О мультипликативных группах свободных и свободных коммутативных квазигрупп

М. М. ГЛУХОВ
Академия криптографии Российской Федерации
e-mail: glukhovmm@rambler.ru

УДК 512.548.7

Ключевые слова: квазигруппа, мультипликативная группа.

Аннотация

В работе исследуется строение мультипликативных групп для относительно свободных алгебр некоторых многообразий квазигрупп, в частности для многообразий всех квазигрупп, всех коммутативных квазигрупп и всех TS-квазигрупп. Во всех этих случаях соответствующая мультипликативная группа свободна. Работа посвящена славной памяти профессора Александра Александровича Нечаева, который в последние годы активно исследовал возможности применения квазигрупп в криптографии.

Abstract

M. M. Glukhov, On the multiplicative groups of free and free commutative quasigroups, Fundamentalnaya i prikladnaya matematika, vol. 20 (2015), no. 1, pp. 23—37.

We study the structure of the multiplicative groups for the relatively free algebras of some quasigroup varieties, in particular, for the varieties of all quasigroups, all commutative quasigroups, and all TS-quasigroups. In all these cases, the corresponding multiplicative group is free. The work is dedicated to the glorious memory of Prof. Alexandr Alexandrovich Nechaev, who actively explored the possibility of application of quasigroups in cryptography during recent years.

Введение

Данная работа инспирирована статьями [5, 6], посвящёнными изучению односторонних мультипликативных групп свободной лупы W (левая мультипликативная группа обозначается $\mathrm{LMlt}(W)$, правая — $\mathrm{RMlt}(W)$). В [5] доказано, что левая (правая) мультипликативная группа свободной лупы W является свободной группой бесконечного ранга, а как группа подстановок на W она является группой Фробениуса. В [6] показано, что для группы $\mathrm{Mlt}(W)$ стабилизатор двух точек нетривиален, и найдена система образующих стабилизатора $\mathrm{Mlt}(W)_{a,b}$ при любых различных $a, b \in W$. Доказано также, что группа $\mathrm{Mlt}(W)_{a,b,c}$ тривиальна при любом $c \neq a, b$. Доказательства основаны на использовании введённых ранее Т. Ивенсом нормальных форм слов [7]. В данной

Фундаментальная и прикладная математика, 2015, том 20, № 1, с. 23—37.

работе предлагается более простое доказательство указанных выше результатов о группах $\mathrm{LMlt}(W)$ и $\mathrm{RMlt}(W)$, а также их распространение на группу $\mathrm{Mlt}(W)$ и на случай, когда W — абсолютно свободная квазигруппа, или свободная коммутативная квазигруппа, или свободная TS-квазигруппа.

1. Основные понятия и обозначения

Под квазигруппой понимается любое непустое множество Q с бинарной операцией умножения $(\cdot)$, в котором для любых $a, b \in Q$ однозначно разрешимо каждое из уравнений $ax = b$, $ya = b$. Квазигруппа с единицей называется лупой.

Множество всех так определённых квазигрупп (луп) не является многообразием алгебр, поскольку не замкнуто относительно подалгебр и гомоморфных образов. Поэтому при решении различных вопросов, связанных с многообразиями квазигрупп и луп, последние рассматривают как алгебры с тремя бинарными операциями $\cdot$, $/$, $\backslash$, где операции $/$, $\backslash$, называемые соответственно левым и правым делением, определяются условиями

$$a \,/\, b = c \Longleftrightarrow cb = a, \quad a \setminus b = c \Longleftrightarrow ac = b.$$

Всюду далее квазигруппы рассматриваются как алгебры в сигнатуре $\Omega = \{\cdot, /, \backslash\}$, а лупы — как алгебры в сигнатуре $\Omega_1 = \{\cdot, /, \backslash, e\}$, где e — символ 0-арной операции, играющий роль единицы. Для квазигруппы Q правой (левой) трансляцией, соответствующей элементу $a \in Q$, называется подстановка R_a (L_a) множества Q, такая что $uR_a = ua$ ($uL_a = au$) для любого элемента $u \in Q$. Множество всех правых (левых) трансляций квазигруппы Q обозначим через R_Q (L_Q). Напомним (см. [1]), что правой (левой) мультипликативной группой квазигруппы Q называют группу $\mathrm{RMlt}(Q)$ ($\mathrm{LMlt}(Q)$) подстановок множества Q, порождённую всеми правыми (левыми) трансляциями квазигруппы Q. Группу, порождённую всеми трансляциями квазигруппы Q, называют её мультипликативной группой и обозначают $\mathrm{Mlt}(Q)$. Таким образом,

$$\mathrm{RMlt}(Q) = \langle R_Q \rangle, \quad \mathrm{LMlt}(Q) = \langle L_Q \rangle, \quad \mathrm{Mlt}(Q) = \langle R_Q \cup L_Q \rangle.$$

Группу подстановок G множества A называют группой Фробениуса, если она транзитивна на A, не регулярна (т. е. имеет нетривиальный стабилизатор G_a для любой точки $a \in A$) и имеет тривиальный стабилизатор $G_{a,b}$ для любых различных точек $a, b \in A$ (см. [9]). Обозначим буквой X некоторое непустое множество символов, которые будем называть переменными, обозначая их буквами x, y, z (возможно, с индексами). Обычным образом индуктивно определяются понятия Ω-слова в алфавите X и его длины. А именно,

1) любой символ из X является Ω-словом длины 1 в алфавите X;
2) если A и B — Ω-слова в алфавите X и $*$ — символ любой операции из Ω, то $(A) * (B)$ — Ω-слово в алфавите X, его длина равна сумме длин слов

A и B, которые называются его главными подсловами или главными компонентами;

3) других слов в алфавите X нет.

При определении Ω_1-слов изменяется лишь пункт 1), в нём к словам длины 1 добавляется ещё сигнатурный символ e.

Тождеством сигнатуры Ω (Ω_1) называют формальное равенство $A = B$ двух Ω-слов (Ω_1-слов) в алфавите X. При этом слова A и B называются соответственно левой и правой частями тождества. Говорят, что тождество $A = B$ выполняется в квазигруппе (лупе) Q, если при замене в нём переменных из X произвольными элементами из Q (при условии, что одинаковые буквы заменяются равными элементами) левая и правая части тождества принимают одинаковые значения из Q.

Многообразия всех квазигрупп и луп в указанных сигнатурах задаются соответственно системами тождеств

$$\Sigma_0 = \{(xy)\,/\,y = x,\ (x\,/\,y)y = x,\ x(x \setminus y) = y,\ x \setminus (xy) = y,$$
$$x\,/(y \setminus x) = y,\ (x\,/\,y) \setminus x = y\},$$
$$\Sigma_e = \Omega_0 \cup \{xe = x,\ ex = x,\ x\,/\,x = e,\ x \setminus x = e\}.$$

Иначе говоря, любая алгебра с системой операций Ω или Ω_1 является квазигруппой или лупой тогда и только тогда, когда в ней выполняется система тождеств Σ_0 или Σ_e соответственно.

Система тождеств называется тривиальной, если она выполняется только в одноэлементных квазигруппах. Системы тождеств называются эквивалентными, если они выполняются в одних и тех же квазигруппах. Многообразие всех квазигрупп, в которых выполняются все тождества некоторой системы Σ, обозначим через $Q(\Sigma)$. Далее мы будем рассматривать лишь свободные квазигруппы многообразий $Q(\Sigma)$ при различных Σ.

Зафиксируем произвольную нетривиальную систему тождеств Σ в сигнатуре Ω, содержащую Σ_0, и рассмотрим многообразие $Q(\Sigma)$.

Пусть M — произвольное множество с частично определёнными операциями из Ω. Его диаграмму, т. е. множество всех соотношений вида $a * b = c$, где $a, b, c \in M$, а $*$ — любая операция из Ω, обозначим через $S(M)$. В частности, $S(M)$ может быть и пустой. Далее соотношения вида $a * b = c$ будем называть табличными. В общем случае из всех слов в алфавите M естественным образом выделяются слова, определённые в M, т. е. имеющие значения в M. В частном случае, когда определены все слова, M будет квазигруппой, а $S(M)$ — её таблицей Кэли.

Следуя [8], будем говорить, что во множестве M с частично определёнными операциями из Ω и с диаграммой $S(M)$ выполняется тождество $U = V$, если при подстановке в него вместо переменных любых элементов из M получатся Ω-слова в алфавите M, для которых выполняется одно из следующих условий: либо оба они определены и имеют одинаковые значения в M, либо оба не определены в M, либо одно из них определено, а в другом не определена

хотя бы одна из главных компонент. Множество M, в котором выполняются в указанном смысле все тождества из Σ, будем называть частичной Σ-квазигруппой. Множество всех частичных Σ-квазигрупп обозначим через $P(\Sigma)$. При определении частичной лупы требуется, чтобы она содержала единицу e. Так как $\Sigma \supseteq \Sigma_0$, то наличие в $S(M)$ для $M \in P(\Sigma)$ любого одного из соотношений $ab = c$, $c \,/\, b = a$, $a \setminus c = b$ влечёт наличие и двух других. Поэтому любые два из них будем называть тривиальными следствиями третьего.

Пусть $M \in P(\Sigma)$, $a, b \in M$ и в M не определено $a * b$. Добавим к M новый элемент c и к $S(M)$ соотношение $a*b = c$, вместе со всеми следствиями системы $\Sigma \cup S(M) \cup \{a * b = c\}$. Для получения этих следствий мы должны производить произвольные подстановки элементов из $M \cup \{c\}$ в тождества из Σ. Если при некоторой подстановке в тождество $U = V$ окажется, что слово в одной из частей тождества определено и имеет значение w, а слово из другой части не определено и имеет вид $A * B$, где главные компоненты A, B определены и имеют соответственно значения u, v, то получаем в качестве следствия новое табличное соотношение $u * v = w$. Если же окажется, что слова в обеих частях тождества определены и имеют разные значения u, v, то получаем следствие $u = v$, после чего заменяем в $S(M)$ элемент v на u и удаляем из M элемент v. В итоге мы получим множество M_1 с системой соотношений $S(M_1)$. Далее ту же процедуру применяем к M_1. В результате всех таких преобразований мы получим частичную Σ-квазигруппу T.

Полученная выше из M частичная квазигруппа T называется простым свободным расширением частичной квазигруппы $M \in P(\Sigma)$ и обозначается $T = [M; a * b = c]$.

Частичная квазигруппа $T \in P(\Sigma)$ называется конечно свободным расширением частичной квазигруппы $M \in P(\Sigma)$, если T получена из M конечной последовательностью простых свободных расширений. Очевидно, что для любого слова W в алфавите M, не определённого в частичной квазигруппе M, можно построить конечно свободное расширение, в котором определено слово W. Ниже для сокращения речи простые и конечно свободные расширения иногда будем называть просто расширениями.

Будем говорить, что система квазигрупповых тождеств удовлетворяет условию R, если любая частичная квазигруппа $M \in P(\Sigma)$ изоморфно вложима в любое её простое свободное расширение $T = [M; a * b = c]$, причём каждое соотношение из $S(T) \setminus S(M)$ не содержит элементов, отличных от a, b, c, и не зависит от соотношений из $S(M)$, т. е. является следствием лишь системы тождеств Σ и соотношения $a * b = c$. Понятие R-многообразия квазигрупп введено в [4]. В [2] все R-многообразия квазигрупп описаны системами тождеств. В частности, R-многообразиями являются многообразия всех квазигрупп, коммутативных квазигрупп, TS-квазигрупп, квазигрупп Штейнера. Всюду далее будем считать, что R-многообразия квазигрупп задаются подсистемами системы тождеств из [2]. Из определения условия R видно, что любая частичная квазигруппа M из $P(\Sigma)$ изоморфно вложима в квазигруппу из $Q(\Sigma)$, заданную системой образующих M и системой определяющих соотношений $S(M)$.

Тогда по известной теореме Ивенса [8] для конечно определённых квазигрупп любого R-многообразия разрешима проблема тождества слов. Кроме того, по доказанному в [3] для конечно определённых квазигрупп любого R-многообразия разрешимы также алгоритмические проблемы изоморфизма и вхождения в подквазигруппу.

Техникой, развитой в [3] для R-многообразий универсальных алгебр, можно воспользоваться и для описания правых (левых) мультипликативных групп свободных квазигрупп и свободных коммутативных квазигрупп.

2. Описание левой и правой мультипликативных групп свободной квазигруппы многообразия $Q(\Sigma_0)$

Рассмотрим сначала вопрос о строении групп $\mathrm{LMlt}(Q)$, $\mathrm{RMlt}(Q)$ для свободной квазигруппы Q в многообразии всех квазигрупп $Q(\Sigma_0)$. Ввиду симметрии достаточно рассмотреть группу $G = \mathrm{RMlt}(Q)$. Заметим, что в этом случае в простом свободном расширении $T = [M; a * b = c]$ соотношениями из $S(T) \setminus S(M)$ будут лишь тривиальные следствия соотношения $a * b = c$.

Лемма 1. *Пусть Q — свободная квазигруппа с базисом M многообразия $Q(\Sigma_0)$ и $G = \mathrm{RMlt}(Q)$. Тогда любой неединичный элемент $g \in G$ оставляет неподвижным не более одного элемента из Q.*

Доказательство. Из условия R следует, что при $\Sigma = \Sigma_0$, т. е. когда $Q(\Sigma_0)$ — многообразие всех квазигрупп, следствиями любого табличного соотношения являются лишь его тривиальные следствия.

Любой отличный от единицы элемент g группы G представляется в виде

$$g = R_{a_1}^{\varepsilon_1} \dots R_{a_k}^{\varepsilon_k}, \quad a_i \in Q, \quad \varepsilon_i \in \{1, -1\}, \quad i = 1, \dots, k, \\ R_{a_{i+1}}^{\varepsilon_{i+1}} \neq R_{a_i}^{-\varepsilon_i} \quad \text{при} \quad i = 1, \dots, k-1. \quad (1)$$

Назовём такое представление элемента g, а также представляющее его слово (т. е. произведение) несократимыми. Несократимым представлением единицы группы G (т. е. тождественной подстановки) будем считать пустое слово. Всюду далее без оговорок будем использовать лишь несократимые представления элементов из G. Заметим, что для трансляции R_a обратная подстановка определяется равенством $uR_a^{-1} = u \,/\, a$. Поэтому действие g на элемент $u \in Q$ запишется в виде

$$ug = \Big(\big(\dots \big((u \circ_1 a_1) \circ_2 a_2 \big) \dots \big) \circ_{k-1} a_{k-1} \Big) \circ_k a_k,$$

где при любом $i \in \{1, \dots, k\}$ операция $\circ_i$ есть $\cdot$ или $/$.

Индукцией по k докажем, что для любых различных $u, v \in Q$ система равенств

$$\Big(\big(\ldots\big((u \circ_1 a_1) \circ_2 a_2\big)\ldots\big) \circ_{k-1} a_{k-1}\Big) \circ_k a_k = u, \tag{2}$$

$$\Big(\big(\ldots\big((v \circ_1 a_1) \circ_2 a_2\big)\ldots\big) \circ_{k-1} a_{k-1}\Big) \circ_k a_k = v \tag{3}$$

несовместна в Q.

При $k = 1$ равенства (2), (3) имеют вид

$$u \circ_1 a_1 = u, \quad v \circ_1 a_1 = v. \tag{4}$$

Рассмотрим частичную квазигруппу M с пустой системой $S(M)$ и построим её минимальное конечно свободное расширение M_1, в котором определены элементы u, v, a_1 (являющиеся значениями слов в алфавите M). Так как Σ_0 не содержит тождества идемпотентности $xx = x$, то в силу условия R в M_1 имеет место неравенство $u \neq a_1$ и выполняются равенства (4). В силу условия минимальности последним присоединённым элементом при построении M_1 должен быть один из элементов u, v, $a1$. Однако из определения простого свободного расширения видно, что последним присоединённым элементом может быть только a_1 и присоединиться он может лишь с соотношением $u * u = a_1$, а соотношения (4) будут его тривиальными следствиями. Отсюда видно, что $u = v$, вопреки условию.

Пусть наше утверждение верно для любых различных $u, v \in Q$ при $k < n$, докажем его для $k = n$.

Допустим, что при $k = n$ выполняются равенства (2), (3). Обозначим

$$\begin{aligned} &u \circ_1 a_1 = b_1,\ b_1 \circ_1 a_2 = b_2,\ \ldots,\ b_{k-2} \circ_{k-1} a_{k-1} = b_{k-1},\ b_{k-1} \circ_k a_k = u,\\ &v \circ_1 a_1 = c_1,\ c_1 \circ_1 a_2 = c_2,\ \ldots,\ c_{k-2} \circ_{k-1} a_{k-1} = c_{k-1},\ c_{k-1} \circ_k a_k = v. \end{aligned} \tag{5}$$

Сразу отметим, что неравенство $u \neq v$ влечёт неравенства $b_i \neq c_i$, $i = 1, \ldots, k-1$.

Построим сначала минимальное конечно свободное расширение M_1 частичной квазигруппы M, в котором определены элементы

$$u,\ a_i,\ b_j, \quad i = 1, \ldots, k,\ j = 1, \ldots, k-1,$$

Рассмотрим ряд случаев.

1. Последний присоединённый элемент есть u.

Тогда в силу условия R в M_1 выполняются соотношения

$$u \circ_1 a_1 = b_1, \quad b_{k-1} \circ_k a_k = u.$$

Так как u — последний присоединённый элемент, то $b_{k-1}, a_k \neq u$ и первое соотношение является тривиальным следствием второго. Отсюда получаем:

а) если $\circ_k$ есть $\cdot$, то $\circ_1$ есть $/$, причём $a_k = a_1$ и $b_{k-1} = b_1$;

б) если $\circ_k$ есть $/$, то $\circ_1$ есть $\cdot$, причём $a_k = a_1$ и $b_{k-1} = b_1$.

В случае $k = 2$ мы получаем противоречие с условием несократимости представления (1) для g, поскольку в условиях а), б) это представление g будет иметь соответственно вид $R_{a_1}^{-1} R_{a_1}$, $R_{a_1} R_{a_1}^{-1}$.

Если $k > 2$, то, подставляя данные из а), б) в равенства (2), (3), получаем равенства

$$(\dots(u_1 \circ_2 a_2)\dots) \circ_{k-1} a_{k-1} = u_1,$$
$$(\dots(v_1 \circ_2 a_2)\dots) \circ_{k-1} a_{k-1} = v_1,$$

где $u_1 = u \,/\, a_1$, $v_1 = v \,/\, a_1$ в случае а) и $u_1 = u{\cdot}a_1$, $v_1 = v{\cdot}a_1$ в случае б). В обоих случаях $u_1 \neq v1$, и мы получаем противоречие с предположением индукции.

2. Последний присоединённый элемент есть b_s, $1 \leqslant s \leqslant k-1$.

Тогда согласно (3) в M_1 выполняются соотношения

$$b_{s-1} \circ_s a_s = b_s, \quad b_s \circ_{s+1} a_{s+1} = b_{s+1}. \tag{6}$$

Из условия R следует, что $b_{s-1}, a_s \neq b_s$ и в (6) второе соотношение есть тривиальное следствие первого. Далее возможны два варианта:

а) если $\circ_s$ есть $\cdot$, то $\circ_{s+1}$ есть $/$, причём $a_{s+1} = a_s$ и $b_{s+1} = b_{s-1}$;

б) если $\circ_k$ есть $/$, то $\circ_1$ есть $\cdot$, причём $a_{s+1} = a_s$ и $b_{s+1} = b_{s-1}$.

В обоих случаях $R_{a_{s+1}}^{\varepsilon_{s+1}} = R_{a_s}^{-\varepsilon_s}$, что противоречит несократимости представления (1) для g.

3. Последний присоединённый элемент есть a_s, $1 \leqslant s \leqslant k$.

Тогда при $s > 1$ в M_1, а значит и в Q, выполняется соотношение

$$b_{s-1} \circ_s a_s = b_s. \tag{7}$$

Если при этом в M_1 уже присутствуют элементы c_{s-1}, c_s, то должно выполняться и соотношение $c_{s-1} \circ_s a_s = c_s$, которое в силу условия R должно быть тривиальным следствием соотношения (7). Однако это возможно лишь при их совпадении. Следовательно, $c_{s-1} = b_{s-1}$, что противоречит условию $u \neq v$. Заметим, что при $s = 1$ рассуждения те же, только вместо b_{s-1} и c_{s-1} будут выступать соответственно u и v.

Если же в M_1 хотя бы один из элементов c_{s-1}, c_s не определён, то построим минимальное конечно свободное расширение M_2 частичной квазигруппы M_1, в котором определены элементы v, c_i, $i = 1, \dots, k-1$. Здесь также возможны два принципиально различных случая: последний присоединённый элемент есть либо v, либо c_t при некотором $t = 1, \dots, k-1$.

Все дальнейшие рассуждения совпадают в первом случае с рассуждениями в случае 1, во втором — с рассуждениями в случае 2 с той лишь разницей, что вместо u и b_s будут использоваться v и c_s. Во всех случаях придём к противоречию либо с условием, либо с предположением индукции. В итоге лемма доказана. □

Напомним, что группа подстановок Φ на множестве A называется группой Фробениуса, если она

1) транзитивна;

2) не регулярна, т. е. стабилизатор Φ_a любой точки $a \in A$ нетривиален;

3) стабилизатор $\Phi_{a,b}$ любых двух различных точек a, b тривиален.

Теорема 1. *Если Q — свободная квазигруппа, то группы $G = \mathrm{RMlt}(Q)$ и $H = \mathrm{LMlt}(Q)$ являются свободными группами с базисами соответственно* $\text{Б} = \{R_a \colon a \in Q\}$ *и* $\text{Б}_1 = \{L_a \colon a \in Q\}$. *Как группы подстановок на Q обе эти группы являются группами Фробениуса.*

Доказательство. Ввиду симметрии достаточно доказать утверждения теоремы лишь для одной из групп G, H. Проделаем это для группы G. Группа G транзитивна, так как для любых $a, b \in Q : aR_{a\backslash b} = b$; стабилизатор $G_a \neq \{\mathcal{E}\}$, так как $uR_{u\backslash u} = u$ для любого $u \in Q$, и $G_{a,b} = \{\mathcal{E}\}$ по доказанной лемме 1. Следовательно, G — группа Фробениуса.

Докажем, что G как абстрактная группа свободна с базисом Б. Для этого достаточно показать, что любой элемент из G однозначно представляется несократимым произведением элементов из Б. Существование такого представления очевидно. Докажем единственность. Допустим, что элемент g имеет два несократимых представления

$$g = R_{a_1}^{\varepsilon_1} \dots R_{a_k}^{\varepsilon_k}, \quad g = R_{b_1}^{\delta_1} \dots R_{b_r}^{\delta_r}. \tag{8}$$

Тогда

$$uR_{a_1}^{\varepsilon_1} \dots R_{a_k}^{\varepsilon_k} R_{b_r}^{-\delta_r} \dots R_{b_1}^{-\delta_1} = u$$

при любом $u \in Q$. Отсюда согласно лемме 1 произведение

$$R_{a_1}^{\varepsilon_1} \dots R_{a_k}^{\varepsilon_k} R_{b_r}^{-\delta_r} \dots R_{b_1}^{-\delta_1}$$

не может быть несократимым. Так как представления (8) различны, то, произведя все возможные сокращения на стыке слов $R_{a_1}^{\varepsilon_1} \dots R_{a_k}^{\varepsilon_k}$ и $R_{b_r}^{-\delta_r} \dots R_{b_1}^{-\delta_1}$, мы получим непустое несократимое слово в алфавите Б, причём соответствующая подстановка оставляет неподвижным любой элемент из Q. Это противоречит лемме 1, и значит, наше допущение неверно. □

3. Описание мультипликативной группы свободной квазигруппы

Рассмотрим теперь группу $F = \mathrm{Mlt}(Q)$. Из теоремы 1 следует, что F как группа подстановок порождается двумя свободными группами $G = \mathrm{RMlt}(Q)$ и $H = \mathrm{LMlt}(Q)$. Естественно поставить вопрос: не является ли F свободным произведением групп G, H. Положительный ответ означал бы, что и группа F является свободной. Ниже приводится доказательство этого факта.

Каждый элемент $g \in F$ представляется в виде

$$g = P_1^{\varepsilon_1} \dots P_n^{\varepsilon_n}, \tag{9}$$

где $P_i \in \text{Б} \cup \text{Б}_1$, $\varepsilon_i \in \{1, -1\}$, $i = 1, \dots, n$. Как и выше, представление (9) назовём несократимым, если $P_{i+1}^{\varepsilon_{i+1}} \neq P_i^{-\varepsilon_i}$, $i = 1, \dots, n-1$. Сгруппируем в (9)

сомножители, относя в одну группу все подряд идущие элементы, содержащиеся в G или H. Тогда получим, что $g = g_1h_1g_2h_2\dots g_kh_k$, где $g_i \in G$, $h_i \in H$, $i = 1,\dots,k$, и все эти подстановки, кроме, может быть, g_1, h_k, неединичные. Обозначим через

$$S_i = R_{a_{i1}}^{\varepsilon_{i1}}\dots R_{a_{is_i}}^{\varepsilon_{is_i}}, \quad T_i = L_{b_{i1}}^{\varepsilon_{i1}}\dots L_{b_{it_i}}^{\varepsilon_{it_i}}$$

несократимые представления соответственно элементов g_i, h_i, $i = 1,\dots,k$. Тогда несократимое представление элемента g будет иметь вид

$$g = S_1T_1\dots S_kT_k. \tag{10}$$

Теорема 2. *Если элемент $g \in F$ имеет непустое несократимое представление, то $g \neq \mathcal{E}$.*

Доказательство. Пусть (9) — непустое несократимое представление g. Докажем индукцией по n неравенство $g \neq \mathcal{E}$. При $n = 1, 2$ оно устанавливается непосредственной проверкой. Предположим, что оно верно при всех $n < m$, и докажем его для $n = m$.

Допустим, что $g = \mathcal{E}$, т. е. для любого $u \in Q$ выполняется равенство

$$ug = u. \tag{11}$$

Если $g = g_1$ или $g = h_1$, то по лемме 1 равенство (11) может выполняться не более чем для одного значения u, и утверждение теоремы 2 верно. Поэтому будем считать, что в записи g присутствуют по крайней мере два нетривиальных сомножителя из разных групп G, H. Очевидно, что достаточно рассмотреть два случая.

I. $g_1 \neq \mathcal{E}$, $h_k \neq \mathcal{E}$.
II. $g_1 \neq \mathcal{E}$, $h_k = \mathcal{E}$.

Два остальных случая сводятся к ним путём перехода от элемента g к g^{-1}.

Случай I.

Введём ещё обозначения

$$S_i' = R_{a_{i1}}^{\varepsilon_{i1}}\dots R_{a_{i\,s_i-1}}^{\varepsilon_{i\,s_i-1}}, \quad S_i'' = R_{a_{i2}}^{\varepsilon_{i1}}\dots R_{a_{i\,s_i}}^{\varepsilon_{i\,s_i}}, \quad S_i''' = R_{a_{i2}}^{\varepsilon_{i2}}\dots R_{a_{i\,s_i-1}}^{\varepsilon_{i\,s_i-1}},$$
$$T_i' = L_{b_{i1}}^{\varepsilon_{i1}}\dots L_{b_{i\,t_i-1}}^{\varepsilon_{i\,t_i-1}}, \quad i = 1,\dots,k.$$

Ввиду большой сложности полной подробной записи равенства (10) мы выпишем подробно лишь его часть, а именно действие на u трансляций из S_1, T_1, первой трансляции из S_2 и последней трансляции из T_k:

$$b_{ks_k} *_{ks_k} \Bigg(\dots\Bigg(\Big(b_{1s_1} *_{1s_1} \big(\dots\big(b_{11} *_{11} \big(\dots\big((u \circ_{11} a_{11}) \circ_{12} a_{12}\big)\dots\big)\big)\dots\big)\Big) \circ_{21} a_{21}\Bigg)\dots\Bigg) = u. \tag{12}$$

Заметим, что подстановка L_a^{-1} действует на x по формуле $xL_a^{-1} = a \setminus x$. Поэтому в (12) операции вида $\circ_{ij}$ совпадают с $\cdot$ или $/$, а операции $*_{ij}$ (как показано

выше) — с $\cdot$ или $\backslash$. Далее, как и в доказательстве леммы 1, мы для частичной квазигруппы M с пустой системой табличных соотношений $S(M)$ будем строить конечно свободное расширение так, чтобы в полученной в итоге частичной квазигруппе слово из левой части равенства (12) было полностью определено при некотором значении u, причём значение u будет выбираться так, чтобы оно при расширении присоединялось последним и не удовлетворяло условию (12). Для доказательства существования такой последовательности простых свободных расширений нам понадобится лемма 2.

Лемма 2. *Пусть в частичной квазигруппе M_1, являющейся конечно свободным расширением M, определены все элементы a_{ij}, b_{ij} из* (12) *и для некоторого элемента c выполняются условия*

а) $cS_1''T_1S_2T_2\dots S_iT_i' \neq a_{i+1,1}$, $i = 1,\dots,k$, $a_{k+1,1} = a_{1,1}$;

б) $cS_1''T_1S_2T_2\dots S_{i-1}T_{i-1}S_i' \neq b_{i1}$, $i = 2,\dots,k$.

Кроме того, пусть при $t_1 = 1$ в M_1 не определены $c \circ_{11}^{-1} a_{11}$ и $b_{11} *_{11} c$, а при $t_1 > 1$ не определены $c \circ_{11}^{-1} a_{11}$ и $c \circ_{12} a_{12}$ и выполняется неравенство $cS_1''' \neq b_{11}$. Тогда существует последовательность простых свободных расширений $M_1, M_2, \dots, M_n$, такая что в M_n определена левая часть равенства (12) *и*

$$M_n = [M_{n-1}; c = u]. \tag{13}$$

Доказательство. Рассмотрим сначала случай, когда $t_1 > 1$. По условию в этом случае в M_1 не определены $c \circ_{11}^{-1} a_{11}$ и $c \circ_{12} a_{12}$. Присоединив к M_1 новый элемент c_{12} с соотношением

$$c \circ_{12} a_{12} = c_{12}, \tag{14}$$

получим частичную квазигруппу M_2. Покажем, что в ней при $s_1 > 2$ не определено $c_{12} \circ_{13} a_{13}$. Допустим, что в M_2 выполняется равенство $c_{12} \circ_{13} a_{13} = d$. Тогда, учитывая, что оно является тривиальным следствием соотношения (4), получаем, что $a_{12} = a_{13}$ и $\circ_{13} = \circ_{12}^{-1}$. Отсюда видно, что представление S_1 сократимо, вопреки условию. Из тех же соображений следует, что, присоединив к M_2 новый элемент c_{13} с соотношением $c_{12} \circ_{13} a_{13} = c_{13}$, получим частичную квазигруппу M_3, в которой не определено $c_{13} \circ_{14} a_{14}$. Продолжая этот процесс, мы получаем частичную квазигруппу M_{s_1} с последним присоединённым элементом

$$c_{1\,s_1} = c_{1\,s_1-1} \circ_{1\,s_1} a_{1\,s_1}. \tag{15}$$

Заметим, что $c_{1\,s_1-1} = cS_1'''$.

Далее согласно равенству (12) мы должны вычислять элемент $b_{11} *_{11} c_{1\,s_1}$. Покажем, что он не определён в M_{s_1}. Допустим, что в M_{s_1} выполняется равенство $b_{11} *_{11} c_{1\,s_1} = d$. Так как оно является тривиальным следствием соотношения (15), то $b_{11} = c_{1\,s_1-1}$, т. е. $cS_1''' = b11$, что противоречит условию. Следовательно, $b_{11} *_{11} c_{1\,s_1}$ не определено в M_{s_1}, и мы можем присоединить новый элемент d_{11} с соотношением

$$b_{11} *_{11} c_{1\,s_1} = d_{11}. \tag{16}$$

Как и выше, покажем, что в полученной частичной квазигруппе M_{s_1+1} не определено $b_{12} *_{12} d_{11}$. Если выполнено соотношение $b_{12} *_{12} d_{11} = d$ при некотором d, то оно является тривиальным следствием соотношения (16). Следовательно, (16) совпадает с соотношением $b_{12} *_{12}^{-1} d = d_{11}$, и потому $b_{11} = b_{12}$ и $*_{11}$ совпадает с $*_{12}^{-1}$. Отсюда видно, что T_1 сократимо, вопреки условию. Продолжая этот процесс, мы получаем частичную квазигруппу $M_{s_1+t_1}$ с последним присоединённым элементом

$$d_{1\,t_1} = b_{1\,t_1} *_{1\,t_1} d_{1\,t_1-1}. \tag{17}$$

Заметим, что $Sd_{1\,t_1-1} = cS_1''T_1'$.

Далее согласно равенству (12) мы должны вычислять элемент $d_{1\,t_1} \circ_{21} a_{21}$. Покажем, что он не определён в $M_{s_1+t_1}$. Допустим, что в $M_{s_1+t_1}$ выполняется равенство $d_{1\,t_1} \circ_{21} a_{21} = d$. Так как оно является тривиальным следствием соотношения (17), то $d_{1\,t_1-1} = a_{21}$, т. е. $cS_1''T1' = a_{21}$. Последнее равенство противоречит условию а) леммы 2 при $i = 1$. Следовательно, $d_{1\,t_1} \circ_{21} a_{21}$ не определено в $M_{s_1+t_1}$, и мы можем присоединить новый элемент c_{21} с соотношением $d_{1\,t_1} \circ_{21} a_{21} = c_{21}$.

Продолжая этот процесс последовательного присоединения по одному новому элементу, мы в итоге получаем частичную квазигруппу M_{n-1}, где $n - 1 = s_1 + t_1 + \ldots + s_k + t_k$, в которой определено слово из левой части равенства (12), причём последним будет присоединён элемент $d_{k\,t_k}$ с соотношением

$$d_{k\,t_k} = b_{k\,t_k} *_{k\,t_k} d_{k\,t_k-1}, \tag{18}$$

где

$$d_{k\,t_k-1} = cS_1''T_1S_2T_2\ldots S_kT_k', \quad d_{k\,t_k} = cS_1''T_1S_2T_2\ldots S_kT_k. \tag{19}$$

По условию в M_1 не было определено $c \circ_{11}^{-1} a_{11}$. Легко убедиться, что эта ситуация сохранится и в M_{n-1}. Действительно, в ходе построения частичной квазигруппы M_{n-1} мы на каждом шаге присоединяли новый элемент с соотношением, в которое входили вновь присоединяемый элемент и элемент, присоединённый на предыдущем шаге. В силу условия R таким же свойством обладали и следствия этих соотношений. Поэтому табличного соотношения с левой частью $c \circ_{11}^{-1} a_{11}$ появиться не могло. Присоединив теперь к M_{n-1} новый элемент u с соотношением $c \circ_{11}^{-1} a_{11} = u$, мы и получим искомое расширение M_n. В случае, когда $t_1 = 1$, рассуждения аналогичны. Разница лишь в том, что здесь на первом шаге будет присоединён новый элемент d_{11} с соотношением $b_{11} *_{11} c = d_{11}$. □

Случай II.

Этот случай отличается от случая I лишь тем, что здесь в представлении (10) для элемента g будет отсутствовать сомножитель T_k. Поэтому тот же процесс последовательного расширения закончится раньше. Здесь $n - 1 = s_1 + t_1 + \ldots + s_{k-1} + t_{k-1} + s_k$ и M_{n-1} будет получен присоединением элемента $c_{k\,s_k}$ с соотношением

$$c_{k\,s_k} = c_{k\,s_k-1} \circ_{k\,s_k} a_{k\,s_k},$$

где

$$c_{k\,s_k-1} = cS_1''T_1S_2T_2\ldots S_k', \quad c_{k\,s_k} = cS_1''T_1S_2T_2\ldots S_k.$$

Построим сначала минимальное конечно свободное расширение M' частичной квазигруппы M, в котором определены все элементы a_{ij}, b_{ij} из (11). Если в M' найдётся элемент c, удовлетворяющий условиям леммы 2, то положим $M_1 = M'$. В противном случае будем расширять M' до тех пор, пока не присоединим элемент, удовлетворяющий условиям леммы 2. Так как условия леммы 2 накладывают на требуемый элемент c лишь конечное число ограничений, а последовательность простых свободных расширений не ограничена, то расширение M_1 с требуемым элементом c найдётся. Больше того, найдётся расширение с любым числом элементов c, удовлетворяющих условиям леммы 2.

Теперь построим конечно свободное расширение M_n частичной квазигруппы M_1 по схеме, указанной в доказательстве леммы 2. Рассмотрим отдельно случаи I, II.

Случай I. По допущению равенство (11) выполняется при любом $u \in Q$, а потому и при $u = c \circ_{11}^{-1} a_{11}$ — последнем присоединённом элементе при построении M_n. Следовательно, в соотношении (15) $d_{k\,t_k} = u$, и оно является тривиальным следствием соотношения $u = c \circ_{11}^{-1} a_{11}$. Отсюда получаем, что $d_{k\,t_k-1} = a_{11}$, что вместе с первым равенством из (16) противоречит условию а) леммы 2 при $i = k$. Следовательно, случай I в действительности невозможен.

Случай II. Из равенства (11) при $u = c \circ_{11}^{-1} a_{11}$ следует, что

$$c_{k-1\,s_{k-1}} = u,$$

и равенство (17) есть тривиальное следствие равенства $u = c \circ_{11}^{-1} a_{11}$. Отсюда получаем, что

$$c_{k\,s_k-1} = c, \circ_{k\,s_k} = \circ_{11}^{-1}, \quad a_{k\,s_k} = a_{11}.$$

Если $\circ_{11}$ есть $\cdot$, то $u \cdot a_{11} = c$, и мы из равенства (11) получаем

$$cS_1''T_1S_2T_2\ldots S_k' = c. \tag{20}$$

К такому же равенству приходим и в случае, когда $\circ_{11}$ есть $/$, т. е. $u/a_{11} = c$. Таким образом, равенство (20) выполняется при всех c, удовлетворяющих условиям леммы 2. Выше было отмечено, что таких элементов существует неограниченное число. Однако в [6] доказано, что при $g \neq \mathcal{E}$ равенству (10) удовлетворяют не более двух элементов. Следовательно,

$$S_1''T_1S_2T_2\ldots S_k' = \mathcal{E},$$

что противоречит предположению индукции. Теорема доказана. □

4. Описание мультипликативной группы свободной коммутативной квазигруппы

Будем считать, что многообразие коммутативных квазигрупп задано системой тождеств, состоящей из системы Σ_0 и тождества $xy = yx$.

Теорема 3. *Если Q — свободная квазигруппа в многообразии всех коммутативных квазигрупп, то*

1) *группы* $\mathrm{Mlt}(Q)$, $\mathrm{RMlt}(Q)$, $\mathrm{LMlt}(Q)$ *совпадают*;
2) *группы* $\mathrm{Mlt}(Q)$, $\mathrm{RMlt}(Q)$, $\mathrm{LMlt}(Q)$ *как абстрактные группы изоморфны свободной группе с базисом* Q.

Доказательство. Из условия коммутативности квазигруппы Q следует, что $xL_a = xR_a$ для любых $a, x \in Q$, т. е. $L_a = R_a$ для любого $a \in Q$. Отсюда и следует утверждение 1). Для доказательства утверждения 2) рассмотрим группу $G = \mathrm{RMlt}(Q)$.

Лемма 3. *Если элемент g группы G имеет непустое несократимое представление в системе образующих $R = \{Ra \colon a \in Q\}$, то $g \neq \mathcal{E}$.*

Доказательство. Пусть (1) есть непустое несократимое представление элемента g. Допустим, что $g = \mathcal{E}$, т. е. равенство (2)

$$\Big(\big(\ldots\big((u \circ_1 a_1) \circ_2 a_2\big)\ldots\big) \circ_{k-1} a_{k-1}\Big) \circ_k a_k = u$$

выполняется при любом $u \in Q$. Построим минимальное конечно свободное расширение M_1 частичной квазигруппы M, в котором определены все элементы $a_1, \ldots, a_k$ и существует элемент c_1, такой что $c_1 \circ_1^{-1} a_1$, $c_1 \circ_2 a_2$ не определены в M_1, $c_1 \neq a_3$. Очевидно, что такое расширение существует. Теперь расширим M_1 до M_2, присоединив новый элемент v с соотношением $v = c_1 \circ_1^{-1} a_1$. Докажем, что $c_1 \circ_2 a_2$ не определено в M_2. Допустим, что $c_1 \circ_2 a_2$ определено в M_2. По условию R каждое следствие последнего соотношения должно содержать элемент v. А так как $c_1, a_2 \in M_1$, а $v \notin M_1$, то $c_1, a_2 \neq v$. Следовательно, $c_1 \circ_2 a_2 = v$. Если $\circ_1^{-1} = \cdot$, то соотношение $c_1 \circ_2 a_2 = v$ может совпадать лишь с соотношением $a_1 \circ_1^{-1} c_1 = v$. Если же $\circ_1^{-1} = \cdot$, то $c_1 \circ_2 a_2 = v$ может совпадать лишь с соотношением $c_1 \circ_1^{-1} a_1 = v$. Во всех случаях получаем $\circ_2 = \circ_1^{-1}$ и $a_1 = a_2$, что свидетельствует о сократимости представления (1). Значит, $c_1 \circ_2 a_2$ не определено в M_2 и можно построить расширение

$$M_3 = [M_2 \colon c_1 \circ_2 a_2 = c_2].$$

Покажем, что в M_3 не определено $c_2 \circ_3 a_3$. Допустим, что $c_2 \circ_3 a_3 = d$. Тогда соотношение $c_2 = d \circ_3^{-1} a_3$ является тривиальным следствием соотношения $c_2 = c_1 \circ_2 a_2$. Возможны два случая.

1. $\circ_2 = /$, т. е. $c_2 = c_1 / a_2$. Так как $\circ_3^{-1} \neq \backslash$, то соотношение $c_2 = d \circ_3^{-1} a_3$ может совпадать лишь с соотношением $c_2 = c_1 / a_2$, что влечёт сократимость представления (1).

2. $\circ_2 = \cdot$, т. е. $c_2 = c_1 \cdot a_2$. Тогда соотношение $c_2 = d \circ_3^{-1} a_3$ должно совпадать с одним из следующих соотношений:

а) $c_2 = c_1 \cdot a_2$,
б) $c_2 = a_2 \cdot c_1$.

Совпадение с а) ведёт к сократимости представления (1), совпадение с б) влечёт $a_3 = c_1$. В каждом случае мы приходим к противоречию с условием.

Таким образом, $c_2 \circ_3 a_3$ не определено в M_3, и мы можем построить расширение

$$M_4 = [M_3 \colon c_2 \circ_3 a_3 = c_3].$$

Продолжая этот процесс, мы построим расширение

$$M_{i+1} = [M_i \colon c_{i-1} \circ_i a_i = c_i], \quad 3 \leqslant i \leqslant k-1.$$

Покажем, что в нём не определено $c_i \circ_{i+1} a_{i+1}$. Допустив, что $c_i \circ_{i+1} a_{i+1} = d$, мы теми же рассуждениями, что и выше, в пунктах 1 и 2, придём либо к сократимости представления (1), что противоречит условию, либо к совпадению соотношения $c_i = d \circ_{i+1}^{-1} a_{i+1}$ с соотношением $a_i \cdot c_{i-1} = c_i$. В последнем случае получаем равенство $c_{i-1} = a_{i+1}$, которое невозможно, поскольку $a_{i+1} \in M_1$, $c_{i-1} \notin M_1$. Отсюда при $i = k-1$ получаем, что в M_k не определено $c_{k-1} \circ_k a_k$. Тогда в M_k, а потому и в Q, $c_{k-1} \circ_k a_k \neq v$. Следовательно, при $u = v$ равенство (2) не выполняется и, значит, $g \neq \mathcal{E}$. Лемма доказана. □

Доказательство теоремы 3 проводится точно так же, как и доказательство утверждения теоремы 1 о свободе группы $\mathrm{RMlt}(Q)$, разница лишь в том что вместо леммы 1 используется лемма 3. □

Аналогичным образом доказывается теорема 4.

Теорема 4. *Если Q — свободная квазигруппа в многообразии всех TS-квазигрупп, то*

1) *группы* $\mathrm{Mlt}(Q)$, $\mathrm{RMlt}(Q)$, $\mathrm{LMlt}(Q)$ *совпадают*;
2) *группы* $\mathrm{Mlt}(Q)$, $\mathrm{RMlt}(Q)$, $\mathrm{LMlt}(Q)$ *как абстрактные группы задаются системой образующих R_Q и системой определяющих соотношений $S = \{R_a^2 \colon a \in Q\}$.*

Замечание. Утверждения теорем 1—3 останутся в силе при замене квазигрупп на лупы. При этом в определении несократимого представления элемента и несократимого слова длины, большей 1, необходимо потребовать отсутствия сомножителей R_e, L_e, соответствующих единице e лупы. В связи с этим трансляции R_e, L_e, являющиеся тождественными подстановками, можно заменить пустым словом. Тогда, как и в случаях с квазигруппами, роль единицы в мультипликативных группах будет играть пустое слово. В доказательствах же следует лишь учесть, что для любого простого свободного расширения $T = [M; a * b = c]$ частичной квазигруппы M в системе $S(T) \setminus S(M)$ кроме соотношений, указанных и использованных в теоремах 1—3, появятся ещё соотношения

$$c \cdot e = c, \quad e \cdot c = c, \quad c / e = c, \quad e \setminus c = c, \quad c / c = e, \quad c \setminus c = e,$$

которые в доказательствах не будут играть существенной роли.

Литература

[1] Белоусов В. Д. Основы теории квазигрупп и луп. — М.: Наука, 1967.

[2] Глухов М. М. R-многообразия квазигрупп и луп // Вопросы теории квазигрупп и луп. — Кишинёв, 1971. — С. 37—47.

[3] Глухов М. М. Свободные разложения и алгоритмические проблемы в R-многообразиях универсальных алгебр // Матем. сб. — 1971. — Т. 85, № 3. — С. 307—338.

[4] Глухов М. М., Гварамия А. А. Решение основных алгоритмических проблем в некоторых классах квазигрупп с тождествами // Сиб. матем. журн. — 1969. — Т. 10, № 2. — С. 297—317.

[5] Drapal A. Multiplication groups of free loops. I // Czech. Math. J. — 1996. — Vol. 46. — P. 121—131.

[6] Drapal A. Multiplication groups of free loops. II // Czech. Math. J. — 1996. — Vol. 46. — P. 201—221.

[7] Evans T. On multiplicative systems defined by generators and relations. I. Normal form theorem // Proc. Cambridge Philos. Soc. — 1951. — Vol. 47. — P. 637—649.

[8] Evans T. The word problem for abstract algebras // J. London Math. Soc. — 1951. — Vol. 28, no. 1. — P. 64—67.

[9] Wielandt H. Finite Permutation Groups. — London: Academic Press, 1964.