ФГБОУ ВО "МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ имени М. В. ЛОМОНОСОВА"
МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ

На правах рукописи

Грибов Алексей Викторович

Алгебраические неассоциативные структуры и их приложения в криптографии

Специальность 01.01.06 —
математическая логика, алгебра и теория чисел

Диссертация на соискание учёной степени
кандидата физико-математических наук

Научный руководитель:
д.ф.-м.н., профессор Михалев Александр Васильевич

Москва - 2015

Содержание

Введение

При рассмотрении алгебраических систем одной из основных задач является построение структурной теории, которая сводит изучение к более простым системам. Одной из конструкций, осуществляющих такое сведение, является радикал. С тех пор, как в 1950-х гг. А.Г. Курош [13] и С.Амицур [26] ввели аксиоматическое понятие радикала для колец и алгебр, теория радикалов распространилась и на другие алгебраические структуры. Понятие радикала в теории групп окончательно сформировалось к началу шестидесятых годов в определении, предложенном А. Г. Курошем [14]. В это же время А. Г. Курош обратил внимание на аналогию между разрешимыми нормальными подгруппами и нильпотентными идеалами, позволившую К. К. Щукину [24] построить теорию первичного радикала групп.

Описание первичного радикала группы как множества строго энгелевых элементов крайне близка к первичному радикалу в теории ассоциативных колец и алгебр. В связи с этим возник естественный вопрос о соотношении между первичным радикалом кольца с единицей и первичным радикалом подгрупп группы его обратимых элементов. Положительный ответ на него был получен А. В. Михалёвым и И. З. Голубчиком в их теореме о первичном радикале линейной группы над ассоциативным кольцом. В дальнейшем структурная теория первичного радикала алгебраических систем активно развивалась в работах [17], [8].

В теории квазигрупп некоторые понятия, например, нормальность, производная и центр, хорошо сочетаются с обычными теоретико-групповыми определениями. Р. Брак [27] показал, что обычные теоретико-групповые определения полностью корректны для луп Муфанг. Наиболее полно теория квазигрупп изложена в работе В.Д. Белоусова [2], различные классы и свойства квазигрупп рассмотрены в работах М.М. Глухова [5], Г.Б. Белявской [3] и А.Х. Табарова [23].

Теория коммутаторов и нового, с точки зрения теории групп, понятия ассоциатора в значительной степени отличается от теоретико-группового случая. Теория коммутаторов в лупах развивается в работе Дж. Смита [61]. В работе Р. Маккензи и Дж. Сноу [48] теория коммутаторов в лупах рассмотрена с точки зрения коммутаторов конгруэнций лупы как универсальной алгебры. Именно с этой точки зрения П. Войтеховский и Д. Становский [66] смогли вычислить взаимный коммутант нормальных подлуп.

Квазигруппы и латинские квадраты имеют богатую историю применений в криптографии. Достаточно полные обзоры использования квазигрупп в криптографии приведены в работе М.М. Глухова [6], где применение квазигрупп

рассмотрено для построения схем шифрования и однонаправленных функций, а такеже в работе В.А. Щербакова [59]. Основные результаты в этих работах получены для симметрической криптографии. Одной из первых работ, где использовались квазигруппы для криптографии с открытым ключом является работа С.Косельны и Г.Мюллена [41].

С алгебраической точки зрения классические задачи в криптографии рассматривались в конечнопорожденных и коммутативных группах [30], [57], [31]. Достаточно полно эти вопросы описаны в пособиях [7], [1]. Следующим шагом в развитии можно считать рассмотрение некоммутативных алгебраических структур и изучение в них вычислительно сложных задач. Одной из первых работ в некоммутативной криптографии является статья Н.Вагнера и М. Магийярика [45], где приведена схема, основанная на неразрешимости слова в конечно представленных группах (для данного представления группы G и элемента $g \in G$ определить, выполняется ли условие $g = 1$.). Достаточно полное описание и изучение аспектов некоммутативной криптографии приведено в монографии В.Шпильрайна, А.Мясникова, А.Ушакова [50]. В работах А.В. Михалева, В.Т. Маркова, А.А. Нечаева и др. [68], [12] исследованы некоторые возможности использования неассоциативных структур в криптографии с открытым ключом. В частности, была построена криптосистема над квазигрупповым кольцом, развивающая подход С.К. Россошека [21]. Также можно выделить работу В.А. Романькова [20], посвященную алгебраическому анализу существующих подходов в некоммутативной и неассоциативной криптографии.

Гомоморфное шифрование позволяет производить определённые математические действия с зашифрованным текстом и получать зашифрованный результат, который соответствует результату операций, выполняемых с открытым текстом. В 2009 году К.Джантри [32] предложил модель, основанную на алгебраических решетках, полногомоморфной алгебраической системы, то есть гомоморфной для операций умножения и сложения (и других операций) одновременно.

Цель работы

Целью диссертационной работы является исследование: строения первичного радикала ряда неассоциативных структур: луп; Ω-луп; луповых колец; связей первичного радикала луп обратимых элементов с первичным радикалом неассоциативных колец; криптографических схем над различными неассоциативными структурами; новых примеров гомоморфной криптографии.

Научная новизна

Результаты диссертации являются новыми и получены автором самостоя-

тельно. Основные результаты диссертации состоят в следующем:

1. Развита теория первичного радикала лупы, исследованы его свойства, доказано его совпадение с множеством строго энгелевых элементов лупы.

2. Получено описание Ω-первичного радикала Ω-лупы, как множества Ω-строго энгелевых элементов.

3. Установлены связи первичного радикала лупы обратимых элементов альтернативного кольца и первичного радикала кольца.

4. Построены криптографические схемы над различными неассоциативными структурами:

   – аналог схемы шифрования Эль-Гамаля над ППС-квазигруппой;

   – схема выработки общего секретного ключа над лупами Пейджа;

   – схема шифрования с открытым ключом на основе покрытий лупы Муфанг.

5. Рассмотрена схема шифрования с открытым ключом над луповым кольцом, проанализированы свойства данной схемы, доказана гомоморфность данной схемы относительно одной из операций.

Основные методы исследования

В работе применяются методы и результаты теории ассоциативных и неассоциативных колец, теории квазигрупп, теории луповых колец и криптографии с открытым ключом

Теоретическая и практическая ценность.

Работа имеет как теоретический, так и прикладной характер. Полученные в ней результаты могут быть использованы в различных задачах теории луп. Построенные криптографические схемы могут быть использованы при построении различных систем безопасности

Апробация диссертации.

Результаты диссертации докладывались на следующих конференциях:

- на семинаре “Algebra and Cryptography”, Нью-Йорк, США, 2013 г.;
- на конференции “New directions in cryptography”, Москва, 12 июня 2014.
- на конференции “Non-associative algebra and Lie theory”, Оахака, Мексика, 26-30 января 2015.

- на конференции “Индо - Российская конференция по алгебре, теории чисел, дискретной математике и их приложений”, Москва, 15-17 октября 2014.

  а также на следующих семинарах кафедры высшей алгебры механико-математического факультета МГУ:

- на научно-исследовательском семинаре кафедры высшей алгебры, 2009–2015 гг., неоднократно;
- на семинаре “Теория колец”, 2009–2015 гг., неоднократно;

Публикации

Основные результаты диссертации опубликованы в работах, список которых приведен в конце библиографии.

Структура диссертации Диссертационная работа состоит из четырех глав. Текст диссертации изложен на 93 листах. Список литературы содержит 72 наименования.

Во **введении** даётся краткий исторический обзор и формулируются основные результаты диссертации.

В **главе 1** в **разделе 1.1** определяются основные понятия, терминология, принятая при изложении, и вспомогательные утверждения.

В **разделе 1.2** излагается понятие коммутанта нормальных подлуп и приводятся порождающие множества этого коммутатнта. Пусть $(L, \cdot)$ – лупа, тогда можно дополнительно рассматривать операции $\backslash, /$ такие, что $x \setminus (x/y) = y; \quad x \cdot (x \setminus y) = y; \quad (y \cdot x)/x = y; \quad (y/x) \cdot x = y$. Для каждого $x \in L$ определим биективные отображения $L_x, R_x, M_x : G \to G$:

$$L_x(y) = xy, R_x(y) = yx, M_x(y) = y \setminus x, y \in G.$$

Далее определим биективные отображения

$$L_{x,y} = L_{xy}^{-1} L_x L_y, \quad R_{x,y} = R_{xy}^{-1} R_x R_y, \quad M_{x,y} = M_{y \setminus x}^{-1} M_x M_y.$$

Следующее утверждение описывает взаимный коммутант нормальных подлуп.

Следствие 1.49. *Пусть L – лупа, A, B – нормальные подлупы лупы L, тогда*

$$[A, B]_L = Ng([a, b]_L, [b, a, x]_L, w_{u_1,u_2}(a)/w_{v_1,v_2}(a) :$$
$$w \in \{L, R, M\}, a \in A, b \in B, u_i/v_i \in B, x \in L),$$

Причем,

1) если L – IP-лупа, то

$$[A,B]_L = Ng([a,b]_L, L_{u_1,u_2}(a)/L_{v_1,v_2}(a) : a \in A, b \in B, u_i/v_i \in B);$$

2) если L – коммутативная лупа, то

$$[A,B]_L = Ng(w_{u_1,u_2}(a)/w_{v_1,v_2}(a) : w \in \{L,M\}, a \in A, u_i/v_i \in B);$$

3) если L – группа, то

$$[A,B]_L =< [a,b]_L : a \in A, b \in B > .$$

где $Ng(X)$ – наименьшая нормальная подлупа, содержащая множество X.

В **разделе 1.3** вводится понятие первичного радикала лупы и строго энгелева элемента.

Определение 1.54. *Лупа $(L,\cdot)$ называется первичной, если для любых ее двух нормальных подлуп A,B из равенства $[A,B]_L = E$ следует, что либо $A = E$, либо $B = E$, где E – единичная подлупа лупы L.*

Определение 1.59. *Пусть $(L,\cdot)$ – лупа. Элемент $a \in L$ называется строго энгелевым, если в любой последовательности $a_0, a_1, \ldots$ элементов лупы L, удовлетворяющей условию $a_0 = a, a_{i+1} \in [Ng(a_i), Ng(a_i)]_L$, начиная с некоторого номера все элементы равны 1.*

Основным результатом этого раздела является:

Теорема 1.61. *Первичный радикал $rad(L)$ лупы $(L,\cdot)$ совпадает с множеством всех строго энгелевых элементов лупы.*

В **разделе 1.4** получено описание первичного радикала Ω-лупы. Лупа $(L,+)$ (не обязательно, коммутативная или ассоциативная) называется лупой с операторами или Ω-лупой, если в L задана помимо сложения еще система n-арных алгебраических операций Ω, причем для всех $\omega \in \Omega$ должно выполняться условие $00\ldots0\omega = 0$. Идеал P в Ω-лупе L называется Ω-первичным, если для любой операции $\omega \in \Omega$ и любых идеалов $I_1, \ldots, I_n \subseteq L$ из включения $(I_1, \ldots, I_n)\omega \subseteq P$ следует, что $I_j \subseteq P$ для некоторого $j = 1, 2, \ldots, n$. Пересечение всех Ω-первичных идеалов Ω-лупы L называется первичным радикалом Ω-$rad(L)$ лупы L. Обозначим через $\{a\}^L$ идеал Ω-лупы L, порождённый элементом $a \in L$. Подмножество M Ω-лупы L называется Ω-m-системой, если для любой операции $\omega \in \Omega$ и любых элементов $a_1, \ldots, a_n \in M$ существуют $a_i' \in \{a_i\}^L$, такие что $a_1' \ldots a_n'\omega \in M$. Теперь каждому элементу $a \in L$ поставим

в соответствие подмножество $M_a \subseteq L$, которое получается следующим образом: $M_a = \cup_i A_i$, где

$$A_0 = a, A_i = \cup_{\lambda\in\Lambda} A_{i,\lambda}, A_{i,\lambda} = \{a_{i,j_1\ldots j_n} = a'_{i-1,j_1}\ldots a'_{i-1,j_n}\omega_\lambda\},$$

где ω_λ – n-арная операция, $a'_{i,j_k} \in \{a_{i,j_k}\}^L$, $a_{i,j_1}, \ldots, a_{i,j_n}$ – всевозможные наборы по n элементов из A_i.

Основной результат:

Теорема 1.72. *Пусть $a \in L$, где L – Ω-лупа, тогда эквивалентны следующие условия:*

1) $a \in \Omega$-$rad(L)$;

2) любая Ω-m-система, содержащая элемент a, содержит 0;

3) любая Ω-m-система M_a, соответствующая элементу a, содержит 0,

В начале **главы 2** излагается описание первичного радикала неассоциативных s-колец и показываются некоторые его свойства (в частности, его совпадение с множеством строго нильпотентных элементов s-кольца).

В **разделе 2.1** приводятся классические результаты для альтернативных колец. Отметим теорему, описывающую лупу обратимых элементов альтернативного кольца.

Теорема 2.13. *Пусть R – альтернативное кольцо с единицей, тогда множество обратимых элементов $U(R)$ является лупой Муфанг.*

Также рассмотрены различные свойства первичных альтернативных колец.

В **разделе 2.2** приведены различные свойства альтернативных луповых колец. Получено необходимое и достаточное условие того, что луповое кольцо является альтернативным.

Определение 2.20. *Лупа L для которой луповое кольцо KL, где K – коммутативное и ассоциативное кольцо с единицей и $charK \neq 2$, является альтернативным неассоциативным кольцом называется RA-лупой.*

Будем называть упорядоченную тройку элементов лупы (a, b, c) неассоциативной, если равенство ассоциативности не выполняется для этих элементов (т.е. $a(bc) \neq (ab)c$). Соответственно, упорядоченная тройка (a, b, c) ассоциативна, если $a(bc) = (ab)c$.

Теорема 2.21. *Лупа L является RA-лупой тогда и только тогда, когда выполняются следующие условия:*

1. *если какие-либо элементы лупы ассоциативны в нектором порядке, то они ассоциативны в любом другом порядке;*

2. *если элементы $a, b, c \in L$ неассоциативны, то $a \cdot bc = ac \cdot b = c \cdot ab$;*

В **разделе 2.3** исследовано строение первичного радикала лупы обратимых элементов альтернативного кольца. Основной результат:

Теорема 2.38. *Если R – альтернативное кольцо с единицей, то для любой подлупы L лупы $U(R)$ выполняется включение $L \cap Z(R, rad\ R) \subseteq radL$.*

В **разделе 2.4** получено описание первичного радикала лупы обратимых элементов альтернативного кольца $GLL(2, R)$ (неассоциативный аналог теоремы А.В. Михалева и И.З. Голубчика). Основным результатом этого раздела является:

Теорема 2.40. *Пусть K – коммутативное и ассоциативное кольцо с единицей, $\mathcal{Z}(K)$ – кольцо матриц Цорна и $GLL(2, K)$ – лупа обратимых матриц из $\mathcal{Z}(K)$, тогда $rad\ GLL(2, K) = Z(\mathcal{Z}(K), rad\ \mathcal{Z}(K))$.*

В **главе 3** описаны некоторые криптографические схемы с открытым ключом. Расширены на лупы некоторые известные алгоритмы для криптографии, основанной на группах.

В **разделе 3.1** построена схема шифрования с открытым ключом над луповым кольцом.

Пусть K – кольцо с единицей (необязательно ассоциативное), Q – квазигруппа, KQ – луповое кольцо.

Участник A :

1. Конструирует автоморфизмы $\sigma \in AutK, \eta \in AutQ$, такие что $|\sigma| \geq t_3, |\eta| \geq t_5$, причем выполняются следующие условия на централизаторы $|C(\sigma) \setminus \langle\sigma\rangle| \geq t_4$ и $|C(\eta) \setminus \langle\eta\rangle| \geq t_6$, где t_3, t_4, t_5, t_6 - параметры безопастности.

2. Случайно выбирает автоморфизмы $\tau \in C(\sigma) \setminus \langle\sigma\rangle$ и $\omega \in C(\eta) \setminus \langle\eta\rangle$.

3. По τ и ω строит секретный автоморфизм $\varphi \in AutKQ$ так: для любого $h \in KQ$ вида $h = a_{q_1}q_1 + \cdots + a_{q_n}q_n$, пусть $\varphi(h) = \tau(a_{q_1})\omega(q_1) + \cdots + \tau(a_{q_n})\omega(q_n)$.

4. Выбирает элементы $a \in KQ, x \in KQ$ и вычисляет $\varphi(x)$ и $\varphi(a)$.

Открытым ключом участника A является:

$$\Big(\sigma, \eta, x, \varphi(x), a, \varphi(a)\Big).$$

Участник B:

1. Выбирает натуральные числа (i, j, k, l) и с помощью пар автоморфизмов (σ^i, η^j),(σ^k, η^l) строит сеансовые автоморфизмы $\psi, \chi \in AutKQ$.

2. Вычисляет $(\chi(a) \cdot \psi(x)$, $\chi(\varphi(a)) \cdot \psi(\varphi(x))$ и левый аннулятор $Ann\big(\chi(\varphi(a)) \cdot \psi(\varphi(x))\big)$.

3. Записывает исходный текст, который надо передать, в виде $m \in KL$ и вычисляет $m \cdot \Big[\chi(\varphi(a)) \cdot \psi(\varphi(x))\Big]$.

4. Отправляет для A криптограмму

$$\Big(\chi(a) \cdot \psi(x),\, m \cdot \Big[\chi\big(\varphi(a)\big) \cdot \psi\big(\varphi(x)\big)\Big]\Big)$$

Получив криптограмму, участник A расшифровывает её:

1. Используя секретный автоморфизм φ, вычисляет $\varphi\big(\chi(a) \cdot \psi(x)\big)$.

2. Расшифровывает посланный текст, пользуясь тем, что χ, ψ и φ коммутируют, поскольку сеансовые автоморфизмы ψ, χ построены на степенях выбранных автоморфизмов σ, η, а секретный автоморфизм φ построен с помощью элементов из централизаторов для σ, η.

В **разделе 3.2** доказана гомоморфность данной схемы по отношению к одной из операций. В **разделе 3.3** приведен аналог схемы шифрования Эль-Гамаля над ППС-квазигруппой и доказана ее гомоморфность для медиальных квазигрупп. В **разделе 3.4** построена MQ-криптосхема над альтернативным кольцом. В **разделе 3.5** исследуются криптографичесие примитивы над лупами. В частности, схема выработки общего секретного ключа над лупами Пейджа и схема шифрования с открытым ключом на основе покрытий лупы Муфанг.

В **приложении** приведена программа на языке компьютерной системы GAP для анализа параметров безопасности криптосхемы на луповом кольце.

1 Квазигруппы, лупы и Ω-лупы: первичный радикал

1.1 Основные понятия и предварительные сведения

Определение 1.1. *Группоидом называется непустое множество G с заданной бинарной операцией, обозначение $(G, \cdot)$.*

Группоид $(Q, \cdot)$ называется квазигруппой, если для любых $a, b \in Q$ уравнения $x \cdot a = b, a \cdot y = b$ всегда разрешимы, причем однозначно.

Пусть $(G, \cdot)$ – группоид. Для каждого $x \in L$ определим биективные отображения (*трансляции*) $L_x, R_x : G \to G$:

$$L_x(y) = xy, R_x(y) = yx, y \in G.$$

Тогда определение квазигруппы эквивалентно следующему: квазигруппа – это такой группоид $(Q, \cdot)$, что отображения L_x и R_x являются биекциями для всех $x \in Q$.

Определение 1.2. *Группоид $(L, \cdot)$ называется лупой, если $(L, \cdot)$ является квазигруппой с единицей.*

Непустое подмножество H множества L называется подлупой лупы $(L, \cdot)$, если $(H, \cdot)$ является лупой.

Также можно определить лупу как универсальную алгебру: лупой называется универсальная алгебра $(L, 1, \cdot, /, \setminus)$ с тождествами:

$$x \cdot 1 = 1 \cdot x = x; \quad x \setminus (x/y) = y; \quad x \cdot (x \setminus y) = y; \quad (y \cdot x)/x = y; \quad (y/x) \cdot x = y.$$

Пусть $(L, \cdot)$ является лупой, H – подлупа лупы L. Если $a \in L$, то определим множества $aH = \{a \cdot h | h \in H\}$ и $Ha = \{h \cdot a | h \in H\}$. Подмножества aH и Ha являются подмножествами в L и называются, соответственно, *левым и правым смежным классом* по подлупе H для элемента $a \in L$.

Будем говорить, что $(L, \cdot)$ *имеет левое (правое) расложение на классы по модулю H*, если множество всех левых (правых) классов по подлупе H является разбиением лупы L.

Теорема 1.3 (см. [54]). *Пусть $(H, \cdot)$ – подлупа лупы L. Лупа $(L, \cdot)$ имеет левое (правое) разложение на классы по подлупе H, тогда и только тогда, когда $(a \cdot h)H = aH (H(h \cdot a) = Ha)$ для всех $a \in L, h \in H$.*

Определение 1.4. *Пусть$(H, \cdot)$ – подлупа лупы $(L, \cdot)$. Тогда H называется нормальной подлупой, если для любых $x, y \in L$:*

$$xH = Hx; (xH)y = x(Hy); x(yH) = (xy)H.$$

Отметим, что если $(H,\cdot)$ – нормальная подлупа лупы $(L,\cdot)$, то лупа $(L,\cdot)$ имеет левое и правое разложение на смежные классы по подлупе H, причем они совпадают.

Определение 1.5. *Пусть $(H,\cdot)$ – нормальная подлупа лупы $(L,\cdot)$, тогда лупа $L/H = (\{aH|a \in L\},\cdot)$ с операцией $xH \cdot yH = (xy)H$ называется факторлупой по нормальной подлупе $(H,\cdot)$.*

Лемма 1.6 (см. [27]). *Пересечение нормальных подлуп лупы является нормальной подлупой. Подлупа, порожденная нормальными подлупами, является нормальной подлупой.*

Рассмотрим понятие мультипликативной группы лупы.

Обратными к отображениям $L_x, R_x, x \in L$, и отображению $M_x : G \to G$ такого, что $M_x(y) = y \setminus x$, являются отображения $L_x^{-1}, R_x^{-1}, M_x^{-1}$ для которых:

$$L_x^{-1}(y) = x \setminus y; R_x^{-1}(y) = y/x; M_x^{-1}(y) = x/y, y \in L,$$

поскольку $L_x(L_x^{-1}(y)) = L_x(x \setminus y) = x(x \setminus y) = y$ и $L_x^{-1}(L_x(y)) = L_x^{-1}(xy) = x \setminus (xy) = y$. Далее, $R_x(R_x^{-1}(y)) = R_x(y/x) = (y/x)x = y$ и $R_x^{-1}(R_x(y)) = R_x^{-1}(yx) = (yx/x) = y$, $M_x(M_x^{-1}(y)) = M_x(x/y) = (x/y)\setminus x = y$ и $M_x^{-1}(M_x(y)) = M_x^{-1}(y \setminus x) = x/(y \setminus x) = y$.

Определение 1.7. *Мультипликативной группой $Mlt(L)$ лупы L называется группа, порожденная всеми правыми и левыми трансляциями*

$$Mlt(L) =< L_x, R_x : x \in L >$$

в моноиде всех отображений из L в L.

Группой внутренних отображений $Inn(L)$ лупы L называется стабилизатор для 1 в группе $Mlt(L)$, т.е. $Inn(L) =< \alpha \in Mlt(L) : \alpha(1) = 1 >$.

Замечание 1.8. *Отметим, что группа $Inn(L)$ может не являться подгруппой группы автоморфизмов $Aut(L)$, хотя для групп это верно.*

Действительно, рассмотрим лупу $(L,\cdot)$ со следующей таблицей умножения:

	1	*2*	*3*	*4*	*5*
1	*1*	*2*	*3*	*4*	*5*
2	*2*	*1*	*5*	*3*	*4*
3	*3*	*5*	*4*	*2*	*1*
4	*4*	*3*	*1*	*5*	*2*
5	*5*	*4*	*2*	*1*	*3*

При этом $Inn(L) =< (2,4,5),(3,5) >$, $Aut(L) \simeq Z_3$. *Таким образом, группа* $Inn(L)$ *не является подгруппой в* $Aut(L)$.

Определение 1.9. *Полной мультипликативной группой* $TotMlt(L)$ *лупы* L *называется группа:*

$$TotMlt(L) =< L_x, R_x, M_x : x \in L > .$$

Аналогично, полной группой внутренних отображений $TotInn(L)$ лупы L называется стабилизатор для 1 в группе $TotMlt(L)$.

Определим биективные отображения $L_{x,y} = L_{xy}^{-1} L_x L_y, \quad R_{x,y} = R_{xy}^{-1} R_x R_y,$ $M_{x,y} = M_{y\backslash x}^{-1} M_x M_y, \quad T_x = R_x^{-1} L_x, \quad U_x = R_x^{-1} M_x$. Также рассмотрим отображения $A^{\circ}_{x,y}, B^{\circ}_{x,y}$, значения которых задаются соотношениями $(z \cdot x) \circ y = A^{\circ}_{x,y}(z) \cdot (x \circ y), \quad y \circ (z \cdot x) = B^{\circ}_{x,y}(z) \cdot (y \circ x)$, где $\circ \in \{\cdot, \backslash, /\}$.

Лемма 1.10 (см. [66]). *Пусть* L *– лупа, тогда*

$$Inn(L) =< L_{x,y}, R_{x,y}, T_x : x, y \in L >=< A^{\cdot}_{x,y}, B^{\cdot}_{x,y} : x, y \in L > .$$

Заметим, что $Inn(L) = 1$ тогда и только тогда, когда L является абелевой группой. Так же, как и в случае групп, группу $Inn(L)$ можно использовать для характеризации нормальных подлуп.

Лемма 1.11 (см. [27]). *Подлупа* H *лупы* $(L, \cdot)$ *является нормальной, тогда и только тогда, когда* $\varphi(H) = H$ *для всех* $\varphi \in Inn(L)$.

Полная группа внутренних отображений $TotInn(L)$ также может использоваться для характеризации нормальных подлуп.

Лемма 1.12 (см. [66]). *Пусть* L *– лупа, тогда*

$$TotInn(L) =< L_{x,y}, R_{x,y}, M_{x,y}, T_x, U_x : x, y \in L >=< A^{\cdot}_{x,y}, B^{\cdot}_{x,y}, A^{\backslash}_{x,y} : x, y \in L > .$$

Следствие 1.13. *Подлупа* H *лупы* $(L, \cdot)$ *является нормальной, тогда и только тогда, когда* $f(H) = H$, *для всех* $f \in TotInn(L)$.

Доказательство. В силу лемм 1.11 и 1.12, остается показать, что если $N \trianglelefteq L$, то $U_x(a) = (a \setminus x)/x \in N$ и $M_{x,y}(a) = (y \setminus x)/((a \setminus y)x) \in N$ для всех $x, y \in L$ и $a \in N$. Пусть ϕ является гомоморфизмом из L в такую лупу, что $N = ker(\phi)$. Тогда $\phi(U_x(a)) = (\phi(a) \setminus \phi(x))/\phi(x) = U_{\phi(x)}(\phi(a)) = U_{\phi(x)}(1) = 1$. Аналогично $\phi(M_{x,y}(a)) = M_{\phi(x),\phi(y)}(\phi(a)) = M_{\phi(x),\phi(y)}(1) = 1$.

□

В работе [66] отмечено, что в общем случае ни одно из этих отображений не может быть удалено из приведенных порождающих отображений группы $TotInn(L)$. Однако, для определенных классов луп можно сократить количество порождающих.

Определение 1.14. *Квазигруппа $(Q,\cdot)$ называется LIP-квазигруппой, если существует биективное отображение $J_\lambda : Q \to Q$ такое, что $J_\lambda : a \to a^\lambda$, где $a^\lambda(ax) = x$ для всех $x \in Q$. Аналогично, квазигруппа $(Q,\cdot)$ называется RIP-квазигруппой, если существует биективное отображение $J_\rho : Q \to Q$ такое, что $J_\rho : a \to a^\rho$, где $(xa)a^\rho = x$ для всех $x \in Q$.*

Квазигруппа, которая обладает обоими свойствами называется IP - квазигруппой.

Техника работы с внутренними отображениями хорошо показана в доказательстве следующей леммы.

Лемма 1.15 (см. также [66]). *Пусть $(L,\cdot)$ – лупа, тогда выполняются следующие утверждения:*

1. *Если L – IP-лупа, то $TotInn(L) =< L_{x,y}, T_x, J : x, y \in L >$;*
2. *Если L – коммутативная лупа, то $TotInn(L) =< L_{x,y}, M_{x,y}, U_x : x, y \in L >$;*
3. *Если L – группа, то $TotInn(L) =< T_x, J : x, y \in L >$.*

Доказательство. 1. Пусть L является IP-лупой, тогда $L_{x^{-1}} = L_x^{-1}, R_{x^{-1}} = R_x^{-1}$ и $M_x(y) = y \setminus x = y^{-1}x = R_xJ(y)$ и $J = R_x^{-1}M_x = U_x$. Таким образом, M_x и J являются внутренними отображениями. Для доказательства первого пункта по лемме 1.12 необходимо показать, что отображения $M_{x,y}, R_{x,y}$ можно выразить через $L_{x,y}, T_x, J$. Заметим. что $M_xM_x(y) = M_x(y^{-1}x) = x^{-1}yx = T_{x^{-1}}(y)$, далее $M_{x,y} = M^{-1}_{y^{-1}x}M_xM_y = (R_{y^{-1}x}J)^{-1}R_xJM_y = JR^{-1}_{y^{-1}x}R_xJM_y = JR^{-1}_{y^{-1}x}R_xR_{y^{-1}}R_yJM_y = JR_{x,y^{-1}}M_yM_y = JR_{x,y^{-1}}T_{y^{-1}}$. Более того из IP-свойства следует $L_{x,y}(z)^{-1} = ((xy)^{-1}\cdot x(yx))^{-1} = (z^{-1}y^{-1})x^{-1}\cdot(y^{-1}x^{-1})^{-1} = R_{x^{-1},y^{-1}}(z^{-1})$, т.е. $JL_{x,y}J = R_{x^{-1},y^{-1}}$.

2. Если L – коммутативная лупа, то $R_{x,y} = L_{x,y}$ и $T_x = 1$. Поэтому второй пункт следует из первого.

3. Если L является группой, то $L_{x,y} = 1$. Поэтому третий пункт также следует из первого.

□

Далее рассмотрим понятие центра лупы.

Определение 1.16. *Центром лупы* $(L, \cdot)$ *называется множество*

$$Z(L) = \{a \in L : ax = xa, a(xy) = (ax)y, x(ay) = (xa)y, x(ya) = (xy)a\}$$

для всех x, y *из* L.

Наряду с центром часто рассматривают следующие ядра лупы.

Определение 1.17. *Левым* N_λ, *средним* N_μ *и правым* N_ρ *ядрами лупы* $(L, \cdot)$ *называются подмножества*

$$N_\lambda = \{a \in L | a(xy) = (ax)y\},$$

$$N_\mu = \{a \in L | ((xa)y = x(ay)\},$$

$$N_\rho = \{a \in L | ((xy)a = x(ya)\}$$

для всех $x, y \in L$.

Ядром лупы L *называется подмножество* $N = N_\lambda \cap N_\mu \cap N_\rho$.

В терминах левых и правых трансляций данные подмножества имеют следующий вид:

$$N_\lambda = \{a \in L | L(ax) = L(x)L(a), \forall x \in L, \};$$

$$N_\mu = \{a \in L | L(xa) = L(a)L(x), \forall x \in L, \};$$

$$N_\rho = \{a \in L | R(xa) = R(x)R(a), \forall x \in L.\};$$

$$Z = \{a \in N | L(a) = R(a)\}.$$

Рассмотрим некоторые свойства центра и ядра.

Теорема 1.18 (см. [54]). *Пусть* $(L, \cdot)$ *– лупа с ядром* N *и центром* Z, *тогда* N *и* Z *являются подгруппами, причем* Z *– коммутативная подгруппа группы* $(N, \cdot)$.

Теорема 1.19 (см. [54]). *Пусть* $(L, \cdot)$ *– лупа с центром* Z, *тогда* Z *является нормальной подлупой лупы* $(L, \cdot)$.

Теорема 1.20 (см. [54]). *Пусть* $(Q, \cdot)$ *– IP-квазигруппа, тогда выполняются следующие тождества:*

1. $J_\lambda^2 = J_\rho^2$ *– тождественные отображения, то есть* $(a^\lambda)^\lambda = a, (a^\rho)^\rho = a$.
2. *Уравнения* $ax = b, ya = b$ *имеют решения* $x = a^\lambda b, y = ba^\rho$, *соответственно.*

3. $(ab)^\lambda = b^\rho a^\rho, (ab)^\rho = b^\lambda a^\lambda$.

4. $R^{-1}(a) = R(a^\rho), L^{-1}(a) = L(a^\lambda)$.

Следствие 1.21. *Пусть* $(L, \cdot)$ *является LIP- или RIP-лупой, тогда* $J_\lambda = J_\rho = J$, *то есть* $a^\lambda = a^\rho = a^{-1}$ *и* $aa^{-1} = a^{-1}a = e$.

Для ядер IP-лупы выполняется равенство $N_\lambda = N_\mu = N_\rho = N$.

Теорема 1.22 (А. А. Алберт, см. [25]). *Центр лупы* $(L, \cdot)$ *изоморфен центру группы* $Mlt(L)$.

Отметим лишь вид вид изоморфизма, используемого в доказательстве: $\phi : z \to R(z) = L(z)$ для всех $z \in Z(L)$.

Некоторые другие свойства центра содержатся в работе Г.Б. Белявской [3].

В дальнейшем нам понадобятся понятия изотопии и автотопии.

Определение 1.23. *Тройка* (α, β, γ) *биективных отображений множества* Q *в множество* H *называется изотопией квазигруппы* $(Q, \cdot)$ *в квазигруппу* $(H, \circ)$, *если для всех* $x, y \in Q$ *выполняется равенство* $x\alpha \circ y\beta = (x \cdot y)\gamma$. *Квазигруппа* $(H, \circ)$ *называется изотопом* $(Q, \cdot)$.

Пусть $(\alpha_1, \beta_1, \gamma_1)$ – изотопия квазигруппы $(Q, \cdot)$ в квазигруппу $(H, \circ)$, $(\alpha_2, \beta_2, \gamma_2)$ – изотопия квазигруппы $(H, \circ)$ в $(K, *)$. Тогда $(\alpha_1\alpha_2, \beta_1\beta_2, \gamma_1\gamma_2)$ – изотопия из $(Q, \cdot)$ в $(K, *)$.

Определение 1.24. *Пусть* α, β *– перестановки множества* Q *и* ε *– тождественное отображение. Тогда тройка* $(\alpha, \beta, \varepsilon)$ *называется главной изотопией квазигруппы* $(Q, \cdot)$ *в квазигруппу* $(Q, \circ)$, *если тройка* $(\alpha, \beta, \varepsilon)$ *является изотопией.*

Теорема 1.25 (см. [54]). *Если* $(Q, \cdot)$ *и* $(H, \circ)$ *являются изотопными квазигруппами, то квазигруппа* $(H, \circ)$ *изоморфна некоторому главному изотопу квазигруппы* $(Q, \cdot)$.

Рассмотрим квазигруппу $(Q, \cdot)$ и зафиксируем элементы $g, h \in Q$. Определим операцию

$$x \circ y = xR^{-1}(g) \cdot yL^{-1}(h)$$

для всех $x, y \in Q$. Тогда $(Q, \circ)$ является главным изотопом $(Q, \cdot)$. Действительно, тройка $R(g), L(h), \varepsilon$ – главная изотопия. Заметим, что $f \cdot h$ является двухсторонним единичным элементом в квазигруппе $(Q, \circ)$. Значит, квазигруппа $(Q, \circ)$ является лупой. Таким образом, каждая квазигруппа изотопна лупе.

Лемма 1.26 (см. [54]). *Если* $(L, \cdot)$ *и* $(H, *)$ *– изотопные лупы, то существуют элементы* $g, h \in L$ *такие, что лупа* $(H, *)$ *изоморфна лупе* $(L, \circ)$, *где* $x \circ y = xR^{-1}(g) \cdot yL^{-1}(h)$ *для всех* $x, y \in L$.

Определение 1.27. *Лупа $(L,\cdot)$ называется G-лупой, если лупа $(L,\cdot)$ изоморфна каждой своей изотопной лупе.*

Лупа $(L,\cdot)$ является G-лупой тогда и только тогда, когда для всех $g,h\in L$ лупа $(L,\cdot)$ изоморфна лупе $(L,\circ)$, где $x\circ y=xR^{-1}(g)\cdot yL^{-1}(h)$ для всех $x,y\in L$. Другими словами, лупа $(L,\cdot)$ является G-лупой тогда и только тогда, когда для всех $g,h\in L$ существует перестановка $\theta(g,h)$ множества L, такая что $x\theta(g,h)R^{-1}(h)\cdot y\theta(g,h)L^{-1}(g)=(x\cdot y)\theta(g,h)$ для всех $x,y\in L$.

Определение 1.28. *Изотопия квазигруппы на себя называется автотопией.*

Теорема 1.29 (см. [54])**.** *Если $T=(U,V,W)$ – автотопия квазигруппы $(Q,\cdot)$, то две компоненты тройки T однозначно определяют третью компоненту.*

Зададим операции на множестве автотопий:

$$(U_1,V_1,W_1)\cdot(U_2,V_2,W_2)=(U_1U_2,V_1V_2,W_1W_2),(U,V,W)^{-1}=(U^{-1},V^{-1},W^{-1}).$$

Теорема 1.30 (см. [54])**.** *Множество всех автотопий квазигруппы $(Q,\cdot)$ образует группу с единицей $(\varepsilon,\varepsilon,\varepsilon)$.*

Если две квазигруппы изотопны, то их группы автотопий изоморфны.

Теорема 1.31 (см. [54])**.** *Каждая автотопия лупы $(L,\cdot)$ имеет форму*

$$(\delta R^{-1}(g),\delta L^{-1}(h),\delta),$$

где g,h – фиксированные элементы дупы, δ – биективное отображение L на себя.

Определение 1.32. *Биективное отображение U множества Q на себя называется псевдо-автоморфизмом квазигруппы $(Q,\cdot)$, если существует по крайней мере один элемент $c\in Q$, такой что для всех $x,y\in Q$ выполняется равенство*

$$xU\cdot(yU\cdot c)=(xy)U\cdot c.$$

Другими словами, биекция U называется псевдо-автоморфизмом квазигруппы $(Q,\cdot)$, если существует элемент $c\in Q$, такой что $(U,UR(c),UR(c))$ является автотопией.

Определим важный для дальнейшего класс луп.

Определение 1.33. *Лупа* $(L, \cdot)$ *называется лупой Муфанг, если выполняется тождество:*

$$(xy)(zx) = [x(yz)]x,$$

где $x, y, z \in L$.

Требуемые свойства элементов лупы Муфанг описывает следующая теорема.

Теорема 1.34 (см. [54])**.** *Для элементов лупы Муфанг верны следующие тождества:*

$1)y^{\lambda} = y^{\rho}$, *что позволяет обозначить* $y^{\lambda} = y^{\rho} = y^{-1}$;
$2)(xy)x = x(yx)$;
$3)(xy)(zx) = x[(yz)x]$;
$4)(xy)y^{-1} = x$;
$5)[(yx)z]x = y[x(zx)]$;
$6)[(xz)x]y = x[z(xy)]$;
$7)(xx)y = x(xy)$;
$8)(xy)y = x(yy)$.

Следствие 1.35. *Следующие утверждения верны для любой лупы Муфанг* $(M, \cdot)$*:*

1. $L_x R_x = R_x L_x$;
2. $L_x^{-1} = L_{x^{-1}}, R_x^{-1} = R_{x^{-1}}$;
3. $JL_x J = R_{x^{-1}}, JR_x J = L_{x^{-1}}$;
4. $L_{x,y} = JR_{x^{-1},y^{-1}}J, R_{x,y} = JL_{x^{-1},y^{-1}}J$;
5. $L_{xy} = R_{x^{-1}}L_y R_x L_x, R_{xy} = L_{y^{-1}}R_x L_y R_y$;
6. $N_{\rho} = N_{\mu} = N_{\lambda} = N$.

Следствие 1.36. *Пусть* L *– лупа Муфанг, тогда* L *является IP-лупой, т.е. для всех элементов* $x, y \in L$ *выполняется тождество* $(xy)^{-1} = y^{-1}x^{-1}$.

Доказательство: Ясно, что $(xy)^{-1}(xy) = 1$. Тогда $[(xy)^{-1}(xy)]y^{-1} = y^{-1} = (xy^{-1})[(xy)y^{-1}] = (xy)^{-1}[x(yy^{-1})] = (xy)^{-1}x$. Значит, $(xy)^{-1} = y^{-1}x^{-1}$.

□

Теорема 1.37 (см. [54])**.** *Каждое внутреннее отображение лупы Муфанг* $(M, \cdot)$ *является псевдо-автоморфизмом.*

Одной из наиболее важных является:

Теорема 1.38 (Р.Муфанг, [49]). *Пусть $(L,\cdot)$ - лупа Муфанг. Если для $x,y,z\in L$ выполняется $x(yz)=(xy)z$, то элементы x,y,z порождают подгруппу в лупе L.*

Следствие 1.39. *Любая лупа Муфанг $(M,\cdot)$ является ди-ассоциативной, то есть любые два ее элемента порождают подгруппу в M.*

Любая лупа Муфанг $(M,\cdot)$ является лупой с ассоциативными степенями.

Определение 1.40. *Центром Муфанг C для лупы Муфанг $(M,\cdot)$ называется множество элементов $c\in M$ таких, что для всех $x,y\in M$*

$$c^2(xy)=(cx)(cy).$$

Таким образом, необязательно, что $cx=xc$ для элементов центра Муфанг произвольной лупы.

Заметим, что используя свойства лупы Муфанг, данное утверждение эквивалентно тому, что

$$cx=xc$$

или

$$L(c)=R(c)$$

для всех $x\in L$.

Теорема 1.41 (см. [54]). *Центр Муфанг C лупы Муфанг $(M,\cdot)$ является подлупой.*

Центр Z лупы Муфанг $(M,\cdot)$ является нормальной подгруппой.

1.2 Коммутаторы в лупах, коммутант нормальных подлуп

Рассмотрим определение коммутатора и новое, с точки зрения теории групп, понятие ассоциатора.

Определение 1.42. *Пусть $(L,\cdot)$ – лупа, тогда коммутатором элементов $x,y\in L$ называется элемент $[x,y]_L\in L$ такой, что $xy=(yx)\cdot[x,y]_L$.*

Ассоциатором элементов $x,y,z\in L$ называется элемент $[x,y,z]_L\in L$, такой что $(xy)z=(x(yz))[x,y,z]_L$. Ассоциаторной подлупой $A(L)$ называется наименьшая нормальная подлупа лупы $(L,\cdot)$, такая что $L/A(L)$ является группой, или, что эквивалентно, наименьшая нормальная подлупа лупы $(L,\cdot)$, содержащая все ассоциаторы $[x,y,z]_L$ лупы $(L,\cdot)$.

Определение 1.43. *Производной подлупой L' лупы $(L,\cdot)$ называется наименьшая нормальная подлупа, такая что L/L' является абелевой группой. Эквивалентно, это наименьшая нормальная подлупа, содержащая все коммутаторы $[x,y]_L$ и ассоциаторы $[x,y,z]_L$ лупы L.*

Лупа $(L,\cdot)$ называется разрешимой, если $L_{[n]}=1$ для некоторого n, где $L_{[0]}=L, L_{[i+1]}=L'_{[i]}$.

Перечисленные выше понятия (нормальность, производная, центр) согласованы с теоретико-групповыми определениями. Р. Брак показал в [27], что теоретико-групповые определения корректны для луп Муфанг.

Однако, теория коммутаторов и ассоциаторов в значительной степени отличается от теоретико-группового случая.

Теория коммутаторов в лупах впервые встречается в работе Дж. Смита [61]. В работе Р. Маккензи и Дж. Соу [48] теория коммутаторов в лупах рассмотрена с точки зрения коммутаторов конгруэнций лупы как универсальной алгебры. Отметим также ряд результатов из работы П. Войтеховского и Д. Становского [66].

Рассмотрим лупу как универсальную алгебру A. Множество конгруэнций образует решетку с наибольшим элементом $1_A = A\times A$ и наименьшим элементом $0_A=(a,a):a\in A$ элементами. Пусть α,β,δ – конгруэнции лупы A. Скажем, что α централизует β над δ (обозначение $C(\alpha,\beta;\delta)$), если для любого терма t сигнатуры $\{1,\cdot,\backslash,/\}$, любой пары элементов a и b, такой что $a\alpha b$, и для любых n пар $u_i\beta v_i, i=1,\dots,n$

$$\text{из } t(a,u_1,\dots,u_n)\delta t(a,v_1,\dots,v_n) \text{ следует } t(b,u_1,\dots,u_n)\delta t(b,v_1,\dots,v_n).$$

Коммутатором $[\alpha,\beta]$ конгруэнций α,β называется наименьшая конгруэнция δ, такая что α централизует β над δ (т.е. $C(\alpha,\beta;\delta)$). В работе [48] разработана теория данной операции над конгруэнциями.

Обозначим через $Cg(X)$ наименьшую конгруэнцию, содержащую множество X, и пусть $\bar u=(u_1,\dots,u_n)$.

Теорема 1.44 (см. [66]). *Пусть V – многообразие сигнатуры $\{1,\cdot,\backslash,/\}$, $\mathcal{W}$ – множество отображений, порождающих все полные мультипликативные группы в V. Тогда*

$$[\alpha,\beta]=Cg((w_{\bar u}(a),w_{\bar v}(a)):w\in\mathcal{W},1\alpha a,u_i\beta v_i),$$

для всех конгруэнций α,β любой лупы L из V.

□

Ранее было установлено, что порождающим множеством полной мультипликативной группы является множество $\{L_{x,y}, R_{x,y}, M_{x,y}, T_x, U_x\}$.

В следующей теореме рассматривается коммутатор конгруэнций в конечных лупах (для луп с конечными правыми и левыми трансляциями).

Теорема 1.45 (см. [66]). *Пусть V – многообразие всех луп, $\mathcal{W}$ – множество отображений, порождающих все мультипликативные группы в V. Если для $L \in V$ существует такое $n > 0$, что $L_x^n = R_x^n = 1$ для любого $x \in L$, то*

$$[\alpha, \beta] = Cg((w_{\bar{u}}(a), w_{\bar{v}}(a)) : w \in \mathcal{W}, 1\alpha a, u_i \beta v_i),$$

для всех конгруэгций α, β лупы L.

Для понимания методов работы с конгруэнциями в лупах приведем доказательство следующей леммы из работы [66].

Лемма 1.46 (см. также [66]). *Пусть $\mathcal{W}$ – множество всех внутренних отображений, $w \in \mathcal{W}$. Также пусть $\equiv$ – конруэнция, которая индуцируется множеством $\mathcal{W}' = \{w' | w' \in \mathcal{W}', w' \neq w\}$ (обозначим ее $Cg((w_{\bar{u}}(a), w'_{\bar{v}}(a)) : w' \in \mathcal{W}', 1\alpha a, u_i \beta v_i)$), тогда:*

1) Отображение $w = U_x$ может быть удалено из множества $\mathcal{W}$, если $[a, x, b]_L \equiv 1$ для каждой лупы L с конгруэнциями α, β и $1\alpha a, 1\beta b, x \in L$;

2) Отображение $w = T_x$ может быть удалено из множества $\mathcal{W}$, если $[a, b]_L \equiv 1, [a, b, x]_L \equiv 1, [b, a, x]_L \equiv 1, [x, b, a]_L \equiv 1$ для каждой лупы L с конгруэнциями α, β и $1\alpha a, 1\beta b, x \in L$.

Доказательство. 1) Тождество $[a, x, b]_L \equiv 1$ может быть записано как $ax \cdot b \equiv a \cdot xb$ или $R_b R_x(a) = R_{xb}(a)$. Заменив x на $a \backslash x$ и разделив обе части слева на a, получим $a \setminus (xb) = (a \setminus x)b$ или $M_{xb} = R_b M_x(a)$ для каждого $1\alpha a, 1\beta b, x \in L$. Заметим, что если $1\alpha a, u\beta v$, то $1 = M_v^{-1} R_v(1) \alpha M_v^{-1} R_v(a)$ и $(v \setminus u)\beta 1$. В этом случае $U_u U_v^{-1}(a) = R_u^{-1} M_u M_v^{-1} R_v(a) = R_u^{-1} M_{v(v\setminus u)} M_v^{-1} R_v(a)$
$\equiv R_u^{-1} R_{v\setminus u} M_v M_v^{-1} R_v(a) = R_u^{-1} R_{v\setminus u} R_v(a) \equiv R_u^{-1} R_{v(v\setminus u)}(a) = R_u^{-1} R_u(a) = a$. Таким образом, $U_u(a) \equiv U_v(a)$.

2) Условия пункта могут быть записаны как $ab \equiv ba, a \cdot bx \equiv ab \cdot x, b \cdot ax \equiv ba \cdot x, x \cdot ba \equiv xb \cdot a$ или $L_b(a) = R_b(a), R_{bx}(a) = R_x R_b(a), L_b R_x(a) = R_x L_b(a), L_x L_b(a) = L_{xb}(a)$ для всех $1\alpha a, 1\beta b, x \in L$. Заметим, что если $1\alpha a$, $u\beta v$, то $1 = L_v^{-1} R_v(1) \alpha L_v^{-1} R_v(a)$ и $(v \backslash u)\beta 1$. В этом случае, $T_u T_v^{-1}(a) = R_u^{-1} L_u L_v^{-1} R_v(a)$ $= R_u^{-1} L_{(u/v)v} L_v^{-1} R_v(a)$. Так как $[u/v, v, L_v^{-1} R_v(a)]_L \equiv 1$, то $R_u^{-1} L_{(u/v)v} L_v^{-1} R_v(a) \equiv R_u^{-1} L_{u/v} L_v L_v^{-1} R_v(a) = R_u^{-1} L_{u/v} R_v(a)$. Так как $[u/v, a, v]_L \equiv 1$, то $R_u^{-1} L_{u/v} R_v(a) \equiv R_u^{-1} R_v L_{u/v}(a)$. Так как $[a, u/v]_L \equiv 1$, то $R_u^{-1} R_v L_{u/v}(a) \equiv R_u^{-1} R_v R_{u/v}(a)$. В заключение, так как $[a, u/v, v]_L \equiv 1$, то $R_u^{-1} R_v R_{u/v}(a) \equiv R_u^{-1} R_{(u/v)v}(a) = R_u^{-1} R_u(a) = a$. Таким образом, $T_u(a) \equiv T_v(a)$.

□

Теперь предположим, что $R_{x,y} \in \mathcal{W}$, тогда $R_{b,x}(a) \equiv R_{1,x}(a) = 1$, где $1\alpha a, 1\beta b, x \in L$, значит $[a, x, b]_L \equiv 1$.

Из теоремы 2.38, леммы 1.46 и вида порождающих отображений для мультипликативных групп вытекает следующее утверждение.

Следствие 1.47. *Пусть L – лупа и α, β – конгруэнции на L, тогда*

$$[\alpha, \beta] = Cg((w_{\bar{u}}(a), w_{\bar{v}}(a)) : w \in \mathcal{W}, 1\alpha a, u_i \beta v_i),$$

для всех конгруэнций α, β лупы L. Причем:

1) Если L – лупа, то $\mathcal{W} = \{L_{x,y}, R_{x,y}, T_x, M_{x,y}\}$;

2) Если L – IP-лупа, то $\mathcal{W} = \{L_{x,y}, T_x\}$;

3) Если L – коммутативная лупа, то $\mathcal{W} = \{L_{x,y}, M_{x,y}\}$;

4) Если L – группа, то $\mathcal{W} = \{T_x\}$.

Теперь определим зависимость между нормальными подлупами и некоторыми конгруэнциями. Пусть N является нормальной подлупой лупы L, и пусть γ_N – конгруэнция, заданная на лупе L следующим образом: $a\gamma_N b \Leftrightarrow a/b \in N$. Если α является конгруэнцией на L, то $N_\alpha = \{a \in L : a\alpha 1\}$ – нормальная подлупа лупы L.

Соответствие $\alpha \to N_\alpha, N \to \gamma_N$ между нормальными лупами и конгруэнциями позволяет сформулировать теорему 2.38 в терминах нормальных подлуп.

Вначале для двух нормальных подлуп A, B лупы L определим взаимный коммутант как

$$[A, B]_L = N_{[\gamma_A, \gamma_B]}.$$

В этих определениях теорема 2.38 примет следующий вид.

Теорема 1.48. *Пусть L – лупа и $\mathcal{W}$ – множество отображений, порождающих группу $TotInn(L)$, тогда*

$$[A, B]_L = Ng(w_{\bar{u}}(a)/w_{\bar{v}}(a) : w \in W, a \in A, u_i/v_i \in B),$$

где $Ng(X)$ – наименьшая нормальная подлупа, содержащая множество X.

Отметим, что данная характеризация сочетается с определением коммутанта для групп. Пусть L – группа и A, B – нормальные подгруппы L, тогда $T_y(x) = y^{-1}xy$. По утверждению 1.47 получим $[A, B]_L =< [a, u]_L/[a, v]_L : a \in A, u/v \in B >$. Далее, пусть $N_1 =< [a, u]_L/[a, v]_L : a \in A, u/v \in B >$ и $N_2 =< [a, b]_L : a \in A, b \in B >$. Выберем $u = b \in B$ и $v = 1$. Тогда получим, что $[a, b]_L = [a, u]_L/[a, v]_L$ и $u/v \in B$, то есть $N_2 \subseteq N_1$. Обратно, в группе L/N_2

имеем $[a,u]_L/[a,v]_L = a^{-1}u^{-1}auv^{-1}a^{-1}va = 1$. Значит, множители $uv^{-1} \in B$ и $a \in A$ коммутитуют и $N_1 \subseteq N_2$.

В [66] приведен пример лупы, показывающий, что,в общем случае, нельзя уменьшить множество порождающих элементов коммутанта.

Следствие 1.49. *Пусть L – лупа, A, B – нормальные подлупы лупы L, тогда*

$$[A,B]_L = Ng([a,b]_L, [b,a,x]_L, w_{u_1,u_2}(a)/w_{v_1,v_2}(a) :$$
$$w \in \{L,R,M\}, a \in A, b \in B, u_i/v_i \in B, x \in L),$$

Причем,

1) если L – IP-лупа, то

$$[A,B]_L = Ng([a,b]_L, L_{u_1,u_2}(a)/L_{v_1,v_2}(a) : a \in A, b \in B, u_i/v_i \in B);$$

2) если L – коммутативная лупа, то

$$[A,B]_L = Ng(w_{u_1,u_2}(a)/w_{v_1,v_2}(a) : w \in \{L,M\}, a \in A, u_i/v_i \in B);$$

3) если L – группа, то

$$[A,B]_L =< [a,b]_L : a \in A, b \in B > .$$

Доказательство. Утверждение следует из леммы 1.47. Пусть N – подлупа лупы L относительно умножения справа.

Проверим, что N удовлетворяет условиям (1) и (2) леммы 1.46. В лупе L/N для всех $a \in A, b \in B, x \in L$ имеем $R_{x,b}(a) = R_{x,1}(a) = a$, поэтому $[a,x,b]_L = 1$, и $R_{b,x}(a) = R_{1,x}(a) = a$. Следовательно, $[a,b,x]_L = 1$ и $L_{x,b}(a) = L_{x,1}(a) = a$. Значит, $[x,b,a]_L = 1$. Теперь по теореме 2.38, с исключением отображений U_x, T_x из порождающих, данный пункт верен.

(1) Достаточно показать, что $[b,a,x]_L \in N$ для всех $a \in A, b \in B, x \in L$. Данное условие эквивалентно тому, что $b \cdot ax = ba \cdot x, ax = b^{-1}(ba \cdot x)$. Далее $a \cdot (ba)^{-1}x = b^{-1}x, (ba)^{-1}x = a^{-1} \cdot b^{-1}x$, и по IP-условию $[a^{-1}, b^{-1}, x]_L = 1$.

(2) Данный пункт следует из предыдущего с условием, что $L_{x,y} = 1$.

(3) Следует из пунта (3) леммы 1.47.

□

Рассмотрим лупу в которой подлупа, порожденная частными, не является нормальной. Пусть L – коммутативная лупа со следующей таблицей умножения:

	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	0	3	2	5	4	7	6
2	2	3	1	0	6	7	4	5
3	3	2	0	1	7	6	5	4
4	4	5	6	7	3	0	1	2
5	5	4	7	6	0	3	2	1
6	6	7	4	5	1	2	3	0
7	7	6	5	4	2	1	0	3

Подлупа $A = \{0, 1, 2, 3\}$ является нормальной в L. Однако, подлупа

$$[A, A]_L =< L_{u_1,u_2}(a)/L_{v_1,v_2}(a), M_{u_1,u_2}(a)/M_{v_1,v_2}(a) : a \in A, u_i/v_i \in A >= \{0, 1\}$$

не является нормальной.

Таким образом, нельзя отказаться от нормального замыкания множества частных. Однако, если группа внутренних отображений является подгруппой группы автоморфизмов $Inn(L) \subseteq Aut(L)$, то подлупа, порожденная частными, будет нормальной.

Так как в гомоморфном образе лупы образ коммутанта подлуп совпадает с коммутантом их образов, то верна следующая лемма.

Лемма 1.50. *Пусть A, U, V – нормальные подлупы лупы $(L, \cdot)$, тогда в факторлупе L/A выполняется неравенство $[\bar{U}, \bar{V}]_{L/A} \neq \bar{E}$ тогда и только тогда, когда $[U, V]_L \not\subseteq A$.*

1.3 Первичный радикал луп

Пусть A, B – нормальные подлупы лупы $(L, \cdot)$, тогда из соотношения $[A, B]_L \subseteq P$, в общем случае, не следует хотя бы одно из включений $A \subseteq P$ или $B \subseteq P$. В связи с этим рассмотрим следующее определение.

Определение 1.51. *Нормальная подлупа P лупы $(L, \cdot)$ называется первичной нормальной подлупой, если из соотношения $[A, B]_L \subseteq P$, следует, что либо $A \subseteq P$, либо $B \subseteq P$.*

Пусть теперь $[Ng(a), Ng(b)]_L \subseteq P$, где P – первичная нормальная подлупа и элементы $a, b \in L$. Если $a \notin P$, то $Ng(a) \not\subseteq P$. Тогда, ввиду первичности нормальной подлупы P, следует, $Ng(b) \subseteq P$, значит, $b \in P$. Аналогично, если $b \notin P$, то $Ng(a) \subseteq P$, значит, $a \in P$.

Обратно, предположим, что нормальной подлупы P лупы L из соотношения $[Ng(a), Ng(b)]_L \subseteq P$ следует, что либо $a \in P$, либо $b \in P$, где $a, b \in L$. Теперь

если для нормальных подлуп A, B лупы L выполняется включение $[A, B]_L \subseteq P$, и, например, $A \nsubseteq P$, то выберем элемент $b \in B$, но $b \notin P$. Для любого $a \in A$ выполняется включение $[Ng(a), Ng(b)]_L \subseteq [A, B] \subseteq P$. Так как $b \notin P$ и $Ng(b) \nsubseteq P$, то ввиду определения первичной подлупы $Ng(a) \subseteq P$ и $a \in P$.

Таким образом, мы получаем следующую лемму.

Лемма 1.52. *Нормальная подлупа P лупы $(L, \cdot)$ является первичной нормальной подлупой, если из соотношения $[Ng(a), Ng(b)]_L \subseteq P$ для $a, b \in L$, следует, что либо $a \in P$, либо $b \in P$.*

Определение 1.53. *Последовательность $a_0, a_1, \ldots$ элементов лупы L называется т-последовательностью, если в L существуют элементы b'_0, b'_1, b''_0, b''_1, такие что $a_{i+1} = [b'_i, b''_i]_L$ и $b'_i, b''_i \in Ng(a_i)$.*

Теперь определим первичную лупу.

Определение 1.54. *Лупа $(L, \cdot)$ называется первичной, если для любых ее двух нормальных подлуп A, B из равенства $[A, B]_L = E$ следует, что либо $A = E$, либо $B = E$, где E – единичная подлупа лупы L.*

Пример 1.55. *Примером первичной лупы является простая некоммутативная и неассоциативная лупа.*

Отметим связь между понятиями первичной лупой и первичной нормальной подлупой.

Лемма 1.56. *Нормальная подлупа $(P, \cdot)$ лупы $(L, \cdot)$ является первичной тогда и только тогда, когда фактор-лупа L/P первична.*

Доказательство.

Пусть L/P – первичная подлупа и A, B – нормальные подлупы лупы L, такие что $[A, B]_L \subseteq P$. Тогда по лемме 1.50 $[\bar{A}, \bar{B}]_{L/P} = \bar{E}$. Значит, либо $\bar{A} = \bar{E}$, либо $\bar{B} = \bar{E}$, откуда следует, что $A \subseteq P$ или $B \subseteq P$, т.е. нормальная подлупа P первична.

Обратно, если P – первичная нормальная подлупа лупы L и нормальные подлупы $\bar{A} = A/P, \bar{B} = B/P$ лупы $\bar{L} = L/P$ удовлетворяют равенству $[\bar{A}, \bar{B}]_{L/P} = \bar{E}$, то $[A, B]_L \subseteq P$, что означает $A \subseteq P$ или $B \subseteq P$. Следовательно, $\bar{A} = \bar{E}$ или $\bar{B} = \bar{E}$, т.е. L – первичная лупа.

□

Теперь введем понятие первичного радикала лупы.

Определение 1.57. *Пересечение всех нормальных первичных подлуп лупы $(L, \cdot)$ называется первичным радикалом $rad(L)$ лупы L.*

Замечание 1.58. *Пусть* $\{P_i\}, i \in I$, *– убывающая цепочка нормальных первичных подлуп лупы* L. *Тогда* $\cap P_i$ *есть нормальная первичная подлупа. Согласно лемме Цорна, каждая первичная подлупа содержит минимальную первичную подлупу. Поэтому первичный радикал – это пересечение всех минимальных первичных подлуп.*

Определение 1.59. *Пусть* $(L, \cdot)$ *– лупа. Элемент* $a \in L$ *называется строго энгелевым, если в любой последовательности* $a_0, a_1, \ldots$ *элементов лупы* L, *удовлетворяющей условию* $a_0 = a, a_{i+1} \in [Ng(a_i), Ng(a_i)]_L$, *начиная с некоторого номера все элементы равны 1.*

Данное определение согласуется с определением строго энгелевых элементов для групп (элемент g группы $(G, \cdot)$ называется *строго энгелевым*, если в любой последовательности $g_0, g_1, \ldots$ элементов группы G, удовлетворяющей условию $g_0 = g, g_{i+1} \in [[l_i, g_i], g_i]$ для всех $l_i \in G$, начиная с некоторого номера все элементы равны 1). В случае, если G является группой, то множества $[[G, g], g]$ и $[Ng(g), Ng(g)]_L$ совпадают [24], поскольку $[[G, g], g] = [Ng(g), g] = [Ng(g), Ng(g)]$.

Замечание 1.60. *Если элемент* a_r *из последовательности для строго энгелевых элементов принадлежит нормальной подлупе* A *лупы* L, *то все элементы этой последовательности* $a_i, i > r$, *содержатся в* A. *Рассмотрим еще одну нормальную подлупу* B, *пересекающуюся с последовательностью* $a_0, a_1, \ldots$, *т.е. содержащую начиная, с некоторого* a_s, *все последующие члены этой последовательности. Тогда все члены последовательности, начиная с* $a_t, t = max(r, s)$, *содержатся в* $A \cap B$.

Теорема 1.61. *Первичный радикал* $rad(L)$ *лупы* $(L, \cdot)$ *совпадает с множеством всех строго энгелевых элементов лупы.*

Доказательство. Покажем сначала, что если элемент a лупы L не принадлежит первичному радикалу, то он не является сторого энгелевым. Пусть $a \notin rad(L)$, т.е. существует нормальная первичная подлупа A такая, что $a \notin A$. Тогда $Ng(a) \not\subseteq A$ Следовательно, образ нормальной подлупы $Ng(a)$ в факторлупе L/A не является единицей: $\overline{Ng(a)} \neq \bar{1}$. Поэтому, согласно определению первичной лупы, $[\overline{Ng(a)}, \overline{Ng(a)}]_{L/A} \neq \bar{1}$. Значит $[Ng(a), Ng(a)]_L \not\subseteq A$. Пусть $a_0 = a$, далее выберем элемент $a_1 \in [Ng(a), Ng(a)]_L \setminus A$. Элемент a_1 не принадлежит первичному радикалу $rad(L)$. Продолжая процесс, построим необрывающаюся последовательность $a_0, a_1, \ldots$, где $a_i \in [Ng(a_{i-1}), Ng(a_{i-1})]_L$. Таким образом, элемент a не является строго энгелевым.

Пусть теперь элемент $a \in L$ не является строго энгелевым, тогда существует последовательность $a_0, a_1, \ldots$, где $a_i \in [Ng(a_{i-1}), Ng(a_{i-1})]_L$, все элементы

которой отличны от единицы. Рассмотрим максимальную нормальную подлупу P, не содержащую ни одного элемента данной последовательности. Пусть U, V – нормальные подлупы лупы L, строго содержащие подлупу P. Ввиду максимальности подлупы P, подлупы U, V пересекаются с данной последовательностью. Значит, начиная с какого-то натурального числа k выполняются условия $a_k \in U \cap V$. Таким образом, $a_k \in [U, V]_L$ и коммутант $[\bar{U}, \bar{V}]_{L/P}$ не равен единичной подлупе $\bar{E}$. Тогда L/P – первичная лупа, и, следовательно, P – первичная нормальная подлупа. Возникает противоречие с определением первичного радикала.

□

Теорема 1.62. *Если $R = rad(L)$ – первичный радикал лупы $(L, \cdot)$, то первичный радикал $rad(L/R)$ факторлупы L/R совпадает с единичной подлупой, т.е.*

$$rad(L/rad(L)) = E.$$

Доказательство. Пусть элемент $\bar{a}$ принадлежит радикалу лупы L/R, тогда этот элемент содержится в каждой первичной подлупе лупы L/R. Если элемент $\bar{a}$ лупы L/R отличен от единичного элемента, то элемент a лупы L не содержится в ее радикале R. Следовательно, в лупе L существует такая первичная нормальная подлупа P, что $a \notin P$. Но факторлупа P/R является первичной нормальной подлупой лупы L/R, причем $\bar{a}$ не содержится в P/R. Это противоречит выбору элемента $\bar{a}$. Таким образом, элемент $\bar{a}$ равен единице.

□

К определению первичного радикала лупы L можно прийти другим путем. Для этого обозначим через $\rho(L)$ подлупу лупы L, порожденную всеми разрешимыми нормальными подлупами этой лупы. Построим теперь возрастающий ряд таких подлуп

$$1 = \rho_0(L) \subset \rho_1(L) \subset \ldots \subset \rho_k(L) \subset \rho_{k+1}(L) \subset \ldots,$$

пользуясь следующим правилом $\rho_{k+1}(L)/\rho_k(L) = \rho(L/\rho_{k+1}(L))$ и для предельного α берем $\rho_\alpha(L) = \cup_{\beta<\alpha}\rho_\beta(L)$. Пусть λ – первое натуральное число, при котором $\rho_\lambda(L) = \rho_{\lambda+1}(L)$. Подлупу $\rho_\lambda(L)$ обозначим через $\overline{rad(L)}$ и назовем *верхним радикалом лупы L.*

Теорема 1.63. *Первичный радикал $rad(L)$ лупы L совпадает с верхним радикалом $\overline{rad(L)}$ этой лупы.*

Доказательство. Лупа $L/rad(L)$ не содержит, согласно теореме 1.62, нетривиальных разрешимых нормальных подлуп. Тогда из построения $\overline{rad(L)}$ следует, что $\overline{rad(L)} \subseteq rad(L)$. Пусть $\overline{rad(L)} \subset rad(L)$, тогда выберем элемент $b \in \overline{rad(L)}$, но $b \notin rad(L)$. Ясно, что $Ng(b) \not\subseteq rad(L)$, тогда $[Ng(b), Ng(b)]_L \not\subseteq rad(L)$. Следовательно, в лупе L существует такой элемент $b_1 \in [Ng(b), Ng(b)]_L$, что $b_1 \notin rad(L)$, причем $b_1 \in \overline{rad(L)}$. Повторяя рассуждения для элемента b_1, построим необрывающуюся последовательность $b = b_0, b_1, \ldots$ элементов лупы L. Вся эта последовательность содержится в $\overline{rad(L)}$ и не пересекается с $rad(L)$. Теперь рассмотрим максимальную нормальную подлупу P, не содержащую ни одного элемента данной последовательности. Пусть U, V – нормальные подлупы лупы L, строго содержащие подлупу P. Ввиду максимальности подлупы P, подлупы U, V пересекаются с данной последовательностью. Значит, начиная с какого-то натурального числа k выполняются условия $b_k \in U \cap V$. Таким образом, $b_k \in [U, V]_L$, и коммутант $[\bar{U}, \bar{V}]_{L/P}$ образов подлуп U, V в факторлупе L/P не равен единичной подлупе $\bar{E}$. Тогда L/P – первичная лупа, и, следовательно, P – первичная нормальная подлупа, причем $rad(L) \not\subseteq P$ и $\overline{rad(L)} \subseteq P$. Возникает противоречие с определением первичного радикала.

□

1.4 Первичный радикал Ω-лупы

Понятия операторных групп и Ω-группы используют аналогию между нормальными подгруппами группы и идеалами колец. В работах П. Хиггинса [38], А.Г. Куроша [16], Б. Брауна и Н. Маккоя [47] были отмечены различные свойства Ω-группы.

Р. Брак [27], Б. Браун и Н. Маккой [47] приводили примеры использования конструкций Ω-луп.

Определение 1.64. *Лупа $(L, +)$ (не обязательно, коммутативная или ассоциативная) называется лупой с операторами или Ω-лупой, если в L задана помимо сложения еще система n-арных алгебраических операций Ω, причем для всех $\omega \in \Omega$ должно выполняться условие* $00\ldots0\omega = 0$.

Для удобства будем использовать для лупы $(L, +)$ аддитивную запись; в частности, нулевой элемент этой лупы будет обозначаться символом 0.

При пустой системе операций Ω мы получаем понятие лупы. С другой стороны, понятие Ω-лупы превращается в понятие кольца, если аддитивная лупа этой Ω-лупы коммутативна и ассоциативна (т.е. абелева группа), а система операций Ω состоит из одного бинарного умножения, связанного со сложением законами дистрибутивности.

Ω-лупу L можно также считать универсальной алгеброй относительно операций аддитивной лупы и операций из Ω. Всякая подалгебра этой алгебры будет подлупой аддитивной лупы и поэтому содержит 0, при этом она сама является Ω-лупой. Поэтому можно говорить не о подалгебрах, а об Ω-подлупах Ω-лупы L.

Определение 1.65. *Непустое подмножество A Ω-лупы L называется идеалом в L, если выполняются следующие два условия:*

1. *A является нормальной подлупой аддитивной лупы;*
2. *для всякой n-арной операции $\omega \in \Omega$, любого элемента $a \in A$ и любых элементов $x_1, x_2, \ldots, x_n \in L$ при $i = 1, 2, \ldots, n$ имеет место включение*

$$-(x_1 x_2 \ldots x_n \omega) + x_1 \ldots x_{i-1}(a + x_i) x_{i+1} \ldots x_n \omega \in A.$$

Для луп понятие идеала совпадает с понятием нормальной подлупы, так как, ввиду пустоты системы операций Ω, условие 2) отпадает.

Заметим, что условие 2) может быть переписано в виде

$$x_1 \ldots x_{i-1}(a + x_i) x_{i+1} \ldots x_n \omega \in (x_1 x_2 \ldots x_n \omega) + A,$$

при $i = 1, 2, \ldots, n$, где справа стоит смежный класс по нормальной подлупе A, порожденный элементом $x_1 x_2 \ldots x_n \omega$. Применяя это включение несколько раз, мы получим следующему утверждению.

Лемма 1.66. *Для любого идеала A Ω-лупы L, любой n-арной операции $\omega \in \Omega$, любых элементов $a_1, a_2, \ldots, a_n \in A$ и любых элементов $x_1, x_2, \ldots, x_n \in L$ имеет место включение*

$$(a_1 + x_1)(a_2 + x_2) \ldots (a_n + x_n)\omega \in x_1 x_2 \ldots x_n \omega + A.$$

Лемма 1.67. *Всякий идеал Ω-лупы L является ее нормальной Ω-подлупой.*

Доказательство. По определению идеал A является нормальной подлупой аддитивной лупы, а из предыдущей леммы для любой n-арной операции $\omega \in \Omega$ и любых $a_1, a_2, \ldots, a_n \in A$ следует при $x_1 = x_2 = \ldots = x_n = 0$ включение $a_1 a_2 \ldots a_n \omega \in A$.

□

Ясно, что идеалами Ω-лупы L будут, в частности, сама лупа L и нулевая подлупа O. Если в L нет других идеалов, то это будет простая Ω-лупа.

Пересечение любой системы идеалов Ω-лупы L само будет идеалом, поэтому можно говорить об идеале, порожденном любой системой элементов $M \subseteq L$.

Заметим, что идеал, порожденный системой идеалов $A_i, i \in I$, Ω-лупы L, совпадает с порожденной этими идеалами нормальной подлупой B аддитивной лупы.

Действительно, подлупа B, порожденная нормальными подлупами, является нормальной подлупой [27]. Теперь пусть даны n-арная операция $\omega \in \Omega$, элемент $b \in B$ и элементы $x_1, x_2, \ldots, x_n \in L$. Так как $A_{i_1}, A_{i_2}, \ldots, A_{i_k}$ являются идеалами, то

$$x_1 \ldots x_{i-1}(a + x_i)x_{i+1} \ldots x_n\omega \in (x_1x_2 \ldots x_n\omega) + A,$$

что и требовалось показать.

Говоря о разложении Ω-лупы L по идеалу A, мы будем понимать под этим разложение аддитивной лупы этой Ω-лупы по A как по нормальной подлупе.

Теорема 1.68. *Все конгруенции произвольной Ω-лупы L исчерпываются ее разложениями по различным идеалам.*

Доказательство. Пусть A – произвольный идеал Ω-лупы L. Для любых $a_1, a_2 \in A$ и $x_1, x_2 \in L$, в силу определения нормальной подлупы, выполняется включение $(x_1 + a_1) + (x_2 + a_2) \in (x_1 + x_2) + A$.

С другой стороны, для любой n-арной операции $\omega \in \Omega$, любых элементов $a_1, a_2, \ldots, a_n \in A$ и $x_1, x_2, \ldots, x_n \in L$ имеет место включение $(a_1 + x_1)(a_2 + x_2) \ldots (a_n + x_n)\omega \in x_1x_2 \ldots x_n\omega + A$. Эти включения показывают, что разложение L в смежные классы по A действительно является конгруенцией в Ω-лупе L.

Пусть теперь в L дана произвольная конгруенция π. Обозначим через A тот класс разбиения π, в котором содержится нуль аддитивной лупы; элементы $a \in A$ характеризуются, следовательно, тем, что имеет место $a\pi 0$. Если $a_1, a_2 \in A$, то $a_1\pi 0, a_2\pi 0$, а поэтому, по определению конгруенции, $(a_1 + a_2)\pi(0 + 0)$, т. е. $(a_1 + a_2)\pi 0$, откуда $a_1 + a_2 \in A$. Далее, если $a \in A$, то

$$[0 + (-a)]\pi[a + (-a)],$$

т. е. $-a\pi 0$, откуда $-a \in A$. Далее, если $a_1, a_2 \in A, x \in L$, то $(x + a_1)\pi(x + 0)$ и $(0 + x)\pi(a_2 + x)$, значит

$$(x + a_1)\pi(a_2 + x),$$

откуда $x + a \in A + x$. Наконец, можно показать, что $(x + y) + a \in x + (y + A)$ и $(x + a) + y \in x + (A + y)$. Этим доказано, что A является нормальной подлупой аддитивной лупы.

Если теперь даны n-арная операция $\omega \in \Omega$, элемент $a \in A$ и элементы $x_1, x_2, \ldots, x_n \in L$, то

$$(a + x_i)\pi(0 + x_i)), \text{ т. е. } (a + x_i \pi x_i),$$

откуда

$$[x_1 \ldots x_{i-1}(a + x_i)x_{i+1} \ldots x_n\omega]\pi(x_1 x_2 \ldots x_n\omega),$$

а поэтому

$$-(x_1 x_2 \ldots x_n\omega) + x_1 \ldots x_{i-1}(a + x_i)x_{i+1} \ldots x_n\omega \in A,$$

$i = 1, 2, \ldots, n$. Следовательно, класс A будет также идеалом Ω-лупы L.

Рассмотрим, наконец, произвольный класс B разбиения π. Если $b \in B, a \in A$, т. е. $a\pi 0$, то

$$(b + a)\pi(b + 0), \text{ т. е. } (b + a)\pi b,$$

откуда для смежного класса $b + A$ следует включение

$$b + a \subseteq B.$$

С другой стороны, если b' – произвольный элемент из класса B, то из $b'\pi b$ следует $(-b + b')\pi 0$ или

$$-b + b' \in A, \text{ т. е. } b' \in b + A.$$

Этим доказано равенство $B = b + A$, т.е. всякий класс разбиения является смежным классом по идеалу A.

□

Далее рассмотрим вопрос об определении первичного радикала Ω-лупы L.

Определение 1.69. *Идеал P в Ω-лупе L называется Ω-первичным, если для любой операции $\omega \in \Omega$ и любых идеалов $I_1, \ldots, I_n \subseteq L$ из включения $(I_1, \ldots, I_n)\omega \subseteq P$ следует, что $I_j \subseteq P$ для некоторого $j = 1, 2, \ldots, n$. Пересечение всех Ω-первичных идеалов Ω-лупы L называется первичным радикалом Ω-$rad(L)$ лупы L.*

Обозначим через $\{a\}^L$ идеал Ω-лупы L, порождённый элементом $a \in L$. Заметим, что этот идеал также является нормальной подлупой $Ng(a)$, порождённой элементом a (наименьшей нормальной подлупой, содержащей a), аддитивной лупы L.

По аналогии с Ω-группами введем определение Ω-m-системы.

Определение 1.70. *Подмножество M Ω-лупы L называется Ω-m- системой, если для любой операции $\omega \in \Omega$ и любых элементов $a_1, \ldots, a_n \in M$ существуют $a'_i \in \{a_i\}^L$, такие что $a'_1 \ldots a'_n \omega \in M$.*

Каждому элементу $a \in L$ поставим в соответствие подмножество $M_a \subseteq L$, которое получается следующим образом: $M_a = \cup_i A_i$, где

$$A_0 = a, A_i = \cup_{\lambda \in \Lambda} A_{i,\lambda}, A_{i,\lambda} = \{a_{i,j_1 \ldots j_n} = a'_{i-1,j_1} \ldots a'_{i-1,j_n} \omega_\lambda\},$$

где ω_λ – n-арная операция, $a'_{i,j_k} \in \{a_{i,j_k}\}^L$, $a_{i,j_1}, \ldots, a_{i,j_n}$ – всевозможные наборы по n элементов из A_i.

Лемма 1.71. *Для любого элемента $a \in L$ множество M_a является Ω-m-системой.*

Доказательство. Пусть $\omega_\lambda \in \Omega$ – это n-арная операция и $a_{i_1}, \ldots, a_{i_n} \in M_a$, где $a_{i_k} \in A_{i_k}$. Покажем, что для каждого a_{i_k} найдется элемент в A_{i_n}, принадлежащий $\{a_{i_k}\}^L$. Действительно, если $a_i \in A_i$, то по построению существует элемент $a_{i+1} \in A_{i_1}$, такой что $a_{i+1} = a'_{i,j_1} \ldots a'_{i,j_n} \omega_\lambda$, где $a'_{i,j_k} \in \{a_i\}^L$ и, следовательно, $a_{i+1} \in \{a_i\}^L, a_{i+1} \in A_{i+1}$.

Рассуждая аналогично, получим, что существуют элементы $b^{(1)}_{i_n}, \ldots b^{(n)}_{i_n}$, где $b^{(k)}_{i_n} \in A_{i_n}$ и $b^{(k)}_{i_n} \in \{a_{i_k}\}^L, k = 1, \ldots, n$. Но тогда надется элемент $c = b'_1 \ldots b'_n \omega_\lambda$, где $b'_k \in \{b^{(k)}_{i_n}\}^L \subseteq \{a_{i_k}\}^L$, такой что $c \in A_{i_n+1}$. Отсюда вытекает, что M_a – Ω-m-система.

□

Теорема 1.72. *Пусть $a \in L$, где L – Ω-лупа, тогда эквивалентны следующие условия:*

1) $a \in \Omega - rad(L)$;

2) любая Ω-m-система, содержащая элемент a, содержит 0;

3) любая Ω-m-система M_a, соответствующая элементу a, содержит 0.

Доказательство.

1) $\Rightarrow$ 2) Пусть элемент $a \in L$ такой,что любая Ω-m-система, содержащая его, не содержит 0. Тогда существует последовательность $M = \{a_0 = a, a_1, \ldots\}$, все элементы которой отличны от 0, такая что $a'_1 \ldots a'_n \omega \in M$ для всех $a'_i \in \{a_i\}^L$. В множестве идеалов Ω-лупы L, которые не содержат ни одного элемента последовательности M, выберем максимальный идеал I. Покажем, что I является Ω-первичным идеалом Ω-лупы L. Если U_1, U_2 – идеалы, строго содержащие идеал I, то ввиду максимальности I, каждый из идеалов пересекается с последовательностью M, т.е. найдутся натуральные числа k и l, такие что $a_k \in U_1$ и $a_l \in U_2$. Пусть $m_1 = max(k, l)$, тогда все элементы последовательности

$a_i, i \geq m_1$, начиная с номера $m_1 + 1$, лежат в пересечении $U_1 \cap U_2$. Таким образом, выберем n идеалов $U_i, i = 1, \ldots, n$, таких, что $U_i \not\subseteq I$ и с некоторого m_n все элементы последовательности M лежат в $\cap_{i=1}^{n} U_i$. Из построения идеала I следует, что $U_1 U_2 \ldots U_n \omega \not\subseteq I$, следовательно, I является Ω-первичным идеалом. В то же время I не содержит ни одного элемента последовательности M. Возникает противоречие с определением Ω-первичного радикала.

2) $\Rightarrow$ 3) следует из предыдущей леммы.

3) $\Rightarrow$ 1) Докажем, что для элемента, который не принадлежит Ω-первичному радикалу, любая Ω-m-система M_a не содержит 0. Пусть $a \notin \Omega\text{-}rad(L)$, тогда существует Ω-первичный идеал $I \subseteq L$, такой что $a \notin I$. В этом случае для любой операции $\omega \in \Omega$ найдутся элементы $a'_1, \ldots, a'_n \in \{a\}^L$, такие что $a'_1 \ldots a'_n \omega \in A_1$ и $a'_1 \ldots a'_n \omega \notin I$. Таким образом, A_1 состоит из элементов, не принадлежащих идеалу I. Продолжая этот процесс, построим подмножество $A_k, k > 1$. Таким образом, $M_a = \cup_i A_i$ не содержит 0, так как имеет пустое пересечение с I.

□

Определение 1.73. *Элемент a Ω-лупы L, удовлетворяющий одному из эквивалентных условий теоремы* 1.72*, называется Ω-строго энгелевым.*

Следствие 1.74. *В Ω-лупе L первичный радикал $\Omega\text{-}rad(L)$ совпадает со множеством Ω-строго энгелевых элементов.*

Случай, когда L является группой, рассмотрен в работах А.Байеса, Г.Гербера [28] и А.В. Михалева, М.А. Шаталовой [17]. Случай градуированной Ω-группы разобран в работе А.В. Михалева, И.Н.Балабы, С.А. Пихтилькова [18].

Теорема 1.75. *Пусть L – Ω-лупа, $\Omega = \{\omega\}$, где ω – операция коммутирования. Тогда $rad(L)$ – первичный радикал лупы L и для $a \in L$ эквивалентны следующие условия:*

1) $a \in rad(L)$;

2) элемент a – строго энгелев (т.е. любая последовательность $a_0, a_1, \ldots$, где $a_0 = a, a_{i+1} \in [Ng(a_i), Ng(a_i)]_L$, содержит нулевой элемент);

3) элемент a – Ω-строго энгелев (т.е. любая последовательность $a_0, a_1, \ldots$, где $a_0 = a, a_{i+1} \in [\{a\}^L, \{a\}^L]_L$, содержит нулевой элемент).

Доказательство. 1) $\Leftrightarrow$ 2) следует из теоремы 1.61.

2) $\Leftrightarrow$ 3) следует из того, что нормальная подлупа Ω-лупы L, порожденная элементом a, совпадает с идеалом Ω-лупы L, порожденным элементом a. Таким образом, совпадают и определения соответствующих строго энгелевых элементов.

□

2 Альтернативные кольца: луповые кольца и лупы обратимых элементов

Хорошо известна характеризация первичного радикала ассоциативного кольца R как множества всех элементов $r \in R$ таких, что любая m - последовательность, начинающаяся с r, содержит нулевой элемент [43]. В работе М.Рича [56] была получена подобная характеризация неассоциативных s-колец (к s-кольцам, в частности, относятся все альтернативные и йордановы кольца).

Определение 2.1. *Кольцо R (необязательно ассоциативное) называется s-кольцом, если для любого идеала A множество A^s сумм различных произведений элементов $a_1, \ldots, a_s \in A$ является идеалом.*

Будем обозначать произведение идеалов со всевозможными способами расстановки скобок через $A_1 A_2 \cdots A_s$.

Определение 2.2. *Идеал P s-кольца R называется первичным идеалом, если из условия $A_1 A_2 \cdots A_s \subseteq P$ следует, что $A_i \subseteq P$ для некоторого i.*

Первичным радикалом s-кольца R называется пересечение всех его первичных идеалов.

Основные свойства первичного радикала $rad(R)$ s-кольца R приведены в работах [55], [63].

Теорема 2.3 (см. [55], [63]). *Пусть $rad(R)$ – первичный радикал s-кольца R, тогда выполнены следующие условия:*

(a) $rad(R) = 0$ тогда и только тогда, когда R не содержит ненулевых нильпотентных идеалов;

(b) $rad(R/rad(R)) = 0$;

(c) $rad(R)$ является пересечением всех идеалов Q в R таких, что R/Q не содержит ненулевых нильпотентных идеалов.

Будем обозначать через $(a)_R$ главный идеал кольца R, порожденный элементом $a \in R$.

Определение 2.4. *Последовательность элементов $\{a_0, a_1, \ldots, a_n, \ldots\}$ из s-кольца R называется P-последовательностью, если $a_n \in (a_{n-1})_R^s$ для всех n.*

Элемент $a \in R$ называется строго нильпотентным, если любая P- последовательность, начинающаяся с a, содержит нулевой элемент.

Теорема 2.5 (см. [56]). *Пусть R – s-кольцо, тогда первичный радикал $P(R)$ состоит из всех строго нильпотентных элементов кольца R.*

2.1 Альтернативные кольца

В неассоциативной теории колец важное место занимают функции коммутатора и ассоциатора.

Определение 2.6. *Коммутатором элементов a, b кольца $(R, \cdot, +)$ называется элемент $[a, b]_R = ab - ba$ кольца R. Ассоциатором элементов a, b, c кольца R называется элемент $[a, b, c]_R = (ab)c - a(bc)$ кольца R.*

Данные функции аддитивны (линейны для алгебр) по каждой переменной. Например, если a_1, a_2, b и c – элементы кольца R, то $[a_1 + a_2, b, c]_R = [a_1, b, c]_R + [a_2, b, c]_R$, а если R – алгебра над полем F и $\alpha \in F$, то $[\alpha a, b, c]_R = \alpha[a, b, c]_R$.

Определение 2.7. *Кольцо R удовлетворяет левому альтернативному тождеству, если $[x, x, y]_R = 0$ (и правому, если $[y, x, x]_R = 0$ для всех $x, y \in R$).*

Кольцо называется альтернативным, если оно удовлетворяет левому и правому альтернативным тождествам.

Полезными являются понятия ядра и центра кольца.

Определение 2.8. *Ядром кольца $(R, \cdot, +)$ называется множество $N(R) = \{z \in R | [z, x, y]_R = [x, z, y]_R = [x, y, z]_R = 0\}$ для всех $z, y \in R$.*

Центром кольца $(R, \cdot, +)$ называется множество $Z(R) = \{z \in R | [z, r]_R = 0, [z, x, y]_R = [x, z, y]_R = [x, y, z]_R = 0\}$ для всех $r, z, y \in R$.

Лемма 2.9 (см. [10]). *Пусть R – кольцо (необязательно ассоциативное), тогда ядро и центр являются подкольцами.*

Приведем используемые свойства коммутатора и ассоциатора.

Лемма 2.10 (см. [34]). *Пусть R – альтернативное кольцо, тогда для всех $x, y, z \in R$ выполнены следующие тождества:*

(1) $[x, y, z]_R = -[x, z, y]_R$;
(2) $[x, y, x]_R = 0$;
(3) $[yx, x, z]_R = x[y, x, z]_R$;
(4) $((xy)x)z = x(y(xz))$;
(5) $((xy)z)y = x(y(zx))$;
(6) $(xy)(zx) = (x(yz))x$;
(7) $[x, n]_R[x, y, z]_R = 0$, *для всех* $n \in N(R)$.
(8) $(xy)[x, y, z]_R = y(x[x, y, z]_R)$;

Лемма 2.11. *Пусть R – альтернативное кольцо, тогда R является 2-кольцом.*

Доказательство. Пусть элементы a, b принадлежат идеалу A кольца R, x – произвольный элемент из кольца R. Тогда $(ab)x = [a, b, x]_R + a(bx)$, где

$[a,b,x]_R = (ab)x - a(bx)$, однако в альтернативных кольцах выполняется тождество $[a,b,x]_R = -[a,x,b]_R$ (равенство (1) леммы 2.10). Значит, $(ab)x = -(ax)b + a(xb) + a(bx)$ и каждое слагаемое принадлежит A^2. Аналогично можно показать, что $x(ab) \in A^2$.

Более того верна следующая теорема.

Теорема 2.12 (критерий Артина, см. [10])**.** *Кольцо R является альтернативным тогда и только тогда, когда подкольцо, порожденное любыми двумя элементами кольца R, является ассоциативным.*

Рассмотрим вопрос об обратимых элементах альтернативного кольца. Элемент $x \in R$ называется обратимым, если существуют элементы y, z, такие что $xy = 1 = zx$. Обозначим множество обратимых элементов кольца R через $U(R)$.

Теорема 2.13. *Пусть R – альтернативное кольцо с единицей, тогда множество обратимых элементов $U(R)$ является лупой Муфанг.*

Доказательство. Сначала покажем, что правый y и левый z обратные элементы совпадают. Действительно, используя равенства (3), (8) из леммы 2.10, получим

$$[x,y,z]_R = (xy)[x,y,z]_R = y(x[x,y,z]_R) = y(x[z,x,y]_R) = y[zx,x,y]_R = 0.$$

Тогда $z = z(xy) = (zx)y = y$. Теперь общий обратный элемент к элементу $x \in R$ будем обозначать через x^{-1}.

Для любого $a \in R$, используя опять равенства (3), (8) из леммы 2.10, имеем $[x^{-1},x,a]_R = (xx^{-1})[x^{-1},x,a]_R = x^{-1}(x[x^{-1},x,a]_R) = x^{-1}[x^{-1}x,x,a]_R = 0$. По теореме 2.12 Артина, элементы x, x^{-1} и a порождают ассоциативную подалгебру алгебры R. В частноти, это показывает, что для обратимых элементов из уравнений $ax = bx, xa = xb$ следует, что $a = b$. А также получаем, что для любых $a, b \in R$ уравнения $ax = b, xa = b$ имеют единственное решение. Таким образом, подмножество $U(R)$ замкнуто относительно умножения, и, значит, является лупой.

Далее, если x – обратимый элемент и $[x,a,b]_R = 0$, то $0 = [x^{-1}x,a,b]_R = x[x^{-1},a,b]_R + [x,a,b]_R x^{-1} = x[x^{-1},a,b]_R = 0$, значит $[x^{-1},a,b]_R = 0$. Теперь пусть x, y – обратимые элементы и$[x,y,xy]_R = 0$, тогда $[x^{-1},y,xy]_R = 0$ и $[x^{-1},y^{-1},xy]_R = 0$. Таким образом, $(xy)(y^{-1}x^{-1}) = 1$. Это показывает, что если $x, y \in U(R)$, то элемент xy обратим и элемент $y^{-1}x^{-1}$ является его обратным. Лупа $U(R)$ является лупой Муфанг, так как в альтернативном кольце R выполняется тождество Муфанг (равенство (6) из леммы 2.10).

□

Рассмотрим некоторые свойства первичных альтернативных колец. Напомним, что альтернативное кольцо (2-кольцо) R называется первичным, если $(0)_R$ является первичным идеалом кольца R. Теперь введем следующее определение.

Определение 2.14. *Альтернативное кольцо R с ненулевым центром $Z(R)$, не содержащим делителей нуля кольца R, называется кольцом Кэли-Диксона.*

В качестве примера кольца Кэли-Диксона можно рассмотреть алгебру октонионов $\mathcal{O}$ над полем F. Каждый элемент алгебры $\mathcal{O}$ является линейной комбинацией базисных элементов $e_0, e_1, ..., e_7 \in \mathcal{O}$ с коэффициентами из поля F. Причем, для базисных элементов имеется следующая таблица умножения:

	e_0	e_1	e_2	e_3	e_4	e_5	e_6	e_7
e_0	e_0	e_1	e_2	e_3	e_4	e_5	e_6	e_7
e_1	e_1	$-e_0$	e_3	$-e_2$	e_5	$-e_4$	$-e_7$	e_6
e_2	e_2	$-e_3$	$-e_0$	e_1	e_6	e_7	$-e_4$	$-e_5$
e_3	e_3	e_2	$-e_1$	$-e_0$	e_7	$-e_6$	e_5	$-e_4$
e_4	e_4	$-e_5$	$-e_6$	$-e_7$	$-e_0$	e_1	e_2	e_3
e_5	e_5	e_4	$-e_7$	e_6	$-e_1$	$-e_0$	$-e_3$	e_2
e_6	e_6	e_7	e_4	$-e_5$	$-e_2$	e_3	$-e_0$	$-e_1$
e_7	e_7	$-e_6$	e_5	e_4	$-e_3$	$-e_2$	e_1	$-e_0$

Отметим, что кроме колец Кэли-Диксона, других первичных альтернативных колец не существует.

Теорема 2.15 (см. [10], Слейтер)**.** *Пусть R – первичная невырожденная неассоциативная альтернативная алгебра. Тогда R является кольцом Кэли-Диксона.*

Много результатов о первичных альтернативных алгебрах и кольцах можно найти в работах [22], [4], [11], citeGolubkov.

Следующая лемма дает описание первичного альтернативного кольца с помощью элементов кольца.

Лемма 2.16 (см. [10])**.** *Пусть R – кольцо Кэли-Диксона. Если элементы $a, b \in R$ и $(aR)b = 0$ (или $a(Rb) = 0$), то либо $a = 0$, либо $b = 0$.*

2.2 Альтернативные луповые кольца

Пусть: K – коммутативное и ассоциативное кольцо с единицей, L – лупа. Рассмотрим множество KL, состоящее из всех формальных сумм вида

$$a = \sum_{l \in L} \alpha_l \cdot l,$$

где $\alpha_l \in K$, в которых лишь конечное число элементов α_l отлично от нуля. Два элемента $a, b \in KL$ считаются равными тогда и только тогда, когда $\alpha_l = \beta_l$ для всех $l \in L$.

На множестве KL определены операции сложения и умножения следующим образом, если $a = \sum_{l \in L} \alpha_l \cdot l$ и $b = \sum_{l \in L} \beta_l \cdot l$, то:

$$a + b = \Big(\sum_{l \in L} \alpha_l \cdot l\Big) + \Big(\sum_{l \in L} \beta_l \cdot l\Big) = \sum_{l \in L} (\alpha_l + \beta_l) \cdot l;$$

$$a \cdot b = \Big(\sum_{l \in L} \alpha_l \cdot l\Big)\Big(\sum_{k \in L} \beta_k \cdot k\Big) = \sum_{l,k \in L} \alpha_l \beta_k \cdot (lk) = \sum_{l \in L} \Big(\sum_{m,n \in L : mn = l} \alpha_m \beta_n\Big) \cdot l = \sum_{l \in L} c_l \cdot l,$$

где $c_l = \sum_{mn=l} \alpha_m \beta_n$

Таким образом, относительно этих операций множество KL является неассоциативным кольцом с единицей (неассоциативной K-алгеброй с элементами лупы в качестве базиса). Удобно отождествить $l \in L$ с элементом $1 \cdot l \in KL$, а $\alpha \in K$ с элементом $\alpha \cdot e$, где e – единица лупы (тогда K и L будут являться подмножествами в KL).

Рассмотрим некоторые утверждения для луповых колец, когда в качестве лупы будет выступать лупа Муфанг. Пусть отображение $* : KL \to KL$ задается как

$$\Big(\sum \alpha_l l\Big)^* = \sum \alpha_l l^{-1}$$

Легко проверить, что

$$(a + b)^* = a^* + b^*$$

и

$$(ab)^* = b^* a^*.$$

Зная, что $(l^{-1})^{-1} = l$ для всех $l \in L$, получаем, что

$$(a^*)^* = a.$$

Таким образом, отображение * – это инволюция.

Пусть теперь $a = \sum_{x \in L} \alpha_x x \in KL$. Определим носитель элемента лупового кольца a:

$$\text{Supp } a = \{x \in L | \alpha_x \neq 0\}.$$

Другими словами, Supp a – это множество всех элементов лупы, которые реально участвуют в представлении элемента a. Поэтому Supp a – конечное подмножество L, такое, что Supp $a = \varnothing$ тогда и только тогда, когда $a = 0$.

Отметим некоторые свойства носителя Supp a. Если $a \in KL, a \neq 0$ и $l \in L$, то Supp $la = l(\text{Supp } a)$ и Supp $al = (\text{Supp } a)l$. В частности, если $x \in \text{Supp } a$, то $1 \in \text{Supp } x^{-1}a$ и $1 \in \text{Supp } ax^{-1}$.

Пусть снова H – подлупа L. Определим проекцию $\pi_H : KL \to KH$, следующим образом

$$\pi_H(\sum_{x \in L} \alpha_x x) = \sum_{x \in H} \alpha_x x,$$

другими словами, если $a \in KL$, то $a = \pi_H(a) + a'$, где Supp a' не пересекается с H и Supp $(a - a') \subseteq H$. Отметим, некоторые основные свойства отображения π_H:

Лемма 2.17. *Пусть H - подлупа лупы МуфангL, $a, b \in KL, c \in KH$. Тогда*

1) $\pi_H(a\alpha + b\beta) = \alpha\pi_H(a) + \beta\pi_H(b)$ для любых $\alpha, \beta \in K$.

2)$\pi_H(ca) = c\pi_H(a), \pi_H(ac) = \pi_H(a)c$;

3) Если H – нормальная подлупа лупы L и $x \in L$, то $\pi_H(x^{-1}ax) = x^{-1}\pi_H(a)x$.

Доказательство:

1) Так как

$$a = a_0 + a_1, b = b_0 + b_1,$$

где $a_0 = \pi_H(a), b_0 = \pi_H(b)$ и $(Supp\ a_1) \cap H = 0, (Supp\ b_1) \cap H = 0$,

Тогда

$$\alpha a + \beta b = (\alpha a_0 + \beta b_0) + (\alpha a_1 + \beta b_1).$$

Так как $(Supp\ \alpha a_1 + \beta b_1) \cap H = 0$, следовательно,

$$\pi_H(\alpha a + \beta b) = \alpha a_0 + \beta b_0.$$

2) Заметим, что $ca = ca_0 + ca_1$ и $ca_0 \in KH$. С другой стороны, если $x \in$ Supp ca_1, то x является произведением элемента из Supp c и элемента из Supp a_1. Так как $(Supp\ a_1) \cap H = 0$, то $(Supp\ a_1 c) \cap H = 0$.

3) Напомним, что в лупе Муфанг $(x^{-1}a)x = x^{-1}(ax)$. Тогда $x^{-1}ax = x^{-1}(a_0 + a_1)x = x^{-1}a_0x + x^{-1}a_1x$, а так как H – нормальная подлупа, то $Supp\ x^{-1}a_0x \subseteq x^{-1}Hx = H$ и $Supp\ x^{-1}a_1x \cap H = 0$. Значит, $\pi_H(x^{-1}ax) = x^{-1}a_0x$.

□

Пусть H – подлупа лупы L. Так как KH является подкольцом кольца KL, то KL – правый или левый неассоциативный KH-модуль, в зависимости от порядка умножения. Из теории групповых колец известно, что этот модуль будет свободным. В случае же квазигрупповых колец это не всегда будет верным.

Лемма 2.18. *Пусть Y – множество представителей левых смежных классов по H в лупе Муфанг L. Тогда любой элемент $a \in KL$ может быть записан единственным образом как*

$$a = \sum_{y \in Y} y \cdot a_y,$$

где $a_y \in KH$ и $a_y = \pi_H(y^{-1}a)$.

Аналогично, если X – множество представителей правых смежных классов по H, то $a = \sum_{x \in X} a_x x$, где $a_x = \pi_H(ax^{-1})$

Доказательство: Пусть $a \in KL$, тогда мы можем записать $a = a_1 + a_2 + \cdots + a_n$, где a_i - частичная сумма тех $a_x \cdot x$, что $x \in y_i H$. Но так как из того, что $x \in y_i H$ следует, что $y_i^{-1}x \in H$, то

$$a = \sum_{i=1}^{n} y_i(y_i^{-1}a_i),$$

где $y_i^{-1}a_i \in KH$.

Таким образом, a может быть записана как сумма $\sum ya_y$, где $a_y \in KH$. Для доказательства единственности разложения, положим $a = \sum ya_y$ и $y_0 \in Y$. Тогда $y_0^{-1}a = \sum y_0^{-1}(ya_y)$, напомним, что $a_y \in KH$, таким образом $a_y = \sum_{h \in H} \alpha_h h$, значит $y_0^{-1}a = y_0^{-1}(\sum \alpha_h(yh)) = \sum \alpha_h(y_0^{-1}(yh))$. Заметим, что $y_0^{-1}(yh) \in H$ тогда и только тогда, когда $yh \in y_0 H \Leftrightarrow y_0 = y$. Значит, $\pi_h(y_0^{-1}a) = y_0^{-1}(y_0 a_{y_0}) = a_{y_0}$.

□

Пусть $L = \{1, 2, 3, 4, 5\}$, умножение $(\cdot)$ задается таблицей:

1	2	3	4	5
2	1	4	5	3
3	5	1	2	4
4	3	5	1	2
5	4	3	2	1

Положим $H = \{1, 2\}$, тогда H – подлупа лупы L и левыми смежными классами по H являются следующие подмножества: $1H = \{1, 2\}, 2H = \{1, 2\}, 3H = \{3, 5\}, 4H = \{3, 4\}, 5H = \{4, 5\}$. Заметим, что $3H \cap 4H \neq 0$. Таким образом, $(L, \cdot)$ не имеет разложения на левые смежные классы.

Пусть $(L, \cdot)$ - лупа Муфанг, H подлупа лупы L. Тогда KL является левым (правым) KH-модулем. Причем, KL – свободный левый (правый) модуль, если L имеет разложение на левые (правые) смежные классы по H.

Лемма 2.19. *Пусть H – подлупа лупы Муфанг L и $a \in KH$. Тогда элемент a обратим в KH тогда и только тогда, когда он обратим в KL. Более того, элемент a – правый (или левый) делитель нуля в KH тогда и только тогда, когда он правый (или левый) делитель нуля в KL.*

Доказательство:

$\Rightarrow$. Очевидно.

$\Leftarrow$. Пусть a - обратим в KL, значит существует $b \in KL$, такое что $ab = 1 = ba$. Тогда по лемме 2.17 $a\pi_H(b) = \pi_H(ab) = \pi_H(1) = 1$ и $\pi_H(b)a = \pi_H(ba) = \pi_H(1) = 1$. Значит $a^{-1} = \pi_H(b) \in KH$.

Теперь рассмотрим делители нуля: пусть $ab = 0$ для некоторого $b \in KL, b \neq 0$, тогда мы можем выбрать $x \in L$, такой что $1 \in \text{Supp } bx$, но так как $a(bx) = 0$(, если $ab = 0 \Rightarrow [(ab)x]b = 0 = b[a(bx)] = 0$, но $b \neq 0$) имеем $a\pi_H(bx) = \pi_H(a(bx)) = \pi_H(0) = 0$, но $\pi_H(bx) \neq 0$, так как $1 \in$ Supp(bx) .

□

Определение 2.20. *Лупа L, для которой луповое кольцо KL, где K – коммутативное и ассоциативное кольцо с единицей и $charK \neq 2$, является альтернативным неассоциативным кольцом называется RA-лупой.*

Будем называть упорядоченную тройку элементов лупы (a, b, c) неассоциативной, если равенство ассоциативности не выполняется для этих элементов (т.е. $a(bc) \neq (ab)c$). Соответственно, упорядоченная тройка (a, b, c) ассоциативна, если $a(bc) = (ab)c$.

Теорема 2.21. *Лупа L является RA-лупой тогда и только тогда, когда выполняются следующие условия:*

a) Если какие-либо элементы лупы ассоциативны в некотором порядке, то они ассоциативны в любом другом порядке.

b) Если $a, b, c \in L$ неассоциативны ни в каком порядке, то $a \cdot bc = ac \cdot b = c \cdot ab$.

Доказательство. Пусть L является RA-лупой и KL является альтернативным кольцом. Пусть $a, b, c \in L$ неассоциативны ни в каком порядке, положим $x = b + c, y = a$. Рассмотрим правое альтернативное тождество $yx \cdot x = yx^2$. Получим

$$ab \cdot b + ab \cdot c + ac \cdot b + ac \cdot c = ab^2 + a \cdot bc + a \cdot cb + ac^2.$$

Так как, $ab \cdot b = ab^2$ и $ac \cdot c = ac^2$, то

$$ab \cdot c + ac \cdot b = a \cdot bc + a \cdot cb.$$

Так как $charK \neq 2$, то элемент лупы $ab \cdot c$ принадлежит носителю как правому, так и левому элементу лупового кольца. Но $ab \cdot c \neq a \cdot bc$. Значит, $ab \cdot c = a \cdot cb$.

Аналогичным образом можно получить равенство $ab \cdot c = b \cdot ac$, если рассмотреть левое альтернативное тождество.

Обратно, предположим, что лупа L удовлетворяет условиям a),b). Для элементов лупового кольца KL $x = \sum \alpha_g g$ и $y = \sum \beta_g g$ элемент $yx \cdot x = yx^2$ является комбинацией элементов вида $ab \cdot c - a \cdot bc$. Отметим, что если $b = c$, то $ab \cdot b = ab^2$ (по свойству b)) и, таким образом, не принадлежит носителю рассматриваемого элемента. Следовательно, $yx \cdot x = yx^2$ является суммой элементов вида

$$(ab \cdot c - a \cdot bc) + (ac \cdot b - a \cdot cb)$$

при $b \neq c$. По свойствам a),b) данный элемент равен 0. Таким образом, выполняется правое альтернативное тождество для лупового кольца KL. Левое альтернативное тождество проверяется аналогичным образом.

□

Замечание 2.22. *В общем случае утверждение a) теоремы 2.21 не верно. Например, для целых чисел с операцией вычитания $(Z, -)$ упорядоченная тройка $(2, 1, 0)$ ассоциативна, а $(2, 0, 1)$ – нет. Действительно, $(2 - 1) - 0 = 1 = 2 - (1 - 0)$ и $(2 - 0) - 1 = 1 \neq 3 = 2 - (0 - 1)$.*

Рассмотрим некоторые свойства RA-луп.

Следствие 2.23. *Если L – RA-лупа, элементы $a, b \in L$ коммутируют, то $ga \cdot b = g \cdot ab$ для всех $g \in L$.*

Доказательство. По теореме 2.21 либо элементы $g, a, b \in L$ ассоциативны $ga \cdot b = g \cdot ab$, либо $ga \cdot b = g \cdot ba = g \cdot ab$. Таким образом, в обоих случаях $ga \cdot b = g \cdot ab$.

□

Следствие 2.24. *Коммутативная RA-лупа является группой.*

Следствие 2.25. *Пусть L – RA-лупа, тогда выполняется тождество $(xy \cdot z)x = x(y \cdot zx)$.*

Доказательство. Если элементы $a, b, c \in L$ ассоциативны, то по теореме Муфанг 1.38 эти элементы порождают подгруппу. Следовательно, $(ab \cdot c)a = a(b \cdot ca)$. Если элементы a, b, c неассоциативны, то по теореме Муфанг 1.38 элементы ab, c, a также неассоциативны. Тогда по теореме 2.21 для элементов ab, c, a выполняется тождество $(ab \cdot c)a = (ab)(ac)$. Элементы a, b, ac неассоциативны. Следовательно, $(ab)(ac) = a(ac \cdot b)$. По теореме 2.21, $ac \cdot b = c \cdot ab = cb \cdot a = b \cdot ca$. Таким образом, $(ab \cdot c)a = a(b \cdot ca)$.

□

Приведем с доказательством теорему, описывающую используемые свойства RA-луп.

Теорема 2.26 (см. также [34]). *Пусть L является RA - лупой, тогда:*

1. $a^2 \in N(L)$ *для всех* $a \in L$;
2. $N(L) = Z(L) = \{a \in L | ax = xa, \forall x \in L\}$;
3. $[a,b]_L = 1$ *для всех* $a, b \in L$ *тогда и только тогда, когда* $[a,b,c]_L = 1$ *для всех* $c \in L$;
4. *если* $a, b, c \in L$ *и* $[a,b,c]_L \neq 1$, *то* $[a,b,c]_L = [a,b]_L = [a,c]_L = [b,c]_L$ *являются центральными элементами порядка 2.*

Доказательство.

1. Альтернативное кольцо FL удовлетворяет следующему тождеству

$$xy \cdot zw + wy \cdot zx = (x \cdot yz)w + (w \cdot yz)x.$$

Рассмотрим элементы лупы $a, b, c \in L \subseteq FL$, такие что $a = x = y, b = z, c = w$. Получим

$$a^2 \cdot bc + ca \cdot cb = (a \cdot ab)c + (c \cdot ab)a.$$

Используя левое альтернативное тождество $a \cdot ab = a^2 b$, преобразуем выражение $(a \cdot ab)c + (c \cdot ab)a = a^2 b \cdot c + (c \cdot ab)a$. Предположим, что a^2, b, c неассоциативны, т.е. $a^2 b \cdot c \neq a^2 \cdot bc$, тогда $a^2 b \cdot c = ca \cdot ba$. По теореме Муфанг 1.38 элементы a, b, c и a, b, ca также неассоциативны. Таким образом, получим

$$cb \cdot a^2 = (cb \cdot a)a = (c \cdot ba)a = ca \cdot ba = a^2 b \cdot c = a^2 \cdot cb = ca^2 \cdot b = c \cdot ba^2.$$

Таким образом, c, b, a^2 ассоциативны и a^2 лежит в ядре FL для всех $a \in L$.

2. Пусть $\mathcal{C}(L)$ – $\{a \in L | ax = xa, \forall x \in L\}$, тогда $Z(L) = \mathcal{C}(L) \cap N(L)$. Если $a \in \mathcal{C}(L)$, то $[a, x, y]_L = 1$ для всех $x, y \in L$, тогда $a \in N(L)$. Таким образом, $\mathcal{C}(L) \subseteq N(L)$ и, следовательно, $Z(L) = \mathcal{C}(L)$. Так как ядро лупы Муфанг является нормальной подлупой, то можно рассмотреть фактор-лупу $L/N(L)$, которая является абелевой группой. Заметим, что $N(L)$ содержится в ядре лупового кольца FL.

Пусть $n \in N(L)$ и $a, b, c \in L$ – неассоциативные элементы. Тогда $ab \cdot c = n_1(a \cdot bc)$ для некоторого $n_1 \in N(L)$, так как $L/N(L)$ является группой. Также $an = (na)n_2$ для некоторого $n_2 \in N(L)$, так как $L/N(L)$ – коммутативная группа. Таким образом, ассоциатор кольца FL $[a,b,c]_L = (n_1 - 1)(a \cdot bc)$ и коммутатор кольца $[a,n]_L = (na)(n_2 - 1)$. Но $[a,n]_L[a,b,c]_L = 0$, тогда

$$((na)(n_2 - 1))((n_1 - 1)(a \cdot bc)) = 0.$$

Так как элемент $n_2 - 1$ принадлежит ядру FL, то

$$(na)(n_2 - 1)(n_1 - 1)(a \cdot bc) = 0.$$

Заметим, что na – обратимый элемент. Значит,

$$(n_2 - 1)(n_1 - 1)(a \cdot bc) = 0.$$

Далее, так как $n_1 - 1$ принадлежит ядру FL, то

$$(n_2 - 1)(n_1 - 1)(a \cdot bc) = (n_2 - 1)(n_1 - 1)(a \cdot bc),$$

а так как $a \cdot bc$ обратимый элемент, то $(n_2 - 1)(n_1 - 1) = 0$. Таким образом, $n_1 + n_2 = 1 + n_2 n_1$, но так как $n_1 \neq 1$, тогда $n_2 = 1$, значит, $an = na$. Следовательно, элемент n коммутирует со всеми элементами не из ядра. Так как L – неассоциативная лупа, то $N(L)$ – простая подлупа и ее замыкание порождает L. Значит, n коммутирует с любым элементом из L.

3. Пусть $a, b \in L$. Предположим, что $[a, b, c]_L = 1$ для всех $c \in L$. Необходимо доказать, что $ab = bc$. По пункту 2, $b \notin N(L)$. Так как $[a, b, x]_L = 0$ для всех $x \in FL$, то $[a, ab]_L \in N(FL)$. Так же $ab \cdot a = n(a \cdot ab)$ для некоторого $n \in N(L)$, так как $L/N(L)$ – коммутативная подлупа. Значит, $ab \cdot a = na^2 b$, откуда $[a, ab]_L = (1 - n)(a^2 b) \in N(FL)$. Следовательно, для всех $g, h \in L$

$$(1 - n)(a^2 b)g \cdot h = (1 - n)(a^n b)(gh).$$

Теперь, $a^2 \in N(L) = Z(L)$ и элемент g^2 обратим. Тогда $(1 - n)ag \cdot h = (1 - n)a(gh)$ для всех $g, h \in L$. Так как $a \notin N(L)$ и лупа $L/N(L)$ ассоциативна, то существуют g, h такие, что $bg \cdot h = n_1(a \cdot gh)$ для некоторого $n_1 \in N(L), n_1 \neq 1$. Таким образом, $(1-n)n_1(a \cdot gh) = (1-n)(a \cdot gh)$. Тогда из равенства $(1-n)n_1 = 1 - n$ получаем, что $n_1 + n = 1 + nn_1$. Так как $n_1 \neq 1$, то $n = 1$. Следовательно, $ab \cdot a = a^2 b$ и значит $hg = gh$.

4. Обозначим $n = [a, b, c]_L$. Заметим, что $n \in N(L) = Z(L)$ (так как $L/N(L)$ является группой). Пусть $n \neq 1$. Тогда

$$ca \cdot b = a \cdot cb = ab \cdot c = n(ab \cdot c) = n(ac \cdot b) = (n \cdot ac)b.$$

Таким образом, $ca = nac$. Следовательно, $n = (c, a) = (a, c)^{-1}$. Но так как $a^2 \in N(L) = Z(L)$ и n – центральный элемент, то

$$a^2 c = ca^2 = xa \cdot a = nac \cdot a = na \cdot ca = na \cdot nac = (na)^2 c = n^2 a^2 c.$$

Таким образом, $n^2 = 1$. Следовательно, $[a, c]_L^{-1} = [a, c]_L$ и $[a, c, b]_L = n = [a, c]_L$. Поменяв местами элементы b и c получим $[a, c, b]_L = [a, b]_L$.

Так как a, b, c не ассоциативны, то по теореме 2.21 $ac \cdot b = a \cdot bc$ и $a \cdot cb = ab \cdot c$. Используя определение ассоциатора $ab \cdot c = (a \cdot bc)[a, b, c]_L$ получаем $a \cdot ca = (ac \cdot b)[a, b, c]_L$. Далее $ac \cdot b = (a \cdot cb)[a, b, c]_L^{-1} = (a \cdot cb)[a, b, c]_L$. Так как $n = [a, b, c]_L$ имеет порядок 2. Таким образом, $[a, c, b]_L = [a, b, c]_L = [a, b]_L = [a, c]_L$.

Аналогичным путем можно показать, что из условий $ba \cdot c = a \cdot bc$ и $b \cdot ac = ab \cdot c$ следует, что $[a, b, c]_L = [b, a, c]_L = [b, c]_L$.

□

Следствие 2.27. *Элементы RA-лупы L удовлетворяет тождеству:*

$$(xy)(zx^3) = (x \cdot yz)x^3.$$

Доказательство. Пусть $x, y, z \in L$, тогда $(x \cdot yz)x^3 = ((x \cdot yz)x)x^2$. Используя тождество Муфанг, получим $((x \cdot yz)x)x^2 = (xy \cdot zx)x^2$. Так как x^2 принадлежит ядру лупы L, то $(xy \cdot zx)x^2 = (xy)(zx \cdot x^2) = (xy)(zx^3)$.

□

Следствие 2.28. *Пусть L является RA-лупой, тогда подлупа H лупы L нормальна тогда и только тогда, когда $xH = Hx$ для всех $x \in L$.*

Доказательство. Покажем, что соотношение $(Hx)y = H(xy)$ следует из соотношения $Hx = xH$ для всех $x, y \in L$. Соотношение $x(yH) = (xy)H$ доказывается аналогично. Пусть $Hx = xH$ для всех $x \in L$ и пусть заданы элементы $y \in L, h \in H$. По теореме 2.21 выполняется или тождество $(hx)y = h(xy)$, или $(hx)y = x(hy) = (xy)h = h'(xy)$ для некоторого $h' \in H$, в обоих случаях $(Hx)y \subseteq H(xy)$. Также, если $h(xy) \neq (hx)y$, то $(xy) = (xh)y = (h'x)y$ для некоторого $h' \in H$, т.е. $H(xy) \subseteq (Hx)y$.

□

Следствие 2.29. *Если L является RA-лупой, то подмножества*

$$Z(L) = \{x \in L | [x, z]_L = 1, z \in L\}$$

и

$$N(L) = \{x \in L | [x, z, w]_L = 1, z, w \in L\}$$

являются подлупами в L.

Доказательство. Если элемент x коммутирует с элементом z, то и x^{-1} также коммутирует с z. Если элементы x и y коммутируют с элементом z, то

$[x,y,z]_L = 1$ по пункту (3) теоремы 2.26. Значит, xy коммутирует с z. Тогда Z(L) – подлупа.

Если $x, y \in N(L)$, то $[x,z,w]_L = [y,z,w]_L = 1$ и $[xy,z,w]_L = [x,z,w]_L \cdot [y,z,w]_L = 1$. Заметим, что элементы x, z, w ассоциативны если и только если x^{-1}, z, w ассоциативны(согласно тождеству Муфанг). Следовательно, $x \in N(L)$ и $x^{-1} \in N(L)$. Таким образом, ядро $N(L)$ замкнуто относительно умножения, т.е. является подлупой.

□

Пусть G – неабелева группа, элемент $g_0 \in Z(G)$ и задана инволюция $g \to g^*$, такая что $g_0^* = g_0$ и $gg^* \in Z(G)$ для всех $g \in G$. Пусть $L = G \cup Gu$ с бинарной операцией, заданной правилами:

$$g(hu) = (hg)u,$$

$$(gu)h = (gh^*)u,$$

$$(gu)(hu) = g_0 h^* g.$$

Ясно, что L является лупой Муфанг. Если L – группа, то для всех $g, h \in G$ выполняется $(gh)u = g(hu) = (hg)u$, т.е. $gh = hg$, но группа G неабелева. Такой класс луп будем обозначать $M(G, *, g_0)$.

Теорема 2.30 (см. [34]). *Если L является RA-лупой Муфанг с коммутатором - ассоциатором $L' =< [L,L,L]_R, [L,L]_R >= \{1, s\}$, то $L = M(G, *, g_0)$, где G – любая группа, содержащая $Z(L)$ и два некоммутирующих элемента лупы L, g_0 – центральный элемент G и инволюция $g \to g_0$ определена следующим образом:*

$$g^* = \begin{cases} g, & \text{если } g \in Z(L) \\ sg, & \text{если } g \notin Z(L) \end{cases}$$

Обратно, для любой неабелевой группы G, единственного неединичного коммутатора s и инволюции $*$ лупа $M(G, *, g_0)$ является RA-лупой для любого $g_0 \in Z(L)$.

Пример 2.31. *Наименьшей RA-лупой является лупа порядка 16. В этом случае, порядок группы G равен 8. Значит, $G = D_4$ или $G = Q_8$. Центр $Z(G)$ является циклической группой порядка 2 с порождающим элементом t_1. Тогда RA-лупами являются следующие лупы $M(D_4, *, 1)$ и $M(Q_8, *, t_1)$.*

2.3 Первичный радикал луповых колец

Выясним связи между первичным радикалом альтернативного лупового кольца RL и первичного радикала подлупы его лупы обратимых элементов $U(RL)$. Согласно теореме 2.13, лупа $U(RL)$ является лупой Муфанг.

Альтернативное кольцо является 2-кольцом (см. теорему 2.12 Артина), поэтому можно воспользоваться теорией для s-колец. А именно: первичным радикалом альтернативного лупового кольца RL называется пересечение всех первичных идеалов этого кольца.

Напомним, что последовательность элементов $\{a_0, a_1, \ldots, a_n, \ldots\}$ из RL называется P - последовательностью, если $a_n \in (a_{n-1})^s$ для всех n. Элемент $a \in RL$ называется строго нильпотентным, если любая P-последовательность, начинающаяся с a, содержит нулевой элемент. По теореме 2.5 первичный радикал $rad\ RL$ состоит из всех строго нильпотентных элементов.

Описание первичного радикала для лупового кольца лупы Муфанг было дано Е.Гудэйром в работе [34]. Пусть R – коммутативное и ассоциативное кольцо и пусть L – лупа Муфанг. Рассмотрим для нормальной подлупы N лупы L каноническое отображение $L \to L/N$ и поднимем его до кольцевого гомоморфизма $\epsilon_N : RL \to R[L/N]$. Обозначим ядро этого отображения через $\Delta_R(L, N), Ker\epsilon(\alpha) = \Delta_R(L, N)$.

В случае, если $N = L$, гомоморфизм

$$\epsilon_L : RL \to R$$

называется фундаментальным отображением и определяется следующим образом: для любого $\alpha = \sum_{l \in L} \alpha_l l$

$$\epsilon(\alpha) = \sum_{l \in L} \alpha_l.$$

Ядро фундаментального отображения называется фундаментальным идеалом и обозначается через $\Delta(L)$.

Лемма 2.32 (см. также [34]). *Пусть L являеся лупой Муфанг, R – коммутативное и ассоциативное кольцо с единицей, RL – альтернативное кольцо и пусть N – нормальная подлупа. Тогда*

$$\Delta_R(L, N) = \sum_{n \in N} RL(1 - n) = \sum_{n \in N} (1 - n)RL.$$

Если $L = M(G, *, g_0)$ является RA-лупой и N – нормальная подлупа, содержащая G, то

$$\Delta(L, N) = \Delta(G, N) + \Delta(G, N)u.$$

Доказательство. Пусть $\alpha = \sum_{l\in L} \alpha_l l \in \Delta_R(L,N)$, где $\alpha_l \in R$. Обозначим через $\bar{\alpha}$ и $\bar{l}$ образы элементов α, l в луповом кольце $R[L/N]$. Пусть $L = \bigcup_{x\in\mathcal{T}} Nx$ для некоторого трансверсаля лупы N в L, тогда

$$\bar{\alpha} = \sum_{x\in\mathcal{T}} (\sum_{l\in L,\bar{l}=\bar{x}} \alpha_l)\bar{x}.$$

Таким образом, для каждого $x \in \mathcal{T}$

$$\sum_{l\in L,\bar{l}=\bar{x}} \alpha_l = 0.$$

Из условия $(lx^{-}1)x = l$ для всех $x, l \in L$ следует, что

$$\sum_{l\in L,\bar{l}=\bar{x}} \alpha_l l = \sum_{l\in L,\bar{l}=\bar{x}} (\alpha_l l x^{-1})x - \sum_{l\in L,\bar{l}=\bar{x}} \alpha_l x = \sum_{l\in L,\bar{l}=\bar{x}} \alpha_l (lx^{-1} - 1)x.$$

Подобным образом устанавливается, что

$$\sum_{l\in L,\bar{l}=\bar{x}} \alpha_l l = \sum_{l\in L,\bar{l}=\bar{x}} \alpha_l x(x^{-1}l) - \sum_{l\in L,\bar{l}=\bar{x}} \alpha_l x = \sum_{l\in L,\bar{l}=\bar{x}} \alpha_l x(x^{-1}l - 1).$$

Далее

$$\alpha = \sum_{x\in\mathcal{T}} (\sum_{l\in L,\bar{l}=\bar{x}} \alpha_l (lx^{-1} - 1))x = \sum_{x\in\mathcal{T}} x(\sum_{l\in L,\bar{l}=\bar{x}} \alpha_l (x^{-}1l - 1)).$$

Так как N нормальная подлупа, то $lx^{-1}, x^{-1}l \in N$ для $\bar{l} = \bar{x}$. Таким образом,

$$\alpha \in \sum_{n\in N} (1-n)RL$$

и

$$\alpha \in \sum_{n\in N} RL(1-n).$$

Следовательно, $\Delta(L,N) \subseteq \sum_{n\in N} RL(1-n)$ и $\Delta(L,N) \subseteq \sum_{n\in N}(1-n)RL$. Обратное включение очевидно.

Теперь докажем второе утверждение. Пусть $L = M(G, *, g_0)$ является RA-лупой и N – нормальная подлупа. Так как $L = G \cup Gu$ для некоторого $u \in L$, то $RL = RG + RGu$ и, значит,

$$\Delta(L,N) = \sum_{n\in N}(1-n)RL = \sum_{n\in N}(1-n)RG + \sum_{n\in N}(1-n)RGu = \Delta(G,N) + \Delta(G,N)u.$$

□

Обозначим через L_p множество всех элементов лупы L порядка p^l для некоторого натурального l.

Теорема 2.33 (см. [34]). *Пусть $L = M(G, *, g_0)$ является RA-лупой и R – коммутативное и ассоциативное кольцо. Для первичного радикала $rad\ RL$ верно равенство:*

$$rad\ RL = (radR)L + \sum_{p \in P}(radR)_p \Delta(L, L_p),$$

где P – множество простых чисел.

Далее изучим связь первичного радикала альтернативного кольца и первичного радикала лупы Муфанг его обратимых элементов. Будем обозначать через $(a)_R$ главный двусторонний идеал кольца R, порожденный элементом $a \in R$, $Ng_L(M)$ – нормальное замыкание множества M в лупе L, $[x, y]_R$ – коммутатор элементов $x, y \in R$, $[A, B]_L$ – взаимный коммутант нормальных подлуп A, B лупы L.

Нам понадобится следующее определение.

Определение 2.34. *Центром кольца R по идеалу I называется множество $Z(R, I) = \{z \in R | [z, r]_R \in I; [z, n, m]_R, [n, z, m]_R, [n, m, z]_R \in I\}$ для всех $r, n, m \in R$.*

Лемма 2.35. *Пусть R является альтернативным кольцом с единицей, I – идеал кольца R, L – некоторая подлупа лупы $U(R)$, $a \in L \cap Z(R, I)$, тогда $Ng_L(a) \subseteq L \cap Z(R, I)$.*

Доказательство. Согласно лемме 1.11, достаточно проверить, что элементы $L_{x,y}(a), R_{x,y}(a)$ и $T_x(a)$ лежат в центре $Z(R, I)$ для всех $x, y \in L$. Рассмотрим элемент $a' = T_x(a)$ для некоторого $x \in L$. Из определения отображения T_x имеем равенство $ax = xa'$, при условии, что $a \in Z(R, I)$ получаем $xa + y = xa'$, где $y \in I$. Далее, из отображения $T_x^{-1} = L_x R_x^{-1}$ имеем равество $xa = a'x$, а значит $a'x + y = xa'$ и, тогда $a' \in Z(R, I)$. Аналогичными рассуждениями можно показать, что образы элемента a при отображениях $L_{x,y}$ и $R_{x,y}$ при при любых элементах $x, y \in L$ также лежат в $Z(R, I)$.

□

Лемма 2.36. *Пусть R – альтернативное кольцо с единицей, I – идеал кольца R, L – подлупа лупы $U(R)$ и $a \in L \cap Z(R, I)$, тогда любой элемент лупы $b \in [Ng_L(a), Ng_L(a)]_L$ имеет вид $b = 1 + x$, где $x \in I$.*

Доказательство. Напомним, что подлупа L лупы Муфанг – также лупа Муфанг. Так как лупа Муфанг является также IP-лупой, то по теореме 1.49 взаимный коммутант нормальных подлуп в лупе L состоит из нормального замыкания элементов $[a_1, a_2]_L$ и $L_{u_1,u_2}(a_3)/L_{v_1,v_2}(a_3)$, где $a_1, a_2, a_3 \in Ng_L(a)$ и $u_1/v_1, u_2/v_2 \in Ng_L(a)$.

По определению коммутатора двух элементов в лупе: $a_1a_2 = (a_2a_1)[a_1, a_2]_L$. Используя определение центра кольца по идеалу получим, что

$$a_1a_2 - (a_1a_2)[a_1, a_2]_L \in I.$$

Умножив слева на обратный элемент к элементу a_1a_2 (правый и левый обратные элементы совпадают по лемме 2.13), получим

$$(a_1a_2)^{-1}(a_1a_2 - (a_1a_2)[a_1, a_2]_L) \in I.$$

Используя свойства лупы Муфанг и дистрибутивность в кольце имеем, что

$$(a_1a_2)^{-1}(a_1a_2) - (a_1a_2)^{-1}((a_1a_2)[a_1, a_2]_L) = 1 - [a_1, a_2]_L \in I.$$

Значит, $[a_1, a_2]_L \in 1 + I$ для всех $a_1, a_2 \in Ng_L(a)$.

Далее рассмотрим элемент кольца $L_{u_1,u_2}(a_3)/L_{v_1,v_2}(a_3)$, где $a_3, u_1/v_1, u_2/v_2 \in Ng_L(a)$. По определению отображения $L_{x,y}$ имеем равество

$$L_{u_1,u_2}(a_3)/L_{v_1,v_2}(a_3)((u_1u_2)^{-1} \cdot u_1(u_2a_3)) = (v_1v_2)^{-1} \cdot v_1(v_2a_3).$$

Обозначим элемент $L_{u_1,u_2}(a_3)/L_{v_1,v_2}(a_3)$ через l. Используя определение центра кольца $u_1(u_2a_3) = (u_1u_2)a_3 + i_1, v_1(v_2a_3) = (v_1v_2)a_3 + i_2$, где $i_1, i_2 \in I$, получим

$$l((u_1u_2)^{-1}((u_1u_2)a_3 + i_1)) = (v_1v_2)^{-1}((v_1v_2)a_3 + i_1).$$

Расскрыв скобки и используя свойство лупы Муфанг (или альтернативного кольца), получим $l(a_3+i_1') = a_3+i_2'$, где $i_1', i_2' \in I$. Домножив справа на обратный элемент a_3^{-1}, получим $(la_3)a_3^{-1} \in 1 + I$. Значит,

$$L_{u_1,u_2}(a_3)/L_{v_1,v_2}(a_3) = l \in 1 + I$$

для всех $a_3, u_1/v_1, u_2/v_2 \in Ng_L(a)$.

Остается использвать тот факт, что $Ng_L(1 + I) = 1 + Ng_L(I) = 1 + I$ для любого идеала I.

□

Лемма 2.37. *Пусть R – альтернативное кольцо с единицей, L – подлупа лупы $U(R)$ и $a = 1 + x \in L$. Тогда в лупе L выполняется включение*

$$[Ng_L(a), Ng_L(a)]_L \subseteq 1 + (x)_R(x)_R.$$

Доказательство. По теореме 1.49, взаимный коммутант нормальных подлуп в лупе Муфанг L состоит из нормального замыкания элементов $[a_1, a_2]_L$ и $L_{u_1,u_2}(a_3)/L_{v_1,v_2}(a_3)$, где $a_1, a_2, a_3 \in Ng_L(a)$ и $u_1/v_1, u_2/v_2 \in Ng_L(a)$.

Отметим, что $Ng(a) = Ng(1 + x) = 1 + Ng(x)$. Пусть $x_1, x_2 \in Ng(x)$. Согласно определению коммутатора в лупе, имеем

$$(1 + x_1)(1 + x_2) = (1 + x_2)(1 + x_1)[1 + x_1, 1 + x_2]_L. \tag{1}$$

Обозначим коммутатор $[1 + x_1, 1 + x_2]_L$ через c. Домножим равенство (1) слева на $((1 + x_2)(1 + x_1))^{-1}$. По свойству лупы Муфанг получим равенство $((1+x_2)(1+x_1))^{-1} \cdot (1+x_1)(1+x_2) = c$. Данное равенство преобразуется к виду

$$((1 + x_1)^{-1}(1 + x_2)^{-1}) \cdot ((1 + x_1)(1 + x_2)) = c. \tag{2}$$

Рассмотрим элемент $(1 + x_1)^{-1}$, его можно представить в виде $1 + x_1'$, где $x_1' = -x_1 - x_1x_1' \in (x_1)_R \subseteq (Ng_L(x))_R \subseteq (x)_R$. Выполнив аналогичные действия для элемента $(1 + x_2)^{-1}$ получим из равентсва (2)

$$((1 + x_1')(1 + x_2'))((1 + x_1)(1 + x_2)) = c \tag{3}$$

Раскрыв скобки, получим равенство $1 + x_1 + x_2 + x_1x_2 + x_1' + x_1'x_1 + x_1'x_2 + x_1'(x_1x_2) + x_2' + x_2'x_1 + x_2'x_2 + x_2'(x_1x_2) + x_1'x_2' + (x_1'x_2')x_1 + (x_1'x_2')x_2 + (x_1'x_2')(x_1x_2)$. Далее из равенств $x_1' + x_1 = -x_1x_1'$ и $x_2' + x_2 = -x_2x_2'$ ясно, что в равенстве (3) все слагаемые являются элементами идеала $(x)_R(x)_R$, так как $x_1, x_2, x_1', x_2' \in (x)_R$. Значит,

$$[1 + x_1, 1 + x_2]_L = c \in 1 + (x)_R(x)_R$$

для всех $x_1, x_2 \in Ng_L(x)$.

Теперь рассмотрим элемент кольца $L_{u_1,u_2}(a_1)/L_{v_1,v_2}(a_1)$, где $a_1, u_1/v_1, u_2/v_2 \in Ng_L(1+x)$. По определению, $L_{u_1,u_2}(1+\bar{x}) = L_{u_1u_2}L_{u_1}L_{u_2}(1+\bar{x})$, где $\bar{x} \in Ng_L(x)$. Значит, выполняется равентсво $L_{u_1,u_2}(1 + \bar{x}) = (u_1u_2)^{-1}(u_1u_2 + u_1(u_2\bar{x})) = 1 + L_{u_1,u_2}(\bar{x})$. Обозначим элемент $L_{u_1,u_2}(a_1)/L_{v_1,v_2}(a_1)$ через l, тогда верно равество

$$l(1 + (u_1u_2)^{-1}(u_1(u_2\bar{x}))) = 1 + (v_1v_2)^{-1}(v_1(v_2\bar{x})). \tag{4}$$

Так как $u_1/v_1, u_2/v_2 \in Ng_L(1 + x)$, то $u_1 = (1 + x_1)v_1, u_2 = (1 + x_2)v_2$, где $x_1, x_2 \in Ng_L(x)$. Теперь отдельно рассмотрим множитель $1 + (u_1u_2)^{-1}(u_1(u_2\bar{x}))$ из равенства (4). С учетом значений для u_1 и u_2 получим

$$1 + (((1 + x_1)v_1)((1 + x_2)v_2))^{-1} \cdot (((1 + x_1)v_1)(((1 + x_2)v_2))\bar{x}). \tag{5}$$

Рассмотрим элемент $(((1+x_1)v_1)((1+x_2)v_2))^{-1}$. По свойству лупы Муфанг имеем $(((1+x_1)v_1)((1+x_2)v_2))^{-1} = (v_2^{-1}(1+x_2)^{-1})(v_1^{-1}(1+x_1)^{-1})$. Заменим элементы $(1+x_1)^{-1}, (1+x_2)^{-1}$ на $1+x_1'$ и $1+x_2'$, где $x_1' = -x_1 - x_1x_1', x_2' = -x_2 - x_2x_2'$. Далее, раскрыв скобки, получим $v_2^{-1}v_1^{-1} + v_2^{-1}(v_1^{-1}x_1') + (v_2^{-1}x_2')v_1^{-1} + (v_2^{-1}x_2')(v_1^{-1}x_1') \in v_2^{-1}v_1^{-1} + (x)_R + (x)_R(x)_R$, с учетом того, что $x_1, x_2 \in (x)_R$. Теперь элемент $u_1(u_2\bar{x}) = ((1+x_1)v_1)((1+x_2)v_2 \cdot \bar{x}) = v_1(v_2\bar{x}) + v_1((x_2v_2)\bar{x}) + (x_1v_1)(v_2\bar{x}) + (x_1v_1)((x_1v_2)\bar{x}) \in v_1(v_2\bar{x}) + (x)_R(x)_R$, с учетом того, что $x_1, x_2 \in (x)_R$. Тогда

$$(((1+x_1)v_1)((1+x_2)v_2))^{-1} \in v_2^{-1}v_1^{-1} \cdot v_1(v_2\bar{x}) + (x)_R(x)_R. \tag{6}$$

Подставив (6) в равенство (4), получим

$$1 + v_2^{-1}v_1^{-1} \cdot v_1(v_2\bar{x}) \in l(1 + v_2^{-1}v_1^{-1} \cdot v_1(v_2\bar{x}) + (x)_R(x)_R).$$

Тогда

$$L_{u_1,u_2}(a_1)/L_{v_1,v_2}(a_1) = l \in 1 + (x)_R(x)_R$$

для всех $a_1, u_1/v_1, u_2/v_2 \in Ng_L(a)$.

□

Теорема 2.38. *Если R – альтернативное кольцо с единицей, то для любой подлупы L лупы $U(R)$ выполняется включение $L \cap Z(R, rad\ R) \subseteq radL$.*

Доказательство. Пусть $a \in L \cap Z(R, rad\ R)$, тогда рассмотрим любую последовательность a_i, такую что $a_0 = a$ и $a_{i+1} \in [Ng_L(a_i), Ng_L(a_i)]_L$. По лемме 2.36 верно, что $a_1 = 1 + x_1, x_1 \in rad\ R$. Далее из леммы 2.37 следует, что $a_i = 1 + x_i, x_i \in (x_{i-1})_R(x_{i-1})_R \subseteq (x)_R(x)_R$. Так как первичный радикал $rad\ R$ альтернативного кольца R состоит из строго нильпотентных элементов кольца R, то $a_i = 1$ для некторого индекса, т.е. элемент a является строго энгелевым в лупе L. Значит, $a \in radL$.

□

Следствием этого результата является:

Теорема 2.39. *Пусть: R – коммутативное и ассоциативное кольцо с единицей, L – лупа и RL – альтернативное луповая алгебра с единицей. Тогда для любой подлупы N лупы $U(RL)$ выполняется включение*

$$N \cap Z(RL, rad\ RL) \subseteq radN.$$

2.4 Первичный радикал лупы $GLL(2,R)$

Пусть R – коммутативное и ассоциативное кольцо с единицей. Рассмотрим кольцо матриц Цорна $\mathcal{Z}(R)$ над R, состоящее из 2×2 матриц вида:

$$\begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix},$$

где $a,b\in R$ и $\alpha,\beta\in R\times R\times R$,

Операция сложения осуществляется поэлементно, а операция умножения имеет следующий вид:

$$\begin{pmatrix} a_1 & \alpha_1 \\ \beta_1 & b_1 \end{pmatrix}\cdot\begin{pmatrix} a_2 & \alpha_2 \\ \beta_2 & b_2 \end{pmatrix}=\begin{pmatrix} a_1a_2+\alpha_1\beta_2 & a_1\alpha_2+b_2\alpha_1-\beta_1\times\beta_2 \\ a_2\beta_1+b_1\beta_2+\alpha_1\times\alpha_2 & \beta_1\cdot\alpha_2+b_1b_2 \end{pmatrix}$$

Заметим, что кольцо $\mathcal{Z}(R)$ является альтернативным.

Элемент

$$A=\begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix},$$

обратим тогда и только тогда, когда в кольце R обратим его детерминант

$$det\begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix}=ab-\alpha\times\beta.$$

В этом случае,

$$A^{-1}=(detA)^{-1}\begin{pmatrix} b & -\alpha \\ -\beta & a \end{pmatrix}.$$

Лупа обратимых элементов кольца $\mathcal{Z}(R)$ является лупой Муфанг (по теореме 2.13) и обозначается $GLL(2,R)$.

Введем следующие обозначения: $e_1=\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, $e_2=\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$.

Для данных элементов выполняются следующие равенства:

$$e_1+e_2=E,\quad e_1\cdot e_2=0,\quad e_1^2=e_1,\quad e_2^2=e_2.$$

Дополнительно рассмотрим следующие элементы кольца:

$e^{11}=\begin{pmatrix} 0 & (1,0,0) \\ 0 & 0 \end{pmatrix}$, $e^{12}=\begin{pmatrix} 0 & (0,1,0) \\ 0 & 0 \end{pmatrix}$, $e^{13}=\begin{pmatrix} 0 & (0,0,1) \\ 0 & 0 \end{pmatrix}$,

$e^{21}=\begin{pmatrix} 0 & 0 \\ (1,0,0) & 0 \end{pmatrix}$, $e^{22}=\begin{pmatrix} 0 & 0 \\ (0,1,0) & 0 \end{pmatrix}$, $e^{23}=\begin{pmatrix} 0 & 0 \\ (0,0,1) & 0 \end{pmatrix}$.

Для данных элементов выполняются следующие равенства:

$$e^{ij}\cdot e^{ij}=0,\ \text{для всех } i=1,2,j=1,2,3,$$

$$e^{1i} \cdot e^{2j} = e^{2j} \cdot e^{1i} = 0 \text{ для всех } i \neq j, i, j = 1, 2, 3,$$
$$e^{1i} \cdot e^{2i} = e_1, e^{2i} \cdot e^{1i} = e_2 \text{ для всех } i = 1, 2, 3.$$

Кроме того верны следующие равенства

$$e^{11} \cdot e^{12} = e^{23}, \quad e^{11} \cdot e^{13} = -e^{22},$$
$$e^{12} \cdot e^{11} = -e^{23}, \quad e^{12} \cdot e^{13} = e^{21},$$
$$e^{13} \cdot e^{11} = e^{22}, \quad e^{13} \cdot e^{12} = -e^{21},$$
$$e^{21} \cdot e^{22} = e^{13}, \quad e^{21} \cdot e^{23} = -e^{12},$$
$$e^{22} \cdot e^{21} = -e^{13}, \quad e^{22} \cdot e^{23} = e^{11},$$
$$e^{23} \cdot e^{21} = e^{12}, \quad e^{23} \cdot e^{22} = -e^{11}.$$

Пусть $A = \begin{pmatrix} a & (\alpha_1, \alpha_2, \alpha_3) \\ (\beta_1, \beta_2, \beta_3) & b \end{pmatrix}$, тогда элемент a будем обозначать как $A^{(10)}$, элемент b – $A^{(20)}$ и соответсвующие элементы из $R \times R \times R$ как $A^{(ij)}, i = 1, 2, j = 1, 2, 3$.

Отметим, что для того, чтобы получить элемент $A^{(ij)}, i = 1, 2, j = 0, 1, 2, 3$ кольца R необходимо применить функцию $\mathcal{F}^{(ij)}(A)$:

$$\mathcal{F}^{(10)}(A) = A^{(10)} = e_1 A e_1, \quad \mathcal{F}^{(20)}(A) = A^{(20)} = e_2 A e_2,$$
$$\mathcal{F}^{(11)}(A) = A^{(11)} = (e^{11}((e^{12}(e_1 A e_2))e^{21}))e^{22},$$
$$\mathcal{F}^{(12)}(A) = A^{(12)} = (e^{12}((e^{11}(e_1 A e_2))e^{22}))e^{21},$$
$$\mathcal{F}^{(13)}(A) = A^{(13)} = (e^{13}((e^{12}(e_1 A e_2))e^{23}))e^{22},$$
$$\mathcal{F}^{(21)}(A) = A^{(21)} = (e^{21}((e^{22}(e_2 A e_1))e^{11}))e^{12},$$
$$\mathcal{F}^{(22)}(A) = A^{(22)} = (e^{22}((e^{21}(e_2 A e_1))e^{12}))e^{11},$$
$$\mathcal{F}^{(23)}(A) = A^{(23)} = (e^{23}((e^{22}(e_2 A e_1))e^{12}))e^{12}.$$

Теперь докажем некоторый неассоциативный аналог теоремы Михалева А.В. и Голубчика И.З.

Теорема 2.40. *Пусть K – коммутативное и ассоциативное кольцо с единицей, $\mathcal{Z}(K)$ – кольцо матриц Цорна, $GLL(2, K)$ – лупа обратимых матриц из $\mathcal{Z}(K)$. Тогда*

$$rad\ GLL(2, K) = Z(\mathcal{Z}(K), rad\ \mathcal{Z}(K)).$$

Доказательство. Введем следующие обозначения: $R = \mathcal{Z}(K)$, $L = GLL(2, K)$. Напомним, что кольцо R является альтернативным, а лупа L

– лупой Муфанг. По теореме 2.38, $Z(R, radR) \subseteq radL$, поэтому остается показать, что $radL \subseteq Z(R, radR)$. Пусть $radL \nsubseteq Z(R, radR)$. Тогда $radL \nsubseteq Z(R, P)$ для некоторого первичного идеала P кольца R. Действительно, достаточно показать, что $Z(R, radR) = \cap_{P \in \mathcal{P}} Z(R, P)$, где $\mathcal{P}$ – совокупность всех первичных идеалов кольца R. Если $radR \subseteq P$, то $Z(R, radR) \subseteq Z(R, P)$ для всех $P \in \mathcal{P}$. Если $a \in \cap_{P \in \mathcal{P}} Z(R, P)$, то элементы $[a, r]_R$, $[a, n, m]_R$, $[n, a, m]_R$, $[n, m, a]_R \in P$ для всех r, $n, m \in R$ и всех $P \in \mathcal{P}$. В этом случае, элементы $[a, r]_R$, $[a, n, m]_R$, $[n, a, m]_R$, $[n, m, a]_R \in radR$, т.е. $a \in Z(R, radR)$.

Теперь, если это необходимо, переходя к фактор-кольцу R/P, будем считать, что R – первичное кольцо и $radL$ – нецентральная подлупа лупы $U(R)$. В этом случае существует неединичная нормальная первичная подлупа A лупы L такая, что

$$A \nsubseteq Z(L) \text{ и } [A, A]_L \subseteq Z(L) \tag{7}$$

иначе первичный радикал $rad(L/Z(L))$ был бы единичной подлупой E (т.к. $rad\ L/Z(L) = E \leftrightarrow E$ является первичной подлупой $\leftrightarrow$ для всех нормальных подлуп A' лупы $L/Z(L)$ из включения $[A', A']_{L/Z(L)} \subseteq E$ следует, что $A' = E$).

В силу первичности кольца R для ненулевого элемента $T \in A \setminus Z(L)$ существует элемент $D \in R$, по лемме 2.16, такой что $T^{(21)} \cdot D^{(11)} \neq 0$. Рассмотрим элемент $B = (T(E + D^{(11)})) \cdot (T^{-1}(E - D^{(11)}))$. Покажем, что $B \notin Z(L)$. Допустим, что $B \in Z(L)$. Тогда элемент B должен коммутировать, в том числе с элементами $X^{(1i)}$ и $X^{(2i)}, i = 1, 2, 3$. Значит, элементы $B^{(ji)}, j = 1, 2, i = 1, 2, 3$ равны 0. Следовательно, B имеет следующий вид $B = \begin{pmatrix} y & 0 \\ 0 & y \end{pmatrix}, y \in K$. По определению элемента B и альтернативности кольца R имеем, $T(E + D^{(11)}) = B \cdot ((E + D^{(11)})T)$. Следовательно, $T + TD^{(11)} = BT + B \cdot D^{(11)}T$. Теперь применим в обеим частям равенства преобразование $\mathcal{F}^{(12)}$: $\mathcal{F}^{(12)}(T) + \mathcal{F}^{(12)}(TD^{(11)}) = \mathcal{F}^{(12)}(BT) + \mathcal{F}^{(12)}(B \cdot D^{(11)}T)$. Данное преобразование получает значение элемента на позиции (12), однако, элементы $TD^{(11)}$ и $B \cdot D^{(11)}T$ имеют нулевой элемент на данной позиции. В итоге имеем, что $T^{(12)} = (BA)^{(12)}$. Следовательно, из формы элемента B имеем, что $B = E$. Тогда $TD^{(11)} = D^{(11)}T$, т.е. $\begin{pmatrix} 0 & * \\ * & d_{11}t_{21} \end{pmatrix} = \begin{pmatrix} t_{21}d_{11} & * \\ * & 0 \end{pmatrix}$, где $d_{11} = D^{(11)}, t_{21} = T^{(21)}$, т.е. $t_{21}d_{11} = d_{11}t_{21} = 0$. Следовательно, $T^{(21)} \cdot D^{(11)} = 0$, противоречие с выбором элемента D.

Теперь в следствие первичности кольца R существует элемент $S \in R$ такой, что $B^{(12)}S^{(22)} \neq 0$. Рассмотрим элемент $M = (B(E + S^{(22)})) \cdot (B^{-1}(E - S^{(22)}))$. Пусть $M \in Z(L)$, тогда $M \cdot ((E + S^{(22)})B) = B(E + S^{(22)})$. Следовательно, $MB + M(S^{(22)B)} = B + BS^{(22)}$. Тогда, используя преобразование $\mathcal{F}^{(23)}$, получим, что $(MB)^{(23)} = B^{(23)}$, значит, $M = E$. Далее, из равенства $BS^{(22)} = S^{(22)}B$, получим, что $B^{(12)}S^{(22)} = 0$, что противоречит выбору эдемента S. Зна-

чит, $M \notin Z(L)$, а, значит, $M^{(23)} \neq 0$. Далее так как $[A,A]_L \subseteq Z(L)$, имеем $M = \lambda\big(((E+S^{(22)})B^{-1})\cdot((E-S^{(22)})B)\big)$.

Покажем, что $\lambda = -E$. Действительно, $\mathcal{F}^{(23)}(M) = M^{(23)} = \mathcal{F}^{(23)}(BB^{-1} - B(B^{-1}S^{(22)}) + (BS^{(22)})B^{-1} - (BS^{(22)})(B^{-1}S^{(22)}))$. Можно показать, что $M^{(23)} = \mathcal{F}^{(23)}((BS^{(22)})B^{-1})$. С другой стороны, $M^{(23)} = \mathcal{F}^{(23)}(\lambda[B^{-1}B - B^{-1}(BS^{(22)}) + (B^{-1}S^{(22)})B - (B^{-1}S^{(22)})(BS^{(22)})])$, т.е. $M^{(23)} = -\mathcal{F}^{(23)}(\lambda[(B^{-1}S^{(22)})B]$. Из двух представлений элемента $M^{(23)}$ и вида элемента из центра можно сделать вывод, что $\lambda = -E$.

Далее рассмотрим элемент $M^{(10)}$. По определению элемента M с одной стороны имеем, что $M^{(10)} = e_1(BB^{-1} - B(B^{-1}S^{(22)}) + (BS^{(22)})B^{-1} - (BS^{(22)})\cdot(B^{-1}S^{(22)}))e_1 = E^{(10)} + e_1((BS^{(22)})B^{-1})e_1$. Так как элементы $B(B^{-1}S^{(22)})$ и $(BS^{(22)})(B^{-1}S^{(22)})$ имеют нулевой элемент на позиции (10). С другой стороны, $M^{(10)} = e_1(\lambda[B^{-1}B - B^{-1}(BS^{(22)}) + (B^{-1}S^{(22)})B - (B^{-1}S^{(22)})(BS^{(22)})])e_1 = E^{(10)} + e_1(\lambda[(B^{-1}S^{(22)})B])e_1$. Тогда $\lambda = E$. В итоге получаем, что $\lambda = -E = E$.

Далее, из двух представлений элемента M получим, что $[B(E+S^{(22)})]^2\cdot[B^{-1}(E+S^{(22)})]^2 = E$. Расскрыв скобки, можно показать, что равенство выполняется при $B^{(12)}S^{(22)} = 0$, что приводит к противоречию с выбором элемента $S^{(22)}$.

□

3 Криптографические схемы над неассоциативными структурами

3.1 Построение алгебраической криптосистемы над квазигрупповым кольцом

С. К. Росошек предложил в [21] криптосистему, все вычисления которой производятся в групповом кольце и в группе его автоморфизмов. Построим подобную криптосистему над неассоциативной структурой – квазигрупповым кольцом.

Пусть K – кольцо с единицей (необязательно ассоциативное), Q – квазигруппа. Рассмотрим квазигрупповое кольцо KQ, состоящее из всех формальных сумм вида $\sum_{q\in Q}\alpha_q\cdot q$ $(\alpha_l\in K)$, в которых конечное число α_q отлично от нуля. Предполагаем, что группы автоморфизмов $AutK$ и $AutQ$ некоммутативны, причём $|AutK|\geq t_1$, $|AutQ|\geq t_2$, где t_1 и t_2 – параметры безопасности. Также предполагаем, что в KL достаточно элементов с нулевым левым аннулятором.

Рассмотрим следующую задачу. Пусть R – алгебраическая структура (например, кольцо или квазигруппа), A некоторое подмножество автоморфизмов в $AutR$, α – случайно выбранный элемент из A. Предположим, что известно некоторое множество пар

$$(x_i,\alpha(x_i)), i=1,\ldots,n,$$

где $x_i\in R$. Требуется найти автоморфизм $\alpha'\in A$, такой что $\alpha'(x_i)=\alpha(x_i)$ для всех $i=1,\ldots,n$, а также $\alpha'(y_j)=\alpha(y_j)$ для некоторых случайно выбранных $y_j\in R, y_j\neq x_i, j=1,\ldots,m, i=1,\ldots,n$, причем злоумышленнику не известны значения $\alpha(y_j), j=1,\ldots,m$. Обозначим эту задачу как $\Omega_n^m(A,R)$.

Заметим, что при отсутствии существенной информации о множествах A и R, задача $\Omega_n(A,R)$ является вычислительно трудной и разрешима полным перебором всех элементов множества A, и для каждого выбранного $\alpha'\in A$ проверкой условия $\alpha'(x_i)=\alpha(x_i), i=1,\ldots,n$ и производных соотношений из этих условий.

Криптосистема имеет следующий вид:

Участник A :

1. Конструирует такой автоморфизм $\sigma\in AutK$, что $|\sigma|\geq t_3$, причём σ имеет нетривиальный централизатор $C(\sigma)$ и $|C(\sigma)\setminus\langle\sigma\rangle|\geq t_4$, где t_3,t_4 - параметры безопастности.

2. Конструирует такой автоморфизм $\eta\in AutQ$, что $|\eta|\geq t_5$, причём η имеет нетривиальный централизатор $C(\eta)$ и $|C(\eta)\setminus\langle\eta\rangle|\geq t_6$, где t_5,t_6 - параметры безопастности.

3. Случайно выбирает автоморфизм $\tau \in C(\sigma) \setminus \langle\sigma\rangle$.

4. Случайно выбирает такой ω, что $\omega \in C(\eta) \setminus \langle\eta\rangle$.

5. По τ и ω строит автоморфизм $\varphi \in AutKQ$ (назовем его секретным автоморфизмом) так: для любого $h \in KQ$ вида

$$h = a_{q_1}q_1 + \cdots + a_{q_n}q_n,$$

где $Q = \{q_1, \ldots, q_n\}$, $a_{q_1}, \ldots, a_{q_n} \in K$, пусть

$$\varphi(h) = \tau(a_{q_1})\omega(q_1) + \cdots + \tau(a_{q_n})\omega(q_n)$$

6. Выбирает элементы $a \in KQ, x \in KQ$.

7. Вычисляет $\varphi(x)$ и $\varphi(a)$.

Открытым ключом участника А является:

$$\Big(\sigma, \eta, x, \varphi(x), a, \varphi(a)\Big).$$

Отметим, что при должных параметрах безопасности t_3, t_4, t_5, t_6 автоморфизмов, подходящих для открытого ключа, достаточно много. Сформированный открытый ключ участник А передает участнику В по открытому каналу.

Участник B:

1. Выбирает натуральные числа (i, j, k, l).

2. Используя открытый ключ участника A, получает пары автоморфизмов (σ^i, η^j),(σ^k, η^l) и по ним строит автоморфизмы $\psi, \chi \in AutKQ$ таким же способом, как и участник A, т.е. для любого $h \in KL$ вида $h = a_{q_1}q_1 + \cdots + a_{q_n}q_n$ полагает $\psi(h) = \sigma^i(a_{q_1})\eta^j(q_1) + \cdots + \sigma^i(a_{q_n})\eta^j(q_n)$, а $\chi(h) = \sigma^k(a_{q_1})\eta^l(q_1) + \cdots + \sigma^k(a_{q_n})\eta^l(q_n)$. Автоморфизмы ψ, χ будем называть сеансовыми.

3. Вычисляет $\chi(a) \cdot \psi(x)$.

4. Вычисляет $\chi(\varphi(a)) \cdot \psi(\varphi(x))$ и левый аннулятор $Ann\big(\chi(\varphi(a)) \cdot \psi(\varphi(x))\big)$.

5. Если полученный аннулятор $Ann\big(\chi(\varphi(a)) \cdot \psi(\varphi(x))\big)$ ненулевой, то производится новый сеанс связи с выбором новых элементов a и x или же выбираются другие сеансовые автоморфизмы.

6. Записывает исходный текст, который надо передать, в виде $m \in KL$ и вычисляет $m \cdot \Big[\chi(\varphi(a)) \cdot \psi(\varphi(x))\Big]$.

7. Отправляет для A криптограмму

$$\Big(\chi(a)\cdot\psi(x),\, m\cdot\Big[\chi\big(\varphi(a)\big)\cdot\psi\big(\varphi(x)\big)\Big]\Big)$$

Получив криптограмму, участник A расшифровывает её:

1. Используя секретный автоморфизм φ, вычисляет $\varphi\big(\chi(a)\cdot\psi(x)\big)$.

2. Расшифровывает посланный текст пользуясь тем, что χ, ψ и φ коммутируют, поскольку сеансовые автоморфизмы ψ, χ построены на степенях выбранных автоморфизмов σ, η, а секретный автоморфизм φ построен с помощью элементов из централизаторов σ, η.

   Участник А знает $m\cdot\Big[\varphi\big(\chi(a)\cdot\psi(x)\big)\Big] = h$ и $\varphi\big(\chi(a)\cdot\psi(x)\big) = r$; следовательно, для получения сообщения m достаточно решить линейную систему $m\cdot r = h$ с коэффициентами из кольца K.

В самом деле, так как $\tau \in C(\sigma)\setminus\langle\sigma\rangle$ и $\omega \in C(\eta)\setminus\langle\eta\rangle$, то коммутируют между собой попарно автоморфизмы τ и σ; ω и η. Поэтому коммутируют и сконструированные на их основе автоморфизмы φ и ψ, φ и χ. Вследствие этого $\chi(\varphi(a))\cdot\psi(\varphi(x)) = \varphi\big(\chi(a)\cdot\psi(x)\big) = q$. Кроме того, элемент $\chi(\varphi(a))\cdot\psi(\varphi(x))$ выбран с нулевым левым аннулятором. Поэтому система уравнений $m\cdot q = h$ с коэффициентами из кольца K имеет единственное решение.

Анализ атак на криптосистему

Рассмотрим некоторые атаки на криптосистему.

1. *Атака только с криптограммой.*

   Пусть злоумышленник располагает открытым ключом участника A и криптограммой. Перед ним стоит следующая задача: по известным парам $\big(a,\varphi(a)\big), \big(x,\varphi(x)\big)$ найти такой $\alpha \in AutKQ$, индуцированный автоморфизмами (σ',η'), что $\varphi(a)=\alpha(a)$, $\varphi(x)=\alpha(x)$. К тому же необходимо, чтобы $\sigma' \in C(\sigma)\setminus\langle\sigma\rangle$, а $\eta' \in C(\eta)\setminus\langle\eta\rangle$.

   Наличие у злоумышленника не одной криптограммы, а некоторого множества криптограмм, не позволяет упростить задачу. В этом случае злоумышленник обладает некоторым подмножеством элементов $r_i \in KQ$ и соответствующими уравнениями из которых ему необходимо найти сообщение: $m_i\cdot\varphi(r_i) = h_i$, не зная автоморфизм φ.

   Попробуем построить автоморфизм α для этого случая. Положим $\alpha(a) := \varphi(a)$, $\alpha(x) := \varphi(x)$. Доопределим его на элементах ax и xa: $\alpha(ax) = \alpha(a)\cdot\alpha(x) := \varphi(a)\cdot\varphi(x)$ и $\alpha(xa) = \alpha(x)\cdot\alpha(a) := \varphi(x)\cdot\varphi(a)$.

Но значение автоморфизма α на элементе $\chi(a) \cdot \psi(x)$ так же должно совпадать со значением автоморфизма φ на этом же элементе. Данную проблему можно решить перебором образа α с последующей проверкой того, что $\sigma' \in C(\sigma) \setminus \langle\sigma\rangle$, а $\eta' \in C(\eta) \setminus \langle\eta\rangle$. Но это вычислительно не легче перебора всех автоморфизмов, индуцированных парами $(\sigma', \eta') \in \big(C(\sigma) \setminus \langle\sigma\rangle\big) \times \big(C(\eta) \setminus \langle\eta\rangle\big)$, удовлетворяющих начальным условиям $\alpha(a) = \varphi(a)$ и $\alpha(x) = \varphi(x)$. В итоге получаем задачу $\Omega_2^1(Y, KQ)$, где Y – это множество автоморфизмов KL, полученных с помощью пар $(\sigma', \eta') \in \Big[\big(C(\sigma) \setminus \langle\sigma\rangle\big) \times \big(C(\eta) \setminus \langle\eta\rangle\big)\Big]$.

Для оценки сложности вскрытия криптосистемы злоумышленником будем рассматривать мощность множества, элементы которого необходимо перебрать. Мощность этого множества равна $t_4 \cdot t_6$. При надлежащем выборе параметров безопасности задача является вычислительно трудной.

2. *Атака на сеансовые автоморфизмы ψ и χ.*

Другой способ атаки – найти автоморфизмы ψ и χ, а затем решить относительно m уравнение $m \cdot \Big[\chi\big(\varphi(a)\big) \cdot \psi\big(\varphi(x)\big)\Big] = h$, где h известен из криптограммы. Пусть ψ был построен с помощью автоморфизмов (σ_1, η_1), а автоморфизм χ с помощью (σ_2, η_2). Для того чтобы найти ψ и χ, криптоаналитику придется перебрать пары $(\sigma_1, \eta_1) \in (\langle\sigma\rangle, \langle\eta\rangle)$ и $(\sigma_2, \eta_2) \in (\langle\sigma\rangle, \langle\eta\rangle)$ с последующей проверкой условия $\chi(a)\psi(x) = h_1$, где h_1 известен из криптограммы. Произведение найденных автоморфизмов должно совпадать с произведением искомых на элементах $\varphi(a), \varphi(x)$. Следовательно, определенная выше сложность атаки будет равна $t_3^2 \cdot t_5^2$. При правильном выборе соответствующих параметров безопасности эта задача является вычислительно трудной.

Поясним, почему для построения сеансового автоморфизма рассматривался не один автоморфизм, а выбрано произведение $\chi(a)\psi(x)$. В случае единственного автоморфизма открытый ключ участника - это: $\big(\sigma, \eta, x, \varphi(x)\big)$, а криптограмма – $\big(\psi(x), m \cdot \psi(\varphi(x))$. В этом случае стали бы возможны следующие атаки:

а) *Атака на сеансовый автоморфизм.* Пусть автоморфизм ψ, как и раньше, построен с помощью (σ^i, η^j). Для нахождения σ^i можно учесть тот факт, что любой автоморфизм отображает единицу в единицу. Тогда из коэффициентов при единице кольца R для x и $\psi(x)$ получаем пару элементов кольца K вида $(a_e, \sigma^i(a_e))$; аналогичные рассуждения верны, если Q является лупой. Таким образом, криптоаналитик получает допол-

нительную информацию о сеансовом автоморфизме ψ. В случае выбора произведения двух сеансовых автоморфизмов, такая атака невозможна, так как коэффициент при единице у элемента $\psi(x) \in KL$ равен $\sum_{lh=e} \alpha_l \beta_h$, где $l, h \in L$, а это не позволяет получить пару вида $(a_e, \sigma^i(a_e))$.

б) *Атака на автоморфизм φ с известным исходным текстом.* Криптоаналитик вычисляет $x \cdot \psi(x) = y$. Тогда $\varphi(x) \cdot \psi(\varphi(x)) = \varphi(x \cdot \psi(x))$. Следовательно, у криптоаналитика имеется кроме $(x, \varphi(x))$ еще и пара $(y, \varphi(y))$. В случае выбора произведения двух сеансовых автоморфизмов такая атака существенно ослаблена, так как не удастся получить вторую пару подобным образом, и придется восстанавливать φ по одной паре.

Таким образом, выбор произведения двух сеансовых автоморфизмов в целом оправдан.

3. **Атака с выбранными исходными текстами**

Эта атака основана на попытке злоумышленника получить $\chi(\varphi(a)) \cdot \psi(\varphi(x)) \in KL$ с последующим решением уравнения $m \cdot \chi(\varphi(a))\psi(\varphi(x))$ относительно m посредством нового сеанса связи с участником B в качестве участника A. Даже если участник B повторяет тот же исходный текст m, то он должен сконструировать новые сеансовые автоморфизмы $\psi' \neq \psi$ и $\chi' \neq \chi$. Поэтому злоумышленник получит не $m \cdot \chi(\varphi(a))\psi(\varphi(x))$, а $m \cdot \chi'(\varphi(a))\psi'(\varphi(x))$. И даже если он решит новое уравнение относительно $\chi'(\varphi(a))\psi'(\varphi(x))$, никакой новой информации относительно $\chi(\varphi(a))\psi(\varphi(x))$ он не получит. Таким образом, злоумышленник может только накапливать значения автоморфизма φ на различных прообразах. Однако при правильно выбранных параметрах безопасности и своевременном обновлении секретного ключа данная атака вычислительно трудна.

Поиск подходящих для шифрования колец и луп.

Рассмотрим некоторые структуры, подходящие для построения криптосистемы. В качестве лупы будем брать прямое произведение нескольких групп и луп, варьируя их количество для подбора параметров безопасности.

Для построения примера рассмотрим следующую неассоциативную лупу Муфанг M порядка 16. Приведем ее таблицу Кэли:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
2	4	8	6	3	1	5	7	14	9	16	10	11	12	13	15
3	5	4	7	6	8	1	2	15	13	9	11	14	16	12	10
4	6	7	1	8	2	3	5	12	14	15	9	16	10	11	13
5	7	2	8	4	3	6	1	13	11	14	16	12	15	10	9
6	1	5	2	7	4	8	3	10	12	13	14	15	9	16	11
7	8	1	3	2	5	4	6	11	16	12	15	10	13	9	14
8	3	6	5	1	7	2	4	16	15	10	13	9	11	14	12
9	10	11	12	16	14	15	13	4	6	7	1	5	2	3	8
10	12	16	14	15	9	13	11	2	4	5	6	3	1	8	7
11	13	12	15	10	16	9	14	3	8	4	7	6	5	1	2
12	14	15	9	13	10	11	16	1	2	3	4	8	6	7	5
13	15	10	16	9	11	14	12	8	7	2	5	4	3	6	1
14	9	13	10	11	12	16	15	6	1	8	2	7	4	5	3
15	16	9	11	14	13	12	10	7	5	1	3	2	8	4	6
16	11	14	13	12	15	10	9	5	3	6	8	1	7	2	4

Отметим, что $|AutM| = 1344$, причем система порождающих в группе $AutM$ (если ее представить в виде подгруппы группы перестановок) состоит из двух элементов

$$[a, b] = [(2, 3)(5, 8)(6, 7)(10, 11)(13, 16)(14, 15),$$

$$(2, 14, 13, 15, 8, 9, 3)(5, 12, 7, 6, 10, 16, 11)].$$

Заметим, что $|a| = 2, |b| = 7$, а $|C(a)| = 16, |C(b)| = 7$. Усложним структуру. Теперь представим $S = Aut(M \times M)$, в виде подгруппы группы перестановок. $|S| = 231211008$.

Система порождающих $[a, b, c] = [(129, 145, 177, 209)(130, 146, 178, 210)$
$(131, 147, 179, 211)(132, 148, 180, 212)(133, 149, 181, 213)(134, 150, 182, 214)$
$(135, 151, 183, 215)(136, 152, 184, 216)(137, 153, 185, 217)(138, 154, 186, 218)$
$(139, 155, 187, 219)(140, 156, 188, 220)(141, 157, 189, 221)(142, 158, 190, 222)$
$(143, 159, 191, 223)(144, 160, 192, 224)(161, 241, 225, 193)(162, 242, 226, 194)$
$(163, 243, 227, 195)(164, 244, 228, 196)(165, 245, 229, 197)(166, 246, 230, 198)$
$(167, 247, 231, 199)(168, 248, 232, 200)(169, 249, 233, 201)(170, 250, 234, 202)$
$(171, 251, 235, 203)(172, 252, 236, 204)(173, 253, 237, 205)(174, 254, 238, 206)$
$(175, 255, 239, 207)(176, 256, 240, 208)$,
$(17, 132, 36, 20, 129, 33)(18, 134, 38, 22, 130, 34)(19, 135, 39, 23, 131, 35)$
$(21, 136, 40, 24, 133, 37)(25, 140, 44, 28, 137, 41)$
$(26, 142, 46, 30, 138, 42)(27, 143, 47, 31, 139, 43)(29, 144, 48, 32, 141, 45)$
$(65, 212, 161)(66, 214, 162)(67, 215, 163)(68, 209, 164)(69, 216, 165)$

$(70, 210, 166)(71, 211, 167)(72, 213, 168)(73, 220, 169)(74, 222, 170)$
$(75, 223, 171)(76, 217, 172)(77, 224, 173)(78, 218, 174)(79, 219, 175)$
$(80, 221, 176)(81, 180, 100, 84, 177, 97)(82, 182, 102, 86, 178, 98)$
$(83, 183, 103, 87, 179, 99)(85, 184, 104, 88, 181, 101)(89, 188, 108, 92, 185, 105)$
$(90, 190, 110, 94, 186, 106)(91, 191, 111, 95, 187, 107)(93, 192, 112, 96, 189, 109)$,
$(113, 148, 225)(114, 150, 226)(115, 151, 227)(116, 145, 228)(117, 152, 229)$
$(118, 146, 230)(119, 147, 231)(120, 149, 232)(121, 156, 233)(122, 158, 234)$
$(123, 159, 235)(124, 153, 236)(125, 160, 237)(126, 154, 238)(127, 155, 239)$
$(128, 157, 240)(193, 196)(194, 198)(195, 199)(197, 200)(201, 204)(202, 206)$
$(203, 207)(205, 208)(241, 244)(242, 246)(243, 247)(245, 248)(249, 252)$
$(250, 254)(251, 255)(253, 256)(2, 17)(3, 33)(4, 49)(5, 65)(6, 81)(7, 97)$
$(8, 113)(9, 129)(10, 145)(11, 161)(12, 177)(13, 193)(14, 209)(15, 225)$
$(16, 241)(19, 34)(20, 50)(21, 66)(22, 82)(23, 98)(24, 114)(25, 130)(26, 146)$
$(27, 162)(28, 178)(29, 194)(30, 210)(31, 226)(32, 242)(36, 51)(37, 67)(38, 83)$
$(39, 99)(40, 115)(41, 131)(42, 147)(43, 163)(44, 179)(45, 195)(46, 211)$
$(47, 227)(48, 243)(53, 68)(54, 84)(55, 100)(56, 116)(57, 132)(58, 148)(59, 164)$
$(60, 180)(61, 196)(62, 212)(63, 228)(64, 244)(70, 85)(71, 101)(72, 117)$
$(73, 133)(74, 149)(75, 165)(76, 181)(77, 197)(78, 213)(79, 229)(80, 245)$
$(87, 102)(88, 118)(89, 134)(90, 150)(91, 166)(92, 182)(93, 198)(94, 214)$
$(95, 230)(96, 246)(104, 119)(105, 135)(106, 151)(107, 167)(108, 183)$
$(109, 199)(110, 215)(111, 231)(112, 247)(121, 136)(122, 152)(123, 168)$
$(124, 184)(125, 200)(126, 216)(127, 232)(128, 248)(138, 153)(139, 169)$
$(140, 185)(141, 201)(142, 217)(143, 233)(144, 249)(155, 170)(156, 186)$
$(157, 202)(158, 218)(159, 234)(160, 250)(172, 187)(173, 203)(174, 219)$
$(175, 235)(176, 251)(189, 204)(190, 220)(191, 236)(192, 252)(206, 221)$
$(207, 237)(208, 253)(223, 238)(224, 254)(240, 255)]$, причем $|a| = 4$, $|b| = 6$, $|c| = 2$.

Рассмотрим централизаторы этих элементов – $|C(a)| = 1376256$, $|C(b)| = 129024$, $|C(c)| = 21504$. Как видим, даже на структурах такого маленького порядка получаются достаточно большие централизаторы. Итак, если включить несколько таких луп M в прямое произведение, то это будет лупа с большим количеством автоморфизмов, среди которых есть элементы с большими централизаторами.

Чтобы увеличить порядок самих автоморфизмов, сделаем следующее. Рассмотрим $H =< a >$ – циклическую группу, порожденную элементом a. Как известно, $|AutH| = \varphi(a)$, где φ – функция Эйлера. Мы всегда можем подобрать порядок a таким образом, чтобы в $AutH$ существовали автоморфизмы большого порядка. Итак, если взять лупу вида $S = M \times M \times \ldots \times M \times H \times H \times \ldots \times H$, то в группе ее автоморфизмов будет достаточно много элементов, подходящих для построения криптосистемы.

В качестве кольца рассмотрим $K = M_2(Z_5)$ – кольцо квадратных матриц второго порядка над Z_5. Пусть $A = \left(\begin{smallmatrix} 1 & 4 \\ 0 & 1 \end{smallmatrix}\right) \in K^*$ и σ – внутренний автоморфизм кольца K, индуцированный матрицей A. Понятно, что степени автоморфизма индуцированы соотвествующими степенями матрицы A, а значит, $|\sigma| = 5$. Для простоты будем рассмотривать централизатор $C'(\sigma)$ автоморфизма σ в группе $IntK$ внутренних автоморфизмов кольца K, и тогда $|C'(\sigma)| = 20$.

Для построения квазигруппового кольца возьмём, например, $K = M_2(Z_5)$ и $S = M \times M$. Так как $|K| = 625$, $|S| = 256$, то $|KS| = 625^{256} > 2^{2304}$. Заметим, что и автоморфизмов достаточно много:

$$|AutK| > |IntK| = |GL_2(Z_5)| = 480, |AutS| = 231211008,$$

а число автоморфизмов KS равно $|AutK| \cdot |AutS| = 11098128384$. Если брать в составе качестве S прямое произведение большего количества M и H, то получим большое число автоморфизмов при сравнительно небольшом размере структуры KS.

Некоторые модификации криптосистемы. Для повышения устойчивости к атакам описанную криптосистему можно модифицировать следующим образом, записывая исходный текст m для передачи, можно домножать его не только справа, но и слева на заданные автоморфизмами лупы и кольца элементы (аналогично сконструировав дополнительные автоморфизмы и домножив m). Зашифрованный текст будет иметь вид:

$$\chi'(\varphi'(a'))\psi'(\varphi'(x')) \cdot \Big[m \cdot \chi(\varphi(a)) \cdot \psi(\varphi(x))\Big]$$

Конечно, здесь предполагается, что у $\chi'(\varphi'(a')) \cdot \psi'(\varphi'(x'))$ есть нулевой правый аннулятор.

Эта модификация значительно ослабит возможности атаки с известным исходным текстом, так как зная сообщение m, злоумышленник не сможет накапливать образы автоморфизмов даже при $\varphi = \varphi'$. А использование несовпадающих автоморфизмов $\varphi \neq \varphi'$ позволяет еще более усложнить задачу злоумышленника во всех атаках.

Другая модификация заключается в следующем. Вместо одного элементов a и x можно использовать множество элементов: $\{a_1, \ldots, a_r\}$ и аналогично построить для них автоморфизмы $\chi_1, \ldots, \chi_r$.

Открытый ключ в этом случае будет выглядеть следующим образом:

$$\Big(\sigma, \eta, a_1, \ldots, a_r, \varphi(a_1), \ldots, \varphi(a_r)\Big).$$

Криптограмма для A в таком случае будет иметь вид:

$$\Big(\chi_1(a_1) \cdot \ldots \cdot \chi_r(a_r), m \cdot \Big[\chi_1\big(\varphi(a_1)\big) \cdot \ldots \cdot \chi_r\big(\varphi(a_r)\big)\Big]\Big).$$

В этой криптограмме в элементах $\chi_1\big(\varphi(a_1)\big)\cdot\ldots\cdot\chi_r\big(\varphi(a_r)\big)$ и $\chi_1(a_1)\cdot\ \ldots\cdot\ \chi_r(a_r)$ намеренно не расставлены скобки, так как порядок перемножения не важен. Главное, чтобы полученный элемент имел нулевой левый аннулятор. Тогда участник А сможет достаточно просто решить систему уравнений для нахождения обратного.

Данное условие позволяет значительно сузить класс автоморфизмов φ' удовлетворяющих не только начальным условиям

$$\varphi'(a_1) = \varphi(a_1), \ldots, \varphi'(a_r) = \varphi(a_r),$$

но и позволяющих правильно расшифровать сообщение из криптограммы.

Злоумышленнику также усложнится атака на сеансовые автоморфизмы, так как ему придется перебирать не только степени автоморфизмов, но и всевозможные порядки умножения элементов. Действительно, элементы $a_1, \ldots, a_r$ и автоморфизмы $\chi_1, \ldots, \chi_r$ выбраны независимо, поэтому, при атаке на сеансовые автоморфизмы злоумышленник сталкивается с задачей $\Omega_1^r(L(\langle\sigma\rangle, \langle\eta\rangle),$ $KL)$, к тому же он вынужден перепробовать всевозможную расстановку скобок. Это существенно усложняет атаку на сеансовые автоморфизмы. Определенная выше сложность атаки на сеансовый автоморфизм будет равна $t_3^{r+1}t_5^{r+1}\cdot\frac{r!(r+1)!}{(2r)!}$.

С другой стороны, в атаке только с криптограммой мы имеем задачу уже не $\Omega_2(L, KQ)$, а $\Omega_{r+1}(Q, KQ)$. Рассуждения приведенные выше дают возможность выбирать элементы (σ, η) из групп $AutK$ и $AutQ$ меньших порядков, но с большими централизаторами. Важную роль здесь играет параметр r. С его помощью можно сбалансировать криптосистему, делая одинаково сложными атаки на φ и $\psi, \chi_1, \ldots, \chi_r$.

3.2 Гомоморфность криптографической системы над квазигрупповым кольцом

Введем формальное определение гомоморфной системы шифрования из [32].

Гомоморфная система шифрования с открытым ключом E определяется четырьмя алгоритмами: $KeyGen, Encrypt, Decrypt$ и $Evaluate$. Алгоритм $KeyGen$ вырабатывает секретный sk и открытый pk ключи, при этом задается множество открытых M и шифртекстов C. Алгоритм $Encrypt$ принимает на вход открытый ключ pk и открытый текст m из M, на выходе алгоритм выдает шифртекст c из C. Алгоритм $Decrypt$ принимает на вход sk и c, на выходе алгоритм выдает открытый текст m. Алгоритм $Evaluate$ принимает на вход открытый ключ pk, функцию F из множества возможных функций $\mathcal{F}$ и набор шифртекстов $(c_1, c_2, \ldots, c_t)$, а на выходе выдает другой шифртекст c.

Определение 3.1 (**корректность шифрования**). *Система шифрования* $E = (KeyGen, Encrypt, Decrypt, Evaluate)$ *корректна для функций из множества* $\mathcal{F}$, *если для любой пары* (sk, pk), *любой функции* F *из* $\mathcal{F}$, *любых* t *открытых текстов* $m_1, m_2, \ldots, m_t$ *и соответсвующих им шифртекстов* $c_i = Encrypt_E(pk, m_i)$ *выполняется следующее равенство:*

$$Decrypt_E(sk, Evaluate_E(pk, F, (c_1, c_2, \ldots, c_t)) = F(m_1, m_2, \ldots, m_t).$$

Определение 3.2 (**компактность шифрования**). *Гомоморфная система шифрования* $E = (KeyGen, Encrypt, Decrypt, Evaluate)$ *компактна, если существует полиномиальная функция* g, *такая что размер выхода алгоритма* $Decrypt$ *не превосходит* g[*размер входа*].

Определение 3.3 (**полногомоморфное шифрование**). *Система шифрования* E *называется полногомоморфной, если она корректна и компакта для всех для функций из множества* $\mathcal{F}$.

Более простым языком гомоморфность системы означает выполнения условий

$$Decrypt(c_1 \cdot c_2) = m_1 \cdot m_2,$$
$$Decrypt(c_1 + c_2) = m_1 + m_2,$$

где c_1, c_2 – шифртексты соответствующих открытых текстов m_1, m_2, а операции $\cdot$ и $+$ – это операции в используемых алгебраических структурах.

В описанной выше схеме

$$Decrypt(c_1 \cdot c_2) = Decrypt(\psi_1(x_1) \cdot \psi_2(x_2), \big[m_1 \cdot \psi_1\big(\varphi(x_1)\big)\big] \cdot \big[m_2 \cdot \psi_2\big(\varphi(x_2)\big)\big]).$$

При расшифровании при помощи секретного автоморфизма φ можно получить: для операции умножения

$$\varphi\big(\psi_1(x_1) \cdot \psi_2(x_2)\big) = \psi_1\big(\varphi(x_1)\big) \cdot \psi_2\big(\varphi(x_2)\big) = h_1;$$

для операции сложения

$$\varphi\big(\psi_1(x_1) + \psi_2(x_2)\big) = \psi_1\big(\varphi(x_1)\big) + \psi_2\big(\varphi(x_2)\big) = h_2.$$

Таким образом, для того, чтобы схема обладала свойством гоморфной корректности шифрования по умножению необходимо получить значение $m_1 \cdot m_2$ из системы

$$\begin{cases} (m_1 \cdot x) \cdot (m_2 \cdot y) = r_1 \\ x \cdot y = h_1 \end{cases}$$

при известных r_1 и h_1.

Данная задача может быть разрешена, если в качестве квазигруппы Q в квазигрупповом кольце KQ использовать медиальные лупы.

Определение 3.4 (**медиальные квазигруппы**). *Квазигруппа* $(Q, \cdot)$ *называется медиальной, если выполняется следующее тождество:*

$$xy \cdot uv = xu \cdot yv.$$

В работах В.Д. Белоусова [2], Р. Брака[27], К. Тойоды [64] показано, что каждую медиальную квазигруппу $(Q, \cdot)$ можно представить как изотоп абелевой группы $(Q, +)$:

$$x \cdot y = \chi(x) + \nu(y) + a,$$

где χ, ν – автоморфизмы абелевой группы $(Q, +)$, такие что $\chi\nu = \nu\chi$ и a – некоторый фиксированный элемент множества Q. Более того, верно и обратное утверждение: для каждой абелевой группы $(Q, +)$, двух автоморфизмов χ, ν группы $(Q, +), \chi\nu = \nu\chi$, и a из Q существует медиальная квазигруппа $(Q, \cdot)$, причем $x \cdot y = \chi(x) + \nu(y) + a$.

Таким образом, можно строить различные примеры медиальных квазигрупп с заданными свойствами, используя изотопию абелевых групп.

В качестве рабочего примера алгебраической структуры для описанной выше схемы можно использовать кольцо Z_2Q, где в качестве Q выбрать следующую конструкцию: пусть $p > 2$ – простое число, $A, B \in F_p, q = p^k$, в качестве абелевой группы используется группа $(E, \oplus)$ точек эллиптичесой кривой $y^2 = x^3 + Ax + B$, в качестве автоморфизмов группы используются χ : $\chi((x, y)) = (x^p, y^p), \nu = 1_E$.

Еще более простым примером является следующая конструкция. Рассмотрим абелеву группу $(Z_p, \oplus)$ и построим медиальную квазигруппу $(Q, \cdot)$ с операцией $x \cdot y = x\alpha \oplus y\beta$, где α, β – это коммутативные автоморфизмы группы $(Z_p, \oplus)$. В качестве автоморфизмов можно выбрать $\alpha : z \to kz, \beta : z \to lz$, где k, l - целые числа.

Теорема 3.5. *Пусть* $(KQ, +, \cdot)$ *– квазигрупповое кольцо, где* Q *– медиальная квазигруппа и* K *– произвольное кольцо(необязательно ассоциативное). Тогда криптосхема является гомомофрной по операции умножения для кольца* KQ.

Доказательство: Корректность гомоморфного шифрования данной схемы отмечена выше. Пусть теперь функция F из алгоритма *Evaluate* осуществляет не одно умножение шифртекстов, а несколько. На примере трех умножений

покажем, что криптосхема удовлетворяет определению компактности шифрования.

Пусть даны шифртексты $c_1 = [\psi_1(x_1), m_1 \cdot \psi_1\big(\varphi(x_1)\big)], c_2 = [\psi_2(x_2), m_2 \cdot \psi_2\big(\varphi(x_2)\big)], c_3 = [\psi_3(x_3), m_1 \cdot \psi_3\big(\varphi(x_3)\big)]$ и функция $F(x, y, z) = x(yz)$. Тогда при расшифровании выполняется $Decrypt(F(c_1, c_2, c_3)) = F(m_1, m_2, m_3)$. Действительно, значение этой функции равно

$$F(c_1, c_2, c_3) = [\psi_1(x_1)\big(\psi_2(x_2)\psi_3(x_3)\big), m_1\psi_1(\varphi(x_1))\big(m_2\psi_2(\varphi(x_2)) \cdot m_3\psi_3(\varphi(x_3))\big)].$$

Используя медиальность квазигруппы, можно получить следующую цепочку равенств $m_1\psi_1(\varphi(x_1))\big(m_2\psi_2(\varphi(x_2))\cdot m_3\psi_3(\varphi(x_3))\big) = m_1\psi_1(\varphi(x_1))\big(m_2m_3\cdot\psi_2(\varphi(x_2))$ $\psi_3(\varphi(x_3))\big) = m_1(m_2m_3) \cdot \psi_1(\varphi(x_1))\big(\psi_2(\varphi(x_2))\psi_3(\varphi(x_3))\big)$. Используя тот факт, что φ – автоморфизм кольца, получим $m_1(m_2m_3) \cdot \psi_1(\varphi(x_1))\big(\psi_2(\varphi(x_2))$ $(\psi_3(\varphi(x_3))\big) = m_1(m_2m_3) \cdot \varphi[\psi_1(x_1)\big(\psi_2(x_2)\psi_3(x_3)\big)]$. Далее, при помощи секретного ключа φ можно определить значение $F(m_1, m_2, m_3) = m_1(m_2m_3)$.

Данные рассуждения легко распространяются на любое количество умножений. Таким образом, можно сделать вывод, что криптосистема гомоморфна по умножению относительно введенных определений, т.е.

$$Decrypt(sk, F(c_1, c_2, \ldots, c_n)) = F(Decrypt(sk, c_1), \ldots, Decrypt(sk, c_n)) =$$

$$= F(m_1, \ldots, m_n).$$

□

3.3 Схема Эль-Гамаля для квазигрупп с перестановочными степенями

Классическая схема Эль-Гамаля – это криптосистема с открытым ключом, предложенная Т. Эль-Гамалем в 1985г. [31]. Стойкость схемы основана на решении задачи дискретного логарифмирования в циклической группе: найти x из уравнения $g^x = h$, где g, h элементы циклической группы G, а x – натуральное число.

В работе С. Катышева, В. Т. Маркова, А.А. Нечаева [12] предлагается рассмотреть класс группоидов с перестановочными степенями для использования в системе выработки открытого ключа Диффи-Хеллмана.

Определение 3.6. *Для элемента g группоида $(G, \star)$ и заданных натуральных чисел r, l правой r-й и левой l-й степенями называются элементы $g^{[r]} = (\ldots((g \star g) \star g)\ldots)$ и ${}^{[l]}g = (\ldots(g \star (g \star g)\ldots)$. Элемент g называется элементом с перестановочными правыми степенями (ППС-элемент),*

если для любых натуральных чисел m, n : $g^{[m][n]} = g^{[n][m]}$. *Если это тождество выполняется для всех элементов* g *из* G, *то группоид* $(G, \star)$ *называется ППС-группоидом.*

Аналогично, с использованием тождества ${}^{[m][n]}g = {}^{[n][m]}g$, определяются элементы и группоиды с перестановочными левыми степенями (ПЛС).

Определение 3.7. *Группоид* $(G, \star)$ *называется группоидом с перестановочными степенями, если он является ППС- и ПЛС-группоидом.*

Стоит отметить, что рассматриваются группоиды с условием $g^{[m][n]} \neq g^{[mn]}$.

В этой же работе доказывается, что примером такого группоидом может служить медиальная квазигруппа. Докажем некоторые нужные нам свойства для медиальных квазигрупп.

Лемма 3.8. *Пусть* $(Q, \cdot)$ – *медиальная квазигруппа, построенная на основе абелевой группы* $(Q, +)$ *и коммутирующих автоморфизмов* $\sigma, \tau : x \cdot y = \sigma(x) + \tau(y)$. *Тогда ППС-элемента* q *из заданной квазигруппы обладает следующим свойством:*

$$(q^{[k]} \cdot q^{[l]})^{[n]} = q^{[k][n]} \cdot q^{[l][n]}.$$

Доказательство: Можно заметить, что для элемента q квазигруппы $(Q, \cdot)$ выполнено равенство: $q^{[k]} = \sigma^{k-1}(q) + \sigma^{k-2}\tau(q) + \ldots + \sigma\tau(q) + \tau(q)$. Используя это равенство, получим $(q^{[k]})^{[n]} = q^{[k][n]} = \sigma^{n-1}(q^{[k]}) + \sigma^{n-2}\tau(q^{[k]}) + \ldots + \sigma\tau(q^{[k]}) + \tau(q^{[k]})$. Далее, $q^{[k][n]} \cdot q^{[l][n]} = \sigma(q^{[k][n]}) + \tau(q^{[l][n]})$.

Расскрыв скобки, получим $q^{[k][n]} \cdot q^{[l][n]} = \sigma^n(q^{[k]}) + \sigma^{n-1}\tau(q^{[k]}) + \ldots + \sigma\tau(q^{[k]}) + \sigma^{n-1}\tau(q^{[l]}) + \sigma^{n-2}\tau^2(q^{[l]}) + \ldots + \tau^2(q^{[l]})$. С другой стороны, $(q^{[k]} \cdot q^{[l]})^{[n]} = (\sigma(q^{[k]}) + \tau(q^{[l]}))^{[n]} = \sigma^{n-1}(\sigma(q^{[k]}) + \tau(q^{[l]})) + \sigma^{n-2}\tau(\sigma(q^{[k]}) + \tau(q^{[l]})) + \ldots + \sigma\tau(\sigma(q^{[k]}) + \tau(q^{[l]})) + \tau((\sigma(q^{[k]}) + \tau(q^{[l]}))$. Расскрыв скобки и использовав коммутативность автоморфизмов , получим

$$(q^{[k]} \cdot q^{[l]})^{[n]} = \sigma^n(q^{[k]}) + \sigma^{n-1}\tau(q^{[l]}) + \sigma^{n-1}(q^{[k]}) + \sigma^{n-2}\tau^2(q^{[l]}) + \ldots + \sigma\tau(q^{[k]}) + \tau^2(q^{[l]}).$$

Заметим, что, переставляя слагаемые в абелевой группе $(Q, +)$, легко получается требуемое равенство.

□

Построим аналог криптосхемы Эль-Гамаля для медиальной квазигруппы.

1. Алгоритм генерация ключей ($Keygen$):

   Пусть $(Q, \cdot)$ – квазигруппа с перестановочными степенями, q – элемент квазигруппы, порождающий достаточно большую подквазигруппу. Участник А случайно выбирает натуральное число x и вычисляет $h = q^{[x]}$.

   Открытым ключом являются (Q, q, h), а секретным x.

2. Алгоритм шифрования ($Encrypt$):

   Для шифрования сообщения m (элемента квазигруппы Q) участник B выполняет следующие действия:

   - случайно выбирает натуральное число y и вычисляет $v_1 = q^{[y]}$,
   - вычисляет $s = h^{[y]} = q^{[x][y]}$ и $v_2 = m \cdot s = m \cdot q^{[x][y]}$.

   Шифртекстом является $(v_1, v_2) = (q^{[y]}, m \cdot s)$.

3. Алгоритм расшифрования ($Decrypt$):

   Для расшифрования шифртекста v_1, v_2 при помощи секретного ключа участник A выполняет следующие действия:

   - вычисляет $s = v_1^{[x]} = q^{[y][x]} = q^{[x][y]}$,
   - решает уравнение в квазигруппе $v_2 = m \cdot s$ относительно m при известных v_2 и s.

Классическая схема Эль-Гамаля является гомоморфной по операции умножения. Криптосхема для медиальных квазигрупп также будет гомоморфной по квазигрупповой операции.

Теорема 3.9. *Пусть $(Q, \cdot)$ – медиальная квазигруппа, тогда криптосистема Эль-Гамаля для квазигруппы Q является гомоморфной относительно квазигрупповой операции.*

Доказательство: Рассмотрим два шифртекста для сообщений m_1, m_2: $c_1 = Encrypt(h, m_1) = (q^{[y_1]}, m_1 \cdot h^{[y_1]})$ и $c_2 = Encrypt(h, m_2) = (q^{[y_2]}, m_2 \cdot h^{[y_2]})$. Покажем корректность шифрования для этих шифртекстов.

Итак, $Decrypt(x, c_1) \cdot Decrypt(x, c_2) = (q^{[y_1]}, m_1 \cdot h^{[y_1]}) \cdot (q^{[y_2]}, m_2 \cdot h^{[y_2]}) = (q^{[y_1]} \cdot q^{[y_2]}, (m_1 \cdot h^{[y_1]})(m_2 \cdot h^{[y_2]}))$. По условию медиальности квазигруппы выражение $(m_1 \cdot h^{[y_1]})(m_2 \cdot h^{[y_2]})$ можно преобразовать к виду $(m_1 \cdot m_2)(h^{[y_1]} \cdot h^{[y_2]})$. Теперь, для того, чтобы расшифровать, достаточно возвести в степень x значение $v_2' = q^{[y_1]} \cdot q^{[y_2]}$. Воспользовавшись доказанной леммой 3.8, получим $(q^{[y_1]} \cdot q^{[y_2]})^{[x]} = q^{[y_1][x]} \cdot q^{[y_2][x]} = q^{[x][y_1]} \cdot q^{[x][y_2]} = h^{[y_1]} \cdot h^{[y_2]} = s'$. В заключение, вычислим значение $m' = (m_1 \cdot m_2)$ из уравнения $v_2' = m' \cdot s'$. Таким образом, выполняется следующее соотношение:

$$Decrypt(x, c_1) \cdot Decrypt(x, c_2) = Decrypt(x, c_1 \cdot c_2).$$

Используя рассуждения для криптосистемы в первом параграфе , можно показать, что гомоморфность также не зависит от количества используемых

умножений. Таким образом,

$$Decrypt(sk, F(c_1, c_2, \ldots, c_n)) = F(Decrypt(sk, c_1), \ldots, Decrypt(sk, c_n)) =$$

$$= F(m_1, \ldots, m_n),$$

где $F \in \mathcal{F}$.

□

3.4 Построение MQ - криптосистемы над альтернативной алгеброй

В работах [58], [53], [36] были представлены криптосхемы, основанные на MQ-проблеме. Стойкость данных схем оценивается сложностью решения многопеременных квадратичных уравнений над конечным полем. Доказано, что данная проблема является NP-полной [53].

Опишем подобную криптосистему над альтернативной алгеброй A над полем F. Рассмотрим систему из m уравнений от n неизвестных над алгеброй A:

$$P = \begin{cases} y_1 = p_1(x_1, ..., x_n) \\ y_2 = p_2(x_1, ..., x_n) \\ \qquad\qquad ... \\ y_m = p_m(x_1, ..., x_n) \end{cases}$$

Многочлены $p_i, (i = 1, .., m)$ имеют вид $p_i(x_1, ..., x_n) = \sum \gamma_{ijk} x_j x_k + \sum \beta_{ij} x_j + \alpha_i$, где $i = 1, ..., m; \gamma_{ijk}, \beta_{ij}, \alpha_i \in F$;

Рассмотрим следующую схему преобразований векторов из алгебры A^n:

входящий $x = (x_1, ..., x_n)$

S ↓

x'

P' ↓

y'

T ↓

$y = (y_1, ..., y_n)$

многочлены $P = (p_1, ..., p_m)$

Секретным ключом данной схемы являются:

- отображения $S, T : A^n \to A^n$;

- система многочленов степени 2: $P' = (p'_1, ..., p'_m)$, где $p'_i = p'_i(x'_1, ..., x'_n)$.

Открытым ключом является система многочленов $(p_1, ..., p_m) = P = T \circ P' \circ S$

Шифрование\расшифрование

Для шифрования сообщения $x = (x_1, ..., x_n) \in A^n$ необходимо вычислить значения многочленов $p_i(x_1, ..., x_n), i = 1, ..., m$. Тогда зашифрованным сообщением является вектор $y = (y_1, ..., y_m) = (p_1(x_1, ..., x_n), ..., p_m(x_1, ..., x_n))$.

Для расшифрования сообщения $y \in A^n$ необходимо выполнить следующие действия:

1. Вычислить $y' = T^{-1}(y)$,
2. Решить систему уравнений и вычислить $x' = (P')^{-1}(y')$,
3. Вычислить $x = S^{-1}(x')$.

Таким образом, необходимым условием является достаточно быстрое решение системы уравнений в п.2. Рассмотрим один из возможных вариантов построения легко решаемой системы уравнений.

STS - схема В качетве обратимой системы уравнений второй степени P' можно использовать STS-схему (stepwise triangular systems). Общая структура STS-схемы имеет следующий вид:

$$\text{Шаг 1}: \begin{cases} p'_1(x'_1, ..., x'_r) \\ p'_2(x'_1, ..., x'_r) \\ \dots \\ p'_r(x'_1, ..., x'_r) \end{cases}$$

$$\dots$$

$$\text{Шаг l}: \begin{cases} p'_{(l-1)r+1}(x'_1, ..., x'_r, ..., x'_{(l-1)r+1}, ..., x'_{lr}) \\ \dots \\ p'_{lr}(x'_1, ..., x'_r, ..., x'_{(l-1)r+1}, ..., x'_{lr}) \end{cases}$$

$$\dots$$

$$\text{Шаг L}: \begin{cases} p'_{(L-1)r+1}(x'_1, ..., x'_r, ..., x'_{(l-1)r+1}, ..., x'_{lr}, ..., x'_{n-r+1}, ..., x'_n) \\ \dots \\ p'_{Lr}(x'_1, ..., x'_r, ..., x'_{(l-1)r+1}, ..., x'_{lr}, ..., x'_{n-r+1}, ..., x'_n) \end{cases}$$

Здесь на каждом из возможных L шагов происходит добавление r новых переменных. Для того, чтобы найти обратное преобразование на каждом шаге необходимо решить систему из r уравнений с r неизвестными:

$$\begin{cases} y'_{(l-1)r+1} = p'_{(l-1)r+1}(x'_1, ..., x'_{lr}) \\ \dots \\ y'_{lr} = p'_{lr}(x'_1, ..., x'_{lr}) \end{cases}$$

При достаточно малых значениях r данная система может быть решена однозначно.

Можно рассмотреть более общий вариант STS-схемы: пусть количество уранений на каждом шаге обозначется набором $r_1, ..., r_L$ таких натуральные числа, что $r_1 + ... + r_L = n$. Количество новых переменных на каждом шаге обозначается $m_1, ..., m_L$, причем $m_1 + ... + m_L = m$.

Пример Рассмотрим пример из работы [58]. В качестве альтернативной алгебры выберем алгебру Кэли-Диксона $C(\mu, \beta, \gamma)$ на полем $F_1 01$. Описание построения данной алгебры описанов работе [10]. Стоит отметить, что в алгебре $C(\mu, \beta, \gamma)$ можно выбрать базис $e_1, e_2, ..., e_7$ со следующей таблицей умножения:

	e_1	e_2	e_3	e_4	e_5	e_6	e_7
e_1	α	e_3	αe_2	e_5	αe_4	$-e_7$	$-\alpha e_5$
e_2	$-e_3$	β	$-\beta e_1$	e_6	e_7	βe_4	βe_5
e_3	$-\alpha e_2$	βe_1	$-\alpha\beta$	e_7	αe_6	$-\beta e_5$	$-\alpha\beta e_4$
e_4	$-e_5$	$-e_6$	$-e_7$	γ	$-\gamma e_1$	$-\gamma e_2$	$-\gamma e_3$
e_5	$-\alpha e_4$	$-e_7$	$-\alpha e_6$	γe_1	$-\alpha\gamma$	γe_3	$\alpha\gamma e_2$
e_6	e_7	$-\beta e_4$	βe_5	γe_2	$-\gamma e_3$	$-\beta\gamma$	$-\beta\gamma e_1$
e_7	αe_6	$-\beta e_5$	$\alpha\beta e_4$	γe_3	$-\alpha\gamma e_2$	$\beta\gamma e_1$	$\alpha\beta\gamma$

Рассмотрим следующую секретную систему уравнений:

$$\begin{cases} x'_1 = y'_1 \\ x'_1 x'_2 = y'_2 \\ (29x'_1 + 43x'_2)x'_3 + (71x'^2_1 + 53x'^2_2 + 89x'_1 x'_2) = y'_3 \end{cases}$$

Секретное линейное отображение S имеет следующий вид:

$$\begin{cases} x_1 = x'_1 + 25x'_2 + 73x'_3 \\ x_2 = x'_1 + 47x'_2 + 11x'_3 \\ x_3 = x'_1 + 83x'_2 + 17x'_3 \end{cases}$$

Секретное линейное отображение T имеет следующий вид:

$$\begin{cases} y_1 = y'_1 \\ y_2 = 39y'_2 + 82y'_3 \\ y_3 = 93y'_2 + 51y'_3 \end{cases}$$

Итоговой открытой системой уравнений является:

$$\begin{cases} x_1 + 25x_2 + 73x_3 = y_1 \\ 78x_1^2 + 37x_2^2 + 6x_3^2 + 54x_1x_2 + 19x_1x_3 + 11x_2x_3 = y_2 \\ 84x_1^2 + 71x_2^2 + 48x_3^2 + 44x_1x_2 + 33x_1x_3 + 83x_2x_3 = y_3 \end{cases}$$

Для шифрованая сообщения $x_1, x_2, x_3 \in C(\mu, \beta, \gamma)$ необходимо вычислить значения y_1, y_2, y_3. Данные вектор является шифр-текстом.

Замечание: Стоит отметить, что сложность решения системы линейных уравнений над алгеброй Кэли-Диксона не превосходит сложность данной проблемы над конечным полем. Однако некоторые атаки, использующщие особенности STS-схемы, не применимы к схеме над неассоциативной альтернативной алгеброй.

3.5 Криптосхемы на основе луп

3.5.1 Криптосхемы на основе луповых действий

Проблема дискретного логарифмирования

В данном разделе на основе протоколов Диффи-Хеллмана и Эль-Гамаля будет рассмотрена проблема дискретного логарифмирования с точки зрения луповых действий.

Классический протокол Диффи-Хеллмана в конечном поле основан на проблеме дискретного логарифмирования. Сложностью такой проблемы в конечном поле F_q является сложность задачи нахождения по известным b, n такого a, что $a^n = b$, где $a, b \in F_q, n \in \mathcal{N}$.

Рассмотрим подробнее аналог данного протокола на языке луповых действий. В качестве алгебраической структуры, в которой будут производиться вычисления, выберем лупу Муфанг.

Протокол выработки общего ключа Диффи-Хеллмана, построенный при помощи лупы L, имеет следующий вид.

Пусть $a, b \in L$ - общеизвестные элементы, такие что $ab \neq ba$. Пусть M и N порядки соответсвенно a и b. Сам протокол, выработки секретного ключа, выглядит следующим образом:

1. Абонент A выбирает случайные натуральные числа $m < M, n < N$ и посылает абоненту B сообщение $u = a^n b^m$.

2. Абонент B выбирает случайные натуральные числа $r < M, s < N$ и посылает сообщение $v = a^r b^s$.

3. Абонент A вычисляет $K_A = (a^n v)b^m$.

4. Абонент B вычисляет $K_B = (a^r u)b^s$.

Непосредственно из следствий теоремы Муфанг следует

$$(a^n(a^r b^s))b^m = a^n((a^r b^s)b^m) = (a^s(a^n b^m))b^s = a^r((a^n b^m)b^s) = a^{r+n}b^{s+m}.$$

Таким образом абонент A и абонент B имеют одинаковый секретный ключ $K = K_A = K_B$.

Рассмотрим какими свойствами должна обладать лупа L для достаточной сложности данного протокола.

Очевидно, что лупа L должна содержать элементы достаточно большого порядка.

Одной из самых известных атак на протокол Диффи-Хеллмана считается атака Похлига-Хелмана. Для успешного противостояния данной атаке, необходимо достаточно малое число классов эквивалентности в лупе, заданных по следующему правилу:

$$a \sim b = \{ac = bc, ca = cb \quad \forall c \in L\}$$

Отметим, что в лупе Муфанг такие классы эквивалентности являются нормальными подлупами. Таким образом, можно рассматривать простые лупы Муфанг для защиты от данной атаки.

Схема шифрования

Следующим примером реализации проблемы дискретного логарифмирования на языке луповых действий является протокол Эль-Гамаля.

Пусть $\alpha, \beta \in L$, тогда протокол Эль-Гамаля можно представить в виде следующего действия лупы Муфанг L:

$$\mathbf{N} \times L \to L \times L$$
$$(n, m) \to (\alpha^n, m\beta^n)$$

Данная схема предназначена для зашифрования информации $m \in L$. Открытым ключом является $(\alpha, \beta) \in L \times L$, а секретным ключом - $k \in \mathbf{N}$, причем $\beta = \alpha^k$.

Шифрование происходит по следующему алгоритму:

1. Выбирается секретный ключ $n \in \mathbf{N}$.

2. Вычисляются $a = \alpha^n$ и $b = m\beta^n$. Таким образом, пара (a, b) является криптограммой.

Расшифрование:

1. Вычисляется $(a^k)^{-1} = (\alpha^{kn})^{-1}$.

2. Вычисляется $b(a^k)^{-1} = (m\beta^n)(a^k)^{-1} = (m\alpha^{kn})(\alpha^{kn})^{-1} = m$

Стоит отметить, что в работе [46] проблема дискретного логарифмирования в конечной лупе Муфанг была сведена к аналогичной проблеме в конечном простом поле.

Проблема сопряжения

В данном разделе будет рассмотрен протокол Ко,Ли [40], основанный на проблеме сопряжения в CC-лупе.

Пусть L - произвольная лупа, рассмотрим множество левых трансляций $\{L_\alpha, \alpha \in L\}$. Напомним, что левой трансляцией называется отображение $L_\alpha : L \to L$, такое что $L_\alpha(x) = \alpha x, \quad \forall x \in L$. Свободная группа, порожденная всеми левыми трансляциями $\mathcal{L} =< L_{\alpha_1}, \ldots, L_{\alpha_n} >$, называется группой ассоциированной с лупой L. Отметим, что $L_\alpha L_\beta \neq L_\gamma$, для некоторого $\gamma \in L$, действительно, в общем случае $\beta(\alpha x) \neq (\beta\alpha)x, \quad \forall x \in L$.

Рассмотрим класс CC-луп:

Определение 3.10. *Лупа L называется CC-лупой, если*

$$L_x^{-1} L_y L_x = L_{(xy)/x}$$

для всех $x, y \in L$.

Для CC-луп определими обратное к L_α отображение $L_\alpha^{-1}(x) = \alpha\backslash x, \quad \forall x \in L$.

Отметим, что для таких луп ассоциированная группа $\mathcal{L}$ будет состоять из элементов вида: $L_{\alpha_1}^{a_1} L_{\alpha_2}^{a_2} \cdots L_{\alpha_n}^{a_n}$, где $a_i \in \{-1, 0, 1\}$.

Теорема 3.11. *Пусть L – CC-лупа, β является произведением $L_{\alpha_1} \cdot L_{\alpha_2} \cdots L_{\alpha_m}$ и $L_g \in \mathcal{L}$, тогда $\beta^{-1} L_g \beta = L_c$, для некоторого $c \in L$.*

Отметим, что β в этом случае можно рассматривать как некоторую перестановку множества элементов L, так как β нельзя представить в виде левой трансляциии.

Теперь определим действие:

$$Sym(L) \times \mathcal{L} \to \mathcal{L}$$
$$(\alpha, L_w) \to \alpha^{-1} L_w \alpha$$

На основе этого действия рассмотим алгоритм выработки общего секретного ключа:

Пусть L - CC-лупа, $\mathcal{L}_\alpha = \langle L_{a_1}, \ldots, L_{a_n} \rangle, \mathcal{L}_\beta = \langle L_{b_1}, \ldots, L_{b_m} \rangle$ общеизвестные подгруппы L. Эти подгруппы порождены такими левыми трансляциями, что $L_{a_i} L_{b_j} = L_{b_j} L_{a_i}$, для всех i, j. Пусть задана левая трансляция $L_w \in \mathcal{L}$.

Протокол:

1. Участник A выбирает α, являющийся произведением элементов $\mathcal{L}_\alpha$, и посылает участнику B: $\alpha^{-1} L_w \alpha$.

2. Участник B выбирает β, являющийся произведением элементов $\mathcal{L}_\beta$, и посылает участнику A: $\beta^{-1} L_w \beta$.

3. Общим ключом участников будет:

$$\alpha^{-1} \beta^{-1} L_w \beta \alpha.$$

Отметим, что α, β не являеются левыми трансляциями. Однако проблема сопряжения в данном протоколе легко сводится к аналогичной проблеме в свободной группе.

Построение криптосистемы на основе квазиавтоморфизмов

Пусть $(Q, \cdot)$ - квазигруппа и $T = (\alpha, \beta, \gamma)$ – автотопия этой квазигруппы.

Определение 3.12. *Главная компонента автотопии γ квазигруппы Q называется квазиавтоморфизмом, если существуют такие две другие подстановки α, β, что $\gamma(xy) = \alpha(x)\beta(y)$.*

Из определения автотопии и из того факта, что одноименные компоненты всех автотопий образуют группы, следует следующая лемма.

Лемма 3.13. *Все квазиавтоморфизмы квазигруппы $(Q, \cdot)$ образуют группу.*

Очевидно, что группа автоморфизмов является подгруппой это группы.

Лемма 3.14. *Любой квазиавтоморфизм γ группы Q имеет вид $\gamma = R_s\gamma_0$, где γ_0 - некоторый автоморфизм группы Q, s - некоторый элемент группы. Обратно, всякая перестановка γ группы Q, такая что $\gamma = R_s\gamma_0$, является квазиавтоморфизмом.*

Криптосхема

Рассмотрим аналог схемы Эль-Гамаля, в которой проблема дискретного логарифмирования рассматривается в группе квазиавтоморфизмов квазигруппы.

Пусть Q - квазигруппа.

Участник А:

1. Случайно выбирает квазиавтоморфизм $\phi : Q \to Q$.
2. Выбирает $n \in N$ и вычисляет ϕ^n.

Открытый ключ участника А:

$$(\phi, \phi^n);$$

Секретный ключ: n.

Участник В:

1. Формирует сообщение $m \in Q$.
2. Выбирает случайное $r \in N$ и вычисляет ϕ^r, ϕ^{nr}.

Криптограмма участника B:

$$\left(\phi^r, \phi^{nr}(m)\right)$$

Участник A:

1. Вычисляет ϕ^{nr}, зная ϕ^n, находит ϕ^{-nr}.

2. Вычисляет при помощи ϕ^{-nr} из криптограммы m.

3.5.2 Протокол выработки общего секретного ключа

Работа Диффи и Хеллмана [30] в 1975 году положила начало криптографии с открытым ключом. В данной работе предложен алгоритм выработки общего ключа, и этот алгоритм решал важную проблему криптографии того времени – распределение ключей.

В оригинале проткола использовалась мультипликативная группа G целых чисел по модулю p, где p является простым числом и g – порождающий элемент группы G.

1. Алиса выбирает случайное число a и посылает Бобу g^a.

2. Боб выбирает случайное число b и посылает g^b Алисе.

3. Алиса вычисляет $K_A = (g^b)^a = g^{ba}$.

4. Боб вычисляет $K_B = (g^a)^b = g^{ab}$.

Так как $ab = ba$, тогда Алиса и Боб имеют один и тот же элемент группы $K = K_A = K_B$, который называется общим ключом.

Отметим, что в протоколе Диффи-Хеллмана вычисления проходят в коммутативной группе. Следующим этапом развития данного протокола является работа Е. Стикела [62]. Алгебраической структурой в этом протоколе является некоммутативная конечная группа G. Пусть $a, b \in G, ab \neq ba$, протокол Стикела имеет следующий вид:

1. Алиса выбирает случайно два натуральных числа n, m и и посылает Бобу $u = a^n b^m$.

2. Боб выбирает случайно два натуральных числа r, s и и посылает Алисе $v = a^r b^s$.

3. Алиса вычисляет $K_A = a^n v b^m = a^{n+r} b^{m+s}$.

4. Боб вычисляет $K_B = a^r u b^s = a^{n+r} b^{m+s}$.

Дальнейшим развитием протокола Диффи-Хеллмана является переход к неассоциативным структурам.

Пусть L – общеизвестная лупа Муфанг, $a, b, c \in L$ – общеизвестные элементы.Пусть M, K и N – порядки соответственно a, b и c. Протокол выработки секретного ключа выглядит следующим образом:

1. Абонент А выбирает случайные натуральные числа $m < M, k < K, n < N$ и посылает абоненту В пару $(u_1, u_2) = (a^m b^k, b^k c^n)$.

2. Абонент В выбирает случайные натуральные числа $r < M, l < K, s < N$ и посылает сообщение $(v_1, v_2) = (a^r b^l, b^l c^s)$.

3. Абонент А вычисляет $(a^m v_1) b^k$ и $(b^k v_2) c^n$.

4. Абонент В вычисляет $(a^r u_1) b^l$ и $(b^l u_2) c^s$.

Общим ключом абонентов А и В является

$$K_{AB} = (a^{m+r} b^{k+l})(b^{k+l} c^{n+s}).$$

Непосредственно из следствий теоремы Муфанг получаем

Лемма 3.15. *Если L - лупа Муфанг, $a, b \in L$, то*

$$(a^n(a^r b^s))b^m = a^n((a^r b^s)b^m) = (a^s(a^n b^m))b^s = a^r((a^n b^m)b^s) = a^{r+n} b^{s+m}.$$

Таким образом, ключ абонента А: $K_A = ((a^m v_1) b^k)(b^k v_2) c^n) =$
$= (a^{m+r} b^{k+l})(b^{k+l} c^{n+s}) = K_{AB}$ и ключ абонента В: $K_B = ((a^r u_1) b^l)((b_l u_2) c^s) = K_{AB}$ совпадают.

Отметим, что элементы a, b, c лупы L являются общеизвестными, а натуральные числа r, k, s, m, l, n – секретными.

Замечание 3.16. *Знания одного из секретных чисел достаточно для получения секретного ключа. Действительно, пусть злоумышленник каким-либо образом получил число m, тогда, сделав следующие вычисления: $(a^{-m} u_1) = b^k$, $b^{-k} u_2 = c^n$, $\Big((a^m v_1) b^k\Big)\Big(b^k (v_2 c^n)\Big) = K$, злоумышленник получает секретный ключ K.*

Поэтому стойкость протокола не превышает сложности нахождения одного секретного ключа.

Замечание 3.17. *Злоумышленник для нахождения ключа может решить задачу дискретного логарифмирования в подгруппе* $< a, b > \subseteq L$ *или* $< b, c > \subseteq L$*, либо найти элемент лупы, который является общим ключом.*

В качестве примера для данной схемы рассмотрим класс луп Пейджа.

Определение 3.18. *Неассоциативная, конечная и простая лупа Муфанг* M *называется лупой Пейджа.*

Следующее описание луп Пейджа было представлено М.Зорном. Пусть $\mathbb{F}_q$ – конечное поле. Для $\alpha, \beta \in \mathbb{F}_q^3$ определим операции $\cdot, \times$ следующим образом:

$$\alpha \cdot \beta = \alpha_1\beta_1 + \alpha_2\beta_2 + \alpha_3\beta_3,$$
$$\alpha \times \beta = (\alpha_2\beta_3 - \alpha_3\beta_2, \alpha_3\beta_1 - \alpha_1\beta_3, \alpha_1\beta_2 - \alpha_2\beta_1).$$

Алгеброй Зорна $Z(q)$ называется множество (2×2)- матриц $\begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix}$, где $a, b \in F_q$ и $\alpha, \beta \in F_q^3$, со следующей операцией:

$$\begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix} \cdot \begin{pmatrix} c & \gamma \\ \delta & d \end{pmatrix} = \begin{pmatrix} ac + \alpha\delta & a\gamma + d\alpha - \beta \times \delta \\ c\beta + b\delta + \alpha \times \gamma & \beta \cdot \gamma + bd \end{pmatrix}$$

Все элементы $Z(q)$ с определителем $M = ab - \alpha\beta = 1$ образуют лупу Пейджа $M^*(q)$ с нейтральным элементом $e = \begin{pmatrix} 1 & (0,0,0) \\ (0,0,0) & 1 \end{pmatrix}$.

Л.Пейдж в [51] показал, что $|M^*(q)| = q^3(q^4 - 1)$, когда q четное и $|M^*(q)| = q^3(q^4 - 1)/2$, если q нечетное.

Пусть $SL_2(q)$ – специальная линейная группа (2×2)- матриц с определителем равным 1 над полем$\mathbb{F}_q$. Обозначим через $L_2(q)$ группу $SL_2(q)/Z(SL_2(q))$.

П.Войтеховски [65] доказал следующую теорему.

Теорема([65]) *Пусть* $S \subseteq Z$ *– множество порядков всех элементов лупы* $M^*(q)$ *и* T *– множество порядков элементов* $L_2(q)$*. Тогда* $S = T$ *и порядок элемента* $\begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix} \in M^*(q)$ *совпадает с порядком элемента* $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \in L_2(q)$ *при* $(\alpha, \beta) = (0, 0)$*, и совпадает с порядком элемента* $\begin{pmatrix} a & 1 \\ \alpha \cdot \beta & b \end{pmatrix}$ *из* $L_2(q)$ *при* $\alpha \neq 0$.

В качестве a, b, c можно выбрать элементы вида $\begin{pmatrix} \eta & e_1 \\ (0,0,0) & \eta^{-1} \end{pmatrix}$, $\begin{pmatrix} \theta & e_2 \\ (0,0,0) & \theta^{-1} \end{pmatrix}$, $\begin{pmatrix} \zeta & e_3 \\ (0,0,0) & \zeta^{-1} \end{pmatrix}$, где η, θ, ζ – примитивные элементы поля F_q. Порядки данных элементов равны $(q-1)/2$.

Использование неассоциативных структур находит свое оправдание в следующем примере. В работе [50] рассмотрена атака на протокол Стикела в группе обратимых $(k \times k)$ - матриц с использованием линейной алгебры. Атака сводится к решению системы уравнений:

$$\begin{cases} xa = ax \\ yb = by \\ u = xy \end{cases}$$

где a, b, u известные матрицы, а x, y – неизвестные $(k \times k)$ - матрицы над $\mathbb{F}_{2^l}$. Для того, чтобы получить линейную систему была использована обратимость искомых матриц. Обозначим за $x_1 = x^{-1}$ матрицу обратную к x. После некоторых преобразований система примет следующий вид:

$$\begin{cases} x_1 a = a x_1 \\ yb = by \\ x_1 u = y \end{cases}$$

Данная система имеет $3k^2$ линенйых уравнений и $2k^2$ неизвестных.

Дальнейшими преобразованиями можно упростить и получить систему:

$$\begin{cases} yu^{-1}a = ayu^{-1} \\ yb = by \end{cases}$$

в которой уже $2k^2$ уравнений и k^2 неизвестных.

Авторы работы [50] предлагают использовать необратимые матрицы над конечным кольцом для невозможности применения этой атаки.

Отметим, что в случае использвания предложенной схемы над неассоциативными структурами (например, над k-кольцами, в этом случае кольцо матриц также образует k-кольцо) даже потенциальная атака такого рода не является возможной.

3.5.3 Схема шифрования на основе покрытий лупы

Пусть L — конечная лупа и задана последовательность $\alpha = [A_1, \ldots, A_s]$, где $A_i \in L^r$ для некоторого натурального числа r, т. е. $A_i = (a_{i,1}, \ldots, a_{i,r})$, $a_{i,j} \in L$. Для каждого $i = 1, \ldots, s$ обозначим через A'_i элемент лупового кольца $\sum\limits_j a_{i,j} \in ZA$. Тогда $A'_1 \cdot \ldots \cdot A'_s = \sum a_l l$.

Определение 3.19. *Последовательность $\alpha = [A_1, \ldots, A_s]$ называется $[s, r]$-покрытием для L, если для элемента лупового кольца $\sum a_l l = A'_1 \cdot \ldots \cdot A'_s$ выполняются условия: $a_l > 0$ для всех $l \in L$ и $|A_i| = r$, $i = 1, \ldots, s$.*

Рассмотрим криптосхему, которая основана на $[s,r]$-покрытиях лупы Муфанг. Пусть L — конечная лупа Муфанг и $\alpha = (a_{i,j})$ — $[s,r]$-покрытие лупы L. В работе [44] показано, что сложность задачи разложения на множители $g = a_{1,j_1} \cdot a_{2,j_2} \cdot a_{3,j_3} \cdot \ldots \cdot a_{s,j_s}$ в конечной группе G эквивалентна сложности задачи дискретного логарифмирования в группе G. Тогда, в общем случае, задача разложения элемента лупы $l \in L$ на множители $l = (a_{1,j_1} \cdot (a_{2,j_2} \cdot (a_{3,j_3} \cdot \ldots \cdot a_{s,j_s})$ с неизвестной расстановкой скобок имеет не меньшую сложность, чем аналогичная задача в конечной группе.

Участник A:

1. Выбирает две лупы Муфанг L, M с достаточно большим количеством порождающих. Генерирует случайное $[s,r]$-покрытие $\alpha = (a_{i,j})$ для L.

2. Выбирает эпиморфизм $f : L \to M$, который он хранит в секрете, и вычисляет $\beta = (b_{i,j}) = f(\alpha) = f(a_{i,j})$. Заметим, что β является $[s,r]$-покрытием для лупы M.

   Открытым ключом является

   $$(\{\alpha\}, \{\beta\}).$$

Участник B:

1. Формирует сообщение $x \in M$.

2. Выбирает произвольное y_1 из покрытия α, причём расстановка скобок осуществляется произвольным способом. Таким образом, $y_1 = a_{1,j_1} \cdot (a_{2,j_2} \cdot (a_{3,j_3} \cdot \ldots \cdot a_{s,j_s})$.

3. Образует $y_2 \in \beta$ с аналогичной пункту 2 расстановкой скобок.

4. Формирует $y_3 = xy_2$.

5. Посылает участнику A криптограмму (y_1, y_3).

Участник A, получив пару (y_1, y_3), вычисляет $f(y_1) = y_2$ и $y_3 y_2^{-1}$. Так как M — лупа Муфанг, то $y_3 y_2^{-1} = (xy_2)y_2^{-1} = x$.

Замечание 3.20. *С практической точки зрения участнику A лучше заранее составить таблицу значений для эпиморфизма f.*

Замечание 3.21. *Конструкция легко может быть обобщена на произвольную квазигруппу, если умножение на y_2^{-1} справа в алгоритме расшифрования заменить на правое деление.*

Замечание 3.22. *Любое* $[s, r]$*-покрытие можно представить в виде матрицы* $\alpha = (a_{i,j})$*, где* $a_{i,j} \in L$*,* $1 \leq i \leq s$*,* $1 \leq j \leq r$*. Тогда, с практической точки зрения,* $[s, r]$*-покрытие удобно задавать случайной* $(s \times r)$*-матрицей с проверкой необходимых условий.*

Заключение

В диссертации рассмотрена теория коммутаторов и ассоциаторов квазигрупп и луп. Развита теория первичного радикала лупы, исследованы его свойства, доказано его совпадение с множеством строго энгелевых элементов лупы и с верхним радикалом этой лупы. Получено описание Ω-первичного радикала Ω-лупы, как множества Ω-строго энгелевых элементов. Установлены связи первичного радикала лупы обратимых элементов альтернативного кольца и первичного радикала кольца.

Построены криптографические схемы над различными неассоциативными структурами:

– аналог схемы шифрования Эль-Гамаля над ППС-квазигруппой;

– схема выработки общего секретного ключа над лупами Пейджа;

– схема шифрования с открытым ключом на основе покрытий лупы Муфанг.

Построена также схема шифрования с открытым ключом над луповым кольцом, проанализированы свойства данной схемы, доказана гомоморфность данной схемы относительно одной из операций.

Работа имеет как теоретический, так и прикладной характер. Полученные в ней результаты могут быть использованы в различных задачах теории луп. Построенные криптографические схемы могут быть использованы при построении различных систем безопасности.

Приложение

Ниже приведен исходный код в системе GAP [37]. Результатом выполнения являются параметры $t_1 - t_6$ для криптосистемы на основе автоморфизмов луповых колец. Данные параметры позволяют определить возможность применения выбранных алгебраических структур на практике.

```
AnalyzeSystem:=function(L,R)

 local A,AR, Gen, GenR,k,x,y,c,c0;

 if IsAssociative(L) then
    Print("L is associative !\n");
 fi;

 Print("Order of quasigroup: ", Size(L), "\n");

 A:=AutomorphismGroup(L);
 Print("Order of Automorphism Group of quasigroup(t_1):",Size(A),
 "\n");
 AR :=AutomorphismGroup(Units(R));
 Print("Order of Automorphism Group of ring(t_2):",Size(AR),"\n");

    Gen:=GeneratorsSmallest(A);
    GenR:=GeneratorsSmallest(AR);

Print("\n Generators of Automorphism Group of quasigroup:",Size(Gen),
"\n");
  k:=0;
  for x in Gen do
    k:=k+1;
    y := Order(x);
    c := Centralizer(A, x);
    c0 := Order(c);
    Print(" Order of element(t_3): ", y);
    Print("Centralizer's order(t_4): ", c0, "\n");
  od;

Print("\n Generators of Automorphism Group of ring: ",Size(GenR),
 "\n");
```

```
  k:=0;
  for x in GenR do
    k:=k+1;
    y := Order(x);
    c := Centralizer(AR, x);
    c0 := Order(c);
    Print(" Order of element(t_5): ", y);
    Print(" Centralizer's order(t_6): ", c0, "\n");
  od;

return 1;

end;
```

Благодарности

Автор выражает глубокую благодарность своему научному руководителю д.ф.-м.н., профессору механико-математического факультета МГУ Александру Васильевичу Михалёву за выбор темы исследования, постановки задач, внимательное руководство в процессе исследовательской деятельности и поддержку, а также доценту Виктору Тимофеевичу Маркову за многочисленные советы и обсуждения. Автор благодарен всему коллективу кафедры высшей алгебры за креативную атмосферу и внимание к работе. Автор приносит благодарность профессору Михаилу Михайловичу Глухову за ценные советы и помощь.

Список литературы

[1] Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии: учебное пособие. Москва: Гелиос АРВ, 2011

[2] Белоусов В.Д. Основы теории квазигрупп и луп. - Москва: Наука, 1967. - 223 с.

[3] Белявская Г.Б. Ассоциаторы, коммутаторы и линейность квазигрупп // Дискрет. матем. - 1995. - т.4. - N.7. - С.116–125.

[4] Бейдар К. И., Михалев А. В., Слинько А. М. Критерии первичности для невырожденных альтернативных и йордановых алгебр // Тр. ММО. 1987. Vol. 50. P. 130–137.

[5] Глухов М.М. T-разбиения квазигрупп и групп // Дискрет. матем. - 1992. - т.4. - N.3. - С.47–56.

[6] Глухов М.М. О применениях квазигрупп в криптографии // Прикладная дискретная математика. - 2008. - N.2.

[7] Глухов М.М., Круглов И.А., Пичкур А.Б., Черемушкин А.В. Введение в теоретико-числовые методы криптографии: учебное пособие. Санкт-Петербург: Лань, 2011.

[8] Голубков А.Ю. Первичный радикал групп над ассоциативными кольцами: дис. канд. физ.-мат. наук - М: 2000.

[9] Голубков А.Ю. Радикал RN и слабо разрешимый радикал линейных групп над ассоциативными кольцами // Фундаментальная и прикладная математика. - 2007. - т.13. - N.2. - С.31–115.

[10] Жевлаков К.А., Слинько А.М., Шестаков И.П.,Ширшов А.И. Кольца, близкие к ассоциативным. - Москва: Наука, Главная редакция физико-математической литературы, 1978.

[11] Зельманов Е. И. Первичные альтернативные супералгебры и нильпотентность радикала свободной альтернативной алгебры // Изв. АН СССР. Сер. матем. 1990. Vol. 54, no. 4. P. 676–693.

[12] Катышев С.Ю., Марков В.Т., Нечаев А.А. Использование неассоциативных группоидов для реализации процедуры открытого распределения ключей // Дискрет. матем.- 2014. - т.26. - N.3. - С.45–64.

[13] Курош А.Г. Радикалы колец и алгебр // Матем. сборн. -1953. - т.33. - N.1. - С.13-26.

[14] Курош А.Г. Радикалы в теории групп// ДАН СССР. - 1961. - т.141. - N.4. - С.789-791.

[15] Курош А.Г., Черников С. Н. Разрешимые и нилъпотентные группы // Успехи Мат. Наук. - 1947. - т.2ю - N.3. - С.18-59.

[16] Курош А.Г. Лекции по общей алгебре. Москва:Наука. - 1973.

[17] Михалев А.В., Шаталова М.А. Первичный радикал Ω-групп и Ω-l-групп // Фундаментальная и прикладная математика. - 1998. - т.4. - N.4. - С.1405–1413.

[18] Михалев А.В., Балаба И.Н., Пихтильков С.А. Первичный радикал градуированной Ω-группы // Фундаментальная и прикладная математика. - 2006. - т.12. - N.2. - С.159–174.

[19] Пчелинцев С.В. Первичные альтернативные алгебры // Фундаментальная и прикладная математика. - 1998. - т.4. - N.2. - С.651–657.

[20] Романьков В.А. Криптографический анализ некоторых схем шифрования, использующий автоморфизмы // Мат.методы криптографии. - 2013. - т.3. - N.21. - С.35–51.

[21] Росошек С.К. Криптосистемы групповых колец // Вестник Томского государственного университета. - 2003. - N.6. - С.57-62.

[22] Скорняков Л. А. Право-альтернативные тела // Изв. АН СССР. Сер. матем.. 1951. Vol. 15, no. 2. P. 177–184.

[23] Табаров А.Х. Тождества и линейность квазигрупп: дис. д-ра физ.-мат. наук - М:2009.

[24] Щукин К.К. RI*-разрешимый радикал групп // Матем. сб., Новая серия. - 1960. т.52. - N.4. - С. 1021-1031.

[25] Albert A. Quasigroups I // Trans. Amer. Math. Soc - 1943. - v.54. - P. 507-519.

[26] Amitsur S.A. A general theory of radicals, II. Radicals in rings and bicategories // SAmer. J. Math. - 1954. - v.76. - N.1. - P. 197-125.

[27] Bruck R.H. A survey of binary systems. Berlin: Springer-Verlag, 1958.

[28] Buys A., Gerber G.K. The prime radical for Ω-groups // Commun. Algebra. - 1982. - v.10. - P.1089–1099.

[29] Denes J., Keedwell A.D. Latin squares and their applications. Budapest: Academiai Kiade, 1974.

[30] Diffie W., Hellman M.E. New directions in cryptography // IEEE Transactions on Information Theory. - 1976. - v.22. - P.644-654.

[31] ElGamal T. A public key cryptosystem and a signature scheme based on discrete logarithms // IEEE Transactions on Information Theory. - 1985. - v.31. - P.469-472.

[32] Gentry C. A fully homomorphic encryption scheme: Ph.D. thesis. - Stanford University. - 2009.

[33] van Dijk M., Gentry C., Halevi S., Vaikuntanathan V. Fully homomorphic encryption over the integers // Proceedings of Advances in Cryptology, EUROCRYPT'10. 2010. P. 24–43.

[34] Goodaire E.G. A brief history of loop rings // 15th School of Algebra. Mat. Contemp. - 1999. - v.16. - P. 93–109.

[35] Goodaire E. G., Jespers E., Polcino Milies C. Alternative loop rings // North-Holland Math. Studies. - 1996. - v.184.

[36] Goubin L., Courtois N. Cryptanalysis of the TTM cryptosystem // In Advances in Cryptology — ASIACRYPT. - 2000. - v.1976.

[37] The GAP Group. GAP - Groups, Algorithms and Programming. Version 4.6.4 [Электронный ресурс]. - 2013. - The GAP Group. - http://www.gapsystem.org.

[38] Higgins P. J. Groups with multiple operators // Proc. London Math. Soc. - 1956. -v.3. - N.6. - P.366–416.

[39] Kalla A. Non-associative public-key cryptography [Электронный ресурс]. - 2012. - http://arxiv.org/abs/1210.82703.

[40] Ko K.H., Lee S.J., Cheon J.H., Han J.W., Kang J., Park C. New public-key cryptosystem using braid groups // Advances in Cryptology – CRYPTO. - 2000. - v.1880. - P.166–183.

[41] Koscielny C., Mullen G.L. A quasigroup-based public-key cryptosystem // Int. J. Appl. Math. Comp. Sci. - 1999. - V. 9. - No. 4. - P.955-963.

[42] Landrock P., Manz O. Classical codes as ideals // Group Algebras, Designs, Codes and Cryptography. - 1992. - v.2. - P.273-285.

[43] Levitski J. Prime ideals and the lower radical // Amer. J. Math. - 1951. - v.73. - P.25–29.

[44] Magliveras S. S., Tran van Trung. New approaches to designing public key cryptosystems using one-way functions and trap-doors in finite groups // J. Cryptology. - 2002. - N.15. - P.285–297.

[45] Magyarik M. R., Wagner N.R. A public key cryptosystem based on the word problem // Advances in Cryptology – CRYPTO. - 1985. - v.196. - P.19–36.

[46] Maze G. Algebraic methods for constructing one-way trapdoor functions: Ph.d. thesis. - University of Notre Dame. - 2003.

[47] McCoy N., Brown B. Some theorems on groups with applications to ring theory //Trans. Amer. Math. Soc. - 1950. -v.69. - P.302–311.

[48] McKenzie R., Snow J. Congruence modular varieties commutator theory and its uses // Structural theory of automata, semigroups and universal algebras. - 2005. - v.207. - P.273–329.

[49] Moufang R. Zur struktur von alternativkorpern// Math. Ann. - 1935. - v.110. - P.416–430.

[50] Myasnikov A., Shpilrain V., Ushakov A. Group-based cryptography. Berlin:Birkhauser Basel, 2008.

[51] Paige L.J. A class of simple Moufang loops // Proc.Math.Soc. -1956.

[52] Passman D.S. The algebraic structure of group rings. New York: Wiley, Interscience, 1977.

[53] Patarin J., Goubin L. Trapdoor one-way permutations and multivariate polynomials // In International Conference on Information Security and Cryptology. - 1997. - v. 1334.

[54] Pflugfelder H.O. Quasigroups and loops: introduction // Sigma Series in Pure Math. - 1990. - v.8.

[55] Rich M. Some radical properties of s-rings // Proceedings of the american mathematical society. - 1971. - v. 30.

[56] Rich M. The prime radical in alternative rings // Proceedings of the american mathematical society. - 1976. - v. 56.

[57] Rivest R.L., Shamir A., Adleman L. A method for obtaining digital signatures and public key cryptosystems // Communications of the ACM. - 1978. - v.21. - P.120-126.

[58] Shamir A. Efficient signature schemes based on birational permutations // Advances in Cryptology — CRYPTO. - 1993. - v. 773.

[59] Shcherbacov V.A. Quasigroups in cryptology // Comput. Sci. J. Moldova. - 2009. - v.17. - N.2. - P.193-228.

[60] Smith J.D.H. An Introduction to quasigroups and their representations, Chapman&Hall/CRC,2007.

[61] Smith J.D.H. On the nilpotence class of commutative Moufang loops // Math. Proc. Cambridge Philos. Soc. -1978. - V. 84. - N. 3. - P.387-404

[62] Stickel E. A new method for exchanging secret keys // Proceedings of theThird International Conference on Information Technology and Applications. - 2005. -v.2. - P.426–430.

[63] Tsai C. The prime radical in a Jordan ring // Proc. Amer. Math. Soc. - 1968. - v.19. - P.1171–1175.

[64] Toyoda K. On axsioms of linear functions // Proc. Imp. Acad.Tokyo. - 1941. - v.17. - P.221-227.

[65] Vojtechovsky P. Finite simple Moufang loops // Iowa State University, 2001.

[66] Vojtechovsky P., Stanovsky D. Commutator theory for loops // Journal of Algebra. - 2014. - v.399. - P.290–322

[67] Wolf C. Introduction to multivariate quadratic public key systems and their applications // France. - 2006.

Публикации автора по теме диссертации

[68] Грибов А. В., Золотых П. А., Михалёв А. В., Построение алгебраической криптосистемы над квазигрупповым кольцом // Математические вопросы криптографии. - 2010. - т.1. - N.4. - С.23-33.

[69] Грибов А. В., Золотых П. А., Марков В.Т., Михалёв А. В., Скаженик С. С., Квазигруппы и кольца в кодировании и построении криптосхем // Прикладная дискретная математика. - 2012. - N.4. - С.31–52.

[70] Грибов А. В., Михалёв А. В., Первичный радикал для луп и Ω-луп: I. // Фундамент. и прикл. мат. - 2014. - т.19. - N.2. - С.25-42.

[71] Грибов А. В., Первичный радикал для альтернативных колец и луп. Фундамент. и прикл. мат. - 2015. - т.20. - N.1. - С.141-162.

[72] Грибов А. В., Гомоморфность некоторых криптографических систем на основе неассоциативных структур // Фундамент. и прикл. мат. - 2015. - т.20. - N.1. - С.131-139.