О Т З Ы В

официального оппонента о диссертационной работе
Грибова Алексея Викторовича
“Алгебраические неассоциативные структуры
и их приложения в криптографии”,
представленной на соискание учёной степени
кандидата физико-математических наук

Теория квазигрупп – важная составная часть общей алгебры, имеющая тесные связи с другими математическими дисциплинами и приложения в математике и в других науках. Вполне вероятно, что отказ от требования выполнения ассоциативности расширяет возможности применения алгебраических методов. Таким образом появились криптографические схемы, основанные на квазигруппах и квазигрупповых кольцах, признанные специалистами весьма перспективными. Несомненно, составляющее основу диссертации изучение квазигрупп и квазигрупповых колец, а также возможных их применений к криптографии является актуальной математической задачей.

В диссертации Грибова А.В. исследованы лупы, лупы с дополнительными операциями (Ω-лупы), а также луповые кольца, в основном вокруг первичного радикала луп и колец. Кроме того, автор применил теорию луп и луповых колец к построению криптографических схем. Результаты диссертации имеют большой научный интерес и прикладное значение.

Автореферат диссертации полно и правильно отражает её содержание.

Введение в диссертацию содержит краткий исторический обзор результатов по теории луп и луповых колец, а также применению этих конструкций к криптографии. Кроме того, во введении автор делает обзор результатов диссертации.

В первой главе диссертации излагаются основные понятия теории луп и строится первичный радикал лупы. Большое значение в теории квазигрупп и луп имеют группы преобразований, порождённые операторами умножения и деления (слева или справа). В теореме 1.48 автор описывает коммутатор двух нормальных подлуп лупы в терминах полной группы внутренних отображений. Доказано, что первичный радикал rad лупы в точности совпадает с множеством её строго энгелевых элементов (теорема 1.61). В теореме 1.62 для произвольной лупы L доказано равенство $\mathrm{rad}(L/\mathrm{rad}\,L)=\{1\}$ – необходимое для радикала в смысле А.Г.Куроша. Наряду с подходом с помощью энгелевых элементов автор рассматривает введение первичного радикала с помощью возрастающего трансфинитного ряда подлуп и доказывает совпадение радикалов, определённых этими способами (теорема 1.63). Кроме того, рассмотрены Ω-лупы. Оказывается, что, как и в кольцах, конгруэнции Ω-лупы – это разложения её в смежные классы по идеалам (теорема 1.68). Определено понятие первичного радикала Ω-лупы и получена характеризация элементов радикала с помощью m-систем (теорема 1.72) и строго энгелевых элементов (теорема 1.74). Отдельно рассмотрен важный частный случай, когда сигнатура Ω состоит из одной операции коммутирования (теорема 1.75).

Во второй главе рассмотрены альтернативные кольца вообще и луповые кольца KL, являющиеся альтернативными. Лупа L в этом случае называется RA-лупой, а такие лупы достаточно хорошо изучены; в частности, известно, что они являются лупами Муфанг. Автор получает характеризацию RA-луп L, где альтернативно кольцо KL для некоторого ассоциативно-коммутативного кольца с единицей K характеристики $\neq 2$ (теорема 2.21). В частности, любые три элемента такой лупы либо образуют ассоциативную тройку, либо удовлетворяют равенству, близкому к ассоциативности. Отмечен ряд свойств RA-луп и найдены некоторые тождества, которым удовлетворяют

все RA-лупы (следствия 2.27, 2.28, 2.29). Исследован первичный радикал альтернативного кольца и установлены связи его с радикалом мультипликативной подлупы (теорема 2.38), а также радикала лупового кольца RL с радикалом подлупы лупы $U(RL)$ обратимых элементов (теорема 2.39). Охарактеризован радикал лупы обратимых элементов кольца матриц Цорна (теорема 2.40).

В главе 3 автором предложены криптографические схемы на основе лупового кольца. Проанализированы возможные атаки на криптосистему. Обсуждены методы подбора луп и луповых колец, обеспечивающие стойкость криптосистемы. Приведены примеры. Кроме этого рассмотрены криптосистемы на основе медиальных квазигрупп, их квазигрупповых колец, а также других группоидов и группоидных колец.

Отмечу некоторые недостатки работы. Умножение отображений в работе молчаливо предполагается выполняемым сначала справа налево (с. 11), затем слева направо (с. 15), потом снова справа налево (с. 21). Автор пишет “отметим ряд результатов из работы Г.Войтеховского и Д.Становского” (с. 20), но не говорит, каких именно. Множество W' в лемме 1. 46 (с. 21) определяется с помощью самого множества W'. Доказательства теорем 1.61, 1.68, 1.72 (с. 26, 30, 32) осуществляются аналогично друг другу и аналогично соответствующим результатам теории ассоциативных колец – это следовало бы подчеркнуть. В теореме 2.21 (с. 41) доказательство пункта a) не приведено (хотя оно следует из рассуждений, доказывающих b). В доказательстве теоремы 2.13 (с. 36) следует объяснить, как из теоремы Артина получается, что алгебра $\langle x, x^{-1}, a \rangle$ ассоциативна, или дать ссылку. На с. 22 трижды делается ссылка на теорему 2.38, хотя должна быть ссылка на теорему 1.44. На с. 23 есть ссылка на “лемму 1.47”, тогда как надо ссылаться на предложение 1.47. В доказательстве леммы 2.37 (с. 51) непонятно равенство $Ng(1+x)=1+Ng(x)$, ведь выполнение соотношения $x \in L$, вообще говоря, не требуется. Также непонятно введение отношения ~ (с. 75), которое ввиду закона сокращения совпадает с отношением равенства. Алгебра матриц определённого вида названа вначале алгеброй Цорна (с. 53), а потом алгеброй Зорна (с. 80). Лемму 1.52 (с. 25) следует формулировать “в обе стороны”. На с. 27 в 5-й снизу строке вместо “первое натуральное число” следовало написать “наименьший ординал”. На с. 41 в 1-й и 2-й строках следовало написать не “принадлежит правому и левому элементу”, а “принадлежит левой и правой частям равенства”. В следствии 1.47 (с. 22) лучше было бы написать не “$W=$”, а “в качестве W может быть взято”. На с. 22 в 17-й сверху строке должно быть “подлупами”, а не “лупами”, а на с. 25 в 11-й снизу строке, наоборот, должно быть “лупа”, а не “подлупа”. Имеются опечатки в формулах: на с. 16 в 5-й снизу строке должно быть “hg” вместо “fh”, на с. 24 (12-я снизу) вместо “A, B” должно быть “A, B, P”, на с. 40 (5-я снизу) вместо “$\neq 0$” должно быть “$\neq \varnothing$”, на с. 43 (13-я снизу) должно быть “в ядре L”, а не “в ядре FL”, на с. 51 (12-я снизу) вместо “$C(L)-$” должно быть “$C(L)=$”, на с. 57 (12-я снизу) нужно “$\Omega_n^m(A,R)$” вместо “$\Omega_n(A,R)$”, в формуле на с. 61 (15-я сверху) нужно добавить “$=h$”. В библиографии на с. 91 (12-я строка сверху) существительные должны быть написаны с большой буквы.

Указанные недостатки не изменяют общего положительного впечатления о работе. Результаты диссертации являются новыми и получены автором самостоятельно. Утверждения снабжены убедительными доказательствами или ссылками. Безусловным достоинством работы является её практическое применение. Следует отметить, что автор хорошо владеет техникой теории квазигрупп и луп и теории неассоциативных колец, а написанная им диссертация показывает его высокую квалификацию как специалиста. Результаты диссертации теоретического характера могут быть использо-

ваны в спецкурсах по общей алгебре, читаемых в МГУ, МПГУ, НГУ и других университетах, а также научно-исследовательских институтах. Результаты прикладного характера имеют очевидное использование.

Ввиду вышеизложенного считаю, что диссертационная работа “Алгебраические неассоциативные структуры и их приложения в криптографии” удовлетворяет всем требованиям “Положения о порядке присуждения учёных степеней” ВАК, а её автор Грибов А.В. заслуживает присуждения учёной степени кандидата физико-математических наук по специальности 01.01.06 – математическая логика, алгебра и теория чисел.

Автор отзыва Кожухов Игорь Борисович, доктор физико-математических наук, профессор.

Место работы, должность: Национальный исследовательский университет “МИЭТ” (124498, Москва, пл. Шокина, 1), профессор кафедры Высшая математика – 1.

Домашний адрес и телефон: 124460, Москва, корпус 1209, кв. 51, +7-916-715-55-02.

Электронная почта: kozhuhov_i_b@mail.ru

Доктор физико-математических наук,
профессор кафедры ВМ-1 НИУ МИЭТ И.Б.Кожухов

Подпись Кожухова И.Б. удостоверяю
Секретарь Учёного Совета НИУ МИЭТ, к.т.н. Н.М.Ларионов