Math-Net.Ru

Общероссийский математический портал

С. В. Полин, Перестановочные решетки отношений эквивалентности на декартовых произведениях и согласованные с ними системы уравнений. I, *Матем. вопр. криптогр.*, 2015, том 6, выпуск 1, 135–158

DOI: <https://doi.org/10.4213/mvk155>

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: 54.157.27.8

26 апреля 2023 г., 16:44:21

УДК 512.57

Перестановочные решетки отношений эквивалентности на декартовых произведениях и согласованные с ними системы уравнений. I

С. В. Полин

Академия криптографии Российской Федерации, г. Москва

Получено 22.IV.2014

Описаны введенные автором ранее GA -решетки и соответствующие им просто решаемые системы уравнений.

Ключевые слова: системы уравнений, решетки отношений

Permutation lattices of equivalence relations on the Cartesian products and systems of equations concordant with these lattices. I

S. V. Polin

Academy of Cryptography of the Russian Federation, Moscow

Abstract. A description of GA -lattices previously introduced by the author is given and easily solved systems of equations concordant with these lattices are presented.

Keywords: systems of equations, lattice of relations

Citation: *Mathematical Aspects of Cryptography*, 2015, vol. 6, no. 1, pp. 135–158 (Russian)

Настоящая работа является завершением цикла работ [9, 10, 11].

В работе [9] был исследован алгоритм решения систем уравнений

$$\begin{cases} f_1(x) = b_1, \\ \dots \\ f_m(x) = b_m \end{cases}$$

методом группирования. Первоначально рассматриваемая система Σ предполагалась произвольной, однако в процессе исследования было установлено, что алгоритм группирования наиболее эффективен в случае, когда под-решетка $\ker \Sigma$ решетки $\mathcal{E}(A)$ отношений эквивалентности множества A , из которого выбираются неизвестные, порожденная всеми отношениями

$$\ker f_i = \langle (a_1, a_2) \in A^2 \mid f_i(a_1) = f_i(a_2) \rangle,$$

является перестановочной¹ решеткой.

Хорошо известно, что для линейных систем Σ уравнений решетка $\ker \Sigma$ всегда перестановочна.

Эти, а также ряд других примеров, позволили выдвинуть гипотезу, состоящую в том, что свойства системы Σ уравнений во многом определяются свойствами решетки $\ker \Sigma$, причем существование эффективных алгоритмов решения более вероятно для систем с перестановочными решетками.

Гипотеза была подтверждена в работе [10], в которой рассматривался вопрос о существовании гауссовоподобных алгоритмов решения систем уравнений. Оказалось, что существование такого алгоритма действительно во многом определяется свойствами решетки $\ker \Sigma$. Там же определены

GA -решетки отношений эквивалентности на множестве $A = \prod_{i=1}^n A_i$ (их определение мы дадим ниже) и показано, что наиболее благоприятным является случай, когда решетка $\ker \Sigma$ содержится в некоторой GA -решетке.

В связи с этим возникает задача описания всех систем Σ уравнений с указанным свойством. Ее решение либо давало бы новый класс легко решаемых систем уравнений, либо еще раз подтверждало, что линейные системы уравнений занимают исключительное положение и что других систем, решаемых столь же эффективно, не существует. Первый исход имел бы практический интерес, а второй, априори более вероятный, имеет теоретическое значение.

Исследование GA -решеток было начато в работе [11], в которой установлены некоторые свойства GA -решеток, открывающие возможность ин-

¹ То есть любые ее два элемента перестановочны [6].

дуктивного построения GA -решеток, при котором вначале строятся решетки для малых значений числа сомножителей n , а затем для больших значений. Настоящая работа посвящена реализации данного подхода. По техническим соображениям она разбита на две части.

В разделе 2 описаны GA -решетки для значений $n = 2$. Таким решеткам соответствуют классы Σ_Ω систем, составленные из уравнений вида $x_1 \circledast x_2 = a$, где операция $\circledast$ выбирается из ортогонального семейства Ω квазигрупповых операций (см. [3]).

Дальнейшая часть работы посвящена описанию GA -решеток для $n \geq 3$. Каждая такая решетка разлагается в прямое произведение неразложимых GA -решеток. Описание последних содержится в разделе 6. Таким решеткам соответствует класс систем уравнений, изотопных линейным системам. Точнее, они состоят из уравнений вида

$$\kappa(c_1\alpha_1(x_1) + c_2\alpha_2(x_2) + \dots + c_n\alpha_n(x_n)) = a,$$

где $\alpha_1, \alpha_2, \dots, \alpha_n$ – фиксированные подстановки, одинаковые для всех уравнений системы, $c_1, c_2, \dots, c_n$ – элементы некоторого поля, κ – подстановка.

Таким образом, можно сделать вывод о том, что алгоритм Гаусса переносится только на системы, мало отличающиеся от линейных. В связи с этим возникает вопрос о существовании модификаций алгоритма, применимых к более широкому классу систем.

1. GA -решетки. Основные определения и свойства

Настоящая работа тесно связана с предыдущей работой [11]. Для того, чтобы она была доступна читателям, не знакомым с этой работой, мы приведем определения введенных в ней объектов и некоторые свойства этих объектов.

Для множества X через $\mathcal{E}(X)$ будем обозначать множество всех отношений эквивалентности на множестве X . Множество $\mathcal{E}(X)$ является решеткой относительно частичного упорядочивания с помощью обычного теоретико-множественного отношения включения. Наибольшим и наименьшим элементами в решетке $\mathcal{E}(X)$ являются отношения $\nabla_X = X^2$ и $\Delta_X = \langle (x, x) \mid x \in X \rangle$.

Отрезком произвольной решетки $\mathbf{M}$ называется каждая подрешетка вида

$$[a, b]_{\mathbf{M}} = \langle c \in \mathbf{M} \mid a \leq c \leq b \rangle,$$

где $a, b \in \mathbf{M}$ и $a \leq b$.

Пусть $h: X \rightarrow Y$ – какое-либо сюръективное отображение. Определим отображение $\zeta_h: E(Y) \rightarrow [\ker h, \nabla_X]_{E(X)}$, положив

$$((x_1, x_2) \in \zeta_h(\theta)) \Leftrightarrow ((h(x_1), h(x_2)) \in \theta).$$

Хорошо известно, что *отображение ζ_h является изоморфизмом решеток.*

В рассматриваемых условиях для произвольной подрешетки $L \subseteq E(X)$ определена подрешетка

$$\zeta_h^{-1}(L) = \langle \theta \in E(Y) \mid \zeta_h(\theta) \in L \rangle$$

решетки $E(Y)$. Если $\ker h \in L$ и $\nabla_X \in L$, то ограничение отображения ζ_h на решетку $\zeta_h^{-1}(L)$ является изоморфизмом решеток $\zeta_h^{-1}(L)$ и $[\ker h, \nabla_X]_L$.

Рассмотрим произвольную решетку M и ее элементы a, b . Говорят, что ее элемент b *покрывает* элемент a , и пишут $a \triangleleft_M b$, если $a < b$ и не существует такого элемента $c \in M$, что $a < c < b$.

Пусть A – множество, разложимое в прямое произведение $A = \prod_{i=1}^n A_i$.

Для каждого подмножества $I \subseteq Z_n = \{1, \dots, n\}$ естественным образом определяется *проекция* $\text{pr}_I: \prod_{i=1}^n A_i \rightarrow A^I = \prod_{i \in I} A_i$. Ее ядро будем обозначать через $\pi_I^{(n)}$. Нетрудно видеть, что

$$((a_1, a_2, \dots, a_n), (b_1, b_2, \dots, b_n) \in \pi_I^{(n)}) \Leftrightarrow (\forall i \in I \ a_i = b_i). \quad (1.1)$$

В частности,

$$\pi_{\emptyset}^{(n)} = \nabla_A, \quad \pi_{Z_n}^{(n)} = \Delta_A. \quad (1.2)$$

Вместо $\pi_{\{j\}}^{(n)}$ будем иногда писать $\pi_j^{(n)}$.

Подрешетку L_A решетки отношений эквивалентности на множестве $A = \prod_{i=1}^n A_i$ назовем *GA-решеткой*, если она удовлетворяет условиям:

- каждое отношение $\pi_i^{(n)}$ принадлежит решетке L_A и является ее коатомом;
- элементы решетки L_A попарно перестановочны (см. [7]).

Следующее утверждение дает пример простейшей GA -решетки.

Лемма 1.1. Множество $\mathbf{D}^{(n)}(A) = \langle \pi_I^{(n)} \mid I \subseteq \{1, \dots, n\} \rangle$ является GA -решеткой отношений эквивалентности на множестве A .

Рассмотрим произвольные подмножества $I, J \subseteq Z_n$. Используя равенство (1.1), получаем

$$\begin{aligned} & \left((a_1, \dots, a_n), (b_1, \dots, b_n) \in \pi_I^{(n)} \wedge \pi_J^{(n)} \right) \Leftrightarrow \\ & \Leftrightarrow \left((a_1, \dots, a_n), (b_1, \dots, b_n) \in \pi_I^{(n)} \right) \& \left((a_1, \dots, a_n), (b_1, \dots, b_n) \in \pi_J^{(n)} \right) \Leftrightarrow \\ & \Leftrightarrow \left(\forall i \in I a_i = b_i \right) \& \left(\forall i \in J a_i = b_i \right) \Leftrightarrow \left(\forall i \in I \cup J a_i = b_i \right). \end{aligned}$$

Таким образом,

$$\pi_I^{(n)} \wedge \pi_J^{(n)} = \pi_{I \cup J}^{(n)}. \quad (1.3)$$

Далее из равенства (1.1) следует, что $\pi_I^{(n)}, \pi_J^{(n)} \subseteq \pi_{I \cap J}^{(n)}$. Поэтому $\pi_I^{(n)} \vee \pi_J^{(n)} \subseteq \pi_{I \cap J}^{(n)}$.

Произвольно выберем пару

$$\left((a_1, a_2, \dots, a_n), (b_1, b_2, \dots, b_n) \right) \in \pi_{I \cap J}^{(n)}.$$

Положим:

$$c_i = \begin{cases} a_i, & i \in I, \\ b_i, & i \notin I. \end{cases}$$

Непосредственно из построений следует, что

$$\left((a_1, a_2, \dots, a_n), (c_1, c_2, \dots, c_n) \right) \in \pi_I^{(n)}.$$

Если $j \in J$, то либо $j \notin I$, и тогда $c_j = b_j$ по построению, либо $j \in I \cap J$, и тогда $c_j = a_j = b_j$. Таким образом,

$$\left((c_1, c_2, \dots, c_n), (b_1, b_2, \dots, b_n) \right) \in \pi_J^{(n)}$$

и

$$\left((a_1, a_2, \dots, a_n), (b_1, b_2, \dots, b_n) \right) \in \pi_I^{(n)} \circ \pi_J^{(n)} \subseteq \pi_I^{(n)} \vee \pi_J^{(n)},$$

т. е.

$$\pi_{I \cap J}^{(n)} \subseteq \pi_I^{(n)} \circ \pi_J^{(n)} \subseteq \pi_I^{(n)} \vee \pi_J^{(n)},$$

что вместе с ранее доказанным неравенством дает

$$\pi_I^{(n)} \circ \pi_J^{(n)} = \pi_I^{(n)} \vee \pi_J^{(n)} = \pi_{I \cap J}^{(n)}. \quad (1.4)$$

Равенства (1.3) и (1.4) показывают, что множество $\mathbf{D}^{(n)}(A)$ является решеткой. Равенства (1.4) также показывают, что отношение $\pi_I^{(n)} \circ \pi_J^{(n)}$ является отношением эквивалентности и, следовательно ([7]), отношения $\pi_I^{(n)}, \pi_J^{(n)}$ перестановочны.

Наконец, из формулы (1.1) следует, что каждое отношение $\pi_i^{(n)}$ является коатомом решетки $\mathbf{D}^{(n)}(A)$. ■

Из формул (1.3) и (1.4) следует, что решетка $\mathbf{D}^{(n)}(A)$ порождается всеми отношениями $\pi_i^{(n)}$ ($i \in Z_n$). Так как каждое такое отношение содержится в любой GA -решетке, то справедливо следующее утверждение.

Лемма 1.2. *Каждая GA -решетка $\mathbf{L}_A$ отношений эквивалентности на множестве $A = \prod_{i=1}^n A_i$ содержит подрешетку $\mathbf{D}^{(n)}(A)$. В частности, отношения Δ_A и ∇_A принадлежат любой GA -решетке решетки $\mathbf{L}_A$.*

Лемма 1.3. *Каждая GA -решетка отношений эквивалентности на множестве $A = \prod_{i=1}^n A_i$ модулярна.*

Утверждение леммы вытекает из теоремы Йенсена [5, с. 258]. ■

Напомним одно из свойств модулярных решеток, которым будем часто пользоваться.

Лемма 1.4. *Пусть $\mathbf{L}$ – модулярная решетка, $a, b \in \mathbf{L}$. Тогда отображения $x \mapsto x \vee b$, $y \mapsto y \wedge a$ являются взаимно обратными изоморфизмами решеток $[a \wedge b, a]_{\mathbf{L}}$ и $[b, a \vee b]_{\mathbf{L}}$. В частности, $a \wedge b \triangleleft_{\mathbf{L}} a$ тогда и только тогда, когда $b \triangleleft_{\mathbf{L}} a \vee b$.*

Доказательство можно найти в любой монографии по теории решеток (например, в [5]).

Следствие 1.1. *Пусть $\mathbf{L}_A$ – GA -решетка отношений эквивалентности на множестве $A = \prod_{i=1}^n A_i$. Тогда для любого подмножества $I \subseteq Z_n$ и любого элемента $k \in I$ справедливо включение $\pi_I^{(n)} \triangleleft_{\mathbf{L}_A} \pi_{I \setminus \{k\}}^{(n)}$.*

Учитывая равенства (1.2), (1.3) и (1.4), находим

$$\begin{aligned}\pi_{I \setminus \{k\}}^{(n)} \vee \pi_k^{(n)} &= \pi_{(I \setminus \{k\}) \cup \{k\}}^{(n)} = \pi_{\emptyset}^{(n)} = \nabla_A, \\ \pi_{I \setminus \{k\}}^{(n)} \wedge \pi_k^{(n)} &= \pi_{(I \setminus \{k\}) \cap \{k\}}^{(n)} = \pi_I^{(n)}.\end{aligned}$$

Так как элемент $\pi_k^{(n)}$ является коатомом, то $\pi_k^{(n)} \triangleleft_{L_A} \pi_{I \setminus \{k\}}^{(n)} \vee \pi_k^{(n)}$. Остается воспользоваться леммами 1.3 и 1.4. ■

Следствие 1.1 показывает, что цепь

$$\Delta_A = \pi_{\{1, \dots, n\}}^{(n)} \subset \pi_{\{2, \dots, n\}}^{(n)} \subset \dots \subset \pi_{\{k, \dots, n\}}^{(n)} \subset \dots \subset \pi_{\emptyset}^{(n)} = \nabla_A$$

максимальна. Все максимальные цепи модулярной решетки L имеют одинаковую длину $\ell + 1$. Величина ℓ называется *длиной* решетки L . Таким образом, справедливо следующее утверждение.

Следствие 1.2. *Длина каждой GA-решетки отношений эквивалентности на множестве $A = \prod_{i=1}^n A_i$ равна n .*

В модулярной решетке L конечной длины для каждого элемента $a \in L$ определена *высота* $\ell(a)$, равная длине отрезка $[0, a]$, где 0 – наименьший элемент решетки L .

Наряду с множествами $A_1, \dots, A_n$ рассмотрим множества $C_1, \dots, C_n$ и их прямое произведение $C = \prod_{i=1}^n C_i$. Допустим, что существует такая подстановка s , что множества $A_{s(i)}$ и C_i равномощны для каждого номера $i \in \{1, \dots, n\}$. Выберем для каждого номера i биекцию $h_i : A_{s(i)} \rightarrow C_i$ и определим отображение $h : A \rightarrow C$, положив

$$h(a_1, a_2, \dots, a_n) = \left(h_1(a_{s(1)}), h_2(a_{s(2)}), \dots, h_n(a_{s(n)}) \right),$$

отображение h также взаимно однозначно. Так как биекция является сюръективным отображением, ядро которого равно Δ_A , то существует подрешетка $\zeta_h^{-1}(L_A) \subseteq E(C)$, изоморфная решетке L_A .

Лемма 1.5. *Подрешетка L_A решетки $E(A)$ является GA-решеткой отношений эквивалентности на множестве $\prod_{i=1}^n A_i$ тогда и только тогда,*

когда подрешетка $\zeta_h^{-1}(\mathbf{L}_A)$ решетки $\mathcal{E}(C)$ является GA -решеткой отношений эквивалентности на множестве $\prod_{i=1}^n C_i$.

Утверждение легко следует из определений. ■

Отображение $\text{pr}_I : \prod_{i=1}^n A_i \rightarrow A^I = \prod_{i \in I} A_i$ сюръективно для каждого подмножества $I \subseteq \{1, \dots, n\}$. В соответствии с ранее введенными определениями оно индуцирует изоморфизм

$$\zeta_{\text{pr}_I} : \mathcal{E}(A^I) \rightarrow [\pi_I^n, \nabla_{A^I}]_{\mathcal{E}(A^I)}$$

решеток, который определяется следующим образом:

$$\begin{aligned} & \left(((a_1, \dots, a_n), (b_1, b_2, \dots, b_n)) \in \zeta_{\text{pr}_{\{i_1, \dots, i_m\}}}(\theta) \right) \Leftrightarrow \\ & \Leftrightarrow \left(((a_{i_1}, \dots, a_{i_m}), (b_{i_1}, \dots, b_{i_m})) \in \theta \right). \end{aligned} \quad (1.5)$$

В дальнейшем для краткости вместо ζ_{pr_I} будем писать ζ_I . Также определена подрешетка $\zeta_I^{-1}(\mathbf{L}_A)$ решетки $\mathcal{E}(A^I)$. Будем обозначать ее $\mathbf{L}_{A^I}$ и называть следом решетки $\mathbf{L}_A$ в решетке $\mathcal{E}(A^I)$.

Теорема 1.1. Пусть $\mathbf{L}_A$ – GA -решетка отношений эквивалентности на множестве $\prod_{i=1}^n A_i$, $\mathbf{L}_{A^I}$ – след решетки $\mathbf{L}_A$ в $\mathcal{E}(A^I)$. Тогда решетка $\mathbf{L}_{A^I}$ является GA -решеткой.

Случай $I = \{1, \dots, n-1\}$ рассмотрен и доказан в работе [11] (следствие 5.2). Случай $I = \{1, \dots, k-1, k+1, \dots, n\}$ сводятся к рассмотренному с помощью леммы 1.5. Общий случай доказывается методом индукции. ■

Рассмотрим множество $A^I \times A^{Z_n \setminus I}$. Решетка $\mathcal{E}(A^I \times A^{Z_n \setminus I})$ содержит в качестве подрешетки изоморфную копию решетки $\mathcal{E}(A^I) \times \mathcal{E}(A^{Z_n \setminus I})$. При этом

$$\left(((\mathbf{a}_I, \mathbf{a}_{Z_n \setminus I}), (\mathbf{b}_I, \mathbf{b}_{Z_n \setminus I})) \in \theta \times \rho \right) \Leftrightarrow ((\mathbf{a}_I, \mathbf{b}_I) \in \theta) \& ((\mathbf{a}_{Z_n \setminus I}, \mathbf{b}_{Z_n \setminus I}) \in \rho).$$

Поэтому решетка $\mathcal{E}(A^I \times A^{Z_n \setminus I})$ содержит в качестве подрешетки изоморфную копию решетки $\mathbf{L}_{A^I} \times \mathbf{L}_{A^{Z_n \setminus I}}$.

Отображению $h: A \rightarrow A^I \times A^{Z_n \setminus I}$, где $h(\mathbf{a}) = (\text{pr}_I(\mathbf{a}), \text{pr}_{Z_n \setminus I}(\mathbf{a}))$, соответствует изоморфизм решеток $\zeta_h: E(A^I \times A^{Z_n \setminus I}) \rightarrow E(A^I)$. Имеем

$$\begin{aligned} & ((x_1, x_2) \in \zeta_h(\theta, \rho)) \Leftrightarrow \\ & \Leftrightarrow ((\text{pr}_I(x_1), \text{pr}_I(x_2)) \in \theta) \& ((\text{pr}_{Z_n \setminus I}(x_1), \text{pr}_{Z_n \setminus I}(x_2)) \in \rho) \Leftrightarrow \\ & \Leftrightarrow ((x_1, x_2) \in \zeta_I(\theta)) \& ((x_1, x_2) \in \zeta_{Z_n \setminus I}(\rho)) \Leftrightarrow ((x_1, x_2) \in \zeta_I(\theta) \wedge \zeta_{Z_n \setminus I}(\theta, \rho)). \end{aligned}$$

Таким образом, отображение $\zeta_I \wedge \zeta_{Z_n \setminus I}: \mathbf{L}_{A^I} \times \mathbf{L}_{A^{Z_n \setminus I}} \rightarrow \mathbf{L}_A$, для которого $\zeta_I \wedge \zeta_{Z_n \setminus I}(\theta, \rho) = \zeta_I(\theta) \wedge \zeta_{Z_n \setminus I}(\rho)$, является мономорфизмом решеток.

Назовем GA -решетку $\mathbf{L}_A$ *разложимой*, если для какого-то непустого собственного подмножества I отображение $\zeta_I \wedge \zeta_{Z_n \setminus I}$ является изоморфизмом решеток, и *неразложимой*, если такого множества не существует.

Ясно, что для описания всех GA -решеток нужно описать все неразложимые GA -решетки.

2. GA -решетки длины 1 и 2

Как мы увидим ниже, разложимость или неразложимость GA -решетки зависит от ее следов длины 2. Поэтому перед рассмотрением общего случая мы изучим решетки малой длины.

Если длина решетки равна 1, то $A = \prod_{i=1}^1 A_i = A_1$. В силу леммы 1.2 отношения $\Delta_{A_1}, \nabla_{A_1}$ принадлежат любой GA -решетке $\mathbf{L}_A$ отношений эквивалентности на множестве A и являются ее наименьшим и наибольшим элементами соответственно. Если бы решетка $\mathbf{L}_A$ содержала элемент $\theta \notin \{\Delta_{A_1}, \nabla_{A_1}\}$, то существовала бы цепь $\Delta_{A_1} \subset \theta \subset \nabla_{A_1}$ длины 3, однако в силу следствия 1.2 решетка имеет длину 1, и цепи длины 3 невозможны. Таким образом, $\mathbf{L}_A = \{\Delta_{A_1}, \nabla_{A_1}\}$.

Теперь исследуем GA -решетку $\mathbf{L}_A$ для случая $A = A_1 \times A_2$. В силу той же леммы 1.2 она содержит подрешетку $\mathbf{D}^{(2)}(A)$, которая в рассматриваемом случае равна множеству $\{\Delta_A, \nabla_{A_1} \times \Delta_{A_2}, \Delta_{A_1} \times \nabla_{A_2}, \nabla_A\}$.

Лемма 2.1. Пусть $\theta \in \mathbf{L}_A \setminus \mathbf{D}^{(2)}(A)$. Тогда существуют такая квазигрупповая операция $\odot$ на множестве A_2 и такое биективное отображе-

ние $f: A_1 \rightarrow A_2$, что отношение θ является ядром отображения $f^\odot(a_1, a_2) = f(a_1) \odot a_2$.

Имеем

$$\Delta_A \subset \theta \subset \nabla_A.$$

Так как решетка $\mathbf{L}_A$ имеет длину 2, то последняя цепочка максимальна, откуда следует, что θ является коатомом решетки $\mathbf{L}_A$.

Теорема 5.2 работы [11] показывает, что имеет место один из трех случаев:

- а) отношение θ равно $\tau \times \nabla_{A_2}$, где τ – коатом GA -решетки $\mathbf{L}_{A_1}$, являющийся следом решетки $\mathbf{L}_A$ в решетке $E(A_1)$;
- б) отношение θ есть ядро проекции $\prod_{i=1}^2 A_i \rightarrow A_2$;
- в) существуют такая квазигрупповая операция $\odot$ на множестве A_2 и такое сюръективное отображение $f: A_1 \rightarrow A_2$, что ядро $\ker f$ является коатомом решетки $\mathbf{L}_{A_1}$, а отношение θ является ядром отображения $f^\odot$.

Из предыдущих рассмотрений следует, что отношение Δ_{A_1} является единственным коатомом решетки $\mathbf{L}_{A_1}$. Поэтому в случае а) имеем $\theta = \Delta_{A_1} \times \nabla_{A_2} = \pi_1^{(2)}$, что противоречит предположениям леммы. В случае б) $\theta = \pi_2^{(2)}$, что опять же противоречит условию леммы.

Поэтому имеет место случай в). Опять же из предыдущих рассмотрений следует, что $\ker f = \Delta_{A_1}$. Значит, отображение f является биекцией, и утверждение леммы верно. ■

Теорема 2.1. Если множества A_1 и A_2 не равномощны, то решетка $\mathbf{D}^{(2)}(A)$ является единственной GA -решеткой отношений эквивалентности на множестве $A_1 \times A_2$.

При сделанном предположении не существует биекций $f: A_1 \rightarrow A_2$, и наше утверждение следует из леммы 2.1. ■

Начиная с этого момента будем считать, что множества A_1 и A_2 равномощны и каждое из них содержит N элементов. Выберем какое-либо множество B , также содержащее N элементов. Лемма 1.5 позволяет перейти

от изучения GA -решеток отношений эквивалентности на множестве A к изучению GA -решеток отношений эквивалентности на множестве B^2 .

Введем некоторые обозначения.

Пусть X – конечное множество. Тогда:

- а) Σ_X – группа подстановок множества X ;
- б) $\mathcal{O}_2(X)$ – множество всех бинарных операций на множестве X ;
- в) $\mathcal{Q}(X)$ – множество всех квазигрупповых операций, определенных на множестве X ;
- г) $\diamond_l, \diamond_r$ – бинарные операции, определенные следующим образом:
 $x_1 \diamond_l x_2 = x_1, \quad x_1 \diamond_r x_2 = x_2$.

Пусть $\kappa \in \Sigma_X$. Определим на множестве $\mathcal{O}_2(X)$ унарную операцию $^\kappa$, положив для $\otimes \in \mathcal{O}_2$

$$x^{\kappa \otimes} y = \kappa(x \otimes y).$$

Ясно, что

$${}^\lambda({}^\kappa \otimes) = ({}^{\lambda \kappa})_{\otimes}. \quad (2.1)$$

Таким образом, множество $\mathcal{O}_2(X)$ вместе с введенными операциями является Σ_X -множеством².

Кроме унарных операций на множестве $\mathcal{O}_2(X)$ можно ввести две нульарных операции, отмечающих операции $\diamond_l, \diamond_r$. Полученная алгебра называется $(\Sigma_X, \diamond)$ -множеством.

В соответствии с общими определениями, подмножество $W \subseteq \mathcal{O}_2(X)$ называется Σ_X -подмножеством, если оно замкнуто относительно всех операций $^\kappa$, и $(\Sigma_X, \diamond)$ -подмножеством, если оно содержит элементы $\diamond_l, \diamond_r$ и является Σ_X -подмножеством. В частности, множество $\mathcal{Q}(X)$ является Σ_X -подмножеством, а множество

$$\mathcal{Q}_\diamond(X) = \mathcal{Q}(X) \cup \langle {}^\kappa \diamond_l \mid \kappa \in \Sigma_X \rangle \cup \langle {}^\kappa \diamond_r \mid \kappa \in \Sigma_X \rangle$$

является $(\Sigma_X, \diamond)$ -подмножеством.

² В литературе наряду с принятым нами термином используются также термины Σ_X -полигон и уноид.

Наименьшее непустое Σ_X -подмножество называется *орбитой действия группы Σ_X* . Орбитой, содержащей операцию $\circledast$, является множество

$$\Sigma_X \circledast = \left\langle {}^\kappa \circledast \mid \kappa \in \Sigma_X \right\rangle.$$

Операции $\circledast, \odot$ назовем *подобными*, если они принадлежат одной орбите. Это эквивалентно тому, что существует такая подстановка κ множества B , что $\odot = {}^\kappa \circledast$.

В ряде случаев полезным является еще одно эквивалентное определение подобия. Чтобы ввести его, заметим, что каждая операция $\circledast \in \mathcal{O}_2(X)$ является отображением $\circledast: X \times X \rightarrow X$. Поэтому на множестве X^2 определено отношение $\ker \circledast$ эквивалентности, для которого

$$\left(((x_1, y_1), (x_2, y_2)) \in \ker \circledast \right) \Leftrightarrow (x_1 \circledast y_1 = x_2 \circledast y_2).$$

Лемма 2.2. *Операции $\circledast \in \mathcal{Q}_\diamond(X)$ и $\odot \in \mathcal{O}_2(X)$ подобны тогда и только тогда, когда $\ker \circledast = \ker \odot$.*

Лемма 2.2 является частным случаем теоремы о гомоморфизме [6]. ■

Базисом Σ_X -подмножества $\Theta \subseteq \mathcal{Q}_\diamond(X)$ назовем такое подмножество $E \subseteq \Theta$, что каждая орбита, содержащаяся в множестве Θ , содержит ровно один элемент из множества E .

Лемма 2.3. *Пусть E – базис Σ_X -подмножества $\Theta \subseteq \mathcal{Q}(X)$. Тогда множество $E_\diamond = E \cup \{\diamond_l, \diamond_r\}$ является базисом Σ_X -подмножества*

$$\Theta_\diamond = \Theta \cup \left\langle {}^\kappa \diamond_l \mid \kappa \in \Sigma_X \right\rangle \cup \left\langle {}^\kappa \diamond_r \mid \kappa \in \Sigma_X \right\rangle. \quad (2.2)$$

Утверждение очевидно.

При выполнении равенства (2.2) каждый базис Σ_X -подмножества $\Theta \subseteq \mathcal{Q}(X)$ будем называть *базисом $(\Sigma_X, \diamond)$ -подмножества $\Theta_\diamond \subseteq \mathcal{Q}_\diamond(X)$* .

Лемма 2.4. *Пусть $\circledast \subseteq \mathcal{Q}_\diamond(B)$. Тогда каждый класс эквивалентности отношения $\ker \circledast$ содержит ровно N элементов.*

Заметим, что классами отношения $\ker \circledast$ являются все непустые подмножества вида

$$[b]_{\circledast} = \left\langle (a_1, a_2) \in B^2 \mid a_1 \circledast a_2 = b \right\rangle.$$

Если $\circledast = {}^{\kappa}\diamond_l$, то

$$[b]_{\circledast} = \left\langle \left(\kappa^{-1}(b), a \right) \in B^2 \mid a \in B \right\rangle.$$

Если $\circledast = {}^{\kappa}\diamond_r$, то

$$[b]_{\circledast} = \left\langle \left(a, \kappa^{-1}(b) \right) \in B^2 \mid a \in B \right\rangle.$$

Наконец, если $\circledast \subseteq \mathcal{Q}(B)$, то

$$[b]_{\circledast} = \left\langle \left(a, a^{-1}\circledast b \right) \mid a \in B \right\rangle,$$

где $a^{-1}\circledast b$ – единственное решение уравнения $a \circledast x = b$.

Во всех трех случаях $\left| [b]_{\circledast} \right| = N$. ■

Следствие 2.1. Пусть $\circledast, \odot \in \mathcal{Q}_{\diamond}(B)$. Тогда либо операции подобны, либо отношения $\ker \circledast, \ker \odot$ не сравнимы.

Допустим, что отношения $\ker \circledast, \ker \odot$ сравнимы, т. е. имеет место по крайней мере одно из включений $\ker \circledast \subseteq \ker \odot$, $\ker \odot \subseteq \ker \circledast$. Для определенности предположим, что выполняется первое неравенство. Второй случай рассматривается аналогично.

Рассмотрим произвольный класс C_1 эквивалентности отношения $\ker \circledast$. При сделанном предположении существует такой класс C_2 эквивалентности отношения $\ker \odot$, что $C_1 \subseteq C_2$. Из леммы 2.4 следует, что классы C_1, C_2 содержат по N элементов и, следовательно, $C_1 = C_2$. Так как класс C_1 выбирался произвольно, то $\ker \circledast = \ker \odot$. Осталось воспользоваться леммой 2.2. ■

Напомним [3], что две операции $\circledast_1, \circledast_2$, определенные на одном и том же конечном множестве X , называются *ортгональными*, если при любых $a, b \in B$ система уравнений

$$\begin{cases} x \circledast_1 y = a, \\ x \circledast_2 y = b \end{cases} \quad (2.3)$$

совместна относительно неизвестных x, y .

Лемма 2.5. Пусть $\circledast \in \mathcal{Q}(B)$. Тогда операции $\diamond_l, \diamond_r, \circledast$ попарно ортгональны.

Утверждение легко доказывается прямой проверкой. ■

Множество $\Theta \subseteq Q_\diamond(B)$ называется *ортгогональным*, если его элементы попарно ортгогональны. Назовем множество $\Theta \subseteq Q_\diamond(B)$ *слабо ортгогональным*, если любые две операции, входящие в множество Θ , либо ортгогональны, либо подобны.

Ортгогональные и слабо ортгогональные множества тесно связаны между собой, поскольку имеет место следующее утверждение.

Лемма 2.6. *Следующие свойства Σ_X -множества $\Theta \subseteq Q_\diamond(B)$ эквивалентны:*

- 1) множество Θ слабо ортгогонально;
- 2) множество Θ обладает ортгогональным базисом;
- 3) любой базис множества Θ ортгогонал.

Пусть множество Θ слабо ортгогонально. Рассмотрим его произвольный базис Ξ и произвольные различные операции, принадлежащие этому базису. По определению базиса они лежат в различных орбитах и, следовательно, не подобны. Поэтому они ортгогональны. Таким образом, базис Ξ ортгогонален и $1 \Rightarrow 3$.

Импликация $3 \Rightarrow 2$ очевидна.

Пусть Ξ – ортгогональный базис множества Θ . Рассмотрим произвольные операции $\odot_1, \odot_2 \in \Theta$. По определению базиса найдутся такие операции $\otimes_1, \otimes_2 \in \Xi$, что операции $\odot_i, \otimes_i$ лежат в одной орбите. Следовательно, найдутся такие подстановки $\kappa_1, \kappa_2 \in \Sigma_B$, что $\odot_i = \kappa_i \otimes_i$.

Если $\otimes_1 = \otimes_2$, то операции $\odot_1, \odot_2$ лежат в одной орбите и, следовательно, подобны.

Пусть $\otimes_1 \neq \otimes_2$. Рассмотрим систему уравнений

$$\begin{cases} x \odot_1 y = a, \\ x \odot_2 y = b. \end{cases}$$

Ее можно записать в виде

$$\begin{cases} \kappa_1(x \otimes_1 y) = a, \\ \kappa_2(x \otimes_2 y) = b, \end{cases}$$

что эквивалентно системе

$$\begin{cases} x \otimes_1 y = \kappa_1^{-1}(a), \\ x \otimes_2 y = \kappa_2^{-1}(b). \end{cases}$$

Так как операции $\otimes_1, \otimes_2$ ортогональны, то последняя система совместна и, следовательно, совместна исходная система, и операции $\odot_1, \odot_2$ ортогональны, т. е. $2 \Rightarrow 1$. ■

Лемма 2.7. Пусть $\otimes_1, \otimes_2 \in \mathcal{Q}_\diamond(B)$, $\theta_i = \ker \otimes_i$. Тогда следующие условия эквивалентны:

- 1) операции $\otimes_1, \otimes_2$ ортогональны;
- 2) выполняется равенство $\theta_1 \circ \theta_2 = \nabla_{B^2}$;
- 3) выполняется равенство $\theta_1 \wedge \theta_2 = \Delta_{B^2}$.

Определим отображение $\Phi: B^2 \rightarrow B^2$, положив

$$\Phi(c, d) = (c \otimes_1 d, c \otimes_2 d).$$

Заметим, что пара (c, d) является решением системы (2.3) уравнений тогда и только тогда, когда $(a, b) \in \Phi(c, d)$. Поэтому операции $\otimes_1, \otimes_2$ ортогональны тогда и только тогда, когда отображение Φ сюръективно.

Далее имеем

$$\begin{aligned} ((c, d), (c', d')) \in \theta_1 \wedge \theta_2 &\Leftrightarrow ((c, d), (c', d')) \in \theta_1 \& ((c, d), (c', d')) \in \theta_2 \Leftrightarrow \\ &\Leftrightarrow ((c \otimes_1 d = c' \otimes_1 d') \& (c \otimes_2 d = c' \otimes_2 d')) \Leftrightarrow (\Phi(c, d) = \Phi(c', d')). \end{aligned}$$

Таким образом, $\theta_1 \wedge \theta_2 = \Delta_{B^2}$ тогда и только тогда, когда отображение Φ инъективно.

Так как множество B^2 конечно, то отображение Φ сюръективно тогда и только тогда, когда оно инъективно. Поэтому условия 1 и 3 эквивалентны.

Установим эквивалентность отношений 1 и 2.

Допустим, что операции $\otimes_1, \otimes_2$ ортогональны. Рассмотрим произвольные пары $(a_1, a_2), (b_1, b_2) \in B^2$. По определению, система уравнений

$$\begin{cases} x \otimes_1 y = a_1 \otimes_1 a_2, \\ x \otimes_2 y = b_1 \otimes_2 b_2 \end{cases}$$

разрешима. Пусть (c, d) – одно из ее решений. Имеем

$$c \otimes_1 d = a_1 \otimes_1 a_2, \quad c \otimes_2 d = b_1 \otimes_2 b_2,$$

откуда следует, что

$$((a_1, a_2), (c, d)) \in \theta_1, \quad ((c, d), (b_1, b_2)) \in \theta_2, \quad (2.4)$$

$$((a_1, a_2), (b_1, b_2)) \in \theta_1 \circ \theta_2$$

и $\theta_1 \circ \theta_2 = \nabla_{B^2}$.

Теперь допустим, что $\theta_1 \circ \theta_2 = \nabla_{B^2}$. Рассмотрим систему уравнений (2.3). Как мы уже отмечали, отображение $\odot: B^2 \rightarrow B$ сюръективно для каждой операции $\odot \in Q_\diamond(B)$. Поэтому существуют такие элементы $a_1, a_2, b_1, b_2 \in B^2$, что $a = a_1 \circledast_1 a_2, b = b_1 \circledast_2 b_2$. По предположению $((a_1, a_2), (b_1, b_2)) \in \theta_1 \circ \theta_2$. Следовательно, существуют такие элементы $c, d \in B$, что справедливы высказывания (2.4). Поэтому

$$c \circledast_1 d = a_1 \circledast_1 a_2 = a,$$

$$c \circledast_2 d = b_1 \circledast_2 b_2 = b.$$

Таким образом, пара (c, d) является решением системы (2.3), и операции $\circledast_1, \circledast_2$ ортогональны. ■

Для подмножества $\Theta \subseteq Q_\diamond(A_2)$ полагаем

$$L_{B^2}(\Theta) = \{\Delta_{B^2}, \nabla_{B^2}\} \cup \langle \ker \circledast \mid \circledast \in \Theta \rangle.$$

Теорема 2.2. Пусть $\Theta \subseteq Q_\diamond(A_2)$. Тогда подмножество $L_{B^2}(\Theta)$ является решеткой в том и только том случае, когда множество Θ слабо ортогонально.

Допустим, что подмножество $L_{B^2}(\Theta)$ является решеткой. Рассмотрим произвольные операции $\circledast_1, \circledast_2 \in \Theta$. Тогда либо

$$\ker \circledast_1 \wedge \ker \circledast_2 = \Delta_{B_2},$$

либо

$$\ker \circledast_1 \wedge \ker \circledast_2 = \ker \circledast_3$$

для некоторой операции $\circledast_3 \in \Theta$. В первом случае операции $\circledast_1, \circledast_2$ ортогональны в силу леммы 2.7. Во втором случае $\ker \circledast_1, \ker \circledast_2 \supseteq \ker \circledast_3$. Применив следствие 2.1, получим, что

$$\ker \circledast_1 = \ker \circledast_3 = \ker \circledast_2,$$

и операции $\circledast_1, \circledast_2$ подобны в силу леммы 2.2.

Теперь допустим, что множество Θ слабо ортогонально. Рассмотрим произвольные отношения $\theta_1, \theta_2 \in \mathbf{L}_{B^2}(\Theta)$ и докажем, что элементы $\theta_1 \vee \theta_2$, $\theta_1 \wedge \theta_2$ принадлежат множеству $\mathbf{L}_{B^2}(\Theta)$. Утверждение очевидно, если хотя бы один из элементов θ_1, θ_2 принадлежит множеству $\{\Delta_{B^2}, \nabla_{B^2}\}$. Например, если $\theta_1 = \nabla_{B^2}$, то $\theta_1 \vee \theta_2 = \nabla_{B^2} \in \mathbf{L}_{B^2}(\Theta)$ и $\theta_1 \wedge \theta_2 = \theta_2 \in \mathbf{L}_{B^2}(\Theta)$.

Осталось рассмотреть случай, когда $\theta_1 = \ker \otimes_1, \theta_2 = \ker \otimes_2$ для операций $\otimes_1, \otimes_2 \in \Theta$. По условию, эти операции либо подобны, либо ортогональны. В первом случае $\theta_1 = \theta_2$ и $\theta_1 \vee \theta_2 = \theta_1 \wedge \theta_2 = \theta_1$. Во втором

$$\theta_1 \vee \theta_2 = \nabla_{B^2} \in \mathbf{L}_{B^2}(\Theta), \quad \theta_1 \wedge \theta_2 = \Delta_{B^2} \in \mathbf{L}_{B^2}(\Theta)$$

в силу леммы 2.7. ■

Теорема 2.3. Следующие свойства подмножества $\mathbf{L}_{B^2} \subseteq \mathcal{E}(B^2)$ эквивалентны:

- 1) $\mathbf{L}_{B^2}$ является GA-решеткой;
- 2) $\mathbf{L}_{B^2} = \mathbf{L}_{B^2}(\Theta_\diamond)$ для слабо ортогонального Σ_B -подмножества $\Theta \subseteq \mathcal{Q}(B)$;
- 3) $\mathbf{L}_{B^2} = \mathbf{L}_{B^2}(E \cup \{\diamond_l, \diamond_r\})$ для ортогонального подмножества $E \subseteq \mathcal{Q}(B)$.

Множество $\Theta_\diamond$ определяется равенством (2.2).

$1 \Rightarrow 2$. Допустим, что подмножество $\mathbf{L}_{B^2} \subseteq \mathcal{E}(B^2)$ является GA-решеткой. Из леммы 2.1 следует, что

$$\mathbf{L}_{B^2} = \{\Delta_{B^2}, \nabla_{B^2}\} \cup \{\pi_1^{(2)}, \pi_2^{(2)}, \ker f_3^{\odot_3}, \ker f_4^{\odot_4}, \dots, \ker f_m^{\odot_m}\}, \quad (2.5)$$

где $f_i: B \rightarrow B$ – взаимно однозначные отображения, $\odot_i \in \mathcal{Q}(B)$.

Положим $\otimes_1 = \diamond_l, \otimes_2 = \diamond_r$ (см. начало раздела 2). Имеем

$$\ker \otimes_1 = \ker \diamond_l = \pi_1^{(2)}, \quad \ker \otimes_2 = \ker \diamond_r = \pi_2^{(2)}. \quad (2.6)$$

Для элементов $b_1, b_2 \in B^2$ положим

$$b_1 \otimes_i b_2 = f_i^{\odot_i}(b_1, b_2) = f_i(b_1) \odot_i b_2.$$

Тем самым определена операция $\otimes_i$ на множестве B . Эта операция изотопна квазигрупповой операции $\odot_i$ и, следовательно, сама является квази-

групповой. Для нее выполняется равенство $\ker f_i^{\odot_i} = \ker \otimes_i$. Отсюда и из равенств (2.5), (2.6) следует, что $\mathbf{L}_{B^2} = \mathbf{L}_{B^2}(\Xi)$, где $\Xi = \{\otimes_1, \dots, \otimes_m\}$.

Положим

$$\Theta = \left\langle {}^{\kappa}\otimes_i \mid i \in \{3, \dots, m\}, \kappa \in \Sigma_B \right\rangle.$$

Из этого определения и (2.2) следует равенство

$$\Theta_{\diamond} = \left\langle {}^{\kappa}\otimes_i \mid i \in \{1, \dots, m\}, \kappa \in \Sigma_B \right\rangle.$$

В силу леммы 2.2 имеем $\ker {}^{\kappa}\otimes_i = \ker \otimes_i$, откуда следует, что

$$\mathbf{L}_{B^2}(\Theta_{\diamond}) = \mathbf{L}_{B^2}(\Xi) = \mathbf{L}_{B^2}.$$

Применив теорему 2.2, получим, что множество $\Theta_{\diamond}$ и, следовательно, множество Θ слабо ортогональны.

2 $\Rightarrow$ 3. Пусть условие 2 выполняется. В качестве E возьмем базис Σ_X -множества Θ . В силу леммы 2.6 базис E ортогонален. В силу леммы 2.3 множество $E_{\diamond} = E \cup \{\diamond_l, \diamond_r\}$ является базисом множества $\Theta_{\diamond}$.

Из определения базиса следует, что

$$\Theta_{\diamond} = \left\langle {}^{\kappa}\otimes \mid \otimes \in E_{\diamond}, \kappa \in \Sigma_B \right\rangle.$$

Теперь так же, как при доказательстве предыдущей импликации, доказываем, что

$$\mathbf{L}_{B^2}(E_{\diamond}) = \mathbf{L}_{B^2}(\Theta_{\diamond}) = \mathbf{L}_{B^2},$$

и условие 3 выполняется.

3 $\Rightarrow$ 2. Пусть условие 3 выполняется. В силу леммы 2.5 множество $E_{\diamond} = E \cup \{\diamond_l, \diamond_r\}$ ортогонально, и из теоремы 2.2 следует, что множество $\mathbf{L}_{B^2} = \mathbf{L}_{B^2}(E_{\diamond})$ является подрешеткой решетки $E(B^2)$. Из формул (2.6) следует, что подрешетка $\mathbf{L}_{B^2}$ удовлетворяет условию п. а) определения GA -решеток, а из леммы 2.7 следует, что эта подрешетка удовлетворяет условию п. б) этого определения. ■

Таким образом, описание GA -решеток длины 2 сводится к описанию ортогональных множеств квазигрупп. Полное описание всех таких множеств является сложной теоретико-квазигрупповой задачей, которая в настоящее время не решена. Тем не менее, были предложены некоторые способы построения систем ортогональных квазигрупп. Их обзор содержится в работе М. М. Глухова [3].

В следующем разделе мы рассмотрим важный для нас пример ортогональных множеств квазигрупп.

3. Слабо ортогональные множества изотопов групп

Пусть $\langle B; + \rangle$ – группа, $\text{Aut} \langle B; + \rangle$ – группа ее автоморфизмов.

Для подстановок $\alpha, \beta \in \Sigma_B$ через ${}_{\alpha+\beta}$ обозначим операцию, определенную следующим образом:

$$a {}_{\alpha+\beta} b = \alpha(a) + \beta(b).$$

В соответствии с построениями предыдущего раздела для каждой подстановки $\kappa \in \Sigma_B$ определена операция ${}^{\kappa}({}_{\alpha+\beta})$, которую мы будем обозначать через ${}^{\kappa}_{\alpha+\beta}$.

Каждая операция ${}^{\kappa}_{\alpha+\beta}$ называется *изотопом операции* $+$. Известно, что все они квазигрупповые.

Если какое-либо из отображений, указанных в обозначении ${}^{\kappa}_{\alpha+\beta}$, равно тождественному отображению 1_B , то в обозначении будем его опускать. Таким образом,

$$a +_{\gamma} b = a + \gamma(b).$$

Подчеркнем, что представление изотопа $\circledast$ в виде $\circledast = {}^{\kappa}_{\alpha+\beta}$ не однозначно. Например, пусть g – автоморфизм группы $\langle B; + \rangle$, $\alpha, \beta, \kappa \in \Sigma_B$; тогда

$$\kappa(g\alpha(x) + \beta(y)) = \kappa g(\alpha(x) + g^{-1}\beta(y)),$$

т. е.

$${}^{\kappa}_{g\alpha+\beta} = {}^{\kappa g}_{\alpha+g^{-1}\beta}. \quad (3.1)$$

Полное описание равенства изотопов дает следующее утверждение

Лемма 3.1. *Операции ${}^{\kappa_1}_{\alpha_1+\beta_1}$, ${}^{\kappa_2}_{\alpha_2+\beta_2}$ совпадают тогда и только тогда, когда существуют такой автоморфизм f группы $\langle B; + \rangle$ и такие элементы $b_1, b_2 \in B$, что*

$$\begin{aligned} \alpha_2(x) &= f\alpha_1(x) + b_1, \\ \beta_2(y) &= -b_1 + f\beta_1(y) + b_2, \\ \kappa_2(z) &= \kappa_1 f^{-1}(z - b_2). \end{aligned} \quad (3.2)$$

Рассматриваемые операции совпадают тогда и только тогда, когда выполняется тождество

$$\kappa_1(\alpha_1(x) + \beta_1(y)) = \kappa_2(\alpha_2(x) + \beta_2(y)).$$

Это тождество можно записать в эквивалентном виде

$$\kappa_2^{-1}\kappa_1(x+y) = \alpha_2\alpha_1^{-1}(x) + \beta_2\beta_1^{-1}(y),$$

т. е. тройка $\langle \kappa_2^{-1}\kappa_1, \alpha_2\alpha_1^{-1}, \beta_2\beta_1^{-1} \rangle$ является автотопией группы $\langle B; + \rangle$. Теперь наше утверждение следует из теоремы 2.6 монографии [1, с. 29]. ■

Следствие 3.1. Пусть операция $\circledast$ является изотопом операции $+$. Тогда существует такое представление $\circledast =_{\alpha}^{\kappa} +_{\beta}$, что $\alpha(0) = \beta(0) = 0$, где 0 – нейтральный элемент группы $\langle B; + \rangle$.

Пусть $\circledast =_{\alpha'}^{\kappa'} +_{\beta'}$. Положим

$$\begin{aligned}\alpha(x) &= \alpha'(x) - \alpha'(0), \\ \beta(y) &= \alpha'(0) + \beta'(y) - (\alpha'(0) + \beta'(0)), \\ \kappa(z) &= \kappa'(z + (\alpha'(0) + \beta'(0))).\end{aligned}$$

Ясно, что $\alpha(0) = 0, \beta(0) = 0$. Равенство $\circledast =_{\alpha}^{\kappa} +_{\beta}$ вытекает из леммы 3.1. ■

Доказанное утверждение позволяет ограничиться рассмотрением только изотопов $_{\alpha}^{\kappa} +_{\beta}$, в которых α, β принадлежат стабилизатору $\Sigma_B^{(0)}$ элемента 0 в группе Σ_B . При этом ограничении условие равенства изотопов несколько упрощается.

Следствие 3.2. Если $\alpha_1, \alpha_2, \beta_1, \beta_2 \in \Sigma_B^{(0)}$, то операции $_{\alpha_1}^{\kappa_1} +_{\beta_1}$, $_{\alpha_2}^{\kappa_2} +_{\beta_2}$ совпадают тогда и только тогда, когда существует такой автоморфизм f группы $\langle B; + \rangle$, что $\alpha_2 = f\alpha_1, \beta_2 = f\beta_1, \kappa_2 = \kappa_1 f^{-1}(z)$.

Легко видеть, что в условиях следствия равенства (3.2) могут выполняться только при $b_1 = b_2 = 0$. ■

Пусть $\alpha, \beta \in \Sigma_B^{(0)}$, $h \in \text{Aut}\langle B; + \rangle$. Полагаем

$$\mathcal{H}(+, \alpha, \beta, \{h\}) = \left\langle {}_{g\alpha}^{\kappa} +_{gh\beta} \mid \kappa \in \Sigma_B, g \in \text{Aut}\langle B; + \rangle \right\rangle.$$

Лемма 3.2. Пусть $\alpha, \beta \in \Sigma_B^{(0)}$. Тогда

- 1) каждое множество $\mathcal{H}(+, \alpha, \beta, \{h\})$ является орбитой действия группы Σ_B ;

2) если $h_1 \neq h_2$, то $\mathcal{H}(+, \alpha, \beta, \{h_1\}) \neq \mathcal{H}(+, \alpha, \beta, \{h_2\})$.

Из равенства (3.1) следует

$${}_{g\alpha}^{\kappa} + {}_{gh\beta} = {}_{\alpha}^{\kappa g} + {}_{h\beta} = {}_{\alpha+h\beta}^{\kappa g},$$

откуда и вытекает первое утверждение.

Пусть $\mathcal{H}(+, \alpha, \beta, \{h_1\}) = \mathcal{H}(+, \alpha, \beta, \{h_2\})$. Тогда операция ${}_{\alpha+h_2\beta}$ принадлежит орбите $\mathcal{H}(+, \alpha, \beta, \{h_1\})$, т. е. ${}_{\alpha+h_2\beta} = {}_{g\alpha}^{\kappa} + {}_{gh_1\beta}$ для подходящих $\kappa \in \Sigma_B$, $g \in \text{Aut}\langle B; + \rangle$. Из следствия 3.2 вытекает, что существует такой автоморфизм f , что $\alpha = f(g\alpha)$, $h_2\beta = f(gh_1\beta)$. Из первого равенства следует, что $f = g^{-1}$. При этом условии второе принимает вид $h_2\beta = h_1\beta$, что невозможно при сделанном предположении. ■

Для подмножества $H \subseteq \text{Aut}\langle B; + \rangle$ полагаем

$$\mathcal{H}(+, \alpha, \beta, H) = \bigcup_{h \in H} \mathcal{H}(+, \alpha, \beta, \{h\}) = \left\langle {}_{g\alpha}^{\kappa} + {}_{gh\beta} \mid \kappa \in \Sigma_B, g \in \text{Aut}\langle B; + \rangle, h \in H \right\rangle.$$

Эквивалентное определение имеет вид

$$\mathcal{H}(+, \alpha, \beta, H) = \left\langle {}_{g\alpha+f\beta}^{\kappa} \mid \kappa \in \Sigma_B, g, f \in \text{Aut}\langle B; + \rangle, g^{-1}f \in H \right\rangle.$$

Вместо $\mathcal{H}(+, \alpha, \beta, \text{Aut}\langle B; + \rangle)$ будем писать $\mathcal{H}(+, \alpha, \beta)$.

Лемма 3.3. Пусть $\alpha, \beta \in \Sigma_B^{(0)}$. Тогда

- 1) подмножество $\Theta \subseteq \mathcal{H}(+, \alpha, \beta)$ является Σ_B -подмножеством тогда и только тогда, когда существует такое подмножество $H \subseteq \text{Aut}\langle B; + \rangle$, что $\Theta = \mathcal{H}(+, \alpha, \beta, H)$;
- 2) одним из базисов Σ_B -множества $\Theta = \mathcal{H}(+, \alpha, \beta, H)$ является множество $E(+, \alpha, \beta, H) = \left\langle {}_{\alpha+h\beta} \mid h \in H \right\rangle$.

Из леммы 3.2 следует, что орбитами множества $\mathcal{H}(+, \alpha, \beta)$ являются все множества вида $\mathcal{H}(+, \alpha, \beta, \{h\})$ и только они.

Хорошо известно, что подмножество множества $\mathcal{H}(+, \alpha, \beta)$ является Σ_B -подмножеством тогда и только тогда, когда оно является объединением нескольких орбит. Отсюда и из определений следует, что $\Theta = \mathcal{H}(+, \alpha, \beta, H)$, где

$$H = \left\langle h \in \text{Aut}\langle B; + \rangle \mid \mathcal{H}(+, \alpha, \beta, \{h\}) \subseteq \Theta \right\rangle.$$

Имеем

$$a +_{h\beta} \in H(+, \alpha, \beta, \{h\}),$$

т. е. множество $E(+, \alpha, \beta, H)$ содержит в точности по одному элементу из каждой орбиты множества $H(+, \alpha, \beta, H)$. ■

Напомним, что автоморфизм $h \in \text{Aut}\langle B; + \rangle$ называется *регулярным* тогда и только тогда, когда $h(a) \neq a$ для всех ненулевых элементов группы $\langle B; + \rangle$ (см. [1]).

В монографии [1, с. 155] доказано следующее утверждение.

Лемма 3.4. *Аutomорфизм $h \in \text{Aut}\langle B; + \rangle$ регулярен тогда и только тогда, когда отображение h' множества B , для которого $h'(x) = x - h(x)$, является подстановкой.*

Лемма 3.5. *Пусть $h_1, h_2 \in \text{Aut}\langle B; + \rangle$. Тогда операции $+_{h_1}$ и $+_{h_2}$ ортогональны в том и только том случае, когда автоморфизм $h_2 h_1^{-1}$ регулярен.*

Рассмотрим систему уравнений

$$\begin{cases} x +_{h_1} y = a, \\ x +_{h_2} y = b. \end{cases} \quad (3.3)$$

Имеем

$$h_2 h_1^{-1}(x +_{h_1} y) - (x +_{h_2} y) = h_2 h_1^{-1}(x) - x.$$

Поэтому уравнение

$$h_2 h_1^{-1}(x) - x = h_2 h_1^{-1}(a) - b \quad (3.4)$$

является следствием системы уравнений (3.3). Таким образом, если система (3.3) совместна, то уравнение (3.4) разрешимо.

Обратно, пусть уравнение (3.4) разрешимо и элемент $c \in B$ является его решением. Тогда положим

$$d = -h_1^{-1}(c) + h_1^{-1}(a).$$

Имеем

$$c +_{h_1} d = c + h_1(-h_1^{-1}(c) + h_1^{-1}(a)) = a,$$

$$\begin{aligned} c +_{h_2} d &= c + h_2(d) = c + h_2(-h_1^{-1}(c) + h_1^{-1}(a)) = c - h_2 h_1^{-1}(c) + h_2 h_1^{-1}(a) = \\ &= -(h_2 h_1^{-1}(c) - c) + h_2 h_1^{-1}(a) = -(h_2 h_1^{-1}(a) - b) + h_2 h_1^{-1}(a) = b, \end{aligned}$$

и система (3.3) разрешима.

Очевидно, что уравнение (3.4) разрешимо при любых значениях a, b тогда и только тогда, когда отображение $x \mapsto h_2 h_1^{-1}(x) - x$ является подстановкой. Остается воспользоваться леммой 3.4. ■

Через $\text{RAut}\langle B; + \rangle$ обозначим подмножество, элементами которого являются все регулярные автоморфизмы группы $\langle B; + \rangle$ и ее тождественный автоморфизм 1_B . Определим на множестве $\text{Aut}\langle B; + \rangle$ отношение ρ , положив

$$((g, f) \in \rho) \Leftrightarrow (g f^{-1} \in \text{RAut}\langle B; + \rangle).$$

Скажем, что подмножество $H \subseteq \text{Aut}\langle B; + \rangle$ является ρ -подмножеством, если $(g, f) \in \rho$ для всех $g, f \in H$.

Теорема 3.1. Пусть $\alpha, \beta \in \Sigma_B^{(0)}$, тогда Σ_B -подмножество $\Theta \subseteq \mathcal{H}(+, \alpha, \beta)$ является слабо ортогональным тогда и только тогда, когда $\Theta = \mathcal{H}(+, \alpha, \beta, H)$ для некоторого ρ -подмножества $H \subseteq \text{Aut}\langle B; + \rangle$.

В соответствии с леммой 3.3 $\Theta = \mathcal{H}(+, \alpha, \beta, H)$ для некоторого множества H . Из лемм 2.6 и 3.3 следует, что множество Θ слабо ортогонально тогда и только тогда, когда базис $E(+, \alpha, \beta, H)$ ортогонален.

Рассмотрим систему уравнений

$$\begin{cases} \alpha(u) +_{h_1} \beta(v) = a, \\ \alpha(u) +_{h_2} \beta(v) = b. \end{cases}$$

С помощью замены $x = \alpha(u)$, $y = \beta(v)$ решение данной системы сводится к решению системы (3.3). Поэтому операции $\alpha +_{h_1 \beta}, \alpha +_{h_2 \beta}$ ортогональны тогда и только тогда, когда ортогональны операции $+_{h_1}, +_{h_2}$.

Теперь из лемм 2.5 и 3.3 следует, что базис $B(H)$ ортогонален тогда и только тогда, когда множество H является ρ -подмножеством. ■

Подгруппа G группы $\text{Aut}\langle B; + \rangle$ называется *регулярной*, если все ее неединичные элементы являются регулярными автоморфизмами.

Следствие 3.3. Если G – регулярная группа автоморфизмов группы $\langle B; + \rangle$ и $h \in \text{Aut} \langle B; + \rangle$, то множество $\mathcal{H}_\phi(+, \alpha, \beta, Gh)$ является слабо ортогональным $(\Sigma_B, \diamond)$ -подмножеством.

Нужно заметить, что в рассматриваемых условиях множество Gh является ρ -подмножеством, и воспользоваться теоремой 3.1. ■

Отметим, что базисами некоторых из указанных в следствии слабо ортогональных множеств являются ортогональные множества, построенные М. М. Глуховым в работе [3].

Список литературы

1. Белоусов В. Д. Основы теории квазигрупп и луп. – М.: Наука, 1967.
2. Белоусов В. Д. Системы квазигрупп с обобщенными тождествами // Успехи матем. наук. – Т. XX. Вып. 1(121). – С. 75–146.
3. Глухов М. М. О методах построения систем ортогональных квазигрупп с использованием групп // Математические вопросы криптографии. – Т. 2. Вып. 4. – М.: 2011. – С. 5–24.
4. Горчинский Ю. Н. О гомоморфизмах многоосновных универсальных алгебр в связи с криптографическими применениями // Труды по дискретной математике. Т. 1. – М.: ТВП, 1977. – С. 67–84.
5. Гретцер Г. Общая теория решеток. – М.: Мир, 1982.
6. Кон П. Универсальная алгебра. – М.: Мир, 1968.
7. Курош А. Г. Лекции по общей алгебре. – М.: Наука, 1973.
8. Мальцев А. И. К общей теории алгебраических систем // Матем. сб. (новая серия). – 1954. – Т. 35(77). – С. 3–20.
9. Полин С. В. Решение уравнений методом последовательного группирования и его оптимизация // Математические вопросы криптографии. – 2012. – Т. 3. Вып. 1. – С. 97–123.
10. Полин С. В. Системы уравнений и решетки конгруэнций универсальных алгебр // Математические вопросы криптографии. – 2013. – Т. 4. Вып. 4. – С. 109–144.
11. Полин С. В. Перестановочные решетки отношений эквивалентности декартовых произведений // Математические вопросы криптографии. – 2014. – Т. 5. Вып. 3. – С. 81–116.
12. Харари Ф. Теория графов. – М.: Мир, 1973.