Записки научных
семинаров ПОМИ
Том 305, 2003 г.

Л. Н. Ерофеева

ОБ ОДНОМ КЛАССЕ ГРУППОИДОВ

В теории квазигрупп ([1]) одним из замечательных классов является класс леводистрибутивных квазигрупп. В такой квазигруппе $G(\circ)$ по определению выполнено тождество $x \circ (y \circ z) = (x \circ y) \circ (x \circ z)$. Изучение леводистрибутивных квазигрупп, как это показано в ([2]), сводится к изучению так называемых φ-групп, что позволяет построить весьма содержательную теорию упомянутых квазигрупп. По определению, φ-группа – это группа Π с автоморфизмом φ таким, что выполняется требование:

$$x\varphi(x^{-1}) \in sTs^{-1} \Rightarrow x \in T. \tag{1}$$

Здесь $s \in \Pi$, а T – подгруппа φ-неподвижных элементов. Условие (1) будем называть φ-свойством. Очевидный интерес представляет следующее ослабление (1). Именно, потребуем выполнения условия

$$x\varphi(x^{-1}) \in T \Rightarrow x \in T \tag{2}$$

В этой работе описывается неассоциативная структура, связанная с группами этого типа. Это L-группоиды, определение и ряд свойств которых рассматривается ниже.

Изучение L-группоидов оправдано не только эстетическими соображениями (замена (1) на (2)), но также и тем, что такие группоиды встречаются в качестве полных характеристик в топологии узлов ([3]).

1.

Определение. L-группоид $G(\circ)$ есть множество G с бинарной операцией $(\circ)$, для которой выполнены следующие аксиомы:

A1: $x \circ (y \circ z) = (x \circ y) \circ (x \circ z)$ для $\forall x, y, z \in G$,

A2: $a \circ x = b$ однозначно разрешимо в G для $\forall a, b \in G$,

A3: $x \circ a = a$ однозначно разрешимо в G для $\forall a \in G$.

Таким образом, аксиоматика L-группоидов отличается от аксиоматики леводистрибутивных квазигрупп лишь в одном пункте: в квазигруппе A3 заменяется более сильным требованием однозначной разрешимости уравнения $x \circ a = b$.

Решение уравнения в A3 описывается следующим образом.

Предложение 1. *В L-группоиде $G(\circ)$ из $x\circ a = a$ следует $x = a$, для $\forall a \in G$, т.е. в L-группоиде выполнено свойство идемпотентности.*

Доказательство. Равенство $x \circ a = a$ влечет $a \circ (x \circ a) = a \circ a$. Согласно A1 $a\circ(x\circ a) = (a\circ x)\circ(a\circ a)$, следовательно $(a\circ x)\circ(a\circ a) = a\circ a$. С другой стороны, $x\circ(a\circ a) = (x\circ a)\circ(x\circ a) = a\circ a$, тогда в силу A3 $x = a\circ x$. Далее, $x\circ(x\circ a) = (x\circ x)\circ(x\circ a)$, т.е. $x\circ(x\circ a) = (x\circ x)\circ a$, но $x \circ (x \circ a) = x \circ a = a$, следовательно $x \circ x = x$. Вместе с $x = a \circ x$ это дает $x \circ x = a \circ x = x$, тогда в силу A3 $x = a$.

Левые трансляции $L_a = (x \to a\circ x | a, x \in G)$ в силу A1 и A2 являются автоморфизмами $G(\circ)$ и порождают группу $Z(G)$ – группу левых трансляций. Она является подгруппой в Aut – группе всех автоморфизмов G.

Отметим некоторые свойства левых трансляций.

Предложение 2. *Для любых $a, b \in G$ и $u \in \mathrm{Aut}\, G$ имеют место равенства $L_{a\circ b} = L_a L_b L_a^{-1}$, $uL_a u^{-1} = L_{u(a)}$.*

Доказательство. Тождество $a \circ (b \circ x) = (a \circ b) \circ (a \circ x)$, очевидно, можно записать как $L_a L_b = L_{a\circ b} L_a$, что дает первое из равенств. Второе следует из определения автоморфизма: $u(a \circ x) = u(a) \circ u(x) \Leftrightarrow uL_a = L_{u(a)}u$.

Предложение 3. *Элемент $a \in G$ однозначно определяется соответствующей трансляцией L_a.*

Доказательство. Надо показать, что из $L_a = L_b$ следует $a = b$. Действительно, $L_a = L_b$ влечет $a\circ x = b\circ x$ при $\forall x \in G$. Взяв $x = a$, получаем $a \circ a = b \circ a$. Идемпотентность и аксиома A3 дают $a = b$.

Предложение 4. *Группа левых трансляций $Z(G)$ является нормальным делителем в группе $\mathrm{Aut}\, G$. Множество левых трансляций $\{L_a | a \in G\}$ есть объединение некоторых классов сопряженности в $\mathrm{Aut}\, G$.*

Доказательство. Из $uL_a u^{-1} = L_{u(a)}$ следует, что сопряжение множества $\{L_a | a \in G\}$ элементом $u \in \mathrm{Aut}\, G$ переводит это множество в себя, что доказывает, что множество $\{L_a | a \in G\}$ есть объединение некоторых классов сопряженности в $\mathrm{Aut}\, G$. Поскольку $Z(G)$ порождается этим множеством, то и $Z(G)$ инвариантно при сопряжении, т.е. $Z(G)$ – нормальный делитель в $\mathrm{Aut}\, G$.

В формулировке предложения 4 группу $\mathrm{Aut}\,G$ можно заменить любой ее подгруппой, содержащей $Z(G)$. Рассуждения остаются прежними. В частности, левые трансляции составляют объединение некоторых классов сопряженности и в $Z(G)$. Фундаментальное отличие L-группоидов от леводистрибутивных квазигрупп, осложняющее изучение первых, состоит в том, что в квазигруппах $\{L_a|a \in G\}$ составляет ровно один класс сопряженности. Действительно, согласно предложению 2, $L_aL_bL_a^{-1} = L_c$ при $c = a \circ b$. В квазигруппах b по заданным a и c определяется однозначно. Следующий пример показывает, что в L-группоидах ситуация может быть иной.

Пусть $G = \mathbb{Z}$, а $x \circ y = 2x - y$. Аксиомы A1–A3 проверяются тривиально. Далее, $L_a = \{x \to 2a - x\}$ и $L_a^2 = 1$. Следовательно, элементы $Z(G)$ есть произведения вида $L_{a_1}L_{a_2}\ldots L_{a_k}$. Это подстановки вида $u = x \to 2a \pm x$ (верхний знак соответствует четному числу сомножителей, а нижний – нечетному). Класс L_b состоит из элементов вида uL_bu^{-1}. Легко подсчитать, что это элементы вида L_{2s+b}.

Ясно, что класс L_0 не совпадает с классом L_1, следовательно, $\{L_b\}$ составляет два класса сопряженности в группе $Z(G)$, хотя, можно проверить, что в $\mathrm{Aut}\,G$ множество $\{L_a\}$ образует все же один класс.

Если $H \subset \mathrm{Aut}\,G$ – подгруппа, содержащая $Z(G)$, то условие, что $\{L_a|a \in G\}$ составляет один класс сопряженности в H означает, что H транзитивно действует на G. Приведенный пример показывает, что L-группоид не обязан быть $Z(G)$-транзитивным. При конструировании примеров L-группоидов автору не удалось найти нетранзитивные группоиды относительно $\mathrm{Aut}\,G$ и, что более интересно, конечные нетранзитивные группоиды относительно $Z(G)$. Возможно таковые и не существуют. Во всяком случае, оправдано следующее

Определение. L-группоид $G(\circ)$ называется транзитивным, если он $Z(G)$-транзитивен.

Как уже отмечалось, это определение эквивалентно тому, что в $G(\circ)$ левые трансляции образуют один класс сопряженности в $Z(G)$. В частности, квазигрупповая структура на L-группоиде обеспечивает его транзитивность. Если группоид нетранзитивен, то множество элементов распадается на непересекающиеся подмножества – орбиты – относительно действия $Z(G)$.

Предложение 5. *Пусть $|G| > 1$. Тогда каждая орбита в $G(\circ)$ относительно действия $Z(G)$ является подгруппоидом и содержит более одного элемента.*

Доказательство. Пусть $H \subset G$ – орбита. Левая трансляция L_a переводит H в себя, т.е. $a \circ h \in H$ для $h \in H$. В частности, $h_1 \circ h_2 \in H$ для $\forall h_1, h_2 \in H$. Аксиомы A1 и A3 в H выполняются очевидным образом. Более того, поскольку L_a – биекция на G, то биекцией является и ее ограничение на орбиту. Но это означает, что $a \circ x = b$ однозначно разрешимо в H для $b \in H$, т.е. выполняется и аксиома A2. Наконец, если бы H состояла из одного элемента h, то было бы $a \circ h = h$ для $\forall a \in G$, что противоречит аксиоме A3.

2. В этом пункте мы изучим связь L-группоидов с однородными пространствами. Под однородным пространством понимается множество смежных классов группы по некоторой ее подгруппе. Пусть Π – группа с выделенным автоморфизмом φ, $T = \{x \in \Pi | \varphi(x) = x\} \subset \Pi$ – подгруппа φ-неподвижных элементов. Следующая теорема показывает, как можно на множестве левых смежных классов ввести структуру L-группоида.

Теорема 1. *Зададим на $G = \Pi/T$ операцию $\circ$, полагая $x \circ y = x\varphi(x^{-1}y) \mod T$. Тогда G превращается в L-группоид тогда и только тогда, когда в Π выполнено ослабленное φ-свойство (2).*

Доказательство. Легко видеть, что бинарная операция определена корректно, т.е. не зависит от выбора представителей x, y левых смежных классов.

Пусть G – L-группоид. Рассмотрим $x \in \Pi$ такой, что $x\varphi(x^{-1}) \in T$, тогда $x\varphi(x^{-1}1) = 1 \mod T$, т.е. $x \circ 1 = 1$, а значит в силу аксиомы A3 и идемпотентности $x = 1 \mod T \Rightarrow x \in T$. Таким образом, ослабленное φ-свойство выполняется. Обратно, пусть ослабленное φ-свойство выполнено. Аксиомы A1 и A2 легко проверяются непосредственно. Остается показать, что уравнение $x \circ a = a$ разрешимо, причем единственным образом.

$x \circ a = x\varphi(x^{-1}a) = a \mod T$,

$a^{-1}x\varphi(x^{-1}a) = 1 \mod T$,

$a^{-1}x\varphi(x^{-1}a) \in T$.

Обозначим $a^{-1}x$ через t, запишем последнее включение в виде $t\varphi(t^{-1}) \in T$, откуда $t \in T$, т.е. $a^{-1}x \in T$ и $x = at = a \mod T$, что доказывает однозначную разрешимость уравнения $x \circ a = a$.

Для квазигрупп связь с однородными пространствами обратима, т.е. каждую леводистрибутивную квазигруппу можно представить однородным пространством способом, указанным выше. Для L-группоидов это проблематично. Однако имеет место следующая

Теорема 2. *Пусть $G(\circ)$ – L-группоид, $\Pi \subset \operatorname{Aut} G$ – транзитивно действующая на G подгруппа, инвариантная при сопряжении фиксированной трансляцией $L_e (e \in G)$. Определим на Π автоморфизм φ с помощью L_e : $\varphi(u) = L_e u L_e^{-1}$. Тогда $G(\circ) \cong \Pi/T$, где правая часть есть множество смежных классов Π по подгруппе T φ-неподвижных элементов. Бинарная операция на Π/T определяется равенством $x \circ y = x\varphi(x^{-1}y) \mod T$.*

Доказательство. Нетрудно видеть, что автоморфизмы класса из Π/T переводят e в один и тот же элемент из G, который сопоставим этому классу. Достаточно проверить, что если $\forall u, \nu \in \Pi$ переводят e в $a, b \in G$, то $u\varphi(u^{-1}\nu)$ переводит e в $a \circ b$, т.е. $uL_e u^{-1} \nu L_e^{-1}(e) = a \circ b$ при $u(e) = a$, $\nu(e) = b$.

Имеем, $L_e(e) = e \circ e = e$, а значит $uL_e^{-1}(e) = a$, $\nu L_e^{-1}(e) = \nu(e) = b$, следовательно $uL_e u^{-1} \nu L_e^{-1}(e) = uL_e u^{-1}(b)$. Но $uL_e u^{-1} = L_{u(e)} = L_a$, т.е. $uL_e u^{-1}(b) = L_a(b) = a \circ b$.

Представление L-группоида однородным пространством (если оно возможно) неоднозначно. Для квазигрупп этот вопрос полностью изучен в [2]. Нам понадобится одна из теорем редукции, рассмотренная в [2], которая верна и для L-группоидов.

Предложение 6. *Если $G \cong \Pi/T$ – представление L-группоида $G(\circ)$ и Γ – φ-инвариантная подгруппа в Π такая, что $\Gamma T = \Pi$, то $G \cong \Gamma/\Gamma \cap T$.*

Доказательство. Классу $g(\Gamma \cap T)$ с $g \in \Gamma$ в $\Gamma/\Gamma \cap T$ сопоставляется класс gT в Π/T. Биективность и гомоморфность отображения легко проверяются.

3. Здесь мы выясняем структуру двух классов конечных L-группоидов. Каждый L-группоид обладает несобственными подгруппоидами: одноэлементными и самим группоидом.

Определение. L-группоид $G(\circ)$ называется минимальным, если он не содержит подгруппоидов, отличных от несобственных.

Теорема 3. *Конечный минимальный L-группоид является квазигруппой и может быть построен из конечного поля $\mathbb{F}_q$, если положить $x \circ y = \mu x + \lambda y$, где $\mu, \lambda \in \mathbb{F}_q$, $\mu + \lambda = 1$, $\lambda \neq 0, 1$.*

Доказательство. Транзитивность минимального L-группоида $G(\circ)$ следует из предложения 5. По теореме 2, $G(\circ)$ может быть представлен однородным пространством $G(\circ) \cong \Pi/T$, где в качестве Π может быть взята группа левых трансляций $Z(G)$. Введем обозначение: для $a \in G(\circ)$ $Z(a) = \{u \in Z(G) | u(a) = a\}$. Покажем, что существует представление с единичной подгруппой φ-неподвижных элементов.

Возьмем $a, b \in G$. $Z(a)$ оставляет на месте a, $Z(b)$ оставляет неподвижным b. Автоморфизмы из $Z(a) \cap Z(b)$ оставляют на месте элементы подгруппоида, порожденного a и b. В силу минимальности это есть весь группоид G, а поэтому $Z(a) \cap Z(b) = (1)$, при $a \neq b$.

Группы $Z(a)$, $Z(b)$ – самонормализуемы.

Действительно, $uZ(a)u^{-1} \subset Z(a) \Rightarrow utu^{-1} \in Z(a)$ для $\forall t \in Z(a)$ $\Rightarrow utu^{-1}(a) = a \Rightarrow tu^{-1}(a) = u^{-1}(a)$, т.е. если взять $t = L_a$, то получим $u^{-1}(a) = a$ и $u \in Z(a)$, что и доказывает самонормализуемость.

Тогда мы находимся в условиях известной теоремы Фробениуса ([4]). Согласно этой теореме $\Gamma = (Z(G) \setminus \cup uZ(e)u^{-1}) \cup \{1\}$ – нормальный делитель в $Z(G)$. Кроме того, Γ выдерживает сопряжение с помощью $Z(e)$. Очевидно, что $\Gamma \cap Z(e) = (1)$. Остается воспользоваться теоремой редукции, описанной в предложении 6, в которой в качестве Π возьмем $Z(G)$, в качестве T возьмем $Z(e)$, а в качестве Γ отмеченную выше группу. Так как $\Gamma \cap T = 1$, то условие (2) в этом случае равносильно условию (1), т.е. G – квазигруппа. То, что минимальная квазигруппа может быть построена из конечного поля описанной в формулировке конструкцией, доказано в работе [2].

Следующий класс L-группоидов, который мы хотим рассмотреть, это класс симметрических группоидов. В них по определению выполняется "тождество левых ключей": $a \circ (a \circ b) = b$, эквивалентное, очевидно, равенству $L_a^2 = 1$. Термин "симметрический" заимствован из теории симметрических пространств дифференциальной геометрии ([5]), где появляется указанное тождество. Пример симметрического группоида был дан выше в п. 1. Этот

группоид не является квазигруппой. В конечном случае ситуация иная. Именно, имеет место следующая

Теорема 4. *Конечный симметрический L-группоид является квазигруппой.*

Доказательство. Сначала установим транзитивность конечного симметрического группоида $G(\circ)$.

Предположим противное. Пусть в $\{L_a|a \in G\}$ имеется по крайней мере два класса сопряженности J_1 и J_2. Выделим в них по трансляции, скажем, $L_a \in J_1$, $L_b \in J_2$. Так как $L_a^2 = L_b^2 = 1$, то подгруппа в $Z(G)$, порожденная L_a и L_b, диэдральна: $\langle L_a, L_b\rangle = \langle \sigma, \tau | \sigma^2 = 1, \sigma\tau\sigma^{-1} = \tau^{-1}$, где $\sigma = L_a$, $\tau = L_aL_b$.

Пусть порядок τ равен n. Вычисляя классы сопряженности, получаем, что класс L_a в $\langle L_a, L_b\rangle$ есть $\{\sigma\tau^{2i}|i = 0, 1, \ldots\}$, а класс L_b есть $\{\sigma\tau^{2i-1}|i = 0, 1, \ldots\}$. Различие этих классов влечет четность n. Действительно, $\sigma\tau^{2i} \neq \sigma\tau^{2j-1} \Leftrightarrow \tau^{2i} \neq \tau^{2j-1}$ и $\tau^{2i-2j+1} \neq 1$. С другой стороны, при четном $n = 2k$ элемент $\sigma\tau^k \in \langle L_a, L_b\rangle$ сопряжен с L_a или с L_b, т.е. $\sigma\tau^k = L_c$ при некотором $c \in G$. Имеем, $L_aL_cL_a^{-1} = L_{a\circ c} = \sigma\sigma\tau^k\sigma^{-1} = \tau^k\sigma^{-1} = \sigma\tau^{-k} = \sigma\tau^k = L_c$, так как $\tau^{-k} = \tau^k$. Поэтому $a \circ c$ и $a = c$, $\sigma\tau^k = \sigma$ и $\tau^k = 1$, что невозможно, поскольку порядок τ равен $n = 2k$. Противоречие. Следовательно, в действительности классы L_a и L_b совпадают, а n – нечетно.

Элементы класса L_a теперь есть трансляции вида $\sigma\tau^i (i = 0, 1, \ldots)$. При соответствии $L_{a_i} \to i$, если $L_{a_i} = \sigma\tau^i$, получаем $L_{a_i \circ a_j} = L_{a_i}L_{a_j}L_{a_i}^{-1} = \sigma\tau^i\sigma\tau^j(\sigma\tau^i)^{-1} = \sigma\tau^i\sigma\tau^{j-1}\sigma^{-1} = \sigma\tau^{2i-j} = L_{a_{2i-j}}$ и подгруппоид, порожденный a и b, изоморфен группоиду $\mathbb{Z}_n(\circ)$, где $x \circ y = 2x - y$.

При n нечетном, последний является квазигруппой, так как $x \circ u = \nu$ дает $2x = u + \nu$ и x однозначно определяется по $\bmod n$. Обращаясь к $G(\circ)$, замечаем, что $x \circ a = b$ разрешимо уже в подгруппоиде $\langle a, b\rangle$. Поскольку отображение $x \to x \circ a$ тогда сюръективно, то из конечности порядка G следует и его инъективность. Это значит, что уравнение $x \circ a = b$ имеет в G единственное решение и $G(\circ)$ – квазигруппа.

В. М. Галкину принадлежит следующий результат о конечных симметрических квазигруппах: такая квазигруппа есть подквазигруппа в $\Pi(\circ)$, где Π – группа нечетного порядка, а $x \circ y = xy^{-1}x$.

Литература

1. В. Д. Белоусов, *Основы теории квазигрупп и луп*. Наука, М. (1967).

2. В. М. Галкин, *Леводистрибутивные квазигруппы конечного порядка.* Квазигруппы и лупы, с. 43–54, Кишинев (1979).
3. С. В. Матвеев, *Дистрибутивные группоиды в теории узлов.* — Математический сборник **119**, No. 1 (1982), с. 78–88.
4. И. Херстейн, *Некомутативные кольца.* Мир, М. (1972), с. 141.
5. O. Loos, *Symmetric spaces.* New York: Amsterdam (1969).

Erofeeva L. N. On a class of groupoids.

The paper studies a new class of left distributive groupoids and their relation to homogeneous spaces.

Нижегородский
государственный университет

Поступило 15 декабря 2003 г.