

Голові спеціалізованої вченої ради
ДФ 20 051.129
Прикарпатського національного
університету імені Василя Стефаника
доктору фізико-математичних наук,
професору Дмитришину Роману Івановичу
(76018, м. Івано-Франківськ,
вул. Шевченка, 57)

ВІДГУК

офіційного опонента, доктора фізико-математичних наук, професора,
завідувача кафедри алгебри, топології та основ математики Львівського
національного університету імені Івана Франка **Банаха Тараса Онуфрійовича**
на дисертаційну роботу **Чоп'юка Юрія Юрійовича**
«Аналіз в кільцях мультимножин, породжених алгебрами
суперсиметричних поліномів на банахових просторах»,
подану на здобуття ступеня доктора філософії в галузі знань
11 Математика та статистика за спеціальністю 111 Математика

Актуальність теми дослідження. Дисертація присвячена систематичному дослідженню алгебраїчних властивостей мультимножин та мультчисел – цікавих алгебро-аналітичних об'єктів, що природно виникають при вивченні спектрів алгебри симетричних поліномів та симетричних аналітичних функцій на класичних банахових просторах. Поняття симетрії є одним з основних об'єднуючих понять в математиці, яке має численні застосування, починаючи від фізики та механіки і закінчуючи музикою, архітектурою та мистецтвом. На відміну від множин, мультимножини містять не лише інформацію про наявність чи відсутність певного елемента у множині, але і про його кратність себто кількість копій елемента у множині. У цьому сенсі мультимножини є ближчими до арифметики, у той час як звичні нам множини моделюють булеві алгебри. Ця багатша інформаційна наповненість мультимножин може бути корисною у застосуваннях, де важливими є кількісні, а не лише якісні характеристики.

Зміст роботи і новизна одержаних результатів. Дисертація (її повний обсяг становить 139 сторінок друкованого тексту) складається зі вступу, п'яти розділів, висновків та списку використаних джерел, що містить 60 найменувань.

У **вступі** обґрунтовано актуальність теми дисертаційного дослідження, встановлено зв'язок дослідження з науково-дослідними роботами та проєктами, сформульовано мету, задачі, об'єкт, предмет та методи дослідження, зазначено наукову новизну, практичне значення отриманих результатів та особистий внесок здобувача, також зазначено, де опубліковано і де було апробовано результати дисертаційного дослідження.

Перший розділ містить детальний історичний огляд розвитку понять, дотичних до симетричних поліномів, починаючи від класичних робіт Вієта, Жирара, Ньютона, Лагранжа, Абеля, Руффіні, Галуа, Сильвестра, Дедекінда,

Вейерштраса і закінчуючи сучасними працями Арона, Гонзалеса, Галіндо, Загороднюка. У цьому розділі також наводиться необхідний алгебраїчний інструментарій (як от конструкція Гротендіка) та означаються мультичисла – один з основних об'єктів вивчення у дисертації.

У **другому розділі** детальніше вивчаються алгебраїчні властивості кільця мультичисел та відповідна двопараметрична модулярна арифметика. Також вибудовуються аналітичні зображення цих кілець в кільцях аналітичних функцій та рядів Діріхле.

У **третьому розділі** вибудовується комплексифікація кілець мультичисел та встановлюються відповідні алгебраїчні властивості такої комплексифікації. Цікаво було б дослідити також проблему алгебраїчної замкненості отриманих алгебраїчних структур.

У **четвертому розділі** вивчаються симетричні, суперсиметричні поліноми та їхні узагальнення, які застосовуються до вивчення кілець мультичисел та встановлення теорем про розклад мультичисел в добуток нерозкладних співмножників.

У **п'ятому розділі** продемонстрована можливість застосувань кілець мультичисел до створення криптографічних інструментів, зокрема криптосистем з відкритим ключем, що нагадують класичну систему RSA.

В цілому дисертація справляє хороше враження. Вона поєднує методи та мотивацію з різних досить віддалених областей математики, зокрема функціональний та комплексний аналіз з алгеброю, теорією чисел та криптологією. Отримані результати є новими, цікавими та вказують на можливі цікаві застосування до практичних задач, зокрема для захисту інформації, що є дуже важливим та актуальним в наш турбулентний час.

Відсутність порушення академічної доброчесності. За результатами перевірки дисертаційної роботи та публікацій не виявлено ознак академічного плагіату, елементів фабрикації та фальсифікації. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело. У дисертаційній роботі відсутні порушення академічної доброчесності.

Обґрунтованість і достовірність одержаних результатів. Усі основні результати дисертації строго обґрунтовані та супроводжуються коректними математичними доведеннями.

Апробація результатів і публікації. Результати дисертації опубліковано в трьох статтях, опублікованих в журналах з високим індексом впливовості, та анонсовано на чотирьох престижних міжнародних конференціях, на яких я, свого часу, і познайомився з автором дисертації та його науковими пошуками та знахідками.

Практичне значення результатів дисертації. Результати дисертації мають як теоретичне, так і практичне значення, зокрема до проблем захисту інформації, про що йшла мова у п'ятому розділі дисертації.

Зауваження. Дисертація акуратно оформлена і дбайливо вчитана. Вона містить цікаві історичні екскурси та цитати класиків. Якихось суттєвих огріхів віднайти не вдалося. От хіба для галочки одне зауваження щодо запропонованих криптографічних застосувань мультичисел. На початку п'ятого розділу автор пише, для достатньо великого числа p знаходження оберненого числа за модулем p є складною алгоритмічною задачею, що не зовсім правда, оскільки її реалізовує добре знаний розширений алгоритм Евкліда, який має лінійну складність. Складність класичних криптографічних інструментів типу RSA чи криптосистеми Ель Гамала базується на складності знаходження коренів чи дискретних логарифмів, а не обчисленні оберненого. У той же час, автор пропонує криптографічний протокол, надійність якого базується на складності задачі обчислення оберненого елемента в кільці мультичисел. Проте доведення того, що ця задача дійсно складна, або зводиться до іншої відомої складної задачі, в дисертації нема. Тобто запропонований протокол можна визнати надійним лише до моменту знаходження швидкого алгоритму знаходження оберненого елемента в кільці мультичисел. А такий елемент мав би знаходитися або за допомогою якоїсь версії розширеного алгоритму Евкліда, або за допомогою відомого швидкого алгоритму піднесення до степеня (обернений до елемента порядку n є його $n+1$ -шим степенем). Проте це зауваження зовсім не перекреслює потенційних можливостей застосувань мультичисел в криптології, а навпаки мотивує до інтенсивніших досліджень у цьому багатообіцяючому напрямку.

Висновок. Вважаю, що дисертаційна робота «Аналіз в кільцях мультимножин, породжених алгебрами суперсиметричних поліномів на банахових просторах» Юрія Юрійовича Чоп'юка є завершеною науковою працею, що містить нові важливі наукові результати з цікавими потенційними застосуваннями до криптології. Основні результати дослідження є добре висвітлені у наукових працях. Робота повністю відповідає усім вимогам спеціальності 111 Математика та вимогам наказу Міністерства освіти і науки України № 40 від 12.01.2017 р. «Про затвердження вимог до оформлення дисертації» (зі змінами), «Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії», затвердженого Постановою Кабінету Міністрів України від 12.01.2022 р. № 44 (зі змінами), а її автор, Чоп'юк Юрій Юрійович, заслуговує на присудження наукового ступеня доктора філософії у галузі знань 11 Математика та статистика за спеціальністю 111 Математика.

Офіційний опонент:

доктор фізико-математичних наук, професор,
завідувач кафедри алгебри, топології та основ математики
Львівського національного університету імені Івана Франка

_____ Тарас БАНАХ