УТВЕРЖДАЮ:
декан механико-математического факультета
ФГБОУ ВО «МГУ имени М.В. Ломоносова»,
доктор физико-математических наук,
профессор
_____ В.Н. Чубариков
«14» февраля 2017 г.

ЗАКЛЮЧЕНИЕ
кафедры высшей алгебры
механико-математического факультета
ФГБОУ ВО «Московский государственный университет имени М.В. Ломоносова»
по диссертации Тумайкина Ильи Николаевича
«Коды Рида-Маллера как групповые коды»
на соискание учёной степени кандидата физико-математических наук
по специальности 01.01.06 – математическая логика, алгебра и теория чисел

Диссертация Тумайкина Ильи Николаевича «Коды Рида-Маллера как групповые коды» **выполнена** на кафедре высшей алгебры механико-математического факультета ФГБОУ ВО «Московский государственный университет имени М.В. Ломоносова».

В период подготовки диссертации соискатель работал младшим научным сотрудником лаборатории автоматизации экспериментальных исследований НИИ механики МГУ имени М.В. Ломоносова.

В 2013 году **окончил с отличием** ФГБОУ ВО «Московский государственный университет имени М.В. Ломоносова» **по специальности «Математика»**, в 2016 году **окончил** очную аспирантуру на кафедре высшей алгебры механико-математического факультета ФГБОУ ВО «Московский государственный университет имени М.В. Ломоносова».

Удостоверение № 2688 о сдаче кандидатских экзаменов выдано в 2016 году отделением математики механико-математического факультета ФГБОУ ВО «Московский государственный университет имени М.В. Ломоносова».

Научный руководитель – Марков Виктор Тимофеевич, к.ф.-м.н., доцент кафедры высшей алгебры механико-математического факультета ФГБОУ ВО «Московский государственный университет имени М.В. Ломоносова».

Присутствовали: заведующий кафедрой, д.ф.-м.н., профессор В.А. Артамонов, д.ф.-м.н., профессор В.Н. Латышев, д.ф.-м.н., профессор Э.Б. Винберг, д.ф.-м.н., профессор Е.С. Голод, д.ф.-м.н., профессор Е.И. Бунина, д.ф.-м.н., профессор А.Э. Гутерман, к.ф.-м.н., доцент В.Т. Марков, к.ф.-м.н., доцент О.В. Куликова, к.ф.-м.н., доцент О.В. Маркова, к.ф.-м.н., доцент А.А. Клячко, к.ф.-м.н., научный сотрудник А.Л. Канунников, к.ф.-м.н., ассистент С.А. Гайфуллин.

Повестка дня: обсуждение диссертационной работы выпускника аспирантуры кафедры высшей алгебры механико-математического факультета ФГБОУ ВО «Московский государственный университет имени М.В. Ломоносова» Тумайкина Ильи Николаевича «Коды Рида-Маллера как групповые коды», представленной на соискание учёной степени кандидата физико-математических наук по специальности 01.01.06 – математическая логика, алгебра и теория чисел.

Слушали: доклад диссертанта Тумайкина Ильи Николаевича.

Представленная работа является исследованием в области алгебраической теории кодов с исправлением ошибок. Целью представленной работы является изучение алгебраической структуры обычных и базисных кодов Рида-Маллера как идеалов групповой алгебры элементарной абелевой p-группы, где p – характеристика основного поля. Перед автором возникли следующие задачи:

1. Доказать, что в случае непростого подполя основного поля базисные коды Рида-Маллера имеют только тривиальные совпадения со степенями радикала соответствующей групповой алгебры;
2. Найти необходимые и достаточные условия теоретико-множественных включений между базисными кодами Рида-Маллера и степенями радикала;
3. Разработать методы, позволяющие распространить полученные результаты для базисных кодов Рида-Маллера на случай обычных кодов Рида-Маллера;
4. На основе полученных методов доказать для обычных кодов Рида-Маллера аналоги перечисленных выше результатов для базисных кодов.

Эти задачи успешно решены автором в данной работе.

Диссертация состоит из введения, шести разделов, заключения, списка цитируемой литературы и приложения.

Во введении описывается структура диссертации и история рассматриваемых вопросов; определяется область исследования; обосновывается актуальность темы и научная новизна полученных результатов; описываются основные результаты диссертации.

В первом разделе, который является вводным, формулируются основные определения и утверждения, которые далее используются в данной научной работе.

Во втором разделе сначала кратко описывается известный случай простого подполя основного поля, при котором базисные коды Рида-Маллера совпадают со степенями радикала соответствующей групповой алгебры, далее рассматривается случай произвольного непростого подполя; с помощью теоретико-кольцевых и элементарных теоретико-числовых методов доказывается отсутствие указанных совпадений, кроме трёх тривиальных случаев.

В третьем разделе изучены теоретико-множественные включения между базисными кодами Рида-Маллера и степенями радикала в случае непростого подполя; сначала рассматривается случай включения базисных кодов в степени радикала, и устанавливается ряд эквивалентных критериев, характеризующих данные включения, с использованием теоретико-кольцевых, теоретико-множественных и числовых условий; далее рассматривается случай включения степеней радикала в базисные коды, и устанавливается ряд эквивалентных теоретико-множественных и числовых критериев данных включений.

В четвёртом разделе подробно исследованы теоретико-кольцевые критерии включения базисных кодов в степени радикала.

В пятом разделе построены базисы специального вида для обычных кодов Рида-Маллера; построенные базисы являются связующим звеном при рассмотрении базисных и обычных кодов Рида-Маллера в совокупности.

В шестом разделе, с помощью развитых в работе методов, для обычных кодов Рида-Маллера доказаны аналоги утверждений, полученных в работе для базисных кодов: показано отсутствие нетривиальных совпадений со степенями радикала над непростым полем, и найдены критерии включений между обычными кодами Рида-Маллера и степенями радикала.

В приложении кратко описаны методы компьютерного моделирования, которые были использованы для получения предварительных результатов.

В качестве рецензента выступил научный сотрудник А.Л. Канунников. Он отметил, что задача исследования совпадений и включений между кодами Рида-Маллера и степенями радикала соответствующей групповой алгебры в случае непростого поля ранее не ставилась. Он указал, что представленные в работе методы исследования базисных и обычных кодов Рида-Маллера не только глубоко затрагивают их структуру с точки зрения теории колец, но и позволяют получить простые числовые соотношения, описывающие указанные включения. Он поддержал рекомендацию диссертации к защите.

В дискуссии приняли участие профессор В.Н. Латышев и профессор В.А. Артамонов. В.Н. Латышев задал вопрос о возможных криптографических приложениях результатов диссертации. Диссертант ответил, что пока такие приложения не разработаны, но существующая глубокая связь между теорией кодирования и криптографией позволяет надеяться, что такие приложения возникнут. В.А. Артамонов задал вопрос о возможности переноса результатов на случай некоммутативного или неассоциативного кольца с единицей. Диссертант ответил, что используемые методы существенным образом опираются на строение группы и свойства выбранного поля, поэтому без значительных изменений не удаётся распространить полученные результаты на указанные случаи. В.Н. Латышев высказал мнение, что диссертация удовлетворяет требованиям предъявляемым к диссертациям, и поддержал рекомендацию диссертации к защите.

Научный руководитель – к.ф.-м.н., доцент В.Т. Марков – отметил актуальность тематики, высокую степень самостоятельности диссертанта, а также новизну и содержательность представленных результатов.

По итогам обсуждения принято следующее заключение:

Представленная диссертация является самостоятельно выполненной, законченной научно-исследовательской работой, посвящённой решению актуальных задач в области алгебраической теории кодов с исправлением ошибок.

Научные результаты диссертации, выносимые на защиту, получены автором лично, являются новыми и обоснованы в виде строгих математических доказательств. Результаты других авторов, упомянутые в тексте диссертации, отмечены соответствующими ссылками.

В диссертации получены следующие основные результаты:

1. Доказано отсутствие нетривиальных совпадений базисных кодов Рида-Маллера со степенями радикала соответствующей групповой алгебры в случае непростого подполя;

2. Получены необходимые и достаточные условия, при которых есть включения между базисными кодами и степенями радикала. Дано теоретико-кольцевое, теоретико-множественное и числовое описание указанных условий;

3. Разработаны методы переноса отдельных классов результатов для базисных кодов Рида-Маллера на случай обычных кодов Рида-Маллера, для чего были построены специальные базисы обычных кодов Рида-Маллера, отличающиеся новыми свойствами;

4. Доказано отсутствие нетривиальных совпадений между обычными кодами Рида-Маллера и степенями радикала в случае непростого поля;

5. Получены необходимые и достаточные условия, при которых есть включения между обычными кодами Рида-Маллера и степенями радикала. Дано теоретико-кольцевое, теоретико-множественное и числовое описание указанных условий.

Методы исследования: В диссертации используются методы теории колец, методы теории чисел и методы теории базисных кодов Рида-Маллера, предложенные группой учёных: Коусело, Гонсалес, Марков, Мартинес, Нечаев. Предварительные результаты были получены с помощью компьютерного моделирования.

Апробация диссертации:

Результаты диссертации докладывались автором на семинарах механико-математического факультета МГУ имени М.В. Ломоносова:

1. Семинар «Кольца и модули» под руководством профессора В.Н. Латышева, профессора А.В. Михалева, профессора В.А. Артамонова, неоднократно в 2013-2016 гг.;
2. Научно-исследовательский семинар кафедры высшей алгебры, 2016 г.

Тема диссертации входит в координационный план РАН.

Регистрационный номер АААА-А16-116070810025-5 «Алгебраические системы: группы, кольца, универсальные алгебры; алгебраическая геометрия; группы Ли и теория инвариантов; компьютерная алгебра, теория кодирования», шифр 1.1.3.6 «Алгебра. Теория колец и модулей».

Утверждение темы диссертации состоялось 27 ноября 2015 года, протокол № 8.

Основное содержание диссертации опубликовано в следующих работах автора:

1. I.N. Tumaikin, “Basic Reed–Muller Codes and Their Connections with Powers of Radical of Group Algebra over a Non-Prime Field”, Moscow University Mathematics Bulletin, 68, 6 (2013), 295–298.

2. И.Н. Тумайкин, “Базисные коды Рида-Маллера как групповые коды”, Фундаментальная и прикладная математика, 18, 4 (2013), 137–154.

3. И.Н. Тумайкин, “Идеалы групповых колец, связанные с кодами Рида-Маллера”, Фундаментальная и прикладная математика, принята к печати.

4. И.Н. Тумайкин, “Коды Рида-Маллера как групповые коды”, готовится к публикации.

Диссертация к защите представлена впервые.

Диссертация «Коды Рида-Маллера как групповые коды» Тумайкина Ильи Николаевича **рекомендуется к защите** на соискание учёной степени кандидата физико-математических наук по специальности 01.01.06 – математическая логика, алгебра и теория чисел – для защиты на диссертационном совете Д.501.001.84, созданного на базе ФГБОУ ВО МГУ имени М.В. Ломоносова.

Заключение принято на заседании кафедры высшей алгебры механико-математического факультета МГУ имени М.В. Ломоносова.

Присутствовало на заседании 12 чел. Результаты голосования: «за» – 12 чел., «против» – нет, «воздержалось» – нет, протокол № 1036 от 21 ноября 2016 года.

Заведующий кафедрой высшей алгебры,
д.ф.-м.н., профессор В.А. Артамонов

Учёный секретарь кафедры высшей алгебры,
к.ф.-м.н., ассистент С.А. Гайфуллин