

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

**С. В. Полин**

*Академия криптографии Российской Федерации, г. Москва*

*Получено 20.IV.2015*

**Аннотация.** 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. II**

**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

Настоящая работа является продолжением [12] и использует введенные в ней обозначения. Нумерация разделов, утверждений и формул продолжает нумерацию указанной работы. Ссылки вида «теорема 1.1», «лемма 2.1», «равенство (3.2)» являются ссылками на соответствующие утверждения и формулы работы [12].

#### 4. Условие неразложимости $GA$ -решеток

Вернемся к рассмотрению общего случая множества  $A = \prod_{i=1}^n A_i$  и  $GA$ -решетки  $\mathbf{L}_A$  отношений эквивалентности на множестве  $A$ .

Для произвольного подмножества  $V \subset Z_n$  через  $V^{\{2\}}$  обозначим множество всех подмножеств множества  $V$ , состоящих из двух различных элементов. Другими словами,  $V^{\{2\}}$  состоит из всех пар  $\{v_1, v_2\}$ , где  $v_1, v_2 \in V$  и  $v_1 \neq v_2$ . При этом пары  $\{v_1, v_2\}$  и  $\{v_2, v_1\}$  считаются одинаковыми.

В соответствии с теоремой 1.1 для всех пар  $\{i_1, i_2\}$  определена  $GA$ -решетка

$$\mathbf{L}_{\{i_1, i_2\}} = \langle \theta \in \mathcal{E}(B^2) \mid \zeta_{\{i_1, i_2\}}(\theta) \in \mathbf{L}_A \rangle$$

отношений эквивалентности на множестве  $A_{\{i_1, i_2\}} = A_{i_1} \times A_{i_2}$ . При этом отображение  $\zeta_{\{i_1, i_2\}}$  осуществляет изоморфизм решетки  $\mathbf{L}_{\{i_1, i_2\}}$  и решетки  $[\pi_{\{i_1, i_2\}}^n, \nabla_A]_{\mathbf{L}_A}$ .

Через  $\mathbf{L}_{\{i_1, i_2\}}^*$  обозначим множество  $\mathbf{L}_{\{i_1, i_2\}} \setminus \mathbf{D}^{(2)}(A_{\{i_1, i_2\}})$ .

**Лемма 4.1.** Пусть  $\theta \in \mathbf{L}_{\{i_1, i_2\}}^*$ . Тогда отношение  $\varphi = \zeta_{\{i_1, i_2\}}(\theta)$  является коатомом решетки  $\mathbf{L}_{B^n}$ .

*Доказательство.* Из формулы (1.5) следует, что  $\zeta_{\{i_1, i_2\}}(\nabla_{A_{\{i_1, i_2\}}}) = \nabla_A$ . Поэтому  $\varphi \neq \nabla_A$ .

Таким образом, если утверждение не верно, то существует такое отношение  $\rho \in \mathbf{L}_A$ , что  $\theta \subset \rho \subset \nabla_A$ . Все три отношения, входящие в эту цепочку, принадлежат решетке  $[\pi_{\{i_1, i_2\}}^n]$ . Поэтому определен элемент  $\zeta_{\{i_1, i_2\}}^{-1}(\rho)$  и имеет место цепочка вложений

$$\Delta_{A_{\{i_1, i_2\}}} \subset \theta \subset \zeta_{\{i_1, i_2\}}^{-1}(\rho) \subset \nabla_{A_{\{i_1, i_2\}}},$$

что противоречит следствию 1.2.  $\square$

В дальнейших рассуждениях нам будет удобно использовать терминологию теории графов. Для этого будем рассматривать каждую пару  $\langle V, \Gamma \rangle$ , где  $V \subseteq Z_n$ ,  $\Gamma \subseteq V^{\{2\}}$ , как граф с множеством  $V$  вершин и множеством  $\Gamma$  ребер, причем ребро  $\{v_1, v_2\}$  инцидентно вершинам  $v_1, v_2$ .

Будем говорить, что ребра графа  $\langle V, \Gamma \rangle$  *помечены*, если каждому ребру  $\{v_1, v_2\} \in \Gamma$  сопоставлено отношение  $\omega_{\{i_1, i_2\}} \in \mathbf{L}_{\{i_1, i_2\}}^*$ . Это эквивалентно тому, что выбран *вектор пометок*  $(\omega_{\{i_1, i_2\}})_{\{i_1, i_2\} \in \Gamma}$ , принадлежащий множеству

$$\Omega \langle V, \Gamma \rangle = \prod_{\{i_1, i_2\} \in \Gamma} \mathbf{L}_{\{i_1, i_2\}}^*.$$

Отметим, что граф  $\langle V, \Gamma \rangle$  нельзя пометить, если для какого-либо ребра  $\{i_1, i_2\} \in \Gamma$  множество  $\mathbf{L}_{\{i_1, i_2\}}^*$  пусто. Это приводит нас к следующему определению.

Граф  $\langle V, \Gamma \rangle$  назовем *допустимым*, если

$$\Gamma \subseteq \Gamma_{\mathbf{L}_A} \stackrel{\text{def}}{=} \langle \{i_1, i_2\} \in Z_n^{\{2\}} \mid \mathbf{L}_{\{i_1, i_2\}}^* \neq \emptyset \rangle.$$

Ясно, что граф можно пометить тогда и только тогда, когда он допустим.

Для вектора пометок

$$\mathbf{w} = (\omega_{\{i_1, i_2\}})_{\{i_1, i_2\} \in \Gamma} \tag{4.1}$$

полагаем

$$T(\mathbf{w}) = \pi_{Z_n \setminus V}^{(n)} \wedge \left( \bigwedge_{\{i_1, i_2\} \in \Gamma} \zeta_{\{i_1, i_2\}}(\omega_{\{i_1, i_2\}}) \right).$$

Если  $\Gamma' \subset \Gamma$ , то существует естественное отображение

$$\Omega \langle S, \Gamma \rangle \rightarrow \Omega \langle S, \Gamma' \rangle,$$

сопоставляющее вектору  $\mathbf{w} \in \Omega \langle S, \Gamma \rangle$  вида (4.1) вектор

$$\mathbf{w}|_{\Gamma'} = (\omega_{\{i_1, i_2\}})_{\{i_1, i_2\} \in \Gamma'}.$$

Согласно определениям

$$\begin{aligned} T(\mathbf{w}) &= \pi_{Z_n \setminus S}^{(n)} \wedge \left( \bigwedge_{\{i_1, i_2\} \in \Gamma \setminus \Gamma'} \zeta_{\{i_1, i_2\}}(\omega_{\{i_1, i_2\}}) \right) \wedge \left( \bigwedge_{\{i_1, i_2\} \in \Gamma'} \zeta_{\{i_1, i_2\}}(\omega_{\{i_1, i_2\}}) \right) = \\ &= T(\mathbf{w}|_{\Gamma'}) \wedge \left( \bigwedge_{\{i_1, i_2\} \in \Gamma \setminus \Gamma'} \zeta_{\{i_1, i_2\}}(\omega_{\{i_1, i_2\}}) \right), \end{aligned} \tag{4.2}$$

откуда следует включение

$$T(\mathbf{w}) \subseteq T(\mathbf{w}|_{\Gamma'}), \tag{4.3}$$

выполняющееся для любого вектора  $\mathbf{w} \in \Omega \langle S, \Gamma \rangle$ .

В ряде случаев неравенство (4.3) может быть уточнено.

**Лемма 4.2.** Пусть  $d = \{u_1, u_2\}$  — такое ребро допустимого графа  $\langle V, \Gamma \rangle$ , что хотя бы одна из вершин  $u_1, u_2$  является висячей. Тогда для любого вектора  $\mathbf{w} \in \Omega \langle V, \Gamma \rangle$  имеет место включение

$$T(\mathbf{w}) \triangleleft_{L_A} T(\mathbf{w}|_{\Gamma \setminus \{d\}}). \quad (4.4)$$

*Доказательство.* Для упрощения обозначений будем считать, что  $d = \{1, 2\}$  и вершина 1 является висячей.

Пусть вектор  $\mathbf{w}$  имеет вид (4.1). В рассматриваемом случае равенство (4.2) приобретает вид

$$T(\mathbf{w}) = T(\mathbf{w}|_{\Gamma \setminus \{d\}}) \wedge \omega_{\{1,2\}}.$$

Согласно леммам 1.3, 1.4 и следствию 1.1 либо имеет место включение (4.4), либо имеет место равенство  $T(\mathbf{w}) = T(\mathbf{w}|_{\Gamma \setminus \{d\}})$ , и нам нужно лишь доказать, что последнее равенство невозможно.

Рассмотрим элементы

$$\mathbf{a} = (a_1, a_2, \dots, a_n), \quad \mathbf{b} = (b, a_2, \dots, a_n),$$

где  $a_i \in A_i$  — произвольные элементы,  $b \neq a_1$ . Так как  $1 \notin V$ , то  $(\mathbf{a}, \mathbf{b}) \in \pi_{Z_n \setminus V}^{(n)}$ . Пусть  $\{i, j\} \in \Gamma \setminus \{d\}$ . Так как 1 — висячая вершина, то  $d$  — единственное ребро, ее содержащее. Поэтому  $1 \notin \{i, j\}$  и  $(\mathbf{a}, \mathbf{b}) \in \pi_{\{i,j\}}^{(n)}$ . Отсюда и из включения  $\pi_{\{i,j\}}^{(n)} \subset \zeta_{\{i,j\}}(\omega_{\{i,j\}})$  следует, что  $(\mathbf{a}, \mathbf{b}) \in \zeta_{\{i,j\}}(\omega_{\{i,j\}})$ . Таким образом,

$$(\mathbf{a}, \mathbf{b}) \in T(\mathbf{w}|_{\Gamma \setminus \{d\}}).$$

Рассмотрим отношение  $\omega_{\{1,2\}} \in \Omega_{\{1,2\}}$ . Из теоремы 2.1 следует, что множества  $A_1, A_2$  равномощны. Применив лемму 2.1, получаем, что существуют биекция  $f: A_1 \rightarrow A_2$  и операция  $\odot \in \mathcal{Q}(A_2)$ , для которых

$$((a_1, a_2), (b_1, b_2)) \in \omega_{\{1,2\}} \Leftrightarrow (f(a_1) \odot a_2 = f(b_1) \odot b_2). \quad (4.5)$$

Из свойств квазигрупповых операций следует, что  $((a_1, a_2), (b, a_2)) \notin \omega_{\{1,2\}}$  для всех таких элементов  $a_1, b \in A_1, a_2 \in A_2$ , что  $b \neq a_1$ . Поэтому  $(\mathbf{a}, \mathbf{b}) \notin \zeta_{\{1,2\}}(\omega_{\{1,2\}})$  и  $(\mathbf{a}, \mathbf{b}) \notin T(\mathbf{w})$ . Следовательно,  $T(\mathbf{w}) \neq T(\mathbf{w}|_{\Gamma \setminus \{d\}})$ .

Лемма доказана.  $\square$

**Лемма 4.3.** Пусть  $\langle V, \Gamma \rangle$  — ациклический допустимый граф. Тогда для любого вектора  $\mathbf{w} \in \Omega \langle V, \Gamma \rangle$  в решетке  $\mathbf{L}_{B^n}$  существует цепь

$$T(\mathbf{w}) = \tau_{n-|V|+|\Gamma|} \triangleleft_{\mathbf{L}_A} \tau_{n-|V|+|\Gamma|-1} \triangleleft_{\mathbf{L}_A} \dots \triangleleft_{\mathbf{L}_A} \tau_1 \triangleleft_{\mathbf{L}_A} \tau_0 = \nabla_A.$$

*Доказательство.* Будем вести доказательство индукцией по величине  $|\Gamma|$ .

Если  $|\Gamma| = 0$ , то  $\Gamma = \emptyset$  и  $\Omega \langle V, \Gamma \rangle$  содержит единственный вектор  $\Lambda$  размерности 0. Для этого вектора  $T(\Lambda) = \pi_{Z_n \setminus V}^{(n)}$ , и утверждение вытекает из следствия 1.2.

Допустим, что утверждение верно для графов, содержащих  $k \geq 0$  ребер, и рассмотрим ациклический граф  $\langle V, \Gamma \rangle$ , содержащий  $k + 1$  ребер. Так как граф  $\langle V, \Gamma \rangle$  ациклический, то его компоненты связности являются деревьями. При сделанном предположении хотя бы одно из них не одноэлементно и, следовательно, содержит висячие вершины (см. [13, гл. 4]). Пусть  $v$  — одна из висячих вершин и  $d \in \Gamma$  — единственное ребро, инцидентное вершине  $v$ .

Очевидно, что граф  $\langle V, \Gamma \setminus \{d\} \rangle$  ациклический и содержит  $k$  ребер. Поэтому применимо предположение индукции и существует цепь

$$T(\mathbf{w}') = \tau_{n-|V|+|\Gamma|-1} \triangleleft_{\mathbf{L}_A} \dots \triangleleft_{\mathbf{L}_A} \tau_1 \triangleleft_{\mathbf{L}_A} \tau_0 = \nabla_A.$$

Объединив эту цепь с включением (4.4), получаем нужную нам цепь.  $\square$

**Теорема 4.1.** Следующие свойства элемента  $\tau$  GA-решетки  $\mathbf{L}_A$  эквивалентны:

1. Существуют такое допустимое дерево  $\langle W, \Gamma \rangle$  и такой вектор пометок  $\mathbf{w} \in \Omega \langle W, \Gamma \rangle$ , что  $\tau = T(\mathbf{w})$ .
2. Отношение  $\tau$  является атомом решетки  $\mathbf{L}_A$ .
3. Отношение  $\tau$  не равно отношению  $\Delta_A$  и существуют такой полный допустимый граф  $\langle V, V^{\{2\}} \rangle$  и такой вектор пометок  $\mathbf{v} \in \Omega \langle V, V^{\{2\}} \rangle$ , что  $\tau \subseteq T(\mathbf{v})$ .

*Доказательство.*  $1 \Rightarrow 2$ . Предположим, что  $\tau = T(\mathbf{w})$  для дерева  $\langle W, \Gamma \rangle$  и вектора  $\mathbf{w} \in \Omega \langle W, \Gamma \rangle$ .

По свойству деревьев граф  $\langle W, \Gamma \rangle$  ациклический и содержит  $|W| - 1$  ребер. Применив лемму 4.3, получаем, что существует цепь

$$\tau = \tau_{n-1} \triangleleft_{\mathbf{L}_A} \tau_{n-2} \triangleleft_{\mathbf{L}_A} \dots \triangleleft_{\mathbf{L}_A} \tau_1 \triangleleft_{\mathbf{L}_A} \tau_0 = \nabla_A. \tag{4.6}$$

Допустим, что отношение  $\tau$  не является атомом. Тогда либо  $\tau = \Delta_A$ , либо существует такой элемент  $\tau' \in \mathbf{L}_A$ , что  $\tau \supset \tau' \supset \Delta_A$ . В первом случае цепь (4.6) является максимальной цепью решетки  $\mathbf{L}_A$  и длина этой решетки равна  $n - 1$ . Во втором существует цепь

$$\nabla_A = \tau_0 \supset \tau_1 \supset \dots \supset \tau_{n-1} = \tau \supset \tau' \supset \Delta_A$$

и длина решетки  $\mathbf{L}_A$  больше или равна  $n + 1$ . Оба случая противоречат следствию 1.2. Таким образом, отношение  $\tau$  является атомом.

2  $\Rightarrow$  3. Предположим, что отношение  $\tau$  является атомом. Положим

$$V = \langle i \in Z_n \mid \tau \not\subseteq \pi_i^{(n)} \rangle.$$

Из определений и равенства (1.3) следует неравенство

$$\tau \subseteq \pi_{Z_n \setminus V}^{(n)}. \quad (4.7)$$

Пусть  $\{i_1, i_2\} \in V^{\{2\}}$ . Рассмотрим элемент  $\tau' = \pi_{\{i_1, i_2\}}^{(n)} \vee \tau$ . Заметим, что

$$\tau' \notin \left\{ \pi_{\{i_1, i_2\}}^{(n)}, \pi_{\{i_1\}}^{(n)}, \pi_{\{i_2\}}^{(n)}, \nabla_A \right\}.$$

Действительно, если  $\tau' = \pi_{\{i_1, i_2\}}^{(n)}$  или  $\tau' = \pi_{\{i_j\}}^{(n)}$ , то  $\tau \subseteq \pi_{i_j}^{(n)}$ , что противоречит определению множества  $V$ . Далее, если  $\tau' = \nabla_A$ , то из леммы 1.4 и следствия 1.1 вытекают включения

$$\pi_{\{i_1, i_2\}}^{(n)} \triangleleft_{\mathbf{L}_A} \pi_{\{i_1\}}^{(n)} \triangleleft_{\mathbf{L}_A} \nabla_A, \quad \pi_{\{i_1, i_2\}}^{(n)} \triangleleft_{\mathbf{L}_A} \nabla_A,$$

что невозможно для модулярных решеток. Теперь имеем

$$\begin{aligned} \zeta_{\{i_1, i_2\}}^{-1}(\tau') &\in \mathbf{L}_{\{i_1, i_2\}} \setminus \zeta_{\{i_1, i_2\}}^{-1} \left( \left\{ \pi_{\{i_1, i_2\}}^{(n)}, \pi_{\{i_1\}}^{(n)}, \pi_{\{i_2\}}^{(n)}, \nabla_A \right\} \right) = \\ &= \mathbf{L}_{\{i_1, i_2\}} \setminus \mathbf{D}^{(2)}(A_{\{i_1, i_2\}}) = \mathbf{L}_{\{i_1, i_2\}}^*. \end{aligned}$$

Последнее включение означает, что  $\mathbf{L}_{\{i_1, i_2\}}^* \neq \emptyset$ . Так как ребро  $\{i_1, i_2\} \in V^{\{2\}}$  выбиралось произвольно, то граф  $\langle V, V^{\{2\}} \rangle$  допустим.

Элемент  $\zeta_{\{i_1, i_2\}}^{-1}(\tau')$  обозначим через  $\varphi_{\{i_1, i_2\}}$ . Имеем

$$\tau \subseteq \pi_{\{i_1, i_2\}}^{(n)} \vee \tau \subseteq \zeta_{\{i_1, i_2\}}(\varphi_{\{i_1, i_2\}}). \quad (4.8)$$

Положим  $\mathbf{v} = (\varphi_{\{i_1, i_2\}})_{\{i_1, i_2\} \in V^{\{2\}}}$ . Из неравенств (4.7) и (4.8) следует неравенство  $\tau \subseteq \mathbf{T}(\mathbf{v})$ , и условие 3 выполняется.

$3 \Rightarrow 1$ . Пусть  $\Delta_A \subset \tau \subseteq T(\mathbf{v})$  для вектора пометок  $\mathbf{v} \in \Omega \langle V, V^{(2)} \rangle$ . Выберем произвольное дерево  $\langle V, \Gamma \rangle$  с множеством  $V$  вершин. Непосредственно из определений следует, что каждый подграф допустимого графа сам является допустимым. Поэтому дерево  $\langle V, \Gamma \rangle$  допустимо. Из неравенства (4.3) следует неравенство

$$\Delta_A \subset \tau \subseteq T(\mathbf{v}) \subseteq T(\mathbf{v}|_\Gamma).$$

Согласно доказанной нами импликации  $1 \Rightarrow 2$  отношение  $T(\mathbf{v}|_\Gamma)$  является атомом решетки  $\mathbf{L}_A$ . Из определения атомов и предыдущих рассуждений следует, что  $\tau = T(\mathbf{v}|_\Gamma)$ .  $\square$

Импликация  $1 \Rightarrow 3$  означает, что для любого допустимого дерева  $\langle W, \Gamma \rangle$  и любого вектора пометок  $\mathbf{w} \in \Omega \langle W, \Gamma \rangle$  найдутся такой допустимый полный граф  $\langle V, V^{(2)} \rangle$  и такой вектор пометок  $\mathbf{v} \in \Omega \langle V, V^{(2)} \rangle$ , что  $T(\mathbf{w}) \subseteq T(\mathbf{v})$ . Нам необходимо усилить это утверждение.

**Теорема 4.2.** Пусть  $\langle W, \Gamma \rangle$  — допустимое дерево. Тогда полный граф  $\langle W, W^{\{2\}} \rangle$  допустим и для каждого вектора  $\mathbf{w} \in \Omega \langle W, \Gamma \rangle$  существует такой вектор  $\mathbf{v} \in \Omega \langle W, W^{\{2\}} \rangle$ , что  $T(\mathbf{w}) = T(\mathbf{v})$  и  $\mathbf{w} = \mathbf{v}|_\Gamma$ .

*Доказательство.* Если  $|W| \leq 2$ , то дерево  $\langle W, \Gamma \rangle$  является полным графом, и утверждение очевидно.

Пусть  $|W| = 3$ . Для упрощения обозначений положим  $W = \{1, 2, 3\}$ ,  $\Gamma = \{\{1, 2\}, \{1, 3\}\}$ . Пусть  $\mathbf{w} = (\omega_{\{1,2\}}, \omega_{\{2,3\}})$  — вектор пометок графа  $\langle W, \Gamma \rangle$ .

В силу теоремы 4.1 отношение  $\tau = T((\omega_{\{1,2\}}, \omega_{\{2,3\}}))$  является атомом. Из той же теоремы следует, что  $\tau \subseteq T(\mathbf{v})$  для подходящего вектора пометок  $\mathbf{v} = (\varphi_{\{i,j\}})_{\{i,j\} \in V^{\{2\}}}$  ребер полного допустимого графа  $\langle V, V^{(2)} \rangle$ .

Справедливы формула (4.5) и аналогичная формула для отношения  $\omega_{\{2,3\}}$ :

$$\begin{aligned} ((a_1, a_2), (b_1, b_2)) \in \omega_{\{1,2\}} &\Leftrightarrow (f(a_1) \odot_{12} a_2 = f(b_1) \odot_{12} b_2), \\ ((a_1, a_2), (b_1, b_2)) \in \omega_{\{2,3\}} &\Leftrightarrow (g(a_1) \odot_{23} a_2 = g(b_1) \odot_{23} b_2), \end{aligned}$$

где  $f: A_1 \rightarrow A_2$ ,  $g: A_2 \rightarrow A_3$  — биекции,  $\odot_{12}$ ,  $\odot_{23}$  — квазигрупповые операции на множествах  $A_2$  и  $A_3$  соответственно.

Выберем произвольно вектор  $\mathbf{a} = (a_1, \dots, a_n) \in A$  и элемент  $b_1 \in A_1 \setminus \{a_1\}$ . В качестве  $b_2$  и  $b_3$  возьмем решения уравнений

$$f(a_1) \odot_{12} a_2 = f(b_1) \odot_{12} x, \quad g(a_2) \odot_{23} a_3 = g(b_2) \odot_{23} y.$$

Теперь из определений следует, что

$$((a_1, a_2, a_3, a_4, \dots, a_n), (b_1, b_2, b_3, a_4, \dots, a_n)) \in \tau,$$

$$((a_1, a_2, a_3, a_4, \dots, a_n), (b_1, b_2, b_3, a_4, \dots, a_n)) \notin \pi_1^{(n)}$$

и  $\tau \not\subseteq \pi_1^{(n)}$ . Следовательно,  $T(\mathbf{v}) \not\subseteq \pi_1^{(n)}$ , что возможно только в случае  $1 \in V$ .

Так же показываем, что  $3 \in V$ .

Поскольку ребра  $\{1, 2\}, \{2, 3\}, \{1, 3\}$  входят в допустимые графы, постольку они принадлежат множеству  $\Gamma_{L_A}$  и полный граф  $\langle \{1, 2, 3\}, \{\{1, 2\}, \{2, 3\}, \{1, 3\}\} \rangle$  допустим. Имеем  $\tau \subseteq T(\mathbf{v}) \subseteq \zeta_{\{1,3\}}(\varphi_{\{1,3\}})$ ,

$$\begin{aligned} \tau &= \tau \wedge \zeta_{\{1,3\}}(\varphi_{\{1,3\}}) = \zeta_{\{1,2\}}(\omega_{\{1,2\}}) \wedge \zeta_{\{2,3\}}(\omega_{\{2,3\}}) \wedge \zeta_{\{1,3\}}(\varphi_{\{1,3\}}) = \\ &= T((\omega_{\{1,2\}}, \omega_{\{2,3\}}, \varphi_{\{1,3\}})), \end{aligned}$$

и утверждение верно.

Пусть теперь  $|W| \geq 4$ . Будем говорить, что вектор пометок  $\mathbf{w}' \in \Omega(W, \Gamma')$ , где  $\Gamma \subseteq \Gamma' \subseteq W^{\{2\}}$ , является продолжением вектора  $\mathbf{w} \in \Omega(W, \Gamma)$ , если  $T(\mathbf{w}) = T(\mathbf{w}')$  и  $\mathbf{w} = \mathbf{w}'|_{\Gamma}$ .

Пусть  $\mathfrak{G}$  — множество таких подмножеств  $\Gamma'$  множества  $W^{\{2\}}$ , что  $\Gamma \subseteq \Gamma'$  и для каждого вектора  $\mathbf{w} \in \Omega(W, \Gamma)$  существует продолжение  $\mathbf{w}' \in \Omega(W, \Gamma')$ .

Ясно, что  $\Gamma \in \mathfrak{G}$ . Поэтому множество  $\mathfrak{G}$  не пусто. Так как множество  $W^{\{2\}}$  конечно, то конечным будет и множество  $\mathfrak{G}$ . Поэтому оно содержит максимальные относительно теоретико-множественного порядка элементы. Пусть  $\Gamma^{(0)}$  — один из таких элементов. Предположим, что  $\Gamma^{(0)} \neq W^{\{2\}}$ .

Так как  $\Gamma \subseteq \Gamma^{(0)}$  и граф  $\langle W, \Gamma \rangle$  связан, то связан и граф  $\langle W, \Gamma^{(0)} \rangle$ . Поэтому при сделанном предположении существуют такие ребра  $\{i_1, i_2\}, \{i_2, i_3\} \in \Gamma^{(0)}$ , что  $i_1 \neq i_3$  и  $\{i_1, i_3\} \notin \Gamma^{(0)}$ .

Рассмотрим произвольный вектор пометок  $\mathbf{w} = (\omega_{\{i,j\}})_{\{i,j\} \in \Gamma}$  и его продолжение  $\mathbf{w}^{(0)} = (\omega_{\{i,j\}})_{\{i,j\} \in \Gamma^{(0)}}$ . Также рассмотрим граф  $\langle \{i_1, i_2, i_3\}, \{\{i_1, i_2\}, \{i_2, i_3\}\} \rangle$ . Тогда пара  $(\omega_{\{i_1, i_2\}}, \omega_{\{i_2, i_3\}})$  является вектором пометок для него. Так как число вершин этого графа равно 3, то доказываемое утверждение для него верно. Это означает, что  $\{i_1, i_3\} \in \Gamma_{L_A}$  и существует такое отношение  $\omega_{\{i_1, i_3\}}$ , что

$$\begin{aligned} \pi_{Z_n \setminus \{i_1, i_2, i_3\}}^{(n)} \wedge \zeta_{\{i_1, i_2\}}(\omega_{\{i_1, i_2\}}) \wedge \zeta_{\{i_2, i_3\}}(\omega_{\{i_2, i_3\}}) = \\ = \pi_{Z_n \setminus \{i_1, i_2, i_3\}}^{(n)} \wedge \zeta_{\{i_1, i_2\}}(\omega_{\{i_1, i_2\}}) \wedge \zeta_{\{i_2, i_3\}}(\omega_{\{i_2, i_3\}}) \wedge \zeta_{\{i_2, i_2\}}(\omega_{\{i_1, i_3\}}). \end{aligned}$$

Отсюда и из леммы 1.4 следует равенство

$$\begin{aligned} & \zeta_{\{i_1, i_2\}}(\omega_{\{i_1, i_2\}}) \wedge \zeta_{\{i_2, i_3\}}(\omega_{\{i_1, i_3\}}) = \\ & = \zeta_{\{i_1, i_2\}}(\omega_{\{i_1, i_2\}}) \wedge \zeta_{\{i_2, i_3\}}(\omega_{\{i_2, i_3\}}) \wedge \zeta_{\{i_1, i_2\}}(\omega_{\{i_1, i_3\}}), \end{aligned}$$

и мы имеем

$$\begin{aligned} & \pi_{Z_n \setminus W}^{(n)} \wedge \left( \bigwedge_{\{i, j\} \in \Gamma^{(0)}} \zeta_{\{i, j\}}(\omega_{\{i, j\}}) \right) \wedge \zeta_{\{i_1, i_3\}}(\omega_{\{i_1, i_3\}}) = \\ & = \pi_{Z_n \setminus W}^{(n)} \wedge \left( \bigwedge_{\{i, j\} \in \Gamma^{(0)}} \zeta_{\{i, j\}}(\omega_{\{i, j\}}) \right) = \pi_{Z_n \setminus W}^{(n)} \wedge \left( \bigwedge_{\{i, j\} \in \Gamma^{(0)}} \zeta_{\{i, j\}}(\omega_{\{i, j\}}) \right). \end{aligned}$$

Таким образом, любой вектор пометок продолжается до вектора пометок, принадлежащего множеству  $\Omega \langle W, \Gamma^{(0)} \cup \{\{i_1, i_3\}\} \rangle$ , что противоречит предположению о максимальности множества  $\Gamma^{(0)}$ .

Полученное противоречие означает, что  $\Gamma^{(0)} = W^{\{2\}}$ , поэтому утверждение теоремы верно.  $\square$

**Следствие 4.1.** *Каждая компонента связности графа  $\langle Z_n, \Gamma_{\mathbf{L}_A} \rangle$  является полным графом.*

Утверждение очевидным образом вытекает из теоремы 4.2.

**Теорема 4.3.** *Каждый элемент GA-решетки  $\mathbf{L}_A$  разлагается в объединение некоторого множества ее атомов.*

*Доказательство.* Пусть  $\theta \in \mathbf{L}_A$ . Если  $\ell(\theta) = 0$ , то  $\theta = \Delta_A$  и  $\theta$  — объединение пустого множества атомов. Если  $\ell(\theta) = 1$ , то  $\theta$  является атомом и утверждение верно.

Допустим, что  $\ell(\theta) = m + 1 \geq 2$  и утверждение верно для всех элементов меньшей высоты. Так как решетка  $\mathbf{L}_A$  конечна, то существует такой атом  $\tau$  решетки  $\mathbf{L}_A$ , что  $\tau \subset \theta$ .

Из равенств (1.2), (1.3) следует соотношение  $\tau \supset \Delta_A = \bigwedge_{k=1}^n \pi_k^{(n)}$ . Поэтому найдется такой номер  $k$ , что  $\tau \not\subseteq \pi_k^{(n)}$ .

Полагаем  $\theta' = \theta \wedge \pi_k^{(n)}$ . Если  $\theta' \subseteq \theta$ , то  $\pi_k^{(n)} \supseteq \theta \wedge \pi_k^{(n)} = \theta' = \theta \supseteq \tau$ , что противоречит выбору номера  $k$ . Значит,  $\theta' \subset \theta$ , откуда следует неравенство  $\ell(\theta') < \ell(\theta)$ . По предположению индукции элемент  $\theta'$  разлагается в объединение атомов  $\theta' = \bigvee_{j=1}^r \tau_j$ .

Из тождества модулярности следует

$$\theta' \vee \tau = \theta \wedge \left( \pi_k^{(n)} \vee \tau \right) = \theta \wedge \nabla_A = \theta, \quad \theta = \theta' \vee \tau = \left( \bigvee_{j=1}^r \tau_j \right) \vee \tau,$$

что дает интересующее нас разложение.  $\square$

**Теорема 4.4.** *GA-решетка  $\mathbf{L}_A$  неразложима тогда и только тогда, когда граф  $\langle Z_n, \Gamma_{\mathbf{L}_A} \rangle$  является полным графом.*

*Доказательство.* Предположим, что решетка  $\mathbf{L}_A$  разложима и отображение  $\zeta_I \wedge \zeta_{Z_n \setminus I}$  является изоморфизмом. Допустим, что существуют такие элементы  $i_1 \in I, i_2 \in Z_n \setminus I$ , что  $\{i_1, i_2\} \in \Gamma_{\mathbf{L}_A}$ . Последнее означает, что множество  $\mathbf{L}_{\{i_1, i_2\}}^*$  не пусто. Пусть  $\omega$  — элемент из множества  $\mathbf{L}_{\{i_1, i_2\}}^*$ . Тогда  $G = \langle \{i_1, i_2\}, \{\{i_1, i_2\}\} \rangle$  — допустимый граф и  $(\omega) \in \Omega(G)$ . Это позволяет построить атом  $\tau = T(\omega) \in \mathbf{L}_A$ .

Для отношения  $\omega$  справедлив аналог формулы (4.5). Используя эту формулу, аналогично доказательству леммы 4.2 показываем, что  $\tau \not\subseteq \pi_I^{(n)}, \tau \not\subseteq \pi_{Z_n \setminus I}^{(n)}$ . Так как отношение  $\tau$  является атомом, то

$$\Delta_A = \tau \wedge \pi_I^{(n)} = \tau \wedge \pi_{Z_n \setminus I}^{(n)}. \quad (4.9)$$

Из сделанного предположения следует, что

$$T(\omega) = \zeta_I(\theta_1) \wedge \zeta_{Z_n \setminus I}(\theta_2)$$

для некоторых отношений  $\theta_1 \in \mathbf{L}_{A^I}, \theta_2 \in \mathbf{L}_{AZ_n \setminus I}$ . Используя равенство (4.9), получаем

$$\pi_I^{(n)} \wedge \pi_{Z_n \setminus I}^{(n)} = \Delta_A = \pi_I^{(n)} \wedge \tau = \pi_I^{(n)} \wedge \zeta_I(\theta_1) \wedge \zeta_{Z_n \setminus I}(\theta_2) = \pi_I^{(n)} \wedge \zeta_{Z_n \setminus I}(\theta_2).$$

Из леммы 1.4 следует, что  $\pi_{Z_n \setminus I}^{(n)} = \zeta_{Z_n \setminus I}(\theta_2)$  и

$$T(\omega) = \zeta_I(\theta_1) \wedge \pi_{Z_n \setminus I}^{(n)} \subseteq \pi_{Z_n \setminus I}^{(n)},$$

что противоречит неравенствам (4.9).

Полученное противоречие показывает, что таких смежных вершин  $i_1, i_2$ , что  $i_1 \in I, i_2 \in Z_n \setminus I$ , не существует, и граф  $\langle Z_n, \Gamma_{\mathbf{L}_A} \rangle$  не связан. Тем более он не является полным.

Теперь предположим, что граф  $\langle Z_n, \Gamma_{\mathbf{L}_A} \rangle$  не полон. В силу следствия 4.1 он не связан. Пусть  $I$  — одна из компонент связности.

Рассмотрим произвольный атом  $\tau$  решетки  $\mathbf{L}_A$ . В силу теоремы 4.1 существуют такое допустимое дерево  $\langle V, \Gamma \rangle$  и такой вектор  $\mathbf{w} \in \Omega \langle V, \Gamma \rangle$ , что  $\tau = T(\mathbf{w})$ . При сделанном предположении либо  $V \subseteq I$ , либо  $V \subseteq Z_n \setminus I$ .

Если  $V \subseteq I$ , то  $\tau \subseteq \pi_{Z_n \setminus I}^{(n)}$ . Отсюда и из тождества модулярности следует, что

$$\left( \tau \vee \pi_I^{(n)} \right) \wedge \pi_{Z_n \setminus I}^{(n)} = \tau \vee \left( \pi_I^{(n)} \wedge \pi_{Z_n \setminus I}^{(n)} \right) = \tau \vee \Delta_A = \tau. \quad (4.10)$$

Так как  $\nabla_A \supseteq \tau \vee \pi_I^{(n)} \supseteq \pi_I^{(n)}$ , то существует такой элемент  $\rho \in \mathbf{L}_{A^I}$ , что  $\tau \vee \pi_I^{(n)} = \zeta_I(\rho)$ . Также имеем  $\pi_{Z_n \setminus I}^{(n)} = \zeta_{Z_n \setminus I}(\Delta_{A_{Z_n \setminus I}})$ . Поэтому равенство (4.10) можно записать в виде

$$\tau = \zeta_I(\rho) \wedge \zeta_{Z_n \setminus I}(\Delta_{A_{Z_n \setminus I}}),$$

т. е.

$$\tau \in \zeta_I(\mathbf{L}_{A^I}) \wedge \zeta_{Z_n \setminus I}(\mathbf{L}_{A_{Z_n \setminus I}}). \quad (4.11)$$

Так же доказываем, что включение (4.11) выполняется и в случае  $V \subseteq Z_n \setminus I$ .

Отсюда и из теоремы 4.3 следует, что  $\mathbf{L}_A = \zeta_I(\mathbf{L}_{A^I}) \wedge \zeta_{Z_n \setminus I}(\mathbf{L}_{A_{Z_n \setminus I}})$ , и решетка  $\mathbf{L}_A$  разложима.  $\square$

**Следствие 4.2.** Если  $A = \prod_{i=1}^n A_i$  и  $GA$ -решетка  $\mathbf{L}_A$  неразложима, то все множества  $A_i$  имеют одинаковую мощность.

*Доказательство.* Пусть  $i, j \in Z_n$  и  $i < j$ . Из теоремы 4.4 следует, что  $GA$ -решетка  $\mathbf{L}_{\{i,j\}}$  отношений эквивалентности на множестве  $A_i \times A_j$  не равна  $\mathbf{D}^{(2)}(A_1 \times A_2)$ . Из теоремы 2.1 следует, что множества  $A_i, A_j$  имеют одинаковую мощность.

Так как номера  $i, j$  выбирались произвольно, то все множества  $A_i$  имеют одинаковую мощность.  $\square$

## 5. I-системы

В настоящем разделе проводятся некоторые рассуждения, которые понадобятся при описании  $GA$ -решеток больших длин. Так же, как выше,  $B$  — конечное множество.

Пусть  $\otimes_1, \otimes_2, \otimes_3 \in \mathcal{Q}(B)$ . Определим на множестве  $B^3$  отношения эквивалентности  $\theta_1, \theta_2, \theta_3$ , положив

$$\begin{aligned} ((b_1, b_2, b_3), (b'_1, b'_2, b'_3) \in \theta_1) &\Leftrightarrow (b_2 \otimes_1 b_3 = b'_2 \otimes_1 b'_3), \\ ((b_1, b_2, b_3), (b'_1, b'_2, b'_3) \in \theta_2) &\Leftrightarrow (b_1 \otimes_2 b_3 = b'_1 \otimes_2 b'_3), \\ ((b_1, b_2, b_3), (b'_1, b'_2, b'_3) \in \theta_3) &\Leftrightarrow (b_1 \otimes_3 b_2 = b'_1 \otimes_3 b'_2). \end{aligned} \quad (5.1)$$

Скажем, что упорядоченная тройка  $(\otimes_1, \otimes_2, \otimes_3)$  инцидентна, если выполняется включение

$$\theta_2 \wedge \theta_3 \subseteq \theta_1. \quad (5.2)$$

**Лемма 5.1.** Пусть тройка  $\langle \otimes_1, \otimes_2, \otimes_3 \rangle$  квазигрупповых операций инцидентна. Тогда операции  $\otimes_1, \otimes_2, \otimes_3$  изотопны некоторой групповой операции  $+$ , определенной на множестве  $B$ , т. е.

$$x \otimes_i y = \kappa_i^{-1} (\lambda_i(x) + \mu_i(y)) \quad (5.3)$$

для подходящих подстановок  $\kappa_i, \lambda_i, \mu_i$ , причем подстановки  $\lambda_i, \mu_i$  могут быть выбраны так, что

$$\lambda_i(0) = \mu_i(0) = 0. \quad (5.4)$$

*Доказательство.* Пусть  $c_2, c_3 \in B$ . Выберем элементы  $b_1, b_2, b_3 \in B$  так, чтобы

$$c_2 = b_1 \otimes_3 b_2, \quad c_3 = b_1 \otimes_2 b_3.$$

Например, это можно сделать следующим образом: элемент  $b_1 \in B$  выбираем произвольно, а в качестве элементов  $b_2, b_3 \in B$  берем решения уравнений  $c_2 = b_1 \otimes_3 y$  и  $c_3 = b_1 \otimes_2 y$  соответственно. Эти уравнения однозначно разрешимы по определению квазигрупп.

Полагаем  $c_2 \odot c_3 = b_2 \otimes_1 b_3$ . Определение этой операции корректно. Действительно, если  $b'_1, b'_2, b'_3 \in B$  — другие элементы и выполняются равенства

$$c_2 = b'_1 \otimes_3 b'_2, \quad c_3 = b'_1 \otimes_2 b'_3,$$

то

$$b_1 \otimes_2 b_3 = b'_1 \otimes_2 b'_3, \quad b_1 \otimes_3 b_2 = b'_1 \otimes_3 b'_2.$$

Из определений (5.1) следует, что справедливо включение

$$((b_1, b_2, b_3), (b'_1, b'_2, b'_3)) \in \theta_2 \wedge \theta_3.$$

Из (5.2) следует, что  $((b_1, b_2, b_3), (b'_1, b'_2, b'_3)) \in \theta_1$  и  $b'_2 \otimes_1 b'_3 = b_2 \otimes_1 b_3 = c_2 \odot c_3$ .

Таким образом, нами определена операция  $\odot$ .

Рассмотрим уравнение  $c_2 \odot x = d$ . Чтобы решить его, опять выберем разложение  $c_2 = b_1 \otimes_3 b_2$ . Пусть  $a$  есть решение уравнения  $b_2 \otimes_1 x = d$ . Тогда

$$c_2 \odot (b_1 \otimes a) = (b_1 \otimes_3 b_2) \odot (b_1 \otimes a) = b_2 \otimes_1 a = d,$$

т. е. рассматриваемое уравнение разрешимо. Однозначность решения вытекает из конечности множества  $B$ .

Так же показываем, что каждое уравнение  $x \odot c_3 = d$  имеет единственное решение.

Таким образом, операция  $\odot$  является квазигрупповой.

Произвольно выберем элементы  $b_1, b_2, b_3 \in B$ . Имеют место тавтологии

$$b_1 \otimes_3 b_2 = b_1 \otimes_3 b_2, \quad b_1 \otimes_2 b_3 = b_1 \otimes_2 b_3.$$

Теперь из определения операции  $\odot$  следует, что

$$(b_1 \otimes_3 b_2) \odot (b_1 \otimes_2 b_3) = b_2 \otimes_1 b_3,$$

т. е. операции  $\otimes_1, \otimes_2, \otimes_3, \odot$  связаны общим тождеством транзитивности.

В [2] доказано, что все операции, входящие в общее тождество транзитивности, изотопны некоторой групповой операции.

Возможность выбора подстановок, обладающих свойством (5.4), вытекает из леммы 3.1.  $\square$

**Теорема 5.1.** Пусть  $\langle B; + \rangle$  — конечная группа,  $\otimes_1, \otimes_2, \otimes_3$  — операции, заданные равенствами (5.3), в которых подстановки  $\lambda_i, \mu_i$  удовлетворяют равенствам (5.4), и тройка  $\langle \otimes_1, \otimes_2, \otimes_3 \rangle$  инцидентна. Тогда существуют такие автоморфизмы  $h, f$  группы  $\langle B; + \rangle$ , что выполняются равенства  $\lambda_3 = (f^{-1}h)\lambda_2$ ,  $\mu_3 = -f\lambda_1$ ,  $\mu_2 = h\mu_1$ .

*Доказательство.* Выберем произвольно элементы  $u, v \in B$ . Для каждого  $a \in B$  полагаем

$$c_{uv}(a) = (a, \mu_3^{-1}(-\lambda_3(a) + u), \mu_2^{-1}(-\lambda_2(a) + v)).$$

Имеем

$$\begin{aligned} \kappa_2^{-1}(\lambda_2(a) + \mu_2(\mu_2^{-1}(-\lambda_2(a) + v))) &= \kappa_2^{-1}(v), \\ \kappa_3^{-1}(\lambda_3(a) + \mu_3(\mu_3^{-1}(-\lambda_3(a) + u))) &= \kappa_3^{-1}(u). \end{aligned}$$

Из этих равенств следует, что каждая пара  $(c_{uv}(a), c_{uv}(a'))$  принадлежит отношению  $\theta_2 \wedge \theta_3$ . Следовательно, каждая такая пара находится в отношении  $\theta_1$ .

В частности,  $(c_{uv}(a), c_{uv}(0)) \in \theta_1$ . Это означает, что выполняется равенство

$$\kappa_1^{-1}(\lambda_1\mu_3^{-1}(-\lambda_3(a) + u) + \mu_1\mu_2^{-1}(-\lambda_2(a) + v)) = \kappa_1^{-1}(\lambda_1\mu_3^{-1}(u) + \mu_1\mu_2^{-1}(v)).$$

Применив к обеим частям равенства подстановку и сгруппировав члены, получим

$$\mu_1\mu_2^{-1}(-\lambda_2(a) + v) - \mu_1\mu_2^{-1}(v) = -\lambda_1\mu_3^{-1}(-\lambda_3(a) + u) + \lambda_1\mu_3^{-1}(u).$$

Левая часть равенства не зависит от величины  $u$ , а правая — от величины  $v$ .

Поэтому обе части равенства не зависят существенно от этих величин и для некоторой функции  $\gamma$

$$\begin{aligned}\mu_1\mu_2^{-1}(-\lambda_2(a) + v) - \mu_1\mu_2^{-1}(v) &= \gamma(a), \\ -\lambda_1\mu_3^{-1}(-\lambda_3(a) + u) + \lambda_1\mu_3^{-1}(u) &= \gamma(a).\end{aligned}$$

Эти равенства можно записать в эквивалентном виде

$$\begin{aligned}\mu_1\mu_2^{-1}(c + v) &= \gamma(-\lambda_2^{-1}(c)) + \mu_1\mu_2^{-1}(v), \\ -\lambda_1\mu_3^{-1}(d + u) &= \gamma(-\lambda_3^{-1}(d)) - \lambda_1\mu_3^{-1}(u).\end{aligned}\tag{5.5}$$

Положив  $u = v = 0$ , получим

$$\mu_1\mu_2^{-1}(c) = \gamma(-\lambda_2^{-1}(c)), \quad -\lambda_1\mu_3^{-1}(d) = \gamma(-\lambda_3^{-1}(d)).\tag{5.6}$$

Подставив последние выражения в равенства (5.5), получим

$$\begin{aligned}\mu_1\mu_2^{-1}(c + v) &= \mu_1\mu_2^{-1}(c) + \mu_1\mu_2^{-1}(v), \\ -\lambda_1\mu_3^{-1}(d + u) &= -\lambda_1\mu_3^{-1}(d) - \lambda_1\mu_3^{-1}(u).\end{aligned}$$

Таким образом, отображения  $\mu_1\mu_2^{-1}$ ,  $-\lambda_1\mu_3^{-1}$  являются автоморфизмами, которые обозначим через  $h$  и  $f$  соответственно.

Из равенств (5.6) следует, что отображение является подстановкой. Поэтому из них же следуют равенства

$$\begin{aligned}\lambda_2^{-1}(c) &= -\gamma^{-1}h(c), \quad \lambda_2(c) = h^{-1}\gamma(-c), \\ \lambda_3^{-1}(d) &= -\gamma^{-1}f(d), \\ \lambda_3(d) &= f^{-1}\gamma(-d) = (f^{-1}h)h^{-1}\gamma(-d) = (f^{-1}h)\lambda_2(d).\end{aligned}$$

□

Пусть  $\Omega_1, \Omega_2, \Omega_3 \subseteq \mathcal{Q}(B)$ . Скажем, что упорядоченная тройка  $\langle \Omega_1, \Omega_2, \Omega_3 \rangle$  образует *I-систему*, если для любой подстановки  $s$  множества  $\{1, 2, 3\}$  и любых операций  $\otimes_{s(1)} \in \Omega_{s(1)}$ ,  $\otimes_{s(2)} \in \Omega_{s(2)}$  найдется такая операция  $\otimes_{s(3)} \in \Omega_{s(3)}$ , что тройка  $\langle \otimes_1, \otimes_2, \otimes_3 \rangle$  инцидентна.

**Лемма 5.2.** Пусть  $\langle \Omega_1, \Omega_2, \Omega_3 \rangle$  — *I-система* и множества  $\Omega_1, \Omega_2, \Omega_3$  не пусты. Тогда существует такая групповая операция  $+$  на множестве  $B$ , что каждая операция из множества  $\Omega_1 \cup \Omega_2 \cup \Omega_3$  изотопна операции  $+$ .

*Доказательство.* Выберем операции  $\otimes_1 \in \Omega_1$ ,  $\otimes_2 \in \Omega_2$ . По определению существует такая операция  $\otimes_3 \in \Omega_3$ , что тройка  $\langle \otimes_1, \otimes_2, \otimes_3 \rangle$  инцидентна. В силу леммы 5.1 существует такая групповая операция  $+$ , что операции  $\otimes_1, \otimes_2, \otimes_3$  ей изотопны.

Выберем еще одну операцию  $\odot_1 \in \Omega_1$ . Опять же по определению существует такая операция  $\odot_3 \in \Omega_3$ , что тройка  $\langle \odot_1, \otimes_2, \odot_3 \rangle$  инцидентна, и в силу леммы 5.1 существует такая групповая операция  $\oplus$ , что операции  $\odot_1, \otimes_2, \odot_3$  ей изотопны.

Таким образом, групповые операции  $+$ ,  $\oplus$  изотопны операции  $\otimes_2$ . Так как отношение изотопии является отношением эквивалентности, то операции  $+$ ,  $\oplus$  изотопны. Следовательно, операции  $+$ ,  $\odot_1$  изотопны операции  $\oplus$ , откуда следует, что операции  $+$ ,  $\odot_1$  изотопны друг другу. Так как операция  $\odot_1 \in \Omega_1$  выбиралась произвольно, то все операции из множества  $\Omega_1$  изотопны операции  $+$ .

Аналогично показываем, что все операции из множеств  $\Omega_2$  и  $\Omega_3$  изотопны операции  $+$ .  $\square$

**Лемма 5.3.** Пусть  $\langle \Omega_1, \Omega_2, \Omega_3 \rangle$  —  $I$ -система, множества  $\Omega_1, \Omega_2, \Omega_3$  не пусты и  $+$  — такая групповая операция на множестве  $B$ , что каждая операция из множества  $\Omega_1 \cup \Omega_2 \cup \Omega_3$  ей изотопна. Тогда существуют такие подстановки  $\alpha_1, \alpha_2, \alpha_3 \in \Sigma_B^{(0)}$ , что

$$\Omega_1 \subseteq \mathcal{H}(+, -\alpha_2, \alpha_3), \quad \Omega_2 \subseteq \mathcal{H}(+, -\alpha_1, \alpha_3), \quad \Omega_3 \subseteq \mathcal{H}(+, -\alpha_1, \alpha_2).$$

*Доказательство.* Выберем произвольно операции  $\otimes_3 \in \Omega_3, \otimes_2 \in \Omega_2$ . В качестве  $\otimes_1$  возьмем такую операцию  $\otimes_1 \in \Omega_1$ , что тройка  $\langle \otimes_1, \otimes_2, \otimes_3 \rangle$  инцидентна. В условиях леммы

$$x \otimes_i y = \kappa_i^{-1}(\lambda_i(x) + \mu_i(y)), \tag{5.7}$$

где  $\lambda_i, \mu_i \in \Sigma_B^{(0)}, \kappa_i \in \Sigma_B$  (см. лемму 3.1).

Применив к тройке  $\langle \otimes_1, \otimes_2, \otimes_3 \rangle$  теорему 5.1, получим, что существуют такие автоморфизмы  $f, h$  группы  $\langle B; + \rangle$ , для которых выполняются равенства

$$\mu_2 = h\mu_1, \quad \lambda_1 = -f^{-1}\mu_3, \quad \lambda_3 = f^{-1}h\lambda_2.$$

Положим

$$\alpha_1 = -\lambda_3, \quad \alpha_2 = \mu_3, \quad \alpha_3 = \mu_2. \tag{5.8}$$

В этих обозначениях имеем

$$\mu_1 = h^{-1}\alpha_3, \quad \lambda_1 = -f^{-1}\alpha_2, \quad \lambda_2 = -h^{-1}f\alpha_1.$$

Выберем еще одну произвольную операцию  $\odot_3 \in \Omega_3$ . Она также представима в виде изотопа

$$x \odot_3 y = \kappa^{-1}(\lambda(x) + \mu(y)).$$

Существуют такие операции  $\odot_1 \in \Omega_1$ ,  $\odot_2 \in \Omega_2$ , что тройки  $\langle \odot_1, \otimes_2, \odot_3 \rangle$ ,  $\langle \otimes_1, \odot_2, \odot_3 \rangle$  инцидентны. Применив к ним теорему 5.1, получим, что существуют автоморфизмы  $g, q$  группы  $\langle B; + \rangle$ , для которых выполняются равенства

$$\mu = -g\lambda_1 = gf^{-1}\alpha_2, \quad \lambda = q\lambda_2 = -qh^{-1}f\alpha_1,$$

т. е.  $\odot_3 \subseteq \mathcal{H}(+, -\alpha_1, \alpha_2)$ . Так как операция  $\odot_3$  выбиралась произвольно, то  $\Omega_3 \subseteq \mathcal{H}(+, -\alpha_1, \alpha_2)$ .

Выбрав произвольно операцию  $\odot_2 \in \Omega_2$  и рассмотрев инцидентные тройки  $\langle \odot_1, \odot_2, \otimes_3 \rangle$ ,  $\langle \otimes_1, \odot_2, \odot_3 \rangle$ , получим, что  $\Omega_2 \subseteq \mathcal{H}(+, -\alpha_1, \alpha_3)$ .

Третье включение доказывается аналогично.  $\square$

**З а м е ч а н и е.** При доказательстве леммы мы указали конструктивный способ построения подстановок  $\alpha_i$ : *выбрать произвольно операции  $\otimes_3 \in \Omega_3$ ,  $\otimes_2 \in \Omega_2$ , рассмотреть одно из их представлений (5.7) в виде изотопы группы и определить подстановки равенствами (5.8).*

В ряде случаев удобно применять другие способы, аналогичные рассмотренному. Например, можно выбрать операции  $\otimes_1 \in \Omega_3$ ,  $\otimes_2 \in \Omega_2$ , рассмотреть представление (5.7) и положить

$$\alpha_1 = -\lambda_2, \quad \alpha_2 = \lambda_1, \quad \alpha_3 = \mu_2$$

или

$$\alpha_1 = -\lambda_2, \quad \alpha_2 = \lambda_1, \quad \alpha_3 = \mu_1.$$

**Лемма 5.4.** Пусть

$$\Omega_1 = \mathcal{H}(+, -\alpha_2, \alpha_3, S_1), \quad \Omega_2 = \mathcal{H}(+, -\alpha_1, \alpha_3, S_2), \quad \Omega_3 = \mathcal{H}(+, -\alpha_1, \alpha_2, S_3)$$

– непустые множества.

Тогда тройка  $\langle \Omega_1, \Omega_2, \Omega_3 \rangle$  является  $I$ -системой в том и только в том случае, когда существуют такая подгруппа  $T \subseteq \text{Aut} \langle B; + \rangle$  и такие элементы  $e_1, e_3 \in \text{Aut} \langle B; + \rangle$ , что  $S_1 = Te_1$ ,  $S_3 = e_3T$ ,  $S_2 = e_3Te_1$ .

**Доказательство.** Рассмотрим произвольные операции  $\otimes_1 \in \Omega_1$ ,  $\otimes_2 \in \Omega_2$ ,  $\otimes_3 \in \Omega_3$ . Учитывая равенство (3.1), их можно представить в виде

$$\begin{aligned} x \otimes_1 y &= \kappa_1^{-1}(-\alpha_2(x) + h_1\alpha_3(y)), \\ x \otimes_2 y &= \kappa_2^{-1}(-\alpha_1(x) + h_2\alpha_3(y)), \\ x \otimes_3 y &= \kappa_3^{-1}(-\alpha_1(x) + h_3\alpha_2(y)), \end{aligned}$$

где  $\kappa_1, \kappa_2, \kappa_3 \in \Sigma_B$ ,  $h_1 \in S_1, h_2 \in S_2, h_3 \in S_3$ .

Теорема 5.1 показывает, что тройка  $\langle \otimes_1, \otimes_2, \otimes_3 \rangle$  инцидентна тогда и только тогда, когда найдутся такие автоморфизмы  $f, q \in \text{Aut} \langle B; + \rangle$ , что выполняются равенства

$$\begin{aligned} h_2 \alpha_3 &= q h_1 \alpha_3, \\ h_3 \alpha_2 &= f \alpha_2, \\ -\alpha_1 &= -f q^{-1} \alpha_1. \end{aligned} \tag{5.9}$$

Легко видеть, что если равенство

$$h_2 = h_3 h_1 \tag{5.10}$$

не выполняется, то система равенств (5.9) не выполняется ни для каких автоморфизмов  $f, q$ . Если равенство (5.10) выполняется, то система равенств (5.9) выполняется при  $q = f = h_3$ .

Таким образом, рассматриваемая тройка  $\langle \otimes_1, \otimes_2, \otimes_3 \rangle$  инцидентна тогда и только тогда, когда выполняется равенство (5.10). Следовательно, тройка  $\langle \Omega_1, \Omega_2, \Omega_3 \rangle$  является  $I$ -системой тогда и только тогда, когда тройка  $\langle S_1, S_2, S_3 \rangle$  удовлетворяет следующему условию: для любой подстановки  $s$  множества  $\{1, 2, 3\}$  и любых элементов  $h_{s(1)} \in S_{s(1)}$ ,  $h_{s(2)} \in S_{s(2)}$  найдется такой элемент  $h_{s(3)} \in S_{s(3)}$ , что выполняется равенство (5.10). Это эквивалентно тому, что выполняются включения

$$S_1 \supseteq S_3^{-1} S_2, \quad S_2 \supseteq S_3 S_1, \quad S_3 \supseteq S_2 S_1^{-1}. \tag{5.11}$$

Легко видеть, что если  $S_1 = T e_1$ ,  $S_3 = e_3 T$ ,  $S_2 = e_3 T e_1$  для некоторой группы  $T$ , то включения (5.11) выполняются и тройка  $\langle \Omega_1, \Omega_2, \Omega_3 \rangle$  является  $I$ -системой.

Допустим, что включения (5.11) выполняются. Выберем произвольно элементы  $e_1 \in S_1$ ,  $e_3 \in S_3$ . Положим  $T = e_3^{-1} S_2 e_1^{-1}$ .

Пусть  $g \in T$ . Тогда  $e_3 g e_1 \in S_2$  и  $e_3 g = (e_3 g e_1) e_1^{-1} \in S_2 S_1^{-1} \subseteq S_3$ , т.е.  $e_3 T \subseteq S_3$ . Обратно пусть  $h \in S_3$ . Тогда  $h e_1 \in S_3 S_1 \subseteq S_2$ ,  $e_3^{-1} h = e_3^{-1} (h e_1) e_1^{-1} \in T$  и  $h = e_3 (e_3^{-1} h) \in e_3 T$ . Таким образом,  $e_3 T = S_3$ .

Аналогично показываем, что  $S_1 = T e_1$ .

Пусть  $g_1, g_3 \in T$ . Тогда произведение  $(e_3 g_3) (g_1 e_1)$  принадлежит множеству  $S_2$  и, следовательно, произведение  $g_3 g_1$  принадлежит множеству  $T$ . Таким образом, множество  $T$  является группой.  $\square$

## 6. $GA$ -решетки длины 3 и более

Исследуем неразложимые  $GA$ -решетки длины 3 и более. Следствие 4.2 и лемма 1.5 показывают, что каждая такая решетка изоморфна  $GA$ -решетке отношений эквивалентности на множестве  $B^n$  для некоторого конечного множества  $B$ .

Рассмотрим множество  $B^n$ , где  $n \geq 3$ , и неразложимую  $GA$ -решетку  $\mathbf{L}_{B^n}$  отношений эквивалентности на множестве  $B^n$ . Будем использовать обозначения, введенные в разделе 4. В частности, там определены  $GA$ -решетки  $\mathbf{L}_{\{i,j\}}$  отношений эквивалентности на множестве  $B^2$ . Из теоремы 2.3 следует, что

$$\mathbf{L}_{\{i,j\}} = \mathbf{L}_{B^2} (\Omega_{\{i,j\}} \cup \{\diamond_r, \diamond_l\})$$

для слабо ортогонального  $\Sigma_B$ -подмножества  $\Omega_{\{i,j\}} \subseteq \mathcal{Q}(B)$ . Из определений следует равенство

$$\mathbf{L}_{\{i,j\}}^* = \langle \ker \otimes \mid \otimes \in \Omega_{\{i,j\}} \rangle.$$

Согласно теореме 4.4 все множества  $\Omega_{\{i,j\}}$  не пусты.

**Следствие 6.1.** Пусть  $i_1 < i_2 < i_3$ . Тогда тройка

$$\langle \Omega_{\{i_2, i_3\}}, \Omega_{\{i_1, i_3\}}, \Omega_{\{i_1, i_2\}} \rangle$$

является  $I$ -системой.

*Доказательство.* Для простоты обозначений будем считать, что  $i_1 = 1$ ,  $i_2 = 2$ ,  $i_3 = 3$ .

Выберем произвольные операции  $\otimes_1 \in \Omega_{\{2,3\}}$ ,  $\otimes_2 \in \Omega_{\{1,3\}}$ . В силу теоремы 4.1 элемент

$$\tau = \pi_{Z_n \setminus \{1,2,3\}}^{(n)} \wedge (\zeta_{\{2,3\}}(\ker \otimes_1) \wedge \zeta_{\{1,3\}}(\ker \otimes_2))$$

является атомом решетки  $\mathbf{L}_{B^n}$ . В силу теоремы 4.2 существует такая операция  $\otimes_3 \in \Omega_{\{1,2\}}$ , что

$$\tau = \pi_{Z_n \setminus \{1,2,3\}}^{(n)} \wedge (\zeta_{\{2,3\}}(\ker \otimes_1) \wedge \zeta_{\{1,3\}}(\ker \otimes_2) \wedge \zeta_{\{1,2\}}(\ker \otimes_3)).$$

Из последнего равенства следует соотношение

$$\tau \subseteq \pi_{Z_n \setminus \{1,2,3\}}^{(n)} \wedge (\zeta_{\{1,3\}}(\ker \otimes_2) \wedge \zeta_{\{1,2\}}(\ker \otimes_3)).$$

Так как обе части неравенства являются атомами, то они равны, значит,

$$\begin{aligned} \pi_{Z_n \setminus \{1,2,3\}}^{(n)} \wedge (\zeta_{\{2,3\}}(\ker \otimes_1) \wedge \zeta_{\{1,3\}}(\ker \otimes_2) \wedge \zeta_{\{1,2\}}(\ker \otimes_3)) &= \\ = \pi_{Z_n \setminus \{1,2,3\}}^{(n)} \wedge (\zeta_{\{1,3\}}(\ker \otimes_2) \wedge \zeta_{\{1,2\}}(\ker \otimes_3)). \end{aligned}$$

Применив лемму 1.4, получим

$$\zeta_{\{2,3\}}(\ker \otimes_1) \wedge \zeta_{\{1,3\}}(\ker \otimes_2) \wedge \zeta_{\{1,2\}}(\ker \otimes_3) = \zeta_{\{1,3\}}(\ker \otimes_2) \wedge \zeta_{\{1,2\}}(\ker \otimes_3),$$

откуда следует, что

$$\zeta_{\{1,3\}}(\ker \otimes_2) \wedge \zeta_{\{1,2\}}(\ker \otimes_3) \subseteq \zeta_{\{2,3\}}(\ker \otimes_1).$$

Сравнив это неравенство с формулами (5.1) и (5.2), получаем, что тройка  $\langle \otimes_1, \otimes_2, \otimes_3 \rangle$  инцидентна.

Аналогично рассматриваются случаи, когда выбраны две другие операции из тройки  $\langle \otimes_1, \otimes_2, \otimes_3 \rangle$ .  $\square$

**Следствие 6.2.** *Все операции из множества  $\bigcup_{1 \leq i < j \leq n} \Omega_{\{i,j\}}$  изотопны некоторой групповой операции.*

*Доказательство.* Применив следствие 6.1 и лемму 5.2 к тройке  $\{1, 2, 3\}$ , получаем, что все операции из множества  $\Omega_{\{1,2\}}$  изотопны некоторой групповой операции  $+$ . Из тех же утверждений, примененных к тройке  $\{1, 2, m\}$  ( $m \geq 3$ ), получаем, что все операции из множества  $\Omega_{\{1,m\}}$  изотопны всем операциям из множества  $\Omega_{\{1,2\}}$ . Так как отношение изотопии является отношением эквивалентности, то все операции из множества  $\Omega_{\{1,m\}}$  изотопны той же операции  $+$ .

Пусть  $1 < i < j$ . Тогда те же утверждения показывают, что все операции из множества  $\Omega_{\{i,j\}}$  изотопны всем операциям из множества  $\Omega_{\{1,i\}}$  и, следовательно, изотопны операции  $+$ .  $\square$

Допустим, что рассматриваемое множество  $B$  является носителем векторного пространства  $\mathbf{B} = \langle B; +, \mathbb{F} \rangle$ ,  $\vec{\alpha} = (\alpha_1, \dots, \alpha_n)$  — семейство подстановок, принадлежащих множеству  $\Sigma_B^{(0)}$ . Через  $\mathcal{F}_{\vec{\alpha}} \langle B; +, \mathbb{F} \rangle$  обозначим множество всех форм  $\sum_{i=1}^n c_i \alpha_i(x_i)$ ,  $c_i \in \mathbb{F}$ , определенных на множестве  $B^n$ . Множество всех отношений, являющихся пересечением какого-либо множества ядер таких форм, обозначим  $\mathcal{L}_{\vec{\alpha}} \langle B; +, \mathbb{F} \rangle$ .

**Теорема 6.1.** *Пусть  $\mathbf{L}_{B^n}$  — неразложимая GA-решетка отношений эквивалентности на множестве  $B^n$  и  $n \geq 3$ . Тогда на множестве  $B$  можно так определить структуру векторного пространства над полем  $\mathbb{F}$ , что  $\mathbf{L}_{B^n} = \mathcal{L}_{\vec{\alpha}} \langle B; +, \mathbb{F} \rangle$  для подходящих подстановок  $\alpha_1, \dots, \alpha_n \in \Sigma_B^{(0)}$ .*

*Доказательство.* В силу следствия 6.2 существует такая групповая операция  $+$  на множестве  $B$ , что все операции из каждого множества  $\Omega_{\{i,j\}}$  ей изотопны.

Произвольно выберем операции  $\otimes_m \in \Omega_{\{1,m\}}$ . В силу выбора операции  $+$  и леммы 3.1 для подходящих подстановок  $\lambda_m, \mu_m \in \Sigma_B^{(0)}$ ,  $\kappa_m \in \Sigma_B$  выполняются равенства  $\kappa_m + \mu_m \in \Omega_{\{1,m\}}$ .

Применив следствие 6.1, леммы 5.3, 3.3 и 5.4 к тройке  $\{1, 2, m\}$ , получим, что

$$\begin{aligned}\Omega_{\{2,m\}} &= \mathcal{H}\left(+, -\alpha_2, \alpha_m, T^{(m)}e_1^{(m)}\right), \\ \Omega_{\{1,m\}} &= \mathcal{H}\left(+, -\alpha_1, \alpha_m, e_3^{(m)}T^{(m)}e_1^{(m)}\right), \\ \Omega_{\{1,2\}} &= \mathcal{H}\left(+, -\alpha_1, \alpha_2, e_3^{(m)}T^{(m)}\right).\end{aligned}\tag{6.1}$$

Здесь  $T^{(m)}$  – подгруппа группы  $\text{Aut}\langle B; + \rangle$ ,  $e_j^{(m)} \in \text{Aut}\langle B; + \rangle$ ,  $\alpha_1 = -\alpha_2$ ,  $\alpha_k = \mu_k$  ( $k \geq 2$ ).

Из определений следует, что  $\kappa_{-\alpha_1 + \alpha_2} \in \mathcal{H}\left(+, -\alpha_1, \alpha_2, e_3^{(m)}T^{(m)}\right)$  тогда и только тогда, когда  $1_B \in e_3^{(m)}T^{(m)}$ , что выполняется тогда и только тогда, когда  $e_3^{(m)} \in T^{(m)}$ . В этом случае  $e_3^{(m)}T^{(m)} = T^{(m)}$  и элемент  $e_3^{(m)}$  можно удалить из формул (6.1).

Теперь

$$\kappa_{-\alpha_1 + \alpha_m} \in \mathcal{H}\left(+, -\alpha_1, \alpha_2, T^{(m)}e_1^{(m)}\right),$$

отсюда так же, как выше, получаем равенство  $T^{(m)}e_1^{(m)} = T^{(m)}$ , поэтому элемент  $e_1^{(m)}$  также можно удалить.

Далее,

$$\mathcal{H}\left(+, -\alpha_1, \alpha_2, T^{(m)}\right) = \mathcal{H}\left(+, -\alpha_1, \alpha_2, T^{(3)}\right).$$

Из определений следует, что последнее равенство выполняется тогда и только тогда, когда  $T^{(m)} = T^{(3)}$  для всех  $m$ . В дальнейшем группу  $T^{(3)}$  будем обозначать через  $T$ , что дает выражение

$$\Omega_{\{1,m\}} = \mathcal{H}\left(+, -\alpha_1, \alpha_m, T\right).$$

Применив те же результаты к тройке  $\{1, i, j\}$ , где  $1 < i < j$ , получим с учетом замечания, приведенного после доказательства леммы 5.3, что

$$\Omega_{\{i,j\}} = \mathcal{H}\left(+, -\alpha_i, \alpha_j, T\right).$$

Пусть  $h_2, h_3 \in T$ . Тогда операция  $\otimes_{1j} = -\alpha_1 + h_j \alpha_j$  принадлежит множеству  $\Omega_{\{1,j\}}$ . Следовательно, каждое отношение  $\ker \otimes_{1j}$  принадлежит решетке  $\mathbf{L}_{\{1,j\}}$ , а отношения

$$\theta_2 = \zeta_{\{1,2\}} (\ker \otimes_{12}) \wedge \pi_3^{(n)}, \quad \theta_3 = \zeta_{\{1,3\}} (\ker \otimes_{13}) \wedge \pi_2^{(n)}$$

принадлежат решетке  $\mathbf{L}_{B^n}$ . Вычислим их объединение  $\rho_{h_2, h_3}$ . Так как отношения  $\theta_2, \theta_3$  перестановочны, то  $\rho_{h_2, h_3} = \theta_2 \circ \theta_3$ , и нам достаточно вычислить произведение рассматриваемых отношений.

Рассмотрим произвольные векторы  $\mathbf{a} = (a_1, \dots, a_n)$ ,  $\mathbf{b} = (b_1, \dots, b_n) \in B^n$ . В соответствии с определением  $(\mathbf{a}, \mathbf{b}) \in \theta_2 \circ \theta_3$  тогда и только тогда, когда существует такой вектор  $\mathbf{x} = (x_1, \dots, x_n)$ , что

$$\begin{cases} -\alpha_1(x_1) + h_2 \alpha_2(x_2) = -\alpha_1(a_1) + h_2 \alpha_2(a_2), \\ x_3 = a_3, \\ -\alpha_1(x_1) + h_3 \alpha_3(x_3) = -\alpha_1(b_1) + h_3 \alpha_3(b_3), \\ x_2 = b_2. \end{cases} \quad (6.2)$$

Другими словами,  $(\mathbf{a}, \mathbf{b}) \in \theta_2 \circ \theta_3$  тогда и только тогда, когда система уравнений (6.2) относительно неизвестных  $x_1, x_2, x_3$  совместна. Нетрудно видеть, что неизвестные  $x_2, x_3$  однозначно определяются, а первое и третье уравнения дают два выражения для неизвестного  $x_1$ . Ясно, что система совместна тогда и только тогда, когда значения этих выражений совпадают, т. е. выполняется равенство

$$-\alpha_1(a_1) + h_2 \alpha_2(a_2) - h_2 \alpha_2(b_2) = -\alpha_1(b_1) + h_3 \alpha_3(b_3) - h_3 \alpha_3(a_3),$$

которое можно записать в эквивалентном виде:

$$h_3 \alpha_3(a_3) - h_3 \alpha_3(b_3) + \alpha_1(b_1) - \alpha_1(a_1) + h_2 \alpha_2(a_2) - h_2 \alpha_2(b_2) = 0. \quad (6.3)$$

Получили явное описание отношения  $\rho_{h_2, h_3} = \theta_2 \vee \theta_3$ : векторы  $(a_1, \dots, a_n)$ ,  $(b_1, \dots, b_n)$  находятся в отношении  $\rho_{h_2, h_3}$  тогда и только тогда, когда выполняется равенство (6.3).

Отношение  $\theta_2 \vee \theta_3$  является отношением эквивалентности. В частности, это означает, что равенство (6.3) выполняется тогда и только тогда, когда выполняется «симметричное» равенство

$$h_3 \alpha_3(b_3) - h_3 \alpha_3(a_3) + \alpha_1(a_1) - \alpha_1(b_1) + h_2 \alpha_2(b_2) - h_2 \alpha_2(a_2) = 0. \quad (6.4)$$

Произвольно выберем элементы  $d_1, d_2 \in B$ . Положим

$$a_1 = \alpha_1^{-1}(d_1), \quad a_2 = (h_2 \alpha_2)^{-1}(-d_2), \quad a_3 = (h_3 \alpha_3)^{-1}(d_2 + d_1), \\ b_1 = b_2 = b_3 = 0.$$

Подставив эти значения в формулу (6.3), получим

$$\begin{aligned} & h_3\alpha_3 \left( (h_3\alpha_3)^{-1} (d_2 + d_1) \right) - h_3\alpha_3 (0) + \alpha_1 (0) - \alpha_1 (\alpha_1^{-1} (d_1)) + \\ & + h_2\alpha_2 \left( (h_2\alpha_2)^{-1} (-d_2) \right) - h_2\alpha_2 (0) = d_2 + d_1 - d_1 - d_2 = 0, \end{aligned}$$

т. е. равенство (6.3) выполняется. Следовательно, для этих значений должно выполняться и равенство (6.4). Таким образом,

$$\begin{aligned} 0 &= h_3\alpha_3 (0) - h_3\alpha_3 \left( (h_3\alpha_3)^{-1} (d_2 + d_1) \right) + \alpha_1 (\alpha_1^{-1} (d_1)) - \alpha_1 (0) + \\ & + h_2\alpha_2 (0) - h_2\alpha_2 \left( (h_2\alpha_2)^{-1} (-d_2) \right) = - (d_2 + d_1) + d_1 + d_2, \end{aligned}$$

и  $d_2 + d_1 = d_1 + d_2$ . Так как элементы  $d_1, d_2$  выбирались произвольно, то группа  $\langle B; + \rangle$  абелева.

Для абелевой группы  $\langle B; + \rangle$  условие (6.3) эквивалентно условию

$$-\alpha_1 (a_1) + h_2\alpha_2 (a_2) + h_3\alpha_3 (a_3) = -\alpha_1 (b_1) + h_2\alpha_2 (b_2) + h_3\alpha_3 (b_3), \quad (6.5)$$

которое и определяет отношение  $\rho_{h_2, h_3}$ .

Пусть  $g \in T$ . Рассмотрим отношение  $\sigma_g = \zeta_{23} (\ker (-\alpha_2 + g\alpha_3))$  и отношение  $\eta = (\rho_{h_2, h_3} \wedge \sigma_g) \vee \pi_{\{1, 2\}}^{(n)}$ . Опять воспользовавшись тем, что решетка  $\mathbf{L}_{B^n}$  перестановочна, получим  $\eta = (\rho_{h_2, h_3} \wedge \sigma_g) \circ \pi_{\{1, 2\}}^{(n)}$ . Поэтому векторы  $\mathbf{a}, \mathbf{b}$  находятся в отношении  $\eta$  тогда и только тогда, когда совместна система уравнений

$$\begin{cases} -\alpha_1 (a_1) + h_2\alpha_2 (a_2) + h_3\alpha_3 (a_3) = -\alpha_1 (x_1) + h_2\alpha_2 (x_2) + h_3\alpha_3 (x_3), \\ -\alpha_2 (a_2) + g\alpha_3 (a_3) = -\alpha_2 (x_2) + g\alpha_3 (x_3), \\ x_1 = b_1, \\ x_2 = b_2. \end{cases}$$

Последние три уравнения однозначно определяют неизвестные значения:

$$\begin{aligned} x_1 &= b_1, \quad x_2 = b_2, \\ x_3 &= \alpha_3^{-1} g^{-1} (\alpha_2 (b) - \alpha_2 (a_2) + g\alpha_3 (a_3)). \end{aligned}$$

Подставив эти значения в первое уравнение, получим цепочку равенств

$$\begin{aligned} & -\alpha_1 (a_1) + h_2\alpha_2 (a_2) + h_3\alpha_3 (a_3) = \\ & = -\alpha_1 (b_1) + h_2\alpha_2 (b_2) + h_3\alpha_3 (\alpha_3^{-1} g^{-1} (\alpha_2 (b) - \alpha_2 (a_2) + g\alpha_3 (a_3))) = \\ & = -\alpha_1 (b_1) + h_2\alpha_2 (b_2) + h_3 g^{-1} \alpha_2 (b) - h_3 g^{-1} \alpha_2 (a_2) + h_3\alpha_3 (a_3), \end{aligned}$$

дающую равенство

$$-\alpha_1 (a_1) + (h_2 + h_3 g^{-1}) \alpha_2 (a_2) = -\alpha_1 (b_1) + (h_2 + h_3 g^{-1}) \alpha_2 (b_2).$$

Отношение  $\zeta_{\{1,2\}}^{-1}(\eta)$  принадлежит решетке  $\mathbf{L}_{\{1,2\}}$ . Поэтому либо  $\zeta_{\{1,2\}}^{-1}(\eta) \in \mathbf{D}^{(2)}(B^2)$ , либо  $\zeta_{\{1,2\}}^{-1}(\eta) \in \mathbf{L}_{\{1,2\}}^*$ . В первом случае отображение  $h_2 + h_3g^{-1}$  является нулевым эндоморфизмом  $O_B$ . Во втором отображение  $h_2 + h_3g^{-1}$  равно некоторому автоморфизму  $f \in T$ .

Так как автоморфизмы  $h_2 + h_3g^{-1}$  выбирались произвольно, то множество  $\mathbb{F} = T \cup \{O_B\}$  замкнуто относительно операции  $+$  и, следовательно, является полем, а множество  $B$  – векторным пространством над этим полем.

Все отношения, входящие в решетку  $\mathcal{L}_{\vec{\alpha}} \langle B; +, \mathbb{F} \rangle$ , перестановочны (см. [8]). Легко проверяется, что и другие свойства, входящие в определение  $GA$ -решеток, также выполняются и  $\mathcal{L}_{\vec{\alpha}} \langle B; +, \mathbb{F} \rangle$  является  $GA$ -решеткой.

Рассмотрим отношение

$$\theta \in \left[ \pi_{\{i,j\}}^{(2)}, \nabla_{B^n} \right]_{\mathcal{E}(B^n)}.$$

Допустим, что  $\theta \in \mathbf{L}_{B^n}$ . Тогда либо  $\theta \in \mathbf{D}^{(n)}(B^n)$ , либо  $\theta \in \Omega_{\{i,j\}}$ . В первом случае  $\theta \in \mathcal{L}_{\vec{\alpha}} \langle B; +, \mathbb{F} \rangle$  в силу леммы 1.2. Во втором отношении  $\theta$  имеет вид  $\zeta_{\{i,j\}}(\ker(\kappa_{-g\alpha_i + gc\alpha_j}))$ . Из равенств (3.1) и (1.5) следует, что отношение  $\theta$  является ядром формы  $(-1_B)(-\alpha_i(x_i) + c\alpha_j(x_j))$ , т. е. оно принадлежит решетке  $\mathcal{L}_{\vec{\alpha}} \langle B; +, \mathbb{F} \rangle$ .

Допустим, что, напротив,  $\theta \in \mathcal{L}_{\vec{\alpha}} \langle B; +, \mathbb{F} \rangle$ . Тогда  $\theta = \ker(\sum_{i=1}^n c_i \alpha_i(x_i))$  для подходящих элементов  $c_1, \dots, c_n \in \mathbb{F}$ . Если хотя бы один из элементов  $c_k$  ( $k \notin \{i, j\}$ ) отличен от  $O_B$ , то неравенство  $\theta \supseteq \pi_{\{i,j\}}^{(n)}$  не выполняется, что противоречит условию. Поэтому все эти элементы равны 0.

Если  $c_i = 0$  или  $c_j = 0$ , то  $\theta \in \mathbf{D}^{(n)}(B^n)$  и  $\theta \in \mathbf{L}_{B^n}$ .

Осталось рассмотреть случай, когда  $c_i, c_j \neq 0$ . Имеем

$$c_i \alpha_i(x_i) + c_j \alpha_j(x_j) = x_i \left( \begin{matrix} -c_i \\ -\alpha_i + (-c_i^{-1}c_j)\alpha_j \end{matrix} \right) x_j,$$

откуда следует, что

$$\theta = \zeta_{\{i,j\}} \left( \ker \left( \begin{matrix} -c_i \\ -\alpha_i + (-c_i^{-1}c_j)\alpha_j \end{matrix} \right) \right),$$

и опять же  $\theta \in \mathbf{L}_{B^n}$ .

Таким образом, следы решеток  $\mathbf{L}_{B^n}$  и  $\mathcal{L}_{\vec{\alpha}} \langle B; +, \mathbb{F} \rangle$  в каждом из множеств  $B_i \times B_j$ , где  $B_i, B_j$  – копии множества  $B$ , одинаковы. Результаты раздела 4 показывают, что множество таких следов однозначно определяет  $GA$ -решетку. Поэтому  $\mathbf{L}_{B^n} = \mathcal{L}_{\vec{\alpha}} \langle B; +, \mathbb{F} \rangle$ .  $\square$

## Список литературы

- [1] Белоусов В. Д., *Основы теории квазигрупп и луп*, М.: Наука, 1967, 224 с.
- [2] Белоусов В. Д., “Системы квазигрупп с обобщенными тождествами”, *Успехи матем. наук*, **XX**:1 (121), 75–146.
- [3] Глухов М. М., “О методах построения систем ортогональных квазигрупп с использованием групп”, *Математические вопросы криптографии*, **2**:4 (2011), 5–24.
- [4] Горчинский Ю. Н., “О гомоморфизмах многоосновных универсальных алгебр в связи с криптографическими применениями”, *Труды по дискретной математике*, **1**, М.: Научное изд-во ТВП, 1997, 67–84.
- [5] Гретцер Г., *Общая теория решеток*, М.: Мир, 1982, 456 с.
- [6] Кон П., *Универсальная алгебра*, М.: Мир, 1968, 359 с.
- [7] Курош А. Г., *Лекции по общей алгебре*, М.: Наука, 1973, 40 с.
- [8] Мальцев А. И., “К общей теории алгебраических систем”, *Матем. сб. (новая серия)*, **35(77)**:1 (1954), 3–20.
- [9] Полин С. В., “Решение уравнений методом последовательного группирования и его оптимизация”, *Математические вопросы криптографии*, **3**:1 (2012), 97–123.
- [10] Полин С. В., “Системы уравнений и решетки конгруэнций универсальных алгебр”, *Математические вопросы криптографии*, **4**:4 (2013), 109–144.
- [11] Полин С. В., “Перестановочные решетки отношений эквивалентности декартовых произведений”, *Математические вопросы криптографии*, **5**:3 (2014), 81–116.
- [12] Полин С. В., “Перестановочные решетки отношений эквивалентности на декартовых произведениях и согласованные с ними системы уравнений. I”, *Математические вопросы криптографии*, **6**:1 (2015), 135–158.
- [13] Харари Ф., *Теория графов*, М.: Мир, 1973, 300 с.