ОТЗЫВ НАУЧНОГО РУКОВОДИТЕЛЯ

на диссертацию
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 Алексея Викторовича Грибова является научно-исследовательской работой, посвященной решению актуальных задач в области теории неассоциативных структур, а именно в теории радикалов луп, Ω-луп и луп обратимых элементов альтернативных колец. Полученные результаты использованы для построения криптографических схем.

Понятие радикала в теории групп было предложено А.Г. Курошем в 1960-х годах. Тогда же А.Г. Курош обратил внимание на аналогию между разрешимыми нормальными подгруппами и нильпотентными идеалами, позволившую К.К. Щукину построить теорию первичного радикала групп. Описание первичного радикала группы как множества строго эпигелевых элементов крайне близка к первичному радикалу в теории ассоциативных колец и алгебр. А.В. Михалёвым и И.З. Голубчиком установили связь между первичным радикалом кольца с единицей и первичным радикалом подгрупп группы его обратимых элементов для случая линейной группы над ассоциативным кольцом. В дальнейшем теория первичного радикала алгебраических систем активно развивалась в работах А.Ю. Голубкова (2000 г.), А.В. Михалева, И.Н. Балабы и С.А. Пихтилькова (2006 г.).

При исследовании структурной теории радикалов неассоциативных структур автором было введено понятие первичного радикала лупы. Показана согласованность введенного определения с понятием первичного радикала группы. Используя технику работы с коммутаторами в лупах, было доказано совпадение первичного радикала и множества строго эпигелевых элементов лупы. Получено описание первичного радикала Ω-лупы. Также автором доказан неассоциативный аналог теоремы А.В. Михалёва и И.З. Голубчика для лупы обратимых элементов альтернативного кольца $GLL(2, R)$ кольца матриц Цорна $\mathcal{Z}(R)$.

Квазигруппы имеют достаточно широкое применение в криптографии. Большое количество примеров использования квазигрупп для симметрической криптографии было приведено М.М. Глуховым (2008). С. Коселлы и Г. Мюллен (1999 г.) одними из первых использовали квазигруппы в теории криптографии с открытым ключом в конечнопорожденных и коммутативных группах. Автором были построены некоторые примеры криптографических схем с открытым ключом, где в качестве алгебраической основы использовались неассоциативные луповые кольца, ИПС-квазигруппы и лупы Пейджа.

Основные результаты диссертации состоят в следующем:

(1) Построен первичный радикал лупы, исследованы его свойства, доказано его совпадение с множеством строго энгелевых элементов лупы.
(2) Описано строение 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) Построена схема шифрования с открытым ключом над луповым кольцом, проанализированы свойства данной схемы, доказана гомоморфность данной схемы относительно одной из операций.

Результаты, полученные в диссертации А. В. Грибова, представляют несомненный интерес для неассоциативной алгебраической теории и криптографии. При работе над диссертацией автор продемонстрировал владение методами теории неассоциативных колец, теории квазигрупп и криптографии с открытым ключом.

Все результаты диссертационной работы А. В. Грибова являются новыми и докладывались на научно-исследовательских семинарах, российских и международных конференциях. Основное содержание работы опубликовано в виде статей в ведущих научных журналах. Автореферат полно и правильно отражает содержание диссертации.

Диссертация Грибова Алексея Викторовича удовлетворяет всем требованиям «Положения о порядке присуждения ученых степеней» ВАК РФ, а ее автор заслуживает присуждения ему степени кандидата физико-математических наук по специальности 01.01.06 — математическая логика, алгебра и теория чисел.

Доктор физико-математических наук,
профессор кафедры высшей алгебры
механико-математического факультета МГУ
Михалев Александр Васильевич

Подпись проф. Михалева А. В.
удостоверяю
и.о. декана механико-математического факультета МГУ
д.ф.-м.н., профессор
Чубариков Владимир Николаевич

02.03.15г.