«УТВЕРЖДАЮ»

Проректор
по научно-исследовательской работе
ФГБОУ ВПО «ТГПУ им. Л.Н. Толстого»
кандидат политических наук, доцент
Подрезов К.А.

«__» _____ 2015 г.

ОТЗЫВ ВЕДУЩЕЙ ОРГАНИЗАЦИИ
федерального государственного бюджетного образовательного учреждения высшего профессионального образования
«Тульский государственный педагогический университет им. Л. Н. Толстого»
на диссертационную работу Грибова Алексея Викторовича
«Алгебраические неассоциативные структуры и их приложения в криптографии»,
представленную
на соискание учёной степени кандидата физико-математических наук
по специальности 01.01.06 – математическая логика, алгебра и теория чисел

Диссертация А.В. Грибова выполнена **на актуальную тему**, она относится к теории неассоциативных алгебраических структур и посвящена исследованию первичного радикала луп и луповых колец, построению криптографических схем над различными неассоциативными структурами.

При изучении алгебраических систем одной из основных задач является описание рассматриваемых алгебраических систем, т.е. построения соответствующей структурной теории. Структурные теоремы сводят изучение рассматриваемых алгебраических систем к изучению более простых. Одной из основных конструкций, позволяющей осуществлять это сведение, является радикал. Первичный радикал исследовался для различных алгебраических систем: Бэром и Маккоем для колец, К.К. Щукиным для групп, А.В. Михалёвым и М.А. Шаталовой для Ω-групп, М. Ричем для неассоциативных s-колец. В представленной диссертации развита теория первичного радикала для ряда неассоциативных алгебраических структур: луп, Ω-луп и луповых колец.

Диссертация А.В. Грибова состоит из введения, трех глав, списка цитированной литературы, включающего 72 наименования, и приложения. Общий ее объём составляет 93 страницы.

Во введении дан краткий исторический обзор и изложены основные результаты диссертации.

Первая глава посвящена построению теории первичного радикала для луп и Ω-луп. В первом параграфе содержатся основные определения, понятия и факты, необходимые для дальнейшего изложения. Далее рассматриваются понятия коммутатора, ассоциатора и взаимного коммутанта нормальных подлуп, приводятся порождающие множества коммутанта нормальных подлуп (следствие 1.49). В следующих двух параграфах первой главы вводятся понятия первичного радикала лупы и Ω-лупы соответственно. Установлено, что первичный радикал лупы совпадает с множеством всех ее строго энгелевых элементов (теорема 1.61), а первичный радикал Ω-лупы совпадает с множеством всех ее Ω-строго энгелевых элементов (следствие 1.74).

Вторая глава связана с исследованием первичного радикала луповых колец. Здесь приведены классические результаты, касающиеся альтернативных колец, рассмотрены свойства первичных альтернативных колец, установлено, что множество обратимых элементов альтернативного кольца с единицей является лупой Муфанг (теорема 2.13). Получен критерий, при котором луповое кольцо является альтернативным (теорема 2.21). Установлена связь между первичным радикалом альтернативного лупового кольца и первичным радикалом подлупы лупы его обратимых элементов (теорема 2.38). В частности, доказано, что первичный радикал лупы обратимых матриц кольца матриц Цорна равен центру кольца матриц Цорна по его первичному идеалу (теорема 2.40). Данная теорема является неассоциативным аналогом хорошо известной теоремы А.В. Михалёва и И.З. Голубчика, устанавливающей связи между первичным радикалом кольца с единицей и первичным радикалом подгруппы группы его обратимых элементов для случая линейной группы над ассоциативным кольцом.

Третья глава диссертационной работы посвящена криптографическим схемам над неассоциативными структурами. Возможности применения квазигрупп в криптографии исследовались в работах М.М. Глухова, С. Косельны и Мюллена, В.А. Щербакова и др., а В.Т. Марков и А.А.Нечаев в криптографии с открытым ключом использовали неассоциативный группоид. В диссертации А.В. Грибова построены примеры криптографических схем с открытым ключом над различными неассоциативными структурами: ППС-квазигруппами, лупами Пейджа и луповыми кольцами. Построенная в работе схема шифрования над луповым кольцом основана на подходе С.К. Росошека для групповых колец. Установлено, что для медиальной квазигруппы данная криптосистема является гомоморфной по отношению к операции умножения (теорема 3.5). Построен аналог криптосистемы Эль-Гамаля над ППС-квазигруппой, доказана ее гомоморфность относительно квазигрупповой операции для медиальных квазигрупп (теорема 3.9). Построена MQ-криптосистема над альтернативной алгеброй над полем. Отметим, что выбор альтернативной алгебры позволяет избежать некоторых атак, использующих особенности STS-схемы. В заключительном параграфе третьей главы исследуются схемы 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 криптосистемы на луповом кольце, позволяющая определить возможность применения их на практике.

В диссертации применяется методы классической теории ассоциативных и ассоциативных колец, теории квазигрупп, а также криптографическими методами.

Существенных замечаний по работе нет. Отметим некоторые недостатки работы, не носящие принципиального характера. Для удобства чтения нумерацию определений, лемм и теорем нужно было разделить, а в автореферате перед формулировкой теоремы 2.38 привести определение центра кольца по идеалу. Имеются опечатки. Например, на стр. 22 несколько раз упоминается теорема 2.38 вместо теоремы 1.45.

Резюмируя вышеизложенное, можно заключить, что диссертация Грибова Алексея Викторовича является научно-квалификационной работой в области неассоциативной алгебры, в которой на основании выполненных автором исследований разработаны теоретические положения, являющиеся существенным научным достижением в теории луп и луповых колец и ее приложений. Работа имеет как теоретический, так и прикладной характер. Построенные автором криптографические схемы могут быть использованы в различных системах безопасности.

Все результаты являются новыми и снабжены строгими математическими доказательствами. Основное содержание диссертации опубликовано в открытой печати в пяти

публикациях автора, две из которых в журналах из Перечня ВАК РФ, а остальные – в журналах, номера которых и их переводные версии входят в международные реферативные базы данных и системы цитирования Scopus, MathSciNet и zbMATH.

Автореферат правильно и полно отражает содержание диссертации.

Результаты диссертации могут быть использованы при решении различных задач в теории луп и криптографии. Они могут быть полезны специалистам, работающим в МГУ им. М.В. Ломоносова, ТГПУ им. Л.Н. Толстого, МГТУ им. Н.Э. Баумана, ВЦ РАН, и в других научных центрах России и зарубежом.

Тематика и содержание диссертации Грибова А. В. отвечает паспорту специальности 01.01.06 – математическая логика, алгебра и теория чисел по формуле специальности и области исследования.

Диссертационная работа Грибова Алексея Викторовича «Алгебраические неассоциативные структуры и их приложения в криптографии», представленная на соискание учёной степени кандидата физико-математических наук по специальности 01.01.06 (математическая логика, алгебра и теория чисел), соответствует требованиям п. 9 «Положения о порядке присуждения ученых степеней» ВАК РФ к кандидатским диссертациям, а автор диссертации – Алексей Викторович Грибов – заслуживает присуждения ему ученой степени кандидата физико-математических наук.

Отзыв подготовлен доктором физико-математических наук, доцентом Балабой Ириной Николаевной.

Диссертация и отзыв обсуждены на кафедре алгебры, математического анализа и геометрии.

Отзыв утвержден на заседании кафедры алгебры, математического анализа и геометрии федерального государственного бюджетного образовательного учреждения высшего профессионального образования «Тульский государственный педагогический университет им. Л.Н. Толстого» «27» августа 2015года, протокол № 1 (голосование единогласно).

Зав. кафедрой алгебры, математического
анализа и геометрии,
доктор физико-математических наук,
профессор Н.М. Добровольский

Профессор кафедры алгебры,
математического анализа и геометрии,
доктор физико-математических наук,
доцент И.Н. Балаба

Подпись Н.М. Добровольского И.Н. Балабы
заверяю. Начальник отдела
делопроизводства и связи

Контактные данные:
ФГБОУ ВПО "ТГПУ им. Л.Н. Толстого", 300026, г. Тула, пр. Ленина, дом 125
Телефон: (4872) 33-36-46
e-mail: tgpu@tula.net
web-сайт: http://www.tsput.ru