НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ
ІНСТИТУТ МАТЕМАТИКИ

СКУРАТОВСЬКИЙ РУСЛАН ВЯЧЕСЛАВОВИЧ

УДК 512.55, 512.58, 512.723

ІДЕАЛИ БІМОДАЛЬНИХ ОСОБЛИВОСТЕЙ ПЛОСКИХ КРИВИХ

01.01.06 – алгебра і теорія чисел

Автореферат
дисертації на здобуття наукового ступеня
кандидата фізико-математичних наук

Київ – 2019

Дисертацією є рукопис.

Роботу виконано на кафедрі інформаційної безпеки
факультету компютерних та інформаційних технологій
Міжрегіональної академії управління персоналом.

Науковий керівник: доктор фізико-математичних наук, професор,
член-кореспондент НАН України
ДРОЗД Юрій Анатолійович,
Інститут математики НАН України
завідувач відділу алгебри і топології.

Офіційні опоненти: доктор фізико-математичних наук,
старший науковий співробітник
ГЛАЗУНОВ Микола Михайлович,
Національний авіаційний університет,
професор кафедри електроніки;

кандидат фізико-математичний наук, доцент
ШАПОЧКА Ігор Валерійович,
Ужгородський національний університет,
завідувач кафедри алгебри.

Захист відбудеться "_8_" _жовтня_ 2019 р. о 15 годині на засіданні спеціалізованої вченої ради Д 26.206.03 Інституту математики НАН України за адресою: 01024, м. Київ, вул. Терещенківська, 3.

З дисертацією можна ознайомитись у бібліотеці Інституту математики НАН України.

Автореферат розіслано "_3_" _вересня_ 2019 р.

Вчений секретар

спеціалізованої вченої ради Полулях Є.О.

ЗАГАЛЬНА ХАКТЕРИСТИКА РОБОТИ

Актуальність теми. Вивчення ідеалів комутативних кілець бере свій початок у теорії чисел, зокрема, з робіт Куммера, який і побудував теорію ідеалів (“ідеальних чисел”) у кільцях цілих алгебраїчних чисел. У ХХ сторіччі в роботах Е. Нетер, Е. Артіна, А. Шпайзера та інших було розроблено загальнішу теорію ідеалів у дедекіндових кільцях.

Якщо ця теорія у своїх загальних рисах є фактично завершеною, то в теорії ідеалів нецілозамкнених кілець залишається велика кількість невирішених питань. Зокрема, це пов’язано з питаннями про будову й кількість класів ідеалів. Перші загальні результати тут одержали З.І. Боревич і Д.К. Фаддєєв для квадратичних кілець. Надалі вони й Х. Басс ці результати узагальнили на набагато ширший клас кілець, які зараз називаються бассовими кільцями або кільцями з циклічним індексом. Вони довели, що кожен ідеал такого кільця є обертовним (тобто локально проективним) над своїм кільцем множників. Зокрема, у локальному випадку такі кільця мають лише скінченну кількість класів ідеалів. Для кубічних кілець Д.К. Фаддєєв довів, що кожен ідеал є або обертовним, або дуальним до обертовного над своїм кільцем множників.

Ю.А. Дрозд узагальнив цей результат на ширший клас кілець, який містить, зокрема, всі локальні кільця особливостей типу Е в розумінні Арнольда. У роботах Г. Якобінського, Ю.А. Дрозда й А.В. Ройтера було дано критерії того, що комутативне локальне кільце без нільпотентних елементів розмірності Крулля 1 має лише скінченну кількість нерозкладних неізоморфних модулів без скруту. Надалі такі кільця ми називатимемо одновимірними особливостями. Якщо це кільце є локальним із нескінченним полем лишків, ті самі умови є необхідними й достатніми для того, щоб це кільце мало скінченну кількість класів ідеалів. Ґ.-М. Ґроєль і Г. Кнеррер установили, що в “геометричному випадку” скінченнопороджених алгебр над алгебраїчно замкненим полем ці умови рівнозначні до того, що дане кільце домінує одну зі простих плоских особливостей у розумінні В.І. Арнольда.

Вивчення модулів без скруту й ідеалів у випадку, коли їх стає нескінченно багато, ґрунтується на понятті модальності або кількості параметрів, які визначають такі модулі, зокрема, ідеали. Перший крок тут зробив А. Шапперт, який установив, що ідеали плоских геометричних (одновимірних) особливостей складають лише однопараметричні сім’ї тоді і тільки тоді, коли ці особливості є унімодальними або бімодальними у класифікації книжки В.І. Арнольда. В інших термінах, прийнятих, наприклад, у роботах С. Волла, такі особливості називаються строго унімодальними.

Ю.А. Дрозд і Ґ.-М. Ґроєль 1998 року встановили, що без обмеження плоскості необхідною й достатньою умовою однопараметричності сімей ідеалів є те, щоб дане кільце домінувало унімодальну або бімодальну плоску особливість. Гіпотеза про те, що такою самою є й умова однопараметричності для модулів без скруту, виявилась неправильною: більшість таких особливостей є дикими в розумінні теорії зображень, зокрема, мають сім'ї модулів без скруту з як завгодно великою кількістю параметрів. Саме Ю.А. Дрозд і Ґ.-М. Ґроєль установили, що необхідною й достатньою умовою того, щоб модулі без скруту над геометричною одновимірною особливістю складали щонайбільше однопараметричні сім'ї, є те, щоб ця особливість домінувала особливість типу Т в розумінні Арнольда. Зокрема, унімодальні плоскі особливості типів E й W є дикими. В роботі Ю.А. Дрозда, Ґ.-М. Ґроєля й І. Кашуби аналогічний результат було отримано для мінімальних еліптичних особливостей поверхонь. При цьому були використані результати роботи Ю.А. Дрозда й Ґ.-М. Ґроєля про параметризацію сімей векторних розшарувань на проективних кривих.

Усе це показує, що вивчення ідеалів комутативних кілець, зокрема параметризації класів ідеалів, є актуальною задачею сучасної алгебри. При цьому досі не розглядалося питання про особливості, які б мали сім'ї ідеалів, щонайбільше p-параметричні при $p > 1$. Зокрема, важливим є вивчення їхніх зв'язків зі класифікацією особливостей за В.І. Арнольдом.

Зв'язок роботи з науковими програмами, планами, темами. Тематика дисертації перебуває в руслі досліджень кафедри інформаційної безпеки і кафедри обчислювальної математики та компютерного моделювання факультету компютерних та інформаційних технологій Міжрегіональної академії управління персоналом.

Мета і завдання дослідження: *Метою дослідження* дисертаційної роботи є вивчення будови ідеалів особливостей алгебраїчних кривих і опис їхніх зображувальних типів, зокрема, пошук критеріїв двопараметричності сімей ідеалів.

Об'єктом дослідження є ідеали локальних кілець одногілкових особливих точок алгебраїчних кривих, кубічні кільця і їхні ідеали, нормальні базиси у скінченному полі.

Предмет дослідження – сім'ї ідеалів і їхня параметризація, умови двопараметричності таких сімей, класифікація кубічних кілець і їхніх ідеалів, алгоритми побудови нормального базису

Методи досліджень. У роботі використовуються методи алгебраїчної геометрії, теорії особливостей, теорії зображень, а також теорії кілець і полів.

Наукова новизна одержаних результатів. Усі результати отримані в роботі, яка виноситься на захист, є новими і полягають у такому:

- Описано кубічні кільця над дискретно нормованим кільцем і їхні ідеали. У геометричному випадку визначено кількість параметрів, від яких залежать класи ідеалів.
- Дано критерій того, що одногілкова особливість алгебраїчної кривої мала щонайбільше двопараметричні сім'ї ідеалів. Цей критерій пов'язаний зі класифікацією плоских особливостей Арнольда.
- Для особливостей зі двопараметричними сім'ями ідеалів дано повний опис ідеалів із точністю до ізоморфізму.
- Розроблено новий метод побудови нормального базису в полі F_q, де $q = p^n$.

Практичне значення отриманих результатів. Дисертаційна робота має теоретичний характер. Результати роботи можуть бути використані в подальших дослідженнях особливостей кривих. Метод побудови нормального базису скінченного поля може бути основою для найшвидшого на цей час алгоритму побудови нормального базису скінченного поля.

Особистий внесок здобувача. Всі наукові результати, які виносяться на захист, автор отримав особисто. У спільних із науковим керівником публікаціях за темою дисертації науковому керівнику належать постановка задачі, визначення напрямку роботи й загальне керівництво, а конкретні результати й обчислення належать дисертанту.

Апробація результатів дисертації. Основні результати дисертації доповідалися й обговорювалися на:

1) 7^{th} International Algebraic Conference in Ukraine. "Ukrainian mathematical congress". Ukraine, (Kharkov, 18 - 23 August, 2009).

2) Міжнародній науковій конференції молодих вчених, присвяченій 70-річчю механіко-математичного факультету Київського національного університету імені Тараса Шевченка, м. Київ, 2010 р.

3) Всеукраїнській науково-методичній конференції «Сучасні наукові проблеми математики у вищій школі», присвяченій Левіщенко С.С., 7-8 жовтня 2016 р.

4) 11-й Міжнародній алгебраїчній конференції в Україні, присвяченій 75-річчю В.В. Кириченка, м. Київ, 2017 р.

5) Міжнародній Конференції молодих вчених із сучасних проблем механіки і математики імені академіка Я. С. Підстригача, КМУ СПММ – 2011 р.

6) 10-й Міжнародній науковій міждисциплінарній конференції студентів, аспірантів і молодих учених "Шевченківська весна", м. Київ, 19-23 березня 2012 р.

7) Засіданні Алгебраїчного семінару Інституту математики НАН України, м. Київ, 2018 р. (керівник — доктор фізико-математичних наук, член-кореспондент НАН України Ю. А. Дрозд).

8) Засіданні семінару з фрактального аналізу, відділу Динамічних систем та фрактального аналізу Інституту математики НАН України, м. Київ, 2019 р.

9) Міжнародній Конференції **"**Сучасні проблеми механіки та математики" в Інституті прикладних проблем механіки і математики ім. Я.С. Підстригача НАН України, м. Львів, 2018 р.

Публікації. Результати дисертаційної роботи опубліковано у 5 наукових працях [1 – 5] у фахових виданнях із переліку, затвердженого Міністерством освіти і науки України (3 без співавторів [1 – 3]), 3 з них опубліковані у виданнях, які входять до міжнародної наукометричної бази даних Scopus.

Структура й обсяг роботи. Дисертація складається зі вступу, 5 розділів, що розділені на підрозділи, висновків і списку літератури, що містить 44 найменування. Обсяг роботи складає 147 сторінок.

Подяка. Автор щиро вдячний науковому керівникові професору Юрієві Анатолієвичу Дрозду за постановку задач, увагу й підтримку.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У вступі обґрунтовано актуальність теми, подано короткий аналіз сучасного стану проблеми, сформульовано мету й завдання дослідження, наукову новизну, практичне значення одержаних результатів і подано відомості про апробацію результатів дисертаційного дослідження.

Розділ 1 присвячено історичному оглядові робіт, які стосуються теми дисертаційного дослідження.

Розділі 2 містить дослідження кубічних кілець. Описано всі такі кільця і їхні ідеали, зокрема, встановлено зміну $\mathrm{par}(\mathbf{C})$ для кубічного кільця $\mathbf{C}$. Як наслідок, було показано, що кубічне кільце є гоpенштейновим тоді й тільки тоді, коли це — кільце плоскої особивості. Нехай $\mathbf{D}$ — кільце дискретного нормування, t — твірний максимального ідеалу, $\mathbf{C}$ — *кубічне кільце,* тобто підкільце у тривимірній алгебрі L над полем частoк $\mathbf{K}$ кільця $\mathbf{D}$, ціле над $\mathbf{D}$. Через $\mathbf{A}$ позначимо максимальне ціле підкільце у $\mathbf{L}$ і запишемо $\mathrm{A}_m = t^m\mathrm{A}+\mathrm{D}$ й $\mathrm{J}_m = t^m\mathrm{A}+\mathrm{D} = rad\mathrm{A}_m$. Залежно від алгебри $\mathbf{L}$ одержано опис кубічних кілець.

Одногілковий випадок розгалужений: $\mathbf{L}$ є полем, максимальний ідеал кільця $\mathbf{A}_0$ дорівнює $\tau\mathbf{A}$, $\mathbf{A}/\tau\mathbf{A}$, $\mathbf{k}$ і $t\mathbf{A} = \tau^3\mathbf{A}$. Позначимо

$\mathrm{C}_{2r}(\alpha) = \mathrm{D} + t^r\alpha\mathrm{D} + t^{2r}\mathrm{A}$, де $v(\alpha) = 1$,

$\mathrm{C}_{2r}(\alpha) = \mathrm{D} + t^r\alpha\mathrm{D} + t^{2r+1}\mathrm{A}$, де $v(\alpha) = 2$.

Теорема 2.3.1. *Кожне надкільце* $\mathbf{A}_m$ *збігається з* $t^k\mathbf{C}_r(\alpha) + \mathbf{D}$ *для деяких* k, r, *таких, що* $r + k \le m$, *і деякого* α. *Кільця* $\mathbf{C}_r(\alpha)$ *є всіма плоскими особливостями алгебраїчних кривих у цьому випадку.*

Одногілковий випадок нерозгалужений: тут $\mathbf{L}$ є полем, максимальний ідеал $\mathbf{A}$ дорівнює $t\mathbf{A}$ і $\mathbf{A}/t\mathbf{A} = \mathbf{k}[\bar{\theta}]$ є кубічним розширенням поля $\mathbf{k}$, де $\bar{\theta}$ є коренем незвідного кубічного многочлена $f(x) \in \mathbf{k}[x]$. Позначимо $\mathbf{C}_r(\alpha) = \mathbf{D} + t^r\alpha\mathbf{D} + t^{2r}\mathbf{A}_0$, де $\alpha \in \mathbf{A}^\times \setminus \mathbf{D}$.

Теорема 2.3.2. *Кожне надкільце* $\mathbf{A}_m$ *збігається з* $t^k\mathbf{C}_r(\alpha) + \mathbf{D}$ *для певних* k, r, *таких, що* $2r + k \le m$, *і деякого* α. *Кільця* $\mathbf{C}_r(\alpha)$ *— це всі плоскі особливості алгебраїчних кривих у цьому випадку.*

Двогілковий випадок із розгалуженням: $\mathbf{L}=\mathbf{K}\times\mathbf{K}_1$, де $\mathbf{K}_1$ є квадратичним розширенням $\mathbf{K}$, $\mathbf{A} = \mathbf{D}_1 \times \mathbf{D}$ і $t\mathbf{D}_1 = \tau^2\mathbf{D}_1$, де τ — первинний елемент із $\mathbf{D}_1$. Нехай

$\mathbf{C}_{l,q}(\alpha) = \mathbf{D} + t^l(e + t^q\alpha)\mathbf{D} + t^r\mathbf{A}$, де $r = 2l + q$,

$\mathbf{C}_{2r+1}(\alpha) = \mathbf{D} + t^r\alpha\mathbf{D} + t^{2r+1}\mathbf{A}$.

Теорема 2.3.3. *Кожне надкільце кільця* $\mathbf{A}_m$ *збігається з* $t^k\mathbf{C}_{l,q}(\alpha) + \mathbf{D}$ *чи з* $t^k\mathbf{C}_r(\alpha) + \mathbf{D}$, *де* $k + r \le m$. *Кільця* $\mathbf{C}_{l,q}(\alpha)$ *і* $\mathbf{C}_r(\alpha)$ *є всіма плоскими особливостями кривих у цьому випадку.*

Двогілковий випадок без розгалуження: $\mathbf{L}=\mathbf{K}\times\mathbf{K}_1$, де $\mathbf{K}_1$ є квадратичним розширенням $\mathbf{K}$, $\mathbf{A} = \mathbf{D}_1 \times \mathbf{D} = \langle 1, e, \alpha \rangle$, максимальний ідеал кільця D_1 – це $t\mathbf{D}_1$ і $\mathbf{D}_1 / t\mathbf{D}_1 = \mathbf{k}[\bar{\theta}]$ є квадратичним розширенням поля $\mathbf{k}$, де $\bar{\theta}$ – це корінь незвідного квадратичного полінома $f(x) \in \mathbf{k}[x]$. У цьому випадку ми визначаємо, що $\mathbf{C}_{l,q}(\alpha) = \mathbf{D} + t^l(e_1 + t^q\alpha)\mathbf{D} + t^r\mathbf{A}$, де $2k + 2r$ і $\alpha \in \mathbf{D}_1 \setminus (e_1\mathbf{D} + t\mathbf{D})$. Тоді α може бути вибраний як $a\theta$, де θ це фіксований праобраз елемента $\bar{\theta}$ в $\mathbf{D}_1$ і $a \in \mathbf{D}$ єдиним чином визначається за модулем t^l.

Елементи {1, e, α} утворюють базу A_0. Отже, $\mathbf{C}_{l,q}(\alpha) = \mathbf{D} + t^l(e_1 + t^q\alpha)\mathbf{D} + t^r\mathbf{A}$.

Теорема 2.3.4. *Кожне надкільце кільця* $\mathbf{A}_m$ *збігається з одним із кілець* $t^k\mathbf{C}_{l,q}(\alpha)+\mathbf{D}$, *де* $k+r \le m$. *Кільця* $\mathbf{C}_{l,q}(\alpha)$ — *це всі плоскі особливості кривих у цьому випадку.*

Тригілковой випадок: $\mathbf{L}=\mathbf{K}^3$, $\mathbf{A}=\mathbf{D}^3$.

Ми визначаємо, що $\mathbf{C}_{l,q}(\alpha) = \mathbf{D} + t^l\alpha\mathbf{D} + t^r\mathbf{A}$, де $\mathbf{A} = \{1, e, e'\}$, причому $\alpha = e + t^q ae'$, $e \ne e'$ – два примітивні ідемпотенти в $\mathbf{A}$.

Теорема 2.3.5. *Кожне надкільце кільця* $\mathbf{A}_m$ *має форму* $t^k\mathbf{C}_{l,q}(\alpha)+\mathbf{D}$ *для деякого* α *і деяких* l, q *з* $k+r \le m$. *Кільця* $\mathbf{C}_{l,q}$ — *це всі плоскі особливості кривих у цьому випадку.*

Також у розділі 2 обчислено всі іделали і знайдено кількість параметрів у класах ідеалів.

Теорема 2.3.7. *Дуальні ідеали до кубічних кілець є такими:*

Випадок одногілковий із розгалуженням:

якщо $\mathbf{B} = \mathbf{D} + t^k\mathbf{C}_r(\alpha)$, *то* $\mathbf{B}^* = \mathbf{D} + t^{[r/2]}\alpha\mathbf{D} + t^{k+r}\mathbf{A}$.

Випадок одногілковий без розгалуження:

якщо $\mathbf{B} = \mathbf{D} + t^k\mathbf{C}_r(\alpha)$, *то* $\mathbf{B}^* = \mathbf{D} + t^{[r/2]}\alpha\mathbf{D} + t^{k+2r}\mathbf{A}$.

Випадок двогілковий із розгалуженням:

(a) Якщо $\mathbf{B} = \mathbf{D} + t^k\mathbf{C}_{l,q}(\alpha)$, *то* $\mathbf{B}^* = \mathbf{D} + t^l(e + t^q\alpha)\mathbf{D} + t^{k+2l+q}\mathbf{A}$.

(b) Якщо $\mathbf{B} = \mathbf{D} + t^k\mathbf{C}_r(\alpha)$, *то* $\mathbf{B}^* = \mathbf{D} + t^r\alpha\mathbf{D} + t^{k+2r+1}\mathbf{A}$.

Випадок двогілковий без розгалуження:

Якщо $\mathbf{B} = \mathbf{D} + t^k\mathbf{C}_{l,q}(\alpha)$, *то* $\mathbf{B}^* = \mathbf{D} + t^l(e + t^q\alpha)\mathbf{D} + t^{k+2l+q}\mathbf{A}$.

Випадок тригілковий:

Якщо $\mathbf{B} = \mathbf{D} + t^k\mathbf{C}_{l,q}(\alpha)$, *то* $\mathbf{B}^* = \mathbf{D} + t^r\alpha\mathbf{D} + t^{k+2r}\mathbf{A}$.

Також у цьому випадку знайдено критерій горенштейновості кубічних кілець.

Наслідок 2.3.2. *Кубічне кільце є горенштейновим тоді й тільки тоді, коли воно є плоскою особливістю кривої.*

Нагадаємо, що для інших особливостей це не завжди правильно.

Для кілець геометричної природи, тобто у випадку, коли **D**=k[[x]] (кільце формальних степеневих рядів наж полем), визначено найбільшу кількість параметрів $par\,(C)$ у сім'ях ідеалів. Зауважимо, що для таких кілець нерозгалужені випадки неможливі.

Теорема 2.4.1. *Якщо* $\mathbf{C}$ *є кубічним кільцем геометричної природи, то* $\mathrm{par}(\mathbf{C}) \le n$ *тоді і тільки тоді, коли* $\mathbf{C}$ *домінує одну з особливостей типу* $E_{12n+i}\ (6 \le i \le 8)$ *чи* $E_{2n+1,q}\ \ q \ge 0$.

У 3-му розділі сформульовано теорему, яка дає критерій того, що найбільша кількість параметрів *par(S)* у сім'ях ідеалів одногілкової особливості *S* не перебільшує 2 (критерій двопараметричності ідеалів).

Основний результат роботи сформульвано у подальшій теоремі.

Основна теорема. *Нехай* S *є одногілковою особливістю. Тоді еквівалентними є такі умови:*

1) $par(\mathrm{S}) \le 2$.

2) Якщо $char\,\mathrm{k} \ne 2$, *то* S *домінує одну з таких особливостей:* $E_{30}, E_{32}, W_{24}, W_{2^*}^{\#}, W_{30}, N_{20}, N_{24}, N_{28}$;

2а) Якщо $char\,\mathrm{k} = 2$, *то* S *домінує одну з таких особливостей:* $E_{30}, E_{32}, W_{18}, W_{1,*}^{\#}, N_{20}, N_{24}$.

Розділ 3 присвячений вивченню особливостей кривих типу W .

Для особливостей типу *E* це випливає з результатів розділу 2. У розділі 3 основна теорема доведена для особливостей типу *W*.

Теорема 3.2.1. *Одногілкова особливість* S *типу W допускає щонайбільше 2-параметричні сімейства ідеалів тоді й лише тоді, коли вона домінує плоску особливість типу* $W_{24}, W_{30}, W_{2,2q-1}^{\#}$.

Розділ 4 присвячений дослідженню особливостей типу *N*.

Означення 4.1.1. *Особливістю типу* ***N*** *називається одногілкова особливість, тобто підалгебра K в k*[[*t*]] *така, що найменший показник, який зустрічається в елементах з K, є 5. Очевидно, тоді можна вважати, що* $t^5 \in K$. *Якщо це – плоска особливість із вектором нормування (5,k+1), вона називається особливістю типу* N_{4k}.

У розділі 4 також доведено критерій двопараметричності ідеалів для особливостей типу *N*.

Теорема 4.1.1. *Якщо* $char\,\mathrm{k} \ne 2$, *то одногілкова особливість типу N має не більше, ніж 2-параметричні сім'ї ідеалів тоді й тільки тоді, коли вона домінує особливість типу* N_{4k} *при* $k \le 7$. *Якщо* $char\,\mathrm{k} = 2$, *то* N *повинна домінувати одну з особливостей* N_{20}, N_{24}.

Теорема 4.1.2. Нижче наведено K_2-ідеали, які не є K_1-ідеалами і є впорядкованими за порядком, індукованим K_3-ідеалами. При цьому позначатимемо $I' = IK_3$.

Тут також явно обчислені ідеали для двопараметричного випадку.

Зауважимо, що в дисертації всі обчислення проводяться для випадку, коли $char\,\mathrm{k} \neq 2$. Випадок, коли $char$k=2, є цілком аналогічним, навіть простішим, оскільки треба розглядати менше випадків.

Розділ 5 дисертації присвячено новому методові побудови нормального базису у скінченному полі, який у класі детермінованих алгоритмів має найкращу побітову оцінку складності $O(n^3 \log_2 p)$. У випадку побудови нормального базису передбачається, що поле F_q уже задано. Тобто вже знайдено деякий незвідний над F_p многочлен P(x) степені n (де n – таке, що $p^n = q$). Задача методу пошуку нормального базису полягає лише в тому, щоб при готовій структурі поля F_q (при готовому поліноміальному базисі) знайти елемент, який породжує нормальний базис.

Для знаходження оператора A піднесення до степеня треба знайти представлення елементів $1^p, \alpha^p, \left(\alpha^2\right)^p, ..., \left(\alpha^{n-1}\right)^p$ у поліноміальному базисі $1, \alpha, \alpha^2, ..., \alpha^{n-1}$, тобто обчислити лишки від ділення за модулем $P\left(x\right)$: $x^p \bmod P(x), \ldots, x^{2p} \bmod P(x), \ldots, x^{(n-1)p} \bmod P(x)$.

Основні кроки нашого алгоритму побудови нормального базису:

1) Обираємо поліноміальний базис для F_q.

2) Будуємо оператор A: $Af = f^q$.

3) Зводимо матрицю оператора A методом триангуляції до форми Фробеніуса або, якщо цей метод не дає змоги це зробити, то зводимо її до блоково-Фробенісової форми зі клітинами Фробеніуса по діагоналі.

4) У другому випадку з п.3 після отримання матриці виду блоково-діагонального виду, де блоки на діагоналі — це клітини Фробеніуса, потрібно послідовно поєднати сусідні блоки методом заміни твірних векторів, що детально описано у цьому розділі.

ВИСНОВКИ

Дисертація присвячена дослідженню ідеалів комутативних кілець, зокрема питанням параметризації сімей ідеалів.

У дисертації одержано такі нові наукові результати:

1. Описано локальні кубічні кільця і їхні ідеали. Встановлено, що кубічне кільце є горенштейновим тоді й тільки тоді, коли воно є плоскою

особливістю. У геометричному випадку знайдено кількість параметрів, які визначають ідеали кубічного кільця, і встановлено зв'язок цих результатів зі класифікацією особливостей за В. Арнольдом.

2. Доведено, що одногілкова особливість алгебраїчної кривої над алгебраїчно замкненим полем має щонайбільше двопараметричні сім'ї ідеалів тоді й тільки тоді, коли вона домінує одну з таких плоских особливостей:

- Якщо характеристика поля не дорівнює 2, то

$E_{30}, E_{32}, W_{24}, W_{2^*}^{\#}, W_{30}, N_{20}, N_{24}, N_{28}$.

- Якщо характеристика поля дорівнює 2, то

$E_{30}, E_{32}, W_{18}, W_{1,*}^{\#}, N_{20}, N_{24}$.

3. Повністю описано ідеали перерахованих плоских особливостей.

4. Розроблено новий алгоритм побудови нормального базису у скінченному полі з оцінкою ефективності порядку $O(n^3)$, де число елементов поля дорівнює p^n.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1) *Скуратовський Р. В.* "Особливості плоских алгебраїчних кривих типу N." / Р. В. Скуратовський // Вісник КНУ ім. Тараса Шевченка, серія фізико-математичні науки. – 2012. – Вип. 1. – С. 33-40.

2) *Скуратовський Р. В.* Побудова нормального базису скінченного поля за детермінований поліноміальний час / *Р. В. Скуратовський* // Вісник механіко-математичного факультету КНУ ім. Тараса Шевченка: Математика. Механіка. – 2011. – Вип. 25. – С. 49-54.

3) *Skuratovskii R.V.* Ideals of one branch curve singularities of type *W.* / Skuratovskii R.V.// Ukrainian Math. J. – 62, №. 4 – 2010. – С. 530-536.

4) *Drozd Y.A., Skuratovskii R.V.* Cubic rings and their ideals (in Ukraniane) / *Y. Drozd* // Ukr. Mat. Zh. – 2010.– V. 62, №11, – P. 464-470. (arXiv:1001.0230 [math.AG])

5) *Drozd Y., Skuratovskii R.* One branch curve singularities with at most 2-parameter families of ideals./ *Y. Drozd //* Algebra and Discrete Math. 13, №.2 – 2012. – 209-219. (arXiv 1201.6579 [math.AC]).

6) *Скуратовський Р.В.* Ідеали одногілкових особливостей степеня 5. Шевченківська весна Частина 1. Київ. – 2012. – С. 43.

7) *Скуратовський Р.В.* Нормальні базиси скінченного поля і їх властивості. Всеукраїнська наукова конференція «Сучасні наукові проблеми математики у вищій школі», присвячена Левіщенко С.С., НПУ ім. М. П. Драгоманова, 7-8 жовтня. – 2016. – С. 78 www.fmi.npu.edu.ua/ua/levischenko-conf

8) *Скуратовський Р.В.* "One branch curve singularities with at most 2-parameter families of ideals". Конференція молодих учених із сучасних проблем механіки і математики імені академіка **Я.** С. ПІДСТРИГАЧА КМУ СПММ–2011.– **С.** 273. http://iapmm.lviv.ua/cpmm2011/

9) *Скуратовський Р. В*. Про ідеали одногілкових кривих. Міжнародна наукова конференція молодих вчених, присвяченій 70-річчю механіко-математичного факультету Київського національного університету імені Тараса Шевченка, м. Київ, – 2010 р. –С. 37

10) *Скуратовський Р. В*. *Мовчан А.А.* Дослідження особливостей скручених кривих Едвардса над F_p. П'ята всеукраїнська наукова конференція молодих вчених "Актуальні проблеми сучасної математики та фізики".– 2016. – С. 56.

11) *Скуратовський Р. В.* "Двопараметричні особливості одногілкових алгебраїчних кривих". Сучасні проблеми механіки та математики. Збірник наукових праць у 3-х т. / за заг. ред. А.М. Самойленка та Р.М. Кушніра [Електронний ресурс] // Інститут прикладних проблем механіки і математики ім. Я.С. Підстригача НАН України. – 2018. – Т. 3. – Режим доступу до ресурсу: www.iapmm.lviv.ua/mpmm2018.

12) *Popovych R. B., Skuratovskii R. V.* Normal bases and elements of high order in finite field extensions based on cyclotomic polynomials. The 11th International Algebraic Conference in Ukraine dedicated to the 75th anniversary of V. V. Kirichenko. – 2017. – at Taras Shevchenko National University of Kiev (Kiev, Ukraine). https://www.imath.kiev.ua/~algebra/iacu2017/

13) *Skuratovskii R.* "A criterion for two-modality of ideals for one branch one-dimensional singularities of type W". 7th International Algebraic Conference in Ukraine. "Ukrainian mathematical congress". Ukraine. 18 - 23 August, – 2009.– P. 132.

АНОТАЦІЇ

Скуратовський Р. В. Ідеали бімодальних особливостей плоских кривих – кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня кандидата фізико-математичних наук за спеціальністю 01.01.06. – Алгебра і теорія чисел. –

Міжрегіональна академія управління персоналом. – Інститут математики НАН України, Київ, 2019.

Вивчення ідеалів кілець є класичним розділом комутативної алгебри, який розпочався під впливом теорії чисел і алгебраїчної геометрії, а у XX сторіччі у роботах Е. Нетер, Е. Артіна, А. Шпайзера та інших сформувався як самостійний напрямок. Якщо для цілозамкнених (неособливих) кілець ця теорія набула повноти й завершеності, то для кілець із особливостями залишається багато невирішених питань. Зокрема, це питання про кількість і будову класів ідеалів. Перші результати тут одержали Д. Фаддєєв і З. Боревич для квадратичних кілець, вони ж і Х. Басс дослідили ширший і загальніший клас кілець, які відомі зараз як бассові. А саме, науковці встановили, що для таких кілець будь-який ідеал є обертовним (над своїм кільцем множників). Надалі Д. Фаддєєв показав, що для кубічних кілець кожен ідеал локально є або обертовним, або дуальним до обертовного, а Ю. Дрозд узагальнив цей результат для широкого класу кілець. Г. Якобінський, Ю. Дрозд і В. Ройтер дали критерій того, що кільце має скінченну кількість класів ідеалів. У роботах Ґ.-М. Гройеля, Г. Кнеррера, Ю. Дрозда й А. Шапперта були встановлені зв'язки цих питань зі класифікацією особливостей за В. Арнольдом, зокрема показано, що особливості зі скінченною кількістю класів ідеалів – це ті, які домінують прості особливості у розумінні В. Арнольда, а особливості з однопараметричними сім'ями ідеалів – це ті, які домінують унімодальні або бімодальні особливості. Подальші дослідження в цьому напрямку, яким і присвячена дисертація, є перспективними й важливими як для самої теорії ідеалів, так і для теорії особливостей і суміжних розділів алгебраїчної геометрії.

Основні результати дисертації пов'язані зі класифікацією кубічних кілець і особливостей зі двопараметричними сім'ями ідеалів. У першому розділі дано огляд теорії ідеалів і наведено відомі технічні результати, які використовуються в роботі. У другому розділі розглядаються кубічні кільця, тобто розширення дедекіндового кільця, які містяться в кубічному розширенні його поля часток. Саме тут дано повний опис локальних кубічних кілець, а також їхніх ідеалів. Зокрема у геометричному випадку, тобто для локальних кілець алгебраїчних кривих над алгебраїчно замкненим полем, обчислено максимальну кількість параметрів у сім'ях ідеалів. Саме ця кількість не перебільшує n тоді й тільки тоді, коли це кільце домінує одну зі плоских особливостей E_{12n+i} $(6 \le i \le 8)$ чи $E_{2n+i,q}$ $(q \ge 0)$.

У розділах 3 і 4 знайдено критерій двопараметричності сімей ідеалів для одногілкових особливостей алгебраїчних кривих. Відповідь також формулюється в термінах домінування і класифікації за Арнольдом. Оскільки для особливостей типу T це завжди так, а для особливостей E випливає з

результатів розділу 2, у розділі 3 розглянуті особливості типу *W*, а в розділі 4 – типу *N*. У двопараметричному випадку дано повний опис усіх ідеалів і їхніх структур.

У розділі 5 викладено метод побудови нормального базису для скінченного поля.

Ключові слова: локальне кільце, сім'ї ідеалів, плоска особливість, кубічне кільце, скінченне поле, нормальна база.

Skuratovskii R.V. Ideals of bimodal singularities of plain curves. – Qualificational scientific work on the rights of the manuscript.

Dissertation for obtaining the degree of candidate of physical and mathematical sciences (doctor of philosophy) for the specialty 01.01.06 – algebra and theory of numbers (111 - mathematics). Interregional Academy of Personnel Management. – Ministry of Education and Science of Ukraine. – Institute of Mathematics, NAS of Ukraine, Kyiv, 2019.

The study of ideals of rings is a classical branch of the commutative algebra, which began under the influence of the theory of numbers and algebraic geometry, and in the 20th century, in works of E. Noeter, E. Artin, A. Speiser and others, formed an independent area.

For the integrally closed (non-special) rings, this theory has gained completeness, whereas for rings with singularities there are many unsolved problems. In particular, this is the question of the number and structure of classes of ideals. The first results here were obtained by D. Faddeev and Z. Borevich for quadratic rings, and by them and H. Bass for a wide class of rings, now known as bassian. It was found that for any such rings any ideal is invertible (over its ring of multipliers). Later, D. Faddeev showed that for each cubic ring, each ideal is either invertible or dual to invertible, and Yu. Drozd summed this result for a wide class of rings. G. Jakobinsky, Yu. Drozd and A. Roiter gave the criterion that the ring has a finite number of classes of ideals. In the work of G.-M. Greuel and G. Knoerrer the relations with the classification of singularities by V. Arnold were established, in particular, it was shown that a singularities with a finite number of classes of ideals are those which dominate simple singularities in the sense of Arnold. For singularities with only one-parameter families of ideals Schappert, Drozd and Greuel showed that they are those which dominate unimodal or bimodal singularities. Further research in this direction, to which is devoted the dissertation, is promising and important both for the theory of ideals itself and for the theory of singularities and related branches of algebraic geometry.

The main results of the dissertation are related to the classification of cubic rings and singularities with two-parameter families of ideals. The first branch gives an overview of the theory of ideals and provides the famous technical results

used in the work. In the second branch, cubic rings are considered, that is, the extensions of a local dedekind ring contained in a cubic expansion of its field of fractions. It is here that a complete description of local cubic rings is given, as well as of their ideals. In particular, in the geometric case, that is for local rings of algebraic curves over an algebraically closed field, the maximum number of parameters in the families of ideals is calculated. Namely, it is at most *n* if and only if this ring dominates one of the plane curve singularities E_{12n+i} $(6 \le i \le 8)$ or $E_{2n+i,q}$ $(q \ge 0)$.

The following two branches are devoted to the criterion that a one-branch singularity of an algebraic curve has at most two-parameter families of ideals. In Section 3 the main result is formulated that connects this question with the classification of singularities by V. Arnold. Namely, it is proved that a one branch singularity has at most two-parameter families of ideals if and only if one of the following conditions hold:

1) $char\,\mathrm{k} \neq 2$ and S dominants one of the following singularities:

E_{30}, $E_{32}, W_{24}, W_{2*}^{\#}, W_{30}, N_{20}, N_{24}, N_{28}$;

2) $char\,\mathrm{k} = 2$ and S dominants one of the following singularities:

E_{30}, $E_{32}, W_{18}, W_{1,*}^{\#}, N_{20}, N_{24}$;

So it turns out that only the singularities that dominate plane curve singularities of types *E, T, W* or *N* can have at most two-parameter families of ideals.

Since for singularities that dominate those of type *T* it is always the case, and for type E the answer follows from the results of section 2, the third section deals with the singularities of the type *W*, and the fourth with the singularities of type *N*. Altogether it gives the proof of the main theorem.

Finally, the fifth section is devoted to the problem of constructing a normal base in a finite field. It is important for computer computations in finite fields, in particular, is related to the coding theory and cryptography. Here is an algorithm that builds a normal base for the order of time $O(n^3 \log^2 p)$ if the number of elements in the field is p^n.

Key words: local ring, family of ideals, flat feature, cubic ring, finite field, normal base.

Скуратовский Р. В. Идеалы бимодальных особенностей плоских кривых. – Квалификационный научный труд на правах рукописи.

Диссертация на соискание учёной степени кандидата физико-математических наук по специальности 01.01.06. – Алгебра и теория чисел. –

Межрегиональная академия управления персоналом. – Министерство образования и науки Украины. – Институт математики НАН Украины, Киев, 2019.

Изучение идеалов колец является классическим разделом коммутативной алгебры, который начался благодаря влиянию теории чисел и алгебраической геометрии, а в XX веке в работах Э. Нётер, Е. Артина, А. Шпайзера и других сформировался как самостоятельное направление. Если для целозамкнутых (неособенных) колец эта теория достигла полноты и завёршенности, то для колец с особенностями остаётся много нерешённых вопросов. В частности, это вопрос о количестве и строении классов идеалов. Первые результаты тут были получены Д. Фаддеевым и З. Боревичем для квадратичных колец, ими же и Х. Бассом для широкого класса колец, известных сейчас как бассовые.

А именно, было установлено, что для таких колец любой идеал является обратимым (над своим кольцом множителей). В дальнейшем Д. Фаддеев показал, что для кубических колец каждый идеал локально является или обратимым, или дуальным к обратимому, а Ю. Дрозд обобщил этот результат для широкого класса колец. Г. Якобинский, Ю. Дрозд и А. Ройтер дали критерий того, что кольцо имеет конечное число классов идеалов.

В работах Ґ.-М. Гройеля и Г. Кнеррера, А. Шапперта, Ю. Дрозда были установлены связи этих вопросов с классификацией особенностей по В. Арнольду, в частности, показано, что особенности с конечным числом классов идеалов – это те, которые доминируют простые особенности в понимании В. Арнольда, а особенности с однопараметрическими семьями идеалов – это те, которые доминируют унимодальные или бимодальные особенности.

Дальнейшие исследования в этом направлении, которым и посвящена диссертация, являются перспективными и важными как для самой теории идеалов, так и для теории особенностей и смежных разделов алгебраической геометрии.

Основные результаты диссертации связаны с классификацией кубических колец и особенностей с двухпараметрическими семействами идеалов. В первой главе дан обзор теории идеалов и приведены известные технические результаты, которые используются в работе.

Во второй главе рассматриваются кубические кольца, то есть расширения дедекиндового кольца, содержащиеся в кубическом расширении его поля частных.

Именно здесь дано полное описание локальных кубических колец, а также их идеалов. В частности, в геометрическом случае, то есть для локальных колец алгебраических кривых над алгебраически замкнутым

полем, вычислено максимальное количество параметров в семьях идеалов. Именно это количество не превышает n тогда и только тогда, когда это кольцо доминирует одну из плоских особенностей E_{12n+i} $(6 \le i \le 8)$ или $E_{2n+i,q}$ $(q \ge 0)$.

В главах 3 и 4 доказывется критерий того, что особенности алгебраических кривых с одной ветвью имеют не более, чем двухпараметрические семейства идеалов. Ответ также даётся в терминах доминирования и классификации Арнольда. Поскольку для особенностей типа T это всегда так, а для особенностей типа E это следует из результатов второй главы, в главе 3 рассмотрены особенности типа W, а в главе 4 – типа N. В двухпараметрическом случае дано полное описание всех идеалов.

В главе 5 излагается метод построения нормального базиса для конечного поля.

Ключевые слова: локальное кольцо, семьи идеалов, плоская особенность, кубическое кольцо, конечное поле, нормальный базис.

Підп. до др. 25.01.2019 р. Формат 60 84/16. Папір офс. Офс. друк.
Умов. друк. арк. 0,9. Фіз. др. арк. 1,0. Тираж 60 прим. Зам. № 30

Інститут математики НАН України, 01004, м. Київ - 4, вул. Терещенківська, 3.