Предложение 3 доказано.

ПРЕДЛОЖЕНИЕ 4. *Группа $H = \langle \pi_{x,y} \mid x, y \in G \rangle$ транзитивна на множестве G .*

ДОКАЗАТЕЛЬСТВО. Пусть $c \in G^{n-2}$, $x \in G$, и $\alpha, \beta \in G$ – произвольные. Наличие элемента $y \in G$, при котором $\beta = \pi_{x,y}(\alpha)$, следует из биективности n -квазигрупповой операции по предпоследнему аргументу, так как

$$\pi_{x,y}(\alpha) = \beta \iff [c, x, \alpha] = [c, y, \beta].$$

Предложение 4 доказано.

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 1. Принимая во внимание предложения 2–4, по теореме 2 (доказываемой в § 3), для некоторой групповой операции на G и $\varphi \in \text{Aut}(G)$ имеем представление $\pi_{x,y} = L_{\varphi(y^{-1}x)}$. Пусть $e \in G$ – единица группы и $[e, \dots, e, v] = v$ для всех $v \in G$. Вычислим $[x_1, \dots, x_n]$. Вначале обозначим $x'_2 = \pi_{x_1, e}(x_2) = \varphi(x_1)x_2$. Последовательно для $i = 3, \dots, n$ обозначим

$$x'_i = \pi_{x'_{i-1}, e}(x_i) = \varphi(x'_{i-1})x_i = \varphi^{i-1}(x_1)\varphi^{i-2}(x_2) \cdots \varphi(x_{i-1})x_i.$$

По свойству слабой обратимости индукцией по $i = 2, \dots, n$ последовательно получаем равенства:

$$\begin{aligned} [e, \dots, e, x_1, x_2] &= [e, \dots, e, x'_2], \\ [e, \dots, e, x_1, x_2, x_3] &= [e, \dots, e, x'_2, x_3] = [e, \dots, e, x'_3], \\ [e, \dots, e, x_1, \dots, x_{i-1}, x_i] &= [e, \dots, e, x'_{i-1}, x_i] = [e, \dots, e, x'_i], \\ [e, \dots, e, x_1, \dots, x_i, x_{i+1}] &= [e, \dots, e, x'_i, x_{i+1}] = [e, \dots, e, x'_{i+1}], \\ [e, x_1, \dots, x_{n-2}, x_{n-1}] &= [e, \dots, e, x'_{n-2}, x_{n-1}] = [e, \dots, e, x'_{n-1}], \\ [x_1, \dots, x_{n-1}, x_n] &= [e, \dots, e, x'_{n-1}, x_n] = [e, \dots, e, x'_n] = x'_n \\ &= \varphi^{n-1}(x_1)\varphi^{n-2}(x_2) \cdots \varphi(x_{n-1})x_n. \end{aligned}$$

Полагая $\sigma = \varphi^{-(n-1)}$, завершаем доказательство теоремы 1.

§ 3. Самоинвариантные семейства подстановок (доказательство теоремы 2)

Пусть $\Pi = \{\pi_{x,y} \in S_G \mid x, y \in G\}$ – самоинвариантное семейство подстановок на множестве G и $G = \coprod_{i \in I} G_i$ – разбиение на орбиты группы $H = \langle \pi_{x,y} \mid x, y \in G \rangle$. Семейство подстановок Π индуцирует самоинвариантные семейства подстановок Π_i , $i \in I$, на каждой орбите G_i , $\Pi_i = \{\pi_{x,y}|_{G_i} \in S_{G_i} \mid x, y \in G_i\}$. Группа подстановок $H_i = \langle \pi_{x,y}|_{G_i} \mid x, y \in G_i \rangle \subseteq S_{G_i}$ для разных $i \in I$ может быть как транзитивной, так и не транзитивной на G_i . Дадим индуктивное определение глубины $h(\Pi)$ самоинвариантного семейства подстановок Π .

ОПРЕДЕЛЕНИЕ 3. Если $|I| = 1$, то $h(\Pi) = 0$, если же $|I| > 1$, то $h(\Pi) = 1 + \max_{i \in I} h(\Pi_i)$.

В теореме 2 утверждается, что самоинвариантные семейства подстановок глубины 0 могут выражаться через групповые операции.

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 2. В условиях этой теоремы группа H транзитивно действует на G . Предположим вначале, что это действие регулярно. Тогда можно считать, что $G = H$ и действие H на G осуществляется левыми сдвигами. Таким образом, если $e \in G$ – единица группы, то $\pi_{x,e} = L_{\varphi(x)}$ для некоторого отображения $\varphi: G \rightarrow G$, причем $\varphi(e) = e$. По определению 2 для самоинвариантного семейства подстановок будем иметь

$$\pi_{a,b} = \pi_{e,b}\pi_{a,e} = \pi_{b,e}^{-1}\pi_{a,e} = L_{\varphi(b)^{-1}}L_{\varphi(a)} = L_{\varphi(b)^{-1}\varphi(a)}.$$

Самоинвариантность нашего семейства подстановок означает, что $\pi_{xa,xb} = \pi_{a,b}$ для всех $x \in G$, поэтому $L_{\varphi(xb)^{-1}\varphi(xa)} = L_{\varphi(b)^{-1}\varphi(a)}$; из последнего равенства следует $\varphi(xb)^{-1}\varphi(xa) = \varphi(b)^{-1}\varphi(a)$. Полагая в последнем равенстве $b = e$, получаем $\varphi(xa) = \varphi(x)\varphi(a)$. Так как подстановки $\pi_{x,y}$, $x, y \in G$, порождают всю группу $H = G$, то гомоморфизм φ обязан быть эпиморфизмом и даже автоморфизмом, поскольку $|G| < \infty$.

Предположим теперь, что действие группы H на множестве G не является регулярным. Рассмотрим каноническое отображение $\tau: H \rightarrow G$, $\tau(h) = h(e)$, $h \in H$. Здесь $e \in G$ – некоторый фиксированный элемент. Самоинвариантное семейство подстановок $\Pi = \{\pi_{x,y} \in S_G \mid x, y \in G\}$ на G индуцирует самоинвариантное (левоинвариантное) семейство подстановок

$$\hat{\Pi} = \{\hat{\pi}_{h_1,h_2} = L_{\pi_{\tau(h_1),\tau(h_2)}} \in S_H \mid h_1, h_2 \in H\}.$$

Равенство $\hat{\pi}_{h_2,h_3}\hat{\pi}_{h_1,h_2} = \hat{\pi}_{h_1,h_3}$ очевидно выполняется. Проверим собственно самоинвариантность.

$$\begin{aligned} \hat{\pi}_{\hat{\pi}_{a,b}(h_1),\hat{\pi}_{a,b}(h_2)} &= \hat{\pi}_{\pi_{\tau(a),\tau(b)} \cdot h_1, \pi_{\tau(a),\tau(b)} \cdot h_2} = L_{\pi_{\tau(\pi_{\tau(a),\tau(b)} \cdot h_1), \tau(\pi_{\tau(a),\tau(b)} \cdot h_2)}} \\ &= L_{\pi_{\pi_{\tau(a),\tau(b)}(h_1(e)), \pi_{\tau(a),\tau(b)}(h_2(e))}} = L_{\pi_{h_1(e), h_2(e)}} = L_{\pi_{\tau(h_1), \tau(h_2)}} = \hat{\pi}_{h_1,h_2}. \end{aligned}$$

В регулярном случае теорема доказана, поэтому имеются другая (возможно) групповая операция “ $\circ$ ” на H и автоморфизм $\Phi \in \text{Aut}(H, \circ)$, при которых $\hat{\pi}_{h_1,h_2} = L_{\Phi(h_2^{-1}(\circ) \circ h_1)}^\circ$. Левый сдвиг и взятие обратного элемента рассматриваются относительно операции “ $\circ$ ”.

Рассмотрим такой элемент $h \in H$, что $h \neq \text{id}_G$, но $h(e) = e$. Из равенств

$$L_{\Phi((\text{id}_G)^{-1}(\circ) \circ h)}^\circ = \hat{\pi}_{h,\text{id}_G} = L_{\pi_{\tau(h),\tau(\text{id}_G)}} = L_{\pi_{e,e}} = L_{\text{id}_G} = \text{id}_H$$

следует $h = \text{id}_G$. Полученное противоречие завершает доказательство теоремы 2.

ЗАМЕЧАНИЕ 1. Если G – группа и $\varphi: G \rightarrow G$ – ее гомоморфизм (не обязательно автоморфизм), то семейство подстановок $\Pi = \{\pi_{x,y} = L_{\varphi(y^{-1}x)} \mid x, y \in G\}$ все равно будет самоинвариантным. Только в этом случае его глубина не обязана быть нулевой. Так, если $G = \mathbb{Z}_{2^n}$ – аддитивная группа вычетов по модулю 2^n , а φ – умножение на 2, то $h(\Pi) = n$.

§ 4. Самоинвариантные семейства подстановок глубины 1

В этом параграфе изучаются самоинвариантные семейства подстановок $\Pi = \{\pi_{x,y} \in S_X \mid x, y \in X\}$ на множестве X глубины 1. Согласно определению 3 в этом случае имеем нетривиальное разбиение $X = \coprod_{i \in I} X_i$ на орбиты X_i при действии группы $H = \langle \pi_{x,y} \mid x, y \in X \rangle$ на X , причем индуцированные самоинвариантные семейства подстановок $\Pi_i = \{\pi_{x,y}|_{X_i} \in S_{X_i} \mid x, y \in X_i\}$ на X_i имеют глубину 0 для всех $i \in I$. В соответствии с теоремой 2 каждое подмножество X_i , $i \in I$, наделяется структурой группы с единицей $e_i \in X_i$.

Для $x \in X_i$, $y \in X_j$ и $k \in I$ будем использовать обозначение $\pi_{x,y}|_{X_k} = {}^k_{ij}\pi_{x,y}$. Если $s_{ij} \in X_i$ – некоторый элемент, то через S_{ij} будем обозначать внутренний автоморфизм: $S_{ij}: X_i \rightarrow X_i$, $S_{ij}(x) = s_{ij}x s_{ij}^{-1}$, $x \in X_i$.

ТЕОРЕМА 3. Пусть $\Pi = \{\pi_{x,y} \in S_X \mid x, y \in X\}$ – самоинвариантное семейство подстановок на множестве X глубины 1 и $X = \coprod_{i \in I} X_i$ – соответствующее разбиение на орбиты группы $H = \langle \pi_{x,y} \mid x, y \in X \rangle$, $o \in I$ – некоторый фиксированный элемент. Тогда все группы X_i , $i \in I$, изоморфны, семейство Π определяется по двум матрицам

$$\Phi = (\varphi_{ij}), \quad i, j \in I, \quad \varphi_{i,j} \in \text{Iso}(X_i, X_j), \quad S = (s_{ij}), \quad i, j \in I, \quad s_{ij} \in X_i,$$

в которых $s_{oo} = e_o$ и для всех $i, j \in I$

$$\varphi_{ij} = \varphi_{oj} \varphi_{oo}^{-1} S_{oi} \varphi_{oo}^2 \varphi_{oi}^{-1}, \quad (4.1)$$

$$s_{ij} = \varphi_{oi} \varphi_{oo}^{-1} (s_{oj} s_{oi}^{-1}), \quad (4.2)$$

а сами подстановки $\pi_{x,y}$ задаются равенствами

$${}^k_{ij}\pi_{x,y} = L_{\varphi_{jk}(y^{-1}) s_{kj} s_{ki}^{-1} \varphi_{ik}(x)}, \quad i, j, k \in I, \quad x \in X_i, \quad y \in X_j. \quad (4.3)$$

Обратно, если имеются изоморфные группы X_i , $i \in I$, и матрицы Φ и S , в которых o -е строки произвольные, за исключением $s_{oo} = e_o$, а элементы остальных строк этих матриц определяются условиями (4.1) и (4.2), то семейство подстановок Π на $\coprod_{i \in I} X_i$, определяемое равенствами (4.3), будет самоинвариантным глубины 1.

ДОКАЗАТЕЛЬСТВО. Обратное утверждение теоремы проверяется непосредственно. Проверка упростится, если предварительно с помощью условий (4.1) и (4.2) проверить для $i, j, k, p, q \in I$ равенства

$$S_{kq}^{-1} \varphi_{qk} \varphi_{jq} = S_{kp}^{-1} \varphi_{pk} \varphi_{jp}, \quad (4.4)$$

$$S_{kq}^{-1} \varphi_{qk} (s_{qi} s_{qj}^{-1}) = S_{kp}^{-1} \varphi_{pk} (s_{pi} s_{pj}^{-1}), \quad (4.5)$$

$$s_{ii} = e_i. \quad (4.6)$$

Докажем первую часть теоремы. Всюду по умолчанию будет предполагаться, что промежуточные выкладки выполняются для всех значений переменных из соответствующих множеств I и X_i , $i \in I$.

По теореме 2 для каждого $i \in I$ найдется автоморфизм $\varphi_{ii}: X_i \rightarrow X_i$ такой, что ${}^i_{ii}\pi_{x,y} = L_{\varphi_{ii}(y^{-1}x)}$. Вид подстановок ${}^j_{ii}\pi_{x,y}$ получим с помощью условия б) определения 2

$$\pi_{\pi_{x,y}(u), \pi_{x,y}(v)} = \pi_{u,v}, \quad u, v, x, y \in X. \quad (4.7)$$

Для $x, y, u, v \in X_i$ равенство (4.7) на множестве X_j примет вид

$${}^j_{ii}\pi_{\varphi_{ii}(y^{-1}x)u, \varphi_{ii}(y^{-1}x)v} = {}^j_{ii}\pi_{u,v}.$$

Таким образом,

$${}^j_{ii}\pi_{zu, zv} = {}^j_{ii}\pi_{u,v}, \quad z, u, v \in X_i. \quad (4.8)$$

Обозначим ${}^j_{ii}\pi_{u, e_i} = f_{ij}(u)$ для некоторого отображения $f_{ij}: X_i \rightarrow S_{X_j}$, $f_{ij}(e_i) = \text{id}_{X_j}$. По условию а) определения 2 тогда получим

$${}^j_{ii}\pi_{u,v} = f_{ij}(v)^{-1}f_{ij}(u). \quad (4.9)$$

Условие (4.8) теперь переписется в виде $f_{ij}(xv)^{-1}f_{ij}(xu) = f_{ij}(v)^{-1}f_{ij}(u)$, а при $v = e_i$ в виде $f_{ij}(xu) = f_{ij}(x)f_{ij}(u)$. После этого из условия (4.9) получаем

$${}^j_{ii}\pi_{u,v} = f_{ij}(v^{-1}u). \quad (4.10)$$

Равенство (4.7) на множестве X_j для $u, v \in X_j$, $x, y \in X_i$ представляется в виде

$$L_{\varphi_{jj}({}^j_{ii}\pi_{x,y}(v)^{-1}, {}^j_{ii}\pi_{x,y}(u))} = L_{\varphi_{jj}(v^{-1}u)},$$

поэтому

$${}^j_{ii}\pi_{x,y}(v)^{-1} \cdot {}^j_{ii}\pi_{x,y}(u) = v^{-1}u,$$

а с учетом (4.10)

$$f_{ij}(y^{-1}x)(v)^{-1}f_{ij}(y^{-1}x)(u) = v^{-1}u$$

или

$$f_{ij}(t)(u)u^{-1} = f_{ij}(t)(v)v^{-1} = \varphi_{ij}(t)$$

для некоторого отображения $\varphi_{ij}: X_i \rightarrow X_j$. Таким образом, $f_{ij}(t) = L_{\varphi_{ij}(t)}$, $t \in X_i$. Коль скоро f_{ij} – гомоморфизм, то φ_{ij} тоже будет гомоморфизмом. Окончательно из (4.10) имеем

$${}^j_{ii}\pi_{x,y} = L_{\varphi_{ij}(y^{-1}x)} \quad (4.11)$$

для некоторой матрицы гомоморфизмов $\Phi = (\varphi_{ij})$, $i, j \in I$, $\varphi_{ij} \in \text{Hom}(X_i, X_j)$, в которой по диагонали располагаются автоморфизмы.

Чтобы полностью представить семейство подстановок $\pi_{x,y}$, $x, y \in X$, осталось определить подстановки ${}^i_{ij}\pi_{e_i, e_j}$. Положив в равенстве (4.7) $u, v \in X_i$, $x = e_i$, $y = e_j$, получим

$${}^i_{ij}\pi_{{}^i_{ij}\pi_{e_i, e_j}(u), {}^i_{ij}\pi_{e_i, e_j}(v)} = {}^i_{ii}\pi_{u,v}.$$

Поскольку φ_{ii} – автоморфизм, последнее равенство означает, что

$${}^i_{ij}\pi_{e_i, e_j}(v)^{-1} \cdot {}^i_{ij}\pi_{e_i, e_j}(u) = v^{-1}u$$

или

$${}_{ij}^i \pi_{e_i, e_j}(v)v^{-1} = {}_{ij}^i \pi_{e_i, e_j}(u)u^{-1} = s_{ij}.$$

Здесь $s_{ij} \in X_i$ – некоторая константа. Таким образом,

$${}_{ij}^i \pi_{e_i, e_j} = L_{s_{ij}}, \quad i, j \in I, \quad (4.12)$$

для некоторой матрицы $S = (s_{ij})$, $i, j \in I$, $s_{ii} = e_i$.

В общем случае по условию а) определения 2 из равенств (4.11) и (4.12) получаем

$$\begin{aligned} {}_{ij}^k \pi_{x, y} &= {}_{jj}^k \pi_{e_j, y} \cdot {}_{kj}^k \pi_{e_k, e_j} \cdot {}_{ik}^k \pi_{e_i, e_k} \cdot {}_{ii}^k \pi_{x, e_i} = {}_{jj}^k \pi_{e_j, y} \cdot {}_{kj}^k \pi_{e_k, e_j} \cdot ({}_{ki}^k \pi_{e_k, e_i})^{-1} \cdot {}_{ii}^k \pi_{x, e_i} \\ &= L_{\varphi_{jk}(y^{-1})} L_{s_{kj}} (L_{s_{ki}})^{-1} L_{\varphi_{ik}(x)} = L_{\varphi_{jk}(y^{-1}) s_{kj} s_{ki}^{-1} \varphi_{ik}(x)}. \end{aligned}$$

Выясним теперь, при каких требованиях на элементы матриц Φ и S семейство подстановок, определяемое равенствами (4.3), будет самоинвариантным. Пока только известно, кроме условия (4.6), что гомоморфизмы φ_{ij} при $i = j$ являются автоморфизмами.

Условие а) определения 2 выполнено при любых матрицах Φ и S . Обратимся к условию б) этого определения. Пусть равенство (4.7) рассматривается на X_k и $x \in X_i$, $y \in X_j$, $u \in X_p$, $v \in X_q$. Тогда оно примет вид

$${}_{pq}^k \pi_{ij}^p \pi_{x, y}(u), {}_{ij}^q \pi_{x, y}(v) = {}_{pq}^k \pi_{u, v}.$$

Из этого равенства, применяя (4.3), получаем

$${}_{pq}^k \pi_{\varphi_{jp}(y^{-1}) s_{pj} s_{pi}^{-1} \varphi_{ip}(x) u, \varphi_{jq}(y^{-1}) s_{qj} s_{qi}^{-1} \varphi_{iq}(x) v} = {}_{pq}^k \pi_{uv},$$

откуда, в свою очередь, имеем

$$\begin{aligned} &\varphi_{qk}(v^{-1}) \varphi_{qk} \varphi_{iq}(x^{-1}) \varphi_{qk}(s_{qi} s_{qj}^{-1}) \varphi_{qk} \varphi_{jq}(y) s_{kq} s_{kp}^{-1} \varphi_{pk} \varphi_{jp}(y^{-1}) \varphi_{pk}(s_{pj} s_{pi}^{-1}) \\ &\times \varphi_{pk} \varphi_{ip}(x) \varphi_{pk}(u) = \varphi_{qk}(v^{-1}) s_{kq} s_{kp}^{-1} \varphi_{pk}(u). \end{aligned}$$

После сокращений последнее равенство преобразуется к виду

$$\begin{aligned} &\varphi_{qk}(s_{qi} s_{qj}^{-1}) \varphi_{qk} \varphi_{jq}(y) s_{kq} s_{kp}^{-1} \varphi_{pk} \varphi_{jp}(y^{-1}) \\ &= \varphi_{qk} \varphi_{iq}(x) s_{kq} s_{kp}^{-1} \varphi_{pk} \varphi_{ip}(x^{-1}) \varphi_{pk}(s_{pi} s_{pj}^{-1}). \end{aligned} \quad (4.13)$$

Полагая в (4.13) $i = j$, $u = x^{-1}y$, находим

$$\varphi_{qk} \varphi_{jq}(u) s_{kq} s_{kp}^{-1} \varphi_{pk} \varphi_{jp}(u^{-1}) = s_{kq} s_{kp}^{-1}. \quad (4.14)$$

Используя (4.14) в равенстве (4.13), получаем

$$\varphi_{qk}(s_{qi} s_{qj}^{-1}) s_{kq} s_{kp}^{-1} = s_{kq} s_{kp}^{-1} \varphi_{pk}(s_{pi} s_{pj}^{-1}). \quad (4.15)$$

Таким образом, условие (4.7) равносильно равенству (4.13), которое, в свою очередь, равносильно двум равенствам (4.14) и (4.15). Равенства (4.14) и (4.15) можно переписать соответственно в виде (4.4) и (4.5).

Полагая в (4.4) $k = p = j$, $q = i$, заключаем, что φ_{ij} являются изоморфизмами.

Для доказательства теоремы 3 осталось из равенств (4.4)–(4.6) получить соотношения (4.1) и (4.2).

Подставив в (4.4) $q = i$, $p = j = o$, получим

$$\varphi_{ik} = S_{ki} S_{ko}^{-1} \varphi_{ok} \varphi_{oo} \varphi_{oi}^{-1}. \quad (4.16)$$

Используя данное представление для φ_{ik} в (4.4), получаем $\varphi_{oq}^{-1} S_{qj} S_{qo}^{-1} \varphi_{oq} = \varphi_{op}^{-1} S_{pj} S_{po}^{-1} \varphi_{op}$ или

$$\varphi_{oq}^{-1} (s_{qj} s_{qo}^{-1}) = \varphi_{op}^{-1} (s_{pj} s_{po}^{-1}) z_{jprq}, \quad (4.17)$$

где $z_{jprq} \in Z(X_o)$ – некоторый элемент из центра группы X_o .

Из равенства (4.17) при $p = o$ получаем

$$s_{qj} = \varphi_{oq} \varphi_{oo}^{-1} (s_{oj}) s_{qo} \varphi_{oq} (z_{joq}). \quad (4.18)$$

Полагая в (4.5) $k = q = j$ и $p = i$, получаем $\varphi_{ij} (s_{ij}) \varphi_{jj} (s_{ji}) = s_{ji}$. Последнее при $j = o$ дает

$$s_{io} = \varphi_{io}^{-1} (s_{oi} \varphi_{oo} (s_{oi}^{-1}) s_{oi}^{-1}). \quad (4.19)$$

Из (4.16) при $k = o$ получаем $\varphi_{io}^{-1} = \varphi_{oi} \varphi_{oo}^{-2} S_{oi}^{-1}$. После этого (4.19) переписывается в виде

$$s_{io} = \varphi_{oi} \varphi_{oo}^{-1} (s_{oi}^{-1}). \quad (4.20)$$

Наконец, из (4.18) с учетом (4.20) получаем

$$s_{qj} = \varphi_{oq} \varphi_{oo}^{-1} (s_{oj} s_{oq}^{-1}) z_{qj}, \quad (4.21)$$

где $z_{qj} \in Z(X_q)$. Из (4.21) и (4.16) получаем (4.1).

Осталось проверить, что $z_{qj} = e_q$, и тогда из (4.21) получим условие (4.2). В силу (4.6) из (4.21) следует, что $z_{oj} = e_o$ и $z_{qq} = e_q$. Подставляя выражения (4.21) и (4.16) в (4.5), получаем $\varphi_{oq}^{-1} (z_{qi} z_{qj}^{-1}) = \varphi_{op}^{-1} (z_{pi} z_{pj}^{-1})$, откуда при $p = o$ следует $z_{qi} = z_{qj} = z_{qq} = e_q$.

Теорема 3 полностью доказана.

В заключение выделим два, в каком-то смысле крайних, случая в теореме 3. Первый охарактеризуем тем, что все элементы матрицы S являются единицами групп X_i , $i \in I$. Во втором случае накладывается требование на матрицу Φ , заключающееся в том, что по диагонали стоят тождественные автоморфизмы групп X_i , $i \in I$, а остальные изоморфизмы матрицы Φ задают структуру декартова произведения $I \times X_o$ на множестве $X = \prod_{i \in I} X_i$.

В первом случае самоинвариантность сводится к равенствам (4.4), означающим коммутативность всех диаграмм

$$\begin{array}{ccc} X_j & \xrightarrow{\varphi_{jp}} & X_p \\ \downarrow \varphi_{jp} & & \downarrow \varphi_{pk} \\ X_q & \xrightarrow{\varphi_{qk}} & X_k. \end{array}$$

Тогда $\varphi_{qk} = \varphi_{ok} \varphi_{oo} \varphi_{oq}^{-1}$ и ${}^k \pi_{x,y} = L_{\varphi_{ok} \varphi_{oo} (\varphi_{oj}^{-1} (y^{-1}) \varphi_{oi}^{-1} (x))}$.

Исходное требование второго случая означает, что $\varphi_{ij} = \varphi_{oj}\varphi_{oi}^{-1}$, $\varphi_{oo} = \text{id}_{X_o}$. Вместо матрицы S можно рассматривать матрицу $C = (c_{ij})$, $c_{ij} \in X_o$, $i, j \in I$, $c_{ij} = \varphi_{oi}^{-1}(s_{ij})$. Из условия (4.1) получаем $s_{oi} = c_{oi} \in Z(X_o)$, а из (4.2) – $c_{ij} = c_{oj}c_{oi}^{-1}$. В этом случае

$${}_{ij}^k\pi_{x,y} = L_{\varphi_{ok}(\varphi_{oj}^{-1}(y^{-1})\varphi_{oi}^{-1}(x)c_{oj}c_{oi}^{-1})}.$$

В результате для элементов декартова произведения $I \times X_o$ получаем

$$\pi_{(i,x),(j,y)}(k,z) = (k, y^{-1}xz c_{oj}c_{oi}^{-1}),$$

где c_{oi} , $i \in I$, – произвольные элементы из центра группы X_o , только $c_{oo} = e_o$.

Список литературы

- [1] А. Г. Курош, *Общая алгебра*, Лекции 1969–1970 учебного года, Наука, М., 1974, 159 с.
- [2] В. Д. Белоусов, *n-арные квазигруппы*, Штиинца, Кишинев, 1972, 227 с.
- [3] А. М. Гальмак, *n-арные группы*, т. 1, ГГУ им. Ф. Скорины, Гомель, 2003, 196 с.
- [4] E. L. Post, “Polyadic groups”, *Trans. Amer. Math. Soc.*, **48:2** (1940), 208–350.
- [5] Л. М. Глускин, “Позиционные оперативы”, *Матем. сб.*, **68(110):3** (1965), 444–472.
- [6] M. Hosszú, “On the explicit form of n -group operations”, *Publ. Math. Debrecen*, **10** (1963), 88–92.
- [7] W. Dörnte, “Untersushungen über einen verallgemeinerten Gruppenbegriff”, *Math. Z.*, **29:1** (1928), 1–19.
- [8] А. М. Гальмак, Г. Н. Воробьев, “О теореме Поста–Глускина–Хоссу”, *ПФМТ*, 2013, № 1(14), 55–60.
- [9] Ф. Н. Сохацкий, “Об ассоциативности многоместных операций”, *Дискрет. матем.*, **4:1** (1992), 66–84.
- [10] Е. И. Соколов, “О теореме Глускина–Хоссу для n -групп Дёрнте”, *Матем. исследования*, **39**, Штиинца, Кишинев, 1976, 187–189.
- [11] А. М. Гальмак, Н. А. Щучкин, “Порождающие множества n -арных групп”, *Чебышевский сб.*, **15:1** (2014), 89–109.
- [12] M. Hosszú, “Algebrai rendszereken értelmezett függvényegyenletek. I”, *Magyar Tud. Akad. Mat. Fiz. Oszt. Kozl.*, **12** (1962), 303–315.
- [13] В. В. Борисенко, “О трансверсалиях распавшихся латинских квадратов четного порядка”, *Матем. вopr. криптогр.*, **5:1** (2014), 5–25.

Фёдор Михайлович Малышев
(Fedor M. Malyshev)

Математический институт им. В. А. Стеклова
Российской академии наук, г. Москва
E-mail: malyshevfm@mi.ras.ru

Поступила в редакцию
11.11.2014 и 20.05.2015