ОТЗЫВ

официального оппонента о диссертации Грибова Алексея Викторовича
«Алгебраические неассоциативные структуры и их приложения к криптографии»,
представленной на соискание учёной степени
кандидата физико-математических наук по специальности
01.01.06 – математическая логика, алгебра и теория чисел

Представленная диссертационная работа посвящена решению двух основных задач, первая из которых состоит построении конструкции (точнее конструкций) первичного радикала луп и исследовании базовых соотношений между ним и первичным радикалом лупового кольца, а вторая — в построении и исследовании устойчивости различных криптографических схем, сконструированных с использованием квазигрупповых колец.

Использование в структурной теории алгебр первичного радикала во многом обусловлено тем, что это отображение, которое не является в общем случае полноценным радикалом с аксиоматической точки зрения и определяет радикал в смысле Куроша—Амицура лишь на некоторых, но, правда, весьма важных классах алгебр (к примеру, на классах альтернативных алгебр и обобщённо специальных алгебр Ли), имеет, тем не менее, естественную поэлементную характеризацию, наличие которой в описании радикальных отображений является скорее приятным исключением, нежели правилом. При этом выполнение для первичного радикала условий определения радикала в смысле Куроша—Амицура на некотором замкнутом относительно взятия идеалов и гомоморфных образов классе алгебр равносильно его совпадению на данном классе с нижним ниль-радикалом, не имеющим приемлемого конструктивного поэлементного описания (он описывается на уровне своего радикального класса с использованием цепи Куроша). Отметим и то, что в теории альтернативных, левоальтернативных (правоальтернативных) и йордановых алгебр первичный радикал подменяет собой в какой-то мере радикал Маккриммона (или Слинько — Маккриммона), который также может рассматриваться в качестве варианта конструкции первичного радикала по причине общности его поэлементного описания с описанием первичного радикала ассоциативных алгебр. В теорию групп конструкция первичного радикала была введена К.К.Щукиным и позднее нашла своё применение в полученном И.З.Голубчиком и А.В.Михалёвым описании первичного радикала линейной группы над ассоциативным кольцом, являющейся составной частью задачи описания структуры нормальных подгрупп классических линейных групп над кольцами. Позднее сходные резуль-

таты были получены А.Ю.Голубковым для унитарных групп над кольцами с инволюцией, групп Шевалле над коммутативными кольцами и подгрупп линейной группы над ассоциативными алгебрами нормализуемых элементарными группами, построенных на базе определения элементарных групп Шевалле, причём, как оказалось, применительно к данным группам первичный радикал является ещё и необходимым инструментом для получения описания их нижнего ниль-радикала и слабо разрешимого радикала. Выводы представленной работы, связанные с понятием первичного радикала, являются первым шагом в направлении переноса перечисленного здесь круга результатов на неассоциативную ситуацию и в первую очередь на лупы Муфанг. Говоря о безусловной перспективности исследований такого рода, будет уместно кратко упомянуть хотя бы некоторые из возможных направлений их ближайшего развития:

1. получение аналогов теорем Х.Цассенхауза об ограниченности ступеней разрешимости и индексов нильпотентности подгрупп полной линейной группы параметрами, определяемыми размерностью матриц, для подлуп луп обратимых элементов алгебр Кэли-Диксона;

2. получение для луп Муфанг соответствующего вида аналогов теоремы А.И.Мальцева о представлении конечно порождённых подгрупп линейной группы над полем в виде предела конечных подгрупп линейных групп той же размерности над полями положительной характеристики;

3. получение на основе этих аналогов теоремы о совпадении первичного и слабо разрешимого радикалов подлуп луп Муфанг альтернативных PI-алгебр с единицей с разрешимым расширением ограниченной ступени разрешимости их пересечений с «конгруэнц-подлупой» уровня первичного радикала алгебры;

4. построение понятия (или группы понятий) элементарной подлупы лупы Муфанг обратимых элементов альтернативной алгебры с единицей с целью получения аналогов для этой ситуации стандартного описания нормальных и субнормальных подгрупп линейных групп над кольцами (первым шагом в этом направлении должно стать получение аналога теоремы Вилсона-Голубчика для лупы обратимых элементов матричной алгебры Кэли-Диксона);

5. перенос на случай луп Муфанг теоремы Томсона о характеризации условия разрешимости конечных групп с целью получения аналогов описания условий локальной разрешимости и локальной нильпотентности PI-представимых групп в духе работ авторского коллектива Е.Б.Плоткина, Ф.Грюневальда, Б.Кунявского и др.

Второй и в действительности наиболее значимый аспект представленной работы лежит в области некоммутативной криптографии. В основе классических

криптографических систем, таких, например, как криптосистема Эль-Гамаля и протокол выработки общего ключа Диффи-Хеллмана, лежат проблемы нахождения дискретного логарифма в конечных полях, нахождения разложения числа на простые множителях и целый ряд проблем конечных абелевых групп, включая проблемы вхождения, равенства, разрешимости и т.п. В ходе последующего развития в арсенал криптографии вошли сперва некоммутативные группы (см., к примеру, протокол выработки общего ключа Стикела), а затем и квазигруппы. В представленной диссертации построены и исследованы различные криптосхемы, использующие неассоциативные алгебраические структуры. Криптосхема, предложенная С.К. Росошеком, была обобщена на случай лупового кольца. Для повышения стойкости данной схемы к некоторым атакам были предложены несколько её модификаций. Кроме того, исследован вопрос её гомоморфности при использовании медиальной лупы и приведена программа на языке компьютерной системы GAP, позволяющая анализировать параметры безопасности криптосхемы и определить возможность их применения на практике. Построен также аналог криптосистемы Эль-Гамаля над квазигруппой с перестановочными степенями и показано, что полученная схема гомоморфна относительно квазигрупповой операции (напомним, что классическая схема Эль-Гамаля гомоморфна по операции умножения). Наконец, развивая подходы Диффи-Хеллмана и Стикела, соискателем был построен протокол выработки общего ключа над лупами Пейджа и показано, что некоторые известные потенциальные атаки в некомутативном случае оказались не применимы к представленному протоколу.

Диссертация состоит из введения и трёх глав. Во введении описываются структура работы и приводится краткий перечень используемых в ней понятий и полученных в её рамках результатов.

Начальные разделы первой главы отведены последовательному изложению основ теории луп и её ключевых понятий, включая понятия нормальной подлупы и её характеризаций с использованием мультипликативных групп лупы, понятия центра лупы, лупы Муфанг и её свойств, понятий коммутатора и ассоциатора элементов лупы и взаимного коммутанта её нормальных подлуп. Основные результаты этой главы сосредоточены в двух её последних разделах, в которых приведены описания конструкций первичного радикала луп и Ω-луп. Следует отметить, что в обсуждении конструкции первичного радикала луп фактически участвуют два подхода к определению разрешимости лупы, на основе которых могут быть построены по сходной схеме два варианта конструкции первичного радикала лупы с описанием в терминах стабилизирующихся единицами цепей элементов, являющимися наименьшими из всех нормальных подлуп лупы, фактор-лупы по которым не содержат не единичных нормальных подлуп с единичным коммутантом в соответствующем смысле этого понятия. При этом вопрос о взаимосвязи между этими понятиями ещё

нуждается в отдельном рассмотрении. Заметим также, что построение первичного радикала Ω-луп сводится к интерпретации последних как универсальных алгебр сигнатуры Ω и потому может быть выполнено с использованием понятийного аппарата монографии Ю.П.Размыслова «Тождества алгебр и их представлений».

Вторая глава, начинающаяся с обсуждения свойств альтернативных колец, луповых колец и RA-луп, содержит основной и наиболее ценный в контексте сказанного ранее результат относительно взаимосвязи между первичными радикалами альтернативного кольца с единицей и подлуп лупы его обратимых элементов, в соответствии с которым центр подлупы по первичному радикалу такого кольца (своего рода аналог полной конгруэнц-подгруппы уровня первичного радикала) входит в её первичный радикал. Стоит заметить, что начальные этапы доказательства участвующих в выводе этого утверждения лемм 2.36 и 2.37 могут быть существенным образом сокращены, так как проводимые в них вычисления осуществляются на уровне ассоциативного кольца.

В третьей главе приведено описание варианта криптосхемы Росошека для квазигрупповых колец и проводится детальный анализ атак на данную криптосхему (атаки с криптограммой, на сеансовые автоморфизмы, с выбранными текстами). Кроме того, приведены примеры подходящих для реализации этой криптосхемы колец и луп и модернизации, улучшающие её устойчивость к различным атакам. Вслед за этим доказывается гомоморфность рассматриваемой криптосхемы для медиальных квазигрупп. Следующие разделы главы посвящены изложению схемы Эль-Гамаля для медиальной квазигруппы, обоснованию её гомоморфности относительно квазигрупповой операции, построению MQ-криптосхемы над альтернативной алгеброй и разнообразных криптосхем на основе луп. В приложении приведён исходный код программы в системе GAP, позволяющий вычислять параметры безопасности криптосхемы на основе автоморфизмов луповых колец.

Оставляя в стороне замечания, связанные с известным количеством опечаток пунктуационного и грамматического порядка, следует указать целый ряд встречающихся в тексте терминологических и смысловых неточностей. Так, например, не вполне оправданным является использование термина «алгебра Цорна» (в гл. 3 «алгебра Зорна») по отношению к стандартной матричной алгебре Кэли-Диксона; описание центра лупы в терминах трансляций на с. 15 не соответствует определению центра лупы, которое аналогично принятому в алгебрах определению центра как пересечения их ассоциативного и коммутативного центров; формулировки теорем 1.44 и 1.45 нуждаются в

уточнениях в плане описания отображений, порождающих все полные и соответственно все мультипликативные группы; в формулировке следствия 1.47 тот факт, что L является лупой становится условием одного из подпунктов утверждения, хотя это уже заявлено в основном условии; на с. 26 тезис о совпадении множеств [[G, g], g] и [N_g(g), N_g(g)] в случае групп не верен по причине того, что первое из них не является подгруппой и представляет собой множество элементов вида [[a, g], g], где a пробегает группу G, а второе является нормальной подгруппой согласно своего определения; в доказательстве теоремы 1.61 заключительная фраза является излишней, так как в действительности ни о каком противоречии здесь речи не идёт; приведённая схема построения первичного радикала луп соответствует в целом схеме его построения для алгебр из книги К.А.Жевлакова, А.М.Слинько, И.П.Шестакова и А.И.Ширшова "Кольца, близкие к ассоциативным", а потому было бы вполне уместно привести соответствующую ссылку; использование термина «верхний радикал» не вполне удачно, порождает ненужные ассоциации с принятым в теории радикалов Куроша–Амицура понятием верхнего радикала, определяемого подклассом основного класса, как такой радикал в смысле Куроша-Амицура на основном классе, что его полупростой подкласс является наименьшим из всех полупростых подклассов основного класса, содержащим данный подкласс; фактически в данном случае речь идёт об построении ещё одного первичного радикала луп, основанного на другом понятии коммутанта (на его первоначальном «внутреннем» определении); данный радикал лупы также имеет поэлементное описание в виде множества её элементов, таких, что содержащие их цепочки элементов, в которых каждый следующий элемент входит в коммутант нормальной подлупы, порождённой своим предшественником, стабилизируются единицей на конечном шаге, и представляет собой наименьшую из всех нормальных подлуп лупы, в фактор-лупах по которым нет неединичных нормальных подлуп с единичным коммутантом во «внутреннем» смысле (т.е. неединичных абелевых нормальных подгрупп); последнее позволяет построить данный радикал посредством трансфинитной индукции как объединение индексированной трансфинитами цепочки нормальных подлуп лупы, построенной аналогично бэровской цепи идеалов на основе отображения, сопоставляющего лупам нормальные подлупы, порождённые всеми их нормальными подлупами с единичным коммутантом; указанная цепь нормальных подлуп гарантированно стабилизируется на шаге, отвечающем трансфиниту мощности равной мощности рассматриваемой лупы; приведённая в тексте сходная конструкция «верхнего радикала» луп должна была быть записана по указанной здесь схеме без упоминания натуральных чисел; вопрос о совпадении конструкций первичного радикала луп нуждается в дальнейшей проработке (теорема 1.63 его не проясняет); в доказательствах леммы 1.71 и теоремы 1.72 имеется большое количество неточностей на уровне взаимосвязи между m-системами и m-последовательностями (m-цепями); поэлементное описание первичного радикала Ω-луп может быть выполнено с использованием определения произведения идеалов алгебр сигнатуры Ω из книги Ю.П.Размыслова "Тождества алгебр и их представлений"; ассоциатор элементов

принято обозначать в круглых скобках, а «левые и правые альтернативные тождества» традиционно называются тождествами левой и правой альтернативности; в альтернативных алгебрах произведения идеалов являются идеалами (см. «Кольца, близкие к ассоциативным»), а потому лемма 2.11, являющаяся частным случаем этого факта, может быть заменена соответствующей ссылкой; теорема 2.13 не нуждается в обосновании, так как представляет собой один из первых и наиболее естественных примеров луп Муфанг; в определении кольца Кэли-Диксона первичность следует заменить сильной первичностью (первичностью и невырожденностью (полупростотой относи-тельно радикала Маккриммона)) или определить их как центральные порядки алгебр Кэли-Диксона (отметим, что первичность здесь можно оставить для тех альтернативных неассоциативных алгебр, аддитивные группы которых не имеют 3-кручения, а также для конечно порождённых альтернативных неассоциативных алгебр над нётеровыми кольцами); лемму 2.16 можно заменить критерием сильной первичности альтернативных алгебр из цитируемой в тексте работы А.В.Михалёва и К.И.Бейдара; появившийся на с. 39 и фигурирующий в ряде последующих рассуждений термин «неассоциативный модуль» не может использоваться вследствие отсутствия подобного понятия в общем случае; следствие 2.24 не соотносится с определением 2.20 и по всей видимости должно быть заменено утверждением о некоммутативности RA-луп; элемент u в определении лупы L на с. 46 не определён, имеются неточности и в формулировке приведённой ниже теоремы 2.30; в начале доказательства леммы 2.37 должно стоять включение N_g(a) в 1+(x)_R, в одном из используемых далее выражений оператор L_{u_1, u_2} должен входить в степени с показателем -1; в формулировке теоремы 2.40 должно стоять пересечение центра матричной алгебры Кэли-Диксона по её первичному радикалу с лупой GLL(2, K); данный пример, справедливость которого не вызывает сомнений, нуждается в существенной переработке своего доказательства, которая, как можно предположить, может быть выполнена по следующему плану: сперва следует найти подсистему (систему) порождающих подлупы элементов лупы GLL(2, K) с единичным детерминантом аналогичную системе матриц элементарных трансвекций и определить элементарную подлупу лупы GLL(2, K) над кольцом, затем следует получить описание идеалов матричной алгебры Кэли-Диксона в терминах идеалов основного кольца, установив подобную взаимосвязь их первичных радикалов, и переформулировать утверждение для подлуп лупы GLL(2, K), содержащих элементарную подлупу или нормализуемых ею, сведя его доказательство к обоснованию центральности подлуп GLL(2, K), имеющих центральный коммутант и нормализуемых элементарной подлупой, в случае, когда основное кольцо является первичным, на основе доработки рассуждений, приведённых в настоящем тексте; в определении элемента группоида с перестановочными нормированными степенями имеется неточность, связанная с определением его степени с показателем [n] [m].

Необходимо подчеркнуть, что отмеченные здесь недостатки представленной диссертационной работы имеют отношение исключительно к вспомогательному материалу работы и нисколько не снижают теоретическую и практическую ценность основных её результатов, демонстрирующих широкий диапазон знаний соискателя терминологической и технической базы современной алгебры и алгебраической криптографии. На основании выше изложенного полагаю, что диссертационная работа А.В.Грибова «Алгебраические неассоциативные структуры и их приложения в криптографии» удовлетворяет всем основным требованиям ВАК, предъявляемым к диссертациям на соискание учёной степени кандидата физико-математических наук, а её автор заслуживает присуждения учёной степени кандидата физико-математических наук по специальности 01.01.06 – математическая логика, алгебра и теория чисел.

К.ф.-м.н., доцент кафедры ИУ-9
“Теоретическая информатика и
компьтерные технологии”
МГТУ им. Н.Э.Баумана, г. Москва, 105005,
2-ая Бауманская ул., д. 5, стр. 1,
тел.: (499)263-65-77,
e-mail: artgolub@hotmail.com

9 сентября 2015 г.

А.Ю.Голубков