Math-Net.Ru

Общероссийский математический портал

С. В. Полин, Перестановочные решетки отношений эквивалентности декартовых произведений, *Матем. вопр. криптогр.*, 2014, том 5, выпуск 3, 81–116

DOI: <https://doi.org/10.4213/mvk130>

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: 54.162.127.20

26 апреля 2023 г., 15:13:04

**Перестановочные решетки отношений
эквивалентности декартовых произведений**

С. В. Полин

Академия криптографии Российской Федерации, г. Москва

Получено 22.IV.2013

Описаны необходимые условия, которым должно удовлетворять отношение θ эквивалентности на множестве A для того, чтобы оно было элементом какой-либо GA -решетки.

Ключевые слова: системы уравнений, решётки отношений

Permutation lattices of equivalence relations on Cartesian products

S. V. Polin

Academy of Cryptography of the Russian Federation, Moscow

Abstract. Necessary conditions for the equivalence relation θ on the set A to be an element of some GA -lattice are obtained.

Keywords: system of equations, lattices of relations

Напомним, что *уравнением* называется пара (f, b) , где $f: A \rightarrow B$ – произвольное отображение, $b \in B$. Множество A называется *областью неизвестных*, множество B – *областью правых частей*, а отображение f – *левой частью* уравнения. Конечное множество $\{(f_1, b_1), \dots, (f_m, b_m)\}$ уравнений с общей областью неизвестных называется *системой уравнений*.

В большинстве практических задач множество A разлагается в декартово произведение $A = \prod_{i=1}^n A_i$. В этом случае уравнение (f, b) обычно записывается в виде

$$f(x_1, \dots, x_n) = b,$$

где x_i – переменная типа A_i .

Пусть $\mathbf{L}_A$ – подрешетка решетки всех отношений эквивалентности на множестве A , содержащая наибольшее отношение A^2 . Будем говорить, что система уравнений

$$\begin{cases} f_1(x_1, \dots, x_n) = b_1, \\ \dots \\ f_m(x_1, \dots, x_n) = b_m. \end{cases}$$

согласована с решеткой $\mathbf{L}_A$, если выполнены следующие условия:

- Областью неизвестных каждого уравнения является множество A , т.е. каждое отображение f_i есть отображение вида $f_i: A \rightarrow B_i$. При этом множества B_i могут быть различными.
- Каждое отображение $f_i: A \rightarrow B_i$ сюръективно.
- Каждое ядро $\ker f_i$ является коатомом¹ решетки $\mathbf{L}_A$.

Класс всех систем уравнений, согласованных с решеткой $\mathbf{L}_A$ обозначим через $\mathcal{F}(A; \mathbf{L}_A)$.

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

¹ Напомним, что элемент τ решетки $\mathbf{M}$ с наибольшим элементом $1_{\mathbf{M}}$ называется *коатомом*, если $\tau < 1_{\mathbf{M}}$ и не существует такого элемента $\sigma \in \mathbf{M}$, что $\tau < \sigma < 1_{\mathbf{M}}$.

- а. Ядро каждой проекции $\prod_{i=1}^n A_i \rightarrow A_i$ принадлежит решетке $\mathbf{L}_A$ и является ее коатомом.
- б. Элементы решетки $\mathbf{L}_A$ попарно перестановочны (см. [5]).

В работе [6] исследовались условия, при которых существует гауссовоподобный алгоритм решения систем уравнений, принадлежащих классу $\mathcal{F}(A; \mathbf{L}_A)$. Оказалось, что существование или несуществование такого алгоритма во многом определяется свойствами решетки $\mathbf{L}_A$. В частности, наиболее благоприятным является случай, когда решетка $\mathbf{L}_A$ является GA -решеткой.

В связи с этим представляет интерес полное или частичное описание GA -решеток и согласованных с ними систем уравнений.

В настоящей работе мы опишем необходимые условия, которым должно удовлетворять отношение θ эквивалентности на множестве $\prod_{i=1}^n A_i$, для того, чтобы оно было элементом какой-либо GA -решетки. Из полученного описания, в частности, вытекает следующее утверждение.

Следствие. Пусть $\mathbf{L}_A$ – GA -решетка отношений эквивалентности на множестве $A = \prod_{i=1}^n A_i$. Тогда существует такая GA -решетка $\mathbf{L}_{A'}$ отношений эквивалентности на множестве $A' = \prod_{i=1}^{n-1} A_i$, что каждая система из класса $\mathcal{F}(A; \mathbf{L}_A)$ разлагается на подсистему, принадлежащую классу $\mathcal{F}(A'; \mathbf{L}_{A'})$, подсистему, состоящую из уравнений вида $\sigma(x_n) = b$ для подходящей перестановки σ множества A_n и подсистему, состоящую из уравнений вида

$$f(x_1, \dots, x_{n-1}) \circledast x_n = b,$$

где f – сюръективное отображение $f: A' \rightarrow A_n$, ядро которого является коатомом решетки $\mathbf{L}_{A'}$, а $\circledast$ – квазигрупповая операция на множестве A_n .

Мы предполагаем в дальнейшем провести исследование систем уравнений, описанных в данном следствии. Можно ожидать, что в результате будут выделены некоторые классы просто решаемых систем уравнений.

1. Бинарные отношения. Основные определения

Для полноты изложения напомним некоторые определения. Большинство из них, а также свойства введенных объектов можно найти в монографии [5].

Бинарным отношением из множества X в множество Y называется любое подмножество $\alpha \subseteq X \times Y$. Как это принято в алгебраических рассматриваниях, записи $(x, y) \in \alpha$ и $x \alpha y$ считаются эквивалентными, и каждая из них означает, что элементы x, y находятся в отношении α . Поскольку мы не будем рассматривать небинарные отношения, то термин "бинарное" будем, как правило, опускать и говорить просто об отношениях. Множество всех отношений из множества X в множество Y будем обозначать через $\mathcal{R}(X, Y)$.

Отношения из множества X в то же самое множество X называются отношениями *на* множестве X , а вместо обозначения $\mathcal{R}(X, X)$ обычно используют обозначение $\mathcal{R}(X)$.

Подмножество множества $\mathcal{R}(X)$, состоящее из всех отношений эквивалентности, будем обозначать $\mathcal{E}(X)$. Если $a \in X$ и $\kappa \in \mathcal{E}(X)$, то класс эквивалентности отношения κ , содержащий элемент a , будем обозначать $[a]_{\kappa}$.

На классе всех отношений естественным образом определяются некоторые алгебраические операции и отношения. Перечислим те из них, которые будут полезны для наших исследований.

Во-первых, каждое множество $\mathcal{R}(X, Y), \mathcal{R}(X), \mathcal{E}(X)$ частично упорядочено с помощью теоретико-множественного отношения включения. Более того, каждое из них является решеткой относительно этого порядка.

Наименьшим элементом решетки $\mathcal{E}(X)$ является отношение Δ_X , для которого $(a_1, a_2) \in \Delta_X$ тогда и только тогда, когда $a_1 = a_2$, а

наибольшим – отношение ∇_X , для которого $(a_1, a_2) \in \nabla_X$ при всех $(a_1, a_2) \in X$.

Пусть $\alpha \in \mathcal{R}(X, Y)$, $\beta \in \mathcal{R}(Y, Z)$. Тогда положим

$$\alpha \circ \beta = \langle (x, z) \in X \times Z \mid \exists y \in Y : (x, y) \in \alpha \& (y, z) \in \beta \rangle.$$

Частичная операция $\circ$, определенная таким образом называется операцией *умножения*. Эта операция ассоциативна, т.е. произведения $(\alpha \circ \beta) \circ \gamma$ и $\alpha \circ (\beta \circ \gamma)$ определены или не определены одновременно и, если они определены, то оба произведения равны.

Пусть $\alpha, \beta \in \mathcal{R}(X)$. Тогда определены произведения $\alpha \circ \beta, \beta \circ \alpha$. Если $\alpha \circ \beta = \beta \circ \alpha$, то отношения α, β называются *перестановочными*. Для краткости любое подмножество Θ отношений будем называть *перестановочным*, если любые его два элемента $\alpha, \beta \in \Theta$ перестановочны.

Отметим, что произведение отношений эквивалентности может быть отношением эквивалентности лишь при дополнительных условиях.

Лемма 1.1. *Произведение отношений θ, τ эквивалентности на множестве является отношением эквивалентности тогда и только тогда, когда они перестановочны. Кроме того, если рассматриваемые отношения эквивалентности перестановочны, то $\theta \circ \tau = \theta \vee \tau$.*

Доказательство приведено в монографии [5, с. 20]. □

Для отношения $\alpha \in \mathcal{R}(X, Y)$ положим

$$\alpha^* = \langle (y, x) \in Y \times X \mid (x, y) \in \alpha \rangle.$$

Тем самым для любых множеств X, Y определена операция *обращения* $*$: $\mathcal{R}(X, Y) \rightarrow \mathcal{R}(Y, X)$. Введенная операция удовлетворяет тождествам

$$(\alpha^*)^* = \alpha, \quad (\alpha \circ \beta)^* = \beta^* \circ \alpha^*.$$

Очевидно, что операции умножения и обращения монотонны относительно теоретико-множественного отношения включения, т.е.

$$(\alpha \subseteq \beta) \Rightarrow (\alpha^* \subseteq \beta^*),$$

$$((\alpha \subseteq \beta) \& (\gamma \subseteq \delta)) \Rightarrow ((\alpha \circ \gamma) \subseteq (\beta \circ \delta)).$$

Последнее условие выполняется всякий раз, когда отношения в правой части определены.

Пусть X, Y – произвольные множества, X_1, Y_1 – подмножества множеств X, Y соответственно, κ, η – отношения эквивалентности на множествах X_1, Y_1 соответственно, $\zeta: X_1/\kappa \rightarrow Y_1/\eta$ – взаимно однозначное отображение. Тогда можно определить отношение $P(X_1, Y_1, \kappa, \eta, \zeta) \in \mathcal{R}(X, Y)$, положив

$$P(X_1, Y_1, \kappa, \eta, \zeta) = \left\langle (x, y) \in X \times Y \mid x \in X_1, y \in Y_1, [x]_\kappa \zeta = [y]_\eta \right\rangle.$$

Каждое отношение такого вида будем называть *отношением Пуппе*.

Одним из примеров отношений Пуппе является пустое отношение $\emptyset \subseteq X \times Y$. Другим примером отношений Пуппе являются отношения эквивалентности $\theta \subseteq X \times X$.

Непосредственно из определений следует

$$P(X_1, Y_1, \kappa, \eta, \zeta)^* = P(Y_1, X_1, \eta, \kappa, \zeta^{-1}). \quad (1.1)$$

В общем случае произведение отношений Пуппе не является отношением Пуппе, однако легко проверяется равенство

$$P(X_1, Y_1, \kappa, \eta, \zeta) \circ P(Y_1, Z_1, \eta, \mu, \xi) = P(X_1, Z_1, \kappa, \mu, \zeta \xi). \quad (1.2)$$

Из равенств (1.1) и (1.2) следует

$$\begin{aligned} & P(X_1, Y_1, \kappa, \eta, \zeta) \circ P(X_1, Y_1, \kappa, \eta, \zeta)^* \circ P(X_1, Y_1, \kappa, \eta, \zeta) = \\ & = P(X_1, Y_1, \kappa, \kappa, \zeta \zeta^{-1}) \circ P(X_1, Y_1, \kappa, \eta, \zeta) = P(X_1, Y_1, \kappa, \eta, \zeta). \end{aligned}$$

Покажем, что это равенство как раз и выделяет отношения Пуппе среди остальных.

Лемма 1.2. Для любого отношения $\alpha \in \mathcal{R}(X, Y)$ выполняется включение $\alpha \subseteq \alpha \circ \alpha^* \circ \alpha$. При этом равенство

$$\alpha = \alpha \circ \alpha^* \circ \alpha. \quad (1.3)$$

имеет место тогда и только тогда, когда α есть отношение Пуппе.

Пусть $\alpha \in \mathcal{R}(X, Y)$ и $(x, y) \in \alpha$. Тогда $(y, x) \in \alpha^*$ и $(x, x) \in \alpha \circ \alpha^*$. Теперь из включений $(x, x) \in \alpha \circ \alpha^*$ и $(x, y) \in \alpha$ следует включение

$$(x, y) \in (\alpha \circ \alpha^*) \circ \alpha = \alpha \circ \alpha^* \circ \alpha.$$

Таким образом, $\alpha \subseteq \alpha \circ \alpha^* \circ \alpha$ и первое утверждение леммы доказано.

Теперь предположим, что выполняется равенство (1.3).

Положим

$$\mathbf{D}\alpha = \langle x \in X \mid \exists y \in Y (x, y) \in \alpha \rangle, \quad (1.4)$$

$$\mathbf{B}\alpha = \mathbf{D}\alpha^* = \langle y \in Y \mid \exists x \in X (x, y) \in \alpha \rangle,$$

На множествах $\mathbf{D}\alpha$ и $\mathbf{B}\alpha$ определим отношения

$$\mathbf{K}\alpha = \langle (x_1, x_2) \in \mathbf{D}\alpha \times \mathbf{D}\alpha \mid (x_1, x_2) \in \alpha \circ \alpha^* \rangle, \quad (1.5)$$

$$\mathbf{I}\alpha = \mathbf{K}\alpha^* = \langle (y_1, y_2) \in \mathbf{B}\alpha \times \mathbf{B}\alpha \mid (y_1, y_2) \in \alpha^* \circ \alpha \rangle.$$

Покажем, что в рассматриваемом случае эти отношения являются отношениями эквивалентности.

Пусть $x \in \mathbf{D}\alpha$. По определению, существует такой элемент $y \in Y$, что $(x, y) \in \alpha$. Выше мы видели, что из этого включения вытекает включение $(x, x) \in \alpha \circ \alpha^*$. Поэтому $(x, x) \in \mathbf{K}\alpha$, т.е. отношение $\mathbf{K}\alpha$ рефлексивно.

Пусть $(x_1, x_2) \in \mathbf{K}\alpha$. Тогда $(x_1, x_2) \in \alpha \circ \alpha^*$ и

$$(x_2, x_1) \in (\alpha \circ \alpha^*)^* = (\alpha^*)^* \circ \alpha^* = \alpha \circ \alpha^*,$$

что дает $(x_2, x_1) \in \mathbf{K}\alpha$, т.е. отношение $\mathbf{K}\alpha$ симметрично.

Пусть $(x_1, x_2), (x_2, x_3) \in \mathbf{K}\alpha$. Тогда $(x_1, x_2), (x_2, x_3) \in \alpha \circ \alpha^*$ и

$$(x_1, x_3) \in (\alpha \circ \alpha^*) \circ (\alpha \circ \alpha^*) = (\alpha \circ \alpha^* \circ \alpha) \circ \alpha^* = \alpha \circ \alpha^*,$$

что дает $(x_1, x_3) \in \mathbf{K}\alpha$, т.е. отношение $\mathbf{K}\alpha$ транзитивно.

То, что отношение $\mathbf{I}\alpha$ является отношением эквивалентности можно доказать аналогично, но можно воспользоваться и *принципом двойственности*. Для этого заметим, что при выполнении равенства (1.3) выполняется и двойственное ему равенство

$$\alpha^* = (\alpha \circ \alpha^* \circ \alpha)^* = \alpha^* \circ (\alpha^*)^* \circ \alpha^*.$$

Поэтому к отношению α^* применимо доказанное утверждение, которое показывает, что отношение $\mathbf{K}\alpha^*$ является отношением эквивалентности на множестве $\mathbf{D}\alpha^*$. Остается воспользоваться тем, что $\mathbf{D}\alpha^* = \mathbf{B}\alpha$ и $\mathbf{K}\alpha^* = \mathbf{I}\alpha$.

Определим отображение $\zeta: \mathbf{D}\alpha/\mathbf{K}\alpha \rightarrow \mathbf{B}\alpha/\mathbf{I}\alpha$, положив

$$([x]_{\mathbf{K}\alpha} \zeta = [y]_{\mathbf{I}\alpha}) \Leftrightarrow ((x, y) \in \alpha). \quad (1.6)$$

Формально, значение $[x]_{\mathbf{K}\alpha} \zeta$ зависит от выбора представителей x, y классов эквивалентности. Докажем, что эта зависимость несущественна.

Пусть $[x]_{\mathbf{K}\alpha} = [x']_{\mathbf{K}\alpha}$ и $[y]_{\mathbf{I}\alpha} = [y']_{\mathbf{I}\alpha}$. По определению, $(x', x) \in \alpha \circ \alpha^*$ и $(y, y') \in \alpha^* \circ \alpha$. Теперь имеем

$$((x, y) \in \alpha) \Rightarrow ((x', y') \in (\alpha \circ \alpha^*) \circ \alpha \circ (\alpha^* \circ \alpha) = \alpha).$$

Обратная импликация доказывается аналогично. Таким образом, определение (1.6) эквивалентно определению

$$([x]_{\mathbf{K}\alpha} \zeta = [y]_{\mathbf{I}\alpha}) \Leftrightarrow (\exists x' \in [x]_{\mathbf{K}\alpha}, y' \in [y]_{\mathbf{I}\alpha} : (x', y') \in \alpha),$$

которое уже не зависит от выбора представителей.

Рассмотрим произвольный элемент $x \in \mathbf{D}\alpha$. В силу определения (1.4) существует такой элемент $y \in Y$, что $(x, y) \in \alpha$. По определению, $y \in \mathbf{B}\alpha$ и $[x]_{\mathbf{K}\alpha} \zeta = [y]_{\mathbf{I}\alpha}$, т.е. элемент $[x]_{\mathbf{K}\alpha} \zeta$ всегда определен.

Допустим, что $(x, y), (x, y') \in \alpha$. Тогда $(y', y) \in \alpha^* \circ \alpha$ и $[y]_{\mathbf{I}\alpha} = [y']_{\mathbf{I}\alpha}$.

Таким образом, в рассматриваемых условиях элемент $[x]_{\mathbf{K}\alpha} \zeta$ определен однозначно, т.е. отображение ζ определено корректно.

Применив принцип двойственности, получаем, что существует такое отображение $\xi: \mathbf{B}\alpha/\mathbf{I}\alpha \rightarrow \mathbf{D}\alpha/\mathbf{K}\alpha$, что

$$([y]_{\mathbf{I}\alpha} \xi = [x]_{\mathbf{K}\alpha}) \Leftrightarrow ((y, x) \in \alpha^*).$$

Сравнив с импликацией (1.6), получаем

$$([x]_{\mathbf{K}\alpha} \zeta = [y]_{\mathbf{I}\alpha}) \Leftrightarrow ([y]_{\mathbf{I}\alpha} \xi = [x]_{\mathbf{K}\alpha}).$$

Отсюда следует, что отображения ζ и ξ взаимно обратны.

Теперь из формулы (1.6) следует, что $\alpha = P(\mathbf{D}\alpha, \mathbf{B}\alpha, \mathbf{K}\alpha, \mathbf{I}\alpha, \zeta)$.

□

2. Отношения эквивалентности на декартовых произведениях и их трансляции

В дальнейших рассмотрениях будут фиксированы множества B, C .

Для произвольного отношения $\theta \in \mathcal{R}(B \times C)$ и элементов $b_1, b_2 \in B$ определим отношение $l_{b_1 b_2}^\theta \in \mathcal{R}(C)$ следующим образом:

$$l_{b_1 b_2}^\theta = \left\langle (c_1, c_2) \in C^2 \mid (b_1, c_1) \theta (b_2, c_2) \right\rangle. \quad (2.1)$$

Каждое такое отношение будем называть *левой трансляцией* отношения θ .

Инволюцией отношения $\theta \in \mathcal{R}(B \times C)$ назовем такое отношение $\theta^\# \in \mathcal{R}(C \times B)$, что

$$\theta^\# = \left\langle ((c_1, b_1), (c_2, b_2)) \mid ((b_1, c_1), (b_2, c_2)) \in \theta \right\rangle.$$

Подчеркнем, что инволюция $\theta^\#$ и обратное отношение θ^* различны.

Нетрудно видеть, что $(\theta^\#)^\# = \theta$. Это приводит еще к одному принципу двойственности, согласно которому каждому утверждению или определению $\mathcal{P}(\theta)$ соответствует *двойственное*, представляющее собой "перевод" утверждения или определения $\mathcal{P}(\theta^\#)$ в терминах отношения θ .

Например, левую трансляцию $l_{c_1 c_2}^{\theta^\#} \in \mathcal{R}(B)$ будем называть *правой трансляцией* отношения θ и обозначать через $r_{c_1 c_2}^\theta$.

Лемма 2.1. Пусть $\theta, \tau \in \mathcal{R}(B \times C)$ и $l_{b_1 b_2}^\theta = l_{b_1 b_2}^\tau$ при всех $b_1, b_2 \in B$.

Тогда $\theta = \tau$.

Из определения трансляций следует

$$\begin{aligned} ((b_1, c_1) \theta (b_2, c_2)) &\Leftrightarrow ((c_1, c_2) \in l_{b_1 b_2}^\theta) \Leftrightarrow ((c_1, c_2) \in l_{b_1 b_2}^\tau) \Leftrightarrow \\ &\Leftrightarrow ((b_1, c_1) \tau (b_2, c_2)). \end{aligned}$$

□

Доказанное утверждение, помимо всего прочего, показывает, что множество левых (правых) трансляций однозначно определяет свойства

отношения и поэтому каждое свойство может быть переформулировано в терминах трансляций.

Лемма 2.2. Пусть $\theta, \eta \in \mathcal{R}(B \times C)$. Тогда для всех элементов $b_1, b_2 \in B$ выполняются равенства

$$l_{b_1 b_2}^{\theta*} = l_{b_2 b_1}^{\theta}, \quad l_{b_1 b_2}^{\theta \circ \eta} = \bigcup_{b \in B} l_{b_1 b}^{\theta} \circ l_{b b_2}^{\eta}.$$

Кроме того, $\theta \subseteq \eta$ тогда и только тогда, когда $l_{b_1 b_2}^{\theta} \subseteq l_{b_1 b_2}^{\eta}$ для всех элементов $b_1, b_2 \in B$.

Имеем

$$\begin{aligned} l_{b_1 b_2}^{\theta*} &= \left\langle (c_1, c_2) \in C^2 \mid (b_1, c_1) \theta^* (b_2, c_2) \right\rangle = \\ &= \left\langle (c_1, c_2) \in C^2 \mid (b_2, c_2) \theta (b_1, c_1) \right\rangle = \left(l_{b_2 b_1}^{\theta} \right)^*, \\ l_{b_1 b_2}^{\theta \circ \eta} &= \left\langle (c_1, c_2) \in C^2 \mid \exists (b, c) \in B \times C : (b_1, c_1) \theta (b, c) \eta (b_2, c_2) \right\rangle = \\ &= \left\langle (c_1, c_2) \in C^2 \mid \exists (b, c) \in B \times C : c_1 l_{b_1 b}^{\theta} c l_{b b_2}^{\eta} c_2 \right\rangle = \bigcup_{b \in B} l_{b_1 b}^{\theta} \circ l_{b b_2}^{\eta}. \end{aligned}$$

Пусть $\theta \subseteq \eta$. Тогда

$$\begin{aligned} \left((c_1, c_2) \in l_{b_1 b_2}^{\theta} \right) &\Rightarrow ((b_1, c_1) \theta (b_2, c_2)) \Rightarrow ((b_1, c_1) \eta (b_2, c_2)) \Rightarrow \\ &\Rightarrow \left((c_1, c_2) \in l_{b_1 b_2}^{\eta} \right) \text{ и } l_{b_1 b_2}^{\theta} \subseteq l_{b_1 b_2}^{\eta}. \end{aligned}$$

Пусть теперь $\theta \not\subseteq \eta$. Тогда найдутся такие пары $(b_1, c_1), (b_2, c_2) \in B \times C$, что $(b_1, c_1) \in \theta, (b_2, c_2) \notin \eta$. Теперь из определений трансляций следует, что $(c_1, c_2) \in l_{b_1 b_2}^{\theta}$ и $(c_1, c_2) \notin l_{b_1 b_2}^{\eta}$, т.е. $l_{b_1 b_2}^{\theta} \not\subseteq l_{b_1 b_2}^{\eta}$. $\square$

Следствие 2.1. Отношение $\theta \in \mathcal{R}(B \times C)$ является отношением эквивалентности тогда и только тогда, когда выполняются следующие условия:

- A. $\Delta_C \subseteq l_{bb}^{\theta}$ для всех $b \in B$;
- B. $\left(l_{b_1 b_2}^{\theta} \right)^* = l_{b_2 b_1}^{\theta}$ для всех $b_1, b_2 \in B$;

$$C. \quad l_{b_1 b_2}^\theta \circ l_{b_2 b_3}^\theta \subseteq l_{b_1 b_3}^\theta \quad \text{для всех } b_1, b_2, b_3 \in B.$$

Из леммы 2.2 следует, что условие В выполняется тогда и только тогда, когда отношение θ симметрично, а условие С – тогда и только тогда, когда отношение θ транзитивно.

Далее имеем

$$l_{bb}^{\Delta_{B \times C}} = \left\langle (c_1, c_2) \in C^2 \mid (b, c_1) = (b, c_1) \right\rangle = \Delta_C.$$

Из этого равенства и той же леммы 2.2 следует, что условие А эквивалентно рефлексивности отношения θ . $\square$

Условие С можно уточнить. Для этого заметим, что

$$\left((c_1, c_2) \in l_{b_1 b_2}^\theta \circ l_{b_2 b_3}^\theta \right) \Leftrightarrow \left(\exists c \in C : \{ (b_1, c_1) \theta (b_2, c) \} \& \{ (b_2, c) \theta (b_3, c_2) \} \right).$$

Из транзитивности отношения θ следует, что

$$\begin{aligned} & \left(\{ (b_1, c_1) \theta (b_2, c) \} \& \{ (b_2, c) \theta (b_3, c_2) \} \right) \Leftrightarrow \\ & \Leftrightarrow \left(\{ (b_1, c_1) \theta (b_2, c) \} \& \{ (b_2, c) \theta (b_3, c_2) \} \& \{ (b_1, c_1) \theta (b_3, c_2) \} \right) \Leftrightarrow \\ & \Leftrightarrow \left(\{ (b_1, c_1) \theta (b_2, c) \} \& \{ (b_1, c_1) \theta (b_3, c_2) \} \right). \end{aligned}$$

Поэтому

$$\left((c_1, c_2) \in l_{b_1 b_2}^\theta \circ l_{b_2 b_3}^\theta \right) \Leftrightarrow \left(\{ \exists c \in C : (b_1, c_1) \theta (b_2, c) \} \& \{ (b_1, c_1) \theta (b_3, c_2) \} \right).$$

Из формул (1.4) и (2.1) следует, что первое высказывание, входящее в правую часть импликации, истинно тогда и только тогда, когда $c_1 \in \mathbf{D}l_{b_1 b_2}^\theta$, а второе – тогда и только тогда, когда $(c_1, c_2) \in l_{b_1 b_1}^\theta$, т.е.

$$\left((c_1, c_2) \in l_{b_1 b_2}^\theta \circ l_{b_2 b_3}^\theta \right) \Leftrightarrow \left(\left\{ c_1 \in \mathbf{D}l_{b_1 b_2}^\theta \right\} \& \left\{ (c_1, c_2) \in l_{b_1 b_1}^\theta \right\} \right).$$

Используя условие В следствия 2.1, получаем

$$\left(l_{b_1 b_2}^\theta \circ l_{b_2 b_3}^\theta \right)^* = \left(l_{b_2 b_3}^\theta \right)^* \circ \left(l_{b_1 b_2}^\theta \right)^* = l_{b_3 b_2}^\theta \circ l_{b_2 b_1}^\theta.$$

Поэтому

$$\begin{aligned}
& \left((c_1, c_2) \in l_{b_1 b_2}^\theta \circ l_{b_2 b_3}^\theta \right) \Leftrightarrow \left((c_2, c_1) \in \left(l_{b_1 b_2}^\theta \circ l_{b_2 b_3}^\theta \right)^* \right) \Leftrightarrow \\
& \Leftrightarrow \left((c_2, c_1) \in l_{b_3 b_2}^\theta \circ l_{b_2 b_1}^\theta \right) \Leftrightarrow \left(\left\{ c_2 \in \mathbf{D}l_{b_3 b_2}^\theta \right\} \& \left\{ (c_2, c_1) \in l_{b_3 b_1}^\theta \right\} \right) \Leftrightarrow \\
& \left(\left\{ c_2 \in \mathbf{D}l_{b_3 b_2}^\theta \right\} \& \left\{ (c_1, c_2) \in l_{b_1 b_3}^\theta \right\} \right).
\end{aligned}$$

Таким образом,

$$l_{b_1 b_2}^\theta \circ l_{b_2 b_3}^\theta = \left(\mathbf{D}l_{b_1 b_2}^\theta \times \mathbf{D}l_{b_3 b_2}^\theta \right) \cap l_{b_1 b_3}^\theta. \quad (2.2)$$

Следствие 2.2. Пусть θ – отношение эквивалентности на множестве $B \times C$. Тогда каждая левая трансляция $l_{b_1 b_2}^\theta$ является отношением Пуппе.

Пусть $b_1, b_2 \in B$. Тогда, используя условия В и С леммы 2.2, получаем

$$\begin{aligned}
l_{b_1 b_2}^\theta \circ \left(l_{b_1 b_2}^\theta \right)^* \circ l_{b_1 b_2}^\theta &= l_{b_1 b_2}^\theta \circ l_{b_2 b_1}^\theta \circ l_{b_1 b_2}^\theta = \left(l_{b_1 b_2}^\theta \circ l_{b_2 b_1}^\theta \right) \circ l_{b_1 b_2}^\theta \subseteq \\
& l_{b_1 b_1}^\theta \circ l_{b_1 b_2}^\theta \subseteq l_{b_1 b_2}^\theta.
\end{aligned}$$

Осталось воспользоваться леммой 1.2. $\square$

Замечание. Пусть $Y \subset X$ и σ – отношение эквивалентности на множестве X . Тогда отношение $\sigma \cap Y^2$ является отношением эквивалентности на множестве Y . Классы эквивалентности элемента $y \in Y$ для этих отношений связаны равенством $[y]_{\sigma \cap Y^2} = [y]_\sigma \cap Y$ и в общем случае могут различаться, однако если множество Y является объединением нескольких классов эквивалентности отношения σ , то $[y]_{\sigma \cap Y^2} = [y]_\sigma$. В частности, в этом случае множество $Y /_{\sigma \cap Y^2}$ является подмножеством множества $X /_{\sigma}$. $\square$

Теорема 2.1. Пусть $\theta \in \mathcal{R}(B \times C)$. Тогда для того, чтобы отношение θ являлось отношением эквивалентности, необходимо и достаточно, чтобы выполнялись следующие условия.

1. Левые трансляции отношения θ являются отношениями Пуппе и имеют вид

$$l_{b_1 b_2}^\theta = P \left(\mathbf{D}l_{b_1 b_2}^\theta, \mathbf{D}l_{b_2 b_1}^\theta, l_{b_1 b_1}^\theta \cap \left(\mathbf{D}l_{b_1 b_2}^\theta \right)^2, l_{b_2 b_2}^\theta \cap \left(\mathbf{D}l_{b_2 b_1}^\theta \right)^2, \zeta_{b_1 b_2} \right) \quad (2.3)$$

для некоторых взаимно однозначных отображений

$$\zeta_{b_1 b_2} : \frac{\mathbf{D}l_{b_1 b_2}^\theta}{l_{b_1 b_1}^\theta \cap \left(\mathbf{D}l_{b_1 b_2}^\theta \right)^2} \rightarrow \frac{\mathbf{D}l_{b_2 b_1}^\theta}{l_{b_2 b_2}^\theta \cap \left(\mathbf{D}l_{b_2 b_1}^\theta \right)^2}. \quad (2.4)$$

2. Для каждого элемента $b \in B$ выполняется равенство $\mathbf{D}l_{bb}^\theta = C$.
3. Каждое множество $\mathbf{D}l_{b_1 b_2}^\theta$ является объединением нескольких классов эквивалентности отношения $l_{b_1 b_1}^\theta$.
4. Для всех элементов $b_1, b_2, b_3 \in B, c \in \mathbf{D}l_{b_2 b_1}^\theta \cap \mathbf{D}l_{b_2 b_3}^\theta$ класс $[c]_{l_{b_2 b_2}^\theta} \zeta_{b_1 b_2}^{-1}$ эквивалентности отношения $l_{b_1 b_1}^\theta$ содержится в множестве $\mathbf{D}l_{b_1 b_3}^\theta$ и $\left([c]_{l_{b_2 b_2}^\theta} \zeta_{b_1 b_2}^{-1} \right) \zeta_{b_1 b_3} = [c]_{l_{b_2 b_2}^\theta} \zeta_{b_2 b_3}$.

Пусть отношение θ является отношением эквивалентности. Тогда в силу следствия 2.2 и доказательства леммы 1.2 левые трансляции отношения θ имеют вид

$$l_{b_1 b_2}^\theta = P \left(\mathbf{D}l_{b_1 b_2}^\theta, \mathbf{B}l_{b_1 b_2}^\theta, \mathbf{K}l_{b_1 b_2}^\theta, \mathbf{I}l_{b_1 b_2}^\theta, \zeta_{b_1 b_2} \right).$$

Используя следствие 2.1 и равенства (1.4), (1.5), получаем

$$\mathbf{B}l_{b_1 b_2}^\theta = \mathbf{D} \left(l_{b_1 b_2}^\theta \right)^* = \mathbf{D}l_{b_2 b_2}^\theta,$$

$$\mathbf{I}l_{b_1 b_2}^\theta = \mathbf{K} \left(l_{b_1 b_2}^\theta \right)^* = \mathbf{K}l_{b_2 b_2}^\theta.$$

Используя равенства (1.5), (2.2) и условие В следствия 2.1, получаем

$$\mathbf{K}l_{b_1 b_2}^\theta = \left\langle (c_1, c_2) \in \left(\mathbf{D}l_{b_1 b_2}^\theta \right)^2 \mid (c_1, c_2) \in \left(\mathbf{D}l_{b_1 b_2}^\theta \right)^2 \cap l_{b_1 b_1}^\theta \right\rangle,$$

т.е. $\mathbf{K}l_{b_1b_2}^\theta = l_{b_1b_1}^\theta \cap \left(\mathbf{D}l_{b_1b_2}^\theta \right)^2$ и левые трансляции отношения θ имеют вид (2.3)

Так как отношение θ является отношением эквивалентности, то $(b,c)\theta(b,c)$ для любого элемента $c \in C$. Отсюда следует, что $c \in \mathbf{D}l_{bb}^\theta$ и $\mathbf{D}l_{bb}^\theta = C$.

Пусть $c_1 \in \mathbf{D}l_{b_1b_2}^\theta$ и $(c_1, c_2) \in l_{b_1b_1}^\theta$. Тогда из первого включения следует, что существует такой элемент $c \in C$, что $(b_1, c_1)\theta(b_2, c)$, а из второго – что $(b_1, c_1)\theta(b_1, c_2)$. Из транзитивности отношения θ следует $(b_1, c_2)\theta(b_2, c)$. Отсюда следует $c_2 \in \mathbf{D}l_{b_1b_2}^\theta$. Поэтому, $[c_1]_{l_{b_1b_1}^\theta} \subseteq \mathbf{D}l_{b_1b_2}^\theta$ и множество $\mathbf{D}l_{b_1b_2}^\theta$ является объединением классов эквивалентности отношения $l_{b_1b_1}^\theta$.

Рассмотрим произвольный элемент $c \in \mathbf{D}l_{b_2b_1}^\theta \cap \mathbf{D}l_{b_2b_3}^\theta$ и произвольные элементы $c_1 \in [c]_{l_{b_2b_2}^\theta} \zeta_{b_1b_2}^{-1}$, $c_2 \in [c]_{l_{b_2b_2}^\theta} \zeta_{b_2b_3}$. Используя равенство (1.6), получаем $(c_1, c) \in l_{b_1b_2}^\theta, (c, c_2) \in l_{b_2b_3}^\theta$. Поэтому

$$(c_1, c_2) \in l_{b_1b_2}^\theta \circ l_{b_2b_3}^\theta = \left(\mathbf{D}l_{b_1b_2}^\theta \times \mathbf{D}l_{b_2b_3}^\theta \right) \cap l_{b_1b_3}^\theta.$$

Отсюда и из равенства (1.6) вытекает утверждение 4 теоремы, что завершает доказательство теоремы в одну сторону.

Справедливость обратного утверждения легко проверяется.

□

3. Нормальные отношения эквивалентности

Ядра проекций произведения $B \times C$ на компоненты B и C обозначим через ρ_B и ρ_C соответственно.

Пусть θ – отношение эквивалентности на множестве $B \times C$. Это отношение назовем *нормальным слева*, если отношение θ перестановочно с отношением ρ_B , а отношение $\theta \wedge \rho_B$ перестановочно с отношением ρ_C . Двойственным образом определяется понятие отношения *нормального*

$\theta \wedge \rho_C$ перестановочно с отношением ρ_B . Отношение, нормальное и слева и справа, назовем *нормальным*.

Значение введенного понятия для наших исследований показывает следующая лемма.

Лемма 3.1. Пусть $\mathbf{L}_{B \times C}$ – перестановочная решетка отношений эквивалентности на множестве $B \times C$, содержащая проекции ρ_B и ρ_C . Тогда каждое отношение $\theta \in \mathbf{L}_{B \times C}$ нормально.

При сделанных предположениях отношения $\theta, \rho_B, \rho_C, \theta \wedge \rho_B, \theta \wedge \rho_C$ принадлежат решетке $\mathbf{L}_{B \times C}$. Поэтому эти пять отношений попарно перестановочны, откуда и следует наше утверждение.

□

Для отношений $\alpha \subseteq B^2, \beta \subseteq C^2$ полагаем

$$\alpha \times \beta = \langle ((b_1, c_1), (b_2, c_2)) \mid (b_1, b_2) \in \alpha, (c_1, c_2) \in \beta \rangle.$$

Из определений следует

$$l_{b_1 b_2}^{\alpha \times \beta} = \langle (c_1, c_2) \in C^2 \mid (b_1, b_2) \in \alpha, (c_1, c_2) \in \beta \rangle = \begin{cases} \beta, & (b_1, b_2) \in \alpha, \\ \emptyset, & (b_1, b_2) \notin \alpha. \end{cases} \quad (3.1)$$

Нетрудно видеть, что $\rho_B = \Delta_B \times \nabla_C$ и $\rho_C = \nabla_B \times \Delta_C$. Соответственно имеем

$$l_{b_1 b_2}^{\rho_B} = \begin{cases} \nabla_C, & b_1 = b_2, \\ \emptyset, & b_1 \neq b_2. \end{cases} \quad (3.2)$$

$$l_{b_1 b_2}^{\rho_C} = \Delta_C. \quad (3.3)$$

Пусть $\theta \in \mathcal{R}(B \times C)$. Тогда из равенств (3.2) и леммы 2.2 следует

$$\begin{aligned} l_{b_1 b_2}^{\theta \circ \rho_B} &= \bigcup_{b \in B} l_{b_1 b}^{\theta} \circ l_{b b_2}^{\rho_B} = l_{b_1 b_2}^{\theta} \circ l_{b_2 b_2}^{\rho_B} \cup \bigcup_{b \neq b_2} l_{b_1 b}^{\theta} \circ l_{b b_2}^{\rho_B} = \\ &= l_{b_1 b_2}^{\theta} \circ \nabla_C \cup \bigcup_{b \neq b_2} l_{b_1 b}^{\theta} \circ \emptyset = l_{b_1 b_2}^{\theta} \circ \nabla_C = \\ &= \langle (c_1, c_2) \in C^2 \mid \exists c \in C (c_1, c) \in l_{b_1 b_2}^{\theta} \& (c, c_2) \in \nabla_C \rangle \\ &= \langle (c_1, c_2) \in C^2 \mid \exists c \in C : (c_1, c) \in l_{b_1 b_2}^{\theta} \rangle. \end{aligned}$$

Используя определение (1.4), получаем

$$l_{b_1 b_2}^{\theta \circ \rho_B} = \mathbf{D}l_{b_1 b_2}^\theta \times C. \quad (3.4)$$

Так же показываем, что

$$l_{b_1 b_2}^{\rho_B \circ \theta} = C \times \mathbf{B}l_{b_1 b_2}^\theta.$$

Теперь из леммы 2.1 следует, что отношения θ и ρ_B перестановочны тогда и только тогда, когда равенство

$$\mathbf{D}l_{b_1 b_2}^\theta \times C = C \times \mathbf{B}l_{b_1 b_2}^\theta \quad (3.5)$$

выполняется для всех элементов $b_1, b_2 \in B$.

Для дальнейших рассмотрений введем следующие определения:

$$\begin{aligned} \mathcal{D}\theta &= \left\langle (b_1, b_2) \in B^2 \mid \exists c_1, c_2 \in C : (b_1, c_1)\theta(b_2, c_2) \right\rangle, \\ \mathcal{B}\theta &= \mathcal{D}\theta^\# = \left\langle (c_1, c_2) \in C^2 \mid \exists b_1, b_2 \in B : (b_1, c_1)\theta(b_2, c_2) \right\rangle, \\ \mathcal{K}\theta &= \left\langle (b_1, b_2) \in B^2 \mid \exists c \in C : (b_1, c)\theta(b_2, c) \right\rangle, \\ \mathcal{I}\theta &= \mathcal{K}\theta^\# = \left\langle (c_1, c_2) \in C^2 \mid \exists b \in B : (b, c_1)\theta(b, c_2) \right\rangle. \end{aligned} \quad (3.6)$$

Сравнив определения (1.4), (2.1) и (3.6), получаем

$$((b_1, b_2) \in \mathcal{D}\theta) \Leftrightarrow (\mathbf{D}l_{b_1 b_2}^\theta \neq \emptyset). \quad (3.7)$$

Теорема 3.1. Пусть θ есть отношение эквивалентности на множестве $B \times C$. Тогда для того, чтобы оно было перестановочно с отношением ρ_B , необходимо и достаточно, чтобы выполнялись следующие равенства:

$$\mathbf{D}l_{b_1 b_2}^\theta = \begin{cases} C, & (b_1, b_2) \in \mathcal{D}\theta, \\ \emptyset, & (b_1, b_2) \notin \mathcal{D}\theta. \end{cases} \quad (3.8)$$

При их выполнении отношение $\mathcal{D}\theta$ является отношением эквивалентности и $\theta \vee \rho_B = \mathcal{D}\theta \times \nabla_C$.

Предположим, что отношения θ и ρ_B перестановочны, и рассмотрим произвольные элементы $b_1, b_2 \in B$.

Допустим, что $(b_1, b_2) \notin \mathcal{D}\theta$. Тогда $\mathbf{D}l_{b_1 b_2}^\theta = \emptyset$ в силу импликации (3.7) и равенство (3.8) выполняется.

Теперь допустим, что $(b_1, b_2) \in \mathcal{D}\theta$. Тогда $\mathbf{D}l_{b_1 b_2}^\theta \neq \emptyset$ в силу импликации (3.7) и левая часть равенства (3.5) не пуста. Следовательно, не пуста и его правая часть. Это показывает, что $\mathbf{B}l_{b_1 b_2}^\theta \neq \emptyset$. Произвольно выберем элементы $c \in C, d \in \mathbf{B}l_{b_1 b_2}^\theta$. Тогда $(c, d) \in C \times \mathbf{B}l_{b_1 b_2}^\theta$ и $(c, d) \in \mathbf{D}l_{b_1 b_2}^\theta \times C$ в силу равенства (3.5), что дает $c \in \mathbf{D}l_{b_1 b_2}^\theta$. Так как элемент c выбирался произвольно, то $\mathbf{D}l_{b_1 b_2}^\theta = C$ и равенство (3.8) выполняется.

Теперь предположим, что равенства (3.8) справедливы. Покажем, что отношение $\mathcal{D}\theta$ является отношением эквивалентности.

Пусть $b \in B$. Тогда $\mathbf{D}l_{bb}^\theta = C$ и $(b, b) \in \mathcal{D}\theta$ в силу теоремы 2.1.

Пусть $(b_1, b_2) \in \mathcal{D}\theta$. По определению, существуют такие элементы $c_1, c_2 \in C$, что $(b_1, c_1)\theta(b_2, c_2)$. Тогда $(b_2, c_2)\theta(b_1, c_1)$ и $(b_2, b_1) \in \mathcal{D}\theta$.

Пусть $(b_1, b_2), (b_2, b_3) \in \mathcal{D}\theta$. По определению, существуют такие элементы $c_1, c_2 \in C$, что $(b_1, c_1)\theta(b_2, c_2)$. Из равенства (3.8) следует, что $\mathbf{D}l_{b_2 b_3}^\theta = C$. Поэтому $c_2 \in \mathbf{D}l_{b_2 b_3}^\theta$ и существует такой элемент $c_3 \in C$, что $(b_2, c_2)\theta(b_3, c_3)$. Тогда $(b_1, c_1)\theta(b_3, c_3)$ и $(b_1, b_3) \in \mathcal{D}\theta$.

В рассматриваемых условиях равенство (3.4) приобретает вид

$$l_{b_1 b_2}^{\theta \circ \rho_B} = \begin{cases} \nabla_C, & (b_1, b_2) \in \mathcal{D}\theta, \\ \emptyset, & (b_1, b_2) \notin \mathcal{D}\theta. \end{cases}$$

Из равенства (3.1) и леммы 2.1 получаем

$$\theta \circ \rho_B = \mathcal{D}\theta \times \nabla_C. \quad (3.9)$$

Таким образом, отношение $\theta \circ \rho_B$ является отношением эквивалентности.

Применив лемму 1.1, получаем, что отношения θ и ρ_B перестановочны.

Из той же леммы и равенства (3.9) вытекает последнее утверждение теоремы. $\square$

Следствие 3.1. Пусть τ – отношение эквивалентности на множестве $B \times C$ и $\tau \leq \rho_C$. Тогда для того, чтобы отношения τ и ρ_B были перестановочными, необходимо и достаточно, чтобы отношение τ было представимо в виде $\tau = \mathcal{D}\tau \times \Delta_C$.

Пусть $\tau = \mathcal{D}\tau \times \Delta_C$. Тогда, применив равенство (3.1), получаем

$$l_{b_1 b_2}^\tau = \begin{cases} \nabla_C, & (b_1, b_2) \in \mathcal{D}\tau, \\ \emptyset, & (b_1, b_2) \notin \mathcal{D}\tau. \end{cases}$$

Отсюда и из импликации (3.7) следует, что выполняется равенство (3.8) и рассматриваемые отношения перестановочны.

Предположим теперь, что отношения τ и ρ_B перестановочны.

Пусть $(b_1, c_1)\theta(b_2, c_2)$. Тогда $(b_1, b_2) \in \mathcal{D}\tau$ и $(c_1, c_2) \in l_{b_1 b_2}^\tau$. Из условия $\tau \leq \rho_C$, леммы 2.2 и формулы (3.3) вытекает неравенство $l_{b_1 b_2}^\tau \subseteq \Delta_C$, откуда следует, что $c_1 = c_2$. Таким образом, $\tau \subseteq \mathcal{D}\tau \times \Delta_C$.

Пусть теперь $(b_1, b_2) \in \mathcal{D}\tau, c_1 \in C$. Тогда $\mathbf{D}l_{b_1 b_2}^\tau = C$ в силу теоремы 3.1. Следовательно, $c_1 \in \mathbf{D}l_{b_1 b_2}^\tau$ и, по определению, существует такой элемент $c_2 \in C$, что $(b_1, c_1)\tau(b_2, c_2)$. Из предыдущего абзаца следует, что $c_2 = c_1$, т.е. $(b_1, c_1)\tau(b_2, c_1)$ и $\mathcal{D}\tau \times \Delta_C \subseteq \tau$.

Таким образом, $\tau = \mathcal{D}\tau \times \Delta_C$. $\square$

Теорема 3.2. Пусть θ – отношение эквивалентности на множестве $B \times C$. Тогда следующие свойства эквивалентны:

1. Отношения $\theta \wedge \rho_B$ и ρ_C перестановочны.
2. Выполняется равенство $\theta \wedge \rho_B = \Delta_B \times \mathcal{I}\theta$.
3. $\Delta_B \times \mathcal{I}\theta \leq \theta$.
4. Все отношения l_{bb}^θ совпадают.

При выполнении условия 1 (и, следовательно, при выполнении каждого из этих условий) отношение $\mathcal{I}\theta$ является отношением эквивалентности.

$1 \Leftrightarrow 2$. Заметим, что

$$\begin{aligned} \mathcal{B}(\theta \wedge \rho_B) &= \left\langle (c_1, c_2) \in C^2 \mid \exists b_1, b_2 \in B (b_1, c_1)(\theta \wedge \rho_B)(b_2, c_2) \right\rangle = \\ &= \left\langle (c_1, c_2) \in C^2 \mid \exists b \in B (b, c_1)\theta(b, c_2) \right\rangle = \mathcal{I}\theta. \end{aligned} \quad (3.10)$$

Отсюда и из утверждения, двойственного следствию 3.1, вытекает, что условия 1 и 2 эквивалентны. Из этого равенства и теоремы 3.1 следует, что

при выполнении условия 1 отношение $\mathcal{I}\theta$ является отношением эквивалентности.

Импликация $2 \Rightarrow 3$ очевидна.

$3 \Rightarrow 2$. Нетрудно заметить, что $\Delta_B \times \mathcal{I}\theta \leq \Delta_B \times \nabla_C = \rho_B$. Поэтому, если условие 3 выполняется, то $\theta \wedge \rho_B \subseteq (\Delta_B \times \mathcal{I}\theta) \wedge \rho_B = \Delta_B \times \mathcal{I}\theta$.

$3 \Rightarrow 4$. Выберем произвольно элементы $b_1, b_2 \in B$. Также произвольно выберем пару $(c_1, c_2) \in l_{b_1 b_1}^\theta$. Из условия 3 следует

$$\begin{aligned} \left((c_1, c_2) \in l_{b_1 b_1}^\theta \right) &\Rightarrow \left(((b_1, c_1), (b_1, c_2)) \in \theta \right) \Rightarrow \left((c_1, c_2) \in \mathcal{I}\theta \right) \Rightarrow \\ &\Rightarrow \left(((b_2, c_1), (b_2, c_2)) \in \Delta_B \times \mathcal{I}\theta \right) \Rightarrow \left(((b_2, c_1), (b_2, c_2)) \in \theta \right) \Rightarrow \\ &\Rightarrow \left((c_1, c_2) \in l_{b_2 b_2}^\theta \right). \end{aligned}$$

Из произвольности выбора всех элементов вытекает выполнение условия 4.

$4 \Rightarrow 3$. Пусть $((b_1, c_1), (b_2, c_2)) \in \Delta_B \wedge \mathcal{I}\theta$. Это эквивалентно тому, что $b_2 = b_1$ и $(c_1, c_2) \in \mathcal{I}\theta$. Последнее означает, что $((b, c_1), (b, c_2)) \in \theta$ для подходящего элемента $b \in B$. Последнее означает, что $(c_1, c_2) \in l_{bb}^\theta$. Из условия 4 следует, что $(c_1, c_2) \in l_{b_1 b_1}^\theta$ и $((b_1, c_1), (b_2, c_2)) \in \theta$. Так как рассматриваемая пара выбиралась произвольно, то включение $\Delta_B \times \mathcal{I}\theta \leq \theta$ выполняется. $\square$

4. Нормальные отображения

Из введения ясно, что для практики представляют интерес не сами нормальные отношения эквивалентности, а отображения $f: B \times C \rightarrow D$, ядра которых нормальны. Будем называть такие отображения *нормальными*. Именно их мы и будем исследовать в настоящем разделе.

Определения многоосновных алгебр и связанных с ними понятий содержатся в работе [2].

Трехосновную алгебру $\langle U, V, W; \otimes \rangle$, где $\otimes$ есть отображение $\otimes: U \times V \rightarrow W$, назовем *трехосновным группоидом*.

Трехосновной группоид $\langle U, V, W; \otimes \rangle$ назовем *трехосновной квазигруппой*, если каждое уравнение вида $u \otimes x = w$ и каждое уравнение вида $x \otimes v = w$, где $u \in U$, $v \in V$, $w \in W$, имеет единственное решение.

Как показывает следующее утверждение, обычные и трехосновные квазигруппы тесно связаны.

Лемма 4.1. *Трехосновный группоид $\mathbf{G} = \langle U, V, W; \otimes \rangle$ является трехосновной квазигруппой тогда и только тогда, когда существуют такая квазигруппа $\langle Q; * \rangle$ и такие взаимно однозначные отображения $\alpha: U \rightarrow Q$, $\beta: V \rightarrow Q$, $\gamma: W \rightarrow Q$, что*

$$u \otimes v = ((u\alpha) * (v\beta))\gamma^{-1} \quad (4.1)$$

для всех элементов $u \in U$, $v \in V$.

Допустим, что трехосновный группоид $\mathbf{G}$ является трехосновной квазигруппой.

Произвольно выберем элементы $e \in U$, $g \in V$ и определим отображения $\lambda: U \rightarrow W$, $\rho: V \rightarrow W$, положив $u\lambda = u \otimes g$, $v\beta = e \otimes v$. Из определения трехосновных квазигрупп следует, что эти отображения взаимно однозначны. Поэтому множества U, V, W имеют одинаковую мощность.

В качестве множества Q выберем какое-либо множество той же мощности. Произвольно выберем взаимно однозначные отображения $\alpha: U \rightarrow Q$, $\beta: V \rightarrow Q$, $\gamma: W \rightarrow Q$. Положим

$$q_1 * q_2 = \left((q_1\alpha^{-1}) \otimes (q_2\beta^{-1}) \right) \gamma.$$

Легко проверить, что группоид $\langle Q; * \rangle$ является квазигруппой и что выполняется равенство (4.1).

Обратное утверждение очевидно. □

Следствие 4.1. *Пусть $\mathbf{G} = \langle U, V, W; \otimes \rangle$ – трехосновная квазигруппа. Тогда*

1. *Основные множества трехосновной квазигруппы имеют одинаковую мощность.*

2. *Если $\alpha: U \rightarrow Q$, $\beta: V \rightarrow Q$, $\gamma: W \rightarrow Q$ – произвольные взаимно однозначные отображения, то на множестве Q можно определить такую квазигрупповую операцию $*$, что выполняется равенство (4.1).*

Утверждение вытекает из доказательства леммы 4.1. □

Пусть I, J – произвольные множества. Тогда множество Q , на котором задано множество $\langle *_{ij} \mid i \in I \times J \rangle$ бинарных операций, будем называть

$I \times J$ -группоидом. Если каждый группоид $\langle Q; *_{ij} \rangle$ является квазигруппой, то такой $I \times J$ -группоид будем называть $I \times J$ -квазигруппой.

Подчеркнем, что некоторые из операций $*_{ij}$ могут совпадать.

Рассмотрим произвольную $I \times J$ -квазигруппу $\mathbf{Q} = \langle Q; \langle *_{ij} \mid i \in I \times J \rangle \rangle$.

Определим операцию

$$*: (Q \times I) \times (Q \times J) \rightarrow Q \times (I \times J),$$

положив

$$(q_1, i) * (q_2, j) = (q_1 *_{ij} q_2, (i, j)).$$

Тем самым мы определили трехосновный группоид

$$\mathfrak{R}(\mathbf{Q}) = \langle Q \times I, Q \times J, Q \times (I \times J); * \rangle.$$

Группоиды вида $\mathfrak{R}(\mathbf{Q})$ и изоморфные им будем называть *рисовскими*.

Очевидно, что каждая квазигруппа является рисовским группоидом. Приведем еще один пример рисовских группоидов.

Для произвольных множеств I, J полагаем $\Sigma_{IJ} = \langle I, J, I \times J; \times \rangle$, где $i \times j = (i, j)$. Каждый группоид такого вида будем называть *связкой*. Легко проверить, что связка Σ_{IJ} изоморфна трехосновному группоиду $\mathfrak{R}(\mathbf{E})$, где $\mathbf{E} = \langle E; \langle \circ_{ij} \mid i \in I \times J \rangle \rangle$, $E = \{1\}$, $1 \circ_{ij} 1 = 1$. Таким образом, каждая связка является рисовским группоидом.

Рассмотрим трехосновный группоид $\mathbf{G} = \langle U, V, W; \otimes \rangle$. Допустим, что существует эпиморфизм трехосновных группоидов

$$\langle \mu, \lambda, \eta \rangle : \langle U, V, W; \otimes \rangle \rightarrow \Sigma_{IJ}. \quad (4.2)$$

Положим

$$U_i = \langle u \in U \mid u\mu = i \rangle, \quad V_j = \langle v \in V \mid v\lambda = j \rangle, \quad W_{ij} = \langle w \in W \mid w\eta = (i, j) \rangle.$$

Пусть $u \in U_i, v \in V_j$. Тогда

$$(u \otimes v)\eta = (u\mu) \times (v\lambda) = i \times j = (i, j).$$

Следовательно, $u \otimes v \in W_{ij}$. Это позволяет определить трехосновный группоид $\mathbf{G}_{ij} = \langle U_i, V_j, W_{ij}; \otimes_{ij} \rangle$, взяв в качестве $\otimes_{ij}$ ограничение операции $\otimes$ на множество $U_i \times V_j$.

Каждый трехосновный группоид $\mathbf{G}_{ij}$ будем называть *ядерным* для эпиморфизма $\langle \mu, \lambda, \eta \rangle$. Множество всех ядерных группоидов гомоморфизма $\langle \mu, \lambda, \eta \rangle$ будем обозначать через $\text{KerGr}\langle \mu, \lambda, \eta \rangle$

Будем также говорить, что трехосновный группоид $\mathbf{G} = \langle U, V, W; \otimes \rangle$ является *расширением* связки Σ_{IJ} при помощи множества $\mathfrak{G}$ *трехосновных группоидов*, если существует такой эпиморфизм вида (4.2), что $\mathfrak{G} = \text{KerGr}\langle \mu, \lambda, \eta \rangle$.

Лемма 4.2. *Трехосновный группоид $\mathbf{G} = \langle U, V, W; \otimes \rangle$ является рисовским тогда и только тогда, когда он является расширением некоторой связки при помощи множества трехосновных квазигрупп.*

Допустим, что группоид $\mathbf{G}$ является рисовским. Тогда существуют такая $I \times J$ -квазигруппа $\mathbf{Q} = \langle Q; \langle *_{ij} | i \in I \times J \rangle \rangle$ и такие взаимно однозначные отображения

$$\alpha: U \rightarrow Q \times I, \beta: V \rightarrow Q \times J, \gamma: W \rightarrow Q \times (I \times J),$$

что тройка $\langle \alpha, \beta, \gamma \rangle$ является изоморфизмом трехосновных группоидов $\mathbf{G}$ и $\mathfrak{R}(\mathbf{Q})$.

Рассмотрим проекции

$$p_I: Q \times I \rightarrow I, p_J: Q \times J \rightarrow J, p_{I \times J}: Q \times (I \times J) \rightarrow (I \times J).$$

Из построений легко следует, что тройка $\langle p_I, p_J, p_{I \times J} \rangle$ является эпиморфизмом трехосновного группоида $\mathfrak{R}(\mathbf{Q})$ на связку Σ_{IJ} . Теперь суперпозиция $\langle \alpha, \beta, \gamma \rangle \langle p_I, p_J, p_{I \times J} \rangle = \langle \alpha p_I, \beta p_J, \gamma p_{I \times J} \rangle$ является эпиморфизмом трехосновного группоида $\mathbf{G}$ на связку Σ_{IJ} .

Рассмотрим произвольные элементы $i \in I, j \in J$ и соответствующий им ядерный группоид $\mathbf{G}_{ij}$. Легко видеть, что его основными множествами являются множества

$$U_i = \langle (q, i) \alpha^{-1} | q \in Q \rangle, \quad V_j = \langle (q, j) \beta^{-1} | q \in Q \rangle, \\ W_{ij} = \langle (q, (i, j)) \gamma^{-1} | q \in Q \rangle.$$

Имеем

$$\begin{aligned} ((q_1, i)\alpha^{-1}) \circledast_{ij} ((q_2, i)\beta^{-1}) &= ((q_1, i)\alpha^{-1}) \circledast ((q_2, i)\beta^{-1}) = \\ &= ((q_1, i) * (q_2, i))\gamma^{-1} = (q_1 *_{ij} q_2, (i, j))\gamma^{-1}, \end{aligned}$$

откуда следует, что группоид $\mathbf{G}_{ij}$ является трехосновной квазигруппой.

Теперь предположим, что существует эпиморфизм (4.2) трехосновного группоида $\mathbf{G} = \langle U, V, W; \circledast \rangle$ на связку Σ_{IJ} , все ядерные группоиды которого являются трехосновными квазигруппами.

Для любых элементов $i_1 \in I, j_1 \in J$ множества $U_{i_1}, V_{j_1}, W_{i_1 j_1}$ являются основными множествами трехосновной квазигруппы. Применив следствие 4.1, получаем, что эти три множества имеют одинаковую мощность. Из произвольности пары (i_1, j_1) следует, что все множества U_i, V_j, W_{ij} ($i \in I, j \in J$) имеют одинаковую мощность.

Выберем какое-либо множество Q , имеющее ту же мощность, и взаимно однозначные отображения $\alpha_i: U_i \rightarrow Q$, $\beta_j: V_j \rightarrow Q$, $\gamma_{ij}: W_{ij} \rightarrow Q$. Применив следствие 4.1, получаем, что существуют такие квазигрупповые операции $*_{ij}$, что

$$u \circledast_{ij} v = ((u\alpha) *_{ij} (v\beta))\gamma^{-1}.$$

Теперь положим

$$u\alpha = (u\alpha_{\mu(u)}, \mu(u)), \quad v\beta = (v\beta_{\lambda(v)}, \lambda(v)), \quad w\gamma = (w\gamma_{\eta(w)}, \eta(w)).$$

Легко проверить, что тройка $\langle \alpha, \beta, \gamma \rangle$ является изоморфизмом трехосновных группоидов $\mathbf{G}$ и $\mathfrak{R}(\mathbf{Q})$. $\square$

Вернемся к рассмотрению отношений эквивалентности на множестве $B \times C$. Пусть θ – нормальное отношение эквивалентности на этом множестве. Тогда в соответствии с теоремами 3.1, 3.2 и двойственным к ним отношения $\mathcal{D}\theta, \mathcal{I}\theta, \mathcal{B}\theta, \mathcal{K}\theta$ являются отношениями эквивалентности.

Лемма 4.3. Пусть θ – нормальное отношение на множестве $B \times C$. Тогда существует такая операция $\circledast^\theta: B/\mathcal{K}\theta \times C/\mathcal{I}\theta \rightarrow B \times C/\theta$, что трехосновный группоид $\mathbf{H}^\theta = \langle B/\mathcal{K}\theta, C/\mathcal{I}\theta, B \times C/\theta; \circledast^\theta \rangle$ является рисовским и

$$((b_1, c_1)\theta(b_2, c_2)) \Leftrightarrow ([b_1]_{\mathcal{K}\theta} \circledast^\theta [c_1]_{\mathcal{I}\theta} = [b_2]_{\mathcal{K}\theta} \circledast^\theta [c_2]_{\mathcal{I}\theta}). \quad (4.3)$$

В силу теоремы 3.2 и двойственного утверждения имеют место включения $\mathcal{K}\theta \times \Delta_C, \Delta_B \times \mathcal{I}\theta \subseteq \theta$. Поэтому

$$(\mathcal{K}\theta \times \mathcal{I}\theta) = (\mathcal{K}\theta \times \Delta_C) \vee (\Delta_B \times \mathcal{I}\theta) \subseteq \theta.$$

Это позволяет определить операцию $\circledast^\theta$ следующим образом:

$$[b]_{\mathcal{K}\theta} \circledast^\theta [c]_{\mathcal{I}\theta} = [(b, c)]_\theta.$$

Очевидно, что для такой операции высказывание (4.3) истинно.

Ясно, что $\mathcal{K}\theta \subseteq \mathcal{D}\theta$. Поэтому существует сюръективное отображение $\mu: B/\mathcal{K}\theta \rightarrow B/\mathcal{D}\theta$, для которого $[b]_{\mathcal{K}\theta} \mu = [b]_{\mathcal{D}\theta}$. Точно так же существует сюръективное отображение $\lambda: C/\mathcal{I}\theta \rightarrow C/\mathcal{B}\theta$, для которого $[c]_{\mathcal{I}\theta} \lambda = [c]_{\mathcal{B}\theta}$.

Из теоремы 3.1 и двойственной к ней следует, что

$$\theta \subseteq \mathcal{D}\theta \times \nabla_C, \quad \theta \subseteq \nabla_B \times \mathcal{B}\theta.$$

Поэтому

$$\theta \subseteq (\mathcal{D}\theta \times \nabla_C) \cap (\nabla_B \times \mathcal{B}\theta) = \mathcal{D}\theta \times \mathcal{B}\theta.$$

Последнее включение позволяет определить сюръективное отображение

$$\eta: B \times C/\theta \rightarrow (B/\mathcal{D}\theta) \times (C/\mathcal{B}\theta),$$

положив

$$[(b, c)]_\theta \eta = ([b]_{\mathcal{D}\theta}, [c]_{\mathcal{B}\theta}).$$

Учитывая определение операции $\circledast^\theta$, последнее равенство можно записать в виде

$$([b]_{\mathcal{K}\theta} \mu, [c]_{\mathcal{I}\theta} \lambda) = (b \circledast^\theta c) \eta.$$

Другими словами, тройка $\langle \mu, \lambda, \eta \rangle$ является эпиморфизмом

$$\langle \mu, \lambda, \eta \rangle: \langle B/\mathcal{K}\theta, C/\mathcal{I}\theta, B \times C/\theta; \circledast^\theta \rangle \rightarrow \langle B/\mathcal{D}\theta, C/\mathcal{B}\theta, (B/\mathcal{D}\theta) \times (C/\mathcal{B}\theta); \times \rangle$$

трехосновных группоидов. Легко видеть, что каждой его ядерный группоид имеет вид $\langle U_P, V_Q, W_{PQ}; *_P \rangle$, где

$$P \in B/\mathcal{D}\theta, Q \in C/\mathcal{B}\theta,$$

$$U_P = \langle [b]_{\mathcal{K}\theta} \mid b \in P \rangle, V_Q = \langle [c]_{\mathcal{I}\theta} \mid c \in Q \rangle, W_{PQ} = \langle [(b, c)]_\theta \mid b \in P, c \in Q \rangle,$$

а операция $*_{PQ}$ есть ограничение операции $\circledast^\theta$ на подмножество $U_P \times V_Q$, т.е.

$$[b]_{\mathcal{K}\theta} *_{PQ} [c]_{\mathcal{I}\theta} = [b]_{\mathcal{K}\theta} \circledast^\theta [c]_{\mathcal{I}\theta} = b \circledast^\theta c = [(b, c)]_\theta. \quad (4.4)$$

Рассмотрим произвольные элементы $b_1, b_2 \in P$, $c_2 \in Q$ и уравнение

$$[b_1]_{\mathcal{K}\theta} *_{PQ} x = [(b_2, c_2)]_\theta,$$

в котором неизвестное принимает значения в множестве V_Q . Из формулы (4.4) следует, что класс $[c_1]_{\mathcal{I}\theta} \in V_Q$ является решением уравнения тогда и только тогда, когда $(b_2, c_2)\theta(b_1, c_1)$.

Так как элементы b_1, b_2 находятся в одном классе отношения $\mathcal{D}\theta$, то $(b_2, b_1) \in \mathcal{D}\theta$. В силу теоремы 3.1 имеем $\mathbf{D}l_{b_2b_1} = C$. Поэтому существует такой элемент $c_1 \in C$, что $(c_2, c_1) \in l_{b_2b_1}^\theta$, что эквивалентно включению $(b_2, c_2)\theta(b_1, c_1)$. Из этого включения следует, что $(c_1, c_2) \in \mathcal{B}\theta$. Поэтому $[c_1]_{\mathcal{I}\theta} \in V_Q$ и класс $[c_1]_{\mathcal{I}\theta}$ является решением рассматриваемого уравнения.

Допустим, что класс $[c'_1]_{\mathcal{I}\theta} \in V_Q$ также является решением. Тогда $(b_2, c_2)\theta(b_1, c'_1)$. В силу транзитивности отношения θ имеет место включение $(b_1, c_1)\theta(b_1, c'_1)$ и, следовательно, $(c_1, c'_1) \in \mathcal{I}\theta$, т.е. $[c_1]_{\mathcal{I}\theta} = [c'_1]_{\mathcal{I}\theta}$.

Двойственным образом показываем, что однозначно разрешимо каждое уравнение вида $y *_{PQ} [c_1]_{\mathcal{I}\theta} = [(b_2, c_2)]_\theta$.

Таким образом, группоид $\langle U_P, V_Q, W_{PQ}; *_{PQ} \rangle$ является трехосновой квазигруппой.

Для завершения доказательства достаточно воспользоваться леммой 4.2. □

Пусть $\langle U, V, W; \circledast \rangle$ – трехосновый группоид, $h: B \rightarrow U, g: C \rightarrow V$ – произвольные отображения. Тогда можно определить отображение $h \circledast g: B \times C \rightarrow W$, положив $(h \circledast g)(b, c) = h(b) \circledast g(c)$.

Теорема 4.1. *Отношение $\theta \in \mathcal{E}(B \times C)$ нормально тогда и только тогда, когда существуют такая $I \times J$ -квазигруппа $\mathbf{Q} = \langle Q; \langle *_{ij} \mid i \in I \times J \rangle \rangle$*

и такие сюръективные отображения $h: B \rightarrow Q \times I, g: C \rightarrow Q \times J$, что отношение θ является ядром отображения $h * g$.

Допустим, что отношение θ нормально. Тогда в силу леммы 4.3 группоид $\mathbf{H}^\theta = \langle B/\kappa_\theta, C/\iota_\theta, B \times C/\theta; \circledast^\theta \rangle$ является рисовским. По определению, существуют $I \times J$ -квазигруппа $\mathbf{Q}$ и изоморфизм $\langle \alpha, \beta, \gamma \rangle: \mathbf{H}^\theta \rightarrow \mathfrak{R}(\mathbf{Q})$. Полагаем

$$h(b) = [b]_{\kappa_\theta} \alpha, \quad g(c) = [c]_{\iota_\theta} \beta.$$

Имеем

$$(h * g)(b, c) = [b]_{\kappa_\theta} \alpha * [c]_{\iota_\theta} \beta = ([b]_{\kappa_\theta} \circledast^\theta [c]_{\iota_\theta}) \gamma.$$

Так как отображение γ взаимно однозначно, то ядра отображений $h * g$ и $[\cdot]_{\kappa_\theta} \circledast^\theta [\cdot]_{\iota_\theta}$ совпадают, и нужное нам равенство $\theta = \ker h * g$ вытекает из формулы (4.3).

Теперь предположим, что существуют $I \times J$ -квазигруппа $\mathbf{Q}$ и отображения h, g , удовлетворяющие условиям теоремы.

По свойствам декартовых произведений существуют такие отображения $h_Q: B \rightarrow Q, h_I: B \rightarrow I, g_Q: C \rightarrow Q, g_J: C \rightarrow J$, что

$$h(b) = (h_Q(b), h_I(b)), \quad g(c) = (g_Q(c), g_J(c)).$$

Имеем

$$\begin{aligned} (h * g)(b, c) &= (h_Q(b), h_I(b)) * (g_Q(c), g_J(c)) = \\ &= (h_Q(b) *_{h_I(b)g_J(c)} g_Q(c), (h_I(b), g_J(c))). \end{aligned}$$

Так как отношение θ является ядром отображения $h * g$, то

$$\begin{aligned} &((b_1, c_1) \theta (b_2, c_2)) \Leftrightarrow \\ &\Leftrightarrow (h_Q(b_1) *_{h_I(b_1)g_J(c_1)} g_Q(c_1) = h_Q(b_2) *_{h_I(b_2)g_J(c_2)} g_Q(c_2)) \& \\ &\& (h_I(b_1) = h_I(b_2)) \& (g_J(c_1) = g_J(c_2)). \end{aligned}$$

Заметим, что истинность или ложность правой части не изменится, если заменить операцию $*_{h_I(b_2)g_J(c_2)}$ операцией $*_{h_I(b_1)g_J(c_1)}$. Поэтому

$$\begin{aligned}
& ((b_1, c_1)\theta(b_2, c_2)) \Leftrightarrow \\
& \Leftrightarrow (h_Q(b_1) *_{h_I(b_1)g_J(c_1)} g_Q(c_1) = h_Q(b_2) *_{h_I(b_1)g_J(c_1)} g_Q(c_2)) \& \quad (4.5) \\
& \& (h_I(b_1) = h_I(b_2)) \& (g_J(c_1) = g_J(c_2)).
\end{aligned}$$

Допустим, что элементы b_1, b_2 выбраны так, что $h_I(b_1) \neq h_I(b_2)$. Тогда высказывание в правой части формулы (4.5) ложно для любых элементов c_1, c_2 . Поэтому высказывание в левой части также ложно при любом выборе элементов c_1, c_2 и $(b_1, b_2) \notin \mathcal{D}\theta$.

Пусть теперь элементы b_1, b_2 выбраны так, что $h_I(b_1) = h_I(b_2)$, а элемент c_1 выбран произвольно. По свойствам квазигрупп существует единственный элемент $q \in Q$, для которого выполняется равенство

$$h_Q(b_1) *_{h_I(b_1)g_J(c_1)} g_Q(c_1) = h_Q(b_2) *_{h_I(b_1)g_J(c_1)} q.$$

В качестве c_2 выберем какой-либо элемент, удовлетворяющий равенству $g(c_2) = (q, g_J(c_1))$. Такой элемент существует ввиду сюръективности отображения g . При таком выборе высказывание в правой части формулы (4.5) истинно. Поэтому истинно и высказывание из левой части формулы. Следовательно, $(b_1, b_2) \in \mathcal{D}\theta$ и $c_1 \in \mathbf{D}l_{b_1 b_2}^\theta$. Так как элемент c_1 выбирался произвольно, то $\mathbf{D}l_{b_1 b_2}^\theta = C$.

Таким образом, выполняется равенство (3.8) и отношение θ перестановочно с отношением ρ_B в силу теоремы 3.1.

Кроме того, мы доказали, что

$$\mathcal{D}\theta = \ker h_I. \quad (4.6)$$

Положим в формуле (4.5) $b_1 = b_2 = b$. Получаем

$$\begin{aligned}
& ((b, c_1)\theta(b, c_2)) \Leftrightarrow \\
& \Leftrightarrow (h_Q(b) *_{h_I(b)g_J(c_1)} g_Q(c_1) = h_Q(b) *_{h_I(b)g_J(c_1)} g_Q(c_2)) \& \\
& \& (g_J(c_1) = g_J(c_2)).
\end{aligned}$$

Из свойств квазигрупп следует, что равенство

$$h_Q(b) *_{h_I(b)g_J(c_1)} g_Q(c_1) = h_Q(b) *_{h_I(b)g_J(c_1)} g_Q(c_2)$$

выполняется тогда и только тогда, когда $g_Q(c_1) = g_Q(c_2)$. Поэтому

$$\begin{aligned} & ((b, c_1)\theta(b, c_2)) \Leftrightarrow \\ & \Leftrightarrow (g_Q(c_1) = g_Q(c_2)) \& (g_J(c_1) = g_J(c_2)) \Leftrightarrow (g(c_1) = g(c_2)). \end{aligned}$$

Теперь из определений следует

$$l_{bb}^\theta = \mathcal{I}\theta = \ker g. \quad (4.7)$$

Так как элемент b произволен, то отношения $\theta \wedge \rho_B$, ρ_C перестановочны в силу теоремы 3.2.

Следовательно, отношение θ нормально слева. Нормальность справа доказывается двойственным образом. $\square$

5. Индуктивное построение GA-решеток

Лемма 5.1. Пусть $\tau \in \mathcal{R}(B), \sigma \in \mathcal{R}(C)$. Тогда отношение $\tau \times \sigma$ является отношением эквивалентности на множестве $B \times C$ тогда и только тогда, когда отношения τ, σ являются отношениями эквивалентности на множествах B и C соответственно.

Пусть $\tau_1, \tau_2 \in \mathcal{E}(B), \sigma_1, \sigma_2 \in \mathcal{E}(C)$. Тогда

$$\begin{aligned} (\tau_1 \times \sigma_1) \cap (\tau_2 \times \sigma_2) &= (\tau_1 \cap \tau_2) \times (\sigma_1 \cap \sigma_2), \\ (\tau_1 \times \sigma_1) \vee (\tau_2 \times \sigma_2) &= (\tau_1 \vee \tau_2) \times (\sigma_1 \vee \sigma_2), \\ (\tau_1 \times \sigma_1) \circ (\tau_2 \times \sigma_2) &= (\tau_1 \circ \tau_2) \times (\sigma_1 \circ \sigma_2). \end{aligned} \quad (5.1)$$

Первое утверждение леммы, а также первое и третье равенства (5.1) легко проверяются. Докажем второе равенство.

Очевидны включения

$$\tau_1 \times \sigma_1 \subseteq (\tau_1 \vee \tau_2) \times (\sigma_1 \vee \sigma_2), \quad \tau_2 \times \sigma_2 \subseteq (\tau_1 \vee \tau_2) \times (\sigma_1 \vee \sigma_2).$$

Поэтому

$$(\tau_1 \times \sigma_1) \vee (\tau_2 \times \sigma_2) \subseteq (\tau_1 \vee \tau_2) \times (\sigma_1 \vee \sigma_2),$$

и нам нужно лишь доказать обратное включение.

Пусть $(b_1, b_2) \in (\tau_1 \vee \tau_2)$, $(c_1, c_2) \in (\sigma_1 \vee \sigma_2)$. Тогда существуют такие элементы $u_0, u_1, \dots, u_{2k} \in B$, что

$$b_1 = u_0, (u_{2i}, u_{2i+1}) \in \tau_1, (u_{2i+1}, u_{2(i+1)}) \in \tau_2, u_{2k} = b_2.$$

Имеем

$$\begin{aligned}(b_1, c_1) &= (u_0, c_1), ((u_{2i}, c_1), (u_{2i+1}, c_1)) \in \tau_1 \times \sigma_1, \\ ((u_{2i+1}, c_1), (u_{2(i+1)}, c_1)) &\in \tau_2 \times \sigma_2, (u_{2k}, c_1) = (b_2, c_1).\end{aligned}$$

Поэтому

$$((b_1, c_1), (b_2, c_1)) \in (\tau_1 \times \sigma_1) \vee (\tau_2 \times \sigma_2).$$

Аналогично показываем, что

$$((b_2, c_1), (b_2, c_2)) \in (\tau_1 \times \sigma_1) \vee (\tau_2 \times \sigma_2),$$

что в силу произвольности рассматриваемых элементов дает нужное нам включение. $\square$

Выберем и фиксируем перестановочную решетку $\mathbf{L}_{B \times C} \subseteq \mathcal{E}(B \times C)$, содержащую отношения ρ_B и ρ_C . Полагаем

$$\mathbf{L}_B = \langle \tau \in \mathcal{E}(B) \mid \tau \times \Delta_C \in \mathbf{L}_{B \times C} \rangle,$$

$$\mathbf{L}_C = \langle \sigma \in \mathcal{E}(C) \mid \Delta_B \times \sigma \in \mathbf{L}_{B \times C} \rangle.$$

Будем называть эти множества *следами* решетки $\mathbf{L}_{B \times C}$ в решетках $\mathcal{E}(B)$ и $\mathcal{E}(C)$.

Следствие 5.1. *Справедливы следующие утверждения:*

1. Множества $\mathbf{L}_B, \mathbf{L}_C$ являются перестановочными решетками отношений эквивалентности на множествах B и C соответственно.
2. Если $\tau \in \mathcal{E}(B), \sigma \in \mathcal{E}(C)$, то $\tau \times \sigma \in \mathbf{L}_{B \times C}$ тогда и только тогда, когда $\tau \in \mathbf{L}_B$ и $\sigma \in \mathbf{L}_C$.
3. $\Delta_B, \nabla_B \in \mathbf{L}_B$, $\Delta_C, \nabla_C \in \mathbf{L}_C$.
4. Если $\theta \in \mathbf{L}_{B \times C}$, то $\mathcal{D}\theta, \mathcal{K}\theta \in \mathbf{L}_B$, $\mathcal{B}\theta, \mathcal{I}\theta \in \mathbf{L}_B$.

Первое утверждение вытекает из равенств (5.1).

Пусть $\tau \times \sigma \in \mathbf{L}_{B \times C}$. Тогда $\Delta_B \times \sigma = (\tau \times \sigma) \wedge \rho_B \in \mathbf{L}_{B \times C}$ и $\sigma \in \mathbf{L}_C$. Аналогично показываем, что $\tau \in \mathbf{L}_B$. Пусть теперь $\tau \in \mathbf{L}_B$ и $\sigma \in \mathbf{L}_C$. Тогда $\tau \times \sigma = (\tau \times \Delta_C) \vee (\Delta_B \times \sigma) \in \mathbf{L}_{B \times C}$, что завершает доказательство утверждения 2.

По условию $\Delta_B \times \nabla_C = \rho_B \in \mathbf{L}_{B \times C}$. Теперь включения $\Delta_B \in \mathbf{L}_B$, $\nabla_C \in \mathbf{L}_C$ вытекают из утверждения 2. Включения $\nabla_B \in \mathbf{L}_B$, $\Delta_C \in \mathbf{L}_C$ доказываются аналогично.

Теорема 3.1 показывает, что $\theta \vee \rho_B = \mathcal{D}\theta \times \nabla_C$. В наших условиях элемент $\theta \vee \rho_B$ принадлежит решетке $\mathbf{L}_{B \times C}$. Поэтому $\mathcal{D}\theta \times \nabla_C \in \mathbf{L}_{B \times C}$, откуда следует, что $\mathcal{D}\theta \in \mathbf{L}_B$. Равенство, двойственное равенству (3.10), показывает, что $\mathcal{K}\theta = \mathcal{D}(\theta \wedge \rho_C)$. Поэтому $\mathcal{K}\theta \in \mathbf{L}_B$.

Двойственным образом показываем, что $\mathcal{B}\theta \in \mathbf{L}_C$ и $\mathcal{I}\theta \in \mathbf{L}_C$. $\square$

Следствие 5.2. Пусть $\mathbf{L}_n$ – GA-решетка отношений эквивалентности на множестве $\prod_{i=1}^n A_i$, $\mathbf{L}_{n-1}, \mathbf{L}_{A_n}$ – следы решетки $\mathbf{L}_n$ в $\mathcal{E}\left(\prod_{i=1}^{n-1} A_i\right)$ и $\mathcal{E}(A_n)$ соответственно. Тогда решетка $\mathbf{L}_{n-1}$ является GA-решеткой и $\mathbf{L}_{A_n} = \{\Delta_{A_n}, \nabla_{A_n}\}$.

Ядро проекции $\prod_{i=1}^m A_i \rightarrow A_j$ обозначим через ρ_j^m . Легко видеть, что если $j < n$, то $\rho_j^n = \rho_j^{n-1} \times \nabla_{A_n}$, и из следствия 5.1 вытекает, что $\rho_j^{n-1} \in \mathbf{L}_{n-1}$.

Допустим, что отношение ρ_j^{n-1} не является коатомом решетки $\mathbf{L}_{n-1}$. Ясно, что $\rho_j^{n-1} \neq \nabla_{\prod_{i=1}^{n-1} A_i}$. Поэтому существует такой элемент $\sigma \in \mathbf{L}_{n-1}$, что $\rho_j^{n-1} \subset \sigma \subset \nabla_{\prod_{i=1}^{n-1} A_i}$. Тогда

$$\rho_j^n = \rho_j^{n-1} \times \nabla_{A_n} \subset \sigma \times \nabla_{A_n} \subset \nabla_{\prod_{i=1}^{n-1} A_i} \times \nabla_{A_{k+1}} = \nabla_{\prod_{i=1}^n A_i},$$

что невозможно, поскольку элемент ρ_j^n является коатомом решетки $\mathbf{L}_n$.

Отсюда и из следствия 5.1 вытекает, что решетка $\mathbf{L}_{n-1}$ является GA-решеткой.

Теперь рассмотрим произвольный элемент $\sigma \in \mathbf{L}_{A_n}$. Тогда

$$\rho_n^n = \nabla_{\prod_{i=1}^{n-1} A_i} \times \Delta_{A_n} \subseteq \nabla_{\prod_{i=1}^{n-1} A_i} \times \sigma \subseteq \nabla_{\prod_{i=1}^{n-1} A_i} \times \nabla_{A_{k+1}} = \nabla_{\prod_{i=1}^n A_i}.$$

Так как проекция ρ_n^n является коатомом, то одно из включений в этой цепочке является равенством, т.е. либо $\Delta_{A_n} = \sigma$, либо $\sigma = \nabla_{A_{k+1}}$. $\square$

Следствие 5.2 можно применить к решетке L_{n-1} , что дает возможность построить GA -решетку L_{n-2} . Продолжая, получим последовательность $L_{n-3}, \dots, L_1$ GA -решеток.

Это приводит к индуктивному методу построения GA -решеток. В этом методе мы последовательно строим решетки $L_1, L_2, \dots, L_n$. Если решетка L_k уже построена, то для построения решетки L_{k+1} нужно указать множество M_{k+1} коатомов решетки L_{k+1} . Поэтому необходимо знать какие отношения могут быть коатомами GA -решеток.

Лемма 5.2. Пусть $\theta, \sigma \in L_{B \times C}$ – нормальные отношения эквивалентности на множестве $B \times C$ и $\theta \subset \sigma$. Тогда

$$\mathcal{D}\theta \subseteq \mathcal{D}\sigma, \quad \mathcal{I}\theta \subseteq \mathcal{I}\sigma, \quad (5.2)$$

причем хотя бы одно из включений является строгим.

Справедливость включений (5.2) вытекает из определений, и нам нужно лишь доказать, что оба включения не могут быть равенствами. Для этого предположим обратное и рассмотрим произвольный элемент

$$((b_1, c_1), (b_2, c_2)) \in \sigma. \quad (5.3)$$

По определению, $(b_1, b_2) \in \mathcal{D}\sigma$. Поэтому $(b_1, b_2) \in \mathcal{D}\theta$ в силу сделанного предположения. Применив теорему 3.1, получаем, что существует элемент $c \in C$, удовлетворяющий включению

$$((b_1, c_1), (b_2, c)) \in \theta. \quad (5.4)$$

Так как $\theta \subset \sigma$, то $((b_1, c_1), (b_2, c)) \in \sigma$. Отсюда и из включения (5.3) следует включение $((b_2, c_2), (b_2, c)) \in \sigma$. По определению, $(c_2, c) \in \mathcal{I}\sigma$. При сделанном предположении $(c_2, c) \in \mathcal{I}\theta$ и $((b_2, c_2), (b_2, c)) \in \Delta_B \times \mathcal{I}\theta$. Применив теорему 3.2, получаем $((b_2, c_2), (b_2, c)) \in \theta$. Отсюда и из включения (5.4) следует, что $((b_1, c_1), (b_2, c_2)) \in \theta$. Таким образом, $\sigma \subseteq \theta$, что противоречит условию леммы.

□

Следствие 5.3. Элемент θ является коатомом решетки $L_{B \times C}$ тогда и только тогда, когда выполняется одно из двух следующих условий:

1. Отношение $\mathcal{D}\theta$ является коатомом решетки L_B и $\mathcal{I}\theta = \nabla_C$.
2. Отношение $\mathcal{I}\theta$ является коатомом решетки L_C и $\mathcal{D}\theta = \nabla_B$.

Предположим, что условие 1 выполняется, но элемент θ не является коатомом. Тогда либо $\theta = \nabla_{B \times C}$, либо существует такой элемент $\sigma \in \mathbf{L}_{B \times C}$, что $\theta \subset \sigma \subset \nabla_{B \times C}$.

В первом случае имеем $\mathcal{D}\theta = \mathcal{D}\nabla_{B \times C} = \nabla_C$, что противоречит сделанному предположению. Во втором случае имеем

$$\nabla_C = \mathcal{I}\theta \subseteq \mathcal{I}\sigma \subseteq \mathcal{I}\nabla_{B \times C} = \nabla_C.$$

Отсюда и из леммы 5.2 следует, что $\mathcal{D}\theta \subset \mathcal{D}\sigma \subset \mathcal{D}\nabla_{B \times C} = \nabla_C$, что опять же противоречит условию 1.

Таким образом, элемент θ , удовлетворяющий условию 1, является коатомом.

Аналогично показываем, что элемент θ , удовлетворяющий условию 2, является коатомом.

Теперь предположим, что элемент θ является коатомом, но ни условие 1, ни условие 2 не выполняются.

Применив теорему 3.1, получаем, что

$$\theta \subseteq \theta \vee \rho_B = \mathcal{D}\theta \times \nabla_C \subseteq \nabla_{B \times C}.$$

Так как $\theta \neq \nabla_{B \times C}$, то включения в цепочке не могут быть одновременно равенствами. Из определения коатома следует, что оба включения также не могут быть одновременно строгими. Таким образом, либо

$$\theta \subset \mathcal{D}\theta \times \nabla_C = \nabla_{B \times C}, \quad (5.5)$$

либо

$$\theta = \mathcal{D}\theta \times \nabla_C \subset \nabla_{B \times C}. \quad (5.6)$$

Допустим, что имеет место цепочка (5.5). Тогда $\mathcal{D}\theta = \nabla_B$. Так как условие 2 не выполняется, то отношение $\mathcal{I}\theta$ не является коатомом. Из неравенства (5.5) и леммы 5.2 следует, что $\mathcal{I}\theta \subset \mathcal{I}\nabla_{B \times C} = \nabla_C$. Следовательно, существует такой элемент $\sigma \in \mathbf{L}_C$, что $\mathcal{I}\theta \subset \sigma \subset \nabla_C$.

Так как элементы θ и $\Delta_B \times \sigma$ перестановочны, то в силу леммы 1.1 выполняется равенство $\theta \vee (\Delta_B \times \sigma) = \theta \circ (\Delta_B \times \sigma)$ и

$$\begin{aligned} \mathcal{I}(\theta \vee (\Delta_B \times \sigma)) &= \mathcal{I}(\theta \circ (\Delta_B \times \sigma)) = \\ &= \langle c_1, c_2 \in C \mid \exists b_1 \in B ((b_1, c_1), (b_1, c_2)) \in \theta \circ (\Delta_B \times \sigma) \rangle = \\ &= \langle c_1, c_2 \in C \mid \exists b_1, b_2 \in B, c \in C ((b_1, c_1) \theta (b_2, c)) \& ((b_2, c)(b_1, c_2) \in (\Delta_B \times \sigma)) \rangle. \end{aligned}$$

По определению

$$((b_2, c)(b_1, c_2) \in (\Delta_B \times \sigma)) \Leftrightarrow (b_2 = b_1) \& (c \sigma c_2).$$

Поэтому

$$\begin{aligned} \mathcal{I}(\theta \vee (\Delta_B \times \sigma)) &= \langle c_1, c_2 \in C \mid \exists b_1 \in B, c \in C ((b_1, c_1)\theta(b_1, c)) \& (c\sigma c_2) \rangle = \\ &= \langle c_1, c_2 \in C \mid \exists bc \in C ((c_1, c) \in \mathcal{I}\theta) \& ((c, c_2) \in \sigma) \rangle = \mathcal{I}\theta \circ \sigma. \end{aligned}$$

Так как $\mathcal{I}\theta \subseteq \sigma$, то $\mathcal{I}\theta \circ \sigma = \sigma$ и окончательно имеем $\mathcal{I}(\theta \vee (\Delta_B \times \sigma)) = \sigma$.

Очевидно, что

$$\theta \subseteq (\theta \vee (\Delta_B \times \sigma)) \subseteq \nabla_{B \times C}. \quad (5.7)$$

Так как

$$\mathcal{I}\theta \subset \sigma = \mathcal{I}(\theta \vee (\Delta_B \times \sigma)) \subset \nabla_C = \mathcal{I}\nabla_{B \times C},$$

то оба включения в цепочке (5.7) строгие, что противоречит сделанному предположению.

Теперь предположим, что справедливо высказывание (5.6). Из него следует, что $\mathcal{D}\theta \subset \nabla_B$ и что $\mathcal{I}\theta = \mathcal{I}(\mathcal{D}\theta \times \nabla_C) = \nabla_C$. Так как условие 1 не выполняется, то отношение $\mathcal{D}\theta$ не является коатомом, и существует такой элемент $\tau \in \mathbf{L}_B$, что $\mathcal{D}\theta \subset \tau \subset \nabla_B$. Имеем

$$\theta = \mathcal{D}\theta \times \nabla_C \subset \tau \times \nabla_C \subset \nabla_B \times \nabla_C,$$

что противоречит сделанным предположениям. $\square$

Теорема 5.1. Пусть $\mathbf{L}_{B \times C}$ – перестановочная решетка отношений эквивалентности на множестве $B \times C$, $\rho_B, \rho_C \in \mathbf{L}_{B \times C}$, $\mathbf{L}_B, \mathbf{L}_C$ – ее проекции на множества. Тогда элемент $\theta \in \mathbf{L}_{B \times C}$ является коатомом решетки $\mathbf{L}_{B \times C}$ в том и только том случае, когда выполняется одно из трех следующих условий:

- $\theta = \nabla_B \times \sigma$, где σ – коатом решетки $\mathbf{L}_C$.
- $\theta = \tau \times \nabla_C$, где τ – коатом решетки $\mathbf{L}_B$.
- Существуют такая квазигруппа $\langle Q; * \rangle$ и такие сюръективные отображения $f: B \rightarrow Q$, $g: C \rightarrow Q$, что ядра $\ker f, \ker g$ являются коатомами решеток $\mathbf{L}_B, \mathbf{L}_C$, отношение θ является ядром отображения $f * g$, определенного следующим образом: $(f * g)(b, c) = f(b) * g(c)$.

Заметим, что $\mathcal{D}(\tau \times \sigma) = \tau$, $\mathcal{I}(\tau \times \sigma) = \sigma$. Отсюда и из следствия 5.3 следует, что элемент $\theta \in \mathbf{L}_{B \times C}$ удовлетворяет одному из условий а), б) тогда и только тогда, когда он принадлежит множеству $\mathbf{L}_B \times \mathbf{L}_C$ и является коатомом решетки $\mathbf{L}_{B \times C}$.

Предположим, что элемент θ удовлетворяет условию с). Из равенств (4.6) и (4.7) следует, что $\mathcal{D}\theta = \nabla_B$ и $\mathcal{I}\theta = \ker g$. Теперь из следствия 5.3 вытекает, что элемент θ является коатомом.

Пусть теперь θ – коатом решетки $\mathbf{L}_{B \times C}$, не принадлежащий множеству $\mathbf{L}_B \times \mathbf{L}_C$. В этих условиях цепочка включений (5.6) невозможна и справедливо высказывание (5.5). Из доказательства следствия 5.3 следует, что в рассматриваемом случае $\mathcal{D}\theta = \nabla_B$, а отношение $\mathcal{I}\theta$ является коатомом решетки $\mathbf{L}_C$. Двойственным образом показываем, что $\mathcal{B}\theta = \nabla_C$, а отношение $\mathcal{K}\theta$ является коатомом решетки $\mathbf{L}_B$.

В силу теоремы 4.1 отношение θ является ядром отображения $h * g$, где $h: B \rightarrow Q \times I, g: C \rightarrow Q \times J$ сюръективные отображения на основные множества группоида $\mathfrak{A}(\mathbf{Q})$. Так же, как при доказательстве теоремы 4.1, определяем отображения h_Q, h_I, g_Q, g_J .

Из сюръективности отображения h , формулы (4.6) и равенства $\mathcal{D}\theta = \nabla_B$ следует, что мощность множества I равна 1. Можно считать, что $I = \{1\}$. В этом случае $h(b) = (h_Q(b), 1)$. Двойственным образом показываем, что $J = \{1\}$ и $g(c) = (g_Q(c), 1)$.

Очевидно, что $\ker g_Q = \ker g$. Применив формулу (4.7), получаем, что $\ker g_Q = \mathcal{I}\theta$ и, следовательно, это ядро является коатомом решетки $\mathbf{L}_C$. Двойственным образом, показываем, что $\ker h_Q$ является коатомом решетки $\mathbf{L}_B$.

Отображения h_Q и g_Q являются отображениями множеств B и C соответственно в квазигруппу $\langle Q; *_{11} \rangle$, что позволяет рассмотреть отображение $h_Q *_{11} g_Q$. Ясно, что

$$(h * g)(b, c) = (h_Q(b) *_{11} g_Q(c), (1, 1)).$$

Из этого равенства следует $\ker h * g = \ker h_Q *_{11} g_Q$ и $\theta = \ker h_Q *_{11} g_Q$, т.е. условие с) справедливо. $\square$

Теорема 5.2. Пусть $\mathbf{L}_n$ – GA-решетка отношений эквивалентности на множестве $\prod_{i=1}^n A_i$, $\mathbf{L}_{n-1}, \mathbf{L}_{A_n}$ – следы решетки $\mathbf{L}_n$ в $\mathcal{E}\left(\prod_{i=1}^{n-1} A_i\right)$ и

$\mathcal{E}(A_n)$ соответственно. Тогда элемент $\theta \in L_n$ является коатомом решетки L_n в том и только том случае, когда выполняется одно из трех следующих условий:

a) $\theta = \tau \times \nabla_{A_n}$, где τ – коатом решетки L_{n-1} .

b) θ есть ядро проекции $\prod_{i=1}^n A_i \rightarrow A_n$.

c) Существуют такая квазигрупповая операция $\otimes$ на множестве A_n и такое сюръективное отображение $h: \prod_{i=1}^{n-1} A_i \rightarrow A_n$, что ядро $\ker f$ является коатомом решетки L_{n-1} , а отношение θ является ядром отображения $h^{\otimes}$, определенного следующим образом: $h^{\otimes}(a_1, \dots, a_n) = h(a_1, \dots, a_{n-1}) \otimes a_n$.

Из следствия 5.2 вытекает, что единственным коатомом решетки L_{A_n} является элемент Δ_{A_n} . Теперь условия a), b) для рассматриваемого случая эквивалентны соответствующим условиям теоремы 5.1.

Покажем, что то же самое верно и для условия c).

Рассмотрим какую-либо квазигруппу $\langle Q; * \rangle$ и такие сюръективные

отображения $f: \prod_{i=1}^{n-1} A_i \rightarrow Q$, $g: A_n \rightarrow Q$, что $\ker g$ – коатом решетки L_{A_n} .

В рассматриваемых условиях имеем $\ker g = \Delta_{A_n}$. Отсюда следует, что отображение g взаимно однозначно.

Введем на множестве A_n операцию $\otimes$, положив

$$a \otimes b = g^{-1}(g(a) * g(b)).$$

Также положим

$$h(a_1, \dots, a_{n-1}) = g^{-1}f(a_1, \dots, a_{n-1}).$$

Легко видеть, что

$$\ker h = \ker f, \quad \ker h^{\otimes} = \ker(f * g) = \theta,$$

что и доказывает эквивалентность условия c) и соответствующего условия теоремы 5.1. $\square$

Следствие 5.4. Пусть $\mathbf{L}_A$ – GA-решетка отношений эквивалентности на множестве $A = \prod_{i=1}^n A_i$. Тогда существует такая GA-решетка

$\mathbf{L}_{A'}$ отношений эквивалентности на множестве $A' = \prod_{i=1}^{n-1} A_i$, что каждая

система из класса $\mathcal{F}(A; \mathbf{L}_A)$ разлагается на подсистему, принадлежащую классу $\mathcal{F}(A'; \mathbf{L}_{A'})$, и подсистему, состоящую из уравнений вида $\sigma(x_n) = b$ для подходящей перестановки σ множества A_n и вида

$$f(x_1, \dots, x_k) \otimes x_{k+1} = b,$$

где f – сюръективное отображение $f: A' \rightarrow A_n$, ядро которого является коатомом решетки $\mathbf{L}_{A'}$, а $\otimes$ – квазигрупповая операция на множестве A_n .

Утверждение вытекает из определений и теоремы 5.2. $\square$

В дальнейшем мы предполагаем выделить среди описанных систем уравнений просто решаемые.

Список литературы

1. Белоусов В.Д. Основы теории квазигрупп и луп. – М. : Наука, 1967.
2. 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.
3. Гретцер Г. Общая теория решеток. – М. : "Мир", 1982.
4. Кон П. Универсальная алгебра. – М. : "Мир", 1968.
5. Курош А.Г. Лекции по общей алгебре. – М. : "Наука", 1973.
6. Полин С. В. Системы уравнений и решетки конгруэнций универсальных алгебр // Математические вопросы криптографии. – 2013. – Т. 4, № 4. – С. 109-144.