

На правах рукопису
Національна академія наук України
Інститут математики

РАЄВСЬКА Марина Юріївна

УДК 512.6

**Локальні майже-кільця з деякими
обмеженнями на мультиплікативні
групи та підгрупи необоротних
елементів, і пов'язані з ними
структури**

01.01.06 — алгебра та теорія чисел

Дисертація
на здобуття наукового ступеня
доктора фізико-математичних наук

Дисертація містить результати власних досліджень.

Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело. М. Ю. Раєвська



Науковий консультант
професор, доктор фіз.-мат. наук
СИСАК Ярослав Прокопович
Київ — 2026

Анотація

Раєвська М. Ю. Локальні майже-кільця з деякими обмеженнями на мультиплікативні групи та підгрупи необоротних елементів, і пов'язані з ними структури. — Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора фізико-математичних наук за спеціальністю 01.01.06 — “алгебра та теорія чисел”. — Інститут математики Національної академії наук України, Київ, 2026.

Дисертацію присвячено вивченню локальних майже-кілець з деякими обмеженнями на мультиплікативні групи та підгрупи необоротних елементів, класифікації локальних майже-кілець та дослідженню їх адитивних груп.

У вступі обґрунтовано актуальність теми дисертації, сформульовано мету та завдання дослідження, наукову новизну одержаних результатів.

Розділ 1 складається з чотирьох підрозділів 1.1, 1.2, 1.3 та 1.4. У розділі 1 наведено огляд літератури за темою дисертації. Підрозділ 1.1 присвячено огляду відомих результатів про майже-поля. Систематичне вивчення скінченних майже-полів було започатковано Цассенхаузом, де доведена абелевість їх адитивної групи та охарактеризовано їх мультиплікативні групи як групи регулярних автоморфізмів абелевих груп. В роботі Лая мультиплікативна група майже-поля названа спадковою, якщо кожна її підгрупа ізоморфна мультиплікативній групі деякого майже-поля, та отримано повну характеристизацію скінченних таких груп майже-полів. У подальшому майже-поля вивчалися головним чином завдяки їх застосуванням у геометрії. Вперше майже-поля застосували в геометрії Веблен і Вадербарн. Теорії майже-полів присвячено монографію Виглінга, в якій систематизовано більшість результатів про майже-поля. У підрозділі 1.2 зроблено огляд результатів про майже-кільця з одиницею. Проблема ви-

значення класів груп, які можуть бути адитивними або мультиплікативними групами майже-кілець з одиницею, є важливою з точки зору як теорії груп, так і теорії майже-кілець. Однак, наразі ця проблема вивчена досить мало. З цієї причини розробка нових методів теорії майже-кілець (зокрема, локальних у випадку, коли множина необоротних елементів є адитивною підгрупою) видається важливою та сприяє їх класифікації. Різні класи груп не можуть бути адитивними групами майже-кілець з одиницею. Клей та Малон довели, що проста група складеного порядку не може бути адитивною групою майже-кілець з одиницею. Лай розширює цей результат, а саме, показує, що скінченна неабелева група з рівно однією нетривіальною власною нормальною підгрупою не може бути адитивною групою майже-кілець з одиницею. Клей визначив усі майже-кільця з одиницею на $(D_4, +)$. Джонсон розглянув майже-кілець, визначені на $(D_n, +)$, дієдральній групі порядку $2n$ та показав, що якщо $(D_n, +, \cdot)$ є майже-кільцем з мультиплікативною одиницею, то нормальні праві підмодулі та праві ідеали $(D_n, +, \cdot)$ збігаються тоді і тільки тоді, коли всі нормальні праві підмодулі є ануляторними правими ідеалами. Доведено існування майже-кільця з мультиплікативною одиницею на $(D_n, +)$, де $n = 2p$, p — просте число. Показуємо, що якщо p — непарне просте число, то існує, з точністю до ізоморфізму, єдине майже-кілець з мультиплікативною одиницею на $(D_n, +)$. Кріммел також (незалежно) зауважив, що існує, з точністю до ізоморфізму, єдине майже-кілець з мультиплікативною одиницею на $(D_n, +)$, $n = 2q$. У підрозділі 1.3 дано огляд результатів про локальні майже-кільця. Кілець з одиницею, множина всіх необоротних елементів якого утворює ідеал в цьому кільці, називається локальним кільцем. Як легко переконатися, в означенні локального кільця достатньо насправді припускати, що множина всіх необоротних елементів є тільки підгрупою адитивної групи кільця. Замінивши в ньому слово “кілець” на “майже-кілець”, отримуємо означення

локальних майже-кілець, вивчення яких вперше було ініційовано Мексоном. В цій же статті встановлено, що адитивна група скінченного нуль-симетричного локального майже-кілля є p -групою. Мексон показав, що з точністю до ізоморфізму існує $p - 1$ локальне майже-кілля з елементарною абелевою адитивною групою порядку p^2 , в яких підгрупи необоротних елементів мають порядок p , тобто тих майже-кілець, які не є майже-полями. Разом із фундаментальною роботою Цассенхауза про майже-поля та роботою Клея та Малоне, отримано повний опис усіх нуль-симетричних локальних майже-кілець порядку p^2 . Мексон показав, що кожна нециклічна абелева p -група порядку $p^n > 4$ є адитивною групою нуль-симетричного локального майже-кілля, яке не є кіллям. Однак у випадку скінчених неабелевих p -груп ситуація інша. Наприклад, ні узагальнена група кватерніонів, ні неабелева група порядку 8 не можуть бути адитивною групою локального майже-кілля. Локальні майже-кілля, мультиплікативні групи яких є абелевими, і які не є кіллями, вивчались Городником [42]. Ним доведено, що множина всіх необоротних елементів такого майже-кілля утворює абелеву підгрупу індексу 2 в його адитивній групі. Зокрема, він описав локальні майже-кілля з циклічними групами одиниць. А саме, якщо мультиплікативна група локального майже-кілля є циклічною, то адитивна група є або групою типу $(2, 2, 2)$, або $(2, 4)$. Амберг, Хуберт, Сисак досліджувалися локальні майже-кілля з мультиплікативною групою діедра та було доведено, що кожне локальне майже-кілля з мультиплікативною групою діедра є скінченим з адитивною групою, яка є або 3-групою порядку не вище 9, або 2-групою порядку не вище 32. Опис таких майже-кілець був продовжений в дисертації Хуберта [45], зокрема, було встановлено, що якщо мультиплікативна група локального майже-кілля є групою діедра, то порядок цього майже-кілля не перевищує 16. Сисак і Ді Терміні [116] показали, що якщо R є локальним майже-кіллям (не обов'язково

нуль-симетричним), мультиплікативна група якого є узагальненою групою кватерніонів, то мультиплікативна група є або групою кватерніонів порядку 8, або узагальненою групою кватерніонів порядку 16 з абелевими адитивними групами наступних типів: $(3, 3)$, $(2, 2, 2, 2)$, $(2, 2, 4)$, $(2, 2, 2, 2, 2)$ та $(2, 2, 2, 4)$.

У підрозділі 1.4 наведені результати, що стосуються систему комп'ютерної алгебри GAP та пакет SONATA. Цей підрозділ складається з чотирьох підпунктів, де описано Бібліотека SmallGroups 1.4.1, Пакет SONATA 1.4.2, Класифікація майже-кілець з одиницею 1.4.3 та локальних майже-кілець 1.4.4.

Розділ 2 складається з семи підрозділів 2.1, 2.2, 2.3, 2.4, 2.5, 2.6 та 2.7. В цьому розділі описано локальні майже-кілець з деякими обмеженнями на їх структуру. У підрозділі 2.1 наведено допоміжні означення та твердження, що стосуються локальних майже-кілець, нільпотентних груп, груп Шмідта, груп Міллера–Морено. У підрозділах 2.2, 2.3, 2.4 та 2.5 отримано результати про локальні майже-кілець з нільпотентною мультиплікативною групою, мультиплікативними групами Шмідта, мультиплікативними групами Міллера–Морено та локальні майже-кілець на скінченних p -групах з циклічними підгрупами індексу p , відповідно. У підрозділі 2.6 досліджуються скінченні майже-кілець з одиницею з моногенною напівгрупою необоротних елементів. У підрозділі 2.7 описано локальні майже-кілець, отримані з бібліотеки пакету SONATA.

Розділ 3 складається з п'яти підрозділів 3.1, 3.2, 3.3, 3.4 та 3.5. В цьому розділі досліджуються локальні майже-кілець на скінченних неабелевих 2-породжених p -групах. У підрозділі 3.1 наведено класифікацію скінченних неабелевих 2-породжених p -груп з циклічним комутантом. У підрозділі 3.2 описано скінченні локальні майже-кілець з розщепленою метациклічною адитивною групою. Цей підрозділ складається з семи підпунктів, а саме 3.2.1, 3.2.2, 3.2.3, 3.2.4, 3.2.5, 3.2.6 та 3.2.7. У підрозділі 3.3

вивчені локальні майже-кілець на групах типу $(B.1)$. Групи $(C.1)$, $(B.2)$ та $(C.2)$ описано в підрозділах 3.4 та 3.5.

Напівдистрибутивні майже-кілець з одиницею та локальні майже-кілець досліджено в розділі 4. Цей розділ складається з двох підрозділів 4.1 та 4.2. У підрозділі 4.1 описано дистрибутивні та напівдистрибутивні майже-кілець з одиницею. Цей підрозділ складається з трьох підпунктів 4.1.1, 4.1.2 та 4.1.3. У підрозділі 4.2 вивчено скінченні напівдистрибутивні локальні майже-кілець.

Розділ 5 складається з п'яти підрозділів 5.1, 5.2, 5.3 та 5.4. В цьому розділі досліджено майже-кілець брейси та локальні майже-кілець. У підрозділі 5.1 наведено результати про брейси та косі брейси. Брейси та косі брейси з пакету YangBaxter охарактеризовано в підрозділах 5.2 та 5.3. У підрозділі 5.4 дано деякі результати про майже-кілець брейси.

Розділ 6 складається з трьох підрозділів 6.1, 6.2 та 6.3. У цьому розділі наведено використання системи комп'ютерної алгебри GAP для побудови та вивчення недистрибутивних алгебраїчних структур, а саме алгоритм побудови скінченних локальних майже-кілець 6.1 та функції для майже-кілець 6.2 і груп 6.3 з пакету LocalNR.

Класифікація локальних майже-кілець малих порядків та ендоециклічні групи описані у розділі 7. Цей розділ складається з двох підрозділів 7.1 та 7.2. У підрозділі 7.1 отримано класифікацію локальних майже-кілець малих порядків. А саме, локальних майже-кілець порядку 64 7.1.1, 81 7.1.2, 243 7.1.3, 343 7.1.4 та 343 7.1.4. У підрозділі 7.2 вивчено ендоециклічні групи та локальні майже-кілець.

Ключові слова: Майже-кілець з одиницею, локальне майже-кілець, мультиплікативна група, підгрупа необоротних елементів, нільпотентна група, група Шмідта, група Міллера-Морено, GAP, SONATA, LocalNR.

Abstract

Raievska M.Iu. Local nearrings with some restrictions on multiplicative groups and subgroups of non-invertible elements, and related structures. — Qualifying scientific work on the rights of the manuscript.

Thesis for the degree of Doctor of Physical and Mathematical Sciences, speciality 01.01.06 “Algebra and Number Theory”. — Institute of Mathematics of National Academy of Sciences of Ukraine, Kyiv, 2026.

The thesis is devoted to the study of local nearrings with some restrictions on multiplicative groups and subgroups of non-invertible elements, the classification of local nearrings and the study of their additive groups.

The introduction substantiates the relevance of the thesis topic, formulates the goal and objectives of the research, and the scientific novelty of the results obtained.

Section 1 consists of four subsections 1.1, 1.2, 1.3 and 1.4. Section 1 provides a review of the literature on the topic of the thesis. Subsection 1.1 is devoted to a review of known results on nearfields. The systematic study of finite nearfields was initiated by Zassenhaus, who proved that their additive group is Abelian and characterized their multiplicative groups as groups of regular automorphisms of abelian groups. In Ligh’s work, the multiplicative group of a nearfield is called hereditary if each of its subgroups is isomorphic to the multiplicative group of some nearfield, and a complete characterization of finite such groups of nearfields was obtained. Subsequently, nearfields were studied mainly due to their applications in geometry. Nearfields were first used in geometry by Veblen and Waderbarn. The theory of nearfields is the subject of a monograph by Wähling, in which most of the results on nearfields are systematized.

In subsection 1.2, a review of results on nearrings with identity is given. The notion of nearrings is quite natural because, e.g., all transformations of an arbitrary group form a nearring. Moreover, every group can be transformed into a nearring. In particular, it is an additive group of a certain nearring but not a nearring with identity. The problem of defining classes of groups that can be additive or multiplicative groups of nearrings with identity is important from the point of view of both group theory and nearring theory. However, this problem has been studied quite little so far. For this reason, the development of new methods of nearring theory (in particular, local methods in the case when the set of non-invertible elements is an additive subgroup) seems important and contributes to their classification. Different classes of groups that cannot be additive groups of nearrings with identity are studied. Clay and Malone proved that a simple group of composite order cannot be an additive group of nearrings with identity. Lai extends this result, namely, he shows that a finite non-Abelian group with exactly one non-trivial proper normal subgroup cannot be the additive group of nearrings with identity. Clay defined all nearrings with identity on $(D_4, +)$. Johnson considered nearrings defined on $(D_n, +)$, a dihedral group of order $2n$, and showed that if $(D_n, +, \cdot)$ is a nearring with multiplicative identity, then the normal right submodules and right ideals of $(D_n, +, \cdot)$ coincide if and only if all normal right submodules are annihilating right ideals. He proved the existence of a nearring with multiplicative identity on $(D_n, +)$, where $n = 2p$, p — a prime number. It is shown that if p is an odd prime, then there exists, up to isomorphism, a unique nearring with identity on $(D_n, +)$. Krimmel also (independently) observed that there exists, up to isomorphism, a unique nearring with identity on $(D_n, +)$, $n = 2q$.

In subsection 1.3, a review of results on local nearrings is given. A ring with identity whose set of all non-invertible elements forms an ideal in this ring is called a local ring. As is easy to see, in the definition of a local ring it

is actually sufficient to assume that the set of all non-invertible elements is just a subgroup of the additive group of the ring. Replacing the word “ring” in it with “nearring”, we obtain the definition of local nearrings, the study of which was first initiated by Maxson. In the same paper it was established that the additive group of a finite zero-symmetric local nearring is a p -group. Maxson showed that up to isomorphism there exists $p - 1$ local nearring with an elementary Abelian additive group of order p^2 , in which the subgroups of non-invertible elements have order p , i.e. those nearrings that are not nearfields. Together with the fundamental work of Zassenhaus on nearfields and the work of Clay and Malone, a complete description of all zero-symmetric local nearrings of order p^2 is obtained. Maxson showed that every non-cyclic Abelian p -group of order $p^n > 4$ is the additive group of a zero-symmetric local nearring that is not a ring. However, in the case of finite non-Abelian p -groups the situation is different. For example, neither the generalized group of quaternions nor the non-Abelian group of order 8 can be the additive group of a local nearring. Therefore the structure of the non-abelian finite p -groups which are the additive groups of local nearrings is an open problem.

Local nearrings whose multiplicative groups are Abelian and which are not rings were studied by Gorodnik [42]. He proved that the set of all non-invertible elements of such a nearring forms an Abelian subgroup of index 2 in its additive group. In particular, he described local nearrings with cyclic groups of units. Namely, if the multiplicative group of a local nearring is cyclic, then the additive group is either a group of type $(2, 2, 2)$ or $(2, 4)$. Amberg, Hubert, Sysak studied local nearrings with a multiplicative group of the dihedral and proved that every local nearring with a multiplicative group of the dihedral is finite with an additive group that is either a 3-group of order not higher than 9 or a 2-group of order not higher than 32. The description of such nearrings was continued in Hubert’s dissertation [45], in particular, it was established that if the multiplicative group of a local nearring is a

dihedral group, then the order of this nearring does not exceed 16. Sysak and Di Termini [116] showed that if R is a local nearring (not necessarily zero-symmetric) whose multiplicative group is a generalized quaternion group, then the multiplicative group is either a quaternion group of order 8 or a generalized quaternion group of order 16 with Abelian additive groups of the following types: $(3, 3)$, $(2, 2, 2, 2)$, $(2, 2, 4)$, $(2, 2, 2, 2, 2)$ and $(2, 2, 2, 4)$.

Subsection 1.4 presents results related to the computer algebra system GAP and the SONATA package. This subsection consists of four subsections, which describe the SmallGroups Library 1.4.1, the SONATA package 1.4.2, the classification of nearrings with identity 1.4.3, and local nearrings 1.4.4.

Section 2 consists of seven subsections 2.1, 2.2, 2.3, 2.4, 2.5, 2.6, and 2.7. This section describes local nearrings with some restrictions on their structure. Subsection 2.1 provides auxiliary definitions and statements concerning local nearrings, nilpotent groups, Schmidt groups, and Miller–Moreno groups. Subsections 2.2, 2.3, 2.4, and 2.5 provide results on local nearrings with nilpotent multiplicative group, multiplicative Schmidt groups, multiplicative Miller–Moreno groups, and local nearrings on finite p -groups with cyclic subgroups of index p , respectively. Subsection 2.6 investigates finite nearrings with identity with a monogenic semigroup of non-invertible elements. Subsection 2.7 describes local nearrings obtained from the SONATA package library.

Section 3 consists of five subsections 3.1, 3.2, 3.3, 3.4 and 3.5. This section studies local nearrings on finite non-Abelian 2-generated p -groups. Subsection 3.1 presents a classification of finite non-Abelian 2-generated p -groups with a cyclic commutator subgroup. Subsection 3.2 describes finite local nearrings with a split metacyclic additive group. This subsection consists of seven subsections, namely 3.2.1, 3.2.2, 3.2.3, 3.2.4, 3.2.5, 3.2.6 and 3.2.7. In subsection 3.3 local nearrings on groups of type $(B.1)$ are studied. The groups $(C.1)$, $(B.2)$ and $(C.2)$ are described in subsections 3.4 and 3.5.

Semidistributive nearrings with identity and local nearrings are studied in section 4. This section consists of two subsections 4.1 and 4.2. Subsection 4.1 describes distributive and semidistributive nearrings with identity. This subsection consists of three subsections 4.1.1, 4.1.2, and 4.1.3. Subsection 4.2 studies finite semidistributive local nearrings.

Section 5 consists of five subsections 5.1, 5.2, 5.3, and 5.4. This section investigates nearring braces and local nearrings. Subsection 5.1 presents results on braces and skew braces. Braces and skew braces from the YangBaxter package are characterized in subsections 5.2 and 5.3. Subsection 5.4 presents some results on nearring braces.

Section 6 consists of three subsections 6.1, 6.2, and 6.3. This section presents the use of the computer algebra system GAP for constructing and studying non-distributive algebraic structures, namely the algorithm for constructing finite local nearrings 6.1 and functions for nearrings 6.2 and groups 6.3 from the LocalNR package.

The classification of local nearrings of small orders and endocyclic groups is described in section 7. This section consists of two subsections 7.1 and 7.2. In subsection 7.1, a classification of local nearrings of small orders is obtained. Namely, local nearrings of order 64 7.1.1, 81 7.1.2, 243 7.1.3, 343 7.1.4 and 343 7.1.4. In subsection 7.2, endocyclic groups and local nearrings are studied.

Key words: Nearring with identity, local nearring, multiplicative group, subgroup of non-invertible elements, nilpotent group, Schmidt group, Miller–Moreno group, GAP, SONATA, LocalNR.

Список публікацій

1. Raievska I., Raievska M., Sysak Ya. LocalNR package and some of its applications. *Algebra Discrete Math.*, 2025, **40** (2), 215–225, <https://doi.org/10.12958/adm2449> (SJR — **Q3**)
2. Раєвська І., Раєвська М. Про ендоеиклічні 2-породжені групи порядку 256 та експоненти 16. *Буковинський матем. журнал*, 2025, 13 (2), 161–169 (Категорія Б)
3. Sysak Ya., Raievska I., Raievska M. Construction of local nearrings using GAP. *Algebra Discrete Math.*, 2025, **40** (1), 133–144, <https://doi.org/10.12958/adm2427> (SJR — **Q3**)
4. Raievska I., Raievska M. Local nearrings and endocyclic groups of small order. *Scientific Bulletin of Uzhhorod University. Series of Mathematics and Informatics*, 2025, **47** (2), 65–71, [https://doi.org/10.24144/2616-7700.2025.47\(2\).65-71](https://doi.org/10.24144/2616-7700.2025.47(2).65-71) (Категорія Б)
5. Raievska I., Raievska M. Braces and skew-braces via gap: YangBaxter and LocalNR packages. *Journal of Mathematical Sciences*, 2025, **294**, 230–241, <https://link.springer.com/article/10.1007/s10958-025-08097-1> (SJR — **Q3**)
6. Raievska M. p -groups with cyclic subgroup of index p and local nearrings. *Прикл. проблеми мех. і мат.*, 2024, **22**, 117–122 (Категорія Б)
7. Raievska I., Raievska M. Local nearrings, their structure, and the GAP system. *Ukrainian Math. J.*, 2025, **76** (11), 1831–1848, <https://doi.org/10.1007/s11253-025-02426-y>; translation of *Ukrain. Mat. Zh.*, 2024, **76** (11), 1629–1644 (SJR — **Q3**)

8. Раєвська М. Про локальні майже-кільця з нільпотентною мультиплікативною групою. *Науковий вісник Ужгородського університету. Серія «Математика і інформатика»*, 2025, **46** (1), 89–92, [https://doi.org/10.24144/2616-7700.2025.46\(1\).89-92](https://doi.org/10.24144/2616-7700.2025.46(1).89-92) (Категорія Б)
9. Raievska I., Raievska M., Sysak Ya. Semidistributive nearrings with identity. *Algebra Discrete Math.*, 36(2) (2023), 217–224, <https://admjournal.luguniv.edu.ua/index.php/adm/article/view/2207/pdf> (SJR — **Q3**)
10. Raievska M. On semidistributive local nearrings. *Науковий вісник Ужгородського університету. Серія “Математика і інформатика”*, **43**(2) (2023), 67–71, [https://doi.org/10.24144/2616-7700.2023.43\(2\).67-71](https://doi.org/10.24144/2616-7700.2023.43(2).67-71) (Категорія Б)
11. Raievska I. Yu., Raievska M. Yu. Local near-rings with a multiplicative Schmidt group. *Ukr. Math. J.*, **71** (2020), No. 10, P. 1643–1649, <https://doi.org/10.1007/s11253-020-01737-6>; перекладено з *Ukr. Mat. Zh.*, 2019, **71**, No. 10, 1435–1440. (in Ukrainian), <http://umj.imath.kiev.ua/index.php/umj/article/view/1526/509> (SJR — **Q3**)
12. Raievska I. Yu., Raievska M. Yu. Local nearrings on finite non-abelian 2-generated p-groups. *Carpathian Math. Publ.*, **12** (1) (2020), 199–207, URL: <https://journals.pnu.edu.ua/index.php/cmp/article/view/3905/4478> (SJR — **Q2**)
13. Raievska I. Yu., Raievska M. Yu. Finite nearrings with identity on Miller-Moreno groups. *Mat. Stud.*, 2014, **42** (1), 15–20, http://matstud.org.ua/texts/2014/42_1/15-20.pdf (Фахове видання)

14. Раєвська І. Ю., Раєвська М. Ю. Локальні майже-кільця з обмеженнями на мультиплікативні групи та підгрупи необоротних елементів. *Науковий часопис НПУ імені М. П. Драгоманова. Серія 1. Фізико-математичні науки*, Київ: НПУ імені М. П. Драгоманова, 2013, **14**, 134–145 (Фахове видання)
15. Raievskia I. Yu., Raievskia M. Yu., Sysak Ya. P. Local nearrings of order 243. *Proceedings CMSM 4*, June 28 — July 2, 2017, Chisinau / ed.: Mitrofan Choban [et al.]. Chisinau: Institute of Mathematics and Computer Science, 2017 (СЕР USM), 149–152.
16. Raievskia I. Yu., Raievskia M. Yu., Sysak Ya. P. Finite local nearrings with split metacyclic additive group. *Algebra and Discrete Mathematics*, (2016), **22** (1), 129–152,
<http://admjournal.luguniv.edu.ua/index.php/adm/article/view/293/pdf> (SJR — **Q4**)
17. Raievskia I., Raievskia M., Sysak Ya. DatabaseEndom64: (v1.0.1) [Data set] (2024). Zenodo,
<https://doi.org/10.5281/zenodo.10820320>
18. Raievskia I., Raievskia M., Sysak Ya. DatabaseEndom243: (v1.0.1) [Data set] (2024). Zenodo,
<https://doi.org/10.5281/zenodo.10820318>
19. Raievskia I., Raievskia M., Sysak Ya. LocalNR, Package of local nearrings, Version 1.0.4 (2024) (GAP package),
<https://gap-packages.github.io/LocalNR/>
20. Raievskia M. p -Groups with cyclic subgroup of index p and local nearrings. 15th Ukraine Algebra Conference, Lviv, Ukraine, July 8–12, 2025. P. 87,
<https://xvuac.mmf.com.ua/index.php/abstracts>

21. Раєвська М. Про локальні майже-кільця з нільпотентною мультиплікативною групою. The conference of young scientists “Pidstryhach Readings — 2025”, Lviv, Ukraine, May 27—29, 2025,
http://iapmm.lviv.ua/chyt2025/abstracts/Raievska_Iryna.pdf
22. Raievskaya I. Yu., Raievskaya M. Yu. Braces, skew-braces, local nearrings via GAP: the YangBaxter and LocalNR packages. Тези доповідей конференції молодих учених “Підстригачівські читання — 2024”. Львів, Україна, 27–29 травня, 2024,
<http://www.iapmm.lviv.ua/chyt2024/abstracts/Raievskaya.pdf>
23. Raievskaya I., Raievskaya M. LocalNR package and its applications, GAP Days Spring 2024, University of Kaiserslautern-Landau, Kaiserslautern, March 11–15, 2024,
<https://www.gapdays.de/gapdays2024-spring/abstracts/raievskaya>
24. Raievskaya I., Raievskaya M. Finite local nearrings and their classification, International conference-workshop “GAP Days Summer 2022”, RWTH Aachen University, Aachen, Germany, October 17–21, 2022,
<https://www.gapdays.de/gapdays2022-summer/abstracts/raievskaya>
25. Raievskaya I., Raievskaya M., Local nearrings and their classification, International Conference “On the Trail of Women in Mathematics “Contemporary Women in Mathematics”, Gdansk, Poland, September 15–17, 2022,
https://otowim22.ptkwm.pl/Abstract_Book.pdf
26. Raievskaya I., Raievskaya M., Local nearrings of order 343. International Algebraic Conference “At the End of the Year 2021”. Kyiv, Ukraine, December 27–28, 2021 (in the form of webinars)
<https://www.imath.kiev.ua/~algebra/algebra2021/abstracts>

27. Abramov A. V., Raievska I. Yu., Raievska M. Yu., Sysak Ya. P., Yurashev V. G. Miller–Moreno groups as multiplicative groups of local nearrings of order 64. 13th International Algebraic Conference in Ukraine. Kyiv, Ukraine, July 6–9, 2021 (in the form of webinars)
<https://drive.google.com/file/d/1wdZLWtj9jeFLH9BjSb7ZX5RFnTfTpstE/view>
28. Abramov A. V., Raievska I. Yu., Raievska M. Yu., Sysak Ya. P., Yurashev V. G. Local nearrings of order 1331. Abstracts of the conference dedicated to the 60th anniversary of the algebra department of Kyiv University. Kyiv, Ukraine, July 14–17, 2020, P. 11;
https://drive.google.com/file/d/1gyNWN20TC6V09mP3uRXw7uG9bg-3S_E7/view
29. Raievska I., Raievska M., The additive groups of local nearrings of order 64. Тези доповідей конференції молодих учених “Підстригачівські читання — 2020”. Львів, Україна, 26–28 травня, 2020,
<http://iapmm.lviv.ua/chyt2020/abstracts/Raievska.pdf>
30. Raievska I. Yu., Raievska M. Yu. Some special p -groups and nearrings with identity. Тези доповідей до XII Міжнародної алгебраїчної конференції в Україні, присвяченій 215-й річниці з дня народження В. Буняковського, 02–06 липня 2019 р., Донецький національний університет імені Василя Стуса, Вінниця, Україна, С. 92–93,
<https://jiac.donnu.edu.ua/article/view/6991>
31. Раєвська І. Ю., Раєвська М. Ю. Локальні майже-кільця на скінченних неабелевих p -групах. Тези доповідей міжнародної конференції “Сучасні проблеми механіки та математики” присвяченої 90-річчю від дня народження академіка НАН України Ярослава Степановича Підстригача та 40-річчю створеного ним Інституту прикладних проблем механіки і математики НАН України, 22–25 травня 2018 р.,

- Інститут прикладних проблем механіки і математики ім. Я. С. Підстригача НАН України, Львів, Т. 3, С. 230,
http://www.iapmm.lviv.ua/mpmm2018/Volume_3.pdf
32. Raievska I. Yu., Raievska M. Yu., Sysak Ya. P. Local nearrings of order 64. Abstracts of the International mathematical conference “Groups and Actions: Geometry and Dynamics, dedicated to the memory of professor Vitaly Sushchansky”. Kyiv, Ukraine, December 19–22, 2016, P. 43.
 33. Raievska I. Yu., Raievska M. Yu. Finite one-sided distributive structures. Тези доповідей XI Літньої школи “Алгебра, Топологія, Аналіз”, 1–14 серпня 2016 р., Одеса, Україна,
http://www.imath.kiev.ua/~topology/ata11/ata11_theses.pdf
 34. Raievska I., Raievska M. Local nearrings on finite 2-generated non-abelian non-metacyclic p -groups. Abstracts of Scientific Conference dedicated to 100th anniversary of K. M. Fishman and M. K. Fage. Chernivtsi, Ukraine, July 1–4, 2015, P. 103.
 35. Raievska I. Yu., Raievska M. Yu., Sysak Ya. P. Local nearrings of order 81. Abstracts of X International Algebraic Conference in Ukraine dedicated to the 70th anniversary of Yu. A. Drozd, Odessa, Ukraine, August 20–27, 2015, P. 94.
 36. Raievska M. Finite local nearrings on non-abelian p -groups with cyclic commutator subgroups. Abstracts of conference “Groups and their actions”. Bedlewo (near Poznan), Poland, June 22–26, 2015,
<http://mat.polsl.pl/groups/bedlewo-2015.pdf>
 37. Raievska I., Raievska M. Finite local nearrings on split metacyclic additive group. Тези доповідей Міжнародної конференції молодих математиків, 3–6 червня 2015 р., Ін-т математики НАН України, Київ, Україна, С. 42.

- 38. Raievska M. On multiplicative groups of finite local nearrings. Abstracts of AAA89: Workshop on General Algebra, Dresden, Germany, February 26 – March 1, 2015,
<http://at.yorku.ca/cgi-bin/abstract/cbkb-72>
- 39. Raievska I., Raievska M. On finite one-sided distributive structures. Abstracts of Humboldt Kolleg “Education and science and their role in social and industrial progress of society”. Kyiv, Ukraine, June 12–15, 2014, P. 45.
- 40. Raievska I., Raievska M., Sysak Ya. Finite local nearrings with multiplicative Miller–Moreno group. Abstracts of 9-th International Algebraic Conference in Ukraine. Lviv, Ukraine, July 8–13, 2013, P. 154.

Зміст

Перелік умовних позначень	24
Вступ	26
Розділ 1	
Огляд літератури та попередні відомості	54
1.1. Майже-поля	54
1.2. Майже-кільця з одиницею	58
1.3. Локальні майже-кільця	67
1.4. Система комп'ютерної алгебри GAP та пакет SONATA . .	77
1.4.1. Бібліотека SmallGroups	77
1.4.2. Пакет SONATA	79
1.4.3. Класифікація майже-кілець з одиницею	85
1.4.4. Класифікація локальних майже-кілець	89
Висновки до розділу 1	90
Розділ 2	
Локальні майже-кільця з деякими обмеженнями на їх структуру	92
2.1. Допоміжні означення та твердження	92
2.2. Локальні майже-кільця з нільпотентною мультиплікативною групою	96
2.3. Локальні майже-кільця з мультиплікативними групами Шмідта	98

2.4. Локальні майже-кільця деякого порядку з мультиплікативними	
групами Міллера–Морено	102
2.4.1. Локальні майже-кільця порядку 32	103
2.4.2. Локальні майже-кільця порядку 64	104
2.4.3. Локальні майже-кільця порядку 128	107
2.5. Локальні майже-кільця на скінченних p -групах	
з циклічними підгрупами індексу p	108
2.5.1. Попередні відомості	108
2.5.2. Скінченні p -групи з циклічною підгрупою індексу p	
як адитивні групи локальних майже-кілець	111
2.6. Скінченні майже-кільця з одиницею з моногенною напів-	
групою необоротних елементів	112
2.7. Локальні майже-кільця, отримані з бібліотеки	
пакету SONATA	114
Висновки до розділу 2	120

Розділ 3

Локальні майже-кільця на скінченних	
неабелевих 2-породжених p-групах	121
3.1. Скінченні неабелеві 2-породженні p -групи з циклічним ко-	
мутантом	121
3.2. Скінченні локальні майже-кільця з розщепленою метаци-	
клічною адитивною групою	124
3.2.1. Майже-кільця з одиницею на групах Міллера–	
Морено	125
3.2.2. Допоміжні означення та твердження	126
3.2.3. Майже-кільце з одиницею на неабелевій розщеплю-	
ваній метациклічній p -групі	135

3.2.4.	Майже-кільце з одиницею на групі $G(p^m, p^n, r)$. . .	140
3.2.5.	Майже-кільце з одиницею на групі $G(2^m, 2^n, -r)$. .	145
3.2.6.	Локальні майже-кільця на групах $G(p^m, p^n, r)$ та $G(2^m, 2^n, -r)$	149
3.2.7.	Групи $G(p^m, p^n, r)$ як адитивні групи локальних майже-кілець	153
3.3.	Локальні майже-кільця на групах типу (B.1)	159
3.3.1.	Допоміжні результати	159
3.3.2.	Майже-кільця з одиницею на групі $G(p^m, p^n, p^d)$. .	163
3.3.3.	Локальні майже-кільця на групі $G(p^m, p^n, p^d)$	168
3.4.	Про групи (C.1)	172
3.5.	Групи (B.2) та (C.2)	179
	Висновки до розділу 3	181

Розділ 4

Напівдистрибутивні майже-кільця з одиницею та локаль-	
ні майже-кільця	183
4.1.	Дистрибутивні та напівдистрибутивні майже-кільця з оди- ницею
	183
4.1.1.	Адитивні групи напівдистрибутивних майже-кілець
	192
4.1.2.	Дистрибутивні елементи в напівдистрибутивних майже-кільцях
	196
4.1.3.	Модулі над майже-кільцями та напівдистрибутивність
	198
4.2.	Скінченні напівдистрибутивні локальні майже-кільця . . .
	200
	Висновки до розділу 4
	205

Розділ 5

Майже-кільцеві брейси та локальні майже-кільця	206
5.1.	Брейси та косі брейси
	206
5.2.	Брейси з пакету YangBaxter
	208

5.3. Косі брейси з пакету YangBaxter	215
5.4. Майже-кільцеві брейси	225
Висновки до розділу 5	227

Розділ 6

Використання системи комп'ютерної алгебри GAP для побудови та вивчення недистрибутивних алгебраїчних структур

228

6.1. Алгоритм побудови скінченних локальних майже-кілець	228
6.2. Пакет LocalNR: функції для майже-кілець	234
6.2.1. TheAdditiveGroupsOfLibraryOfLNRsOfOrder	235
6.2.2. TheLibraryOfLNRsOnGroup	236
6.2.3. LocalNearRing	239
6.2.4. AllLocalNearRings	241
6.2.5. IsAdditiveGroupOfLibraryOfLNRs	242
6.2.6. InfoLocalNearRing	244
6.3. Пакет LocalNR: функції для груп	246
6.3.1. IsMinimalNonAbelianGroup	246
6.3.2. IsMetacyclicPGroup	248
6.3.3. EndoOrbitsOfGroup	249
6.3.4. IsEndoCyclicGroup	252
Висновки до розділу 6	253

Розділ 7

Класифікація локальних майже-кілець малих порядків та ендосиклічні групи

255

7.1. Класифікація локальних майже-кілець малих порядків	255
7.1.1. Локальні майже-кільця порядку 64	255
7.1.2. Локальні майже-кільця порядку 81	258
7.1.3. Локальні майже-кільця порядку 243	259

7.1.4. Локальні майже-кільця порядків 343	264
7.1.5. Локальні майже-кільця порядків 1331	264
7.2. Ендоциклічні групи та локальні майже-кільця	265
7.2.1. Локальні майже-кільця та ендоциклічні 2-породжені групи порядку 64	266
7.2.2. 2-Породжені ендоциклічні групи порядку 256	269
Висновки до розділу 7	287
Основні результати та висновки	288
Список використаних джерел	291
Додаток А	
Список публікацій і апробація результатів	305

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

Перелік умовних позначень

Символ	Опис
$\emptyset$	Порожня множина
C_n	Циклічна група порядку n
$\mathbb{Z}_n$	Кільце лишків по модулю n
$\langle X \rangle$	Група, породжена множиною X
Q_8	Група кватерніонів порядку 8
D_n	Група діедра порядку n
$A \trianglelefteq B$	A є нормальною підгрупою групи B ; A є ідеалом майже-кільця B
$A \triangleleft B$	A є власною нормальною підгрупою групи B ; A є власним ідеалом майже-кільця B
$G \cong H$	G та H ізоморфні
$ M $	Потужність множини M
$ G : H $	Індекс підгрупи H в групі G
$\exp(G)$	Експонента групи G
$Z(G)$	Центр групи G
$C_G(H)$	Централізатор підгрупи H в групі G
$N_G(H)$	Нормалізатор підгрупи H в групі G
$\text{End}(G)$	Моноїд всіх ендоморфізмів групи G
$\text{Aut}(G)$	Група всіх автоморфізмів групи G
$\text{Inn}(G)$	Група внутрішніх автоморфізмів групи G
$[a, b]$	Комутатор групових елементів a та b , тобто $-a - b + a + b$ для адитивно записаних груп,

	$a^{-1}b^{-1}ab$ для мультиплікативно записаних груп
$[A, B]$	$\langle [a, b] a \in A, b \in B \rangle$
G'	Комутант групи G , тобто $[G, G]$
$A \times B$	Прямий добуток груп A та B
$A \rtimes B$	Напівпрямий добуток груп A та B , в якому A є нормальною підгрупою
$\alpha : A \rightarrow B$	α є відображенням з A в B
$\text{Ker}(\alpha)$	Ядро гомоморфізму α
R^+	Адитивна група майже-кільця R
$M(G)$	Майже-кільце відображень з групи G в G
L	Множина всіх елементів майже-кільця R , які не мають прaviх обернених в R
R^*	Група оборотних елементів майже-кільця R
$\Phi(G)$	Підгрупа Фраттіні групи G
x^A	$\{x^a \mid a \in A\}$, де A — підмножина групи $\text{Aut } G$ всіх автоморфізмів групи G та $x \in G$

Вступ

Дисертацію присвячено вивченню локальних майже-кілець з деякими обмеженнями на мультиплікативні групи та підгрупи необоротних елементів, класифікації локальних майже-кілець та дослідженню їх адитивних груп.

Обґрунтування вибору теми дослідження.

Перші дослідження майже-кілець були зроблені Діксоном [34]. Було показано, що існують “поля з одним дистрибутивним законом” та наведено приклади, які показують, що такі системи — названі Цассенхаузом майже-полями — можуть бути недистрибутивними. Цассенхауз [121] довів, що приклади Діксона охоплюють усі, крім сімох скінченних майже-полів, які не є тілами. Більшість результатів про майже-поля містяться в монографії Виглінга [120].

Майже-кілеця є широкими узагальненнями асоціативних кілець, в означенні яких адитивна група не обов’язково абелева, а додавання та множення пов’язані хоча б одним, лівим або правим, дистрибутивним законом. У цьому сенсі локальні майже-кілеця є узагальненням локальних кілець.

Універсальним прикладом майже-кілеця є множина всіх функцій на довільній групі відносно операцій додавання та суперпозиції функцій. Майже-кілеця виникають природним чином при вивченні систем нелінійних відображень і вивчаються вже багато десятиліть. Оскільки асоціативні кілеця є по суті кільцями лінійних функцій на абелевих групах, то

перехід від кілець до майже-кілець характеризується переходом від лінійних методів досліджень до нелінійних, а тому вивчення майже-кілець та розробка теоретико-групових методів їх досліджень є важливою та актуальною задачею.

Добре відомо, що кожне кільце вкладається в кільце $End(A)$ усіх ендоморфізмів абелевої групи A . Аналогічно, кожне майже-кільце можна вкладати в $Map(G)$ для деякої групи G . З цієї точки зору теорія кілець описує «лінійні» відображення на групах, тоді як майже-кілець обробляють загальний нелінійний випадок.

Майже-кільце R — це непорожня множина з двома бінарними операціями, додаванням “+” і множенням “ $\cdot$ ”, яка відрізняється від кільця тим, що комутативність першої операції та один із дистрибутивних законів (у нашому випадку, правий) не обов’язково виконуються (див., наприклад, [70]).

Основні визначення та багато результатів, що стосуються майже-кілець, можна знайти, наприклад, у книзі Пільца [70].

Очевидно, що кожне асоціативне кільце є майже-кільцем, і кожна група є адитивною групою майже-кілець, але не обов’язково майже-кільцем з одиницею. Питання, яка група може бути адитивною групою майже-кілець з одиницею, є відкритим.

Проблема знаходження груп, які можуть бути адитивними групами майже-кілець з одиницею, вивчається з кінця 1960-х років. Один з перших результатів у цьому напрямку був отриманий у [31], де було показано, що існує єдине майже-кільце з одиницею, адитивна група якого є циклічною, і, що насправді, це майже-кільце є комутативним кільцем.

Класифікація всіх майже-кілець до певних порядків є відкритою проблемою, вирішення якої вимагає значних обчислень, і найбільш підходящою платформою для їх реалізації є система комп’ютерної алгебри GAP [40].

Локальні майже-кільця, мультиплікативна група яких є абелевою і які не є кільцями, вивчалися Городником [42]. Ним, зокрема, доведено, що множина всіх необоротних елементів такого майже-кільця утворює абелеву підгрупу індексу 2 в його адитивній групі та повністю описані локальні майже-кільця з циклічною мультиплікативною групою. Наступним природним кроком є дослідження локальних майже-кілець, мультиплікативна група яких є групою Міллера-Морено, тобто мінімальною неабелевою. Випадок, коли адитивна група такого майже-кільця є p -групою з $p \neq 2$ розглядався М. Раєвською [8]. В статті [9] вивчалися локальні майже-кільця порядку 2^n з мультиплікативною групою Міллера-Морено. В дисертаційній роботі продовжено дослідження та класифікація мультиплікативних груп скінченних локальних майже-кілець.

Зв'язок роботи з науковими програмами, планами, темами.

Робота виконувалася в Інституті математики НАН України у відділі алгебри і топології згідно із загальним планом досліджень у рамках науково-дослідних тем “Теорія зображень та її застосування в алгебрі, геометрії й топології” (номер державної реєстрації 0111U002096, 2011–2015 рр.), “Розробка й застосування нових методів у теорії зображень, абстрактній алгебрі та алгебраїчній геометрії” (номер державної реєстрації 0116U003125, 2016–2020 рр.), “Дослідження динамічних систем та еволюційних задач топологічними, стохастичними та алгебричними методами” (номер державної реєстрації 0117U004091, 2017–2021 рр.) та “Категорні, комбінаторні та аналітичні методи дослідження проблем теорії зображень, алгебраїчної геометрії, алгебраїчної та диференціальної топології” (номер державної реєстрації 0121U100395, 2021–2025 рр.), “Сучасні методи алгебри і топології та їх застосування” (номер державної реєстрації 0126U000346, 2026–2030 рр.).

Мета і завдання дослідження.

Метою дослідження є розвиток теорії локальних майже-кілець та пов'язаних з ними структури.

Об'єктом дослідження є скінченні локальні майже-кільця.

Предметом дослідження є мультиплікативні групи та групи необоротних елементів скінченних локальних майже-кілець.

Завдання дослідження:

- Встановити зв'язок між нільпотентною мультиплікативною групою та адитивною групою в локальному майже-кільці.
- Класифікувати локальні майже-кільця, які не є полями та мультиплікативна група яких є групою Шмідта.
- Знайти адитивні групи локальних майже-кілець порядку 32 та 128 з мультиплікативними групами Міллера–Морено.
- Вивчити скінченні p -групи з циклічною підгрупою індексу p як адитивні групи локальних майже-кілець.
- Отримати локальні майже-кільця з бібліотеки пакету SONATA системи комп'ютерної алгебри GAP.
- Проаналізувати скінченні неабелеві 2-породженні p -групи з циклічним комутантом.
- Показати, що не існує майже-кілець з одиницею, адитивна група якого ізоморфна групі $G(p^m, p^n)$ з $p > 2$ і $2 \leq m \leq n$.
- Вивчити скінченні локальні майже-кільця з розщепленою метациклічною адитивною групою.

- Отримати необхідні і достатні умови існування локальних майже-кілець на групах типу (B.1). Довести, що індекс підгрупи всіх необоротних елементів таких майже-кілець в адитивній групі дорівнює p . А також, показати, що кожна група типу (B.1) є адитивною групою майже-кілля з одиницею.
- Ввести та дослідити напівдистрибутивні майже-кілля з одиницею.
- Вивчити напівгрупу необоротних елементів локальних майже-кілець, адитивна група якого ізоморфна абелевій групі типу $(2^m, 2^n)$ з $m \geq n > 1$.
- Використовуючи пакет YangBaxter, надати класифікації брейсів (до порядку 32) та косих брейсів (до порядку 16) відповідно до адитивних або мультиплікативних груп, які є p -групами Міллера–Морено.
- Навести деяку інформацію щодо майже-кілцевих брейсів, що стосуються, пакету LocalNR.
- Отримати алгоритм побудови скінченних локальних майже-кілець.
- Навести функції для локальних майже-кілець з пакету LocalNR, а саме:
 - TheAdditiveGroupsOfLibraryOfLNRSOfOrder,
 - TheLibraryOfLNRSOnGroup,
 - LocalNearRing,
 - AllLocalNearRings,
 - IsAdditiveGroupOfLibraryOfLNRS,
 - InfoLocalNearRing.
- Навести функції для груп з пакету LocalNR, а саме:

- IsMinimalNonAbelianGroup,
 - IsMetacyclicPGroup,
 - EndoOrbitsOfGroup,
 - IsEndoCyclicGroup.
- Класифікувати локальні майже-кільця на 2-породжених групах порядків 64 та 243.
 - Навести класифікацію локальних майже-кілець порядків 81 та 1331.
 - Вивчити локальні майже-кільця та ендоеиклічні 2-породжені групи порядків 64 та 256.

Наукова новизна одержаних результатів.

Результати роботи, що виносяться на захист, є новими і полягають у наступному:

- Встановлено зв'язок між нільпотентною мультиплікативною групою та адитивною групою в локальному майже-кільці.
- Класифіковано локальні майже-кільця, які не є полями та мультиплікативна група яких є групою Шмідта.
- Знайдені адитивні групи локальних майже-кілець порядку 32 та 128 з мультиплікативними групами Міллера–Морено.
- Вивчені скінченні p -групи з циклічною підгрупою індексу p як адитивні групи локальних майже-кілець.
- Отримано локальні майже-кільця з бібліотеки пакету SONATA системи комп'ютерної алгебри GAP.

- Проаналізовано скінченні неабелеві 2-породженні p -групи з циклічним комутантом.
- Показано, що не існує майже-кілець з одиницею, адитивна група якого ізоморфна групі $G(p^m, p^n)$ з $p > 2$ і $2 \leq m \leq n$.
- Вивчено скінченні локальні майже-кілець з розщепленою метациклічною адитивною групою.
- Отримано необхідні і достатні умови існування локальних майже-кілець на групах типу (B.1). Доведено, що індекс підгрупи всіх необоротних елементів таких майже-кілець в адитивній групі дорівнює p . А також, показано, що кожна група типу (B.1) є адитивною групою майже-кілець з одиницею.
- Введено та досліджено напівдистрибутивні майже-кілець з одиницею.
- Вивчено напівгрупу необоротних елементів локальних майже-кілець, адитивна група якого ізоморфна абелевій групі типу $(2^m, 2^n)$ з $m \geq n > 1$.
- Використовуючи пакет YangBaxter, надано класифікації брейсів (до порядку 32) та косих брейсів (до порядку 16) відповідно до адитивних або мультиплікативних груп, які є p -групами Міллера–Морено.
- Наведено деяку інформацію щодо майже-кілецевих брейсів, що стосуються, пакету LocalNR.
- Отримано алгоритм побудови скінченних локальних майже-кілець.
- Наведено функції для локальних майже-кілець з пакету LocalNR, а саме:

– TheAdditiveGroupsOfLibraryOfLNRsOfOrder,

- TheLibraryOfLNRsOnGroup,
 - LocalNearRing,
 - AllLocalNearRings,
 - IsAdditiveGroupOfLibraryOfLNRs,
 - InfoLocalNearRing.
- Наведено функції для груп з пакету LocalNR, а саме:
 - IsMinimalNonAbelianGroup,
 - IsMetacyclicPGroup,
 - EndoOrbitsOfGroup,
 - IsEndoCyclicGroup.
 - Класифіковано локальні майже-кільця на 2-породжених групах порядків 64 та 243.
 - Наведено класифікацію локальних майже-кілець порядків 81 та 1331.
 - Вивчено локальні майже-кільця та ендочиклічні 2-породжені групи порядків 64 та 256.

Практичне значення одержаних результатів.

Дисертаційна робота носить теоретичний характер. Результати роботи, а також методика їх отримання, можуть бути використані для подальшого розвитку теорії майже-кілець, теорії груп, теорії брейсів та системи комп'ютерної алгебри GAP.

Методи дослідження.

У роботі використовуються методи теорії груп, теорії майже-кілець та теорії брейсів. Для побудови прикладів локальних майже-кілець були написані алгоритми та програми на мові GAP, які було реалізовано на кластерах та суперкомп'ютерах:

- CIRCA (м. Сент Андрюс, Шотландія, Велика Британія);
- CIRUS (м. Единбург, Шотландія, Велика Британія);
- Інституту математики Польської Академії Наук (м. Варшава, Польща);
- Інституту математики НАН України (м. Київ, Україна);
- Інституту кібернетики НАН України (м. Київ, Україна);
- Київського політехнічного інституту імені Ігоря Сікорського (м. Київ, Україна).

Особистий внесок здобувача.

Основні результати дисертації, які виносяться на захист, отримані автором особисто. Визначення напрямку досліджень, постановка задач, ідеї відносно вибору методик розв'язування належать науковому консультанту. Три статті опубліковано без співавторів. У спільних з науковим консультантом та І. Ю. Раєвською публікаціях за темою дисертації розподіл особистих внесків такий:

- у роботах [1, 3, 9, 15, 16, 17, 18, 19] — визначення напрямку досліджень, побудова алгоритму, брав участь у написанні функцій, побудові локальних майже-кілець, обговорення результатів, контроль якості викладення результатів належить науковому консультанту Я. П. Сисаку.

- у статті [3] — в дисертацію включено теорему 2. Здобувачка брала участь у написанні алгоритму та функцій для пакету LocalNR:
 - TheAdditiveGroupsOfLibraryOfLNRsOfOrder,
 - TheLibraryOfLNRsOnGroup,
 - LocalNearRing,
 - AllLocalNearRings,
 - IsAdditiveGroupOfLibraryOfLNRs,
 - InfoLocalNearRing.
- у статті [1] — в дисертацію включено зауваження 1, теорему 1. Здобувачка брала участь у написанні функцій для груп:
 - IsMinimalNonAbelianGroup,
 - IsMetacyclicPGroup,
 - EndoOrbitsOfGroup,
 - IsEndoCyclicGroup.
- у статті [2] — внесок авторів рівноцінний. В дисертацію включено лему 3.
- у статті [4] — внесок авторів рівноцінний. В дисертацію включено лему 3, теорему 3.
- у статтях [5, 9, 12, 14, 15, 16, 17, 18] — співавторка І. Ю. Раєвська перевіряла результати та брала участь обговорення результатів, постановці гіпотез та фінальному оформленню результатів.
- у статті [7] — внесок авторів рівноцінний. В дисертацію включено лему 6, теорему 8, теорему 9, теорему 10, теорему 25.

- у статті [11] — внесок авторів рівноцінний. В дисертацію включено теорему 5.
- у статті [13] — внесок авторів рівноцінний. В дисертацію включено наслідок 1.
- у пакеті [19] — здобувачка та І.Ю. Раєвська брали участь у написанні функцій, побудові локальних майже-кілець, оформленні та перевірці.

Апробація результатів дисертації.

Основні результати дисертації доповідалися та обговорювалися на:
Конференціях та школах:

- Воркшоп, присвячений 70-річчю Юрія Вікторовича Боднарчука, 23 грудня 2025 року, Національний університет “Києво-Могилянська академія”, Київ, Україна;
- Ukraine Mathematics Conference “At the End of the Year 2025”, December 18–19, 2025, Taras Shevchenko National University of Kyiv, Kyiv, Ukraine,
<https://sites.google.com/knu.ua/umc-2025/>
- 15th Ukraine Algebra Conference, July 8–12, 2025, Lviv, Ukraine,
<https://xvuac.mmf.com.ua/index.php/abstracts>
- The conference of young scientists “Pidstryhach Readings — 2025”, May 27–29, 2025, Lviv, Ukraine,
http://iapmm.lviv.ua/chyt2025/abstracts/Raievska_Maryna.pdf
- Конференція молодих учених “Підстригачівські читання – 2024”, 27–29 травня 2024 року, Львів, Україна,
<http://www.iapmm.lviv.ua/chyt2024/index.html>

- GAP Days Spring 2024, March 11–15, 2024, University of Kaiserslautern-Landau, Kaiserslautern, Germany,
<https://www.gapdays.de/gapdays2024-spring/abstracts/raievska>
- The 14th International Algebraic Conference in Ukraine (online), July 3–7, 2023, Sumy, Ukraine,
<https://sites.google.com/view/iacu2023/home>
- Online Twinning Conference (online), March 27–30, 2023, Digital Theme UK-Ukraine Twinning Initiative, Great Britain,
<https://irp.cdn-website.com/ee30e730/files/uploaded/Final\%20Programme\%20UA-DIGITAL\%202023.pdf>
- International conference-workshop “GAP Days Summer 2022”, October 17–21, 2022, RWTH Aachen University, Aachen, Germany,
<https://www.gapdays.de/gapdays2022-summer/abstracts/raievska>
- International Conference “On the Trail of Women in Mathematics “Contemporary Women in Mathematics”, September 15–17, 2022, Gdansk, Poland,
<https://otowim22.ptkwm.pl/>
- International Algebraic Conference “At the End of the Year 2021” (online), December 27–28, 2021, Kyiv, Ukraine,
<https://www.imath.kiev.ua/~algebra/algebra2021/>
- 3rd TA visitors meeting (TAM) (online), November 3–4, 2021, Amsterdam, Netherlands, <https://www.hpc-europa.org/3rdTAM>
- The 13th International Algebraic Conference in Ukraine, July 6–9, 2021, Kyiv, Ukraine,
<https://drive.google.com/file/d/1wdZLWtj9jeFLH9BjSb7ZX5RFnTfTpstE/view>

- Міжнародна конференція молодих математиків (online), 3–5 червня 2021 року, Київ, Україна,
https://www.imath.kiev.ua/~young/youngconf2021/Abstracts_2021.pdf
- The conference dedicated to the 60th anniversary of the algebra department of Kyiv University, July 14–17, 2020, Kyiv, Ukraine,
<https://sites.google.com/view/kyiv-algebra60/home>
- GAP-Singular-Meeting as part of the OpenDreamKit project, August 15–23, 2019, PfalzAkademie, Lambrecht, Germany,
<https://opendreamkit.org/meetings/2019-04-02-GAPsingularMeeting/>
- XII International Algebraic Conference in Ukraine dedicated to the 215th anniversary of V. Bunyakovsky, July 02–06, 2019, Vinnytsia, Ukraine,
<https://xvuac.mmf.com.ua/index.php/history/all-history/90-xii-iacu>
- 4th Conference of Mathematical Society of Moldova CMSM4'2017, June 28 – July 2, 2017, Chisinau, Republic of Moldova,
<http://cmsm4.math.md/>
- International mathematical conference “Groups and Actions: Geometry and Dynamics, dedicated to the memory of professor Vitaly Sushchanskyy”, December 19–22, 2016, Kyiv, Ukraine,
<https://www.ukma.edu.ua/eng/index.php/news/667-international-conference-groups-and-actions-geometry-and-dynamics>
- XI Літня школа “Алгебра, Топологія, Аналіз”, 1–14 серпня 2016 року,

Одеса, Україна,

<https://www.imath.kiev.ua/~topology/ata11/>

- Summer School on Algebra, Statistics and Combinatorics, June 27 – July 2, 2016, Espoo, Finland,
<https://www.aalto.fi/en/news/summer-school-on-algebra-statistics-and-combinatorics>
- XVII Міжнародна наукова конференція ім. акад. Михайла Кравчука, 19–20 травня 2016 року, Київ, Україна,
<https://matan.kpi.ua/uk/kravchuk-conf2016.html>
- X Міжнародна алгебраїчна конференція в Україні присвячена 70-річчю Ю. А. Дрозда, 20–27 серпня 2015 року, Одеса, Україна
- X Літня школа “Алгебра, Топологія, Аналіз”, 3–15 серпня 2015 року, Одеса, Україна,
<https://imath.kiev.ua/~topology/xata/>
- Наукова конференція, присвячена 100-річчю від дня народження К. М. Фішмана та М. К. Фаге, 1–4 липня 2015 року, Чернівці, Україна
- Conference “Groups and their actions”, June 22–26, 2015, Bedlewo (near Poznan), Poland
- Міжнародна конференція молодих математиків, 3–6 червня 2015 року, Київ, Україна
- AAA89: Workshop on General Algebra, February 26 – March 01, 2015, Dresden, Germany,
<https://tu-dresden.de/mn/math/algebra/forschung/tagungen/aaaseries/aaa89>

- IX-а Літня школа “Алгебра, топологія і аналіз”, 7–18 липня 2014 року, Поляниця, Україна,
https://imath.kiev.ua/~topology/xata/xata_program.pdf
- Humboldt Kolleg “Education and Science and their Role in Social and Industrial Progress of Society”, June 12–15, 2014, Kyiv, Ukraine,
<http://hk2014.humboldt.org.ua/>
- 9th International Algebraic Conference in Ukraine, July 08–13, 2013, Lviv, Ukraine,
<http://iapmm.lviv.ua/iacu2013/>

Семінарах:

- засіданнях Вченої ради Інституту математики НАН України (20 червня 2023 р. — онлайн, 24 червня 2025 р. — онлайн)
- лабораторії топології (Топологічний семінар) Інституту математики НАН України (керівник: чл.-кор. С. І. Максименко, Київ, Україна) (19 квітня 2023 р. — онлайн)
<https://www.imath.kiev.ua/events/index.php?seminarId=34&archiv=1>
- “Алгебра” Варшавського університету (керівник: проф. Ян Окнінський, Варшава, Польща) (21 квітня 2022 р., 9 березня 2023 р., 18 січня 2024 р.)
<https://www.mimuw.edu.pl/en/seminars/seminar-algebra/>
- “Secant group” в ІМ ПАН (керівник: проф. Ярослав Бучинський, Варшава, Польща) (31 січня 2023 р.)
- “Algebra and Discrete Mathematics” в Університеті міста Лінц (керівник: проф. Мануель Кауерс, Лінц, Австрія) (18 квітня 2024 р.)

<http://www.algebra.uni-linz.ac.at/teaching/seminar/schedule.php?term=ss2024>

- Алгебраїчний семінар Інституту математики НАН України (керівники: чл.-кор. Ю. А. Дрозд, чл.-кор. С. І. Максименко, Київ, Україна) (6 жовтня 2015 р., 18 грудня 2018 р., 26 червня 2024 р. — онлайн, 12.11.2025 р.)
<https://www.imath.kiev.ua/events/index.php?seminarId=22&archiv=1>
- розширене засідання “Під кінець року” Алгебраїчного семінару Київського національного університету імені Тараса Шевченка (керівник: проф. А. П. Петравчук) (26 грудня 2017 р.)
- Семінар молодих вчених Інституту математики НАН України (організатор: Рада молодих вчених ІМ НАНУ, Київ, Україна) (29 вересня 2016 р.)
<https://www.imath.kiev.ua/events/index.php?seminarId=85>
- Scientific Seminar “Geometry, Topology, Applications” (керівник: проф. Т. О. Банах, Львів, Україна) (9 березня 2026 р.)
<http://www.math.lviv.ua/seminar/past.php>

Публікації.

Результати дисертації висвітлено у 40 наукових публікаціях (див. список публікацій здобувача на с. 12–18), з них 14 — статті у наукових виданнях, внесених до переліку наукових фахових видань України та закордонних виданнях, а також 21 публікації у тезах доповідей і матеріалах міжнародних та вітчизняних конференцій. Статті [1, 3, 5, 7, 9, 11,

[12, 16] проіндексовані у міжнародних наукометричних базах Scopus або Web of Science. Статтю [12] опубліковано у виданні з квартиля Q2 відповідно до класифікації SCImago Journal and Country Rank, статті [1, 3, 5, 7, 9, 11] у виданнях з квартиля Q3, статтю [16] у виданні з квартиля Q4. Відповідно до п. 2 Наказу № 1220 МОН України від 23.09.2019 вказані 14 статей зараховуються як 22 наукові публікації. Роботи [1, 2, 3, 4, 7, 8, 9, 10, 11, 12, 13] проіндексовано у базі Zentrablatt Math, а роботи [3, 7, 9, 11, 12, 13, 16] проіндексовано у базі MathSciNet. Статті [6, 8, 10] одноосібні.

Структура й об'єм дисертації.

Дисертація складається з переліку умовних позначень, вступу, семи розділів, висновків, списку використаних джерел, що містить 121 найменувань та додатку зі списком публікацій і апробацією результатів. Повний обсяг роботи становить 318 сторінок друкованого тексту із них список використаних джерел міститься на 14 сторінках, а додаток — на 14 сторінках.

Державні нагороди (премії) України або інших держав.

За роботу “Дослідження алгебраїчних структур теоретико-груповими методами”, у складі колективу Плакош А. І., Раєвська І. Ю., Раєвська М. Ю., Сорока Ю. Ю. присуджено премію Верховної Ради України молодим ученим за 2020 рік (ПОСТАНОВА Верховної Ради України № 1918-IX). До зазначеної роботи увійшли 4 статті, а саме статті [11, 13, 14, 15] зі списку публікацій.

Стипендія.

Стипендія Президента України для молодих вчених (жовтень 2016 р. — вересень 2018 р).

Гранти.

1. Проект “LocalNearRings” повністю підтримано HPC-Europa3 Programme, що підтримується European Commission’s Horizon 2020 програмою під Grant Agreement 730897 (01.03-15.03.2020);
2. Grant of the Polish Academy of Sciences (PAN) and National Academy of Sciences (NAS) (1.04–30.06.2022);
3. Institute of International Education’s Scholar Rescue Fund (IIE-SRF) fellowship (1.10.2022–30.09.2023);
4. Institute of International Education’s Scholar Rescue Fund (IIE-SRF) fellowship (1.10.2023–30.09.2024);
5. Grant from the Simons Foundation (SFI-PD-Ukraine-00014586 (04.2025–03.2026));
6. the European Union’s Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 873071, SOMPATY.

Подяки.

Висловлюю щирю вдячність науковому консультанту провідному науковому співробітнику відділу алгебри і топології, доктору фізико-математичних наук, професору Ярославу Прокоповичу СИСАКУ за підтримку, постійну увагу, допомогу в роботі та корисні обговорення одержаних результатів, а також співробітникам відділу алгебри і топології.

Основний зміст дисертації

У вступі обґрунтовано актуальність теми дисертації, сформульовано мету, завдання дослідження та наукову новизну одержаних результатів.

У розділі 1 наведено огляд літератури за темою дисертації.

У розділі 2 наведено основні означення та результати, що стосуються локальних майже-кілець. У підрозділі 2.1 наведено результати про нільпотентні групи, групи Шмідта, які буде використано в подальших дослідженнях.

Вивчення локальних майже-кілець було започатковано Мексоном [61], який встановив, зокрема, що адитивна група скінченного локального майже-кілля повинна бути p -групою.

Означення 2.1. *Майже-кіллець R з одиницею називається локальним, якщо множина $L = R \setminus R^*$ всіх необоротних елементів із $(R, \cdot)$ утворює адитивну підгрупу в R^+ , та майже-полем, коли $L = 0$.*

Наведемо означення нільпотентної групи (див., наприклад, [49]).

Нехай G — група. Нормальний ряд

$$\{e\} = G_0 \subset G_1 \subset G_2 \subset \dots \subset G_n = G,$$

групи G називається *центральним*, якщо при $i = 0, 1, \dots, n-1$ фактор-група G_{i+1}/G_i міститься в центрі фактор-групи G/G_i . Група G , що має хоча б один центральний ряд, називається *нільпотентною*.

Групою Шмідта або мінімальною ненільпотентною групою називається скінченна ненільпотентна група, будь-яка власна підгрупа якої нільпотентна. Вивчення таких груп було започатковано О. Ю. Шмідтом в [113].

Підрозділ 2.3 присвячено вивченню локальних майже-кілець з нільпотентною мультиплікативною групою.

В наступній теоремі встановлений зв'язок між нільпотентною мультиплікативною групою та адитивною групою в локальному майже-кіллі.

Теорема 2.9. *Нехай R — локальне майже-кіллець порядку p^n з нільпотентною мультиплікативною групою R^* . Якщо $p > 2$ або $p = 2$ та $-i \in Z(R^*)$, то мають місце такі твердження:*

1. *Адитивна група R^+ — абелева.*

2. L — абелева та має індекс 2 в R^+ .

Зокрема, R/L є поле.

Підрозділ 2.3 присвячено вивченню локальних майже-кілець з мультиплікативними групами Шмідта.

Оскільки майже-поля з мультиплікативною групою Шмідта повністю описані в [8, теорема 6], то розглянемо локальні майже-кілець, підгрупи необоротних елементів яких є нетривіальними.

Нагадаємо, що просте число виду $p = 2^{2^s} + 1$ з цілим числом $s \geq 0$ називається *простим числом Ферма*.

Теорема 2.10. *Нехай R — локальне майже-кілець порядку p^n , яке не є майже-полем та мультиплікативна група R^* якого є групою Шмідта. Тоді мають місце наступні твердження:*

- 1) якщо $p > 2$, то $|R| = p^2$ для деякого простого числа Ферма p , адитивна група R^+ є елементарною абелевою та існує такий необоротний елемент a із R , що

$$R^+ = \langle i \rangle + \langle a \rangle,$$

де i — одиниця в R , $a^2 = 0$ та $(ik)a = -ak$ для довільного первісного кореня k за модулем p . Зокрема, для кожного простого числа Ферма p існує єдине локальне майже-кілець порядку p^2 , мультиплікативна група якого є групою Міллера–Морено;

- 2) якщо $p = 2$, то $|R| = 2^n$ з $n = 2t$, де t — просте число, для якого $2^t - 1$ є простим числом Мерсенна, та R^* є групою Міллера–Морено.

У підрозділі 2.5 досліджено локальні майже-кілець на скінченних p -групах з циклічними підгрупами індексу p .

В [13, Theorem 12.5.1] доведено, що існує сім типів p -груп з циклічною підгрупою індексу p .

Теорема 2.17. *Групи порядку p^n , які містять циклічну підгрупу з індексом p , мають такі типи: абелеві,*

$n \geq 1$, циклічні:

1) $a^{p^n} = 1$;

$n \geq 2$:

2) $a^{p^{n-1}} = 1, b^p = 1, ba = ab$;

неабелеві,

p — непарне, $n \geq 3$:

3) $a^{p^{n-1}} = 1, b^p = 1, ba = a^{1+p^{n-2}}b$;

$p = 2, n \geq 3$:

4) *узагальнена групи кватерніонів:*

$a^{2^{n-1}} = 1, b^2 = 1, ba = a^{-1}b$;

$p = 2, n \geq 3$:

5) *група дієдра:*

$a^{2^{n-1}} = 1, b^2 = 1, ba = a^{-1}b$;

$p = 2, n \geq 4$:

6) $a^{2^{n-1}} = 1, b^2 = 1, ba = a^{1+2^{n-2}}b$;

$p = 2, n \geq 4$:

7) $a^{2^{n-1}} = 1, b^2 = 1, ba = a^{-1+2^{n-2}}b$.

Теорема 2.21. *Нехай G — p -група з циклічною підгрупою індексу p . G — адитивна група майже-кілля з одиницею тоді і тільки тоді, коли виконується одне з наступних тверджень:*

1. $G = \langle a \mid a^{p^n} \rangle, n \geq 1$.

2. $G = \langle a, b \mid a^{p^{n-1}}, b^p, ba = ab \rangle, n \geq 2$.

3. $G = \langle a, b \mid a^{p^{n-1}}, b^p, ba = a^{1+p^{n-2}}b \rangle, p$ — непарне, $n \geq 3$.

4. $G = \langle a, b \mid a^4, b^2, ba = a^{-1}b \rangle$.

5. $G = \langle a, b \mid a^{2^{n-1}}, b^2, ba = a^{1+2^{n-2}}b \rangle, n \geq 4$.

У розділі 3 вивчаються локальні майже-кільця на скінченних неабелевих 2-породжених p -групах.

Класифікація скінченних неабелевих 2-породжених p -груп з циклічним комутантом для непарних простих чисел p дана Мехом [67] (див. також [66]).

Теорема 3.1. *Нехай G — скінченна неабелева 2-породжена p -група з циклічним комутантом для непарних простих чисел p . Далі дані визначальні співвідношення всіх неізоморфних груп G .*

$$(A.1) \quad G = \langle a, b \mid a^{p^l} = b^{p^m} = 1, b^a = b^a = b^{1+p^s} \rangle, \text{ де } 1 \leq s < m \text{ та } m - s \leq l.$$

$$(A.2) \quad G = \langle a, b \mid b^{p^m} = 1, b^a = b^{1+p^s}, a^{p^l} = b^{p^h} \rangle, \text{ де } 1 \leq s < h < m \text{ та } m - s \leq h < l.$$

$$(B.1) \quad G = \langle a, b, u \mid a^{p^l} = b^{p^m} = u^{p^n} = 1, b^a = bu, u^a = u^b = u \rangle, \text{ де } 1 \leq n \leq m \leq l.$$

$$(B.2) \quad G = \langle a, b, u \mid a^{p^l} = u^{p^n} = 1, b^{p^m} = u^{p^k}, b^a = bu, u^a = u^b = u \rangle, \text{ де } n \leq l, n \leq m, 1 \leq k < n.$$

$$(B.3) \quad G = \langle a, b, u \mid u^{p^n} = 1, a^{p^l} = u^{p^h}, b^{p^m} = u^{p^k}, b^a = bu, u^a = u^b = u \rangle, \text{ де } 1 \leq k < h < n \leq m, m + h - k < l.$$

$$(C.1) \quad G = \langle a, b, u \mid a^{p^l} = b^{p^m} = u^{p^n} = 1, u^{p^n} = 1, b^a = bu, u^a = u^{1+p^s}, u^b = u \rangle, \text{ де } n \leq l, n \leq m, 0 < s < n.$$

$$(C.2) \quad G = \langle a, b, u \mid a^{p^l} = u^{p^n} = 1, b^a = bu, u^a = u^{1+p^s}, u^b = u, b^{p^m} = u^{rp^k} \rangle, \text{ де } n \leq l, k \leq m, r \not\equiv 0(p), 0 < k < n, 0 < s < n, p^m \equiv rp^{k+s}(p^n).$$

$$(D.1) \quad G = \langle a, b, u \mid a^{p^l} = u^{p^h}, b^a = bu, u^a = u^{1+p^s}, u^b = u, b^{p^m} = u^{p^n} = 1 \rangle, \text{ де } n \leq l, n - s \leq h < n \leq m, 0 < s < n.$$

(D.2) $G = \langle a, b, u \mid a^{p^l} = u^{p^h}, u^{p^n} = 1, b^a = bu, u^a = u^{1+p^s}, u^b = u, b^{p^m} = u^{rp^k} \rangle$, $\partial e \ 0 < h < n \leq l, 0 < s < n, n - s \leq h, r \equiv 0(p), 0 < k < n, k < m, p^m \equiv rp^{k+s}(p^n)$, *та якщо $k < h$, то $l + k > m + h$, якщо $h \leq k$, то $m + n - s > l + k - h$.*

(E.1) $G = \langle a, b, u \mid b^{p^m} = u^{p^n} = 1, b^a = bu, u^a = u^{1+p^s}, u^b = u, b^{p^h} = a^{p^l} \rangle$, $\partial e \ 0 < s < n, 0 < h < m, 0 < l - h < n - s, n \leq h$.

(E.2) $G = \langle a, b, u \mid b^{p^m} = u^{p^n} = 1, b^a = bu, u^a = u^{1+p^s}, u^b = u, a^{p^l} = b^{p^h} u^{tp^j} \rangle$ $\partial e \ n \leq l, 0 < h < m, 0 < s < n, 0 < l - h < n - s, n \leq m, t \not\equiv 0(p), 0 \leq j < h, j < n, p^h + tp^{s+j} \equiv 0(p^n)$ *та $n \leq j + m - h$.*

(E.3) $G = \langle a, b, u \mid b^{p^m} = u^{p^n} = 1, b^a = bu, u^a = u^{1+p^s}, u^b = u, a^{p^l} = b^{p^h} u^{tp^j} \rangle$ $\partial e \ n \leq l, 0 < h < m, 0 < s < n, 0 < l - h < n - s, n \leq m, t \not\equiv 0(p), 0 \leq j < h, j < n, p^h + tp^{s+j} \equiv 0(p^n)$ *та $n > j + m - h$.*

(F.1) $G = \langle a, b, u \mid u^{p^n} = 1, b^a = bu, u^a = u^{1+p^s}, u^b = u, b^{p^m} = u^{rp^k}, a^{p^l} = b^{p^h} u^{tp^j} \rangle$ $\partial e \ 0 < s < n, 0 < k < n, s < m, k < m, p^m \equiv rp^{k+s}(p^n), r \not\equiv 0(p), h < l, h < m, l - h < n - s, t \not\equiv 0(p), n \leq l, p^h + tp^{j+s} \equiv 0(p^n), rp^k + tp^{j+m-h} \equiv 0(p^n)$.

(F.2) $G = \langle a, b, u \mid u^{p^n} = 1, b^a = bu, u^a = u^{1+p^s}, u^b = u, a^{p^l} = b^{p^h} u^{tp^j}, b^{p^m} = u^{rp^k} \rangle$, $\partial e \ 0 < s < n, 0 < k < n, k < m, s < m, p^m \equiv rp^{k+s}(p^n), r \not\equiv 0(p), h < l, h < m, l - h < n - s, t \not\equiv 0(p), n \leq l, p^h + tp^{j+s} \equiv 0(p^n), rp^k + tp^{j+m-h} \not\equiv 0(p^n), j + m + n > l + s + k$.

В статті Менегаццо [66] знайдено групи автоморфізмів скінченних неабелевих 2-породжених p -груп з циклічним комутантом ($p > 2$).

Лема 3.4. *Групи автоморфізмів груп типів (A.2), (B.3), (D.1), (D.2), (E.1), (E.2), (E.3), (F.1) і (F.2) є p -групами.*

Як наслідок маємо наступне твердження.

Лема 3.5. *Не існує локальних майже-кілець з адитивною групою одного з типів (A.2), (B.3), (D.1), (D.2), (E.1), (E.2), (E.3), (F.1) чи (F.2).*

Наступна теорема дає достатні умови для існування скінченних локальних майже-кілець, адитивна група яких ізоморфна групі $G(p^m, p^n, r)$.

Теорема 3.35. *Для кожного простого числа p та таких додатних цілих m, n , що або $m \geq n + r \geq 2r + \lfloor \frac{2}{p} \rfloor$, або $p = 2$, $2 < m \leq n$ та $r = 1$ існує локальне майже-кілець R , адитивна група якого R^+ ізоморфна групі $G(p^m, p^n, r)$.*

У підрозділі 3.3 вивчаються локальні майже-кілець на групах типу B.1.

Нехай R — локальне майже-кілець з одиницею i , група R^+ якого ізоморфна групі $G(p^m, p^n, p^d)$. Тоді $R^+ = \langle a \rangle + \langle b \rangle + \langle c \rangle$ з елементами a, b та c , що задовольняють співвідношення $ap^m = bp^n = cp^d = 0$, $-b + a + b = a + c$ та $-a + c + a = -b + c + b = c$ з $1 \leq d \leq n \leq m$, де $a = i$ та кожен елемент $x \in R$ однозначно записується у вигляді $x = ax_1 + bx_2 + cx_3$ з коефіцієнтами $0 \leq x_1 < p^m$, $0 \leq x_2 < p^n$ та $0 \leq x_3 < p^d$.

Покажемо, що множина L усіх необоротних елементів R є підгрупою індексу p в R^+ .

Теорема 3.49. *Мають місце такі твердження:*

1. $L = \langle a \cdot p \rangle + \langle b \rangle + \langle c \rangle$ і, зокрема, підгрупа L має індекс p в R^+ та $|R^*| = p^{m+n+d-1}(p-1)$;
2. $x = ax_1 + bx_2 + cx_3$ є оборотним елементом тоді і тільки тоді, коли $x_1 \not\equiv 0 \pmod{p}$.

Отримуємо наступну формулу для множення елементів $x = ax_1 + bx_2 + cx_3$ та $y = ay_1 + by_2 + cy_3$ у локальному майже-кілці R .

Наслідок 3.50. Якщо $x, y \in R$ з $1 \leq d \leq n \leq m$ і $xb = a\alpha(x) + b\beta(x) + c\gamma(x)$, то

$$\begin{aligned} xy &= a(x_1y_1 + y_2\alpha(x)) + b(x_2y_1 + y_2\beta(x)) + \\ &+ c(-x_1x_2\binom{y_1}{2} - \binom{y_2}{2}\alpha(x)\beta(x) - x_2y_1y_2\alpha(x) + \\ &+ x_3y_1 + y_2\gamma(x) + x_1y_3\beta(x) - x_2y_3\alpha(x)), \end{aligned}$$

де відображення $\alpha: R \rightarrow \mathbb{Z}_{p^m}$, $\beta: R \rightarrow \mathbb{Z}_{p^n}$ і $\gamma: R \rightarrow \mathbb{Z}_{p^d}$, та мають місце наступні твердження:

(0) $\alpha(0) \equiv 0 \pmod{p^m}$, $\beta(0) \equiv 0 \pmod{p^n}$ and $\gamma(0) \equiv 0 \pmod{p^d}$ тоді і тільки тоді, коли майже-кільце R є нуль-симетричним;

(1) $\alpha(x) \equiv 0 \pmod{p}$;

(2) якщо $\beta(x) \equiv 0 \pmod{p}$, то $x_1 \equiv 0 \pmod{p}$;

(3) $\alpha(xy) \equiv x_1\alpha(y) + \alpha(x)\beta(y) \pmod{p^m}$;

(4) $\beta(xy) \equiv x_2\alpha(y) + \beta(x)\beta(y) \pmod{p^n}$;

(5) $\gamma(xy) \equiv -x_1x_2\binom{\alpha(y)}{2} - \alpha(x)\beta(x)\binom{\beta(y)}{2} - x_2\alpha(x)\alpha(y)\beta(y)$

$$+ x_3\alpha(y) + \gamma(x)\beta(y) + x_1\beta(x)\gamma(y) - x_2\alpha(x)\gamma(y) \pmod{p^d}.$$

Наступна теорема показує, що умови, наведені в теоремі 3.49, є достатніми для існування скінченних локальних майже-кільць на $G(p^m, p^n, p^d)$. Більш того, кожна група $G(p^m, p^n, p^d)$ є адитивною групою майже-кільця з одиницею.

Теорема 3.51. Для кожного простого числа p та додатних цілих чисел m, n та d з $1 \leq d \leq n \leq m$ існує локальне майже-кільце R , адитивна група якого R^+ ізоморфна групі $G(p^m, p^n, p^d)$.

Як наслідок маємо наступне твердження.

Наслідок 3.52. *Кожна група $G(p^m, p^n, p^d)$ є адитивною групою майже-кільця з одиницею.*

У розділі 4 досліджуються напівдистрибутивні майже-кільця з одиницею та локальні майже-кільця.

Наведемо означення напівдистрибутивного майже-кільця.

Означення 4.5. *(Ліве) майже-кільце R називається напівдистрибутивним, якщо таким є множення справа відносно його додавання. Іншими словами, для будь-яких елементів $r, s, t \in R$ виконується рівність $(r + s + r)t = rt + st + rt$.*

Відомо, що адитивна група будь-якого дистрибутивного майже-кільця з одиницею є абелевою. Наступне твердження поширює цей факт на напівдистрибутивні майже-кільця.

Лема 4.8. *Адитивна група кожного напівдистрибутивного майже-кільця R з одиницею є абелевою.*

Теорема 4.15. *Напівдистрибутивне майже-кільце R з одиницею є простим як майже-кільце тоді і тільки тоді, коли R є простим асоціативним кільцем.*

У розділі 5 використовуючи пакет YangBaxter [119], надано класифікацію брейсів (до порядку 32) та косих брейсів (до порядку 16) відповідно до адитивних або мультиплікативних груп, які є p -групами Міллера–Морено. Крім того, ми надаємо деяку інформацію щодо брейсів, що стосуються, пакету LocalNR.

У розділі 6 наведено алгоритм побудови скінченних локальних майже-кілець, функції для майже-кілець та груп для пакету LocalNR, класифікація локальних майже-кілець малих порядків. Також вивчаються ендоециклічні групи та локальні майже-кільця.

Алгоритм побудови майже-кілець з одиницею базується на наступній теоремі (див. [115, Theorem 1]).

Теорема 6.3. *Нехай G — група, і нехай множина $\text{End } G$ усіх ендое-*

морфізмів G розглядається як моноїд щодо композиції ендоморфізмів. Тоді G — адитивна група майже-кілця з одиницею тоді і тільки тоді, коли існують елемент $g \in G$ та підмоноїд F групи $\text{End } G$ такі, що $G = g^F$ та $g^\phi = g^\psi$ лише тоді, коли $\phi = \psi$ для будь-яких $\phi, \psi \in F$.

Наступна теорема описує умови, за яких майже-кілець $Nr = (G, \cdot, \star_F)$, побудоване на G моноїдом F , є локальним.

Теорема 6.4. *Нехай група G , її елемент g та підмоноїд F з $\text{End } G$ задовольняють висновок теореми 6.3 і нехай $A = F \cap \text{Aut } G$. Майже-кілець $Nr = (G, \cdot, \star_F)$ є локальним тоді й тільки тоді, коли існує така підгрупа L групи G , що $G = g^A \cup L$ та $g^A \cap L = \emptyset$.*

Функції для майже-кілець для пакету LocalNR:

- TheAdditiveGroupsOfLibraryOfLNRsOfOrder
- TheLibraryOfLNRsOnGroup
- LocalNearRing
- AllLocalNearRings
- IsAdditiveGroupOfLibraryOfLNRs
- InfoLocalNearRing

Функції для груп для пакету LocalNR:

- IsMinimalNonAbelianGroup
- IsMetacyclicPGroup
- EndoOrbitsOfGroup
- IsEndoCyclicGroup

Класифіковано 2-породженні групи є адитивними групами локальних майже-кілець порядку 64 (теорема 7.1).

Теорема 7.4 описує такі групи порядку $81 = 3^4$. Зокрема, серед 15 неізоморфних груп цього порядку лише 9 є такими групами.

Зазначимо, що існують 15 неізоморфних груп порядку $81 = 3^4$, з яких 9 є адитивними групами локальних майже-кілець. Теорема 7.5 описує 2-породжені групи порядку $243 = 3^5$ з цією властивістю. Зокрема, серед 29 неізоморфних 2-породжених груп цього порядку лише 10 є такими адитивними групами.

Відомо, що існує 5 неізоморфних груп порядку $11^3 = 1331$. Виявляється, що всі вони є адитивними групами локальних майже-кілець. Теорема 7.8 містить список усіх неізоморфних майже-кілець цього порядку.

Існує 267 неізоморфних груп порядку $64 = 2^6$, з яких 53 є 2-породженими групами, і лише 39 з цих груп є ендоеиклічними (лема 7.10). Більше того, 24 з цих груп є адитивними групами локальних майже-кілець.

Теорема 7.11. *Нехай G — 2-породжена група порядку 64. Якщо G — адитивна група локального майже-кілля R , то G є ендоеиклічною.*

Існує 56092 неізоморфних груп порядку $256 = 2^8$, з яких 540 є 2-породженими групами: 3 групи мають експоненту 128, 9 груп мають експоненту 64, 30 груп мають експоненту 32, 107 груп мають експоненту 16, 84 групи мають експоненту 8, та 3 групи мають експоненту 4.

Визначено всі ендоеиклічні 2-породжені групи G порядку 256 експоненти 16 та порядок множини всіх елементів групи G , порядок яких дорівнює експоненті цієї групи (лема 7.17).

Розділ 1

Огляд літератури та попередні відомості

1.1. Майже-поля

Майже-полем називається непорожня множина F з визначеними на ній двома алгебраїчними операціями, додаванням та множенням, що задовольняє наступним умовам:

- 1) F утворює абелеву групу відносно додавання, яка називається *адитивною групою* майже-поля F та позначається через F^+ ;
- 2) множина ненульових елементів $F \setminus 0$ із F утворює групу відносно множення, яка називається *мультиплікативною групою* майже-поля F та позначається через F^* ;
- 3) виконується односторонній дистрибутивний закон $a(b + c) = ab + ac$ для всіх $a, b, c \in F$.

Нижче $SL(2, q)$ позначає спеціальну лінійну групу степеня 2 над скінченним полем із q елементів, C_n — циклічну групу порядку n .

Систематичне вивчення скінченних майже-полів було започатковано Цассенхаузом у [121], де доведена абелевість їх адитивної групи та охарактеризовано їх мультиплікативні групи як групи регулярних автоморфізмів абелевих груп (див., М. Холл [13], теорема 20.7.2).

Теорема 1.1. *Нехай F — скінченне майже-поле. Тоді його порядок є степенем деякого простого числа, а його мультиплікативна група F^* є або метациклічною групою, або ізоморфною одній з наступних семи груп:*

I) $SL(2, 3);$

II) $SL(2, 3) \times C_5;$

III) підгрупа $O(2, 7)$ порядку 48 групи $SL(2, 7);$

IV) $O(2, 7) \times C_{11};$

V) $SL(2, 5);$

VI) $SL(2, 5) \times C_7;$

VII) $SL(2, 5) \times C_{29}.$

Майже-поле по суті те саме, що група з групою автоморфізмів, що діє точно транзитивно на її нетривіальних елементах. Група G діє точно транзитивно (точно 2-транзитивно) на множині S , якщо для кожних двох різних елементів $s, t \in S$ (кожних двох пар s_1, s_2 та t_1, t_2 різних елементів S) існує рівно один $g \in G$ з $s^g = t$ ($s^g_i = t_i$ для $i = 1, 2$).

Якщо N є майже-полем, то напівпрямий добуток $N^+ \rtimes N^*$ допускає точно 2-транзитивну дію на N , в якій N^+ діє додаванням, а N^* — множенням. Давня гіпотеза стверджує, що зворотне також вірне. У скінченному випадку це було доведено Цассенхаузом у вищезгаданій статті. Загальний випадок залишається відкритим.

Ньюман [68] поширює результат Цассенхауза на всі майже-поля.

S — група, записана адитивно, задана разом з автоморфізмом.

A) У S рівняння $x + x = a$ має рішення для кожного a .

В) У S рівняння $x + x = a$ має не більше одного рішення для будь-якого a .

С) Даний автоморфізм має порядок 2.

Д) Цей автоморфізм не залишає незмінним жодного елемента S , окрім 0.

Теорема 1.2 (Theorem, [68]). *Група з властивостями A)–D) є абелевою.*

В роботі Лая [55] мультиплікативна група майже-поля названа спадковою, якщо кожна її підгрупа ізоморфна мультиплікативній групі деякого майже-поля, та отримано повну характеристику скінченних таких груп майже-полів.

Нагадаємо, що просте число p вигляду $p = 2^n - 1$ для деякого цілого n називається простим Мерсенна. Це невирішена проблема, чи існує нескінченно багато простих Мерсенна.

Означення 1.3 (Definition 1, [55]). Додатне ціле m називається z -числом, якщо кожен дільник $d > 1$ числа m має вигляд $q^n - 1$, де q — просте число, n — додатне ціле число.

Теорема 1.4 (Theorem 1, [55]). *Додатне ціле m є z -числом тоді і тільки тоді, коли $m = 2, 4, 6, 8, 12, 16, 24, 48$ або простим Мерсенна.*

Теорема 1.5 (Theorem 3, [55]). *Скінченна група G є спадковою групою майже-поля тоді і тільки тоді, коли G є однією з наступних груп:*

- 1) G є циклічною групою порядку z -числа.
- 2) $G \cong Q_8$.
- 3) $G \cong C_8 \rtimes C_3$.
- 4) $G \cong Q_8 \rtimes C_3$.

Майже-поля з неабелево спадковими мультиплікативними групами, в яких умова ізоморфізму з мультиплікативними групами майже-полів накладається лише на неабелеві підгрупи, були класифіковані у статті [1].

Теорема 1.6 (Теорема 3, [1]). *Нехай F — скінченне майже-поле, мультиплікативна група F^* якого є неабелево спадковою. Тоді F^* — група одного з наступних типів:*

- 1) *циклічна група;*
- 2) *група кватерніонів Q_8 ;*
- 3) *неабелева метациклічна група порядку 24;*
- 4) *група $SL(2, 3)$;*
- 5) *неабелева метациклічна група порядку 63;*
- 6) *неабелева метациклічна група порядку 80.*

Оскільки групи типу 3)–6) теорема 1.6 є групами Шмідта, то переформулюємо цю теорему:

Теорема 1.7. *Нехай F — скінченне майже-поле, мультиплікативна група F^* якого є неабелево спадковою. Тоді F^* — група одного з наступних типів:*

- 1) *циклічна група;*
- 2) *група кватерніонів Q_8 ;*
- 3) *група Шмідта.*

В цій статті [1] також описано майже-поля з мультиплікативною групою Міллера–Морено.

Лема 1.8 (Лема 6, [1]). *Нехай F — скінченне майже-поле, мультиплікативна група F^* якого є групою Міллера–Морено. Тоді F^* є або групою кватерніонів порядку 8, або неабелевою метациклічною групою одного з порядків 24, 63 або 80.*

У статті [8] дано опис всіх майже-полів з мультиплікативною групою Шмідта. А саме, якщо R — майже-поле, то мультиплікативна група R^* ізоморфна або групі $SL(2, 3)$, або одній із груп Міллера–Морено порядків 24, 63 та 80.

Теорема 1.9 (Теорема 6, [8]). *Нехай F — скінченне майже-поле p^s , мультиплікативна група F^* якого є групою Шмідта. Тоді F^* — група одного з наступних типів:*

- 1) група $SL(2, 3)$;
- 2) неабелева метациклічна група одного з порядків 24, 63, 80.

У подальшому майже-поля вивчалися головним чином завдяки їх застосуванням у геометрії. Вперше майже-поля застосували в геометрії Веблен і Вадербарн [118]. Теорії майже-полів присвячено монографію Виглінга [120], в якій систематизовано більшість результатів про майже-поля.

1.2. Майже-кільця з одиницею

Майже-кільце — це непорожня множина з двома бінарними операціями (додавання та множення), яка відрізняється від кільця тим, що комутативність першої операції та один із дистрибутивних законів (у аналізованому випадку, правий) не обов'язково є істинними. У визначенні не вимагається, щоб майже-кільце мало одиницю. Отже, відсутність

одного з дистрибутивних законів у визначенні майже-кілець є важливішою умовою, ніж відсутність комутативності операції додавання, що створює основні труднощі в їх дослідженні.

Проблема визначення класів груп, які можуть бути адитивними або мультиплікативними групами майже-кілець з одиницею, є важливою з точки зору як теорії груп, так і теорії майже-кілець. Однак, наразі ця проблема вивчена досить мало. З цієї причини розробка нових методів теорії майже-кілець (зокрема, локальних у випадку, коли множина необоротних елементів є адитивною підгрупою) видається важливою та сприяє їх класифікації.

До початку 40-х рр. минулого сторіччя відбувалося дослідження основних загальних властивостей майже-кілець, описання деяких класів скінченних майже-кілець, застосування в теорії груп підстановок (Цассенхауз [121], Таусскі-Тод [117], Веблен та Ваддербарн [118]). Подальший розвиток цієї теорії стимулювали роботи Блекетта [26], Х. Нойман [69], Бетча [24], Бейдлемана [20] та інші. З початку 40-х рр. до кінця 70-х рр. теорія майже-кілець застосовується в задачах класифікації нелінійних математичних структур. Закладено основи структурної теорії майже-кілець. У цей період виявлено простоту майже-кілець деяких класів і, зокрема, повних майже-кілець перетворень груп (симетричних майже-кілець на групах) та поліноміальних майже-кілець над полями нульової характеристики. Отримано аналоги теорем Джекобсона, Ваддербарна—Артіна, деяких інших теорем структурної теорії кілець. Покладено початок теорії радикалів майже-кілець.

Загальній теорії майже-кілець присвячені монографії Пільца [70], Мелдрума [65], Клея [29], К. Ферреро та Г. Ферреро [37], Локхарта [56]. До проблематики теорії майже-кілець звертались Курош, Плоткін та їх учні. Деяким питанням теорії майже-кілець та її зв'язками з теорією мультиоператорних груп присвячено роботи Поліна, Кузьміна, Марина,

Каарлі та інших. Пізніше з'явилися роботи, пов'язані з вивченням групових відображень та майже-кілець перетворень (Калужніна та Суцанського, Кириченко, Усенко, Кіртадзе, Міхайлова, Рябухо).

Локхарт в своїй книзі [56] відмітив, що багато ранніх робіт з майже-кілецевих моделей прагнули використати явні успіхи теорії кілець та комутативної алгебри. Це було найбільш помітно в теорії представлень та радикалів, з багатьма статтями [20], [21], [39] на ці теми в 1960-х та 1970-х роках [70], але це також включало узагальнення стандартних тем, таких як групові майже-кілеця [65], тензорні добутки [57], теорія категорій [43].

Природним прикладом є майже-кілець $\text{Map}(G)$ усіх відображень групи G в себе з додаванням та множенням, визначених як $x^{f+g} = x^f x^g$ та $x^{fg} = (x^f)^g$ для всіх $x \in G$. Зокрема, для будь-якої нетривіальної групи G в $\text{Map}(G)$ дійсний лише лівий розподільний закон $f(g+h) = fg + fh$.

Якщо e є нейтральним елементом G , то відображення o , i з $x^o = e$ та $x^i = x$ для всіх $x \in G$ дорівнюють нулю та є одиничним елементом $\text{Map}(G)$.

Адитивна група $\text{Map}(G)^+$ групи $\text{Map}(G)$ ізоморфна декартовому добутку $|G|$ копій G , а мультиплікативна група $\text{Map}(G)^*$ збігається із симетричною групою $\text{Sym}(G)$ на G .

Множини $\{f \in \text{Map}(G) | e^f = e\}$ та $\{g \in \text{Map}(G) | x^g = \text{const}\}$ є підмайже-кілецями $\text{Map}(G)$, які називаються його нуль-симетричною та константною частинами та позначаються $\text{Map}_0(G)$ та $\text{Map}_c(G)$, відповідно.

Оскільки $\text{Map}_0(G)^+$ є нормальною групою в $\text{Map}(G)^+$, $\text{Map}_c(G)$ ізоморфна G та $\text{Map}(G) = \text{Map}_0(G) + \text{Map}_c(G)$, де $\text{Map}_0(G) \cap \text{Map}_c(G) = \{o\}$, то $\text{Map}(G)$ є напівпрямою сумою $\text{Map}_0(G)$ та $\text{Map}_c(G)$.

Багато прикладів майже-кілець виникають по суті однаково. Стандартні приклади мають форму множини всіх відображень групи в себе та певні підмножини цієї множини. Множення майже-кілець у цих

випадках зазвичай є композицією відображень. В основі цих прикладів лежить загальний категоріальний механізм для побудови майже-кілець, який також включає інші типи майже-кілець, утворених за досить різних обставин. Голкомб [43] сформулював теорію представлень, використовуючи найбільш тісно пов'язану категорію для забезпечення представлення об'єктів, а не традиційний підхід N -груп або N -модулів.

Лай [52] довів наступну теорему.

Теорема 1.10 (Theorem, [52]). *Нехай R — скінченне майже-кілець з одиницею 1 таке, що $(-1)x = x$ означає, що $x = 0$. Тоді $(R, +)$ є абелевим.*

А також наведено приклад майже-кілеця, яке задовольняє умови теореми, але не є майже-полем.

Приклад 1.11 (Example, [52]). Нехай R — таке скінченне майже-поле, що $(R, +)$ не має елементів другого порядку. Розглянемо

$$G = R \times R = \{(r, s) : r \in R, s \in R\}.$$

Визначимо “+” та “ $\cdot$ ” наступним чином:

$$(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2)$$

та

$$(r_1, s_1) \cdot (r_2, s_2) = (r_1 \cdot r_2, s_1 \cdot s_2).$$

Тоді легко перевірити, що $(G, +, \cdot)$ є майже-кілцем, яке задовольняє умови теореми 1.10. Оскільки G містить нульові дільники, ми робимо висновок, що G не є майже-полем.

Різні класи груп не можуть бути адитивними групами майже-кілець з одиницею. Використовуючи глибоку теорему про те, що група непарного порядку є розв'язною [36].

Теорема 1.12 (Theorem, [36]). *Всі скінченні групи непарного порядку є розв'язними.*

Клей та Малон [31] довели, що проста група складеного порядку не може бути адитивною групою майже-кілець з одиницею.

Наслідок 1.13 (Corollary, [31]). *Проста група складеного порядку не може бути адитивною групою майже-кілець з одиницею.*

Використовуючи результат з [36], Лай [53] розширює цей результат, а саме, показує, що скінченна неабелева група з рівно однією нетривіальною власною нормальною підгрупою не може бути адитивною групою майже-кілець з одиницею.

Теорема 1.14 (Theorem 1, [53]). *Нехай $(G, +)$ — скінченна некомутативна група з рівно однією власною нормальною підгрупою. Тоді $(G, +)$ не може бути адитивною групою майже-кілець з одиницею i .*

Використовуючи лише методи теорії чисел, в статтях [31] та [30] відповідно показано, що симетричні групи S_n , $n \geq 3$ та знакозмінні групи A_n , $n \geq 4$, не можуть бути адитивними групами майже-кілець з одиницею.

Теорема 1.15 (Theorem 4, [31]). *Нехай $(S_n, +)$ — симетрична група на n символах. Не існує майже-кілець з одиницею адитивна група якого $(S_n, +)$ при $n \geq 3$.*

Крімел [48] навів дуже простий доказ теореми, яка значною мірою узагальнює попередні результати.

Теорема 1.16 (Theorem, [48]). *Нехай $(G, +)$ — група, що має елементи M різних простих порядків. Якщо кожен антиланцюг решітки нормальних підгруп групи G має потужність меншу за M , то $(G, +)$ не може бути адитивною групою майже-кілець з одиницею.*

Клей [28] визначив усі майже-кільця з одиницею на $(D_4, +)$. Джонсон [50] розглянув майже-кільця, визначені на $(D_n, +)$, дієдральній групі порядку $2n$ та показав, що якщо $(D_n, +, \cdot)$ є майже-кільцем з мультиплікативною одиницею, то нормальні праві підмодулі та праві ідеали $(D_n, +, \cdot)$ збігаються тоді і тільки тоді, коли всі нормальні праві підмодулі є ануляторними правими ідеалами. Доведено існування майже-кільця з мультиплікативною одиницею на $(D_n, +)$, де $n = 2p$, p — просте число. Показуємо, що якщо p — непарне просте число, то існує, з точністю до ізоморфізму, єдине майже-кільце з мультиплікативною одиницею на $(D_n, +)$. Крімел також (незалежно) зауважив, що існує, з точністю до ізоморфізму, єдине майже-кільце з мультиплікативною одиницею на $(D_n, +)$, $n = 2q$.

В роботі [79] показано, що не існує майже-кільця з одиницею, адитивна група яких ізоморфна групі Шмідта.

Майже-кільце R називається *дистрибутивно породженим*, якщо існує піднапівгрупа $S \leq (R_d, \cdot)$ така, що адитивна група R^+ породжена S . У цьому випадку часто пишуть $R = (R, S)$.

Дистрибутивно породжені майже-кільця дозволяють створити багато сильнішу теорію структур та теорію представлень, ніж майже-кільця загалом. Багато фундаментальних теорем про кільця можна відповідним чином узагальнити, тоді як, з іншого боку, структурні концепції, властиві майже-кільцям, призводять до значних результатів [38].

Означення 1.17 (Definition 1.2.1, [38]). Елемент c майже-кільця R є дистрибутивним відносно пари елементів a, b з R , якщо $(a+b)c = ac+bc$. Елемент c з R , який є дистрибутивним відносно пар елементів x, y для всіх $x, y \in R$, є дистрибутивним.

Означення 1.18 (Definition 1.2.2, [38]). Майже-кільце R , в якому кожен елемент є дистрибутивним, є дистрибутивним майже-кільцем.

Приклад 1.19 (Example 2, [38]). Нехай R^+ — будь-яка група по додаванню з одиницею 0. Визначимо для всіх $x, y \in R^+$, $xy = 0$. Це множення визначає дистрибутивне майже-кільце R .

Теорема 1.20 (Theorem 4.4.3, [38]). *Нехай R — дистрибутивно породжене майже-кільце з одиницею. Кожна з наступних умов є (необхідною та) достатньою для того, щоб R було кільцем:*

- R є дистрибутивним,
- R^+ є комутативним.

Статті [39] є продовженням [38], в якій вивчається представлення дистрибутивно породжених майже-кільць відображеннями груп.

Гопкінс [44] довів наступну теорему: якщо R — кільце, яке задовольняє умову спадного ланцюга на правих ідеалах і має або ліву одиницю, або праву одиницю, то R задовольняє умову зростаючого ланцюга на правих ідеалах.

Бейдлман [19] довів подібну теорему для дистрибутивно породжених майже-кільць R з одиницею, адитивна група яких R^+ є розв'язною.

Теорема 1.21 (Theorem, [19]). *Нехай R — дистрибутивно породжене майже-кільце, адитивна група якого R^+ є розв'язною. Якщо R задовольняє умову спадного ланцюга на R -підгрупах, то R є нетеровим.*

Стаття [20] здебільшого присвячена вивченню примітивного радикала дистрибутивно породженого майже-кільця. Примітивний радикал дистрибутивно породженого майже-кільця R містить радикал R , який, у свою чергу, містить як квазірадикал, так і радикал-підгрупу.

Теорема 1.22 (Theorem 1, [20]). *Радикал дистрибутивно породженого майже-кільця R міститься в примітивному радикалі R .*

Отже, можна очікувати, що примітивний радикал буде корисним для визначення певних властивостей квазірадикала та радикала. Стаття [21]

здебільшого є продовженням [20]. Розглядаються лише дистрибутивно породжені майже-кільця R з одиницею. Нагадаємо з [20], що примітивний радикал R містить радикал R , який містить квазірадикал R . Нільрадикал R , який є сумою всіх нільпотентних ідеалів R , міститься в квазірадикалі R . Ідея статті полягає в розвитку певних властивостей нільрадикала дистрибутивно породженого майже-кільця. Дослідження нільрадикалу забезпечить кілька характеристик примітивного радикала, радикала та квазірадикала певних класів дистрибутивно породжених майже-кілець.

Означення 1.23 (Definition 1, [20]). Примітивний ідеал B дистрибутивно породженого майже-кільця R називається строго примітивним тоді і тільки тоді, коли R/B є простим дистрибутивно породженим майже-кільцем.

Означення 1.24 (Definition 2, [20]). Нехай L позначає множину всіх строго примітивних ідеалів майже-кільця R мається на увазі ідеал

$$P(R) = \cap B(B \in L).$$

У роботі [54] використано результат статті [53] і визначимо всі неізоморфні дистрибутивно породжені майже кільця, визначені на симетричних групах $S_n (n \geq 5)$ та скінченних діедральних групах D_p порядку $2p$, p — непарне просте число.

У статті [58] досліджуються два основні питання щодо скінченних діедральних груп порядку $2n$, де n — непарне, та дистрибутивно породжених майже-кілець. Показано, що дистрибутивно породжені майже-кільця, породжені відповідно внутрішніми автоморфізмами, автоморфізмами та ендоморфізмами такої групи, є ідентичними, порядку, що дорівнює $2n^3$.

Теорема 1.25 (Theorem 3, [58]).

$$I(D_{2n}) = A(D_{2n}) = E(D_{2n})$$

та

$$|E_n| = 2n^3.$$

Також отримано результати щодо структури ідеалів цих майже-кілець. Визначено кількість неізоморфних дистрибутивно породжених майже-кілець, які можна визначити на такій дієдральній групі. Це число дорівнює $1 + 2^r$, де r — кількість різних простих чисел, що зустрічаються у розкладі числа n .

Теорема 1.26 (Theorem 7, [58]). *Кількість неізоморфних дистрибутивно породжених майже-кілець, які можна визначити на D_{2n} , дорівнює $1 + 2^r$, де r — кількість різних простих чисел, що входять до факторизації n .*

У наступній статті [59] описано дистрибутивно породжені майже-кілець, породжені відповідно внутрішніми автоморфізмами, автоморфізмами та ендоморфізмами дієдральної групи порядку $2n$, n — парне.

Теорема 1.27 (Theorem 3.1, [59]).

$$|I(D_{2n})| = n^3/4.$$

Теорема 1.28 (Theorem 3.2, [59]).

$$|A(D_{2n})| = n^3/2, \quad n \geq 4.$$

Теорема 1.29 (Theorem 4.1, [59]). *Якщо $4|n$, але $8 \nmid n$, то порядок $E(D_{2n})$ є $n^7/64$. В іншому випадку, порядок $E(D_{2n})$ є $2n^3(n|\gcd(n, 4))^4$.*

У [60] визначено всі типи ізоморфізму дистрибутивно породжених (лівих) майже-кілець, адитивна група яких є нескінченною дієдральною групою D . А саме показано, що на нескінченній дієдральній групі можна визначити рівно шість неізоморфних дистрибутивно породжених майже кілець. Одне має нульове множення, два мають тривіальні множення, в

яких група лівих ануляторів має індекс два, а три є дистрибутивними та мають свої множини добутків, що дорівнюють підгрупі порядку 2.

Берман та Сільверман [22] показали, що в майже-кільці $(N, +, \cdot)$ з двостороннім нулем (тобто $x \cdot 0 = 0 \cdot x = 0$, для всіх $x \in N$) правий ідеал також є правим підмодулем. Якщо $(N, +, \cdot)$ насправді є дистрибутивно породженим майже-кільцем, то всі нормальні праві підмодулі також є правими ідеалами (див. [38]).

Майже-кільця тісно пов'язані з брейсами, які дають розв'язки комбінаторних рівнянь Янга–Бакстера, які відіграють важливу роль у теоретичній фізиці, зокрема, у теорії струн.

1.3. Локальні майже-кільця

Кільце з одиницею, множина всіх необоротних елементів якого утворює ідеал в цьому кільці, називається локальним кільцем. Як легко переконатися, в означенні локального кільця достатньо насправді припускати, що множина всіх необоротних елементів є тільки підгрупою адитивної групи кільця. Замінивши в ньому слово “кільце” на “майже-кільце”, отримуємо означення локальних майже-кільць, вивчення яких вперше було ініційовано Мексоном [61]. В цій же статті встановлено, що адитивна група скінченного нуль-симетричного локального майже-кільця є p -групою.

Наслідок 1.30 (Corollary 7.6, [61]). *Адитивна група скінченного локального кільця є p -групою.*

Більш загальний результат, з якого випливає, що періодична і, зокрема, скінченна адитивна група кожного локального майже-кільця є p -групою скінченної експоненти, отриманий в Амбергом, Хубертом та Сисаком [18].

Мексон [62] показав, що з точністю до ізоморфізму існує $p-1$ локальне майже-кілець з елементарною абелевою адитивною групою порядку p^2 , в яких підгрупи необоротних елементів мають порядок p , тобто тих майже-кілець, які не є майже-полями.

Наслідок 1.31 (Corollary 1.11, [62]). *З точністю до ізоморфізму існує $p-1$ локальних майже-кілець $N = (N, +, \cdot)$ з адитивною групою, ізоморфною $(C_p \times C_p, +)$, які не є майже-полями.*

Разом із фундаментальною роботою Цассенхауза про майже-поля та роботою Клея та Малоне [31], отримано повний опис усіх нуль-симетричних локальних майже-кілець порядку p^2 .

Мексон показав у [63], що кожна нециклічна абелева p -група порядку $p^n > 4$ є адитивною групою нуль-симетричного локального майже-кілця, яке не є кільцем.

Теорема 1.32 ([63]). *Для кожної скінченної нециклічної абелевої p -групи $(G, +)$ порядку $|G| > 4$ існує локальне майже-кілець $N \equiv (N, +, \cdot)$ з $(N, +) = (G, +)$ таке, що N не є кільцем.*

Однак у випадку скінченних неабелевих p -груп ситуація інша. Наприклад, ні узагальнена група кватерніонів, ні неабелева група порядку 8 не можуть бути адитивною групою локального майже-кілця [64].

Локальні майже-кілця порядку p^3 досліджувалися в статтях [5], [83].

Наступне твердження містить класифікацію груп порядку p^3 (див. [13]).

Твердження 1.33. *Нехай G — група порядку p^3 . Далі дані визначальні співвідношення всіх неізоморфних груп G .*

Абелеві групи:

- 1) $a^{p^3} = 1$;
- 2) $a^{p^2} = 1, b^p = 1, ab = ba$;

3) $a^p = b^p = c^p = 1$, $ab = ba$, $ac = ca$, $cb = bc$.

Неабелеві групи порядку $2^3 = 8$:

4) група діедра, $a^4 = 1$, $b^2 = 1$, $a^{-1}b = ba$;

5) група кватерніонів, $a^4 = 1$, $b^2 = a^2$, $a^{-1}b = ba$.

Неабелеві групи порядку p^3 , p — непарне:

4*) $a^{p^2} = 1$, $b^p = 1$, $b^{-1}ab = a^{1+p}$;

5*) $a^p = 1$, $b^p = 1$, $c^p = 1$, $ab = bac$, $ac = ca$, $bc = cb$.

А саме, отримано наступні результати.

Наведено приклади добутоків в локальних майже-кільцях на елементарній абелевій групі порядку p^3 .

Лема 1.34 (Лема 4, [5]). Нехай G ізоморфна групі $G(p, p, p)$. Якщо $x = ax_1 + bx_2 + cx_3$ та $y = ay_1 + by_2 + cy_3 \in G$, то множення

$$x \cdot y = ax_1y_1 + b(x_2y_1 + \beta(x)y_2) + c(x_3y_1 + \nu(x)y_2)$$

з одним з наступних наборів функцій

- $\beta(x) = 1$ та $\nu(x) = 1$;
- $\beta(x) = x_1$ та $\nu(x) = x_1$;
- $\beta(x) = x_1^2$ та $\nu(x) = x_1^2$;
- ...
- $\beta(x) = x_1^{p-1}$ та $\nu(x) = x_1^{p-1}$

визначає локальне майже-кільце $R = (G, +, \cdot)$.

Теорема 1.35 (Теорема 4, [5]). Існує щонайменше p неізоморфних локальних майже-кільць на елементарній абелевій групі порядку p^3 .

Твердження 1.36 (Proposition 2, [83]). *На кожній групі порядку p^3 з $p > 2$ існує локальне майже-кілець.*

Теорема 1.37 (Theorem 2, [83]). *На кожній неметациклічній неабелевій групі порядку p^3 існує щонайменше $p + 1$ неізоморфних локальних майже-кілець.*

Теорема 1.38 (Theorem 3, [83]). *На кожній метациклічній абелевій групі порядку p^3 існує щонайменше $p + 1$ неізоморфних локальних майже-кілець.*

Далі в роботах [84], [85], [86] були вивчені локальні майже-кілець порядку p^4 .

Групи порядку p^4 з $p > 3$ описано в такій теоремі (див., наприклад, [17], [27]).

Теорема 1.39. *Існує 10 неізоморфних груп порядку p^4 з $p > 3$, які є: 6 неізоморфних груп класу нільпотентності 2, які є:*

- $G_1 = \langle a, b \mid a^{p^2} = b^p = [a, [a, b]] = [b, [a, b]] = [a, b]^p = e \rangle = (C_{p^2} \times C_p) \rtimes C_p$;
- $G_2 = \langle a, b \mid a^{p^2} = b^{p^2} = e, [b, a] = b^p \rangle = C_{p^2} \rtimes C_{p^2}$;
- $G_3 = \langle a, b \mid a^{p^3} = b^p = e, [b, a] = a^{p^2} \rangle = C_{p^3} \rtimes C_p$;
- $G_4 = \langle a, b, d \mid a^p = b^p = c^p = d^p = [a, c] = [b, c] = [a, d] = [b, d] = [c, d] = e \rangle = C_p \times ((C_p \times C_p) \rtimes C_p)$, де $c = [a, b]$;
- $G_5 = \langle a, b, c \mid a^{p^2} = b^p = c^p = [a, c] = [b, c] = e, [b, a] = a^p \rangle = C_p \times (C_{p^2} \rtimes C_p)$;
- $G_6 = \langle a, b, c \mid a^{p^2} = b^p = c^p = [a, b] = [a, c] = e, [c, b] = a^p \rangle = (C_{p^2} \times C_p) \rtimes C_p$.

4 неізоморфні групи класу нільпотентності 3, які є:

- $H_1 = \langle a, b \mid a^p = b^p = c^p = [a, c]^p = [b, c] = e, [a, [a, c]] = [b, [a, c]] = e \rangle = (C_p \times C_p \times C_p) \rtimes C_p, \text{ де } c = [a, b];$
- $H_2 = \langle a, b \mid a^{p^2} = b^p = [a, b]^p = [b, [a, b]] = e, [a, [a, b]] = a^p \rangle = (C_{p^2} \rtimes C_p) \rtimes C_p;$
- $H_3 = \langle a, b \mid a^{p^2} = b^p = [a, b]^p = [a, [a, b]] = e, [b, [a, b]] = a^p \rangle = (C_{p^2} \rtimes C_p) \rtimes C_p;$
- $H_4 = \langle a, b \mid a^{p^2} = b^p = [a, b]^p = [a, [a, b]] = e, [b, [a, b]] = a^{2p} \rangle = (C_{p^2} \times C_p) \rtimes C_p.$

Наведемо приклади локальних майже-кілець на групі G_4 .

Лема 1.40 (Lemma 8, [85]). *Нехай R — локальне майже-кілець, адитивна група якого R^+ ізоморфна G_4 і $|R : L| = p$. Якщо $x = ax_1 + bx_2 + cx_3 + dx_4$, $y = ay_1 + by_2 + cy_3 + dy_4 \in R$, тоді відображення $\beta: R \rightarrow \mathbb{Z}_p$, $\gamma: R \rightarrow \mathbb{Z}_p$, $\varphi: R \rightarrow \mathbb{Z}_p$, $\mu: R \rightarrow \mathbb{Z}_p$, $\nu: R \rightarrow \mathbb{Z}_p$ і $\psi: R \rightarrow \mathbb{Z}_p$ може бути одним із наступних:*

$$1) \beta(x) = x_1^i \text{ and } \psi(x) = x_1^i \ (0 < i < p),$$

$$\gamma(x) = \varphi(x) = \mu(x) = \nu(x) = 0;$$

$$2) \beta(x) = 1 \text{ and } \psi(x) = 1, \gamma(x) = \varphi(x) = \mu(x) = \nu(x) = 0.$$

Як наслідок леми 1.40 маємо наступний результат.

Теорема 1.41 (Theorem 4, [85]). *Для кожного непарного простого числа p існує локальне майже-кілець R , адитивна група якого R^+ ізоморфна G_4 .*

Далі, наведемо приклади локальних майже-кілець на групі G_5 .

Лема 1.42 (Lemma 13, [85]). *Нехай R — локальне майже-кілець, адитивна група якого R^+ ізоморфна G_5 , та $|R : L| = p$. Якщо $x = ax_1 + bx_2 + cx_3$, $y = ay_1 + by_2 + cy_3 \in R$, тоді відображення*

$\alpha : R \rightarrow \mathbb{Z}_{p^2}$, $\beta : R \rightarrow \mathbb{Z}_p$, $\gamma : R \rightarrow \mathbb{Z}_p$, $\nu : R \rightarrow \mathbb{Z}_{p^2}$, $\mu : R \rightarrow \mathbb{Z}_p$ та $\phi : R \rightarrow \mathbb{Z}_p$ можуть бути одними з наступних:

$$1) \beta(x) = \phi(x) = \begin{cases} 1, & x_1 \not\equiv 0 \pmod{p}; \\ 0, & x_1 \equiv 0 \pmod{p}, \end{cases}$$

$$\alpha(x) = \gamma(x) = \mu(x) = \nu(x) = 0;$$

$$2) \beta(x) = \phi(x) = 1, \alpha(x) = \gamma(x) = \mu(x) = \nu(x) = 0.$$

Як наслідок леми 1.42 маємо наступний результат.

Теорема 1.43 (Theorem 5, [85]). *Для кожного непарного простого числа p існує локальне майже-кільце R , адитивна група якого R^+ ізоморфна G_5 .*

Далі ми наводимо приклади локальних майже-кілець, адитивна група яких R^+ ізоморфна H_1 .

Лема 1.44 (Lemma 7, [86]). *Нехай R — локальне майже-кільце, адитивна група якого R^+ ізоморфна H_1 , та $|R : L| = p$. Якщо $x = ax_1 + bx_2 + cx_3 + dx_4$, $y = ay_1 + by_2 + cy_3 + dy_4 \in R$, тоді відображення $\beta : R \rightarrow \mathbb{Z}_p$, $\gamma : R \rightarrow \mathbb{Z}_p$ і $\phi : R \rightarrow \mathbb{Z}_p$ можуть бути $\beta(x) \equiv x_1^2 \pmod{p}$ та*

$$\phi(x) = \begin{cases} x_2^2, & x_1 \equiv 0 \pmod{p} \\ 0, & x_1 \not\equiv 0 \pmod{p} \end{cases},$$

$$\gamma(x) \equiv 0 \pmod{p}.$$

Як наслідок леми 1.44 маємо наступний результат.

Теорема 1.45 (Theorem 5, [86]). *Для кожного простого числа $p > 3$ існує локальне майже-кільце R , адитивна група якого R^+ ізоморфна H_1 .*

Наступна теорема дає достатні умови для існування скінченного локального майже-кілеця, адитивна група якого ізоморфна групі H_2 .

Теорема 1.46 (Theorem 3, [84]). *Для кожного простого $p > 3$ існує локальне майже-кілець R , адитивна група якого R^+ ізоморфна H_2 .*

Зазначимо, що залишається відкритим питання, які неабелеві групи порядку p^n можуть бути адитивними групами локальних майже-кілець [35].

Основні результати, що стосуються локальних майже-кілець, підсумовані в оглядах Сисака [114], Раєвської І. і Раєвської М. [4].

Ряд робіт було спрямовано на встановлення взаємозв'язків між локальним майже-кілцем та його мультиплікативною групою. Наведемо деякі з цих результатів.

Локальні майже-кілця, мультиплікативні групи яких є абелевими, і які не є кілцями, вивчалися Городником [42]. Ним доведено, що множина всіх необоротних елементів такого майже-кілця утворює абелеву підгрупу індексу 2 в його адитивній групі. Зокрема, він описав локальні майже-кілця з циклічними групами одиниць. А саме, якщо мультиплікативна група локального майже-кілця є циклічною, то адитивна група є або групою типу $(2, 2, 2)$, або $(2, 4)$.

Наступним природним кроком є дослідження локальних майже-кілець, мультиплікативні групи яких є в певному сенсі близькими до абелевих, зокрема, мінімальними неабелевими або, в іншій термінології, групами Міллера–Морено. Локальні майже-кілця з мультиплікативною 2-групою Міллера–Морено вивчалися в [9].

Теорема 1.47 (Теорема 2, [9]). *Нехай R — локальне майже-кілець, мультиплікативна група R^* якого є 2-групою Міллера–Морено. Тоді виконуються наступні твердження:*

- 1) $|R| = 2^n$ з $n \geq 4$, L — підгрупа індексу 2 в R^+ та $R^* = i + L$ — група порядку 2^{n-1} ;
- 2) якщо $n \geq 6$, то група R^* неметациклічна;

3) якщо $n \geq 7$, то підгрупа L абелева, а експонента групи R^* не перевищує 2^{n-4} .

Локальні майже-кілець з мультиплікативною групою Міллера–Морено вивчені в [8], а саме доведено наступну теорему:

Теорема 1.48 (Теорема 7, [8]). *Нехай R — локальне майже-кілець порядку p^n ($n > 2$), мультиплікативна група якого є групою Міллера–Морено та L підгрупа всіх необоротних елементів з R . Тоді виконуються наступні твердження:*

- 1) якщо R — майже-поле, то R^* є або групою кватерніонів, або неабелевою метациклічною групою одного з порядків 24, 63, 80;
- 2) якщо $p > 2$, то p — просте число Ферма, $R^+ \cong C_p \times C_p$ або $R^+ \cong C_{p^2}$, $|L| = p$ та $R^* \cong C_p \rtimes C_{p-1}$
- 3) якщо $p = 2$ та індекс $|R : L| \neq 2$, то L — елементарна абелева 2-група та R^+ — 2-група експоненти не вище 4.

Наступна теорема підсумовує результати, отримані в 1.48 і 1.47, та дає характеристику скінченних локальних майже-кілець, мультиплікативні групи яких є групами Міллера–Морено (див., наприклад, [10]).

Теорема 1.49. *Нехай R — локальне майже-кілець порядку p^n , мультиплікативна група якого є групою Міллера–Морено, та L підгрупа всіх необоротних елементів з R . Тоді виконуються наступні твердження:*

- (I) якщо R — майже-поле, то R^* є або групою кватерніонів порядку 8, або неабелевою метациклічною групою одного з порядків 24, 63 або 80;
- (II) якщо $p \neq 2$, то $|L| = p$, де p — число Ферма, $R^+ \cong C_p \times C_p$ або $R^+ \cong C_{p^2}$ та $R^* \cong C_p \rtimes C_{p-1}$;

- (III) якщо $p = 2$ та $|R : L| > 2$, то $n \geq 4$, R^+ — група порядку 2^{2q} та експоненти не вище 4, де q — просте число, для якого число $2^q - 1$ є простим числом Мерсенна, R^* — група Міллера–Морено порядку $2^q(2^q - 1)$ та L — елементарна абелева 2-група, в якій $xy = 0$ для всіх $x, y \in L$;
- (IV) якщо $p = 2$ та $|R : L| = 2$, то при $n \geq 6$ R^* — неметациклічна група Міллера–Морено порядку 2^{n-1} та експоненти не вище 2^{n-4} , а при $n \geq 7$ підгрупа L абелева.

У статті [18] досліджувалися локальні майже-кільця з мультиплікативною групою діедра та було доведено, що кожне локальне майже-кільце з мультиплікативною групою діедра є скінченним з адитивною групою, яка є або 3-групою порядку не вище 9, або 2-групою порядку не вище 32.

Теорема 1.50 (Main Theorem, [18]). *Нехай R — локальне майже-кільце, мультиплікативна група якого R^* є групою діедра, і L_R — підгрупа всіх необоротних елементів R . Тоді виконуються такі твердження.*

- (1) *Майже-кільце R є скінченним.*
- (2) *Адитивна група R — це або 3-група порядку не більше 9, або 2-група порядку не більше 32.*
- (3) *Підгрупа L — це або абелева група, або група порядку 16 з комутаторною підгрупою порядку 2. Зокрема, L має абелеву підгрупу індексу 2.*

Опис таких майже-кілець був продовжений в дисертації Хуберта [45], зокрема, було встановлено, що якщо мультиплікативна група локального майже-кільця є групою діедра, то порядок цього майже-кільця не

перевищує 16. Сисак і Ді Терміні [116] показали, що якщо R є локальним майже-кільцем (не обов'язково нуль-симетричним), мультиплікативна група якого є узагальненою групою кватерніонів, то мультиплікативна група є або групою кватерніонів порядку 8, або узагальненою групою кватерніонів порядку 16 з абелевими адитивними групами наступних типів: $(3, 3)$, $(2, 2, 2, 2)$, $(2, 2, 4)$, $(2, 2, 2, 2, 2)$ та $(2, 2, 2, 4)$, а підгрупа необоротних елементів є тривіальною в першому випадку та елементарною абелевою індексу 2 в інших.

Теорема 1.51 (Theorem B, [116]). *Нехай R — локальне майже-кільце, мультиплікативна група якого R^* є узагальненою групою кватерніонів. Тоді виконуються такі твердження.*

- (1) *Група R^* є або кватерніоном порядку 8, або узагальненою групою кватерніонів порядку 16.*
- (2) *Адитивна група R^+ з R є абелевою одного з типів $(3, 3)$, $(2, 2, 2, 2)$, $(2, 2, 4)$, $(2, 2, 2, 2, 2)$ та $(2, 2, 2, 4)$.*
- (3) *Підгрупа L_R усіх незворотних елементів R є тривіальною, якщо R^+ має тип $(3, 3)$, і є елементарною абелевою групою індексу 2 в R^+ в іншому випадку.*

Навпаки, для кожної абелевої групи типу, переліченого в твердженні (2), існує принаймні одне майже-кільце R з адитивною групою R^+ цього типу, мультиплікативна група R^ якого є узагальненою групою кватерніонів.*

Скінченні локальні майже-кільця з циклічною підгрупою необоротних елементів описані в [2].

Теорема 1.52 (Теорема 1, [2]). *Нехай R — локальне майже-кільце порядку p^n з $n > 1$, підгрупа L якого циклічна та нетривіальна. Тоді його адитивна група R^+ або сама циклічна, або є елементарною абелевою*

групою порядку p^2 . В першому випадку R є комутативним локальним кільцем, ізоморфним кільцю лишків $\mathbb{Z}/p^n\mathbb{Z}$ з $n \geq 2$, а в другому — існує p попарно неізоморфних таких майже-кілець R з $|L| = p$, із яких $p - 1$ є нуль-симетричними, та мультиплікативні групи R^* яких ізоморфні наівпрямому добутку двох циклічних підгруп порядків p та $p - 1$.

Теорема 1.53 ([61]). Якщо R — скінченне локальне майже-кільце, яке не є майже-полем, то $|R| \leq |L|^2$.

Отримані результати знайдуть застосування при вивченні недистрибутивних структур на цих групах та класифікації цих об'єктів. Локальні майже-кільця тісно пов'язані з брейсами, які дають розв'язки комбінаторних рівнянь Янга–Бакстера [111].

1.4. Система комп'ютерної алгебри GAP та пакет SONATA

GAP надає мову програмування, також відому як GAP, бібліотеку математичних алгоритмів, реалізованих цією мовою, та різні бібліотеки математичних об'єктів, такі як, наприклад, 423164062 групи порядку не більше 2000 (за винятком 49487365422 груп порядку 1024).

1.4.1. Бібліотека SmallGroups

В цьому підпункті наведено інформацію з сайту системи GAP <https://docs.gap-system.org/pkg/smallgrp/doc/chap1.html>

Бібліотека SmallGroups надає доступ до всіх груп певних малих порядків. Групи відсортовані за їхніми порядками та перелічені до ізомор-

фізму; тобто для кожного з доступних порядків надається повний та ненадлишковий список представників типів ізоморфізму груп.

Бібліотека також має функцію ідентифікації: вона повертає номер бібліотеки заданої групи. Ця функція визначає номери бібліотек, використовуючи інваріанти груп. Функція доступна для всіх порядків у бібліотеці, крім порядків 512 та 1536, а також для порядків p^5 , p^6 та p^7 вище 2000.

Бібліотека організована в 11 шарів. Кожен шар містить групи певних порядків та відповідні їм процедури ідентифікації груп. Можна встановити перші n шарів бібліотеки груп та перші m шарів ідентифікації груп для кожного $1 \leq m \leq n \leq 11$. Це може бути корисним для економії місця на диску. Наведемо короткий опис цих шарів:

1. групи, порядок яких розкладається на множники щонайбільше на 3 прості числа;
2. решта груп порядку не більше 1000, крім 512 та 768;
3. решта груп порядку $2^n \cdot p$, де $n \leq 8$ та p — непарне просте число;
4. решта груп порядку 5^5 , 7^4 та порядку $q^n \cdot p$, де q^n ділить 3^6 , 5^5 або 7^4 та $p \neq q$ — просте число;
5. решта груп порядку не більше 2000, крім 1024, 1152, 1536 та 1920;
6. групи порядків 1152 та 1920;
7. групи порядку 512;
8. групи порядку 1536;
9. решта груп порядку p^n для $4 \leq n \leq 6$;
10. решта груп вільного від кубів порядку не більше 50000 та порядку вільного від квадратів;

11. решта груп порядку p^7 для $p = 3, 5, 7, 11$.

1.4.2. Пакет SONATA

Наведемо деякі функції для побудови майже-кілець з пакету SONATA (див. [16]):

- `NearRingMultiplicationByOperationTable( G, table, elmlist )` (Функція `NearRingMultiplicationByOperationTable` повертає майже-кілецеве множення на групі G , яке визначено таблицею множення. Замість елементів групи, записи таблиці є позиціями елемента групи у списку `elmlist` (перший елемент у `elmlist` дорівнює 1, другий — 2 тощо). Зазвичай нейтральним елементом групи буде перший).

Приклад.

```
# G — циклічна група порядку 4
gap > G := CyclicGroup(4);
< pc group of size 4 with 2 generators >
# Виводить породжуючі елементи групи G
gap > GeneratorsOfGroup(G);
[f1, f2]
# a — перший з попереднього списку твірний групи G
gap > a := last[1];
f1
# Виводить порядок твірного a
gap > Order(a);
4
gap > # a справді породжує G
gap > elmlist := List([0..3], x -> a^x);
[< identity > of ..., f1, f2, f1 * f2]
```

```

gap > # Нехай: 1 := identity of ..., 2 := f1, 3 := f2,
4 := f1 * f2
gap > # Розглянемо наступну таблицю множення на G:
gap > OT := [[1, 1, 1, 1],
> [1, 4, 3, 2],
> [1, 1, 1, 1],
> [1, 2, 3, 4]];;
# mul — майже-кільцеве множення на групі G, яке визначено та-
блицею множення OT
gap > mul :=
NearRingMultiplicationByOperationTable(G, OT, elmlist);
function(x, y)...end
# Перевірка чи є множення mul майже-кільцевим множенням на
групі G
gap > IsNearRingMultiplication(G, mul);
true

```

- `ExplicitMultiplicationNearRing( G, mul )` (Функція-конструктор `ExplicitMultiplicationNearRing` повертає майже-кільце, визначене групою G , та множення майже-кільця mul . `ExplicitMultiplicationNearRing` викликає `IsNearRingMultiplication`, щоб переконатися, що mul справді є майже-кільцевим множенням. Якщо майже-кільцеве множення не потрібно перевіряти, `ExplicitMultiplicationNearRingNC( G, mul )`).
- `IsExplicitMultiplicationNearRing( obj )` (`IsExplicitMultiplicationNearRing` повертає значення `true`, якщо об'єкт obj є майже-кільцем, визначеним групою та множенням, як у випадку з `ExplicitMultiplicationNearRing`).

- `PrintTable( nr )` (Функція `PrintTable` друкує адитивні та мультиплікативні таблиці Келі для майже-кільця `nr`. Ця функція працює так само, як і для груп). Приклад.

`# n — майже-кільце на циклічній групі порядку 3 з множенням`
`mul_l`

`gap > n :=`

`ExplicitMultiplicationNearRingNC(CyclicGroup(3), mul_l);`

`ExplicitMultiplicationNearRing(< pcgroup of size 3 with`
`1 generators >, multiplication)`

`# Множина символів із трьох елементів ["0" "1" "2"] на майже-кільці`

`n gap > SetSymbols(n, ["0" "1" "2"]);`

`# Друк таблиці Келі майже-кільця n`

`gap > PrintTable(n);`

Let:

`0 := (< identity > of ...)`

`1 := (f1)`

`2 := (f12)`

`# Таблиця додавання майже-кільця n`

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

`# Таблиця множення майже-кільця n`

*	0	1	2
0	0	1	2
1	0	1	2
2	0	1	2

- `IsNearRingMultiplication( G, mul, [lcs] )` (Аргументами функції `IsNrMultiplication` є група G , GAP-функція mul , яка має два аргументи x та y , обидва з яких повинні бути елементами групи G , і повертає елемент z з G . Mul визначає бінарну операцію на G . Як необов'язковий третій параметр, `IsNrMultiplication` приймає список керуючих рядків lcs . `IsNearRingMultiplication` повертає `true` (`false`), якщо mul є (не є) майже-кільцевим множенням на G , тобто перевіряє, чи є воно коректно визначеним, асоціативним та ліводистрибутивним над груповою операцією G . Список lcs може містити один або декілька рядків “closed”, “ass” та “rdistr”, і в цьому випадку відповідна властивість не перевіряється. У цьому випадку передбачається, що користувач перевірів її. Цю функцію слід використовувати лише у випадках, коли перевірка певних законів по-елементно займе забагато часу, і користувач абсолютно впевнений у їх правильності). Приклад.

```
gap > G := TWGroup(24,6);
```

```
24/6
```

```
# mul_l — функція множення
```

```
gap > mul_l := function(x,y) return y; end;
```

```
function(x,y)...end
```

```
# Перевірка чи є множення mul_l майже-кільцевим множенням на групі G
```

```
gap > IsNearRingMultiplication(G, mul_l);
```

```
true
```

```

#  $mul_r$  — функція множення
gap >  $mul_r := function(x, y) return x; end;$ 
 $function(x, y) ... end$ 
# Перевірка чи є множення  $mul_r$  майже-кільцевим множенням на
групі  $G$ 
gap >  $IsNearRingMultiplication(G, mul_r);$ 
# І задане множення не є ліво-дистрибутивним.
 $false$ 
gap >  $IsNearRingMultiplication(G, mul_r, ["closed" "ldistr"]);$ 
 $true$ 

```

Функції для визначення властивостей майже-кільця з пакету SONATA (див., [16]), а саме,

- $IsAbelianNearRing(nr)$ (Функція $IsAbelianNearRing$ повертає відповідне логічне значення **true** або **false**).

Означення 1.54. Майже-кільце називається абелевим, якщо його адитивна група є абелевою.

- $IsBooleanNearRing(nr)$ (Функція $IsBooleanNearRing$ просто перевіряє, чи всі елементи є ідемпотентними, та повертає відповідне логічне значення **true** або **false**).

Означення 1.55. Ліве майже-кільце N називається булевим, якщо всі його елементи ідемпотентні відносно множення.

- $IsNilNearRing(nr)$ (Функція $IsNilNearRing$ перевіряє, чи всі елементи є нільпотентними, та повертає відповідне логічне значення **true** або **false**).

Означення 1.56. Майже-кільце N називається нільмайже-кільцем, якщо всі його елементи нільпотентні.

- `IsNilpotentNearRing( nr )` (Функція `IsNilpotentNearRing` перевіряє, чи є майже кільце nr нільпотентним, і повертає відповідне логічне значення `true` або `false`).

Означення 1.57. Майже-кільце N називається нільпотентним, якщо існує додатне ціле число k , s.t. $N^k = \{0\}$.

- `IsCommutative( nr )` (Функція `IsCommutative` повертає відповідне значення `true` або `false`).

Означення 1.58. Майже-кільце $(N, +, \cdot)$ називається комутативним, якщо його мультиплікативна напівгрупа є комутативною.

- `IsPrimeNearRing( nr )` (Функція `IsPrimeNearRing` перевіряє, чи є nr простим майже-кільцем, використовуючи умову для всіх ненульових ідеалів I, J : $I \cdot J \neq \{0\}$ та повертає відповідне значення `true` або `false`).

Означення 1.59. Майже-кільце $(N, +, \cdot)$ з нульовим елементом 0 називається простим, якщо ідеал $\{0\}$ є простим ідеалом.

- `IsNearField( nr )` (Функція `IsNearField` перевіряє, чи має nr одиницю, і чи кожен ненульовий елемент має мультиплікативний обернений елемент, і повертає відповідне значення `true` або `false`).
- `IsPlanarNearRing( nr )` (Функція `IsPlanarNearRing` повертає відповідне значення `true` або `false` для `nearring nr`).
- `IsWdNearRing( nr )` (Функція `IsWdNearRing` повертає відповідне значення `true` або `false` для `nearring nr`).

Означення 1.60. Ліве майже-кільце $(N, +, \cdot)$ називається слабко подільним, якщо $a, b \in N$ $x \in N$ $a \cdot x = b$ або $b \cdot x = a$.

- `IsRegularNearRing( nr )` (Функція `IsRegularNearRing` просто перевіряє, чи всі елементи `nearring nr` є регулярними, та повертає відповідне логічне значення `true` або `false`).

Означення 1.61. Майже-кільце N називається регулярним, якщо всі його елементи регулярні.

- `IsQuasiregularNearRing( nr )` (Функція `IsQuasiregularNearRing` просто перевіряє, чи всі елементи майже кільця `nr` є квазірегулярними, та повертає відповідне логічне значення `true` або `false`).

Означення 1.62. Майже-кільце N називається квазірегулярним, якщо всі його елементи квазірегулярні.

1.4.3. Класифікація майже-кільць з одиницею

Пакет SONATA містить список усіх неізоморфних майже-кільць з одиницею порядку менше ніж 32.

Позначимо через C_n , D_n та Q_n циклічну, дієдральну та кватерніонну групи порядку n відповідно.

Нехай $m(G)$ — кількість усіх неізоморфних майже-кільць з одиницею R , адитивна група яких R^+ ізоморфна групі G .

Групу G назвемо *ендоморфно циклічною*, коли в ній існує елемент g , для якого $G = g^{\text{End } G}$.

Наступна лема отримана за допомогою GAP, пакетів LocalNR [98] та SONATA.

Лема 1.63 (Lemma 1, [87]). *Наступні групи G порядку менше 32 є ендоциклічними. Більш того, якщо G є адитивною групою майже-кільця з одиницею R , то виконується наступне.*

- $IdGroup(G) = [4, 1], G \cong C_4 \text{ } ma \text{ } m(G) = 1;$
- $IdGroup(G) = [4, 2], G \cong C_2 \times C_2 \text{ } ma \text{ } m(G) = 5;$
- $IdGroup(G) = [5, 1], G \cong C_5 \text{ } ma \text{ } m(G) = 1;$
- $IdGroup(G) = [6, 2], G \cong C_6 \text{ } ma \text{ } m(G) = 1;$
- $IdGroup(G) = [7, 1], G \cong C_7 \text{ } ma \text{ } m(G) = 1;$
- $IdGroup(G) = [8, 1], G \cong C_8 \text{ } ma \text{ } m(G) = 1;$
- $IdGroup(G) = [8, 2], G \cong C_4 \times C_2 \text{ } ma \text{ } m(G) = 10;$
- $IdGroup(G) = [8, 3], G \cong D_8 \text{ } ma \text{ } m(G) = 7;$
- $IdGroup(G) = [8, 4], G \cong Q_8 \text{ } ma \text{ } m(G) = 0;$
- $IdGroup(G) = [8, 5], G \cong C_2 \times C_2 \times C_2 \text{ } ma \text{ } m(G) = 35;$
- $IdGroup(G) = [9, 1], G \cong C_9 \text{ } ma \text{ } m(G) = 1;$
- $IdGroup(G) = [9, 2], G \cong C_3 \times C_3 \text{ } ma \text{ } m(G) = 10;$
- $IdGroup(G) = [10, 2], G \cong C_{10} \text{ } ma \text{ } m(G) = 1;$
- $IdGroup(G) = [11, 1], G \cong C_{11} \text{ } ma \text{ } m(G) = 1;$
- $IdGroup(G) = [12, 2], G \cong C_{12} \text{ } ma \text{ } m(G) = 1;$
- $IdGroup(G) = [12, 4], G \cong D_{12} \text{ } ma \text{ } m(G) = 1;$
- $IdGroup(G) = [12, 5], G \cong C_6 \times C_2 \text{ } ma \text{ } m(G) = 9;$
- $IdGroup(G) = [13, 1], G \cong C_{13} \text{ } ma \text{ } m(G) = 1;$
- $IdGroup(G) = [14, 2], G \cong C_{14} \text{ } ma \text{ } m(G) = 1;$
- $IdGroup(G) = [15, 1], G \cong C_{15} \text{ } ma \text{ } m(G) = 1;$

- $IdGroup(G) = [16, 1]$, $G \cong C_{16}$ $ma\ m(G) = 1$;
- $IdGroup(G) = [16, 2]$, $G \cong C_4 \times C_4$ $ma\ m(G) = 51$;
- $IdGroup(G) = [16, 3]$, $G \cong (C_4 \times C_2) \rtimes C_2$ $ma\ m(G) = 132$;
- $IdGroup(G) = [16, 4]$, $G \cong C_4 \rtimes C_4$ $ma\ m(G) = 40$;
- $IdGroup(G) = [16, 5]$, $G \cong C_8 \times C_2$ $ma\ m(G) = 37$;
- $IdGroup(G) = [16, 6]$, $G \cong C_8 \rtimes C_2$ $ma\ m(G) = 33$;
- $IdGroup(G) = [16, 7]$, $G \cong D_{16}$ $ma\ m(G) = 0$;
- $IdGroup(G) = [16, 10]$, $G \cong C_4 \times C_2 \times C_2$ $ma\ m(G) = 470$;
- $IdGroup(G) = [16, 11]$, $G \cong C_2 \times D_8$ $ma\ m(G) = 708$;
- $IdGroup(G) = [16, 12]$, $G \cong C_2 \times Q_8$ $ma\ m(G) = 4$;
- $IdGroup(G) = [16, 14]$, $G \cong C_2 \times C_2 \times C_2 \times C_2$ $ma\ m(G) = 2798$;
- $IdGroup(G) = [17, 1]$, $G \cong C_{17}$ $ma\ m(G) = 1$;
- $IdGroup(G) = [18, 2]$, $G \cong C_{18}$ $ma\ m(G) = 1$;
- $IdGroup(G) = [18, 3]$, $G \cong C_3 \times S_3$ $ma\ m(G) = 8$;
- $IdGroup(G) = [18, 5]$, $G \cong C_6 \times C_3$ $ma\ m(G) = 17$;
- $IdGroup(G) = [19, 1]$, $G \cong C_{19}$ $ma\ m(G) = 1$;
- $IdGroup(G) = [20, 2]$, $G \cong C_{20}$ $ma\ m(G) = 1$;
- $IdGroup(G) = [20, 4]$, $G \cong D_{20}$ $ma\ m(G) = 1$;
- $IdGroup(G) = [20, 5]$, $G \cong C_{10} \times C_2$ $ma\ m(G) = 9$;
- $IdGroup(G) = [21, 2]$, $G \cong C_{21}$ $ma\ m(G) = 1$;

- $IdGroup(G) = [22, 2], G \cong C_{22} \text{ } ma \text{ } m(G) = 1;$
- $IdGroup(G) = [23, 1], G \cong C_{23} \text{ } ma \text{ } m(G) = 1;$
- $IdGroup(G) = [24, 2], G \cong C_{24} \text{ } ma \text{ } m(G) = 1;$
- $IdGroup(G) = [24, 5], G \cong \text{ } ma \text{ } m(G) = 1;$
- $IdGroup(G) = [24, 6], G \cong D_{24} \text{ } ma \text{ } m(G) = 0;$
- $IdGroup(G) = [24, 9], G \cong C_{12} \times C_2 \text{ } ma \text{ } m(G) = 14;$
- $IdGroup(G) = [24, 10], G \cong C_3 \times D_8 \text{ } ma \text{ } m(G) = 7;$
- $IdGroup(G) = [24, 11], G \cong C_3 \times Q_8 \text{ } ma \text{ } m(G) = 0;$
- $IdGroup(G) = [24, 13], G \cong C_2 \times A_4 \text{ } ma \text{ } m(G) = 8;$
- $IdGroup(G) = [24, 14], G \cong C_2 \times C_2 \times S_3 \text{ } ma \text{ } m(G) = 10;$
- $IdGroup(G) = [24, 15], G \cong C_6 \times C_2 \times C_2 \text{ } ma \text{ } m(G) = 136;$
- $IdGroup(G) = [25, 1], G \cong C_{25} \text{ } ma \text{ } m(G) = 1;$
- $IdGroup(G) = [25, 2], G \cong C_5 \times C_5 \text{ } ma \text{ } m(G) = 16;$
- $IdGroup(G) = [26, 2], G \cong C_{26} \text{ } ma \text{ } m(G) = 1;$
- $IdGroup(G) = [27, 1], G \cong C_{27} \text{ } ma \text{ } m(G) = 1;$
- $IdGroup(G) = [27, 2], G \cong C_9 \times C_3 \text{ } ma \text{ } m(G) = 20;$
- $IdGroup(G) = [27, 3], G \cong (C_3 \times C_3) \rtimes C_3 \text{ } ma \text{ } m(G) = 22;$
- $IdGroup(G) = [27, 4], G \cong C_9 \rtimes C_3 \text{ } ma \text{ } m(G) = 4;$
- $IdGroup(G) = [27, 5], G \cong C_3 \times C_3 \times C_3 \text{ } ma \text{ } m(G) = 202;$
- $IdGroup(G) = [28, 2], G \cong C_{28} \text{ } ma \text{ } m(G) = 1;$

- $\text{IdGroup}(G) = [28, 3]$, $G \cong D_{28}$ та $m(G) = 1$;
- $\text{IdGroup}(G) = [28, 4]$, $G \cong C_{14} \times C_2$ та $m(G) = 9$;
- $\text{IdGroup}(G) = [29, 1]$, $G \cong C_{29}$ та $m(G) = 1$;
- $\text{IdGroup}(G) = [30, 4]$, $G \cong C_{30}$ та $m(G) = 1$;
- $\text{IdGroup}(G) = [31, 1]$, $G \cong C_{31}$ та $m(G) = 1$.

З леми 1.63 випливає наступна теорема.

Теорема 1.64 (Theorem 1, [87]). *Нехай G — група порядку менше 32. Якщо G — адитивна група майже-кілець з одиницею R , то G є ендоморфічною.*

1.4.4. Класифікація локальних майже-кілець

Класифікація всіх майже-кілець до певних порядків є відкритою проблемою. Вона вимагає великих обчислень, і найбільш підходящою платформою для їх реалізації є система обчислювальної алгебри GAP. Поточна версія пакета LocalNR [98] містить усі неізоморфні локальні майже-кілець порядку не більше 361, крім порядків 32, 64, 128, 243 та 256.

Існує 51 неізоморфна група порядку 32, з яких 19 є адитивними групами локальних майже-кілець (див., наприклад, [4]).

Теорема 1.65 (Теорема 19, [4]). *Наступні групи, і тільки вони, є адитивними групами локальних майже-кілець порядку 32:*

- $\text{IdGroup}(G) = [32, 1]$, $G \cong C_{32}$ та $n(G) = 1$;
- $\text{IdGroup}(G) = [32, 2]$, $G \cong (C_4 \times C_2) \rtimes C_4$ та $n(G) = 1396$;
- $\text{IdGroup}(G) = [32, 3]$, $G \cong C_8 \times C_4$ та $n(G) = 879$;

- $IdGroup(G) = [32, 4], G \cong C_8 \rtimes C_4 \text{ ma } n(G) = 797;$
- $IdGroup(G) = [32, 5], G \cong (C_8 \times C_2) \rtimes C_2 \text{ ma } n(G) = 1944;$
- $IdGroup(G) = [32, 6], G \cong ((C_4 \times C_2) \rtimes C_2) \rtimes C_2 \text{ ma } n(G) = 432;$
- $IdGroup(G) = [32, 7], G \cong (C_8 \rtimes C_2) \rtimes C_2 \text{ ma } n(G) = 224;$
- $IdGroup(G) = [32, 8], G \cong C_2 \cdot ((C_4 \times C_2) \rtimes C_2) \text{ ma } n(G) = 208;$
- $IdGroup(G) = [32, 12], G \cong C_4 \rtimes C_8 \text{ ma } n(G) = 2406;$
- $IdGroup(G) = [32, 16], G \cong C_{16} \times C_2 \text{ ma } n(G) = 128;$
- $IdGroup(G) = [32, 17], G \cong C_{16} \rtimes C_2 \text{ ma } n(G) = 128;$
- $IdGroup(G) = [32, 21], G \cong C_4 \times C_4 \times C_2 \text{ ma } n(G) = 135500;$
- $IdGroup(G) = [32, 22], G \cong C_2 \times ((C_4 \times C_2) \rtimes C_2) \text{ ma } n(G) = 149205;$
- $IdGroup(G) = [32, 23], G \cong C_2 \times (C_4 \rtimes C_4) \text{ ma } n(G) = 157845;$
- $IdGroup(G) = [32, 24], G \cong (C_4 \times C_4) \rtimes C_2 \text{ ma } n(G) = 262480;$
- $IdGroup(G) = [32, 36], G \cong C_8 \times C_2 \times C_2 \text{ ma } n(G) = 177110;$
- $IdGroup(G) = [32, 37], G \cong C_2 \times (C_8 \rtimes C_2) \text{ ma } n(G) = 527226;$
- $IdGroup(G) = [32, 45], G \cong C_4 \times C_2 \times C_2 \times C_2 \text{ ma } n(G) > 6684533;$
- $IdGroup(G) = [32, 51], G \cong C_2 \times C_2 \times C_2 \times C_2 \times C_2 \text{ ma } n(G) > 7007053.$

Висновки до розділу 1

У цьому розділі зроблено стислий огляд літератури за темою дисертації.

Підсумовуючи вищевикладене, можна стверджувати, що хоча в цій області було одержано ряд результатів, однак питання вивчення впливу на будову локального майже-кілця його мультиплікативної групи та підгрупи необоротних елементів є недостатньо вивченим. Тому актуальним є дослідження локальних майже-кілець деякими обмеженнями на їх структуру. Також залишається важливим питання класифікації певних класів майже-кілець.

Розділ 2

Локальні майже-кільця з деякими обмеженнями на їх структуру

В розділі досліджено локальні майже-кільця, мультиплікативні групи яких є в певному сенсі близькими до абелевих, зокрема, нільпотентними. Описано p -групи з циклічною підгрупою індексу p як адитивні групи та мультиплікативні групи локальних майже-кілець. Крім того, наведено класифікацію таких майже-кілець. Класифіковано локальні майже-кільця, які не є полями та мультиплікативна група яких є групою Шмідта. Отримано локальні майже-кільця з бібліотеки пакету SONATA системи комп'ютерної алгебри GAP.

2.1. Допоміжні означення та твердження

Непорожня множина R з двома бінарними операціями “+” та “.” є *(лівим) майже-кільцем*, якщо

1. $(R, +) = R^+$ — група з нейтральним елементом 0;
2. $(R, \cdot)$ — напівгрупа;
3. $x \cdot (y + z) = x \cdot y + x \cdot z$ для всіх $x, y, z \in R$.

З умови 3 означення випливає, що для кожної підгрупи M групи R^+ та кожного елемента $x \in R$ множина

$$xM = \{xy | y \in M\}$$

є підгрупою в R^+ і, зокрема, $x0 = 0$. Майже-кільце R називається *нуль-симетричним*, якщо $0x = 0$ для всіх $x \in R$, та *майже-кільцем з одиницею* i , якщо напівгрупа $(R, \cdot)$ є моноїдом з одиничним елементом i . Група R^* оборотних елементів моноїда $(R, \cdot)$ називається *мультиплікативною*, а група R^+ — *адитивною* групою майже-кільця R . Підгрупа M із R^+ називається *R^* -інваріантною*, якщо $rM \leq M$ для кожного $r \in R^*$, та *(R, R) -підгрупою*, якщо $xMy \subseteq M$ для довільних $x, y \in R$.

Вивчення локальних майже-кільць було започатковано Мексоном [61], який встановив, зокрема, що адитивна група скінченного локального майже-кільця повинна бути p -групою.

Означення 2.1. [61, Definition 2.1] Майже-кільце R з одиницею називається *локальним*, якщо множина $L = R \setminus R^*$ всіх необоротних елементів із $(R, \cdot)$ утворює адитивну підгрупу в R^+ , та *майже-полем*, коли $L = 0$.

Надалі будемо позначати через L — підгрупу в R^+ всіх необоротних елементів із R .

Актуальним є питання встановлення взаємозв'язків між локальним майже-кільцем та його мультиплікативною групою. Городником [42] вивчалися локальні майже-кільця, мультиплікативні групи яких є абелевими, і які не є кільцями. А саме, доведено, що множина всіх необоротних елементів такого майже-кільця утворює абелеву підгрупу індексу 2 в його адитивній групі. Зокрема, він описав локальні майже-кільця з циклічними групами одиниць, тобто, якщо мультиплікативна група локального майже-кільця є циклічною, то адитивна група є або групою типу $(2, 2, 2)$, або $(2, 4)$.

Дослідження локальних майже-кілець, мультиплікативні групи яких є в певному сенсі близькими до абелевих, зокрема, мінімальними неабелевими або, в іншій термінології, *групами Міллера–Морено* є природним узагальненням. В статтях [1], [8], [9] описано локальні майже-кілець та майже-поля з мультиплікативними групами Міллера–Морено.

Наведемо означення нільпотентної групи (див., наприклад, [49]).

Нехай G — група. Нормальний ряд

$$\{e\} = G_0 \subset G_1 \subset G_2 \subset \dots \subset G_n = G,$$

групи G називається *центральним*, якщо при $i = 0, 1, \dots, n-1$ фактор-група G_{i+1}/G_i міститься в центрі фактор-групи G/G_i . Група G , що має хоча б один центральний ряд, називається *нільпотентною*.

Наступна лема визначає експоненту адитивної групи скінченного майже-кілець з одиницею (див., наприклад, [31], теорема 3).

Лема 2.2. *Експонента адитивної групи скінченного майже-кілець R з одиницею i дорівнює адитивному порядку i , який співпадає з адитивним порядком кожного оборотного елемента R .*

Наступна лема (див. [18, Lemma 3.2]) характеризує основні властивості локальних майже-кілець.

Лема 2.3. *Нехай R — скінченне локальне майже-кілець з одиницею i . Тоді R^+ — p -група для деякого простого p , експонента якої збігається з порядком елемента i в R^+ , та виконуються наступні твердження:*

- 1) L — ідеал в R та (R, R) -підгрупа в R^+ ;
- 2) кожна власна R^* -інваріантна підгрупа із R^+ міститься в L ;
- 3) множина $i + L$ утворює нормальну силовську p -підгрупу мультиплікативної групи R^* ;
- 4) фактор-група R^+/L^+ є елементарною абелевою p -групою;

5) фактор-група $R^*/i + L$ ізоморфна мультиплікативній групі майже-поля R/L .

Як наслідок з 3) та 5) леми 2.3 маємо наступне твердження.

Лема 2.4. *Нехай R — скінченне локальне майже-кільце з одиницею i . Тоді*

$$R^* = (i + L) \rtimes K$$

для деякої підгрупи K групи R^* , що ізоморфна мультиплікативній групі майже-поля R/L .

Має місце наступна теорема [62, Theorem 2.1] про зв'язок порядків локального майже-кільця та підгрупи необоротних елементів.

Теорема 2.5. *Якщо R — локальне майже-кільце, яке не є майже-полем, то $|R| \leq |L|^2$.*

Скінченні локальні майже-кільця з циклічною підгрупою необоротних елементів описані в [2, теорема 1].

Теорема 2.6. *Нехай R — локальне майже-кільце порядку p^n з $n > 1$, підгрупа L якого циклічна та нетривіальна. Тоді його адитивна група R^+ або сама циклічна, або є елементарною абелевою групою порядку p^2 . В першому випадку R є комутативним локальним кільцем, ізоморфним кільцю лишків $\mathbb{Z}/p^n\mathbb{Z}$ з $n \geq 2$, а в другому — існує p попарно неізоморфних таких майже-кільць R з $|L| = p$, із яких $p - 1$ є нуль-симетричними, та мультиплікативні групи R^* яких ізоморфні напівпрямому добутку двох циклічних підгруп порядків p та $p - 1$.*

Як відомо, прості числа виду $2^n - 1$ мають назву *простих чисел Мерсенна*.

Наступна лема доведена в [55, Lemma 1].

Лема 2.7. *Нехай p — непарне просте число. Якщо m та n — додатні цілі числа, для яких $2^n - 1 = p^m$, то $m = 1$ та n — просте число.*

Нагадаємо, що *групою Шмідта* або *мінімальною ненільпотентною групою* називається скінченна ненільпотентна група, будь-яка власна підгрупа якої нільпотентна. Вивчення таких груп було започатковано О. Ю. Шмідтом в [113]. В наступній теоремі дано структурний опис цих груп (див. [46, Satz 5.5.2]).

Теорема 2.8. *Скінченна група G тоді і лише тоді є групою Шмідта, коли вона розкладається в напівпрямий добуток $G = S \rtimes T$ своїх нормальної силовської p -підгрупи S порядку p^s з $s \geq 1$ та циклічної силовської q -підгрупи $T = \langle b \rangle$ порядку q^t з $t \geq 1$, що задовольняють таким умовам:*

- 1) $Z(G) = \Phi(G) = \Phi(S) \times \langle b^q \rangle$, де $\Phi(G)$ — підгрупа Фраттіні групи G ;
- 2) $G' = S$, $S' = \Phi(S)$, $G'' = S'$, експонента S' не перевищує число p ;
- 3) якщо S — неабелева, то $Z(S) = S' = \Phi(S)$.

Скінченна група називається *мінімальною неабелевою групою* або *групою Міллера–Морено*, якщо вона неабелева, а всі її власні підгрупи є абелевими. Очевидно, що непримарні групи Міллера–Морено є групами Шмідта.

2.2. Локальні майже-кільця з нільпотентною мультиплікативною групою

В наступній теоремі встановлений зв'язок між нільпотентною мультиплікативною групою та адитивною групою в локальному майже-кільці.

Теорема 2.9. *Нехай R — локальне майже-кільце порядку p^n з нільпотентною мультиплікативною групою R^* . Якщо $p > 2$ або $p = 2$ та $-i \in Z(R^*)$, то мають місце такі твердження:*

1. Адитивна група R^+ — абелева.

2. L — абелева та має індекс 2 в R^+ .

Зокрема, R/L є поле.

Доведення. Очевидно, що $-i \in Z(R^*)$ при $p > 2$.

Нехай $r, s, r + s \in R^*$. Маємо

$$\begin{aligned} (-i)(r + s) &= (-i)r + (-i)s = r(-i) + s(-i) = \\ &= -r - s = (r + s)(-i) = (-i)(s + r). \end{aligned}$$

Звідки,

$$r + s = s + r \quad (2.1)$$

Далі, нехай $r \in R^*$ та $l \in L$. Тоді

$$\begin{aligned} (l + r)(-i) &= -(l + r) = -r - l = r(-i) - l = (-i)r - l = \\ &= (-i)(r - l(-i)) = (r - l(-i))(-i). \end{aligned}$$

Домножуючи справа на $(-i)$, отримаємо

$$-r + l + r = -l(-i). \quad (2.2)$$

Для будь-яких $r \in R^*$ маємо

$$(r')' = (-i)(-((-i)(-r))) = (-i)(-i)r = r.$$

Отже,

$$(r')' = r. \quad (2.3)$$

Нехай $l, s \in L$. Застосовуючи (2.2) двічі, отримаємо

$$(i + l) + s = s' + (i + l) = (i + s - i) + i + l = i + s + l.$$

Отже, підгрупа L — абелева.

Розглянемо два випадки, тобто коли $|R^+ : L^+| = 2$ та $|R^+ : L^+| > 2$.

Очевидно, якщо $|R^+ : L^+| = 2$, то R^+ — абелева.

Нехай тепер $|R^+ : L^+| > 2$. В групі R^* існують такі r та s , що $r + s \in R^*$. Застосовуючи (2.2) та (2.3),

$$l' = -(r + s) + l + (r + s) = -s + (-r + l + r) + s = (l')' = l,$$

для кожного $l \in L$. Це означає, що $L^+ \leq Z(R^+)$.

Нехай $r, s \in R^*$. Якщо $r + s \in R^*$, то $r + s = s + r$ за (2.1). Зараз припустимо, що $r + s \in L$. Тоді існує такий елемент $t \in R^*$, що $r + t \in R^*$. За (2.1), $r + t = t + r$. Отже,

$$r + t + s = t + (r + s) = (r + s) + t, \quad (2.4)$$

за припущенням. Звідки, t та s комутують. Елемент $t + (r + s) \in R^*$. Знову за (2.1), отримаємо

$$(t + r) + s = s + (t + r) = s + r + t. \quad (2.5)$$

Комбінуючи (2.4) та (2.5), маємо $r + s = s + r$. Звідки, R^+ — абелева.

Отже, адитивна група R^+ є абелевою чи $|R^+ : L^+| = 2$. $\square$

2.3. Локальні майже-кільця з мультиплікативними групами Шмідта

Оскільки майже-поля з мультиплікативною групою Шмідта повністю описані в [8, теорема 6], то розглянемо локальні майже-кільця, підгрупи необоротних елементів яких є нетривіальними.

Нагадаємо, що просте число виду $p = 2^{2^s} + 1$ з цілим числом $s \geq 0$ називається *простим числом Ферма*.

Теорема 2.10. *Нехай R — локальне майже-кільце порядку p^n , яке не є майже-полем та мультиплікативна група R^* якого є групою Шмідта. Тоді мають місце наступні твердження:*

- 1) *якщо $p > 2$, то $|R| = p^2$ для деякого простого числа Ферма p , адитивна група R^+ є елементарною абелевою та існує такий необоротний елемент a із R , що*

$$R^+ = \langle i \rangle + \langle a \rangle,$$

де i — одиниця в R , $a^2 = 0$ та $(ik)a = -ak$ для довільного первісного кореня k за модулем p . Зокрема, для кожного простого числа Ферма p існує єдине локальне майже-кільце порядку p^2 , мультиплікативна група якого є групою Міллера–Морено;

- 2) *якщо $p = 2$, то $|R| = 2^n$ з $n = 2t$, де t — просте число, для якого $2^m - 1$ є простим числом Мерсенна, та R^* є групою Міллера–Морено.*

Доведення. Оскільки підгрупа L є нетривіальною власною підгрупою R^+ , то $|L| = p^m$ з $1 \leq m < n$. Покладемо $l = n - m$. В силу того, що $R = R^* \cup L$, маємо

$$|R^*| = p^n - p^m = p^m(p^l - 1).$$

За теоремою 2.8 порядок групи Шмідта ділиться на два простих числа, звідки $p^l - 1 = q^k$. Далі, якщо через i позначити одиницю майже-кільця R , то за лемою 2.8 група R^* розкладається в напівпрямий добуток $R^* = S \rtimes \langle b \rangle$ з нормальною силовською p -підгрупою $S = i + L$ та циклічною підгрупою $\langle b \rangle = K$ порядку q^k . Більш того, за теоремою 2.8 b^q лежить в центрі групи R^* .

Нехай $p > 2$. Враховуючи, що число $p^l - 1$ є парним, звідси отримуємо $p^l - 1 = 2^k$ для деякого $k \geq 1$. Оскільки елемент b індукує на фактор-

групі S/S' незвідний автоморфізм порядку 2, то це можливо лише у випадку, коли $|S/S'| = p$. Звідси, $|S| = p$.

Оскільки $|S| = |L| = p$, то за теоремою 2.6 R^+ є елементарною абелевою групою порядку p^2 . Звідси $n = 2$, а отже, $l = 1$. Таким чином, $p = 2^k + 1$. Очевидно, що $k = 2^s$ для деякого цілого $s \geq 0$ і тому $p = 2^{2^s} + 1$ є простим числом Ферма.

Якщо a — твірний елемент L , то $R^+ = \langle i \rangle + \langle a \rangle$, де $\langle i \rangle$ — підгрупа, породжена одиницею i майже-кільця R . Нехай k — первісний корінь за модулем p та T — мультиплікативна підгрупа ненульових елементів з адитивної підгрупи $\langle i \rangle$. Тоді T — циклічна підгрупа порядку $p - 1$ з твірним елементом ik мультиплікативної групи R^* і тому $R^* = S \rtimes T$. За теоремою 2.8 елемент $(ik)^2$ централізує підгрупу S , а тому

$$(ik)^2(i + a) = (i + a)(ik)^2.$$

Враховуючи, що $(ik)^2 = ik^2$, звідси виводимо

$$(ik)^2 a = ak^2. \quad (2.6)$$

Далі, за твердженням 1) леми 2.3 $xa \in L$ для всіх $x \in R$. Отже, $xa = a\rho(x)$ для кожного $x \in R$, де число $\rho(x)$ однозначно визначено за модулем p . Для довільних $x, y \in R$ з останньої рівності випливає

$$a\rho(xy) = (xy)a = x(ya) = x(a\rho(y)) = (xa)\rho(y) = a(\rho(x)\rho(y)),$$

звідки маємо $(xy)a = a(\rho(x)\rho(y))$. Зокрема, поклавши $x = y = ik$, з рівності (2.6) отримуємо

$$ak^2 = (ik)^2 a = a\rho(ik)^2.$$

Це означає, що

$$\rho(ik)^2 \equiv k^2 \pmod{p},$$

звідки $\rho(ik) \equiv \pm k \pmod{p}$. Якщо $\rho(ik) \equiv k \pmod{p}$, то

$$(ik)(i + a) = ik + (ik)a = ik + ak = (i + a)(ik)$$

і тому група R^* буде абелевою, що суперечить умові теореми. Отже, $\rho(ik) \equiv -k \pmod{p}$, тобто $(ik)a = -ak$. Помноживши цю рівність зліва на 0, маємо

$$0a = (0(ik))a = -(0a)k,$$

звідки $(0a)(k+1) = 0$. Оскільки k — довільний первісний корінь за модулем p , то з останньої рівності отримуємо $0a = 0$.

З іншого боку, за означенням числа $\rho(x)$ маємо $a^2 = a\rho(a)$, звідки в силу лівого дистрибутивного закону маємо $a(a - i\rho(a)) = 0$. Оскільки $a \neq 0$, то з рівності $0a = 0$ випливає, що елемент $a - i\rho(a)$ є необоротним, тобто $a - i\rho(a) \in L$, що можливо лише при $\rho(a) = 0$. Отже, $a^2 = 0$. Таким чином, в майже-кільці R виконуються співвідношення $(ik)a = -ak$ та $a^2 = 0$, а це означає, зокрема, що для кожного простого числа Ферма p існує єдине локальне майже-кільце порядку p^2 , мультиплікативна група якого є групою Міллера–Морено. Отже, твердження 1) теореми доведено.

Нехай тепер $p = 2$. Очевидно, що мультиплікативна група локального майже-кільця R порядку 2^n тоді і тільки тоді не є 2-групою, коли L є підгрупою в R^+ індексу $|R^+ : L| > 2$. Тоді $|R : L| = 2^l$ та $|L| = 2^m$, звідки $|R^* : S| = 2^l - 1$. Оскільки $2^l - 1 = q^k$, то в силу леми 2.7 це можливо лише, коли $k = 1$ та m — просте число. Зокрема, $|| = q = 2^l - 1$. Крім того, елемент b індукує незвідний автоморфізм порядку $q = 2^l - 1$ на фактор-групі S/S' . Оскільки $|S/S'| = 2^{m-s}$ з $s \geq 0$, то $q = 2^l - 1$ — дільник числа $2^{m-s} - 1$ (див., наприклад, [41, Lemma 5.6.3]). Припустимо, що підгрупа S — неабелева. Тоді за [41, Theorem 5.6.5] $2^l - 1$ ділить $2^r + 1$, де $r \leq (m-s)/2$. Очевидно, $r = tm + w$, де $t \in N$ та $0 \leq w < m$. Оскільки

$$2^r + 1 = 2^{tm+w} + 1 = 2^w(2^{tm} - 1) + 2^w + 1,$$

то $2^l - 1$ ділить $2^r + 1$ лише при $r = 1$ та $m = 2$. Звідси $|R : L| = 2^2 = 4$ та $|| = 3$, а тому $|S/S'| = 4$. Звідси та за [41, Theorem 5.4.5]) S

ізоморфна або групі діедра, або групі кватерніонів порядку 8. А отже, $n = 5$, $|R| = 32$ та $|S| = |L| = 8$. За допомогою системи комп'ютерної алгебри GAP перевірено, що не існує локальних майже-кілець порядку 32 з підгрупою L порядку 8. Отже, підгрупа S — абелева, а тому, елементарна абелева порядку 2^m . Звідси R^* — група Міллера–Морено, що доводить твердження 2) теореми. $\square$

2.4. Локальні майже-кілець деякого порядку з мультиплікативними групами Міллера–Морено

Нагадаємо, що скінченна група називається групою Міллера–Морено, якщо вона неабелева і всі її власні підгрупи є абелевими. Очевидно, що непримарні групи Міллера–Морено є групами Шмідта. Структура цих груп повністю описується відомою теоремою Редєї (див., [109]).

Теорема 2.11. *Скінченні групи Міллера–Морено є групами наступних типів:*

- 1) група кватерніонів Q_8 ;
- 2) група $G = \langle a \rangle \rtimes \langle b \rangle$ порядку p^{m+n} з $a^{p^m} = b^{p^n} = 1$ і $b^{-1}ab = a^{1+p^{m-1}}$, де p є простим числом, $m \geq 2$ and $n \geq 1$;
- 3) група $G = (\langle a \rangle \times \langle c \rangle) \rtimes \langle b \rangle$ порядку p^{m+n+1} з $a^{p^m} = b^{p^n} = c^p = 1$, $b^{-1}ab = ac$ і $b^{-1}cb = c$, де $m \geq n \geq 1$ і $m + n > 2$ для $p = 2$;
- 4) група $G = P \rtimes \langle b \rangle$ порядку $p^r q^s$ з елементарною абелевою підгрупою P порядку p^r , в якій елемент b індукує незвідний автоморфізм простого порядку q , а також, $b^{q^s} = 1$ та $\langle b^q \rangle = Z(G)$, де p та q — різні прості числа, а r, s — натуральні числа.

2.4.1. Локальні майже-кільця порядку 32

Нагадаємо, що існує 51 неізоморфна група порядку 32.

Зауваження 2.12. Очевидно, існують три неізоморфні групи Міллера–Морено порядку 16, а саме:

- 1) $G = \langle a \rangle \rtimes \langle b \rangle$ з $|a| = 8$, $|b| = 2$, $b^{-1}ab = a^5$,
- 2) $G = \langle a \rangle \rtimes \langle b \rangle$ з $|a| = 4$, $|b| = 4$, $b^{-1}ab = a^3$ та
- 3) $G = (\langle a \rangle \times \langle c \rangle) \rtimes \langle b \rangle$ з $|a| = 4$, $|b| = 2$, $|c| = 2$, $b^{-1}ab = ac$,
 $b^{-1}cb = c$.

Теорема 2.13. *Наступні групи, і тільки вони, є адитивними групами R^+ локальних майже-кільць R порядку 32 з мультиплікативними групами Міллера–Морено R^* .*

I. *Якщо R^* — група типу 1) із зауваження 2.12, то R^+ ізоморфна одній із груп (кількість локальних майже-кільць на такій групі):*

- $C_4 \times C_4 \times C_2$ [32, 21] (2);
- $C_2 \times ((C_4 \times C_2) \rtimes C_2)$ [32, 22] (30);
- $C_4 \times C_2 \times C_2 \times C_2$ [32, 45] (32);
- $C_2 \times C_2 \times C_2 \times C_2 \times C_2$ [32, 51] (32).

II. *Якщо R^* — група типу 2) із зауваження 2.12, то R^+ ізоморфна одній із груп (кількість локальних майже-кільць на такій групі):*

- $C_4 \times C_4 \times C_2$ [32, 21] (136);
- $C_2 \times ((C_4 \times C_2) \rtimes C_2)$ [32, 22] (3120);
- $C_2 \times (C_4 \rtimes C_4)$ [32, 23] (4);

- $C_4 \times C_2 \times C_2 \times C_2$ [32, 45] (47904);
- $C_2 \times C_2 \times C_2 \times C_2 \times C_2$ [32, 51] (17100).

III. Якщо R^* — група типу 3) із зауваження 2.12, то R^+ ізоморфна одній із груп (кількість локальних майже-кілець на такій групі):

- $(C_4 \times C_2) \rtimes C_4$ [32, 2] (369);
- $C_8 \times C_4$ [32, 3] (208);
- $C_8 \rtimes C_4$ [32, 4] (238);
- $(C_8 \times C_2) \rtimes C_2$ [32, 5] (548);
- $((C_4 \times C_2) \rtimes C_2) \rtimes C_2$ [32, 6] (64);
- $(C_8 \rtimes C_2) \rtimes C_2$ [32, 7] (32);
- $C_2 \cdot ((C_4 \times C_2) \rtimes C_2) = (C_2 \times C_2) \cdot (C_4 \times C_2)$ [32, 8] (32);
- $C_4 \rtimes C_8$ [32, 12] (624);
- $C_4 \times C_4 \times C_2$ [32, 21] (634);
- $C_2 \times ((C_4 \times C_2) \rtimes C_2)$ [32, 22] (5936);
- $C_2 \times (C_4 \rtimes C_4)$ [32, 23] (458);
- $C_8 \times C_2 \times C_2$ [32, 36] (448);
- $C_2 \times (C_8 \rtimes C_2)$ [32, 37] (496);
- $C_4 \times C_2 \times C_2 \times C_2$ [32, 45] (40447);
- $C_2 \times C_2 \times C_2 \times C_2 \times C_2$ [32, 51] (23205).

2.4.2. Локальні майже-кілець порядку 64

Нехай R — локальне майже-кілець порядку 64, мультиплікативна група якого R^* є 2-групою Міллера–Морено. Як впливає з леми 9 [108], тоді

R^* може бути лише неметациклічною групою порядку 32. Отже, R^* — одна з двох груп G з $IdGroup(G) = [32, 2]$ та $IdGroup(G) = [32, 5]$. Тут $IdGroup(G) = [n, i]$, якщо G — i -та група порядку n . Якщо C_n — циклічна група порядку n , то неметациклічні групи Міллера-Морено порядку 32 — це 1) $G \cong (C_4 \times C_2) \rtimes C_4$ та 2) $G \cong (C_8 \times C_2) \rtimes C_2$.

Нехай $n(G)$ — кількість неізоморфних локальних майже-кілець з мультиплікативною групою G .

Твердження 2.14. *Якщо G — група типу 1), то R^+ може бути однією з наступних груп відповідно:*

- $((C_4 \times C_2) \rtimes C_4) \rtimes C_2$ [64, 61];
- $(C_4 \times C_4) \rtimes C_4$ [64, 65];
- $C_4 \times C_4 \times C_2 \times C_2$ [64, 192] та $n(G) \geq 2304$;
- $C_2 \times C_2 \times ((C_4 \times C_2) \rtimes C_2)$ [64, 193];
- $C_2 \times C_2 \times (C_4 \rtimes C_4)$ [64, 194] та $n(G) \geq 416$;
- $C_2 \times ((C_4 \times C_4) \rtimes C_2)$ [64, 195] та $n(G) \geq 4096$;
- $C_4 \times C_2 \times C_2 \times C_2 \times C_2$ [64, 260];
- $C_2 \times C_2 \times C_2 \times Q_8$ [64, 262];
- $C_2 \times C_2 \times C_2 \times C_2 \times C_2 \times C_2$ [64, 267].

Твердження 2.15. *Якщо G — група типу 2), то R^+ може бути однією з наступних груп відповідно:*

- $C_8 \times C_8$ [64, 2] та $n(G) = 96$;
- $C_8 \rtimes C_8$ [64, 3] та $n(G) = 96$;
- $C_8 \rtimes C_8$ [64, 15] та $n(G) = 96$;

- $C_8 \rtimes C_8$ [64, 16] $ma\ n(G) = 96$;
- $C_{16} \times C_4$ [64, 26] $ma\ n(G) = 16$;
- $C_{16} \rtimes C_4$ [64, 27] $ma\ n(G) = 16$;
- $C_4 \times C_4 \times C_4$ [64, 55] $ma\ n(G) = 1092$;
- $(C_4 \times C_4) \rtimes C_4$ [64, 57] $ma\ n(G) = 1092$;
- $(C_2 \times ((C_4 \times C_2) \rtimes C_2)) \rtimes C_2$ [64, 60] $ma\ n(G) = 1680$;
- $((C_4 \times C_2) \rtimes C_4) \rtimes C_2$ [64, 62] $ma\ n(G) = 1296$;
- $(C_4 \times C_4) \rtimes C_4$ [64, 63] $ma\ n(G) = 1024$;
- $(C_4 \times C_4) \rtimes C_4$ [64, 65] $ma\ n(G) = 1024$;
- $C_8 \times C_4 \times C_2$ [64, 83] $ma\ n(G) = 1088$;
- $C_2 \times (C_8 \rtimes C_4)$ [64, 84] $ma\ n(G) = 1088$;
- $(C_2 \times (C_8 \rtimes C_2)) \rtimes C_2$ [64, 88] $ma\ n(G) = 2176$;
- $(C_4 \rtimes C_8) \rtimes C_2$ [64, 104] $ma\ n(G) = 2048$;
- $C_4 \times C_4 \times C_2 \times C_2$ [64, 192];
- $C_2 \times C_2 \times ((C_4 \times C_2) \rtimes C_2)$ [64, 193];
- $C_2 \times C_2 \times (C_4 \rtimes C_4)$ [64, 194];
- $C_2 \times ((C_4 \times C_4) \rtimes C_2)$ [64, 195];
- $C_8 \times C_2 \times C_2 \times C_2$ [64, 246] $ma\ n(G) = 1088$;
- $C_2 \times C_2 \times (C_8 \rtimes C_2)$ [64, 247] $ma\ n(G) = 1088$;
- $C_4 \times C_2 \times C_2 \times C_2 \times C_2$ [64, 260];
- $C_2 \times C_2 \times C_2 \times Q_8$ [64, 262].

2.4.3. Локальні майже-кільця порядку 128

Наприклад, у GAP можна отримати наступне твердження.

Зауваження 1. Існує 6 неізоморфних груп Міллера–Морено порядку 64, а саме:

- $C_8 \rtimes C_8$ [64, 3];
- $(C_8 \times C_2) \rtimes C_4$ [64, 17];
- $C_{16} \rtimes C_4$ [64, 27];
- $(C_{16} \times C_2) \rtimes C_2$ [64, 29];
- $C_4 \rtimes C_{16}$ [64, 44];
- $C_{32} \rtimes C_2$ [64, 51].

Ми надаємо GAP-код для цих розрахунків.

G — список груп з бібліотеки *AllSmallGroups* порядку 64.

```
gap> G:=AllSmallGroups(64);;
```

Розмір списку G .

```
gap> Size(G);
```

```
267
```

Фільтруємо всі групи Міллера–Морено з списку G .

```
gap> F:=Filtered(G,x->IsMinimalNonAbelianGroup(x)=true);;
```

Розмір списку F .

```
gap> Size(F);
```

```
6
```

Виводимо список *IdGroup*, знайдених у попередньому списку підгруп.

```
gap> List(F,IdGroup);
```

```
[[64, 3], [64, 17], [64, 27], [64, 29], [64, 44], [64, 51]]
# Виводимо список зі структурним описом груп зі списку F.
gap> List(F, StructureDescription);
["C8 ⋈ C8", "(C8 × C2) ⋈ C4", "C16 ⋈ C4", "(C16 × C2) ⋈ C2", "C4 ⋈ C16", "C32 ⋈ C2"]
```

Нехай R — локальне майже-кільце на 2-породженій групі порядку 128, мультиплікативна група якого R^* є групою Міллера–Морено порядку 64. Як впливає з леми 9 [108], R^* може бути лише неметациклічною групою. Отже, R^* є однією з двох груп G з $IdGroup(G) = [64, 17]$ та $IdGroup(G) = [64, 29]$.

Наступна теорема є результатом обчислень, виконаних за допомогою GAP та пакета LocalNR.

Після аналізу 2-породжених груп порядку 128 як адитивних груп локальних майже-кілець з неметациклічними мультиплікативними групами Міллера–Морено порядку 64 за допомогою GAP було виявлено, що таких локальних майже-кілець немає. Це дозволяє нам зробити наступне припущення.

Теорема 2.16. *На 2-породжених групах порядку 128, мультиплікативна група яких є групою Міллера–Морено порядку 64, немає локальних майже-кілець.*

2.5. Локальні майже-кільця на скінченних p -групах з циклічними підгрупами індексу p

2.5.1. Попередні відомості

В [13, Theorem 12.5.1] доведено, що існує сім типів p -груп з циклічною підгрупою індексу p .

Теорема 2.17. *Групи порядку p^n , які містять циклічну підгрупу з індексом p , мають такі типи:*

абелеві, $n \geq 1$, циклічні:

$$1) a^{p^n} = 1;$$

$$n \geq 2:$$

$$2) a^{p^{n-1}} = 1, b^p = 1, ba = ab;$$

неабелеві, p — непарне, $n \geq 3$:

$$3) a^{p^{n-1}} = 1, b^p = 1, ba = a^{1+p^{n-2}}b;$$

$$p = 2, n \geq 3:$$

4) узагальнена групи кватерніонів:

$$a^{2^{n-1}} = 1, b^2 = a^{2^{n-2}}, ba = a^{-1}b;$$

$$p = 2, n \geq 3:$$

5) група дієдра:

$$a^{2^{n-1}} = 1, b^2 = 1, ba = a^{-1}b;$$

$$p = 2, n \geq 4:$$

$$6) a^{2^{n-1}} = 1, b^2 = 1, ba = a^{1+2^{n-2}}b;$$

$$p = 2, n \geq 4:$$

$$7) a^{2^{n-1}} = 1, b^2 = 1, ba = a^{-1+2^{n-2}}b.$$

Як було показано в [61, Теорема 7.4], адитивна група скінченного локального майже-кільця є p -групою для простого p .

Маємо наступний результат.

Твердження 2.18. *Нехай R — локальне майже-кільце порядку p^n , а L — порядку p^k . Мультиплікативна група R^* має порядок степеня простого числа тоді і тільки тоді, коли $p = 2$ і $k = n - 1$, тобто $|R^*| = 2^{n-1}$.*

Доведення. За визначенням 2.1 $R = R^* \cup L$, що означає $|R| = |R^*| + |L|$. Тому

$$|R^*| = |R| - |L| = p^n - p^k = p^k(p^{n-k} - 1).$$

Отже, $|R^*|$ може бути степенем простого числа тоді і тільки тоді, коли $p = 2$ та $k = n - 1$, тобто $|R^*| = 2^{n-1}$ як вимагалось. $\square$

У [51] дослідження було зосереджено на майже-кільцях з одиницею на групах з представленням вигляду

$$H = \langle a, b \mid a^{p^{n-1}} = 1, b^p = 1, a^b = a^{1+p^{n-2}} \rangle, p - \text{просте}, n \geq 3. \quad (2.7)$$

Зрозуміло, що ці групи є групами Міллера–Морено, тобто вони неабелеві, а всі її власні підгрупи є абелевими.

Позначимо через $n(G)$ кількість усіх неізоморфних нуль-симетричних майже-кільць з одиницею R , адитивна група яких R^+ ізоморфна групі G .

Наступна теорема містить кількість всіх майже-кільць з одиницею на групах H представлення (2.7) (див. [51, Theorem 7.1] і [28]).

Теорема 2.19. (i) Якщо $p = 2$ і $n = 3$, то $n(H) = 7$.

(ii) Якщо $p = 2$ і $n = 4$, то $n(H) = 32$.

(iii) Якщо $p = 2$ і $n > 4$, то $n(H) = 2^{n+2}$.

(iv) Якщо $p = 3$, то $n(H) = 3^{n-2}$.

(v) Якщо $p > 3$, то $n(H) = p^{n-3}$.

Наступний результат одразу випливає з [51, Theorem 4.2]

Твердження 2.20. Існує рівно одне неізоморфне ненуль-симетричне майже-кільце з одиницею на кожній групі представлення (2.7).

2.5.2. Скінченні p -групи з циклічною підгрупою індексу p як адитивні групи локальних майже-кілець

Теорема 2.21. *Нехай G — p -група з циклічною підгрупою індексу p . G — адитивна група майже-кілець з одиницею тоді і тільки тоді, коли виконується одне з наступних тверджень:*

1. $G = \langle a \mid a^{p^n} \rangle, n \geq 1$.
2. $G = \langle a, b \mid a^{p^{n-1}}, b^p, ba = ab \rangle, n \geq 2$.
3. $G = \langle a, b \mid a^{p^{n-1}}, b^p, ba = a^{1+p^{n-2}}b \rangle, p$ — непарне, $n \geq 3$.
4. $G = \langle a, b \mid a^4, b^2, ba = a^{-1}b \rangle$.
5. $G = \langle a, b \mid a^{2^{n-1}}, b^2, ba = a^{1+2^{n-2}}b \rangle, n \geq 4$.

Доведення. Групи порядку p^n , що містять циклічну підгрупу індексу p , повністю описані в теоремі 2.17.

Як було показано в [31, Теорема 1], циклічна група є адитивною групою майже-кілець з одиницею, тобто комутативних кілець. Отже, ми отримуємо твердження 1 теореми.

Як прямий наслідок з [32, Theorem] ми отримуємо твердження 2 теореми.

Групи з тверджень 3 та 5 є метациклічними групами Міллера–Морено. Тому ці групи є шуканими групами.

Групи типу 4) з теореми 2.17 не можуть бути адитивними групами майже-кілець з одиницею згідно [32].

Оскільки групи типу 5) є дієдральними групами з $p = 2$, і з результатів роботи [50], ми отримуємо твердження 4 теореми.

Як наслідок з [94, Лема 14], не існує майже-кілець з одиницею, визначеною на групах типу 7) з теореми 2.17. $\square$

Зрозуміло, що кожна неабелева група з теореми 2.21 має представлення (1) або дієдральну групу порядку 8. Отже, теорема 2.19 описує всі майже-кільця з одиницею на таких групах.

Цікаво знати, що відбувається з твердженням теореми 2.21 у випадку, коли майже-кільце є локальним.

Наслідок 2.22. *Нехай G — група з теореми 2.17. G — адитивна група локального майже-кільця тоді і тільки тоді, коли виконується одне з наступних тверджень:*

1. G є групою типу 1).
2. G є групою типу 2).
3. G є групою типу 3).
4. G є групою типу 6).

Було зазначено, що якщо G має тип 1), то R є локальним комутативним кільцем і навпаки. Тому ми розглядаємо групи, які не є циклічними.

Твердження 2.23. *Нехай G — нециклічна група з теореми 2.21. Якщо L — циклічна, то G — елементарна абелева група порядку p^2 .*

Доведення. Це одразу випливає з [2, Theorem 1]. □

Прямим наслідком [102, Lemma 6] є наступне твердження.

Твердження 2.24. *Нехай G — група типу 3) чи 6) з теореми 2.17. Тоді $|R : L| = p$ або $|R : L| = 2$, відповідно.*

2.6. Скінченні майже-кільця з одиницею з моногенною напівгрупою необоротних елементів

Нагадаємо, що напівгрупа S є моногенною, якщо вона породжена одним елементом.

Зауважимо, що в скінченному майже-кільці R з одиницею моногенність напівгрупи L означає, що $L = \{x, x^2, \dots, x^k = 0\}$, де $|L| = k$.

Теорема 2.25. *Якщо напівгрупа необоротних елементів L скінченного майже-кільця R з одиницею є моногенною, то R є майже-полем або нуль-симетричним локальним майже-кільцем порядку 4.*

Доведення. У випадку, коли R — майже-поле, тоді за означенням $L = 0$ — моногенна.

Нехай R — майже-кільце з одиницею i та моногенною напівгрупою необоротних елементів $L \neq 0$.

Припустимо, що $x^k + x^m \in R^*$ для $k < m$ та $x \in R$. Тоді $x^k(i + x^s) = y \in R^*$, де $s = m - k$. Звідси та моногенності L маємо $x^k = (i + x^s)^{-1}y \notin R^*$, бо $x^k \in L$. Отримали протиріччя. Тоді для всіх $x \in R$ $x^k + x^m \in L$ та $(L, +)$ є піднапівгрупою в R^+ , а отже, $(L, +)$ є підгрупою в R^+ . Отже, R — локальне майже-кільце. Звідси $|R| = p^n$ та $k = p^l$ з $l < n$.

Нехай для $x \in L$ та $0 < s < l$ має місце $x + x^2 = x^s$. Помножимо на x^{l-s} . Маємо

$$x^{l-s+1} + x^{l-s+2} = 0.$$

Звідси

$$x^{l-s+1}(i + x) = 0.$$

Помноживши зліва на $i + x$ отримаємо $x^{l-s+1} = 0$, звідки $k = 1$. Отже, $x^2 = 0$, тобто $|R| = 4$. А оскільки для всіх $x \in R$ $0x = x0 = 0$, то R — нуль-симетричне локальне майже-кільце порядку 4. $\square$

2.7. Локальні майже-кільця, отримані з бібліотеки пакету SONATA

Пакет SONATA системи комп'ютерної алгебри GAP містить бібліотеку всіх майже-кілець з одиницею порядку не вище 31. В цій бібліотеці майже-кільця впорядковані за їх адитивними групами, а команда

$$R := \text{LibraryNearRingWithOne}(G, t)$$

визначає майже-кільце R з одиницею на адитивній групі G з номером t .

Щоб визначити, чи буде вибране майже-кільце N локальним, за допомогою команди $u := \text{Size}(\text{NearRingUnits}(R))$ знаходимо порядок u мультиплікативної групи R^* цього майже-кільця. Далі, за допомогою команди $Id := \text{NearRingIdeals}(R)$ визначаємо список всіх ідеалів майже-кільця R , а командою $Ord := \text{List}(Id, \text{Size})$ — відповідний список їх порядків. Найбільший з цих порядків — це порядок t майже-кільця R . Якщо число $t - u$ міститься в списку Ord , то майже-кільце R є локальним, в противному разі — ні.

Нагадаємо, що абелева група є групою типу $(p^k, p^l, \dots, p^m)$, якщо вона ізоморфна прямій сумі циклічних p -груп порядків $p^k, p^l, \dots, p^m$, відповідно, де p — просте та $k, l, \dots, m$ — натуральні числа.

Позначимо через C_n циклічну групу порядку n .

Як зазначено вище, кожне майже-кільце з одиницею, адитивна група якого циклічна, є насправді комутативним кільцем, а отже, ізоморфним кільцю лишків $\mathbb{Z}/n\mathbb{Z}$ для деякого цілого числа n . Тому надалі не будемо розглядати локальні майже-кільця з циклічними адитивними групами.

Наступні пропозиції — результат обчислень, виконаних з використанням системи комп'ютерної алгебри GAP.

Твердження 2.26. *Нехай R — локальне майже-кільце порядку не вище 31, яке не є майже-полем. Тоді мультиплікативна група R^* ізоморфна одній з наступних груп:*

- 1) C_2 ;
- 2) C_4 ;
- 3) $(2, 2)$;
- 4) C_6 ;
- 5) $(4, 2)$;
- 6) $(2, 2, 2)$;
- 7) $(6, 2)$;
- 8) $(6, 3)$;
- 9) C_{20} ;
- 10) симетричній групі S_3 ;
- 11) $C_3 \times S_3$;
- 12) групі кватерніонів Q_8 ;
- 13) групі діедра D_8 ;
- 14) знакозмінній групі A_4 ;
- 15) $(C_3 \times C_3) \rtimes C_2$;
- 16) групі Міллера–Морено $C_5 \rtimes C_4$;
- 17) групі $C_5 \rtimes C_4$ з тривіальним центром.

Твердження 2.27. Нехай $n(G)$ — число всіх попарно неізоморфних локальних майже-кілець з мультиплікативною групою G з пропозиції 5.24, $R^+(G)$ — адитивна група відповідного майже-кілля та $L(G)$ — підгрупа його необоротних елементів. Мають місце наступні твердження.

1. Якщо G ізоморфна групі C_2 , то $n(G) = 2$ та $R^+(G)$ є групою типу $(2, 2)$ з підгрупою $L(G)$ порядку 2.
2. Якщо G ізоморфна групі C_4 , то $n(G) = 4$, а саме:
 - 2 майже-кілля на групі $R^+(G)$ типу $(4, 2)$ з підгрупою $L(G)$ типу $(2, 2)$ та
 - 2 — на групі $R^+(G)$ типу $(2, 2, 2)$ з підгрупою $L(G)$ типу $(2, 2)$.
3. Якщо G ізоморфна групі $(2, 2)$, то $n(G) = 7$, а саме:
 - 3 майже-кілля на групі $R^+(G)$ типу $(4, 2)$ з підгрупою $L(G)$ типу $(2, 2)$ та
 - 4 — на групі $R^+(G)$ типу $(2, 2, 2)$ з підгрупою $L(G)$ типу $(2, 2)$.
4. Якщо G ізоморфна групі C_6 , то $n(G) = 1$ та $R^+(G)$ є групою типу $(3, 3)$ з підгрупою $L(G)$ порядку 3.
5. Якщо G ізоморфна групі $(4, 2)$, то $n(G) = 227$, а саме:
 - 8 майже-кілля на групі $R^+(G)$ типу $(8, 2)$ з підгрупою $L(G)$ типу $(4, 2)$ та
 - 10 — на групі $R^+(G)$ типу $(4, 4)$ з підгрупою $L(G)$ типу $(4, 2)$;
 - 97 — на групі $R^+(G)$ типу $(4, 2, 2)$ з підгрупою $L(G)$ типу $(2, 2, 2)$;
 - 83 — на групі $R^+(G)$ типу $(2, 2, 2, 2)$ з підгрупою $L(G)$ типу $(2, 2, 2)$;

- 14 — на групі $R^+(G) \cong (C_4 \times C_2) \rtimes C_2$ з підгрупою $L(G)$ типу $(2, 2, 2)$;
- 7 — на групі $R^+(G) \cong C_4 \rtimes C_4$ з підгрупою $L(G)$ типу $(4, 2)$;
- 8 — на групі $R^+(G) \cong C_8 \rtimes C_2$ типу $(4, 4)$ з підгрупою $L(G)$ типу $(4, 2)$.

6. Якщо G ізоморфна групі $(2, 2, 2)$, то $n(G) = 114$, а саме:

- 9 майже-кільця на групі $R^+(G)$ типу $(8, 2)$ з підгрупою $L(G)$ типу $(4, 2)$ та
- 6 — на групі $R^+(G)$ типу $(4, 4)$ з підгрупою $L(G)$ типу $(4, 2)$;
- 41 — на групі $R^+(G)$ типу $(4, 2, 2)$ з підгрупою $L(G)$ типу $(2, 2, 2)$;
- 37 — на групі $R^+(G)$ типу $(2, 2, 2, 2)$ з підгрупою $L(G)$ типу $(2, 2, 2)$;
- 6 — на групі $R^+(G) \cong (C_4 \times C_2) \rtimes C_2$ з підгрупою $L(G)$ типу $(2, 2, 2)$;
- 7 — на групі $R^+(G) \cong C_4 \rtimes C_4$ з підгрупою $L(G)$ типу $(4, 2)$;
- 8 — на групі $R^+(G) \cong C_8 \rtimes C_2$ типу $(4, 4)$ з підгрупою $L(G)$ типу $(4, 2)$.

7. Якщо G ізоморфна групі $(6, 2)$, то $n(G) = 4$, а саме:

- 2 майже-кільця на групі $R^+(G)$ типу $(4, 4)$ з підгрупою $L(G)$ типу $(2, 2)$ та
- 2 — на групі $R^+(G)$ типу $(2, 2, 2, 2)$ з підгрупою $L(G)$ типу $(2, 2)$.

8. Якщо G ізоморфна групі $(6, 3)$, то $n(G) = 14$, а саме:

- 9 майже-кільця на групі $R^+(G)$ типу $(9, 3)$ з підгрупою $L(G)$ типу $(3, 3)$ та
 - 5 — на групі $R^+(G)$ типу $(3, 3, 3)$ з підгрупою $L(G)$ типу $(3, 3)$.
9. Якщо G ізоморфна групі C_{20} , то $n(G) = 1$ та $R^+(G)$ є групою типу $(5, 5)$ з підгрупою $L(G)$ порядку 5.
10. Якщо G ізоморфна симетричній групі S_3 , то $n(G) = 2$ та обидві $R^+(G)$ є групами типу $(3, 3)$ з підгрупою $L(G)$ порядку 3.
11. Якщо G ізоморфна групі $C_3 \times S_3$, то $n(G) = 15$, а саме:
- 4 майже-кільця на групі $R^+(G)$ типу $(9, 3)$ з підгрупою $L(G)$ типу $(3, 3)$ та
 - 3 — на групі $R^+(G)$ типу $(3, 3, 3)$ з підгрупою $L(G)$ типу $(3, 3)$;
 - 4 — на групі $R^+(G) \cong (C_3 \times C_3) \rtimes C_2$ з підгрупою $L(G)$ типу $(3, 3)$;
 - 4 — на групі $R^+(G) \cong C_9 \rtimes C_3$ з підгрупою $L(G)$ типу $(3, 3)$.
12. Якщо G ізоморфна групі кватерніонів Q_8 , то $n(G) = 48$, а саме:
- 24 майже-кільця на групі $R^+(G)$ типу $(4, 2, 2)$ з підгрупою $L(G)$ типу $(2, 2, 2)$ та
 - 24 — на групі $R^+(G)$ типу $(2, 2, 2, 2)$ з підгрупою $L(G)$ типу $(2, 2, 2)$.
13. Якщо G ізоморфна групі діедра D_8 , то $n(G) = 236$, а саме:
- 16 майже-кілець на групі $R^+(G)$ типу $(8, 2)$ з підгрупою $L(G)$ типу $(4, 2)$,
 - 9 — на групі $R^+(G)$ типу $(4, 4)$ з підгрупою $L(G)$ типу $(4, 2)$,

- 90 — на групі $R^+(G)$ типу $(4, 2, 2)$ з підгрупою $L(G)$ типу $(2, 2, 2)$,
- 77 — на групі $R^+(G)$ типу $(2, 2, 2, 2)$ з підгрупою $L(G)$ типу $(2, 2, 2)$,
- 17 — на групі $R^+(G) \cong (C_4 \times C_2) \rtimes C_2$ з підгрупою $L(G)$ типу $(2, 2, 2)$,
- 10 — на групі $R^+(G) \cong C_4 \rtimes C_4$ з підгрупою $L(G)$ типу $(4, 2)$ та
- 17 — на групі $R^+(G) \cong C_8 \rtimes C_2$ з підгрупою $L(G)$ типу $(4, 2)$.

14. Якщо G ізоморфна знакозмінній групі A_4 , то $n(G) = 9$, а саме:

- 2 майже-кільця на групі $R^+(G)$ типу $(4, 4)$ з підгрупою $L(G)$ типу $(2, 2)$,
- 2 — на групі $R^+(G) \cong C_2 \times Q_8$ з підгрупою $L(G)$ типу $(2, 2)$ та
- 5 — на групі $R^+(G)$ типу $(2, 2, 2, 2)$ з підгрупою $L(G)$ типу $(2, 2)$.

15. Якщо G ізоморфна групі $(C_3 \times C_3) \rtimes C_2$, то $n(G) = 4$ та всі $R^+(G)$ є групами типу $(3, 3, 3)$ з підгрупою $L(G)$ типу $(3, 3)$.

16. Якщо G ізоморфна групі Міллера–Морено $C_5 \rtimes C_4$, то $n(G) = 1$ та $R^+(G)$ є групою типу $(5, 5)$ з підгрупою $L(G)$ порядку 5.

17. Якщо G ізоморфна групі $C_5 \rtimes C_4$ з тривіальним центром, то $n(G) = 3$ та $R^+(G)$ є групою типу $(5, 5)$ з підгрупою $L(G)$ порядку 5.

Висновки до розділу 2

У даному розділі:

- встановлено зв'язок між нільпотентною мультиплікативною групою та адитивною групою в локальному майже-кільці;
- класифіковано локальні майже-кільця, які не є полями та мультиплікативна група яких є групою Шмідта;
- знайдені адитивні групи локальних майже-кілець порядку 32 та 128 з мультиплікативними групами Міллера–Морено;
- вивчені скінченні p -групи з циклічною підгрупою індексу p як адитивні групи локальних майже-кілець;
- отримано локальні майже-кільця з бібліотеки пакету SONATA системи комп'ютерної алгебри GAP.

Основні результати даного розділу опубліковано у працях [8, 11, 6, 14] зі списку публікацій і, відповідно, [11], [79], [106], [2] зі списку використаних джерел, а також опубліковано у тезах конференцій [20, 21, 27, 30, 38, 40] і, відповідно, [107], [12], [15], [76], [103], [92].

Розділ 3

Локальні майже-кільця на скінченних неабелевих 2-породжених p -групах

У даному розділі проаналізовано скінченні неабелеві 2-породженні p -групи з циклічним комутантом та вивчено скінченні локальні майже-кільця з розщепленою метациклічною адитивною групою. Отримано необхідні і достатні умови існування локальних майже-кілець на групах типу (A.1) та (B.1).

3.1. Скінченні неабелеві 2-породженні p -групи з циклічним комутантом

Класифікація скінченних неабелевих 2-породжених p -груп з циклічним комутантом для непарних простих чисел p дана Мехом [67] (див. також [66]).

Теорема 3.1. [66] *Нехай G — скінченна неабелева 2-породжена p -група з циклічним комутантом для непарних простих чисел p . Далі дані визначальні співвідношення всіх неізоморфних груп G .*

(A.1) *група $G = \langle a, b \mid a^{p^l} = b^{p^m} = 1, b^a = b^a = b^{1+p^s} \rangle$, де $1 \leq s < m$ та $m - s \leq l$.*

(A.2) *эпына* $G = \langle a, b \mid b^{p^m} = 1, b^a = b^{1+p^s}, a^{p^l} = b^{p^h} \rangle$, *де* $1 \leq s < h < m$
ма $m - s \leq h < l$.

(B.1) *эпына* $G = \langle a, b, u \mid a^{p^l} = b^{p^m} = u^{p^n} = 1, b^a = bu, u^a = u^b = u \rangle$, *де*
 $1 \leq n \leq m \leq l$.

(B.2) *эпына* $G = \langle a, b, u \mid a^{p^l} = u^{p^n} = 1, b^{p^m} = u^{p^k}, b^a = bu, u^a = u^b = u \rangle$,
де $n \leq l, n \leq m, 1 \leq k < n$.

(B.3) *эпына* $G = \langle a, b, u \mid u^{p^n} = 1, a^{p^l} = u^{p^h}, b^{p^m} = u^{p^k}, b^a = bu, u^a = u^b = u \rangle$, *де*
 $1 \leq k < h < n \leq m, m + h - k < l$.

(C.1) *эпына* $G = \langle a, b, u \mid a^{p^l} = b^{p^m} = u^{p^n} = 1, u^{p^n} = 1, b^a = bu, u^a = u^{1+p^s}, u^b = u \rangle$, *де*
 $n \leq l, n \leq m, 0 < s < n$.

(C.2) *эпына* $G = \langle a, b, u \mid a^{p^l} = u^{p^n} = 1, b^a = bu, u^a = u^{1+p^s}, u^b = u, b^{p^m} = u^{rp^k} \rangle$, *де*
 $n \leq l, k \leq m, r \not\equiv 0(p), 0 < k < n, 0 < s < n, p^m \equiv rp^{k+s}(p^n)$.

(D.1) *эпына* $G = \langle a, b, u \mid a^{p^l} = u^{p^h}, b^a = bu, u^a = u^{1+p^s}, u^b = u, b^{p^m} = u^{p^n} = 1 \rangle$, *де*
 $n \leq l, n - s \leq h < n \leq m, 0 < s < n$.

(D.2) *эпына* $G = \langle a, b, u \mid a^{p^l} = u^{p^h}, u^{p^n} = 1, b^a = bu, u^a = u^{1+p^s}, u^b = u, b^{p^m} = u^{rp^k} \rangle$, *де*
 $0 < h < n \leq l, 0 < s < n, n - s \leq h, r \equiv 0(p), 0 < k < n, k < m, p^m \equiv rp^{k+s}(p^n)$, *ма* *якщо* $k < h$, *мо* $l + k > m + h$,
якщо $h \leq k$, *мо* $m + n - s > l + k - h$.

(E.1) *эпына* $G = \langle a, b, u \mid b^{p^m} = u^{p^n} = 1, b^a = bu, u^a = u^{1+p^s}, u^b = u, b^{p^h} = a^{p^l} \rangle$, *де*
 $0 < s < n, 0 < h < m, 0 < l - h < n - s, n \leq h$.

(E.2) *эпына* $G = \langle a, b, u \mid b^{p^m} = u^{p^n} = 1, b^a = bu, u^a = u^{1+p^s}, u^b = u, a^{p^l} = b^{p^h} u^{tp^j} \rangle$ *де*
 $n \leq l, 0 < h < m, 0 < s < n, 0 < l - h < n - s, n \leq m$,
 $t \not\equiv 0(p), 0 \leq j < h, j < n, p^h + tp^{s+j} \equiv 0(p^n)$ *ма* $n \leq j + m - h$.

(E.3) група $G = \langle a, b, u \mid b^{p^m} = u^{p^n} = 1, b^a = bu, u^a = u^{1+p^s}, u^b = u, a^{p^l} = b^{p^h} u^{tp^j} \rangle$ де $n \leq l, 0 < h < m, 0 < s < n, 0 < l - h < n - s, n \leq m, t \not\equiv 0(p), 0 \leq j < h, j < n, p^h + tp^{s+j} \equiv 0(p^n)$ та $n > j + m - h$.

(F.1) група $G = \langle a, b, u \mid u^{p^n} = 1, b^a = bu, u^a = u^{1+p^s}, u^b = u, b^{p^m} = u^{rp^k}, a^{p^l} = b^{p^h} u^{tp^j} \rangle$ де $0 < s < n, 0 < k < n, s < m, k < m, p^m \equiv rp^{k+s}(p^n), r \not\equiv 0(p), h < l, h < m, l - h < n - s, t \not\equiv 0(p), n \leq l, p^h + tp^{j+s} \equiv 0(p^n), rp^k + tp^{j+m-h} \equiv 0(p^n)$.

(F.2) група $G = \langle a, b, u \mid u^{p^n} = 1, b^a = bu, u^a = u^{1+p^s}, u^b = u, a^{p^l} = b^{p^h} u^{tp^j}, b^{p^m} = u^{rp^k} \rangle$, де $0 < s < n, 0 < k < n, k < m, s < m, p^m \equiv rp^{k+s}(p^n), r \not\equiv 0(p), h < l, h < m, l - h < n - s, t \not\equiv 0(p), n \leq l, p^h + tp^{j+s} \equiv 0(p^n), rp^k + tp^{j+m-h} \not\equiv 0(p^n), j + m + n > l + s + k$.

Наступна лема (див. [18, Лема 3.2]) характеризує основні властивості локальних майже-кілець.

Лема 3.2. Нехай R — скінченне локальне майже-кілець з одиницею i . Тоді R^+ — p -група для деякого простого p , експонента якої збігається з порядком елемента i в R^+ , та виконуються наступні твердження:

- 1) L — ідеал в R та (R, R) -підгрупа в R^+ ;
- 2) кожна власна R^* -інваріантна підгрупа із R^+ міститься в L ;
- 3) множина $i + L$ утворює нормальну силовську p -підгрупу мультиплікативної групи R^* ;
- 4) фактор-група R^+/L^+ є елементарною абелевою p -групою;
- 5) фактор-група $R^*/i + L$ ізоморфна мультиплікативній групі майже-поля R/L .

Взаємозв'язок між групою автоморфізмів адитивної групи майже-кілець з одиницею та його мультиплікативною групою встановлює наступна лема.

Лема 3.3 ([9]). *Нехай R — майже-кільце з одиницею i . Тоді в групі автоморфізмів $\text{Aut } R^+$ існує підгрупа A , яка ізоморфна мультиплікативній групі R^* та задовольняє умові*

$$i^A = \{i^a \mid a \in A\} = R^*.$$

В статті МЕНЕГАЦЦО [66] знайдено групи автоморфізмів скінченних неабелевих 2-породжених p -груп з циклічним комутантом ($p > 2$).

Лема 3.4. *Групи автоморфізмів груп типів (A.2), (B.3), (D.1), (D.2), (E.1), (E.2), (E.3), (F.1) і (F.2) є p -групами.*

Як наслідок маємо наступне твердження.

Лема 3.5. *Не існує локальних майже-кільців з адитивною групою одного з типів (A.2), (B.3), (D.1), (D.2), (E.1), (E.2), (E.3), (F.1) чи (F.2).*

Доведення. Оскільки за лемою 3.2 R^+ є групою порядку p^n з непарним простим числом p та $n \geq 1$, то $|L| = p^m$ для деякого $1 \leq m < n$, звідки

$$p^n - p^m = p^m(p^{n-m} - 1) = |R^*| \neq p^k$$

для будь-якого k . Оскільки за лемою 3.4 групи автоморфізмів груп типів (A.2), (B.3), (D.1), (D.2), (E.1), (E.2), (E.3), (F.1) та (F.2) є p -групами, то в групі автоморфізмів $\text{Aut } R^+$ не існує підгрупи A , яка ізоморфна мультиплікативній групі R^* . Тоді за лемою 3.3 не існує локального майже-кільця на цих групах. $\square$

3.2. Скінченні локальні майже-кільця з розщепленою метациклічною адитивною групою

Нагадаємо, що майже-кільце R з одиницею називається локальним, якщо множина всіх необоротних елементів R утворює підгрупу адитивної групи R .

В цьому підрозділі розглядаються розщеплювальні метациклічні групи, які є адитивними групами скінченних локальних майже-кілець.

3.2.1. Майже-кільца з одиницею на групах Міллера—Морено

Узагальнимо результати, отримані в [7] і [102].

Теорема 3.6 (Theorem 2, [71]). *Група Міллера—Морено G є адитивною групою локального майже-кілля R тоді і тільки тоді, коли вона є p -групою для деякого простого p і виконується одне з наступних тверджень:*

- 1) *група G ізоморфна одній із груп $G(p^m, p^n)$ з $p^{m+n} > 8$ і $m > n$ і циклічна підгрупа порядку p^m , породжена i , є нормальною в G ;*
- 2) *$p = 2$, група G ізоморфна одній із груп $G(2^m, 2^n)$ з $m \leq n$ і циклічна підгрупа порядку 2^n , породжена i , не є нормальною в G ;*
- 3) *група G ізоморфна одній із груп $G(p^m, p^n, p)$ і циклічна підгрупа, породжена i , не є нормальною в G .*

Далі описано всі можливі типи груп Міллера—Морено, які є адитивними групами майже-кілець з одиницею.

Теорема 3.7 (Theorem 3, [71]). *Нехай G — група Міллера—Морено. Група G є адитивною групою майже-кілля R з одиницею тоді і тільки тоді, коли G є або однією з груп теореми 3.6, або групою $G(4, 2)$.*

Наступне твердження є прямим наслідком теореми 3.7.

Наслідок 3.8. *Не існує майже-кілля з одиницею, адитивна група якого ізоморфна групі $G(p^m, p^n)$ з $p > 2$ і $2 \leq m \leq n$.*

3.2.2. Допоміжні означення та твердження

Спочатку згадаємо деякі позначення та факти, що стосуються майже-кілець та метациклічних груп.

Означення 3.9. (Ліве) майже-кілець є множиною $R = (R, +, \cdot)$ з такими двома бінарними операціями, додаванням “+” та множенням “ $\cdot$ ”, що

- 1) $(R, +)$ є групою з нейтральним елементом 0;
- 2) $(R, \cdot)$ є напівгрупою;
- 3) $x(y + z) = xy + xz$ для всіх $x, y, z \in R$.

Група $(R, +)$ майже-кілеця R позначається як R^+ і називається адитивною групою в R . Легко бачити, що для кожної підгрупи M з R^+ і кожного елемента $x \in R$ множина $xM = \{x \cdot y | y \in M\}$ є підгрупою в R^+ і, зокрема, $x \cdot 0 = 0$. Якщо додатково $0 \cdot x = 0$, то майже-кілець R називається нуль-симетричним. Більш того, R є майже-кілцем з одиницею i якщо напівгрупа $(R, \cdot)$ є моноїдом з одиничним елементом i . В останньому випадку група всіх обернених елементів моноїда $(R, \cdot)$ позначається як R^* і називається мультиплікативною групою R . Підгрупа M в R^+ називається R^* -інваріантною, якщо $rM \leq M$ для кожного $r \in R^*$, і (R, R) -підгрупою, якщо $xMy \subseteq M$ для довільних $x, y \in R$.

Як звичайно, для кожного елемента $r \in R$ і кожного цілого $n \in \mathbb{Z}$ ми визначимо елемент rn в R наступним чином:

$$rn = \begin{cases} \underbrace{r + \cdots + r}_{n \text{ times}}, & \text{якщо } n > 0, \\ 0 & \text{if } n = 0, \\ \underbrace{(-r) + \cdots + (-r)}_{-n \text{ times}}, & \text{якщо } n < 0. \end{cases}$$

Тоді $r(m+n) = rm + rn$ для будь-яких цілих m і n , так, що ми можемо ідентифікувати нейтральний елемент 0 з цілим 0 . З іншого боку, якщо i є одиницею в R , тоді ми не будемо ідентифікувати i з цілим 1 , тому, що в цілому $(in)r \neq rn = r(in)$ для $n \neq 1$. Таким чином, щоб уникнути плутанини, ми не використовуємо позначення nr з цілим числом n .

Наступні дві леми є добре відомими.

Лема 3.10. *Нехай R скінченне майже-кільце R з одиницею i . Тоді експонента адитивної групи R^+ дорівнює адитивному порядку i , який співпадає з адитивним порядком кожного елемента з мультиплікативною групою R^* .*

Доведення. Дійсно, якщо $ik = 0$ для деякого цілого k , тоді для кожного $x \in R$ ми маємо

$$xk = (xi)k = x(ik) = x0 = 0.$$

З іншого боку, якщо $y \in R^*$ і $yl = 0$ для додатнього цілого l , тоді $il = y^{-1}(yl) = 0$, оскільки адитивні порядки r і i співпадають. $\square$

Лема 3.11. *Нехай R майже-кільце з одиницею i і $a \in R^*$. Для будь-яких елементів $x, y \in R$ ми покладемо $x \circ y = xa^{-1}y$. Тоді по відношенню до операції “+” і “ $\circ$ ” множина $(R, +, \circ)$ є майже-кільцем з одиницею a , яке ізоморфне R .*

Доведення. Легко перевірити, що операція “ $\circ$ ” асоціативна та ліво-дистрибутивна по відношенню до додавання та відображення $r \mapsto ar$ визначає ізоморфізм майже-кільця R в $(R, +, \circ)$. $\square$

Означення 3.12. [61] Майже-кільце R з одиницею називається локальним якщо множина $L = R \setminus R^*$ всіх необоротних елементів R є підгрупою в R^+ .

Наступна лема характеризує загальні властивості скінченних локальних майже-кілець (див., наприклад, [18, Lemma 3.2]).

Лема 3.13. *Нехай R є локальним майже-кільце з одиницею i і L підгрупа всіх необоротних елементів в R . Тоді виконуються наступні твердження:*

- 1) L є (R, R) -підгрупою R^+ ;
- 2) кожна власна R^* -інваріантна підгрупа в R^+ міститься в L ;
- 3) множина $i + L$ утворює підгрупу в мультиплікативній групі R^* .

Нагадаємо, що група G називається *метациклічною*, якщо існує така циклічна нормальна підгрупа $\langle a \rangle$, що фактор-група $G/\langle a \rangle$ є циклічною. Для кожного простого p , метациклічна p -група G є *розщеплюваною*, тоді і тільки тоді, коли розкладається в прямий добуток $G = \langle a \rangle \rtimes \langle b \rangle$ циклічної нормальної підгрупи $\langle a \rangle$ і циклічної підгрупи $\langle b \rangle$.

Наступна корисна характеристика неабелевих розщеплюваних метациклічних p -груп згідно Б. Кінг (див. [47], Theorem 3.2 та Proposition 4.10).

Твердження 3.14. *Нехай $G = \langle a \rangle \rtimes \langle b \rangle$ є неабелевою розщеплюваною метациклічною p -групою з $a^{p^m} = b^{p^n} = 1$ для деяких додатніх цілих m та n . Тоді експонента G дорівнює $\max\{p^m, p^n\}$ і виконується одне з наступних тверджень :*

$$I. \ b^{-1}ab = a^{1+p^{m-r}} \text{ з } 1 \leq r < \min\{m, n+1\} \text{ і } r < m-1 \text{ для } p=2;$$

$$II. \ p=2 \text{ і } b^{-1}ab = a^{-1+2^{m-r}} \text{ з } 0 \leq r < \min\{m-1, n+1\}.$$

Нехай група G , що задовольняє одне з тверджень I або II пропозиції 3.14 будемо позначати через $G(p^m, p^n, r)$ або $G(2^m, 2^n, -r)$, відповідно. Крім того, для будь-яких цілих чисел l і $k \geq 0$ покладемо $j(l, 0) = 0$ та

$$j(l, k) = 1 + l + \dots + l^{k-1}$$

для $k \geq 1$.

Зауваження 3.15. Очевидно, що групи $G(p^m, p^n, r)$ ізоморфні групам типу (A.1) з теореми 3.1.

Тепер нехай m, n і r додатні цілі, що задовольняють твердження I з пропозиції 3.14, і нехай t таке найменше натуральне число, що

$$t(1 + p^{m-r}) \equiv 1 \pmod{p^m}.$$

Легко бачити, що $t = 1 + hp^{m-r}$ для деякого h з $0 < h < p^r$ і $(h, p) = 1$.

Лема 3.16. Нехай $p > 2$ чи $p = 2$ і $m-r > 1$. Якщо d і k є невід'ємними, тоді виконуються наступні конгруенції:

$$1) \quad t^d \equiv t^{dt} \equiv 1 + dhp^{m-r} \pmod{p^{2(m-r)}};$$

$$2) \quad j(t^d, k) \equiv k + \binom{k}{2} dhp^{m-r} \pmod{p^{2(m-r)}}.$$

Доведення. 1) Оскільки

$$\begin{aligned} t^d &= (1 + hp^{m-r})^d = 1 + dhp^{m-r} + \binom{d}{2} h^2 p^{2(m-r)} + \dots + h^d p^{d(m-r)} \\ &\equiv 1 + dhp^{m-r} \pmod{p^{2(m-r)}}, \end{aligned}$$

тоді випливає, що

$$\begin{aligned} t^{dt} &= (t^d)^t \equiv (1 + dhp^{m-r})^t \\ &\equiv 1 + tdhp^{m-r} = 1 + dhp^{m-r} + \\ &+ dh^2 p^{2(m-r)} \equiv 1 + dhp^{m-r} \pmod{p^{2(m-r)}}. \end{aligned}$$

2) З визначень та твердження 1) маємо

$$\begin{aligned} j(t^d, k) &= 1 + t^d + \dots + t^{(k-1)d} \\ &\equiv 1 + (1 + dhp^{m-r}) + (1 + 2dhp^{m-r}) + \dots + (1 + (k-1)dhp^{m-r}) \\ &= k + \binom{k}{2} dhp^{m-r} \pmod{p^{2(m-r)}}. \end{aligned}$$

□

Припустимо, що цілі m , n і r задовольняють твердження II пропозиції 3.14 і нехай t є найменшим натуральним числом, що задовольняє конгруенцію

$$t(-1 + 2^{m-r}) \equiv 1 \pmod{2^m}.$$

Легко перевірити, що $t = -1 + h2^{m-r}$ для деякого непарного h з $0 < h < 2^r$.

Лема 3.17. *Нехай $r > 0$. Тоді для не невід'ємних цілих d і k наступні конгруенції мають місце:*

$$1) \ t^{d2^k} \equiv \begin{cases} (-1)^d(1 - dh2^{m-r}) \pmod{2^{2(m-r)}} & \text{якщо } k = 0 \text{ and} \\ 1 - dh2^{m-r+k} \pmod{2^{2(m-r)+k-1}} & \text{якщо } k > 0. \end{cases}$$

$$2) \ j(t^d, k) \equiv \begin{cases} \frac{1-(-1)^k}{2} + \frac{(2k-1)(-1)^k+1}{4}dh2^{m-r} & \pmod{2^{2(m-r)}} \\ & \text{якщо } d \equiv 1 \pmod{2}, \\ k - \binom{k}{2}dh2^{m-r} & \pmod{2^{2(m-r)}} \\ & \text{якщо } d \equiv 0 \pmod{2}. \end{cases}$$

Доведення. Дійсно,

$$\begin{aligned} t^{d2^k} &= (-1 + h2^{m-r})^{d2^k} = (-1)^{d2^k} + (-1)^{d2^k-1}d2^k h2^{m-r} \\ &+ (-1)^{d2^k-2} \binom{d2^k}{2} h^2 2^{2(m-r)} + \dots + h^{d2^k} 2^{d2^k(m-r)} \end{aligned}$$

і

$$\binom{d2^k}{2} \equiv 0 \pmod{2^{k-1}},$$

що доводить 1).

Наступне, випливає з 1), що

$$\begin{aligned} j(t^d, k) &= 1 + t^d + \dots + t^{(k-1)d} \\ &\equiv 1 + (-1)^d(1 - dh2^{m-r}) + (-1)^{2d}(1 - 2dh2^{m-r}) + \dots \\ &+ (-1)^{(k-1)d}(1 - (k-1)dh2^{m-r}) \pmod{2^{2(m-r)}}. \end{aligned}$$

Звідси для непарного d ми маємо

$$\begin{aligned}
 j(t^d, k) &\equiv 1 + (-1 + dh2^{m-r}) + (1 - 2dh2^{m-r}) + \dots \\
 &+ ((-1)^{k-1} + (-1)^{k-2}(k-1)dh2^{m-r}) = \frac{1 - (-1)^k}{2} \\
 &+ (1 - 2 + 3 - \dots + (-1)^{k-2}(k-1))dh2^{m-r} = \frac{1 - (-1)^k}{2} \\
 &+ \frac{(2k-1)(-1)^k + 1}{4}dh2^{m-r} \pmod{2^{2(m-r)}}.
 \end{aligned}$$

Якщо d є парним, тоді ми маємо

$$\begin{aligned}
 j(t^d, k) &\equiv 1 + (1 - dh2^{m-r}) + \\
 &+ (1 - 2dh2^{m-r}) + \dots + (1 - (k-1)dh2^{m-r}) \\
 &= k - (1 + 2 + \dots + (k-1))dh2^{m-r} = \\
 &= k - \binom{k}{2}dh2^{m-r} \pmod{2^{2(m-r)}}.
 \end{aligned}$$

□

Лема 3.18. *Нехай G адитивно записана група, елементи a і b якої задовольняють співвідношенню $a + b = b + as$ для деякого натурального числа s . Якщо t таке найменше натуральне число, що $ast = 0$, тоді для будь-яких невід'ємних цілих d, k і u виконуються рівності*

$$au + bd = bd + as^d u, \quad bd + au = aut^d + bd,$$

$$(au + bd)k = auj(t^d, k) + bdk$$

i

$$(bd + au)k = bdk + auj(s^d, k).$$

Доведення. Оскільки $-b + a + b = as$ і

$$-b + at + b = (-b + a + b)t = ast = a,$$

ми маємо $b + a = at + b$ і тоді $b + au = atu + b$. За індукцією по d , ми отримаємо $au + bd = bd + as^d u$ і $bd + au = at^d u + bd$. Отже,

$$(au + bd)k = au(1 + t^d + \dots + t^{d(k-1)}) + \\ + bdk = auj(t^d, k) + bdk$$

і звідси

$$(bd + au)k = bdk + au(1 + s^d + \dots + s^{d(k-1)}) = \\ = bdk + auj(s^d, k).$$

□

Наступну пропозицію про групу автоморфізмів неабелевої розщеплюваної метациклічної p -групи можна знайти в [25, Theorem 3.1], для $p > 2$ і в [33, Theorem 3.5], для $p = 2$.

Твердження 3.19. *Нехай G є розщеплюваною метациклічною p -групою і нехай S є силовською p -підгрупою групи автоморфізмів $\text{Aut}(G)$. Тоді S є нормальною підгрупою індексу $p-1$ в $\text{Aut}(G)$. Зокрема, якщо $p = 2$, тоді $\text{Aut}(G)$ є 2-групою.*

Інформацію про орбіти групи G відносно дії її групи автоморфізмів $\text{Aut}(G)$ дається в наступній лемі.

Лема 3.20. *Нехай $G = G(p^m, p^n, r)$ з $m \leq n + r$, $A = \text{Aut}(G)$ і нехай $\langle x \rangle$ є циклічною підгрупою G . Тоді виконуються наступні твердження:*

1) якщо $\langle x \rangle$ є нормальною підгрупою порядку p^m в G , тоді

$$|x^A| \leq p^{2m-r-1}(p-1);$$

2) якщо $p > 2$, $m \leq n$ і $\langle x \rangle$ не є нормальною підгрупою порядку p^n , тоді $x^{-1} \notin x^A$.

Доведення. Якщо $G = \langle a \rangle \rtimes \langle b \rangle$ with $b^{-1}ab = a^{1+p^{m-r}}$ і $\langle x \rangle$ є нормальною підгрупою порядку p^m в G , тоді або $\langle a \rangle \cap \langle x \rangle = 1$ і тоді $\langle x \rangle$ централізатор підгрупи $\langle a \rangle$, або $a^{p^{m-1}} \in \langle x \rangle$. Оскільки $G' = \langle a^{p^{m-r}} \rangle$ є характеристичною підгрупою G , звідки випливає, що в першому випадку $\langle a \rangle \cap \langle x^\alpha \rangle = 1$ для кожної $\alpha \in A$. Звідки $x^A \subseteq C_G(a) = \langle a \rangle \times \langle b^{p^r} \rangle$ і тоді $|x^A| \leq p^{2m-r-1}(p-1)$. В другому випадку $G = \langle x \rangle \rtimes \langle b \rangle$ і тоді $G' = \langle a^{p^{m-r}} \rangle \leq \langle x \rangle$. Тоді

$$|\langle x \rangle \langle x^\alpha \rangle| = \frac{|x||x^\alpha|}{|\langle x \rangle \cap \langle x \rangle^\alpha|} \leq p^{2m-r},$$

звідси

$$\langle x \rangle \langle x^\alpha \rangle \leq \langle x \rangle \rtimes \langle b^{p^{n+r-m}} \rangle$$

і, зокрема,

$$x^\alpha \in \langle x \rangle \rtimes \langle b^{p^{n+r-m}} \rangle.$$

Враховуючи, що кількість елементів порядку p^m в $\langle x \rangle$ рівна $p^{m-1}(p-1)$, маємо $|x^A| \leq p^{2m-r-1}(p-1)$, що доводить твердження 1).

Тепер нехай $p > 2$, $m \leq n$ і нехай $\langle x \rangle$ не є нормальними підгрупами порядку p^n в G . Оскільки $G' = \langle a^{p^{m-r}} \rangle$, звідси випливає, що

$$\langle a \rangle \cap \langle x \rangle = \langle a^{p^s} \rangle$$

для такого деякого цілого s , що $m \geq s > m-r$ і тоді

$$\langle a^{p^s} \rangle = \langle x^{p^{n-m+s}} \rangle.$$

Отже, $x = a^u b^{vp^{m-s}}$ для деяких цілих u і v з $(v, p) = 1$ і звідки

$$[a, x] = [a, b^{vp^{m-s}}] = a^{wp^{2m-r-s}},$$

де

$$w = \frac{(1 + p^{m-r})vp^{m-s}-1}{p^{2m-r-s}}$$

і, зокрема, $(w, p) = 1$.

Припустимо, що $x^\alpha = x^{-1}$ для деякого автоморфізма $\alpha \in A$. Як було показано вище,

$$a^\alpha \in \langle a \rangle \rtimes \langle b^{p^{n+r-m}} \rangle,$$

звідки $a^\alpha = a^k b^{lp^{n+r-m}}$ для деяких цілих k і l з $(k, p) = 1$. Більш того,

$$\langle a^{p^{m-r}} \rangle^\alpha = \langle a^{p^{m-r}} \rangle$$

і тоді

$$\begin{aligned} (a^{p^{m-r}})^\alpha &= (a^k b^{lp^{n+r-m}})^{p^{m-r}} = \\ &= a^{kp^{m-r}} b^{lp^n} = a^{kp^{m-r}}. \end{aligned}$$

Оскільки $(a^{p^{m-r}})^\alpha = a^{kp^{m-r}}$. З іншого боку, тому, що $m \leq n$ звідки випливає, що

$$b^{lp^{n+r-m}} \in \langle b^r \rangle \leq Z(G).$$

Отже,

$$\begin{aligned} a^{kwp^{m-r}} &= (a^{wp^{m-r}})^\alpha = [a, x]^\alpha = \\ &= [a^\alpha, x^{-1}] = [a^k b^{lp^{n+r-m}}, x^{-1}] = [a^k, x^{-1}] = \\ &= [a, x^{-1}]^k = ([a, x]^{-k})^{x^{-1}} = (a^{-kwp^{m-r}})^{x^{-1}}. \end{aligned}$$

Звідки

$$(a^{kwp^{m-r}})^x = a^{-kwp^{m-r}}.$$

В той же час, при $p > 2$ остання рівність має місце лише у випадку $a^{kwp^{m-r}} = 1$. Оскільки $(kw, p) = 1$, це означає, що $a^{p^{m-r}} = 1$, що суперечить гіпотезі леми. Отже, $x^{-1} \notin x^A$, як стверджувалося в твердженні 2). $\square$

Лема 3.21. *Нехай R з розщеплювальною метациклічною адитивною p -групою R^+ і нехай L є її підгрупою всіх необоротних елементів з R . Якщо R^+ є неабелевою, тоді $|R^+ : L| = p$.*

Доведення. Дійсно, маємо $|R^+ : L| = p^k$ для деяких $k \geq 1$ і тоді $|R| = p^k |L|$. Оскільки $R = R^* \cup L$ з $R^* \cap L = \emptyset$, то

$$|R^*| = p^k |L| - |L| = (p^k - 1)|L|$$

і, таким чином, порядок R^* ділиться на $p^k - 1$. З іншого боку, для кожного елемента $r \in R^*$ відображення $x \mapsto rx$ з $x \in R$ є автоморфізмом R^+ , тому, що $r(x + y) = rx + ry$ для всіх $x, y \in R$. Тому R^* можна розглядати як підгрупу $\text{Aut}(R^+)$. Крім того, це впливає з пропозиції 3.19, що порядок $\text{Aut}(R^+)$ ділиться на $p^k - 1$ тільки якщо $k = 1$. Отже, $|R^+ : L| = p$, як вимагалось. $\square$

Як прямий наслідок з лем 3.14, 3.11 і 3.21 ми маємо наступне твердження.

Наслідок 3.22. *Нехай R є локальним майже-кільцем чия адитивна група R^+ є неабелевою розщеплюваною p -групою. Тоді група R^+ породжується елементами a і b порядків p^m і p^n , відповідно, один з яких збігається з одиничним елементом R і $a + b = b + a(1 + p^{m-r})$, якщо R^+ є ізоморфною групі $G(p^m, p^n, r)$, і $a + b = b + a(-1 + 2^{m-r})$, якщо R^+ є ізоморфною групі $G(2^m, 2^n, -r)$.*

3.2.3. Майже-кільце з одиницею на неабелевій розщеплюваній метациклічній p -групі

Нехай R є майже-кільцем з одиницею адитивні група якого R^+ є розщеплюваною неабелевою метациклічною p -групою з $p \geq 2$. Тоді $R^+ = \langle a \rangle + \langle b \rangle$ для деяких елементів a і b з R задовольняють співвідношення $ap^m = bp^n = 0$ і $b + a = at + b$ з $(p, t) = 1$. Зокрема, кожний елемент $x \in R$ однозначно записується у вигляді $x = ax_1 + bx_2$ з коефіцієнтами

$0 \leq x_1 < p^m$ і $0 \leq x_2 < p^n$. У цьому розділі ми розглянемо випадки, коли один із елементів a чи b належить R^* .

Припустимо спочатку, що $a \in R^*$. Тоді R^+ є групою з експонентою p^m за лемою 3.10 and so $m \geq n$. Далі, згідно леми 3.11, ми можемо без втрати загальності припустити, що a є одиницею в R , тобто $ax = xa = x$ для кожного $x \in R$. Крім того, для кожного $x \in R$ існують такі коефіцієнти $\alpha(x)$ і $\beta(x)$, що $xb = a\alpha(x) + b\beta(x)$. Зрозуміло, що вони однозначно визначені по модулю p^m і p^n , відповідно, тому визначені деякі відображення $\alpha : R \rightarrow Z_{p^m}$ та $\beta : R \rightarrow Z_{p^n}$.

Лема 3.23. *Нехай $x = ax_1 + bx_2$ і $y = ay_1 + by_2$ є елементами майже-кілля R . Якщо a одиницею в R , тоді $r < m \geq n$ і наступні твердження виконуються:*

(0) $\alpha(0) = \beta(0) = 0$ тоді і тільки тоді, коли майже-кілля R є нуль-симетричним;

(1) $\alpha(a) = 0$ і $\beta(a) = 1$;

(2) $xy = a[x_1j(t^{x_2}, y_1) + \alpha(x)j(t^{\beta(x)}, y_2)t^{x_2y_1}] + b(x_2y_1 + \beta(x)y_2)$;

(3) $\alpha(x)(t^{x_2t} - 1) \equiv x_1(t^{\beta(x)} - j(t^{x_2}, t)) \pmod{p^m}$;

(4) $x_2(t - 1) \equiv 0 \pmod{p^n}$.

Доведення. Оскільки $0 \cdot a = a \cdot 0 = 0$, звідси випливає R є нуль-симетричним наближенням тоді і тільки тоді, коли

$$0 = 0 \cdot b = a\alpha(0) + b\beta(0)$$

або еквівалентно $\alpha(0) = \beta(0) = 0$. Більш того, оскільки

$$b = ab = a\alpha(a) + b\beta(a),$$

ми маємо $\alpha(a) = 0$ і $\beta(a) = 1$, так, що виконуються твердження (0) і (1).

Далі використовуючи ліводистрибутивний закон

$$xy = (xa)y_1 + (xb)y_2 = (ax_1 + bx_2)y_1 + (a\alpha(x) + b\beta(x))y_2.$$

Застосовуючи лему 3.18, ми також маємо

$$(ax_1 + bx_2)y_1 = ax_1j(t^{x_2}, y_1) + bx_2y_1,$$

$$(a\alpha(x) + b\beta(x))y_2 = a\alpha(x)j(t^{\beta(x)}, y_2) + b\beta(x)y_2$$

і

$$bx_2y_1 + a\alpha(x)j(t^{\beta(x)}, y_2) = a\alpha(x)j(t^{\beta(x)}, y_2)t^{x_2y_1} + bx_2y_1.$$

Отже,

$$xy = a[x_1j(t^{x_2}, y_1) + \alpha(x)j(t^{\beta(x)}, y_2)t^{x_2y_1}] + b(x_2y_1 + \beta(x)y_2)$$

і тому виконується твердження (2). Покладаючи в цій формулі $y = at + b$, ми отримаємо

$$xy = a[x_1j(t^{x_2}, t) + \alpha(x)t^{x_2t}] + b(x_2t + \beta(x)).$$

З іншого боку, $y = b + a$ і так

$$xy = xb + x = a(\alpha(x) + x_1t^{\beta(x)}) + b(x_2 + \beta(x))$$

за лемою 3.18. Порівнюючи коефіцієнти біля a і b в двох останніх виразах для xy , отримуємо для кожного $x \in R$ рівність

$$\alpha(x)(t^{x_2t} - 1) \equiv x_1(t^{\beta(x)} - j(t^{x_2}, t)) \pmod{p^m}$$

і

$$x_2(t - 1) \equiv 0 \pmod{p^n},$$

тобто твердження (3) і (4), як стверджувалося. □

Розглянемо тепер випадок, коли $b \in R^*$.

Лема 3.24. *Якщо $b \in R^*$, тоді $a \notin R^*$, $p = 2$ і $r + 1 < m \leq n$.*

Доведення. Нехай $b \in R^*$. Тоді R^+ є експонентою p^n за лемою 3.10 і тоді $m \leq n$. Розглянемо мультиплікативну групу R^* як підгрупу групи автоморфізмів $A = \text{Aut}(R^+)$ в R^+ , ми маємо $R^*x \subseteq x^A$ для кожного $x \in R$ і, зокрема, $R^* = R^*b \subseteq b^A$. Якщо $a \in b^A$, то $a = b^\phi$ для деякого автоморфізму $\phi \in A$ і тоді $\langle a \rangle^\phi = \langle b \rangle$. Оскільки підгрупа $\langle a \rangle$ є нормальною в R^+ і $\langle b \rangle$ не є нормальною, остання рівність неможлива. Тому $a \notin b^A$ і, отже, $a \notin R^*$. Припустимо, що $p > 2$. Тоді $-b \notin b^A$ за лемою 3.20 і тоді $-b \notin R^*$. З іншого боку, якщо i є одиницею в R , тоді

$$b^{-1}(-b) = -(b^{-1}b) = -i.$$

Оскільки $(-i)^2 = -(-i) = i$, з цього випливає $b^{-1}(-b) = -i \in R^*$ і тоді $-b \in bR^* = R^*$. Це протиріччя показує, що $p = 2$ і тоді $r + 1 < m$ за пропозицією 3.14. $\square$

Як і вище, згідно леми 3.11, у випадку $b \in R^*$ ми можемо припустити, що b є одиницею в R і для кожного $x \in R$ існують коефіцієнти $\alpha(x)$ і $\beta(x)$ які однозначно визначаються x за модулем 2^m і 2^n , відповідно такі, що $xa = a\alpha(x) + b\beta(x)$.

Лема 3.25. *Нехай $x = ax_1 + bx_2$ і $y = ay_1 + by_2$ є елементами майже-кільця R . Якщо b є одиницею в R , тоді $p = 2$, $r+1 < m \leq n$ і справедливі наступні твердження:*

(0) $\alpha(0) = \beta(0) = 0$ тоді і тільки тоді, коли майже-кільце R є нуль-симетричним;

(1) $\alpha(b) = 1$ і $\beta(b) = 0$;

(2) $xy = a[\alpha(x)j(t^{\beta(x)}, y_1) + x_1j(t^{x_2}, y_2)t^{\beta(x)y_1}] + b(\beta(x)y_1 + x_2y_2)$;

(3) $\alpha(x)(j(t^{\beta(x)}, t) - t^{x_2}) \equiv x_1(1 - t^{\beta(x)t}) \pmod{2^m}$;

(4) $\beta(x)(t - 1) \equiv 0 \pmod{2^n}$.

Доведення. Спочатку розглянемо $p = 2$ і $r + 1 < m \leq n$ за лемою 3.24. Оскільки $0 \cdot b = b \cdot 0 = 0$, майже-кільце R є нуль-симетричним тоді і тільки тоді, коли

$$0 = 0 \cdot a = a\alpha(0) + b\beta(0),$$

звідки $\alpha(0) = \beta(0) = 0$. Так само і рівність $a = ba = a\alpha(b) + b\beta(b)$ означає, що $\alpha(b) = 1$ і $\beta(b) = 0$, тобто виконуються твердження (0) і (1). Далі використовуючи ліводистрибутивний закон, ми отримаємо

$$xy = (xa)y_1 + (xb)y_2 = (a\alpha(x) + b\beta(x))y_1 + (ax_1 + bx_2)y_2.$$

Застосовуючи лему 3.18, ми також маємо

$$(a\alpha(x) + b\beta(x))y_1 = a\alpha(x)j(t^{\beta(x)}, y_1) + b\beta(x)y_1,$$

$$(ax_1 + bx_2)y_2 = ax_1j(t^{x_2}, y_2) + bx_2y_2$$

та

$$b\beta(x)y_1 + ax_1j(t^{x_2}, y_2) = ax_1j(t^{x_2}, y_2)t^{\beta(x)y_1} + b\beta(x)y_1.$$

Тому

$$xy = a[\alpha(x)j(t^{\beta(x)}, y_1) + x_1j(t^{x_2}, y_2)t^{\beta(x)y_1}] + b(\beta(x)y_1 + x_2y_2),$$

що підтверджує твердження (2). Підставляючи $y = at + b$ у цій рівності ми отримуємо

$$xy = a[\alpha(x)j(t^{\beta(x)}, t) + x_1t^{\beta(x)t}] + b(x_2 + \beta(x)t).$$

З іншого боку, $y = b + a$ і, таким чином

$$xy = x + xa = a(x_1 + \alpha(x)t^{x_2}) + b(x_2 + \beta(x)).$$

Порівнюючи коефіцієнти біля a і b в двох останніх виразах для xy , отримуємо рівності

$$\alpha(x)j(t^{\beta(x)}, t) + x_1t^{\beta(x)t} \equiv x_1 +$$

$$\alpha(x)t^{x_2} \pmod{2^m}$$

та

$$x_2 + \beta(x)t \equiv x_2 + \beta(x) \pmod{2^n},$$

з яких прямо випливають твердження (3) і (4). $\square$

3.2.4. Майже-кільце з одиницею на групі $G(p^m, p^n, r)$

Наступні дві леми описують множення в майже-кільці R адитивна група якого R^+ є ізоморфною групі $G(p^m, p^n, r)$, тобто R^+ породжується елементами a і b задовольняє співвідношення $ap^m = bp^n = 0$ і $b+a = at+b$ з $t = 1 + hp^{m-r}$, де $0 < h < p^r$ і $(h, p) = 1$. Як зазначалося вище, ми обмежимося випадками, коли один з елементів a і b є одиницею в R . Надалі, $x = ax_1 + bx_2$ і $y = ay_1 + by_2$ є довільними елементами з R .

Лема 3.26. *Якщо a є одиничним елементом в R , то $m \geq n + r \geq 2r$ і*

$$xy = a(x_1y_1 + \alpha(x)y_2 - x_1x_2 \binom{y_1}{2} p^{m-r}) + b(x_2y_1 + \beta(x)y_2).$$

Крім того, справедливі наступні твердження:

$$(1) \alpha(x) \equiv 0 \pmod{p^{m-n}};$$

$$(2) x_1(\beta(x) - 1) \equiv 0 \pmod{p^r} \text{ або } p = 2, m = 2r, n = r \text{ та } x_1(\beta(x) - 1) \equiv 0 \pmod{2^{r-1}};$$

$$(3) \alpha(xy) = x_1\alpha(y) + \alpha(x)\beta(y) - x_1x_2 \binom{\alpha(y)}{2} p^{m-r};$$

$$(4) \beta(xy) = x_2\alpha(y) + \beta(x)\beta(y).$$

Доведення. Оскільки $t - 1 = hp^{m-r}$ з $(h, p) = 1$ і $x_2(t - 1) \equiv 0 \pmod{p^n}$ за твердженням (4) леми 3.23, ми маємо $m - r \geq n$. Тому

$$m \geq n + r \geq 2r \tag{3.1}$$

і, зокрема, $2(m-r) \geq m$. Крім того, з

$$(1 + hp^{m-r})(1 + p^{m-r}) \equiv 1 \pmod{p^m}$$

випливає

$$hp^{m-r} \equiv -p^{m-r} \pmod{p^m}. \quad (3.2)$$

Звідси і леми 3.16 отримуємо

$$j(t^{x_2}, y_1) \equiv y_1 - x_2 \binom{y_1}{2} p^{m-r} \pmod{p^m}, \quad (3.3)$$

$$j(t^{\beta(x)}, y_2) \equiv y_2 - \beta(x) \binom{y_2}{2} p^{m-r} \pmod{p^m} \quad (3.4)$$

та

$$t^{x_2 y_1} \equiv 1 - x_2 y_1 p^{m-r} \pmod{p^m}. \quad (3.5)$$

Підставляючи тепер у формулу (2) леми 3.23 замість лівих частин конгруенцій (3.3)–(3.5) їх праві частини, одержуємо рівність

$$\begin{aligned} xy = a[(x_1 y_1 + \alpha(x) y_2) - (x_1 x_2 \binom{y_1}{2} + \alpha(x) \beta(x) \binom{y_2}{2} + \\ + \alpha(x) x_2 y_1 y_2) p^{m-r}] + b(x_2 y_1 + \beta(x) y_2). \end{aligned} \quad (3.6)$$

Підставляючи в цій рівності $y = bp^n = 0$, маємо

$$\begin{aligned} 0 = x(bp^n) &= a(\alpha(x)p^n - \alpha(x)\beta(x) \binom{p^n}{2} p^{m-r}) \\ &= a\alpha(x)p^n(1 - \beta(x) \binom{p^n}{2} p^{m-r-n}). \end{aligned}$$

Оскільки $m-r \geq 1$ для $p > 2$ та $m-r \geq 2$ для $p = 2$, то

$$1 - \beta(x) \binom{p^n}{2} p^{m-r-n} \equiv 1 \pmod{p}$$

і $a\alpha(x)p^n = 0$. Тому

$$\alpha(x) \equiv 0 \pmod{p^{m-n}}, \quad (3.7)$$

тобто твердження (1) виконується. Більш того, оскільки $m - n \geq r$ згідно (3.1), з цього випливає, що $a\alpha(x)p^{m-r} = 0$ а, отже, рівність (3.6) можна переписати у вигляді

$$xy = a(x_1y_1 + \alpha(x)y_2 - x_1x_2\binom{y_1}{2}p^{m-r}) + b(x_2y_1 + \beta(x)y_2),$$

як стверджувалося.

Оскільки

$$x(yb) = (xy)b = a\alpha(xy) + b\beta(xy),$$

замінивши в останній рівність y на $yb = a\alpha(y) + b\beta(y)$ та порівнюючи коефіцієнти при a і b у двох виразах отримані для $x(yb)$, отримуємо формули

$$\alpha(xy) = a(x_1\alpha(y) + \alpha(x)\beta(y) - x_1x_2\binom{\alpha(y)}{2}p^{m-r})$$

і

$$\beta(xy) = b(x_2\alpha(y) + \beta(x)\beta(y))$$

твердження (3) і (4) леми.

Далі, використовуючи лему 3.16, також маємо

$$t^{x_2t} \equiv 1 - x_2p^{m-r} \pmod{p^m}, \quad (3.8)$$

$$t^{\beta(x)} \equiv 1 - \beta(x)p^{m-r} \pmod{p^m} \quad (3.9)$$

та

$$j(t^{x_2}, t) \equiv \begin{cases} 1 - p^{m-r} & \pmod{p^m}, \text{ якщо } p > 2, \\ 1 - 2^{m-r}(1 - x_22^{m-r-1}) & \pmod{2^m} \text{ якщо } p = 2. \end{cases} \quad (3.10)$$

Підставляючи праві частини конгруенцій (3.7)–(3.9) в конгруенцію (3) з леми 3.23, отримаємо конгруентності

$$\alpha(x)x_2 \equiv x_1(\beta(x) - 1) \pmod{p^r} \quad (3.11)$$

для $p > 2$ та

$$\alpha(x)x_2 \equiv x_1(\beta(x) - 1 + x_2 2^{m-r-1}) \pmod{2^r} \quad (3.12)$$

для $p = 2$. Оскільки $m - n \geq r$ за (3.1), то з умов (3.7), (3.11) та (3.12) випливає, що

$$x_1(\beta(x) - 1) \equiv 0 \pmod{p^m}$$

для $p > 2$ і

$$x_1(\beta(x) - 1 + x_2 2^{m-r-1}) \equiv 0 \pmod{2^r}$$

для $p = 2$. Більш того, якщо $m > 2r$, то

$$x_1(\beta(x) - 1) \equiv 0 \pmod{2^r}$$

тому в цьому випадку виконується твердження (2). В іншому випадку $p = 2$, $m = 2r$, $n = r$ та

$$x_1(\beta(x) - 1) \equiv 0 \pmod{2^{r-1}}.$$

□

Лема 3.27. Якщо b є одиницею в R , то $p = 2 < m \leq n$, $r = 1$ та

$$xy = a[\alpha(x)y_1 + x_1 j(t^{x_2}, y_2)] + b(\beta(x)y_1 + x_2 y_2).$$

Більш того, справедливі наступні твердження:

$$(0) \quad \alpha(0) = \beta(0) = 0;$$

$$(1) \quad \beta(x) \equiv 0 \pmod{2^{n-m+1}};$$

$$(2) \quad \alpha(x)(1 - x_2) \equiv 0 \pmod{2};$$

$$(3) \quad \alpha(xy) = \alpha(x)\alpha(y) + x_1 j(t^{x_2}, \beta(y));$$

$$(4) \quad \beta(xy) = \beta(x)\alpha(y) + x_2 \beta(y).$$

Доведення. Це випливає з лема 3.25, що $p = 2$ та $m \leq n$. Крім того, твердження (4) з цієї лема і рівності $t - 1 = h2^{m-r}$ з $(h, 2) = 1$ випливає, що

$$\beta(x) \equiv 0 \pmod{2^{n-m+r}}.$$

З цього та лема 3.16 випливає, що для кожного цілого числа $k \geq 0$ виконуються конгруенції

$$t^{\beta(x)k} \equiv 1 \pmod{2^n} \quad (3.13)$$

та

$$j(t^{\beta(x)}, k) \equiv k \pmod{2^n}. \quad (3.14)$$

Зокрема, приймаючи $k = y_1$ і застосовуючи ці конгруенції до формули (2) в лемі 3.25, ми отримуємо для R формулу множення

$$xy = a[\alpha(x)y_1 + x_1j(t^{x_2}, y_2)] + b(\beta(x)y_1 + x_2y_2), \quad (3.15)$$

як вимагалось. Далі, виражаючи ліву частину рівності $x(ya) = (xy)a$ за формулою (3.15) і враховуючи це $ya = a\alpha(y) + b\beta(y)$ та

$$(xy)a = a\alpha(xy) + b\beta(xy),$$

виведемо формули для $\alpha(xy)$ та $\beta(xy)$, тобто твердження (3) та (4) лема.

Далі, покладаючи $k = t$ в конгруенціях (3.13) та (3.14), ми маємо

$$1 - t^{\beta(x)t} \equiv 0 \pmod{2^n} \quad (3.16)$$

та

$$j(t^{\beta(x)}, t) - t^{x_2} \equiv t - t^{x_2} \pmod{2^n}. \quad (3.17)$$

Оскільки $m \leq n$, конгруенції (3.3), (3.4) та твердження (3) лема 3.25 випливає, що

$$\alpha(x)(t - t^{x_2}) \equiv 0 \pmod{2^n}. \quad (3.18)$$

З іншого боку,

$$t^{x_2} \equiv 1 + x_2h2^{m-r} \pmod{2^{2(m-r)}}$$

за лемою 3.16 і, отже,

$$t - t^{x_2} \equiv (1 - x_2)h2^{m-r} \pmod{2^{2(m-r)}}. \quad (3.19)$$

Тому конгруенції (3.5) та (3.7) означають це

$$\alpha(x)(1 - x_2) \equiv 0 \pmod{2^{\min\{r, m-r\}}}.$$

Зокрема,

$$\alpha(-b)(1 + 1) \equiv 0 \pmod{2^{\min\{r, m-r\}}}$$

і, отже,

$$\alpha(-b) \equiv 0 \pmod{2^{\min\{r, m-r\}-1}}. \quad (3.20)$$

Нарешті, оскільки $b = (-b)^2$ та $\alpha(b) = 1$ за твердженням (1) з леми 3.25, звідси випливає $\alpha((-b)^2) = 1$. Однак, $\alpha((-b)^2) = \alpha(-b)^2$ за твердженням (3) з леми, так що $\alpha(-b) \equiv \pm 1 \pmod{2}$. Порівняння цього та конгруенцій (vii), отримуємо, що $\min\{r, m-r\} = 1$ та

$$\alpha(x)(1 - x_2) \equiv 0 \pmod{2},$$

тобто виконується твердження (2) леми. Більш того, оскільки $r < m - 1$ за пропозицією 3.14, впливає, що $r = 1$ і, таким чином $\beta(x) \equiv 0 \pmod{2^{n-m+1}}$. Зокрема, якщо $x = 0$, потім обидва $\alpha(0)$ та $\beta(0)$ є парними цілими числами. Оскільки $\alpha(0) = \alpha(0)^2$ та $\beta(0) = \beta(0)\alpha(0)$ за твердженнями (3) та (4) леми, з цього випливає, що $\alpha(0) = \beta(0) = 0$. Це доводить твердження (0) та (1) леми і завершує доведення. $\square$

3.2.5. Майже-кільце з одиницею на групі $G(2^m, 2^n, -r)$

У цьому підрозділі ми описуємо множення в майже-кільці R , адитивна група R^+ якого ізоморфна групі $G(2^m, 2^n, -r)$ і один із двох твірних a та b цієї групи збігається з одиницею в R . Нагадаємо, що породжуючи a

та b в R^+ задовольняють співвідношення $a2^m = b2^n = 0$ та $b + a = at + b$ з $t = -1 + h2^{m-r}$, де $0 \leq r < \min\{m-1, n+1\}$ та $0 < h < 2^r$ з $(h, 2) = 1$. Як і раніше, $x = ax_1 + bx_2$ та $y = ay_1 + by_2$ позначають довільні елементи R .

Лема 3.28. *Якщо a є одиничним елементом в R , то $m = 2$, $n = 1$ та $r = 0$, тобто, R^+ є дієдральною групою порядку 8.*

Доведення. Оскільки

$$x_2(-2 + h2^{m-r}) \equiv 0 \pmod{2^n}$$

за твердженням (4) леми 3.23, випливає, що

$$-1 + h2^{m-r-1} \equiv 0 \pmod{2^{n-1}},$$

а, отже, $n = 1$. Звідси $0 \leq r \leq 1$ і таким чином або $r = 0$ та $t = -1 + 2^m$ чи $r = 1$ та $t = -1 + 2^{m-1}$. Але якщо $t = -1 + 2^m$, тоді $R^+ = \langle a \rangle + \langle b \rangle$ є ізоморфною дієдральній групі порядку 2^{m+1} а це можливо тільки в тому випадку, якщо $m = 2$ за [50, Proposition 4.4].

Нехай $t = -1 + 2^{m-1}$. Тоді твердження (3) з леми 3.23 випливає, що

$$\alpha(x)(t^{x_2 t} - 1) \equiv x_1(t^{\beta(x)} - j(t^{x_2}, t)) \pmod{2^m}$$

для кожного $x = ax_1 + bx_2$. Зокрема, якщо $x = a + b$, тоді

$$\alpha(x)(t^t - 1) \equiv t^{\beta(x)} - j(t, t) \pmod{2^m}.$$

Крім того,

$$t^t \equiv -1 - 2^{m-1} \pmod{2^m}, \quad j(t, t) \equiv 1 - 2^{m-1} \pmod{2^m}$$

та

$$t^{\beta(x)} \equiv (-1)^{\beta(x)}(1 - \beta(x)2^{m-1}) \pmod{2^m}$$

за лемою 3.17. Тому

$$\alpha(x)(-2 - 2^{m-1}) \equiv ((-1)^{\beta(x)} - 1) -$$

$$-((-1)^{\beta(x)}\beta(x) - 1)2^{m-1} \pmod{2^m}.$$

Проте, якщо $\beta(x) \equiv 1 \pmod{2}$, тоді

$$\alpha(x)(-2 - 2^{m-1}) \equiv -2 \pmod{2^m},$$

з чого випливає, що $\alpha(x) \equiv 1 \pmod{2}$ з $m \geq 3$. З іншого боку, $b2 = 0$ і $xb = a\alpha(x) + b\beta(x)$, так, що $\alpha(x) \equiv 2 \pmod{2^m}$. Тому $\beta(x) \equiv 0 \pmod{2}$ і звідси $xb = a\alpha(x)$. Але тоді $\alpha(x) \equiv 2^{m-1} \pmod{2^m}$ а, отже,

$$0 \equiv \alpha(x)(-2 - 2^{m-1}) \equiv 2^{m-1} \pmod{2^m},$$

що неможливо для $m > 1$. Це протиріччя завершує доведення. $\square$

Лема 3.29. *Якщо b є одиничним елементом в R , тоді $2 < m \leq n$, $0 \leq r \leq 1$ та*

$$xy = a[\alpha(x)y_1 + x_1j(t^{x_2}, y_2)] + b(\beta(x)y_1 + x_2y_2).$$

Крім того, мають місце наступні твердження:

$$(0) \quad \alpha(0) = \beta(0) = 0 \text{ або } \alpha(0) = 1;$$

$$(1) \quad \beta(x) \equiv 0 \pmod{2^{n-1}};$$

$$(2) \quad \alpha(xy) = \begin{cases} \alpha(x)\alpha(y) + x_1\beta(y), & \text{якщо } m = n \text{ та } x_2 \equiv 0 \pmod{2}, \text{ та} \\ \alpha(x)\alpha(y), & \text{інакше;} \end{cases}$$

$$(3) \quad \beta(xy) = \beta(x)\alpha(y) + x_2\beta(y).$$

Доведення. Спочатку зазначимо, що $r + 1 < m \leq n$ за лемою 3.24 та $\beta(x)(t - 1) \equiv 0 \pmod{2^n}$ за твердженням (4) леми 3.25. Оскільки $t = -1 + h2^{m-r}$ для деякого непарного цілого числа h , маємо

$$\beta(x)(-2 + h2^{m-r}) \equiv 0 \pmod{2^n}$$

та $\beta(x) \equiv 0 \pmod{2^{n-1}}$, тобто, виконується твердження (1) леми. Як $2(m - r) + n - 2 \geq m + n - r$ та

$$t^{\beta(x)} \equiv 1 + h2^{m+n-r-1} \pmod{2^{m+n-r}}$$

за твердженням 1) леми 3.17, випливає, що $t^{\beta(x)k} \equiv 1 \pmod{2^m}$ а, отже, $j(t^{\beta(x)}, k) \equiv k \pmod{2^m}$ для кожного цілого $k \geq 0$. Зокрема, покладемо $k = y_1$ і використання двох останніх конгруенцій у твердженні (2) леми 3.25, ми можемо переписати формулу для xy у вигляді

$$xy = a[\alpha(x)y_1 + x_1j(t^{x_2}, y_2)] + b(\beta(x)y_1 + x_2y_2), \quad (3.21)$$

як вимагалось.

Далі, якщо $k = t$, тоді згадані вище конгруенції та твердження (3) з леми 3.25 випливає, що

$$\alpha(x)(t - t^{x_2}) \equiv 0 \pmod{2^m}.$$

Зокрема, якщо $x = -b = b(2^n - 1)$, тоді $x_2 = 2^n - 1$ і

$$t - t^{x_2} = t - t^{2^n-1} \equiv t^2 - t^{2^n} \pmod{2^m}.$$

Оскільки $t^{2^{m-1}} \equiv 1 \pmod{2^m}$ та $m \leq n$, випливає, що

$$t - t^{x_2} \equiv t^2 - 1 = h2^{m-r+1}(-1 + h2^{m-r-1}) \pmod{2^m}.$$

Отже,

$$\alpha(-b)2^{m-r+1} \equiv 0 \pmod{2^m},$$

так, що $r = 0$ або $r \geq 1$ та

$$\alpha(-b) \equiv 0 \pmod{2^{r-1}}. \quad (3.22)$$

Тепер виражаємо обидві частини рівності $x(ya) = (xy)a$ за формулою (3.21) і підрівнюючи коефіцієнти при a та b , отримуємо

$$\alpha(xy) = \alpha(x)\alpha(y) + x_1j(t^{x_2}, \beta(y)) \quad (3.23)$$

та

$$\beta(xy) = \beta(x)\alpha(y) + x_2\beta(y). \quad (3.24)$$

Зокрема, якщо $x = y = -b$, тоді $x_1 = 0$ і від рівності (3.23) випливає, що $\alpha((-b)^2) = \alpha(-b)^2$. Як $(-b)^2 = -(-b) = b$ and $\alpha(b) = 1$ за твердженням (1) з леми 3.25, з цього випливає $\alpha(-b) \equiv \pm 1 \pmod{2^m}$ і, отже, конгруентність (3.22) виконується якщо і тільки якщо $r = 1$.

Нарешті, це випливає з твердження 2) леми 3.17, що

$$j(t^{x_2}, \beta(x)) \equiv 0 \pmod{2^{n-1}}$$

для $x_2 \equiv 0 \pmod{2}$ та

$$j(t^{x_2}, \beta(x)) \equiv 0 \pmod{2^n}$$

для $x_2 \equiv 1 \pmod{2}$. Тому твердження (2) і (3) леми безпосередньо випливають з рівностей (3.23) та (3.24). Крім того, якщо $x = y = 0$, тоді $\alpha(0) = \alpha(0)^2$ за рівністю (3.23) та $\beta(0) = \beta(0)\alpha(0)$ за рівністю (3.24), так що $\alpha(0) = \beta(0) = 0$ або $\alpha(0) = 1$. Це підтверджує твердження (0) леми і завершує доведення. $\square$

3.2.6. Локальні майже-кільця на групах $G(p^m, p^n, r)$ та $G(2^m, 2^n, -r)$

Тепер ми застосуємо результати попереднього розділу для опису локальних майже-кільць, адитивні групи яких є неабелевими розщеплюваними метациклічними групами. Нагадаємо, що якщо R є таким локальним майже-кільцем, то його адитивна група R^+ є порядку p^{m+n} для деякого простого числа p і тому є ізоморфною до однієї з груп $G(p^m, p^n, r)$ чи $G(2^m, 2^n, -r)$ за пропозицією 3.14. Отже, $R^+ = \langle a \rangle + \langle b \rangle$ з елементами a та b такими, що $ap^m = bp^n = 0$ та $\langle a \rangle$ є нормальною підгрупою в R^+ . Зокрема, кожен елемент $x \in R$ однозначно записаний у вигляді $x = ax_1 + bx_2$ з коефіцієнтами $0 \leq x_1 < p^m$ та $0 \leq x_2 < p^n$. Крім того,

множина L всіх необоротних елементів в R є підгрупою індексу p в R^+ за лемою 3.21.

Теорема 3.30. *Нехай R є локальним майже-кільцем адитивна група R^+ , якого є ізоморфною групі $G(p^m, p^n, r)$. Тоді $R^+ = \langle a \rangle + \langle b \rangle$, один з елементів a чи b збігається з одиничним елементом в R і виконуються наступні твердження:*

- 1) $ap^m = bp^n = 0$ та $a + b = b + a(1 + p^{m-r})$ з $1 \leq r < \min\{m, n + 1\}$ та $r < m - 1$ для $p = 2$;
- 2) якщо a є одиницею в R , тоді $m \geq n + r \geq 2r$, $L = \langle ap \rangle + \langle b \rangle$ та $R^* = \{ax_1 + bx_2 \mid x_1 \not\equiv 0 \pmod{p}\}$;
- 3) якщо b є одиницею в R , тоді $p = 2 < m \leq n$, $r = 1$, $L = \langle a \rangle + \langle b2 \rangle$ та $R^* = \{ax_1 + bx_2 \mid x_2 \equiv 1 \pmod{2}\}$.

Доведення. Це випливає з наслідків 3.22, що $R^+ = \langle a \rangle + \langle b \rangle$ для деяких елементів a та b , один з яких співпадає з одиницею в R , а, отже, виконується твердження 1) теореми.

Якщо a є одиницею в R , то $m \geq n + r \geq 2r$ за лемою 3.26. Зокрема, $m > n$ і тому $b \in L$ за лемою 3.10. Тому $L = \langle ap \rangle + \langle b \rangle$. Оскільки $R^* = R \setminus L$, елемент $x = ax_1 + bx_2$ належить R^* тоді і тільки тоді, коли $x_1 \not\equiv 0 \pmod{p}$.

Аналогічно, якщо b є одиницею в R , тоді з лем 3.24 та 3.27 випливає, що $a \in L$, $p = 2 < m \leq n$ і $r = 1$. Звідси $L = \langle a \rangle + \langle b2 \rangle$ і тому елемент $x = ax_1 + bx_2$ належить R^* тоді і тільки тоді, коли $x_2 \equiv 1 \pmod{2}$. $\square$

Застосовуючи зараз твердження 2) і 3) теореми 3.30 до лем 3.26 і 3.27, відповідно, отримуємо наступні формули множення будь-яких двох елементів $x = ax_1 + bx_2$ та $y = ay_1 + by_2$ в локальному майже-кільці R , адитивна група якого ізоморфна $G(p^m, p^n, r)$.

Наслідок 3.31. Якщо a є одиницею в R і $xb = a\alpha(x) + b\beta(x)$, то $m \geq n + r \geq 2r$ і

$$xy = a(x_1y_1 + \alpha(x)y_2 - x_1x_2\binom{y_1}{2}p^{m-r}) + b(x_2y_1 + \beta(x)y_2)$$

з коефіцієнтами $\alpha(x)$ та $\beta(x)$, що задовольняють наступні умови:

(0) $\alpha(0) = \beta(0) = 0$ тоді і тільки тоді, коли майже-кільце R є нуль-симетричним;

(1) $\alpha(a) = 0$ і $\beta(a) = 1$;

(2) $\alpha(x) \equiv 0 \pmod{p^{m-n}}$;

(3) $x_1(\beta(x) - 1) \equiv 0 \pmod{p^r}$;

(4) $\alpha(xy) = x_1\alpha(y) + \alpha(x)\beta(y) - x_1x_2\binom{\alpha(y)}{2}p^{m-r}$;

(5) $\beta(xy) = x_2\alpha(y) + \beta(x)\beta(y)$.

Наслідок 3.32. Якщо b є одиницею в R і $xa = a\alpha(x) + b\beta(x)$, то $p = 2 < m \leq n$, $r = 1$ та

$$xy = a[\alpha(x)y_1 + x_1j(t^{x_2}, y_2)] + b(\beta(x)y_1 + x_2y_2)$$

з коефіцієнтами $\alpha(x)$ та $\beta(x)$, що задовольняють наступні умови:

(0) $\alpha(0) = \beta(0) = 0$;

(1) $\alpha(b) = 1$ and $\beta(b) = 0$;

(2) $\beta(x) \equiv 0 \pmod{2^{n-m+1}}$;

(3) $\alpha(x)(1 - x_2) \equiv 0 \pmod{2}$;

(4) $\alpha(xy) = \alpha(x)\alpha(y) + x_1j(t^{x_2}, \beta(y))$;

(5) $\beta(xy) = \beta(x)\alpha(y) + x_2\beta(y)$.

Теорема 3.33. *Нехай R є локальним майже-кільцем, адитивна група якого R^+ ізоморфна групі $G(2^m, 2^n, -r)$. Тоді $R^+ = \langle a \rangle + \langle b \rangle$, елемент b є одиницею в R і виконуються наступні твердження:*

- 1) $2 < m \leq n$ та $r = 1$;
- 2) $a2^m = b2^n = 0$ та $a + b = b + a(-1 + 2^{m-1})$;
- 3) $L = \langle a \rangle + \langle b2 \rangle$ та $R^* = \{ax_1 + bx_2 \mid x_2 \equiv 1 \pmod{2}\}$.

Доведення. Як і в доведенні теореми 3.30, це випливає з наслідку 3.22 що існує розкладання $R^+ = \langle a \rangle + \langle b \rangle$ в якому один з елементів a або b співпадає з одиницею R та твердженням 2) теореми має місце. Однак, якщо a є одиницею в R , тоді група R^+ є дієдральною порядку 8 за лемою 3.28 і тому вона не може бути адитивною групою локального майже-кільця за [64]. Отже, елемент b є одиницею R . Тоді $2 < m \leq n$ і $r = 1$ за лемою 3.29 та $a \in L$ за лемою 3.24. Тому $L = \langle a \rangle + \langle b2 \rangle$ за лемою 3.10 і, отже,

$$R^* = \{ax_1 + bx_2 \mid x_2 \equiv 1 \pmod{2}\},$$

як стверджувалося. □

Як наслідок лем 3.25, 3.29 і теореми 3.33, маємо таку формулу для множення будь-яких двох елементів у локальному майже-кільці R , адитивна група якого ізоморфна $G(2^m, 2^n, -r)$.

Наслідок 3.34. *Якщо $x = ax_1 + bx_2$ і $y = ay_1 + by_2$ є елементами в R , то*

$$xy = a[\alpha(x)y_1 + x_1j(t^{x_2}, y_2)] + b(\beta(x)y_1 + x_2y_2)$$

з коефіцієнтами $\alpha(x)$ і $\beta(x)$ задовольняють наступні умови:

- (0) $\alpha(0) = \beta(0) = 0$;
- (1) $\alpha(b) = 1$ і $\beta(b) = 0$;

$$(2) \beta(x) \equiv 0 \pmod{2^{n-1}};$$

$$(3) \alpha(xy) = \begin{cases} \alpha(x)\alpha(y) + x_1\beta(y), & \text{якщо } m = n \text{ та } x_2 \equiv 0 \pmod{2}, \text{ та} \\ \alpha(x)\alpha(y), & \text{інакше;} \end{cases}$$

$$(4) \beta(xy) = \beta(x)\alpha(y) + x_2\beta(y).$$

3.2.7. Групи $G(p^m, p^n, r)$ як адитивні групи локальних майже-кілець

Наступна теорема дає достатні умови для існування скінченних локальних майже-кілець, адитивна група яких ізоморфна групі $G(p^m, p^n, r)$. Разом з теоремами 3.30 та 3.33 це завершує нашу класифікацію всіх розщеплюваних метациклічних груп, які є адитивними групами локальних майже-кілець.

Теорема 3.35. *Для кожного простого числа p та таких додатніх цілих m, n , що або $m \geq n + r \geq 2r + \lfloor \frac{2}{p} \rfloor$, або $p = 2$, $2 < m \leq n$ та $r = 1$ існує локальне майже-кілець R , адитивна група якого R^+ ізоморфна групі $G(p^m, p^n, r)$.*

Доведення. Нехай G — адитивно записана група $G(p^m, p^n, r)$ з твірними a, b які задовольняють співвідношення $ap^m = 0, bp^n = 0, a + b = b + a(1 + p^{m-r})$. Тоді $G = \langle a \rangle + \langle b \rangle$ і кожен елемент $x \in G$ однозначно записується у вигляді $x = ax_1 + bx_2$ з коефіцієнтами $x_1 \in Z_{p^m}$ і $x_2 \in Z_{p^n}$. Щоб визначити множення “ $\cdot$ ” на G таке, що система $R = (G, +, \cdot)$ є локальним майже-кілецем.

I. Почнемо з випадку $m \geq n + r \geq 2r$, де для довільних елементів $x = ax_1 + bx_2$ і $y = ay_1 + by_2$ групи G визначимо множення $x \cdot y$ за правилом

$$x \cdot y = a(x_1y_1 - x_1x_2 \binom{y_1}{2} p^{m-r}) + b(x_2y_1 + \beta(x)y_2),$$

$$\text{де } \beta(x) = \begin{cases} 1, & x_1 \not\equiv 0 \pmod{p}; \\ 0, & x_1 \equiv 0 \pmod{p}. \end{cases}$$

Легко побачити, що елемент a є мультиплікативною одиницею для $(G, \cdot)$ і $xb = b\beta(x)$ для кожного $x \in G$. Покажемо, що стосовно операцій “+” і “ $\cdot$ ” система $(G, +, \cdot)$ є майже-кільцем з одиничним елементом a . Очевидно, що достатньо перевірити, що якщо $x \cdot (y + z) = x \cdot y + x \cdot z$ є довільним елементом $z = az_1 + bz_2$ в R і $(x \cdot y) \cdot b = x \cdot (y \cdot b)$.

Дійсно, за означенням множення маємо

$$x \cdot z = a(x_1z_1 - x_1x_2 \binom{z_1}{2} p^{m-r}) + b(x_2z_1 + \beta(x)z_2).$$

За лемами 3.16 і 3.18,

$$\begin{aligned} & b[x_2y_1 + \beta(x)y_2] + a[x_1z_1 - x_1x_2 \binom{z_1}{2} p^{m-r}] \\ &= a[(1 + (x_2y_1 + \beta(x)y_2)hp^{m-r})(x_1z_1 - x_1x_2 \binom{z_1}{2} p^{m-r})] \\ & \quad + b[x_2y_1 + \beta(x)y_2]. \end{aligned}$$

Тому

$$\begin{aligned} x \cdot y + x \cdot z &= a[x_1y_1 + x_1z_1 - x_1x_2 \binom{y_1}{2} p^{m-r} - x_1x_2 \binom{z_1}{2} p^{m-r} \\ & \quad + x_1x_2y_1z_1hp^{m-r} + x_1\beta(x)y_2z_1hp^{m-r}] \\ & \quad + b[x_2y_1 + x_2z_1 + \beta(x)y_2 + \beta(x)z_2]. \end{aligned}$$

З іншого боку,

$$\begin{aligned} y + z &= (ay_1 + by_2) + (az_1 + bz_2) = \\ &= a(y_1 + z_1 + y_2z_1hp^{m-r}) + b(y_2 + z_2), \end{aligned}$$

тому що

$$by_2 + az_1 = a(1 + y_2hp^{m-r})z_1 + by_2$$

за лемою 3.18. За означенням множення маємо

$$\begin{aligned} x \cdot (y + z) &= a[x_1(y_1 + z_1 + y_2 z_1 h p^{m-r}) \\ &\quad - x_1 x_2 \binom{y_1 + z_1 + y_2 z_1 h p^{m-r}}{2} p^{m-r}] + \\ &\quad + b[x_2(y_1 + z_1) + \beta(x)(y_2 + z_2)]. \end{aligned}$$

Як показано вгорі, рівності

$$x_1 \beta(x) y_2 z_1 h p^{m-r} = x_1 y_2 z_1 h p^{m-r}$$

і твердження (2) леми 3.26, отримуємо $x \cdot (y + z) = x \cdot y + x \cdot z$, як вимагалось.

Далі, $y \cdot b = b\beta(y)$, і, отже,

$$x \cdot (y \cdot b) = (x \cdot b)\beta(y) = b\beta(x)\beta(y).$$

Оскільки $\beta(x \cdot y) = b\beta(x)\beta(y)$ для всіх $x, y \in G$, випливає, що

$$(x \cdot y) \cdot b = b\beta(x \cdot y) = b\beta(x)\beta(y) = x \cdot (y \cdot b).$$

Тому щодо операцій “+” і “.” система $R = (G, +, \cdot)$ є майже-кільцем з одиничним елементом a .

Нарешті покажемо, що $R = (G, +, \cdot)$ є локальним майже-кільцем, у якому підгрупа $L = \langle ap \rangle + \langle b \rangle$ складається з усіх необоротних елементів з R . Очевидно, що достатньо довести, що елемент $x = ax_1 + bx_2$ оборотний справа тоді і тільки тоді, коли $x_1 \not\equiv 0 \pmod{p}$, оскільки в цьому випадку множина $R \setminus L$ збігається з мультиплікативною групою R^* за лемою 3.13.

Дійсно, якщо x оборотний справа, то існує такий елемент $y = ay_1 + by_2$, що $x \cdot y = a$. З нашого визначення

$$x_1 y_1 - x_1 x_2 \binom{y_1}{2} p^{m-r} \equiv 1 \pmod{p^m}.$$

Але тоді $x_1 y_1 \equiv 1 \pmod{p}$, звідси $x_1 \not\equiv 0 \pmod{p}$.

І навпаки, якщо останнє виконується, то $\beta(x) \equiv 1 \pmod{p}$ за умовою (3) наслідку 3.31, тому існують такі натуральні числа y_1, y_2 , що $x_1 y_1 \equiv 1 \pmod{p^m}$ і

$$x_2 y_1 + \beta(x) y_2 \equiv 0 \pmod{p^n}.$$

Поклавши $y = ay_1 + by_2$ і

$$z_1 = 1 - x_1 x_2 \binom{y_1}{2} p^{m-r},$$

за означенням множення маємо $x \cdot y = az_1$. Тоді існує таке натуральне число s , що $z_1 s \equiv 1 \pmod{p^m}$, звідси

$$x \cdot (ys) = (x \cdot y)s = (az_1)s = a.$$

Таким чином, елемент x оборотний справа, а отже, майже-кільце R є локальним.

II. Розглянемо тепер випадок $p = 2$, $2 < m \leq n$ і $r = 1$, де для довільних елементів $x = ax_1 + bx_2$ і $y = ay_1 + by_2$ в G визначаємо множення $x \cdot y$ за правилом

$$x \cdot y = a(\alpha(x)y_1 + x_1 j(t^{x_2}, y_2)) + b(x_2 y_2),$$

$$\text{де } \alpha(x) = \begin{cases} 1, & x_1 \not\equiv 0 \pmod{2}; \\ 0, & x_1 \equiv 0 \pmod{2}. \end{cases}$$

Легко побачити, що елемент b є мультиплікативною одиницею в $(G, \cdot)$ і $xa = a\alpha(x)$ для кожного $x \in G$. Покажемо, що стосовно операцій “+” and “ $\cdot$ ” система $(G, +, \cdot)$ є майже-кільцем з одиничним елементом b . Очевидно, що достатньо перевірити, що $x \cdot (y + z) = x \cdot y + x \cdot z$ для довільного $z = az_1 + bz_2$ з R і $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.

Дійсно, маємо

$$x \cdot z = a(\alpha(x)z_1 + x_1 z_2 + x_1 x_2 \binom{z_2}{2} h 2^{m-r}) + b(x_2 z_2)$$

за означенням і

$$\begin{aligned} & b[x_2y_2] + a[\alpha(x)z_1 + x_1z_2 + x_1x_2\binom{z_2}{2}h2^{m-r}] \\ &= a[(1 + x_2y_2h2^{m-r})(\alpha(x)z_1 + x_1z_2 + \\ & \quad + x_1x_2\binom{z_2}{2}h2^{m-r})] + b(x_2y_2) \end{aligned}$$

за лемами 3.16 і 3.18. Отже,

$$\begin{aligned} x \cdot y + x \cdot z &= a[\alpha(x)(y_1 + z_1) + \\ & \quad + x_1(y_2 + z_2) + (x_1x_2\binom{y_2}{2} + x_1x_2\binom{z_2}{2} \\ & \quad + x_2y_2\alpha(x)z_1 + x_1x_2y_2z_2)h2^{m-r}] + b(x_2(y_2 + z_2)). \end{aligned}$$

З іншого боку,

$$y + z = a(y_1 + z_1 + y_2z_1h2^{m-1}) + b(y_2 + z_2)$$

і, отже,

$$\begin{aligned} x \cdot (y + z) &= a[\alpha(x)(y_1 + z_1 + y_2z_1h2^{m-1}) + x_1(y_2 + z_2) \\ & \quad + x_1x_2\binom{y_2 + z_2}{2}h2^{m-1}] + b[x_2(y_2 + z_2)]. \end{aligned}$$

Тому

$$\begin{aligned} & -x \cdot (y + z) + x \cdot y + x \cdot z \\ &= -b[x_2(y_2 + z_2)] + a[(\alpha(x)(y_1 + z_1 + y_2z_1h2^{m-1}) \\ & \quad + x_1(y_2 + z_2) + x_1x_2\binom{y_2 + z_2}{2}h2^{m-1}) \\ & \quad + a[\alpha(x)(y_1 + z_1) + x_1(y_2 + z_2) + (x_1x_2\binom{y_2}{2} + x_1x_2\binom{z_2}{2} \\ & \quad + x_2y_2\alpha(x)z_1 + x_1x_2y_2z_2)h2^{m-r}] + b(x_2(y_2 + z_2)). \end{aligned}$$

Так як за нашою умовою

$$a\alpha(x)(1 - x_2)y_2z_2h2^{m-r} = 0$$

випливає, що

$$-x \cdot (y + z) + x \cdot y + x \cdot z = 0$$

як вимагалось.

Далі,

$$\begin{aligned} (x \cdot y) \cdot z &= a(\alpha(x \cdot y)z_1 + (\alpha(x)y_1 + \\ &\quad + x_1y_2 + x_1x_2 \binom{y_2}{2} h2^{m-r})z_2 \\ &\quad + (\alpha(x)y_1 + x_1y_2 + x_1x_2 \binom{y_2}{2} h2^{m-r})x_2y_2 \binom{z_2}{2} h2^{m-r}) \\ &\quad + b(x_2y_2z_2) = a(\alpha(x \cdot y)z_1 + \alpha(x)y_1z_2 + x_1y_2z_2 \\ &\quad + x_1x_2 \binom{y_2}{2} z_2 h2^{m-r} + (x_2\alpha(x)y_1y_2 + x_1x_2y_2^2 \\ &\quad + x_1x_2^2y_2 \binom{y_2}{2} h2^{m-r}) \binom{z_2}{2} h2^{m-r} + b(x_2y_2z_2)) \\ &= a(\alpha(x \cdot y)z_1 + \alpha(x)y_1z_2 + x_1y_2z_2 + x_1x_2 \binom{y_2}{2} z_2 h2^{m-r} \\ &\quad + x_2\alpha(x)y_1y_2 \binom{z_2}{2} h2^{m-r} + x_1x_2y_2^2 \binom{z_2}{2} h2^{m-r} + b(x_2y_2z_2)). \end{aligned}$$

З іншого боку,

$$\begin{aligned} x \cdot (y \cdot z) &= a(\alpha(x)(\alpha(y)z_1 + y_1z_2 + y_1y_2 \binom{z_2}{2} h2^{m-r} + x_1y_2z_2 \\ &\quad + x_1x_2 \binom{y_2z_2}{2} h2^{m-r}) + b(x_2y_2z_2)) \\ &= a(\alpha(x)\alpha(y)z_1 + \alpha(x)y_1z_2 + \alpha(x)y_1y_2 \binom{z_2}{2} h2^{m-r} + x_1y_2z_2 \\ &\quad + x_1x_2 \binom{y_2z_2}{2} h2^{m-r} + b(x_2y_2z_2)). \end{aligned}$$

Отже, $x \cdot (y \cdot z) = (x \cdot y) \cdot z$. Тому $(R, +, \cdot)$ є майже-кільцем з одиничним елементом b .

Для завершення доведення залишається показати, що множина всіх необоротних елементів $(R, +, \cdot)$ збігається з $L = \langle a \rangle + \langle b2 \rangle$. Як і в попередньому випадку, достатньо довести, що елемент $x = ax_1 + bx_2$ оборотний справа тоді і тільки тоді, коли $x_2 \equiv 1 \pmod{2}$.

Справді, якщо існує такий елемент $y = ay_1 + by_2$, що $x \cdot y = b$, то $x_2y_2 \equiv 1 \pmod{2^n}$ за нашим означенням $x \cdot y$. Звідки $x_2 \equiv 1 \pmod{2}$.

І навпаки, якщо виконується остання конгруенція, то $\alpha(x) \equiv 1 \pmod{2}$, тому існують такі натуральні числа y_1, y_2 , що $x_2y_2 \equiv 1 \pmod{2}$ і

$$\alpha(x)y_1 + x_1y_2 \equiv 0 \pmod{2^m}.$$

Але тоді $x \cdot y = b$ і тому елемент x оборотний справа. Отже, майже-кілеце R є локальним, і це завершує доведення. $\square$

3.3. Локальні майже-кілеця на групах типу (B.1)

Доведено, що кожна неметациклічна p -група Міллера–Морено порядку $p^n > 8$ є адитивною групою локального майже-кілеця, а мультиплікативна група такого майже-кілеця є групою порядку $p^{n-1}(p-1)$ [7]. У цьому підрозділі досліджуються скінченні неабелеві неметациклічні 2-породжені p -групи ($p > 2$) класу нільпотентності 2 з циклічною комутаторною підгрупою.

3.3.1. Допоміжні результати

Нехай G — група типу (B.1) з теореми 3.1. Тоді G — скінченна неабелева неметациклічна 2-породжена p -група ($p > 2$) класу нільпотентності 2 з циклічною комутаторною підгрупою.

Позначимо через G' та $Z(G)$ комутаторну підгрупу та центр G , відповідно.

Нехай a та b будуть твірними для G такими, що $G/G' = \langle aG' \rangle \times \langle bG' \rangle$, aG' має порядок p^m та bG' має порядок p^n . Тоді $c = [a, b]$ породжує G' , c має порядок p^d з $1 \leq d \leq n \leq m$, та

$$c \in Z(G) = \langle a^{p^m}, b^{p^n}, c \rangle.$$

Припустимо, що $\langle a \rangle \cap G' = \langle b \rangle \cap G' = 1$. Тоді

$$G = \langle a, b, c \mid a^{p^m} = b^{p^n} = c^{p^d} = 1, a^b = ac, c^a = c^b = c \rangle$$

і кожен елемент G можна однозначно записати у вигляді $a^{x_1}b^{x_2}c^{x_3}$, $x_1 \in C_{p^m}$, $x_2 \in C_{p^n}$, $x_3 \in C_{p^d}$. Тому групу G з $p > 2$ позначатимемо як $G(p^m, p^n, p^d)$.

Лема 3.36. *Для будь-яких натуральних чисел k та l виконується рівність $[a^k, b^l] = c^{kl}$.*

Доведення. Оскільки $b^{-1}ab = ac$, то $b^{-l}ab^l = ac^l$. Отже,

$$b^{-l}a^kb^l = (ac^l)^k = a^kc^{kl},$$

а тому $a^{-k}b^{-l}a^kb^l = c^{kl}$. □

Наслідок 3.37. *Нехай група $G(p^m, p^n, p^d)$ є адитивно записаною. Тоді для будь-яких натуральних чисел k та l виконуються рівності*

$$-ak - bl + ak + bl = c(kl) \text{ та } bl + ak = -c(kl) + ak + bl.$$

Лема 3.38. *Для будь-яких натуральних чисел k , l та r виконується рівність*

$$(a^kb^l)^r = a^{kr}b^{lr}c^{-kl\binom{r}{2}} \quad (3.25)$$

Доведення. Для $r = 1$ нічого доводити. Індукцією по r отримуємо

$$(a^k b^l)^r = a^{kr} b^{lr} c^{-kl \binom{r}{2}}.$$

Замінивши r на $r + 1$ у рівності (3.25), маємо

$$\begin{aligned} (a^k b^l)^{(r+1)} &= a^{kr} b^{lr} a^k b^l c^{-kl \binom{r}{2}} = \\ &= a^{k(r+1)} b^{l(r+1)} c^{-klr} c^{-kl \binom{r}{2}} \\ &= a^{k(r+1)} b^{l(r+1)} c^{-kl(r + \binom{r}{2})} = a^{k(r+1)} b^{l(r+1)} c^{kl \binom{r+1}{2}}. \end{aligned}$$

Отже, рівність (3.25) виконується для довільного r . □

Наслідок 3.39. *Нехай група $G(p^m, p^n, p^d)$ є адитивно записаною. Тоді для будь-яких натуральних чисел k, l та r виконується рівність*

$$(ak + bl)r = akr + blr - ckl \binom{r}{2}.$$

Очевидно, що експонента групи $G(p^m, p^n, p^d)$ дорівнює p^m для $1 \leq d \leq n \leq m$.

Лема 3.40. *Якщо x — елемент порядку p^m групи $G(p^m, p^n, p^d)$, то існують такі твірні a, b, c цієї групи, що $a = x$ та $a^{p^m} = b^{p^n} = c^{p^d} = 1$, $a^b = ac$, $c^a = c^b = c$.*

Доведення. Дійсно, для кожного $x \in G(p^m, p^n, p^d)$ існують такі додатні цілі числа α, β та γ , що $x = a^\alpha b^\beta c^\gamma$. Таким чином, маємо

$$\begin{aligned} x^{p^m} &= (a^\alpha b^\beta c^\gamma)^{p^m} = (a^\alpha b^\beta)^{p^m} c^{\gamma p^m} = \\ &= a^{\alpha p^m} b^{\beta p^m} c^{\gamma p^m - \alpha \beta \binom{p^m}{2}} = \\ &= a^{p^m \alpha} b^{p^m \beta} c^{p^m(\gamma - \alpha \beta \frac{p^m - 1}{2})} = 1 \end{aligned}$$

за лемою 3.38. Оскільки $|a| = p^m$ та $1 \leq d \leq n \leq m$, де $m > 1$ та $p > 2$, то експонента групи $G(p^m, p^n, p^d)$ дорівнює p^m .

Якщо

$$x^{p^{m-1}} = a^{p^{m-1}\alpha} b^{p^{m-1}\beta} c^{p^{m-1}(\gamma - \alpha\beta \frac{p^{m-1}-1}{2})} \neq 1,$$

тоді або $(\alpha, p) = 1$, або $(\beta, p) = 1$ для $m = n$, або $(\gamma, p) = 1$ для $m = n = d$. Отже, без обмеження загальності, можна вважати, що $(\alpha, p) = 1$. Тоді

$$\langle x, b \rangle = \langle a^\alpha b^\beta c^\gamma, b \rangle = \langle a^\alpha, b \rangle = \langle a, b \rangle = G$$

і

$$b^{-1}xb = b^{-1}(a^\alpha b^\beta c^\gamma)b = (ac)^\alpha b^\beta c^\gamma = (a^\alpha b^\beta c^\gamma)c^\alpha = xc^\alpha.$$

Крім того, підставляючи c^α замість c для твірних x та b групи $G(p^m, p^n, p^d)$, ми маємо подібні вирази, як і для твірних a та b , таким чином замінюючи елемент a на x . $\square$

Наступне твердження щодо групи автоморфізмів $G(p^m, p^n, p^d)$ є прямим наслідком твердження (B1) [66].

Лема 3.41. *Нехай $G = G(p^m, p^n, p^d)$ та $\text{Aut}(G)$ — група автоморфізмів G . Тоді виконуються такі твердження:*

- 1) *якщо $m = n$, то $|\text{Aut}(G)| = p^{2d+4m-5}(p^2 - 1)(p - 1)$;*
- 2) *якщо $m > n$, то $|\text{Aut}(G)| = p^{2d+3n+m-2}(p - 1)^2$.*

Інформацію про групу автоморфізмів $G(p^m, p^m, p^d)$ дає наступна лема.

Лема 3.42. *Нехай $G = G(p^m, p^m, p^d)$ і існує підгрупа A групи $\text{Aut}(G)$ порядку $p^{2m+d-2}(p^2 - 1)$, де $m, d > 1$ з непарним p . Якщо елемент $g \in G$ порядку p^m та A містить силовську нормальну p -підгрупу, то $G \neq g^A \cup \Phi(G)$.*

Доведення. Припустимо, що $G = g^A \cup \Phi(G)$. Тоді $G = (\langle a \rangle \times \langle c \rangle) \rtimes \langle b \rangle$ з твірними a, b порядку p^m та центральним комутатором $c = [a, b]$ порядку p^d за визначенням. Отже,

$$\Phi(G) = (\langle a^p \rangle \times \langle c \rangle) \rtimes \langle b^p \rangle,$$

і таким чином усі елементи порядку p^m містяться в g^A . Крім того, $a = g^u$ для деякого $u \in A$, отже $g^A = a^A$, тобто $G = a^A \cup \Phi(G)$. Оскільки $|G| = p^{2m+d}$ та $|\Phi(G)| = p^{2m+d-2}$, то випливає, що

$$|a^A| = |G| - |\Phi(G)| = p^{2m+d-2}(p^2 - 1),$$

і тому централізатор $C_A(a)$ для a в A дорівнює 1. Зокрема,

$$(a\langle c^p \rangle)^A = (a\langle c^p \rangle)^B = a\langle c^p \rangle$$

для нормальної підгрупи $B = C_A(a\langle c^p \rangle)$ порядку p^{d-1} в A .

Враховуючи фактор-групу $\bar{G} = G/\langle c^p \rangle$ і $\bar{A} = A/B$. Беручи до уваги, що

$$|\bar{a}^{\bar{A}}| = p^{2m-1}(p^2 - 1),$$

маємо

$$\bar{G} = \bar{a}^{\bar{A}} \cup \Phi(\bar{G}).$$

Оскільки $|\Phi(\bar{G})| = |Z(\bar{G})|$ та $xy = yx$ для всіх $x \in \Phi(\bar{G})$, $y \in \bar{G}$, маємо $\Phi(\bar{G}) = Z(\bar{G})$. Отже, $\bar{G}$ є групою Міллера–Морено. Оскільки $\bar{G} = \bar{a}^{\bar{A}} \cup Z(\bar{G})$, остання рівність неможлива згідно з [7, Лема 7]. Ця суперечність завершує доведення. $\square$

3.3.2. Майже-кільця з одиницею на групі $G(p^m, p^n, p^d)$

Наступне твердження є загальновідомим.

Лема 3.43. *Нехай R — скінченне майже-кільце з одиницею i . Тоді експонента R^+ дорівнює адитивному порядку i , який збігається з адитивним порядком кожного елемента R^* .*

Як прямий наслідок лем 3.40 та 3.43 маємо наступний наслідок.

Наслідок 3.44. *Нехай R — майже-кільце з одиницею i , група якого R^+ ізоморфна групі $G(p^m, p^n, p^d)$. Тоді $R^+ = \langle a \rangle + \langle b \rangle + \langle c \rangle$ з елементами a, b та c , що задовольняють співвідношення $ap^m = bp^n = cp^d = 0$, $-b + a + b = a + c$ та $-a + c + a = -b + c + b = c$ з $1 \leq d \leq n \leq m$, де $a = i$.*

Наступне твердження [9, Lemma 1] встановлює зв'язок між групою автоморфізмів адитивної групи майже-кільця з одиницею та її мультиплікативною групою.

Лема 3.45. *Нехай R — майже-кільце з одиницею i . Тоді існує підгрупа A групи автоморфізмів $\text{Aut}(R^+)$, яка ізоморфна R^* та задовольняє умову*

$$i^A = \{i^a \mid a \in A\} = R^*.$$

Підгрупа A , визначена в лемі 3.45, називається групою автоморфізмів групи R^+ , пов'язаної з групою R^* .

Наступне твердження [114, Theorem 54] стосується структури L , яка є підгрупою всіх необоротних елементів скінченного локального майже-кільця R . Нехай $\Phi(G)$ позначає підгрупу Фраттіні G .

Теорема 3.46. *Нехай R — локальне майже-кільце порядку p^n , а $G(R) = R^+ \rtimes R^*$ — група, асоційована з R . Тоді $H = R^+ \rtimes (i + L)$ — це силовська нормальна p -підгрупа $G(R)$, а $L = R^+ \cap \Phi(H)$. Зокрема, якщо L неабелева, то її центр нециклічний.*

Враховуючи $\Phi(R^+) \leq \Phi(H)$, маємо наступний наслідок.

Наслідок 3.47. $\Phi(R^+) \leq L = \Phi(H) \cap R^+$.

Нехай R — майже-кільце з одиницею i , група R^+ якого ізоморфна групі $G(p^m, p^n, p^d)$. З наслідку 3.44 випливає, що $R^+ = \langle a \rangle + \langle b \rangle + \langle c \rangle$ з елементами a, b та c , що задовольняють співвідношення $ap^m = bp^n = cp^d = 0$, $-b + a + b = a + c$ та $-a + c + a = -b + c + b = c$ з $1 \leq$

$d \leq n \leq m$, де $a = i$ та кожен елемент $x \in R$ однозначно записується у вигляді $x = ax_1 + bx_2 + cx_3$ з коефіцієнтами $0 \leq x_1 < p^m$, $0 \leq x_2 < p^n$ і $0 \leq x_3 < p^d$.

Крім того, можна припустити, що $xa = ax = x$ для кожного $x \in R$. Тоді існують такі однозначно визначені відображення $\alpha: R \rightarrow \mathbb{Z}_{p^m}$, $\beta: R \rightarrow \mathbb{Z}_{p^n}$ та $\gamma: R \rightarrow \mathbb{Z}_{p^d}$, що

$$xb = a\alpha(x) + b\beta(x) + c\gamma(x). \quad (3.26)$$

Лема 3.48. *Якщо $x = ax_1 + bx_2 + cx_3$ і $y = ay_1 + by_2 + cy_3$ є довільними елементами R , то*

$$\begin{aligned} xy &= a(x_1y_1 + y_2\alpha(x)) + b(x_2y_1 + y_2\beta(x)) + \\ &+ c(-x_1x_2\binom{y_1}{2} - \binom{y_2}{2}\alpha(x)\beta(x) - x_2y_1y_2\alpha(x) + \\ &+ x_3y_1 + y_2\gamma(x) + x_1y_3\beta(x) - x_2y_3\alpha(x)), \end{aligned}$$

де відображення $\alpha: R \rightarrow \mathbb{Z}_{p^m}$, $\beta: R \rightarrow \mathbb{Z}_{p^n}$ і $\gamma: R \rightarrow \mathbb{Z}_{p^d}$ задовольняють умови:

(0) $\alpha(0) \equiv 0 \pmod{p^m}$, $\beta(0) \equiv 0 \pmod{p^n}$ і $\gamma(0) \equiv 0 \pmod{p^d}$ тоді і тільки тоді, коли майже-кільце R є нуль-симетричним;

(1) $\alpha(xy) \equiv x_1\alpha(y) + \alpha(x)\beta(y) \pmod{p^m}$;

(2) $\beta(xy) \equiv x_2\alpha(y) + \beta(x)\beta(y) \pmod{p^n}$;

(3) $\gamma(xy) \equiv -x_1x_2\binom{\alpha(y)}{2} - \alpha(x)\beta(x)\binom{\beta(y)}{2} - x_2\alpha(x)\alpha(y)\beta(y) + x_3\alpha(y) + \gamma(x)\beta(y) + x_1\beta(x)\gamma(y) - x_2\alpha(x)\gamma(y) \pmod{p^d}$.

Доведення. Якщо R — нуль-симетричне майже-кільце, то

$$0 = 0 \cdot b = a\alpha(0) + b\beta(0) + c\gamma(0),$$

таким чином $\alpha(0) \equiv 0 \pmod{p^m}$, $\beta(0) \equiv 0 \pmod{p^n}$ та $\gamma(0) \equiv 0 \pmod{p^d}$.
З іншого боку, якщо останні конгруенції виконуються, то

$$0 \cdot b = a \cdot 0 + b \cdot 0 + c \cdot 0 = 0.$$

Оскільки a є мультиплікативною одиницею в R , маємо $0 \cdot a = a \cdot 0 = 0$.
Більш того, з рівності $c = -a - b + a + b$ та лівого дистрибутивного закону випливає, що

$$0 \cdot c = -0 \cdot a - 0 \cdot b + 0 \cdot a + 0 \cdot b = 0,$$

отже,

$$0 \cdot x = 0 \cdot (ax_1 + bx_2 + cx_3) = (0 \cdot a)x_1 + (0 \cdot b)x_2 + (0 \cdot c)x_3 = 0.$$

Це доводить твердження (0).

Далі, використовуючи (3.26) та наслідок 3.37, отримуємо

$$\begin{aligned} xc &= -xa - xb + xa + xb = -cx_3 - bx_2 - ax_1 - \\ &\quad -c\gamma(x) - b\beta(x) - a\alpha(x) \\ &\quad + ax_1 + bx_2 + cx_3 + a\alpha(x) + b\beta(x) + c\gamma(x) \\ &= -bx_2 - ax_1 - b\beta(x) - a\alpha(x) + ax_1 + bx_2 + a\alpha(x) + b\beta(x) \\ &= -bx_2 + cx_1\beta(x) - b\beta(x) - ax_1 - \\ &\quad -a(\alpha(x) - x_1) + bx_2 + a\alpha(x) + b\beta(x) \\ &= cx_1\beta(x) - b(x_2 + \beta(x)) - a\alpha(x) + bx_2 + \\ &\quad + a\alpha(x) + b\beta(x) = cx_1\beta(x) - b(x_2 + \beta(x)) - \\ &\quad -a\alpha(x) - cx_2\alpha(x) + a\alpha(x) + bx_2 + b\beta(x) \\ &= c(x_1\beta(x) - x_2\alpha(x)) - b(x_2 + \beta(x)) + \\ &\quad + bx_2 + b\beta(x) = c(x_1\beta(x) - x_2\alpha(x)). \end{aligned}$$

Тому

$$xy = (ax_1 + bx_2 + cx_3)y_1 + (a\alpha(x) + b\beta(x) + c\gamma(x))y_2 + (cx_1\beta(x) - x_2\alpha(x))y_3.$$

За наслідком 3.39, маємо

$$\begin{aligned} (ax_1 + bx_2)y_1 &= ax_1y_1 + bx_2y_1 - cx_1x_2\binom{y_1}{2}, \\ (a\alpha(x) + b\beta(x))y_2 &= ay_2\alpha(x) + \\ &+ by_2\beta(x) - c\binom{y_2}{2}\alpha(x)\beta(x) \end{aligned}$$

і

$$bx_2y_1 + ay_2\alpha(x) = ay_2\alpha(x) + bx_2y_1 - cx_2y_1y_2\alpha(x).$$

Згідно з лівим дистрибутивним законом, маємо

$$\begin{aligned} xy &= a(x_1y_1 + y_2\alpha(x)) + b(x_2y_1 + y_2\beta(x)) + \\ &+ c(-x_1x_2\binom{y_1}{2} - \binom{y_2}{2}\alpha(x)\beta(x) - x_2y_1y_2\alpha(x) + \\ &+ x_3y_1 + y_2\gamma(x) + x_1y_3\beta(x) - x_2y_3\alpha(x)). \end{aligned}$$

Зрештою, асоціативність множення для всіх $x, y \in R$ означає, що

$$(xy)b = x(yb). \quad (3.27)$$

Таким чином,

$$(xy)b = a\alpha(xy) + b\beta(xy) + c\gamma(xy) \quad (3.28)$$

і $yb = a\alpha(y) + b\beta(y) + c\gamma(y)$ за формулою (3.26). Підставляючи останній вираз у праву частину рівності (3.27), отримуємо

$$\begin{aligned} x(yb) &= a(x_1\alpha(y) + \alpha(x)\beta(y)) + b(x_2\alpha(y) + \\ &+ \beta(x)\beta(y)) + c(-x_1x_2\binom{\alpha(y)}{2} - \alpha(x)\beta(x)\binom{\beta(y)}{2} - \end{aligned} \quad (3.29)$$

$$\begin{aligned}
& -x_2\alpha(x)\alpha(y)\beta(y) + x_3\alpha(y) + \gamma(x)\beta(y) + \\
& + x_1\beta(x)\gamma(y) - x_2\alpha(x)\gamma(y)).
\end{aligned}$$

Порівнюючи коефіцієнти a , b та c у (3.28) та (3.29) за рівністю (3.27), отримуємо твердження (1)–(3) леми. $\square$

3.3.3. Локальні майже-кільця на групі $G(p^m, p^n, p^d)$

Нехай R — локальне майже-кільце з одиницею i , група R^+ якого ізоморфна групі $G(p^m, p^n, p^d)$. Тоді $R^+ = \langle a \rangle + \langle b \rangle + \langle c \rangle$ з елементами a , b та c , що задовольняють співвідношення $ap^m = bp^n = cp^d = 0$, $-b + a + b = a + c$ та $-a + c + a = -b + c + b = c$ з $1 \leq d \leq n \leq m$, де $a = i$ та кожен елемент $x \in R$ однозначно записується у вигляді $x = ax_1 + bx_2 + cx_3$ з коефіцієнтами $0 \leq x_1 < p^m$, $0 \leq x_2 < p^n$ та $0 \leq x_3 < p^d$.

Покажемо, що множина L усіх необоротних елементів R є підгрупою індексу p в R^+ .

Теорема 3.49. *Мають місце такі твердження:*

1. $L = \langle a \cdot p \rangle + \langle b \rangle + \langle c \rangle$ і, зокрема, підгрупа L має індекс p в R^+ та $|R^*| = p^{m+n+d-1}(p-1)$;
2. $x = ax_1 + bx_2 + cx_3$ є оборотним елементом тоді і тільки тоді, коли $x_1 \not\equiv 0 \pmod{p}$.

Доведення. Припустимо, що $|R^+ : L| = p^t$, $t > 1$. Оскільки $R = R^* \cup L$, то випливає, що

$$\begin{aligned}
|R^*| &= |R| - |L| = p^{m+n+d} - p^{m+n+d-t} = \\
&= p^{m+n+d-t}(p^t - 1).
\end{aligned}$$

Згідно з лемою 3.45, група R^* ізоморфна підгрупі A групи автоморфізмів R^+ , тому $|R^*|$ ділить $|\text{Aut}(R^+)|$. Згідно з твердженням 1) леми 3.41 це можливо лише тоді, коли $t = 2$ та $m = n$.

Припустимо, що $|R^+ : L| = p^2$ і $m = n$. Якщо $d = 1$, то це неможливо за [7, Theorem 2]. Тепер нехай $d > 1$. Оскільки $|R^+ : \Phi(R^+)| = p^2$ та наслідок 3.47, маємо $L = \Phi(R^+)$. Отже, за лемою 3.45, отримуємо $R^+ = a^A \cup \Phi(R^+)$, що неможливо за лемою 3.42. Ця суперечність показує, що наше припущення хибне, і тому $|R^+ : L| = p$.

Зрозуміло, що R/L є майже-полем, а отже, фактор-група R^+/L^+ є елементарною абелевою p -групою. Таким чином, для $a \notin L$ маємо $ap \in L$ і тому

$$L = \langle a \cdot p \rangle + \langle b \rangle + \langle c \rangle.$$

Отже, $R^* = R \setminus L$ і тому

$$R^* = \{ax_1 + bx_2 + cx_3 \mid x_1 \not\equiv 0 \pmod{p}\}.$$

□

Застосовуючи твердження (1) теореми 3.49 до леми 3.48, отримуємо наступну формулу для множення елементів $x = ax_1 + bx_2 + cx_3$ та $y = ay_1 + by_2 + cy_3$ у локальному майже-кільці R .

Наслідок 3.50. *Якщо $x, y \in R$ з $1 \leq d \leq n \leq m$ і $xb = a\alpha(x) + b\beta(x) + c\gamma(x)$, то*

$$\begin{aligned} xy = & a(x_1y_1 + y_2\alpha(x)) + b(x_2y_1 + y_2\beta(x)) + \\ & + c(-x_1x_2\binom{y_1}{2} - \binom{y_2}{2}\alpha(x)\beta(x) - x_2y_1y_2\alpha(x) + \\ & + x_3y_1 + y_2\gamma(x) + x_1y_3\beta(x) - x_2y_3\alpha(x)), \end{aligned}$$

де відображення $\alpha: R \rightarrow \mathbb{Z}_{p^m}$, $\beta: R \rightarrow \mathbb{Z}_{p^n}$ і $\gamma: R \rightarrow \mathbb{Z}_{p^d}$, та мають місце наступні твердження:

(0) $\alpha(0) \equiv 0 \pmod{p^m}$, $\beta(0) \equiv 0 \pmod{p^n}$ and $\gamma(0) \equiv 0 \pmod{p^d}$ *тоді і тільки тоді, коли майже-кілець R є нуль-симетричним;*

(1) $\alpha(x) \equiv 0 \pmod{p}$;

(2) *якщо $\beta(x) \equiv 0 \pmod{p}$, то $x_1 \equiv 0 \pmod{p}$;*

(3) $\alpha(xy) \equiv x_1\alpha(y) + \alpha(x)\beta(y) \pmod{p^m}$;

(4) $\beta(xy) \equiv x_2\alpha(y) + \beta(x)\beta(y) \pmod{p^n}$;

(5) $\gamma(xy) \equiv -x_1x_2\binom{\alpha(y)}{2} - \alpha(x)\beta(x)\binom{\beta(y)}{2} - x_2\alpha(x)\alpha(y)\beta(y) + x_3\alpha(y) + \gamma(x)\beta(y) + x_1\beta(x)\gamma(y) - x_2\alpha(x)\gamma(y) \pmod{p^d}$.

Доведення. Дійсно, твердження (0), (3)–(5) повторюють твердження (0)–(4) леми 3.48. Оскільки $L = \langle a \cdot p \rangle + \langle b \rangle + \langle c \rangle$ за теоремою 3.49, а $L \in (R, R)$ -підгрупою в R за твердженням 2) [18, Лема 3.2], то $xb \in L$, а отже, $\alpha(x) \equiv 0 \pmod{p}$, що доводить твердження (1). Взявши $y = c$, маємо

$$xc = c(x_1\beta(x) - x_2\alpha(x)).$$

Таким чином, якщо $\beta(x) \equiv 0 \pmod{p}$, то $xc = 0 \pmod{p}$, і тому $x \in L$. Отже, $x_1 \equiv 0 \pmod{p}$ за теоремою 3.49, що доводить твердження (2). $\square$

Наступна теорема показує, що умови, наведені в теоремі 3.49, є достатніми для існування скінченних локальних майже-кілець на $G(p^m, p^n, p^d)$. Більш того, кожна група $G(p^m, p^n, p^d)$ є адитивною групою майже-кілеця з одиницею.

Теорема 3.51. *Для кожного простого числа p та додатних цілих чисел m, n та d з $1 \leq d \leq n \leq m$ існує локальне майже-кілець R , адитивна група якого R^+ ізоморфна групі $G(p^m, p^n, p^d)$.*

Доведення. Нехай R — адитивно записана група $G(p^m, p^n, p^d)$ з твірними a, b та c , що задовольняють співвідношення $|a| = p^m, |b| = p^n, |c| = p^d, b^{-1}ab = ac$ та $a^{-1}ca = b^{-1}cb = c$. Тоді $G = \langle a \rangle + \langle b \rangle + \langle c \rangle$ і кожен елемент $x \in R$ однозначно записується у вигляді $x = ax_1 + bx_2 + cx_3$ з коефіцієнтами $0 \leq x_1 < p^m, 0 \leq x_2 < p^n$ та $0 \leq x_3 < p^d$. Щоб визначити множення “ $\cdot$ ” на R таким чином, щоб $(R, +, \cdot)$ було локальним майже-кільцем.

Припустимо, що $1 \leq d \leq n \leq m$ і нехай відображення з наслідку 3.50 визначаються конгруенціями $\alpha(x) \equiv 0 \pmod{p^m}, \beta(x) \equiv x_1 \pmod{p^n}$ та $\gamma(x) \equiv 0 \pmod{p^d}$ для кожного $x \in G$. Тоді

$$x \cdot y = ax_1y_1 + b(x_2y_1 + x_1y_2) + c(-x_1x_2 \binom{y_1}{2} + x_3y_1 + x_1^2y_3).$$

Достатньо показати, що відображення $\alpha : G \rightarrow \mathbb{Z}_{p^m}, \beta : G \rightarrow \mathbb{Z}_{p^n}$ та $\gamma : G \rightarrow \mathbb{Z}_{p^d}$ відносно множення “ $\cdot$ ” задовольняють твердження (0)–(5) наслідку 3.50.

Дійсно, $\alpha(0) \equiv 0 \pmod{p^m}, \beta(0) \equiv 0 \pmod{p^n}$ та $\gamma(0) \equiv 0 \pmod{p^d}$ за означенням. Оскільки

$$0 \cdot y = a \cdot 0 + b \cdot 0 + c \cdot 0 = 0$$

для кожного $y \in G$ це означає, що множення “ $\cdot$ ” є нуль-симетричним, і тому доводиться твердження (0) наслідку 3.50. Дійсно, маємо $\alpha(x) \equiv 0 \pmod{p}$ та $x_1 \equiv 0 \pmod{p}$, якщо $\beta(x) \equiv 0 \pmod{p}$, тобто виконуються твердження (1) та (2) наслідку 3.50. Очевидно, виводимо твердження (3)–(5) наслідку 3.50. $\square$

Як наслідок маємо наступне твердження.

Наслідок 3.52. *Кожна група $G(p^m, p^n, p^d)$ є адитивною групою майже-кільця з одиницею.*

3.4. Про групи (C.1)

Нехай G — група типу (C.1) з теореми 3.1. Тоді G є неметациклічною групою класу нільпотентності 2.

Прийmemo наступні позначення: a, b — твірні групи G такі, що $G/G' = \langle aG' \rangle \times \langle bG' \rangle$, aG' має порядок p^m та bG' має порядок p^n . Тоді $c = [a, b]$ породжує G' , c має порядок p^d з $d \leq m, d \leq n, c \in Z(G)$. G має представлення $G = \langle a, b, c | a^{p^m} = b^{p^n} = c^{p^d} = 1, a^b = ac, c^a = c^{1+p^{d-r}}, c^b = c \rangle$, та кожний елемент групи G може бути записаний у вигляді $a^x b^y c^z$, $x \in Z/p^m Z$, $y \in Z/p^n Z$, $z \in Z/p^d Z$. Позначимо групу G як $G(p^m, p^n, p^d, r)$.

Надалі, для кожного простого числа p та натуральних чисел m, n, d, s з $d \leq m, d \leq n, 0 \leq r \leq n$ позначимо через $G(p^m, p^n, p^d, r)$ напівпрямий добуток $(\langle a \rangle \times \langle c \rangle) \rtimes \langle b \rangle$, де $|a| = p^m, |b| = p^n, |c| = p^d, b^{-1}ab = ac, a^{-1}ca = c^{1+p^{d-r}}$ та $b^{-1}cb = c$.

Для довільних цілих чисел h та $k \geq 0$ покладемо $j(h, k) = \frac{h^k - 1}{h - 1}$, якщо $h \neq 1$ та $j(1, k) = k$.

Лема 3.53. *Нехай $q = 1 + p^{d-r}$. Для довільних цілих $w, k \geq 0$ мають місце наступні конгруентності:*

- 1) $q^w \equiv q^{wq} \equiv 1 + wp^{d-r} \pmod{p^{2(d-r)}};$
- 2) $j(q^w, k) \equiv k + \binom{k}{2} wp^{d-r} \pmod{p^{2(d-r)}};$
- 3) $1 + q + \dots + q^{k-1} \equiv k + \binom{k}{2} p^{d-r} \pmod{p^{2(d-r)}}.$

Доведення. Враховуючи, що $j(h, k) = \frac{h^k - 1}{h - 1}$ при $h \neq 1, j(1, k) = k$ та $q = 1 + p^{d-r}$.

$$1) q^w = (1 + p^{d-r})^w =$$

$$1 + wp^{d-r} + \binom{w}{2} p^{2(d-r)} + \dots + p^{w(d-r)} \equiv$$

$$1 + wp^{d-r} \pmod{p^{2(d-r)}}.$$

Тоді

$$\begin{aligned} q^{wq} &= (q^w)^q = (1 + wp^{d-r})^q = \\ &= 1 + qwp^{d-r} = 1 + (1 + p^{d-r})wp^{2(d-r)} = \\ &= 1 + wp^{d-r} + wp^{2(d-r)} \equiv 1 + wp^{d-r} \pmod{p^{2(d-r)}}, \end{aligned}$$

що доводить твердження 1).

$$\begin{aligned} 2) \ j(q^w, k) &= \frac{(1+wp^{d-r})^k - 1}{1+wp^{d-r} - 1} = \\ &= \frac{1 + kwp^{d-r} + \binom{k}{2}wp^{2(d-r)} + \dots + wp^{w(d-r)-1}}{wp^{d-r}} \equiv \\ &= k + \binom{k}{2}wp^{d-r} \pmod{p^{2(d-r)}}, \end{aligned}$$

що доводить твердження 2).

$$3) \ 1 + q + \dots + q^{k-1} =$$

$$\begin{aligned} &1 + (1 + p^{d-r}) + \dots + (1 + (k-1)p^{d-r}) \equiv \\ &k + \binom{k}{2}p^{d-r} \pmod{p^{2(d-r)}}, \end{aligned}$$

що доводить твердження 3). □

Лема 3.54. Для будь-яких натуральних чисел v та u в групі $G(p^m, p^n, p^d, r)$ виконується співвідношення

$$vc + a = a + vqc$$

та

$$vc + ua \equiv ua + vq^u c \pmod{p^{2(d-r)}}.$$

Доведення. Очевидно, що

$$-a + c + a = qc,$$

$$c = a + qc - a,$$

$$c + c = a + qc - a + a + qc - a,$$

$$2c = a + qc + qc - a,$$

$$2c = a + 2qc - a,$$

$$\begin{aligned} vc = vc + c &= a + vqc - a + a + qc - a = \\ &= a + vqc + qc - a = a + (v + 1)qc - a. \end{aligned}$$

А також,

$$vc + a = a + vqc,$$

$$vc + a + a = a + vqc + a,$$

$$vc + 2a = a + a + vq^2c = 2a + vq^2c,$$

$$\begin{aligned} vc + a + a + a &= vc + 3a = 2a + vq^2c + a = \\ &= 2a + a + vq^2qc = 3a + vq^3c. \end{aligned}$$

Зауважимо, що

$$vc + ua \equiv ua + vq^u c \pmod{p^{2(d-r)}}.$$

Далі, за індукцією по u , маємо

$$\begin{aligned} vc + (u + 1)a &= ua + vq^u c + a = \\ &= ua + a + vq^u qc \equiv (u + 1)a + vq^{u+1} c \pmod{p^{2(d-r)}}. \end{aligned}$$

Що доводить твердження леми. □

Лема 3.55. Для будь-яких натуральних чисел k та l в групі $G(p^m, p^n, p^d, r)$ виконуються співвідношення

$$-ka - lb + ka + lb = lj(q, k)c$$

та

$$lb + ka = ka + lb - lj(q, k)c.$$

Доведення. Оскільки $-a - b + a + b = c$, то $-b + a + b = a + c$, звідки $-lb + a + lb = a + lc$. Враховуючи лему 3.54, маємо

$$-lb + ka + lb = ka + l(1 + q + \dots + q^{k-1})c.$$

Далі, за індукцією по k , маємо

$$\begin{aligned} -lb + (k+1)a + lb &= ka + l(1 + q + \dots + q^{k-1})c + a + lc = \\ &= ka + a + l(1 + q + \dots + q^{k-1})qc + lc = \\ &= (k+1)a + l((1 + q + \dots + q^{k-1})q + 1)c = \\ &= (k+1)a + l(1 + q + \dots + q^k)c. \end{aligned}$$

Однак, застосувавши твердження 3) леми 3.53, маємо

$$-lb + ka + lb = ka + l(k + \binom{k}{2}p^{d-r})c$$

або

$$-ka - lb + ka + lb = l(k + \binom{k}{2}p^{d-r})c.$$

Отже, за твердженням 2) леми 3.53, маємо

$$-ka - lb + ka + lb = lj(q, k)c,$$

звідси

$$lb + ka = ka + lb - lj(q, k)c.$$

□

Лема 3.56. Для будь-яких натуральних чисел k, l, v та t в групі $G(p^m, p^n, p^d, r)$ виконується співвідношення

$$\begin{aligned} (ak + bl + cv)t &= akt + blt + \\ &+ c(-lj(q, k)(j(q^k, t-2) + 1) + vj(q^k, t-2)). \end{aligned}$$

Доведення. Враховуючи леми 3.54 та 3.55, маємо

$$\begin{aligned} & (ak + bl + cv)t = \\ & = akt + blt + c(-lj(q, k)(n - 1 + (n - 2)q^k + \dots + q^{(n-2)k}) + \\ & \quad + v(1 + q^k + \dots + q^{(n-2)k})). \end{aligned}$$

Тоді

$$\begin{aligned} & (ak + bl + cv)(t + 1) = akt + blt + c(-lj(q, k)(n - 1 + \\ & \quad + (n - 2)q^k + \dots + q^{(n-2)k}) + v(1 + q^k + \dots + q^{(n-2)k})) + \\ & \quad + ak + bl + cv = akt + blt + ak + c(-lj(q, k)(n - 1 + \\ & \quad + (n - 2)q^k + \dots + q^{(n-2)k}) + v(1 + q^k + \dots + q^{(n-2)k}))q^k + bl + vc = \\ & \quad akt + ak + blt -ctlj(q, k) + c(-lj(q, k)(n - 1 \\ & \quad + (n - 2)q^k + \dots + q^{(n-2)k}) + v(1 + q^k + \dots + q^{(n-2)k}))q^k + bl + cv = \\ & = a(t + 1)k + b(t + 1)l + c(-tlj(q, k) + (-lj(q, k)(t - 1 + \\ & \quad + (t - 2)q^k + \dots + q^{(t-2)k}) + \\ & \quad + v(1 + q^k + \dots + q^{(t-2)k})q^k + v) = \\ & = a(t + 1)k + b(t + 1)l + c(-tlj(q, k) - lj(q, k)(t - 1 + \\ & \quad + (t - 2)q^k + \dots + q^{(t-2)k})q^k + \\ & \quad + v(1 + q^k + \dots + q^{(t-2)k})q^k + v) = \\ & = a(t + 1)k + b(t + 1)l + c(-tlj(q, k) - lj(q, k)((t - 1)q^k + \\ & \quad + (t - 2)q^{2k} + \dots + q^{(t-2)k+k}) + \\ & \quad + v(1 + q^k + q^{2k} + \dots + q^{(t-2)k+k}) = \\ & = a(t + 1)k + b(t + 1)l + c(-lj(q, k)(t + (t - 1)q^k + \dots + q^{(t-1)k}) + \\ & \quad + v(1 + q^k + q^{2k} + \dots + q^{(t-1)k})) = \end{aligned}$$

Отже,

$$= akt + blt + c(-lj(q, k)(j(q^k, t - 2) + 1) + vj(q^k, t - 2)).$$

□

За допомогою системи GАР покажемо, що група $G(3^2, 3^2, 3^2, 1)$ не може бути адитивною групою локального майже-кільця.

Знайдемо *IdGroup* групи $G(3^2, 3^2, 3^2, 1)$.

```
gap > f := FreeGroup("a", "b", "u");;
gap > G := f/[f.1^9, f.2^9, f.3^9, f.2^ - 1 * f.1^ - 1 * f.2 * f.1 * f.3^ -
1, f.3^ - 4 * f.1^ - 1 * f.3 * f.1, f.3^ - 1 * f.2^ - 1 * f.3 * f.2];
< fp group on the generators [a, b, u] >
# Знайдемо порядок групи G.
gap > Size(G);
729
# G — група з IdGroup [729, 30].
gap > IdGroup(G);
[729, 30]
# Опис структури групи G.
gap > StructureDescription(G);
“(C9 × C9) ⋈ C9”
```

Доведемо наступне твердження.

Лема 3.57. *Не існує локального майже-кільця, адитивна група якого ізоморфна групі $G(3^2, 3^2, 3^2, 1)$.*

Доведення. Нехай R — локальне майже-кільце на групі $G(3^2, 3^2, 3^2, 1)$.

За лемою 1.53 $|R| \leq |L|^2$. Враховуючи, інформацію зі стор. 88 [66], маємо $|R : L| = 3$. Звідси $|L| = 3^5 = 243$.

В силу того, що $R = R^* \cup L$, маємо

$$|R^*| = p^n - p^m = p^m(p^l - 1).$$

Тоді $|R^*| = 486$.

В середовищі системи GAP завантажуюмо пакет SONATA.

```
gap > LoadPackage("sonata");
```

G — група, ізоморфна $G(3^2, 3^2, 3^2, 1)$.

```
gap > G := SmallGroup(729, 30);
```

```
< pc group of size 729 with 6 generators >
```

Перевірка, чи є група G ендосиклічною.

```
gap > IsEndoCyclicGroup(G);
```

```
true
```

Aut — група автоморфізмів групи G .

```
gap > Aut := AutomorphismGroup(G);
```

```
< group of size 39366 with 10 generators >
```

Перевірка, чи є в групі Aut підгрупи порядку 486 та довжиною орбіти 486.

```
gap > is := IsomorphismPermGroup(Aut);
```

```
< action isomorphism >
```

```
gap > Au := Image(is);
```

```
< permutation group of size 39366 with 10 generators >
```

```
gap > Ccs := ConjugacyClassesSubgroups(Au);;
```

```
gap > Sub := [];
```

```
[]
```

```
gap > for x in Ccs do
```

```
> d := Representative(x);
```

```
> Add(Sub, d);
```

```
> od;
```

```
gap > Su := Filtered(Sub, x -> Size(x) = 486);;
```

```
gap > Size(Su);
```

```
421
```

```
gap > Mul := [];
```

```

□
gap > for x in u do
> c := PreImage(is, x);
> Add(Mul, c);
> od;
gap > U0 := Filtered(Mul, x -> Maximum(OrbitLengths(x, G)) =
486);;
gap > Size(U0);
0

```

□

Сформулюємо наступну гіпотезу.

Гіпотеза 3.58. *Не існує локального майже-кільця, адитивна група якого ізоморфна групі типу (C.1) з теореми 3.1.*

3.5. Групи (B.2) та (C.2)

Аналіз груп (B.2) та (C.2) з теореми 3.1 порядку 729 за допомогою GАР дозволяє зробити наступне припущення.

Гіпотеза 3.59. *Не існує локального майже-кільця, адитивна група якого ізоморфна (B.2) чи (C.2).*

Для прикладу розглянемо групу типу (B.2), а саме групу з *IdGroup* [729, 33].

```

gap > f := FreeGroup("a", "b", "u");;
gap > G := f/[f.1^9, f.3^9, f.2^ - 1 * f.1^ - 1 * f.2 * f.1 * f.3^ -
1, f.1^ - 1 * f.3 * f.1 * f.3^ - 4, f.3^ - 1 * f.2^ - 1 * f.3 * f.2, f.2^9 * f.3^3];
< fp group on the generators [a, b, u] >
# Знайдемо порядок групи G.
gap > Size(G);

```

729

G — група з *IdGroup* [729, 33].*gap* > *IdGroup*(G);

[729, 33]

Опис структури групи G .*gap* > *StructureDescription*(G);“($C_{27} \times C_3$) $\rtimes C_9$ ”# Aut — група автоморфізмів групи G .*gap* > $Aut := AutomorphismGroup(G)$;< *group of size 13122 with 9 generators* ># Перевірка, чи є в групі Aut підгрупи порядку 486 та довжиною орбіти 486.*gap* > $is := IsomorphismPermGroup(Aut)$;< *action isomorphism* >*gap* > $Au := Image(is)$;< *permutation group of size 13122 with 9 generators* >*gap* > $Ccs := ConjugacyClassesSubgroups(Au)$;;*gap* > $Sub := []$;

[]

gap > *for* x *in* Ccs *do*> $d := Representative(x)$;> $Add(Sub, d)$;> *od*;*gap* > $Su := Filtered(Sub, x \rightarrow Size(x) = 486)$;;*gap* > $Size(Su)$;

346

gap > $Mul := []$;

[]

gap > *for* x *in* Su *do*

```

> c := PreImage(is, x);
> Add(Mul, c);
> od;
gap > U0 := Filtered(Mul, x -> Maximum(OrbitLengths(x, G)) =
486);;
gap > Size(U0);
0

```

Отже, сформулюємо наступний результат.

Лема 3.60. *Не існує локального майже-кілля, адитивна група якого ізоморфна групі [729, 33].*

Висновки до розділу 3

У даному розділі:

- проаналізовано скінченні неабелеві 2-породженні p -групи з циклічним комутантом;
- показано, що не існує майже-кілля з одиницею, адитивна група якого ізоморфна групі $G(p^m, p^n)$ з $p > 2$ і $2 \leq m \leq n$;
- вивчено скінченні локальні майже-кілля з розщепленою метациклічною адитивною групою;
- отримано необхідні і достатні умови існування локальних майже-кілля на групах типу (B.1). Доведено, що індекс підгрупи всіх необоротних елементів таких майже-кілля в адитивній групі дорівнює p . А також, показано, що кожна група типу (B.1) є адитивною групою майже-кілля з одиницею.

Основні результати даного розділу опубліковано у працях [12, 16, 7, 13] зі списку публікацій і, відповідно, [78], [94], [89], [71] зі списку використаних джерел, а також опубліковано у тезах конференцій [31, 37, 36, 37] і, відповідно, [3], [74], [104], [74].

Розділ 4

Напівдистрибутивні майже-кільця з одиницею та локальні майже-кільця

В розділі введено та досліджено напівдистрибутивні майже-кільця з одиницею. Також вивчено напівгрупу необоротних елементів локальних майже-кілець, адитивна група якого ізоморфна абелевій групі типу $(2^m, 2^n)$ з $m \geq n > 1$.

4.1. Дистрибутивні та напівдистрибутивні майже-кільця з одиницею

Спочатку нагадаємо деякі основні означення теорії майже-кілець.

Означення 4.1. Множина R з двома бінарними операціями “+” та “.” називається (лівим) майже-кільцем, якщо виконуються такі твердження:

- (1) $(R, +)$ — (не обов’язково абелева) група з нейтральним елементом 0;
- (2) $(R, \cdot)$ — напівгрупа;
- (3) $x \cdot (y + z) = x \cdot y + x \cdot z$ для всіх $x, y, z \in R$.

Якщо R є майже-кільцем, то група $R^+ = (R, +)$ називається адитивною групою R . Крім того, якщо M є підгрупою R^+ , то з твердження (3) випливає, що для кожного елемента $x \in R$ множина $xM = \{x \cdot y | y \in M\}$ є підгрупою R^+ і, зокрема, $x \cdot 0 = 0$. Якщо крім того $0 \cdot x = 0$, то майже-кільце R називається нуль-симетричним, а якщо напівгрупа $(R, \cdot)$ є моноїдом, тобто вона має одиничний елемент i , то R є майже-кільцем з одиницею i . В останньому випадку група R^* усіх оборотних елементів моноїда $(R, \cdot)$ називається мультиплікативною групою R . Підгрупа M групи R^+ називається R^* -інваріантною, якщо $rM \leq M$ для кожного $r \in R^*$ та M є (R, R) -підгрупою, якщо $xMy \subseteq M$ для довільних елементів $x, y \in R$.

Добре відомо, що множина всіх ендоморфізмів групи G утворює моноїд відносно композиції ендоморфізмів. Цей моноїд буде позначатися $\text{End}(G)$ і називатися моноїдом ендоморфізмів G . Очевидно, що група автоморфізмів $\text{Aut}(G)$ є підмоноїдом $\text{End}(G)$, що складається з множини всіх оборотних елементів $\text{End}(G)$. Наступна лема встановлює зв'язок між деякими напівгрупами ендоморфізмів адитивної групи майже-кільця та його мультиплікативними піднапівгрупами.

Лема 4.2. *Нехай R — майже-кільце з одиницею i , а S — напівгрупа $(R, \cdot)$. Тоді моноїд ендоморфізму $\text{End}(R^+)$ містить піднапівгрупу T , ізоморфну S і задовольняє умову*

$$i^T = \{i^t | t \in T\} = S.$$

Зокрема, якщо $S = (R, \cdot)$, то перетин $A = \text{Aut}(R^+) \cap T$ є підгрупою в $\text{Aut}(R^+)$ ізоморфною мультиплікативній групі R^ та*

$$i^A = \{i^a | a \in A\} = R^*.$$

Підгрупа A групи автоморфізмів $\text{Aut}(R^+)$, визначеної в лемі 4.2, називається підгрупою $\text{Aut}(R^+)$ асоційованою з групою R^* .

Нагадаємо, означення дистрибутивного та дистрибутивно породженого майже-кільця.

Означення 4.3. Ліве майже-кільце N називається дистрибутивним майже-кільцем, якщо його множення також є дистрибутивним справа.

Означення 4.4 ([16]). Майже-кільце $(N, +, \cdot)$ називається дистрибутивно породженим, якщо $(N, +)$ породжене адитивно дистрибутивними елементами майже-кільця.

Наступні функції, які визначають чи є майже-кільце дистрибутивним чи дистрибутивно породженим реалізовані в пакеті SONATA системи GAP.

IsDistributiveNearRing(nr) (функція)

Повертає: логічний оператор

Аргументом є майже-кільце nr . Вивід має значення **true**, якщо майже-кільце є дистрибутивним, інакше вивід має значення **false**.

Приклад.

```
gap > n := LibraryNearRing( GTW12_4, 8 );
LibraryNearRing(12/4, 8)
gap > IsDistributiveNearRing( n );
false
```

IsDgNearRing(nr) (функція)

Повертає: логічний оператор

Аргументом є майже-кільце nr . Вивід має значення **true**, якщо майже-кільце є дистрибутивно породженим, інакше вивід має значення **false**.

Приклад.

```
gap > n := LibraryNearRing( GTW12_4, 8 );
LibraryNearRing(12/4, 8)
gap > IsDgNearRing( n );
false
```

Наведемо означення напівдистрибутивного майже-кільця.

Означення 4.5. (Ліве) майже-кільце R називається напівдистрибутивним, якщо таким є множення справа відносно його додавання. Іншими словами, для будь-яких елементів $r, s, t \in R$ виконується рівність $(r + s + r)t = rt + st + rt$.

Функція, яка визначає чи майже-кільце є напівдистрибутивним реалізована в пакеті LocalNR.

IsSemiDistributiveNearRing(R) (функція)

Повертає: логічний оператор

Аргументом є майже-кільце R . Вивід має значення **true**, якщо майже-кільце є напівдистрибутивним, інакше вивід має значення **false**.

Приклад.

```
gap > N := LocalNearRing(16,10,8,2,7);
ExplicitMultiplicationNearRing ( <pc group of size 16 with 4 generators>
, multiplication )
gap > IsDistributiveNearRing(N);
false
gap > IsDgNearRing(N);
false
gap > IsSemiDistributiveNearRing(N);
true
```

Нехай $m(G)$, $d(G)$, $dg(G)$ та $sd(G)$ — кількість усіх неізоморфних майже-кілець з одиницею R , адитивна група яких R^+ ізоморфна групі G , усіх неізоморфних дистрибутивних, дистрибутивно породжених та напівдистрибутивних майже-кілець з одиницею R , адитивна група яких R^+ ізоморфна групі G .

Наступна лема отримана за допомогою леми 1.63, GAP, пакетів LocalNR та SONATA.

Лема 4.6. *Нехай G є адитивна група майже-кілця з одиницею R порядку менше 32, то виконується наступне.*

- $IdGroup(G) = [4, 1]$, група $G \cong C_4$, $m(G) = 1$, $d(G) = 1$, $dg(G) = 1$ та $sd(G) = 1$;
- $IdGroup(G) = [4, 2]$, група $G \cong C_2 \times C_2$, $m(G) = 5$, $d(G) = 3$, $dg(G) = 3$ та $sd(G) = 5$;
- $IdGroup(G) = [5, 1]$, група $G \cong C_5$, $m(G) = 1$, $d(G) = 1$, $dg(G) = 1$ та $sd(G) = 1$;
- $IdGroup(G) = [6, 2]$, група $G \cong C_6$, $m(G) = 1$, $d(G) = 1$, $dg(G) = 1$ та $sd(G) = 1$;
- $IdGroup(G) = [7, 1]$, група $G \cong C_7$, $m(G) = 1$, $d(G) = 1$, $dg(G) = 1$ та $sd(G) = 1$;
- $IdGroup(G) = [8, 1]$, група $G \cong C_8$, $m(G) = 1$, $d(G) = 1$, $dg(G) = 1$ та $sd(G) = 1$;
- $IdGroup(G) = [8, 2]$, група $G \cong C_4 \times C_2$, $m(G) = 10$, $d(G) = 3$, $dg(G) = 3$ та $sd(G) = 7$;

- $IdGroup(G) = [8, 3]$, $\text{epyna } G \cong D_8$, $m(G) = 7$, $d(G) = 0$, $dg(G) = 1$
ma $sd(G) = 0$;
- $IdGroup(G) = [8, 5]$, $\text{epyna } G \cong C_2 \times C_2 \times C_2$, $m(G) = 35$, $d(G) = 7$,
 $dg(G) = 7$ ma $sd(G) = 35$;
- $IdGroup(G) = [9, 1]$, $\text{epyna } G \cong C_9$, $m(G) = 1$, $d(G) = 1$, $dg(G) = 1$
ma $sd(G) = 1$;
- $IdGroup(G) = [9, 2]$, $\text{epyna } G \cong C_3 \times C_3$, $m(G) = 10$, $d(G) = 3$,
 $dg(G) = 3$ ma $sd(G) = 3$;
- $IdGroup(G) = [10, 2]$, $\text{epyna } G \cong C_{10}$, $m(G) = 1$, $d(G) = 1$, $dg(G) =$
 1 ma $sd(G) = 1$;
- $IdGroup(G) = [11, 1]$, $\text{epyna } G \cong C_{11}$, $m(G) = 1$, $d(G) = 1$, $dg(G) =$
 1 ma $sd(G) = 1$;
- $IdGroup(G) = [12, 2]$, $\text{epyna } G \cong C_{12}$, $m(G) = 1$, $d(G) = 1$, $dg(G) =$
 1 ma $sd(G) = 1$;
- $IdGroup(G) = [12, 4]$, $\text{epyna } G \cong D_{12}$, $m(G) = 1$, $d(G) = 0$, $dg(G) =$
 0 ma $sd(G) = 0$;
- $IdGroup(G) = [12, 5]$, $\text{epyna } G \cong C_6 \times C_2$, $m(G) = 9$, $d(G) = 3$,
 $dg(G) = 3$ ma $sd(G) = 5$;
- $IdGroup(G) = [13, 1]$, $\text{epyna } G \cong C_{13}$, $m(G) = 1$, $d(G) = 1$, $dg(G) =$
 1 ma $sd(G) = 1$;
- $IdGroup(G) = [14, 2]$, $\text{epyna } G \cong C_{14}$, $m(G) = 1$, $d(G) = 1$, $dg(G) =$
 1 ma $sd(G) = 1$;
- $IdGroup(G) = [15, 1]$, $\text{epyna } G \cong C_{15}$, $m(G) = 1$, $d(G) = 1$, $dg(G) =$
 1 ma $sd(G) = 1$;

- $IdGroup(G) = [16, 1]$, $\text{epyna } G \cong C_{16}$, $m(G) = 1$, $d(G) = 1$, $dg(G) = 1$ *ma* $sd(G) = 1$;
- $IdGroup(G) = [16, 2]$, $\text{epyna } G \cong C_4 \times C_4$, $m(G) = 51$, $d(G) = 6$, $dg(G) = 6$ *ma* $sd(G) = 10$;
- $IdGroup(G) = [16, 3]$, $\text{epyna } G \cong (C_4 \times C_2) \rtimes C_2$, $m(G) = 132$, $d(G) = 0$, $dg(G) = 6$ *ma* $sd(G) = 0$;
- $IdGroup(G) = [16, 4]$, $\text{epyna } G \cong C_4 \rtimes C_4$, $m(G) = 40$, $d(G) = 0$, $dg(G) = 4$ *ma* $sd(G) = 0$;
- $IdGroup(G) = [16, 5]$, $\text{epyna } G \cong C_8 \times C_2$, $m(G) = 37$, $d(G) = 3$, $dg(G) = 3$ *ma* $sd(G) = 7$;
- $IdGroup(G) = [16, 6]$, $\text{epyna } G \cong C_8 \rtimes C_2$, $m(G) = 33$, $d(G) = 0$, $dg(G) = 8$ *ma* $sd(G) = 0$;
- $IdGroup(G) = [16, 10]$, $\text{epyna } G \cong C_4 \times C_2 \times C_2$, $m(G) = 470$, $d(G) = 15$, $dg(G) = 15$ *ma* $sd(G) = 264$;
- $IdGroup(G) = [16, 11]$, $\text{epyna } G \cong C_2 \times D_8$, $m(G) = 708$, $d(G) = 0$, $dg(G) = 6$ *ma* $sd(G) = 0$;
- $IdGroup(G) = [16, 12]$, $\text{epyna } G \cong C_2 \times Q_8$, $m(G) = 4$, $d(G) = 0$, $dg(G) = 1$ *ma* $sd(G) = 0$;
- $IdGroup(G) = [16, 14]$, $\text{epyna } G \cong C_2 \times C_2 \times C_2 \times C_2$, $m(G) = 2798$, $d(G) = 25$, $dg(G) = 25$ *ma* $sd(G) = 2798$;
- $IdGroup(G) = [17, 1]$, $\text{epyna } G \cong C_{17}$, $m(G) = 1$, $d(G) = 1$, $dg(G) = 1$ *ma* $sd(G) = 1$;
- $IdGroup(G) = [18, 2]$, $\text{epyna } G \cong C_{18}$, $m(G) = 1$, $d(G) = 1$, $dg(G) = 1$ *ma* $sd(G) = 1$;

- $IdGroup(G) = [18, 3]$, $\text{epyna } G \cong C_3 \times S_3$, $m(G) = 8$, $d(G) = 0$, $dg(G) = 2$ $\text{ma } sd(G) = 0$;
- $IdGroup(G) = [18, 5]$, $\text{epyna } G \cong C_6 \times C_3$, $m(G) = 17$, $d(G) = 3$, $dg(G) = 3$ $\text{ma } sd(G) = 3$;
- $IdGroup(G) = [19, 1]$, $\text{epyna } G \cong C_{19}$, $m(G) = 1$, $d(G) = 1$, $dg(G) = 1$ $\text{ma } sd(G) = 1$;
- $IdGroup(G) = [20, 2]$, $\text{epyna } G \cong C_{20}$, $m(G) = 1$, $d(G) = 1$, $dg(G) = 1$ $\text{ma } sd(G) = 1$;
- $IdGroup(G) = [20, 4]$, $\text{epyna } G \cong D_{20}$, $m(G) = 1$, $d(G) = 0$, $dg(G) = 0$ $\text{ma } sd(G) = 0$;
- $IdGroup(G) = [20, 5]$, $\text{epyna } G \cong C_{10} \times C_2$, $m(G) = 9$, $d(G) = 3$, $dg(G) = 3$ $\text{ma } sd(G) = 5$;
- $IdGroup(G) = [21, 2]$, $\text{epyna } G \cong C_{21}$, $m(G) = 1$, $d(G) = 1$, $dg(G) = 1$ $\text{ma } sd(G) = 1$;
- $IdGroup(G) = [22, 2]$, $\text{epyna } G \cong C_{22}$, $m(G) = 1$, $d(G) = 1$, $dg(G) = 1$ $\text{ma } sd(G) = 1$;
- $IdGroup(G) = [23, 1]$, $\text{epyna } G \cong C_{23}$, $m(G) = 1$, $d(G) = 1$, $dg(G) = 1$ $\text{ma } sd(G) = 1$;
- $IdGroup(G) = [24, 2]$, $\text{epyna } G \cong C_{24}$, $m(G) = 1$, $d(G) = 1$, $dg(G) = 1$ $\text{ma } sd(G) = 1$;
- $IdGroup(G) = [24, 5]$, $\text{epyna } G \cong$, $m(G) = 1$, $d(G) = 0$, $dg(G) = 0$ $\text{ma } sd(G) = 0$;
- $IdGroup(G) = [24, 9]$, $\text{epyna } G \cong C_{12} \times C_2$, $m(G) = 14$, $d(G) = 3$, $dg(G) = 3$ $\text{ma } sd(G) = 7$;

- $IdGroup(G) = [24, 10]$, $epyna\ G \cong C_3 \times D_8$, $m(G) = 7$, $d(G) = 0$, $dg(G) = 1$ $ma\ sd(G) = 0$;
- $IdGroup(G) = [24, 13]$, $epyna\ G \cong C_2 \times A_4$, $m(G) = 8$, $d(G) = 0$, $dg(G) = 2$ $ma\ sd(G) = 0$;
- $IdGroup(G) = [24, 14]$, $epyna\ G \cong C_2 \times C_2 \times S_3$, $m(G) = 10$, $d(G) = 0$, $dg(G) = 0$ $ma\ sd(G) = 0$;
- $IdGroup(G) = [24, 15]$, $epyna\ G \cong C_6 \times C_2 \times C_2$, $m(G) = 136$, $d(G) = 7$, $dg(G) = 7$ $ma\ sd(G) = 35$;
- $IdGroup(G) = [25, 1]$, $epyna\ G \cong C_{25}$, $m(G) = 1$, $d(G) = 1$, $dg(G) = 1$ $ma\ sd(G) = 1$;
- $IdGroup(G) = [25, 2]$, $epyna\ G \cong C_5 \times C_5$, $m(G) = 16$, $d(G) = 3$, $dg(G) = 3$ $ma\ sd(G) = 3$;
- $IdGroup(G) = [26, 2]$, $epyna\ G \cong C_{26}$, $m(G) = 1$, $d(G) = 1$, $dg(G) = 1$ $ma\ sd(G) = 1$;
- $IdGroup(G) = [27, 1]$, $epyna\ G \cong C_{27}$, $m(G) = 1$, $d(G) = 1$, $dg(G) = 1$ $ma\ sd(G) = 1$;
- $IdGroup(G) = [27, 2]$, $epyna\ G \cong C_9 \times C_3$, $m(G) = 20$, $d(G) = 4$, $dg(G) = 4$ $ma\ sd(G) = 4$;
- $IdGroup(G) = [27, 3]$, $epyna\ G \cong (C_3 \times C_3) \rtimes C_3$, $m(G) = 22$, $d(G) = 0$, $dg(G) = 2$ $ma\ sd(G) = 0$;
- $IdGroup(G) = [27, 4]$, $epyna\ G \cong C_9 \rtimes C_3$, $m(G) = 4$, $d(G) = 0$, $dg(G) = 0$ $ma\ sd(G) = 0$;
- $IdGroup(G) = [27, 5]$, $epyna\ G \cong C_3 \times C_3 \times C_3$, $m(G) = 202$, $d(G) = 7$, $dg(G) = 7$ $ma\ sd(G) = 7$;

- $IdGroup(G) = [28, 2]$, група $G \cong C_{28}$, $m(G) = 1$, $d(G) = 1$, $dg(G) = 1$ та $sd(G) = 1$;
- $IdGroup(G) = [28, 3]$, група $G \cong D_{28}$, $m(G) = 1$, $d(G) = 0$, $dg(G) = 0$ та $sd(G) = 0$;
- $IdGroup(G) = [28, 4]$, група $G \cong C_{14} \times C_2$, $m(G) = 9$, $d(G) = 3$, $dg(G) = 3$ та $sd(G) = 5$;
- $IdGroup(G) = [29, 1]$, група $G \cong C_{29}$, $m(G) = 1$, $d(G) = 1$, $dg(G) = 1$ та $sd(G) = 1$;
- $IdGroup(G) = [30, 4]$, група $G \cong C_{30}$, $m(G) = 1$, $d(G) = 1$, $dg(G) = 1$ та $sd(G) = 1$;
- $IdGroup(G) = [31, 1]$, група $G \cong C_{31}$, $m(G) = 1$, $d(G) = 1$, $dg(G) = 1$ та $sd(G) = 1$.

4.1.1. Адитивні групи напівдистрибутивних майже-кілець

Очевидно, що кожне дистрибутивне майже-кілець є напівдистрибутивним, але не навпаки. Наприклад, майже-кілець $Map(G)$ усіх функцій на групі G порядку 2 є напівдистрибутивним, а не дистрибутивним.

Лема 4.7. *Нехай R — напівдистрибутивне майже-кілець, n — натуральне число і r, s — будь-які елементи з R . Тоді справедливі такі твердження:*

- (1) $(-r) \cdot s = -(r \cdot s)$ і тому $0 \cdot s = 0$ або $0 \cdot s$ є елементом порядку 2 в R^+ . Зокрема, якщо r є елементом непарного порядку в R^+ , то $0 \cdot r = 0$;
- (2) $(r \cdot n)s = (rs) \cdot n$ для непарних n і $(r \cdot n)s = (rs) \cdot n + 0 \cdot s$ для парних n ;

(3) якщо r і s — елементи взаємно простих порядків, то $r \cdot s = 0$.

Доведення. Оскільки

$$r \cdot s = (r + (-r) + r) \cdot s = r \cdot s + (-r) \cdot s + r \cdot s,$$

випливає, що $0 = (-r) \cdot s + r \cdot s$, звідки $(-r) \cdot s = -(r \cdot s)$. Зокрема, якщо $r \cdot m = 0$ для деякого непарного m , то $1 = 2n - m$ для $n = \frac{m+1}{2}$ і тому

$$0 \cdot r = (0 \cdot r) \cdot 2n - (0 \cdot r) \cdot m = 0,$$

як вимагалось.

Для $n = 1$ твердження (2) є очевидним. Якщо $n > 1$, то

$$\begin{aligned} (r \cdot n)s &= (r + r \cdot (n - 2) + r)s = \\ &= rs + (r \cdot (n - 2))s + rs = (rs) \cdot 2 + (r \cdot (n - 2))s. \end{aligned}$$

За допомогою індукції по n маємо

$$(r \cdot (n - 2))s = (rs) \cdot (n - 2)$$

для непарних n і

$$(r \cdot (n - 2))s = (rs) \cdot (n - 2) + 0 \cdot s$$

для парних n . Тому

$$(r \cdot n)s = (rs) \cdot 2 + (rs) \cdot (n - 2) = (rs) \cdot n$$

для непарних n і

$$\begin{aligned} (r \cdot n)s &= (rs) \cdot 2 + (rs) \cdot (n - 2) = \\ &= (rs) \cdot n + 0 \cdot s \end{aligned}$$

для парних n , що доводить (2).

Нарешті, нехай m і n — порядки r і s відповідно. Якщо $(m, n) = 1$, то одне з цих чисел, скажімо m , є непарним, тому

$$(rs) \cdot m = (r \cdot m)s = 0 \cdot s = 0$$

за твердженням (2). З іншого боку,

$$(rs) \cdot n = r(s \cdot n) = r \cdot 0 = 0.$$

Тому $rs = 0$, як вимагалось. □

Відомо, що адитивна група будь-якого дистрибутивного майже-кілець з одиницею є абелевою. Наступне твердження поширює цей факт на напівдистрибутивні майже-кілець.

Лема 4.8. *Адитивна група кожного напівдистрибутивного майже-кілець R з одиницею є абелевою.*

Доведення. Дійсно, якщо i є одиницею в R , то $(-i)s = -s$ для кожного $s \in R$ згідно з твердженням (1) леми 4.7 і тому

$$(-i)(r + s) = -(r + s) = -s - r.$$

З іншого боку,

$$(-i)(r + s) = (-i)r + (-i)s = -r - s$$

за лівою дистрибутивністю. Отже, $-s - r = -r - s$ і, таким чином, $r + s = s + r$, як стверджується. □

З іншого боку, адитивні групи напівдистрибутивних майже-кілець без одиниці не повинні бути абелевими, як показує наступний приклад.

Приклад 4.9. Нехай N — майже-кілець, адитивна група якого N^+ ізоморфна симетричній групі степеня 3. Тоді $N^+ = \langle a \rangle + \langle b \rangle$ з $a \cdot 3 = b \cdot 2 = 0$ і $b + a + b = a \cdot 2$. Зокрема, кожен елемент N^+ можна однозначно записати у вигляді $a \cdot m + b \cdot n$ з $0 \leq m \leq 2$ і $0 \leq n \leq 1$. Множення $*$ на N^+ визначимо наступною таблицею:

$*$	0	a	$a \cdot 2$	b	$a + b$	$a \cdot 2 + b$
0	0	0	0	0	0	0
a	0	$a + b$	$a + b$	0	0	$a + b$
$a \cdot 2$	0	b	b	0	0	b
b	0	0	0	0	0	0
$a + b$	0	0	0	0	0	0
$a \cdot 2 + b$	0	$a \cdot 2 + b$	$a \cdot 2 + b$	0	0	$a \cdot 2 + b$

Аналізуючи таблицю з прикладу 4.9, можна побачити, що $(N, +, *)$ є майже-кільцем, яке є напівдистрибутивним і нуль-симетричним.

Зауважимо, що пакет SONATA системи комп'ютерної алгебри GAP містить бібліотеку всіх майже-кілець порядку не більше 15. Зокрема, існує 39 неізоморфних майже-кілець, адитивні групи яких ізоморфні симетричній групі степеня 3, серед яких лише 4 напівдистрибутивні, у тому числі, 2 дистрибутивні.

Лема 4.10. *Нехай R — напівдистрибутивне майже-кільце з одиницею. Якщо адитивна група R^+ без скруту, то R є кільцем.*

Доведення. Очевидно, що достатньо довести, що в R виконується правий дистрибутивний закон. Дійсно, оскільки адитивна група R^+ є абелевою за лемою 4.8, для будь-яких елементів $r, s, t \in R$ маємо

$$\begin{aligned}
 (r + s)t &= (r + s + (-(r + s)) + s + r)t = \\
 &= rt + (s + (-(r + s)) + s)t + rt = \\
 &= rt2 + st2 + (-(r + s))t
 \end{aligned}$$

і $(-(r + s))t = -(r + s)t$ за твердженням (1) леми 4.7. Отже, $((r + s)t - rt - st)2 = 0$, звідки $(r + s)t = rt + st$, як стверджується. $\square$

4.1.2. Дистрибутивні елементи в напівдистрибутивних майже-кільцях

Нагадаємо, що елемент t майже-кільця R називається дистрибутивним в R , якщо $(r + s)t = rt + st$ для будь-яких елементів $r, s \in R$.

Лема 4.11. *Нехай R — напівдистрибутивне майже-кільце з одиницею. Тоді елементи непарних порядків адитивної групи R є дистрибутивними в R . Зокрема, кожне напівдистрибутивне майже-кільце непарного порядку є кільцем.*

Доведення. Нехай t — елемент непарного порядку n в R^+ і $m = \frac{n+1}{2}$. Тоді $u = tm$ є елементом порядку n і $t = u + u$. Оскільки майже-кільце R є напівдистрибутивним, для будь-яких елементів $r, s \in R$ маємо

$$(r + s)u = (r + (s - r) + r)u = ru + (s - r)u + ru$$

і аналогічно

$$(s + r)u = (s + (r - s) + s)u = su + (r - s)u + su.$$

Крім того, як $r + s = s + r$ за лемою 4.8 і

$$(r - s)u = (-(s - r))u = -(s - r)u$$

за твердженням (1) леми 4.7 випливає, що

$$(r + s)u = ru + (s - r)u + ru = su - (s - r)u + su.$$

Тому

$$(r + s)t = (r + s)(u + u) = r(u + u) + s(u + u) = rt + st,$$

отже, елемент t є дистрибутивним. Зокрема, якщо R має непарний порядок, то R є дистрибутивним майже-кільцем з одиницею, отже, кільцем. $\square$

Нагадаємо, що поняття *підмайже-кілеця* та *майже-кілецевого гомоморфізму* визначаються так само, як і для кілець. Зокрема, якщо λ є майже-кілецевим гомоморфізмом R , то його ядро $\text{Ker } \lambda$ є підмайже-кілецем R , адитивна підгрупа якого нормальна в R^+ . Підмайже-кілеце I з R є ідеалом в R , якщо $I = \text{Ker } \lambda$ для деякого λ . Можна просто перевірити, що I є ідеалом R тоді і тільки тоді, коли I^+ є нормальною підгрупою R^+ і для будь-яких елементів $r, s \in R$ і $a \in I$ виконуються включення $ra \in I$ та $(r + a)s - rs \in I$.

Лема 4.12. *Нехай R — напівдистрибутивне майже-кілеце з одиницею. Якщо p — просте число, а P — p -компонента адитивної групи R^+ , то P — ідеал в R .*

Доведення. Оскільки адитивна група R^+ є абелевою за лемою 4.8, кожен p -елемент з R належить до P і для кожного $a \in P$ існує таке натуральне число n , що $ap^n = 0$. Оскільки

$$(ra)p^n = r(ap^n) = r0 = 0$$

для кожного $r \in R$, це означає $ra \in P$. Таким чином, щоб довести, що P є ідеалом R , залишається показати, що для кожного $s \in R$ елемент $x = (r + a)s - rs$ належить P .

Припустимо спочатку, що p непарне, тому a має непарний порядок. Тоді існує елемент $b \in P$ такого ж порядку, що $a = b + b$. Поклавши $t = s + s$, ми маємо

$$x = (b + r + b)s - rs = bs + rs + bs - rs = bs + bs = bt$$

і тому

$$xp^n = (bt)p^n = (bp^n)t = 0t = 0$$

за твердженням (2) леми 4.8. Тому $x = 0 \in P$, як вимагалось.

Нехай тепер $p = 2$, отже $a2^n = 0$. Тоді

$$x2^n = ((r + a)s - rs)2^n = ((r + a)s)2^n - (rs)2^n.$$

Далі, застосовуючи твердження (2) леми 4.7, маємо

$$\begin{aligned} ((r + a)s)2^n + 0s &= ((r + a)2^n)s = \\ &= (r2^n + a2^n)s = (r2^n)s = (rs)2^n + 0s. \end{aligned}$$

З цього випливає, що

$$((r + a)s)2^n = (rs)2^n$$

і, отже,

$$x2^n = ((r + a)s)2^n - (rs)2^n = 0.$$

Отже, $x \in P$ і це завершує доведення. $\square$

4.1.3. Модулі над майже-кільцями та напівдистрибутивність

Нехай R — майже-кільце, а G — адитивна група. Тоді G називається (правим) R -модулем, якщо для будь-яких елементів $g \in G$ та $r \in R$ існує єдиний елемент $gr \in G$ такий, що $(gr)s = g(rs)$ та $g(r + s) = gr + gs$ для кожного $s \in R$. Зрозуміло, що адитивна група майже-кільця R є R -модулем над R відносно майже-кільцевого множення справа як дії. Крім того, якщо H є підмножиною R -модуля G , то множина $\text{Ann}_R(H) = \{x \in R \mid Hx = 0\}$ називається (правим) анулятором H в R . R -модуль G називається *точним*, якщо $\text{Ann}_R(G) = 0$.

Лема 4.13. *Якщо R — майже-кільце, а G — R -модуль, то анулятор $\text{Ann}_R(G)$ — ідеал R .*

Доведення. Дійсно, нехай $g \in G$ та $x \in \text{Ann}_R(G)$. Оскільки $gr \in G$ для кожного $r \in R$, то випливає, що $g(rx) = (gr)x = 0$. Отже, $rx \in \text{Ann}_R(G)$,

а тому $\text{Ann}_R(G)$ є лівим ідеалом R . Щоб довести, що $\text{Ann}_R(G)$ є ідеалом R , достатньо показати, що для будь-яких $r, s \in R$ елемент $t = (r + x)s - rs$ належить $\text{Ann}_R(G)$. Оскільки G є R -модулем і $gx = 0$, маємо $g(r + x) = gr + gx = gr$ і тому

$$\begin{aligned} gt &= g((r + x)s) + g(-rs) = (g(r + x))s + g(-rs) = \\ &= g(rs) + g(-rs) = g0 = 0. \end{aligned}$$

Це означає, що $t \in \text{Ann}_R(G)$, і таким чином $\text{Ann}_R(G)$ є ідеалом R , як і стверджувалося. $\square$

Наступна лема доведена в [65, Лема 3.7].

Лема 4.14. *Нехай R — майже-кільце, а G — R -модуль з властивостями:*

- (i) G є точним як R -модуль,
- (ii) $(G, +)$ є абелевою групою,
- (iii) для кожного $r \in R$ відображення $\hat{r}: G \rightarrow G$, задане як $\hat{r}: g \rightarrow gr$, є ендоморфізмом G .

Тоді R є кільцем.

Доведення. Нехай s, t — елементи R та $r = s + t$. Тоді

$$gr = g(s + t) = gs + gt = gt + gs = g(t + s)$$

за властивістю (ii). Крім того, з (iii) випливає, що

$$\begin{aligned} g(s + t)r &= (gs + gt)^{\hat{r}} = \\ &= (gs)r + (gt)r = g(sr + tr). \end{aligned}$$

Зрештою, оскільки R -модуль G є точним згідно з (i), це означає $(s + t)r = sr + tr$, а отже, R є дистрибутивним кільцем. $\square$

Теорема 4.15. *Напівдистрибутивне майже-кільце R з одиницею є простим як майже-кільце тоді і тільки тоді, коли R є простим асоціативним кільцем.*

Доведення. Як зазначалося вище, адитивну групу $G = R^+$ можна розглядати як R -модуль над R відносно майже-кільцевого множення справа як дії. Якщо майже-кільце R просте, воно не має власних ідеалів, а отже $\text{Ann}(R(G)) = 0$ за лемою 4.13. Отже, G є точним як R -модуль, а $G = R^+$ є абелевою групою за лемою 4.8. Зрештою, для кожного $r \in R$ відображення $\rho: G \rightarrow G$, задане як $\rho: g \rightarrow gr$, є ендоморфізмом G , оскільки

$$\rho(g + h) = r(g + h) = rg + rh = \rho(g) + \rho(h)$$

для кожного $g, h \in G$. Застосовуючи тепер лему 4.14, виводимо, що R — просте кільце. Зворотнє очевидне. $\square$

4.2. Скінченні напівдистрибутивні локальні майже-кільця

Мексон показав у [63], що кожна нециклічна абелева p -група порядку $p^n > 4$ є адитивною групою нуль-симетричного локального майже-кільця, яке не є кільцем.

Означення 4.16. Майже-кільце R з одиницею називається локальним, якщо множина $L = R \setminus R^*$ усіх необоротних елементів R є підгрупою R^+ .

Наступна лема характеризує основні властивості скінченних локальних майже-кілець (див. [18]).

Лема 4.17. *Нехай R — скінченне локальне майже-кільце з одиницею i , а L — підгрупа R^+ усіх необоротних елементів з R . Тоді R^+ — це*

p -група для деякого простого числа p , експонента якого є адитивним порядком одиниці i .

Наступний результат визначає структурну особливість скінченних локальних майже-кілець.

Твердження 4.18. *Кожне нетривіальне підмайже-кілець з одиницею скінченного локального майже-кілля є локальним майже-кіллям.*

Доведення. Нехай $R = (R, +, \cdot)$ — скінченне локальне майже-кілець, а L — підгрупа R^+ усіх необоротних елементів з R . Нехай R_1 — нетривіальне підкілець з одиницею в R , а $(L_1, +)$ — напівгрупа необоротних елементів R_1 . Оскільки $(L_1, +)$ є піднапівгрупою L , то $(L_1, +)$ є підгрупою L , а отже, підгрупою в R_1^+ . Отже, R_1 є локальним майже-кіллям за визначенням. Твердження доведено. $\square$

Як прямий наслідок із лем 4.8, 4.11 та 4.17 маємо таке твердження.

Лема 4.19. *Нехай R — скінченне напівдистрибутивне локальне майже-кілець, яке не є кіллям. Тоді R^+ є абелевою 2-групою.*

Нехай R — скінченне напівдистрибутивне локальне майже-кілець на 2-породженній 2-групі R^+ . Отже, R^+ є абелевою групою типу $(2^m, 2^n)$ з $m \geq n \geq 1$ як наслідок з леми 4.19. Нехай $|R : L| = 2^k$ з $1 \leq k < m + n$. Тоді $R^+ = \langle a \rangle + \langle b \rangle$, де $a2^m = b2^n = 0$ з $m \geq n \geq 1$ і $a+b = b+a$. Отже, R^+ має експоненту 2^m і, отже, a співпадає з одиницею R за лемою 4.17. Крім того, кожен елемент $x \in R$ однозначно записується у вигляді $x = ax_1 + bx_2$ з коефіцієнтами $0 \leq x_1 < 2^m$ і $0 \leq x_2 < 2^n$. Отже, $xa = ax = x$ для кожного $x \in R$. Крім того, для кожного $x \in R$ існують такі однозначно визначені цілі $\alpha(x) \in Z_{2^m}$ і $\beta(x) \in Z_{2^n}$, що $xb = a\alpha(x) + b\beta(x)$ і тому деякі відображення $\alpha : R \rightarrow Z_{2^m}$ і $\beta : R \rightarrow Z_{2^n}$ визначені. Таким чином, $b \in L$, звідки $L = \langle a2^k \rangle + \langle b \rangle$. Крім того, $R^* = R \setminus L$, отже, елемент $x = ax_1 + bx_2$ належить до R^* тоді і тільки тоді, коли $x_1 \not\equiv 0 \pmod{2^k}$.

Лема 4.20. Нехай $x = ax_1 + bx_2$ і $y = ay_1 + by_2$ є елементами R . Тоді

$$xy = a(x_1y_1 + \alpha(x)y_2) + b(x_2y_1 + \beta(x)y_2).$$

Крім того, для відображень $\alpha : R \rightarrow Z_{2^m}$ і $\beta : R \rightarrow Z_{2^n}$ виконуються такі твердження:

(0) $\alpha(0) = \beta(0) = 0$ тоді і тільки тоді, коли майже-кільце R є нуль-симетричним;

(1) $\alpha(a) = 0$ і $\beta(a) = 1$;

(2) $\alpha(x) \equiv 0 \pmod{2^{m-n}}$;

(3) $\alpha(xy) = x_1\alpha(y) + \alpha(x)\beta(y)$;

(4) $\beta(xy) = x_2\alpha(y) + \beta(x)\beta(y)$.

Доведення. Оскільки $0 \cdot a = an \cdot 0 = 0$, майже-кільце R є нуль-симетричним тоді і тільки тоді, коли

$$0 = 0 \cdot b = a\alpha(0) + b\beta(0).$$

Звідси $\alpha(0) = \beta(0) = 0$, доводить твердження (0). Крім того, з рівності

$$b = ab = a\alpha(a) + b\beta(a)$$

випливає, що $\alpha(a) = 0$ та $\beta(a) = 1$, і тому виконується твердження (1).

Далі, згідно з лівим дистрибутивним законом, маємо

$$xy = (xa)y_1 + (xb)y_2 = (ax_1 + bx_2)y_1 + (a\alpha(x) + b\beta(x))y_2 = \quad (4.1)$$

$$= ax_1y_1 + bx_1y_1 + a\alpha(x)y_2 + b\beta(x)y_2 =$$

$$= a(x_1y_1 + \alpha(x)y_2) + b(x_2y_1 + \beta(x)y_2)$$

ЯК ВИМАГАЛОСЯ.

Далі, за формулою (4.1) для $y = b2^n = 0$ маємо

$$0 = x(b2^n) = a\alpha(x)2^n.$$

Таким чином, $\alpha(x) \equiv 0 \pmod{2^{m-n}}$, як стверджується в (2).

Зрештою, асоціативність множення в R означає, що

$$x(yb) = (xy)b = a\alpha(xy) + b\beta(xy).$$

Крім того, підставляючи $yb = a\alpha(y) + b\beta(y)$ замість y у формулу (4.1), також маємо

$$xy = a((x_1\alpha(y) + \alpha(x)\beta(y)) + b(x_2\beta(y) + \beta(x)\beta(y))).$$

Порівнюючи коефіцієнти при a та b у двох виразах, отриманих для $x(yb)$, отримуємо твердження (3) та (4) леми. $\square$

Теорема 4.21. *Нехай R — напівдистрибутивне локальне майже-кільце, адитивна група якого R^+ ізоморфна абелевій групі типу $(2^m, 2^n)$ з $m \geq n > 1$. Тоді напівгрупа $(L, \cdot)$ є комутативною.*

Доведення. Якщо $x = ax_1 + bx_2$ і $y = ay_1 + by_2 \in L$, то $x_1 \equiv 0 \pmod{2^k}$ і $y_1 \equiv 0 \pmod{2^k}$. Нехай $x_1 = 2s$ і $y_1 = 2t$, де $s, t \in N$. Тоді для кожного $x, y \in L$ з використанням лівого дистрибутивного і напівдистрибутивного законів маємо:

$$\begin{aligned} xy &= (ax_1 + bx_2)y = (a2s + bx_2)y = (as + bx_2 + as)y = \\ &= (as)y + (bx_2)y + (as)y = as(y + y) + (bx_2)y = \\ &= (as)(y2) + (bx_2)y = as(a2y_1 + b2y_2) + bx_2(ay_1 + by_2) = \\ &= a2sy_1 + b2sy_2 + bx_2y_1 + a\alpha(b)x_2y_2 + b\beta(b)x_2y_2 = \\ &= ax_1y_1 + bx_1y_2 + bx_2y_1 + a\alpha(b)x_2y_2 + b\beta(b)x_2y_2 = \\ &= a(x_1y_1 + \alpha(b)x_2y_2) + b(x_1y_2 + x_2y_1 + \beta(b)x_2y_2). \end{aligned}$$

При цьому отримуємо:

$$\begin{aligned}
 yx &= (ay_1 + by_2)x = (a2t + by_2)x = (at + by_2 + at)x = \\
 &= (at)x + (by_2)x + (at)x = at(x + x) + (by_2)x = \\
 &= (at)(x_2) + (by_2)x = at(a2x_1 + b2x_2) + by_2(ax_1 + bx_2) = \\
 &= a2tx_1 + b2tx_2 + by_2x_1 + a\alpha(b)x_2y_2 + b\beta(b)x_2y_2 = \\
 &= ax_1y_1 + bx_2y_1 + bx_1y_2 + a\alpha(b)x_2y_2 + b\beta(b)x_2y_2 = \\
 &= a(x_1y_1 + \alpha(b)x_2y_2) + b(x_1y_2 + x_2y_1 + \beta(b)x_2y_2).
 \end{aligned}$$

Тому $xy = yx$ для кожного $x, y \in L$ і тому $(L, \cdot)$ є комутативним, як і стверджувалося. $\square$

Як приклад, існує 1068 неізоморфних локальних майже-кілець на 2-породжених абелевих 2-групах порядку не більше 32, серед яких 42 є напівдистрибутивними. Наступну таблицю отримано з пакетів SONATA та LocalNR системи комп'ютерної алгебри GAP.

Адитивна група	Кількість локальних майже-кілець	Кількість напівдистрибутивних локальних майже-кілець
$C_2 \oplus C_2$	2	2
$C_4 \oplus C_2$	5	5
$C_4 \oplus C_4$	29	9
$C_8 \oplus C_2$	23	5
$C_8 \oplus C_4$	880	16
$C_{16} \oplus C_2$	129	5

Висновки до розділу 4

У даному розділі:

- введено та досліджено напівдистрибутивні майже-кілеця з одиницею;
- вивчено напівгрупу необоротних елементів локальних майже-кілець, адитивна група якого ізоморфна абелевій групі типу $(2^m, 2^n)$ з $m \geq n > 1$.

Основні результати даного розділу опубліковано у працях [9, 10] зі списку публікацій і, відповідно, [97], [105] зі списку використаних джерел, а також опубліковано у тезах конференцій [33, 39] і, відповідно, [75], [72].

Розділ 5

Майже-кільцеві брейси та локальні майже-кільця

Використовуючи пакет YangBaxter [119], надаємо класифікації p -брейсів (до порядку 32) та косих p -брейсів (до порядку 16) відповідно до адитивних або мультиплікативних груп, які є p -групами Міллера–Морено. Крім того, ми надаємо деяку інформацію щодо майже-кільцевих брейсів, що стосуються, пакету LocalNR.

5.1. Брейси та косі брейси

Для скінченного брейса $A = (A, +, \circ)$, де $(A, +)$ та $(A, \circ)$ — такі дві абелеві групи, що $a \circ (b + c) = a \circ b - a + a \circ c$ виконується для всіх $a, b, c \in A$.

Якщо адитивна група є циклічною, то брейс A називається циклічним.

Косий брейс — це трійка $(A, +, \circ)$, де $(A, +)$ та $(A, \circ)$ — дві (не обов’язково абелеві) групи такі, що рівність $a \circ (b + c) = a \circ b - a + a \circ c$ виконується для всіх $a, b, c \in A$.

Румп [110] класифікував брейси двох типів: $(A, +)$ — циклічна p -група; $(A, +)$ — циклічна група така, що $(A, \circ)$ також є циклічною.

Кватерніонний брейс — це брейс, мультиплікативна група якого ізоморфна деякій узагальненій групі кватерніонів Q_{2^m} . Румп [112] встановив повну класифікацію кватерніонних брейсів порядку ≥ 32 .

З огляду на вищезазначені результати, наступним природним кроком є розгляд брейсів та косих брейсів, адитивні та мультиплікативні групи яких є мінімальними неабелевими або, в іншій термінології, групами Міллера–Морено.

Нагадаємо, що скінченна група називається групою Міллера–Морено, якщо вона неабелева, а всі її власні підгрупи є абелевими. Структура цих груп повністю описується відомою теоремою Редеї.

Далі, ми зосередимося на брейсах та косих брейсах порядку p^n , які ми також називаємо p -брейсами та p -косими брейсами, відповідно.

Ми кажемо, що p -брейс (p -косий брейс) є Міллера–Морено, якщо його мультиплікативна (спряжена) група є p -групою Міллера–Морено.

Далі, наведемо означення локального майже-кільця зі статті Румпа [111], а також означення розщеплювального локального майже-кільця та майже кільцевого брейса з цієї роботи.

Означення 5.1. [111] Майже-кільце N називається локальним, якщо N є майже-кільце з одиницею, а елементи $r \in N$ з $Nr = N$ утворюють підмодуль $J(N)$, радикал N . Тоді $N^* = N \setminus J(N)$.

Означення 5.2. [111, Definition 9] Ми кажемо, що локальне майже-кільце N розщеплюється, якщо існує підмайже-поле K для N з $N = K \oplus J(N)$ як адитивними групами. Якщо K можна вибрати підмайже-полем центру

$$Z(N) = \{r \in N : \forall s \in N : rs = sr\},$$

то кажемо, що N повністю розщеплюється.

Зауваження 5.3. [111] Якщо N повністю розщеплюване, то будь-яке майже-поле $K \subset Z(N)$ є комутативним, а отже, полем.

Означення 5.4. [111, Definition 10] Визначимо майже-кільцевий брейс як брейс A з такою майже-кільцевою структурою, що $(ab)c = a(bc)$ та $a(bc + c) = (ab)c$ виконуються для всіх $a, b, c \in A$. Якщо A є K -лінійним як брейс та як майже-кільце, ми говоримо про майже-кільцевий K -брейс.

Наступний приклад випливає з [111, Example 8].

Приклад 5.5. Нехай N — локальне майже-кільце. Радикал $J(N)$ — це косий брейс.

Теорема 5.6. [111, Theorem 5] Нехай K — поле. З точністю до ізоморфізму, $N \mapsto J(N)$ задає бієкцію між повністю розщепленими локальними майже-кільцями N з $N/J(N) \cong K$ та майже-кільцевими K -брейсами.

5.2. Брейси з пакету YangBaxter

Пакет YangBaxter надає функціональність для побудови класичних та косих брейсів. Він також включає базу даних класичних та косих брейсів малих порядків.

Пакет YangBaxter містить бібліотеки брейсів *AllBraces* та косих брейсів *AllSmallSkewbraces* малого порядку. У цих бібліотеках брейси впорядковуються відповідно до їхнього порядку, і, наприклад, команди $B := \text{AllBraces}(n)$ та $S := \text{AllSmallSkewbraces}(n)$ визначають списки брейсів B та косих брейсів S порядку n , відповідно. Наприклад, брейси порядків 64 та 128 не реалізовані в бібліотеці *AllBraces*.

Функції для отримання мультиплікативних та адитивних груп брейсів (косих брейсів) — це *UnderlyingMultiplicativeGroup* та *UnderlyingAdditiveGroup*, відповідно. Пакет містить функції для виводу списків всіх брейсів та косих брейсів заданого порядку, тобто *AllSmallBraces* та *AllSmallSkewbraces*, відповідно.

Нехай $[n, i]$ — i -та група порядку n у бібліотеці SmallGroups в системі GAP. Позначимо через C_n , D_n та Q_n циклічну групу, групу дієдра та групу кватерніонів порядку n , відповідно.

Твердження 5.7. *Нехай $(A, +, \circ)$ — Міллера–Морено p -брейс до порядку 32. Тоді $(A, \circ)$ ізоморфна одній з наступних груп:*

- 1) D_8 [8, 3];
- 2) Q_8 [8, 4];
- 3) $(C_4 \times C_2) \rtimes C_2$ [16, 3];
- 4) $C_4 \rtimes C_4$ [16, 4];
- 5) $C_8 \rtimes C_2$ [16, 6];
- 6) $(C_4 \times C_2) \rtimes C_4$ [32, 2];
- 7) $C_8 \rtimes C_4$ [32, 4];
- 8) $(C_8 \times C_2) \rtimes C_2$ [32, 5];
- 9) $C_4 \rtimes C_8$ [32, 12];
- 10) $C_{16} \rtimes C_2$ [32, 17].

Наведемо класифікацію брейсів Міллера–Морено з мультиплікативною групою ізоморфною групі D_8 [8, 3].

Твердження 5.8. *Існує 8 брейсів Міллера–Морено з*

$$(A, \circ) \cong D_8 [8, 3],$$

тобто:

- 1 брейс з адитивною групою
 $(A, +) \cong C_8 [8, 1];$

- 5 брейсів з адитивною групою

$$(A, +) \cong C_4 \times C_2 [8, 2];$$

- 2 брейси з адитивною групою

$$(A, +) \cong C_2 \times C_2 \times C_2 [8, 5].$$

Наведемо класифікацію брейсів Міллера–Морено з мультиплікативною групою ізоморфною групі Q_8 [8, 4].

Твердження 5.9. *Існує 3 брейсів Міллера–Морено з*

$$(A, \circ) \cong Q_8 [8, 4],$$

тобто:

- 1 брейс з адитивною групою

$$(A, +) \cong C_8 [8, 1];$$

- 1 брейс з адитивною групою

$$(A, +) \cong C_4 \times C_2 [8, 2];$$

- 1 брейс з адитивною групою

$$(A, +) \cong C_2 \times C_2 \times C_2 [8, 5].$$

Наведемо класифікацію брейсів Міллера–Морено з мультиплікативною групою ізоморфною групі $(C_4 \times C_2) \rtimes C_2$ [16, 3].

Твердження 5.10. *Існує 65 брейсів Міллера–Морено з*

$$(A, \circ) \cong (C_4 \times C_2) \rtimes C_2 [16, 3],$$

тобто:

- 19 брейсів з адитивною групою

$$(A, +) \cong C_4 \times C_4 [16, 2];$$

- 2 брейси з адитивною групою

$$(A, +) \cong C_8 \times C_2 [16, 5];$$

- 36 брейсів з адитивною групою

$$(A, +) \cong C_4 \times C_2 \times C_2 [16, 10];$$

- 8 брейсів з адитивною групою

$$(A, +) \cong C_2 \times C_2 \times C_2 \times C_2 [16, 14].$$

Наведемо класифікацію брейсів Міллера–Морено з мультиплікативною групою ізоморфною групі $C_4 \rtimes C_4$ [16, 4].

Твердження 5.11. *Існує 45 брейсів Міллера–Морено з*

$$(A, \circ) \cong C_4 \rtimes C_4 [16, 4],$$

тобто:

- 14 брейсів з адитивною групою

$$(A, +) \cong C_4 \times C_4 [16, 2];$$

- 4 брейси з адитивною групою

$$(A, +) \cong C_8 \times C_2 [16, 5];$$

- 23 брейсів з адитивною групою

$$(A, +) \cong C_4 \times C_2 \times C_2 [16, 10];$$

- 4 брейси з адитивною групою

$$(A, +) \cong C_2 \times C_2 \times C_2 \times C_2 [16, 14].$$

Наведемо класифікацію брейсів Міллера–Морено з мультиплікативною групою ізоморфною групі $C_8 \rtimes C_2$ [16, 6].

Твердження 5.12. *Існує 11 брейсів Міллера–Морено з*

$$(A, \circ) \cong C_8 \rtimes C_2 [16, 6],$$

тобто:

- 1 брейс з адитивною групою

$$(A, +) \cong C_{16} [16, 1];$$

- 2 брейси з адитивною групою
 $(A, +) \cong C_4 \times C_4$ [16, 2];
- 6 брейсів з адитивною групою
 $(A, +) \cong C_8 \times C_2$ [16, 5];
- 1 брейс з адитивною групою
 $(A, +) \cong C_4 \times C_2 \times C_2$ [16, 10];
- 1 брейс з адитивною групою
 $(A, +) \cong C_2 \times C_2 \times C_2 \times C_2$ [16, 14].

Наведемо класифікацію брейсів Міллера–Морено з мультиплікативною групою ізоморфною групі $(C_4 \times C_2) \rtimes C_4$ [32, 2].

Твердження 5.13. *Існує 296 брейсів Міллера–Морено з*

$$(A, \circ) \cong (C_4 \times C_2) \rtimes C_4 \text{ [32, 2],}$$

тобто:

- 6 брейсів з адитивною групою
 $(A, +) \cong C_8 \times C_4$ [32, 3];
- 125 брейсів з адитивною групою
 $(A, +) \cong C_4 \times C_4 \times C_2$ [32, 21];
- 8 брейсів з адитивною групою
 $(A, +) \cong C_8 \times C_2 \times C_2$ [32, 36];
- 135 брейсів з адитивною групою
 $(A, +) \cong C_4 \times C_2 \times C_2 \times C_2$ [32, 45];
- 22 брейси з адитивною групою
 $(A, +) \cong C_2 \times C_2 \times C_2 \times C_2 \times C_2$ [32, 51].

Наведемо класифікацію брейсів Міллера–Морено з мультиплікативною групою ізоморфною групі $C_8 \rtimes C_4$ [32, 4].

Твердження 5.14. *Існує 30 брейсів Міллера–Морено з*

$$(A, \circ) \cong C_8 \rtimes C_4 \text{ [32, 4],}$$

тобто:

- 18 брейсів з адитивною групою
 $(A, +) \cong C_8 \times C_4$ [32, 3];
- 2 брейси з адитивною групою
 $(A, +) \cong C_{16} \times C_2$ [32, 16];
- 10 брейсів з адитивною групою
 $(A, +) \cong C_8 \times C_2 \times C_2$ [32, 36].

Наведемо класифікацію брейсів Міллера–Морено з мультиплікативною групою ізоморфною групі $(C_8 \times C_2) \rtimes C_2$ [32, 5].

Твердження 5.15. *Існує 101 брейсів Міллера–Морено з*

$$(A, \circ) \cong (C_8 \times C_2) \rtimes C_2 \text{ [32, 5],}$$

тобто:

- 30 брейсів з адитивною групою
 $(A, +) \cong C_8 \times C_4$ [32, 3];
- 2 брейси з адитивною групою
 $(A, +) \cong C_{16} \times C_2$ [32, 16];
- 15 брейсів з адитивною групою
 $(A, +) \cong C_4 \times C_4 \times C_2$ [32, 21];
- 36 брейсів з адитивною групою
 $(A, +) \cong C_8 \times C_2 \times C_2$ [32, 36];

- 12 брейсів з адитивною групою
 $(A, +) \cong C_4 \times C_2 \times C_2 \times C_2$ [32, 45];
- 6 брейсів з адитивною групою
 $(A, +) \cong C_2 \times C_2 \times C_2 \times C_2 \times C_2$ [32, 51].

Наведемо класифікацію брейсів Міллера–Морено з мультиплікативною групою ізоморфною групі $C_4 \rtimes C_8$ [32, 12].

Твердження 5.16. *Існує 48 брейсів Міллера–Морено з*

$$(A, \circ) \cong C_4 \rtimes C_8 \text{ [32, 12],}$$

тобто:

- 26 брейсів з адитивною групою
 $(A, +) \cong C_8 \times C_4$ [32, 3];
- 2 брейси з адитивною групою
 $(A, +) \cong C_{16} \times C_2$ [32, 16];
- 20 брейсів з адитивною групою
 $(A, +) \cong C_8 \times C_2 \times C_2$ [32, 36].

Наведемо класифікацію брейсів Міллера–Морено з мультиплікативною групою ізоморфною групі $C_{16} \rtimes C_2$ [32, 17].

Твердження 5.17. *Існує 12 брейсів Міллера–Морено з*

$$(A, \circ) \cong C_{16} \rtimes C_2 \text{ [32, 17],}$$

тобто:

- 1 брейс з адитивною групою
 $(A, +) \cong C_{32}$ [32, 1];
- 11 брейсів з адитивною групою
 $(A, +) \cong C_{16} \times C_2$ [32, 16].

5.3. Косі брейси з пакету YangBaxter

Застосовуючи систему GAP та пакет YangBaxter, наведемо класифікацію косих брейсів з мультиплікативними та адитивними групами Міллера–Морено малих порядків.

Твердження 5.18. *Нехай $(A, +, \circ)$ — косий p -брейс Міллера–Морено до порядку 16. Тоді $(A, \circ)$ ізоморфна одній з наступних груп:*

- 1) D_8 [8, 3];
- 2) Q_8 [8, 4];
- 3) $(C_4 \times C_2) \rtimes C_2$ [16, 3];
- 4) $C_4 \rtimes C_4$ [16, 4];
- 5) $C_8 \rtimes C_2$ [16, 6].

Наведемо класифікацію косих брейсів Міллера–Морено з мультиплікативною групою ізоморфною групі D_8 [8, 3].

Твердження 5.19. *Існує 14 косих брейсів Міллера–Морено з*

$$(A, \circ) \cong D_8 [8, 3],$$

тобто:

- 1 косий брейс з адитивною групою
 $(A, +) \cong C_8$ [8, 1];
- 5 косих брейсів з адитивною групою
 $(A, +) \cong C_4 \times C_2$ [8, 2];
- 4 косих брейси з адитивною групою
 $(A, +) \cong D_8$ [8, 3];

- 2 косих брейси з адитивною групою
 $(A, +) \cong Q_8$ [8, 4];
- 2 косих брейси з адитивною групою
 $(A, +) \cong C_2 \times C_2 \times C_2$ [8, 5].

Наведемо класифікацію косих брейсів Міллера–Морено з мультиплікативною групою ізоморфною групі Q_8 [8, 4].

Твердження 5.20. *Існує 7 косих брейсів Міллера–Морено з*

$$(A, \circ) \cong Q_8$$
 [8, 4],

тобто:

- 1 косий брейс з адитивною групою
 $(A, +) \cong C_8$ [8, 1];
- 1 косий брейс з адитивною групою
 $(A, +) \cong C_4 \times C_2$ [8, 2];
- 2 косих брейси з адитивною групою
 $(A, +) \cong D_8$ [8, 3];
- 2 косих брейси з адитивною групою
 $(A, +) \cong Q_8$ [8, 4];
- 1 косий брейс з адитивною групою
 $(A, +) \cong C_2 \times C_2 \times C_2$ [8, 5].

Наведемо класифікацію косих брейсів Міллера–Морено з мультиплікативною групою ізоморфною групі $(C_4 \times C_2) \rtimes C_2$ [16, 3].

Твердження 5.21. *Існує 189 косих брейсів Міллера–Морено з*

$$(A, \circ) \cong (C_4 \times C_2) \rtimes C_2$$
 [16, 3],

тобто:

- 19 косих брейсів з адитивною групою
 $(A, +) \cong C_4 \times C_4$ [16, 2];
- 43 косих брейсів з адитивною групою
 $(A, +) \cong (C_4 \times C_2) \rtimes C_2$ [16, 3];
- 36 косих брейсів з адитивною групою
 $(A, +) \cong C_4 \rtimes C_4$ [16, 4];
- 2 косих брейси з адитивною групою
 $(A, +) \cong C_8 \times C_2$ [16, 5];
- 2 косих брейси з адитивною групою
 $(A, +) \cong C_8 \rtimes C_2$ [16, 6];
- 36 косих брейсів з адитивною групою
 $(A, +) \cong C_4 \times C_2 \times C_2$ [16, 10];
- 30 косих брейсів з адитивною групою
 $(A, +) \cong C_2 \times D_8$ [16, 11];
- 13 косих брейсів з адитивною групою
 $(A, +) \cong C_2 \times Q_8$ [16, 12];
- 8 косих брейсів з адитивною групою
 $(A, +) \cong C_2 \times C_2 \times C_2 \times C_2$ [16, 14].

Наведемо класифікацію косих брейсів Міллера–Морено з мультиплікативною групою ізоморфною групі $C_4 \rtimes C_4$ [16, 4].

Твердження 5.22. *Існує 162 косих брейсів Міллера–Морено з*

$$(A, \circ) \cong C_4 \rtimes C_4 \text{ [16, 4],}$$

тобто:

- 14 косих брейсів з адитивною групою
 $(A, +) \cong C_4 \times C_4$ [16, 2];
- 38 косих брейсів з адитивною групою
 $(A, +) \cong (C_4 \times C_2) \rtimes C_2$ [16, 3];
- 40 косих брейсів з адитивною групою
 $(A, +) \cong C_4 \rtimes C_4$ [16, 4];
- 4 косих брейси з адитивною групою
 $(A, +) \cong C_8 \times C_2$ [16, 5];
- 2 косих брейси з адитивною групою
 $(A, +) \cong C_8 \rtimes C_2$ [16, 6];
- 23 косих брейсів з адитивною групою
 $(A, +) \cong C_4 \times C_2 \times C_2$ [16, 10];
- 11 косих брейсів з адитивною групою
 $(A, +) \cong C_2 \times D_8$ [16, 11];
- 13 косих брейсів з адитивною групою
 $(A, +) \cong C_2 \times Q_8$ [16, 12];
- 4 косих брейси з адитивною групою
 $(A, +) \cong C_2 \times C_2 \times C_2 \times C_2$ [16, 14].

Наведемо класифікацію косих брейсів Міллера–Морено з мультиплікативною групою ізоморфною групі $C_8 \rtimes C_2$ [16, 6].

Твердження 5.23. *Існує 79 косих брейсів Міллера–Морено з*

$$(A, \circ) \cong C_8 \rtimes C_2 \text{ [16, 6],}$$

тобто:

- 1 косий брейс з адитивною групою
 $(A, +) \cong C_{16}$ [16, 1];
- 2 косих брейси з адитивною групою
 $(A, +) \cong C_4 \times C_4$ [16, 2];
- 2 косих брейси з адитивною групою
 $(A, +) \cong (C_4 \times C_2) \rtimes C_2$ [16, 3];
- 4 косих брейси з адитивною групою
 $(A, +) \cong C_4 \rtimes C_4$ [16, 4];
- 6 косих брейсів з адитивною групою
 $(A, +) \cong C_8 \times C_4$ [16, 5];
- 6 косих брейсів з адитивною групою
 $(A, +) \cong C_8 \rtimes C_4$ [16, 6];
- 8 косих брейсів з адитивною групою
 $(A, +) \cong D_{16}$ [16, 7];
- 16 косих брейсів з адитивною групою
 $(A, +) \cong QD_{16}$ [16, 8];
- 8 косих брейсів з адитивною групою
 $(A, +) \cong Q_{16}$ [16, 9];
- 1 косий брейс з адитивною групою
 $(A, +) \cong C_4 \times C_2 \times C_2$ [16, 10];
- 7 косих брейсів з адитивною групою
 $(A, +) \cong C_2 \times D_8$ [16, 11];
- 7 косих брейсів з адитивною групою
 $(A, +) \cong C_2 \times Q_8$ [16, 12];

- 8 косих брейсів з адитивною групою
 $(A, +) \cong (C_4 \times C_2) \rtimes C_2$ [16, 13];
- 1 косий брейс з адитивною групою
 $(A, +) \cong C_2 \times C_2 \times C_2 \times C_2$ [16, 14].

Твердження 5.24. *Нехай $(A, +, \circ)$ — косий p -брейс з адитивною групою Міллера–Морено $(A, +)$ до порядку 16. Тоді $(A, +)$ ізоморфна одній з наступних груп:*

- 1) D_8 [8, 3];
- 2) Q_8 [8, 4];
- 3) $(C_4 \times C_2) \rtimes C_2$ [16, 3];
- 4) $C_4 \rtimes C_4$ [16, 4];
- 5) $C_8 \rtimes C_2$ [16, 6].

Наведемо класифікацію косих брейсів з адитивною групою Міллера–Морено ізоморфною групі D_8 [8, 3].

Твердження 5.25. *Існує 12 косих брейсів з адитивною групою*

$$(A, +) \cong D_8 [8, 3],$$

тобто:

- 2 косих брейси з мультиплікативною групою
 $(A, \circ) \cong C_8$ [8, 1];
- 3 косих брейси з мультиплікативною групою
 $(A, \circ) \cong C_4 \times C_2$ [8, 2];
- 4 косих брейси з мультиплікативною групою
 $(A, \circ) \cong D_8$ [8, 3];

- 2 косих брейси з мультиплікативною групою
 $(A, \circ) \cong Q_8$ [8, 4];
- 1 косий брейс з мультиплікативною групою
 $(A, \circ) \cong C_2 \times C_2 \times C_2$ [8, 5].

Наведемо класифікацію косих брейсів з адитивною групою Міллера–Морено ізоморфною групі Q_8 [8, 4].

Твердження 5.26. *Існує 8 косих брейсів з адитивною групою*

$$(A, +) \cong Q_8$$
 [8, 4],

тобто:

- 2 косих брейси з мультиплікативною групою
 $(A, \circ) \cong C_8$ [8, 1];
- 1 косий брейс з мультиплікативною групою
 $(A, \circ) \cong C_4 \times C_2$ [8, 2];
- 2 косих брейси з мультиплікативною групою
 $(A, \circ) \cong D_8$ [8, 3];
- 2 косих брейси з мультиплікативною групою
 $(A, \circ) \cong Q_8$ [8, 4];
- 1 косий брейс з мультиплікативною групою
 $(A, \circ) \cong C_2 \times C_2 \times C_2$ [8, 5].

Наведемо класифікацію косих брейсів з адитивною групою Міллера–Морено ізоморфною групі $(C_4 \times C_2) \rtimes C_2$ [16, 3].

Твердження 5.27. *Існує 191 косих брейсів з адитивною групою*

$$(A, +) \cong (C_4 \times C_2) \rtimes C_2$$
 [16, 3],

тобто:

- 14 косих брейси з мультиплікативною групою $(A, \circ) \cong C_4 \times C_4$ [16, 2];
- 43 косих брейси з мультиплікативною групою $(A, \circ) \cong (C_4 \times C_2) \rtimes C_2$ [16, 3];
- 38 косих брейси з мультиплікативною групою $(A, \circ) \cong C_4 \rtimes C_4$ [16, 4];
- 2 косих брейси з мультиплікативною групою $(A, \circ) \cong C_8 \times C_2$ [16, 5];
- 2 косих брейси з мультиплікативною групою $(A, \circ) \cong C_8 \rtimes C_2$ [16, 6];
- 2 косих брейси з мультиплікативною групою $(A, \circ) \cong QD_{16}$ [16, 8];
- 2 косих брейси з мультиплікативною групою $(A, \circ) \cong Q_{16}$ [16, 9];
- 21 косих брейси з мультиплікативною групою $(A, \circ) \cong C_4 \times C_2 \times C_2$ [16, 10];
- 38 косих брейси з мультиплікативною групою $(A, \circ) \cong C_2 \times D_8$ [16, 11];
- 7 косих брейси з мультиплікативною групою $(A, \circ) \cong C_2 \times Q_8$ [16, 12];
- 19 косих брейси з мультиплікативною групою $(A, \circ) \cong (C_4 \times C_2) \rtimes C_2$ [16, 13];
- 3 косих брейси з мультиплікативною групою $(A, \circ) \cong C_2 \times C_2 \times C_2 \times C_2$ [16, 14].

Наведемо класифікацію косих брейсів з адитивною групою Міллера–Морено ізоморфною групі $C_4 \rtimes C_4$ [16, 4].

Твердження 5.28. *Існує 190 косих брейсів з адитивною групою*

$$(A, +) \cong C_4 \rtimes C_4 \text{ [16, 4],}$$

тобто:

- 12 косих брейсів з мультиплікативною групою $(A, \circ) \cong C_4 \times C_4$ [16, 2];
- 36 косих брейсів з мультиплікативною групою $(A, \circ) \cong (C_4 \times C_2) \rtimes C_2$ [16, 3];
- 40 косих брейсів з мультиплікативною групою $(A, \circ) \cong C_4 \rtimes C_4$ [16, 4];
- 4 косих брейси з мультиплікативною групою $(A, \circ) \cong C_8 \times C_2$ [16, 5];
- 4 косих брейси з мультиплікативною групою $(A, \circ) \cong C_8 \rtimes C_2$ [16, 6];
- 4 косих брейси з мультиплікативною групою $(A, \circ) \cong D_{16}$ [16, 7];
- 4 косих брейси з мультиплікативною групою $(A, \circ) \cong QD_{16}$ [16, 8];
- 18 косих брейсів з мультиплікативною групою $(A, \circ) \cong C_4 \times C_2 \times C_2$ [16, 10];
- 38 косих брейсів з мультиплікативною групою $(A, \circ) \cong C_2 \times D_8$ [16, 11];

- 8 косих брейсів з мультиплікативною групою $(A, \circ) \cong C_2 \times Q_8$ [16, 12];
- 20 косих брейсів з мультиплікативною групою $(A, \circ) \cong (C_4 \times C_2) \rtimes C_2$ [16, 13];
- 2 косих брейси з мультиплікативною групою $(A, \circ) \cong C_2 \times C_2 \times C_2 \times C_2$ [16, 14].

Наведемо класифікацію косих брейсів з адитивною групою Міллера–Морено ізоморфною групі $C_8 \rtimes C_2$ [16, 6].

Твердження 5.29. *Існує 66 косих брейсів з адитивною групою*

$$(A, +) \cong C_8 \rtimes C_2 \text{ [16, 6],}$$

тобто:

- 2 косих брейси з мультиплікативною групою $(A, \circ) \cong C_4 \times C_4$ [16, 2];
- 2 косих брейси з мультиплікативною групою $(A, \circ) \cong (C_4 \times C_2) \rtimes C_2$ [16, 3];
- 2 косих брейси з мультиплікативною групою $(A, \circ) \cong C_4 \rtimes C_4$ [16, 4];
- 6 косих брейсів з мультиплікативною групою $(A, \circ) \cong C_8 \times C_4$ [16, 5];
- 8 косих брейсів з мультиплікативною групою $(A, \circ) \cong C_8 \rtimes C_4$ [16, 6];
- 4 косих брейси з мультиплікативною групою $(A, \circ) \cong D_{16}$ [16, 7];

- 10 косих брейсів з мультиплікативною групою $(A, \circ) \cong QD_{16}$ [16, 8];
- 6 косих брейсів з мультиплікативною групою $(A, \circ) \cong Q_{16}$ [16, 9];
- 3 косих брейси з мультиплікативною групою $(A, \circ) \cong C_4 \times C_2 \times C_2$ [16, 10];
- 7 косих брейсів з мультиплікативною групою $(A, \circ) \cong C_2 \times D_8$ [16, 11];
- 5 косих брейсів з мультиплікативною групою $(A, \circ) \cong C_2 \times Q_8$ [16, 12];
- 11 косих брейсів з мультиплікативною групою $(A, \circ) \cong (C_4 \times C_2) \rtimes C_2$ [16, 13].

5.4. Майже-кільцеві брейси

Зауважимо, що брейси розміру 64 не реалізовані в бібліотеці AllBraces. З пакету LocalNR можемо завантажити локальні майже-кільця порядку 128, де аргументи k, l, m, n походять з *IdGroup* адитивної групи та мультиплікативної групи відповідно, w — позиція у списку бібліотеки.

Як приклад, ми наводимо майже-кільце

$$R := LocalNearRing(128, 160, 64, 183, 2)$$

з $|R : L| = 2$. Очевидно, що $R^* = 1 + L$, і тому ми можемо виділити майже-кільцевий ідеал $I = (L, +, \cdot)$, мультиплікативну та адитивну групи майже-кільцевого брейсу [111] $B = (L, 1 + L)$ порядку 64. Зрозуміло, що $R^* = 1 + L \cong C_{16} \times C_2 \times C_2$ та $L \cong C_{32} \times C_2$.

Цю інформацію отримано за допомогою команд:

R — задане майже-кільце.

$$R := \text{LocalNearRing}(128, 160, 64, 183, 2);$$

G — мультиплікативна група R .

$$G := \text{SmallGroup}(64, 183);$$

Структурний опис G .

$$\text{StructureDescription}(G);$$

L — підгрупа необоротних елементів R .

$$L := \text{NonUnitsAsAdditiveSubgroup}(R);$$

Структурний опис L .

$$\text{StructureDescription}(L);$$

Відмітимо, що в пакеті LocalNR є функція *NonUnitsAsNearRingIdeal*, за допомогою якої можна знаходити ідеали локальних майже-кілець або майже-кільцеві брейси.

NonUnitsAsNearRingIdeal(R) (атрибут)

Повертає: ідеал

Аргументом є локальне майже-кільце R .

Вивід є ідеал, породжений усіма необоротними елементами з R .

Приклад.

R — задане майже-кільце.

$$R := \text{LocalNearRing}(128, 160, 64, 183, 2);$$

```
ExplicitMultiplicationNearRing ( <pc group of size 128 with 7
generators> , multiplication )
```

```
#  $I$  — ідеал майже-кільця  $R$ .
```

```
gap>  $I := NonUnitsAsNearRingIdeal(R);$ 
```

```
< nearring ideal >
```

```
# Знаходимо порядок ідеалу  $I$ .
```

```
gap> Size(I);
```

```
54
```

Отже, ідеал I локального майже-кільця R є майже-кільцевим брейсом B .

Висновки до розділу 5

У даному розділі:

- використовуючи пакет YangBaxter, надано класифікації брейсів (до порядку 32) та косих брейсів (до порядку 16) відповідно до адитивних або мультиплікативних груп, які є p -групами Міллера–Морено;
- наведено деяку інформацію щодо майже-кільцевих брейсів, що стосуються, пакету LocalNR.

Основні результати даного розділу опубліковано у працях [5] зі списку публікацій і, відповідно, [88] зі списку використаних джерел, а також опубліковано у тезах конференцій [22] і, відповідно, [90].

Розділ 6

Використання системи комп'ютерної алгебри GAP для побудови та вивчення недистрибутивних алгебраїчних структур

В розділі наведено алгоритм побудови скінченних локальних майже-кілець, функції для майже-кілець та груп для пакету LocalNR з прикладами їх використання.

6.1. Алгоритм побудови скінченних локальних майже-кілець

Нагадаємо, що за Мексоном [61], майже-кілеце R з одиницею $1 \neq 0$ називається *локальним*, якщо множина $L = R \setminus R^*$ усіх необоротних елементів R утворює підгрупу адитивної групи R^+ . Зокрема, якщо $L = 0$, то R — *майже-поле*.

Наведемо деякі приклади.

- Кожне локальне кільце є локальним майже-кілцем, а кожне кільце з діленням є майже-полем.

- Якщо G — група порядку 2, то $\text{Map}(G)$ — це локальне майже-кільце порядку 4, яке не є кільцем.
- Якщо G — скінченна p -група, а A — p -група автоморфізмів G , що містить групу внутрішніх автоморфізмів $\text{Inn}(G)$, то підкільце $\text{Map}(G)$, породжене A , є локальним.

Лема 6.1. *[18, Лема 3.2] Нехай R — локальне майже-кільце. Тоді виконуються наступні твердження:*

- елементи L не мають ні лівих, ні правих оборотних елементів в R , а $R = L \cup R^*$;
- $RLR = L$, тобто L є (R, R) -підгрупою R ;
- L містить таку підгрупу M , що $RM = M$, M є нормальною в групі R^+ та фактор-група $R^+ = M$ є або p -групою з простого експонентою p , або подільною групою без кручення;
- множина $1 + L$ є підгрупою R^* , тому L є “конструктивною підгрупою” у сенсі П. Губерта.;
- напівпрямий добуток $G = L \rtimes (1 + L)$ має такі підгрупи A та B , ізоморфні $1 + L$, що $G = AB = L \rtimes A = L \rtimes B$ та $A \cap B = 1$.

Для майже-кільця R , його ідеал I є такою нормальною підгрупою R^+ , що $(r + x)s - rs \in I$ для кожного $x \in I$ та кожних $r, s \in R$. Наразі невідомо, чи для кожного локального майже-кільця R підгрупа L є ідеалом R чи навіть нормальною підгрупою R^+ . Але у скінченному випадку маємо наступне твердження (див., наприклад, [18]).

Лема 6.2. *Якщо R є скінченним локальним майже-кільцем, то виконуються такі твердження:*

- R^+ є p -групою, тому $|R| = p^n$ для деяких $n \geq 1$;

- L є ідеалом R ;
- фактор майже-кільце R/L є майже-полем;
- $1 + L$ є нормальною силовською p -підгрупою групи R^* ;
- $R^* = (1 + L) \rtimes K$ для p' -підгрупи K ізоморфної $(R/L)^*$.

Алгоритм побудови майже-кільця з одиницею базується на наступній теоремі.

Теорема 6.3 (Theorem 1, [115]). *Нехай G — група, і нехай множина $\text{End } G$ усіх ендоморфізмів G розглядається як моноїд щодо композиції ендоморфізмів. Тоді G — адитивна група майже-кільця з одиницею тоді і тільки тоді, коли існують елемент $g \in G$ та підмоноїд F групи $\text{End } G$ такі, що $G = g^F$ та $g^\phi = g^\psi$ лише тоді, коли $\phi = \psi$ для будь-яких $\phi, \psi \in F$.*

Наступна теорема описує умови, за яких майже-кільце $Nr = (G, \cdot, \star_F)$, побудоване на G моноїдом F , є локальним.

Теорема 6.4. *Нехай група G , її елемент g та підмоноїд F з $\text{End } G$ задовольняють висновок теореми 6.3 і нехай $A = F \cap \text{Aut } G$. Майже-кільце $Nr = (G, \cdot, \star_F)$ є локальним тоді й тільки тоді, коли існує така підгрупа L групи G , що $G = g^A \cup L$ та $g^A \cap L = \emptyset$.*

Доведення. Якщо G — скінченна група, то множина $\text{End } G \setminus \text{Aut } G$ є піднапівгрупою $\text{End } G$. Отже, всі неавтоморфізми $F \subset \text{End } G$ утворюють таку A -інваріантну піднапівгрупу X , що $F = A \cup X$ та $A \cap X = \emptyset$. Оскільки $G = g^F = g^A \cup L$, то $L = g^X$. $\square$

Використовуючи мову програмування GAP та пакет SONATA, розроблено алгоритм, який дозволяє класифікувати локальні майже-кільця порядку 32 і більше.

Нехай G — скінченна група, що міститься в бібліотеці системи комп'ютерної алгебри GAP. Розглянемо як приклад групу $G = (\langle a \rangle \rtimes \langle b \rangle) \rtimes \langle c \rangle$ порядку 32 з $a^8 = b^2 = c^2 = 1$, $[a, c] = b$, $[a, b] = a^4$ та $[b, c] = 1$.

Нехай $[n, i]$ — i -та група порядку n у бібліотеці `SmallGroups` в GAP.
 G — група з бібліотеки `AllSmallGroups` з `IdGroup` = [32, 7].

```
gap > G := SmallGroup(32, 7);
```

```
< pc group of size 32 with 5 generators >
```

Виведемо структурний опис заданої групи.

```
gap > StructureDescription(G);
```

```
"(C8 : C2) : C2"
```

Знаходимо групу автоморфізмів заданої групи та її порядок.

```
gap > A := AutomorphismGroup(G);
```

```
< group >
```

```
gap > Size(A);
```

```
128
```

Шукаємо довжини орбіт заданої групи в її групі автоморфізмів.

```
gap > OrbitLengths(A, G);
```

```
[1, 16, 8, 2, 4, 1]
```

Повертаємо другу орбіту зі списку орбіт заданої групи в її групі автоморфізмів.

```
gap > Or := OrbitsDomain(A, G)[2];;
```

```
gap > Size(Or);
```

```
16
```

Шукаємо різницю елементів групи та знайденої орбіти.

```
gap > L := Difference(G, Or);;
```

Повертаємо підгрупу зі знайденої різниці.

```
gap > L := Subgroup(G, L);
```

$Group([< identity > of \dots, f2, f3, f4, f5, f2 * f3, f2 * f4, f2 * f5, f3 * f4, f3 * f5, f4 * f5, f2 * f3 * f4, f2 * f3 * f5, f2 * f4 * f5, f3 * f4 * f5, f2 * f3 * f4 * f5])$

Шукана підгрупа має однаковий порядок з кількістю елементів різниці.

```
gap > Size(L);
```

16

Виводимо структурний опис знайденої підгрупи необоротних елементів.

```
gap > StructureDescription(L);
```

" $C2 \times D8$ "

Знаходимо підгрупи групи автоморфізмів.

```
gap > S := SubgroupsSolvableGroup(A);;
```

Фільтруємо всі підгрупи порядку 16 зі знайденого списку підгруп.

```
gap > T := Filtered(S, x -> Size(x) = 16);;
```

Шукаємо в знайденому списку всі підгрупи, в яких задана група має довжину орбіти 16.

```
gap > U := Filtered(T, x -> Maximum(OrbitLengths(x, G)) = 16);;
```

Виводимо розмір отриманого списку.

```
gap > Size(U);
```

6

Виводимо список *IdGroup*, знайдених у попередньому списку підгруп.

```
gap > List(U, IdGroup);
```

[[16, 3], [16, 11], [16, 11], [16, 13], [16, 8], [16, 7]]

Шукаємо всі ендоморфізми заданої групи та виводимо розмір отриманого списку.

```
gap > En := AllEndomorphisms(G);;
```

```
gap > Size(En);
```

```
320
```

Фіксуємо перший елемент списку ендоморфізмів.

```
gap > o := En[1];;
```

Знаходимо нільпотентні ендоморфізми з отриманого раніше списку.

```
gap > Nil := [];
```

```
[]
```

```
gap > for x in En do;
```

```
> if  $x^5 = o$  then Add(Nil, x); fi;
```

```
> od;
```

Знаходимо розмір списку *Nil* нільпотентних ендоморфізмів.

```
gap > Size(Nil);
```

```
64
```

```
gap > ...
```

Наводимо структурний опис отриманих мультиплікативних груп локальних майже-кілець на заданій групі.

```
gap > StructureDescription(U[1]);
```

```
"(C4 × C2) : C2"
```

```
gap > StructureDescription(U[2]);
```

```
"C2 × D8"
```

```
gap > StructureDescription(U[3]);
```

```
"C2 × D8"
```

```
gap > StructureDescription(U[4]);
```

```
"(C4 × C2) : C2"
```

```
gap > ...
```

Це означає, зокрема, що є лише такі тричі факторизовані групи $M \rtimes A = M \rtimes B = AB$ з $A \cap B = 1$ та $M \cong C_2 \times D_8$, а саме групи, в яких $A \cong B$ ізоморфна одній з груп

- $C_2 \times D_8$,
- $(C_4 \times C_2) \rtimes C_2$,
- D_{16} або
- QD_{16} .

Алгоритм побудови скінченних локальних майже-кілець на адитивній групі [32, 7] можна отримати за допомогою GAP, використовуючи пакети LocalNR та SONATA.

На даний момент ми використовуємо послідовні коди. Нас цікавить їх паралелізація для побудови локальних майже-кілець більших порядків. Паралелізація GAP принципово відрізняється від загальноновживаних підходів до числових обчислень, таких як, наприклад, OpenMP або MPI, через різні типи об'єктів, з якими працює GAP. В перспективі для паралелізації обчислень GAP можна використовувати пакет GAP SCSCP <https://gap-packages.github.io/scscp/>, який забезпечує основну структуру для розподілених паралельних обчислень у GAP.

6.2. Пакет LocalNR: функції для майже-кілець

Для дослідників майже-кілець список усіх 698 неізоморфних локальних майже-кілець порядку не більше 31 міститься у пакеті SONATA. Однак класифікація всіх локальних майже-кілець порядку більше 32 є значною проблемою.

Мотивовані цим, ми реалізували алгоритми для обчислення всіх локальних майже-кілець подальших порядків у новому пакеті GAP під назвою LocalNR. Поточна версія цього пакету містить усі 37441 локальних

майже-кілець порядку не більше 361, крім порядків 32, 64, 128, 243, 256 та деякі функції для аналізу скінченних майже-кілець. Поточна версія цього пакету — 1.0.4, опублікована 15.03.2024.

Надамо деякі функції для локальних майже-кілець з пакету LocalNR.

6.2.1. TheAdditiveGroupsOfLibraryOfLNRsOfOrder

TheAdditiveGroupsOfLibraryOfLNRsOfOrder(n) (функція)

Повертає: інформація

Аргумент — n . Вивести список IdGroup адитивних груп локальних майже-кілець порядку n з бібліотеки.

Приклад.

Виведемо список IdGroup всіх можливих груп порядку 81, які є адитивними групами локальних майже-кілець з бібліотеки.

```
gap> List(TheAdditiveGroupsOfLibraryOfLNRsOfOrder(81),IdGroup);
[ [ 81, 1 ], [ 81, 2 ], [ 81, 3 ], [ 81, 5 ], [ 81, 6 ], [ 81, 11 ],
[ 81, 12 ], [ 81, 13 ], [ 81, 15 ] ]
```

Наведемо програмну реалізацію цієї функції на мові GAP, що міститься в пакеті LocalNR.

```
# TheAdditiveGroupsOfLibraryOfLNRsOfOrder
InstallGlobalFunction(TheAdditiveGroups
OfLibraryOfLNRsOfOrder, function(n)
local t, cont, i, h, j, f, g, r, us;
t := DirectoriesPackageLibrary("LocalNR
Concatenation("Endom/ String(n)));
```

```

    if IsEmpty(t) then Error("the order must be
PrimePowerInt and  $3 < n$  and  $n < 1331$ 
(except orders 128, 256, 512, 625, 729, 1024)");
    else
    cont := DirectoryContents(t[1]);
    Size(cont);
    for i in cont do
    RemoveCharacters(i, "Endom\\.txt\\.gz");
    od;
    h := [];
    for j in cont do
    f := SplitStringInternal(j, "_", "");
    Add(h, f);
    od;
    g := [];
    for i in h do
    if Size(i) > 0 then
    Add(g, i[2]); fi; od;
    us := Set(g, Int);
    r := [];
    for i in us do
    Add(r, SmallGroup(n, i)); od;
    return r; fi;
end);

```

6.2.2. TheLibraryOfLNRsOnGroup

TheLibraryOfLNRsOnGroup(G) (функція)

Повертає: інформація

Аргументом є група G . Вивід списку каталогів локальних майже-кілець на групі G з бібліотеки.

Приклад.

G — група з *IdGroup* [81, 2].

```
gap> G := SmallGroup(81,2);
```

```
<pc group of size 81 with 4 generators>
```

Виведемо список каталогів локальних майже-кілець на групі G .

```
gap> TheLibraryOfLNRsOnGroup(G);
```

```
[ "AllLocalNearRings(81,2,54,3)", "AllLocalNearRings(81,2,54,6)",  
  "AllLocalNearRings(81,2,54,9)", "AllLocalNearRings(81,2,54,10)",  
  "AllLocalNearRings(81,2,54,11)", "AllLocalNearRings(81,2,54,15)",  
  "AllLocalNearRings(81,2,72,14)", "AllLocalNearRings(81,2,72,19)",  
  "AllLocalNearRings(81,2,72,24)", "AllLocalNearRings(81,2,72,26)" ]
```

Наведемо програмну реалізацію цієї функції на мові GAP, що міститься в пакеті LocalNR.

```
# TheLibraryOfLNRsOnGroup
InstallGlobalFunction(TheLibraryOfLNRsOnGroup,
function(G)
  local s, t, cont, i, h, j, f, hj, g, r, ee, ww, b, w;
  Знайдемо порядок групи G.
  s := Size(G);
  t := DirectoriesPackageLibrary("LocalNR",
Concatenation("Endom/", String(s)));
  if IsEmpty(t) then Error("false");
  else
```

```

cont := DirectoryContents(t[1]);
Size(cont);
for i in cont do
  RemoveCharacters(i,
    “Endom\ .txt\ .gz”);
od;
h := [];
for j in cont do
  f := SplitStringInternal(j, “_”, “-”);
  Add(h, f);
od;
fi;
hj := IdGroup(G);
g := [];
for i in h do
  if Size(i) > 0 and EvalString(i[2]) = hj[2] then
    Add(g, i);
  fi;
od;
ww := function(b, w)
  if Int(b[3]) = Int(w[3]) then
    return Int(b[4]) < Int(w[4]);
  else
    return Int(b[3]) < Int(w[3]);
  fi;
end;
Sort(g, ww);
ee := [];
for i in g do

```

```

    if Size(i) > 0 then
      Add(ee, Concatenation("AllLocalNearRings
(", i[1], ", ", i[2], ", ", i[3], ", ", i[4], ", ")");
    fi; od;
  return ee;
end);

```

6.2.3. LocalNearRing

LocalNearRing(k, l, m, n, w) (операція)

Повертає: майже-кільце

Аргументи: k, l, m, n, w . Вивід: локальне майже-кільце з бібліотеки без перевірки. Аргументи k, l, m, n взяті з IdGroup адитивної групи та мультиплікативної групи відповідно, w — це позиція у списку бібліотеки.

Приклад.

L — локальне майже-кільце з адитивною групою $[81, 12]$, мультиплікативною групою $[54, 8]$, яке є 3 в списку бібліотеки.

```
gap> L := LocalNearRing(81,12,54,8,3);
```

```
ExplicitMultiplicationNearRing (<pc group of size 81 with
4 generators> , multiplication )
```

Наведемо програмну реалізацію цієї функції на мові GAP, що міститься в пакеті LocalNR.

```

# LocalNearRing(< k,l,m,n,w >)
InstallMethod(LocalNearRing,
"Local nearring",

```

```

[IsInt, IsInt, IsInt, IsInt, IsInt],
function(k, l, m, n, w)
  local h, dio, G, P, P1, H, R, Li, t, gr, Pos, x, y, d, z, hom,
f, const, constructor, u, B, A, k1, Or, a, g, Em, ma, mul, Nr;
  h := DirectoriesPackageLibrary("LocalNR",
Concatenation("Endom/", String(k)));
  if IsEmpty(h) then return false;
  else
    gap > ...
    G := SmallGroup(k, l);
    P1 := ReadAsFunction(dio)();
    P := P1[w];
    H := [];
    R := [];
    Li := AsSortedList(G);
    t := Size(P);
    gr := MinimalGeneratingSet(G);
    Pos := [];
    for x in gr do
      Add(Pos, Position(Li, x)); od;
    for y in [1..t] do
      d := [];
      for z in Pos do
        Add(d, Li[P[y][z]]); od;
      Add(H, d); od;
    hom := [];
    for x in H do
      d := GroupHomomorphismByImagesNC(G, G, gr, x);
      Add(hom, d); od;

```

```

    f := function(x, y) return x * y; end;
    const := function(y) return function(x) return y^x; end; end;
    constructor := function(z) return function(u)
return function(x, y)
return u(PreImage(z, y) * PreImage(z, x)); end; end; end;
    B := Filtered(hom, x -> IsInjective(x));
    A := GroupByGenerators(B);
    k1 := Position(OrbitLengths(A, G), Size(A));
    Or := OrbitsDomain(A, G)[k1];
    a := Or[1];
    g := const(a);
    Em := MagmaWithOne(hom);
    ma := MappingByFunction(Em, G, g);
    mul := constructor(ma)(a);
    Nr := ExplicitMultiplicationNearRingNC(G, mul);
    return Nr; fi;
end);

```

6.2.4. AllLocalNearRings

AllLocalNearRings(k, l, m, n) (operation)

Повертає: список

Аргументи: k , l , m , n . Вихідними даними є список всіх локальних майже-кілець з бібліотеки без перевірки. Аргументи k , l , m , n такі ж, як і вище.

Приклад.

L —список локальних майже-кілець з адитивною групою $[81, 12]$ та мультиплікативною групою $[54, 8]$ зі списку бібліотеки.

```
gap> L := AllLocalNearRings(81,12,54,8);;
gap> Size(L);
30
```

6.2.5. IsAdditiveGroupOfLibraryOfLNRs

IsAdditiveGroupOfLibraryOfLNRs(G) (функція)

Повертає: логічний оператор

Аргументом є група G . Вивід має значення `true`, якщо в бібліотеці існує локальне майже-кілець, адитивна група якого ізоморфна G , інакше вивід має значення `false`.

Приклад.

G — група з *IdGroup* $[25, 2]$.

```
gap> G := SmallGroup(25,2);
<pc group of size 25 with 2 generators>
```

Перевірка, чи існує локальне майже-кілець, адитивна група якого ізоморфна G .

```
gap> IsAdditiveGroupOfLibraryOfLNRs(G);
true
```

Перевірка, чи існує локальне майже-кілець, адитивна група якого ізоморфна групі з *IdGroup* $[81, 14]$.

```
gap> IsAdditiveGroupOfLibraryOfLNRs(SmallGroup(81,14));
false
```

Наведемо програмну реалізацію цієї функції на мові GAP, що міститься в пакеті LocalNR.

```

# IsAdditiveGroupOfLibraryOfLNRs
InstallGlobalFunction(IsAdditiveGroup
OfLibraryOfLNRs, function(G)
  local s, t, cont, i, h, j, f, g, r, us, d, k;
  # s — порядок групи G.
  s := Size(G);
  # t — шлях до каталогу, що містить майже-кільця порядку s.
  t := DirectoriesPackageLibrary("LocalNR",
Concatenation("Endom/", String(s)));
  if IsEmpty(t) then Error("false");
  else
    # t — містить список назв файлів, що містяться в директорії t.
    cont := DirectoryContents(t[1]);
    # Знаходимо розмір cont.
    Size(cont);
    # Перевірка, чи містить директорія cont файли, в яких є IdGroup(G).
    for i in cont do
      RemoveCharacters(i,
"Endom\ .txt\ .gz");
    od;
    h := [];
    for j in cont do
      gap > ...
      Add(h, f); od;
    g := [];
    for i in h do

```

```

if Size(i) > 0 then
  Add(g, i[2]); fi;
od;
us := Set(g, Int);
r := [];
for i in us do
  Add(r, [s, i]); od;
fi;
k := Size(r);
d := Filtered([1..k], x -> IdGroup(G) = r[x]);
if Size(d) > 0 then Print("true");
else Print("false"); fi;
end);

```

6.2.6. InfoLocalNearRing

InfoLocalNearRing(G) (function)

Повертає: інформація

Аргументом є група G . Вивід: деяка інформація про локальні майже-кільця на G з бібліотеки.

Приклад.

Вивід інформації бібліотеки *AllLocalNearRings* про локальні майже-кільця на групі з ідентифікатором [361,2] з бібліотеки *AllSmallGroups*.

```
gap> InfoLocalNearRing(SmallGroup(361,2));
```

The local nearrings are sorted by their multiplicative groups.

```
[ "AllLocalNearRings(361,2,342,1) (2)",
```

```
"AllLocalNearRings(361,2,342,2) (2)",
```

```

"AllLocalNearRings(361,2,342,4) (1)",
"AllLocalNearRings(361,2,342,6) (1)",
"AllLocalNearRings(361,2,342,7) (7)",
"AllLocalNearRings(361,2,342,8) (6)",
"AllLocalNearRings(361,2,360,4) (1)",
"AllLocalNearRings(361,2,360,15) (1)"
|

```

Наведемо програмну реалізацію цієї функції на мові GAP, що міститься в пакеті LocalNR.

```

# InfoLocalNearRing
InstallGlobalFunction(InfoLocalNearRing,
function(G)
  local R, s, T, i, K, t, h;
  # h — шлях до каталогу "Endom/"
  h := DirectoriesPackageLibrary("LocalNR",
  "Endom/");
  # t — шлях до файлу, що містить інформацію про майже-кільця на
  заданій групі з бібліотеки пакету LocalNR.
  t := Filename(h, Concatenation("info", ".txt"));
  # R — містить інформацію з файлу з назвою t.
  R := ReadAsFunction(t)();
  # K — ідентифікатор групи G в бібліотеці AllSmallGroups.
  K := IdGroup(G);
  # s — розмір R.
  s := Size(R);

```

Далі, наводимо інформацію про локальні майже-кільця на G з бібліотеки.

```

T := [];
for i in [1..s] do
  if R[i][1] = K[1] and R[i][2] = K[2] then
    Add(T, Concatenation(" AllLocalNearRings( String(R[i][1]),
String(R[i][2]), String(R[i][3]), String(R[i][4]), )( String(R[i][5]), ")"));
    fi;
  od;
  if Size(T) > 1 then Print("The local nearrings are
sorted by their multiplicative groups.
  elif Size(T) = 1 then Print(T);
  else return Error("group is not recognized
in the library"); fi;
end);

```

6.3. Пакет LocalNR: функції для груп

Наведемо деякі функції для груп з пакету LocalNR.

6.3.1. IsMinimalNonAbelianGroup

IsMinimalNonAbelianGroup(*G*) (властивість)

Повертає: логічний оператор

Аргументом є група *G*. Вивід має значення **true**, якщо *G* є мінімальною неабелевою групою, інакше вивід має значення **false**.

Приклад.

H — група з ідентифікатором $[120,4]$ з бібліотеки *AllSmallGroups*.

```
gap> H := SmallGroup(120,4);
```

```
<pc group of size 120 with 5 generators>
```

Перевірка, чи є група H мінімальною неабелевою групою.

```
gap> IsMinimalNonAbelianGroup(H);
```

```
false
```

K — група з ідентифікатором $[16,6]$ з бібліотеки *AllSmallGroups*.

```
gap> K := SmallGroup(16,6);
```

```
<pc group of size 16 with 4 generators>
```

Перевірка, чи є група K мінімальною неабелевою групою.

```
gap> IsMinimalNonAbelianGroup(K);
```

```
true
```

Перевірка, чи є група з ідентифікатором $[16,8]$ з бібліотеки *AllSmallGroups* мінімальною неабелевою групою.

```
gap> IsMinimalNonAbelianGroup(SmallGroup(16,8));
```

```
false
```

Наведемо програмну реалізацію цієї функції на мові GAP, що міститься в пакеті LocalNR.

```
# IsMinimalNonAbelianGroup(< G >)
```

```
InstallMethod(IsMinimalNonAbelianGroup,
```

```
  "Is minimal non – abelian group",
```

```
  [IsGroup],
```

```
  function(G)
```

```
    if IsAbelian(G) then
```

```
      return false;
```

```
    else
```

```
      if IsPGroup(G) and FrattiniSubgroup(G) = Centre(G) and
```

```

Size(MinimalGeneratingSet(G)) = 2
then
return true;
else
if Size(AsSet(Factors(Size(G)))) = 2 and
ForAll(MaximalSubgroups(G), x -> IsAbelian(x)) then
return true;
else return false;
fi;
fi;
fi;
end);

```

6.3.2. IsMetacyclicPGroup

IsMetacyclicPGroup(*G*) (властивість)

Повертає: логічний оператор

Аргументом є група G . Вивід має значення **true**, якщо G є метациклічною p -групою, інакше вивід має значення **false**.

Приклад.

Перевірка, чи є група K з попередньої підсекції метациклічною p -групою.

```

gap> IsMetacyclicPGroup(K);
true

```

Перевірка, чи є групи з ідентифікаторами [81,4] та [81,15] з бібліотеки *AllSmallGroups* метациклічними p -групами.

```

gap> IsMetacyclicPGroup(SmallGroup(81,4));
true

```

```
gap> IsMetacyclicPGroup(SmallGroup(81,15));
false
```

Наведемо програмну реалізацію цієї функції на мові GAP, що міститься в пакеті LocalNR.

```
# IsMetacyclicPGroup(< G >)
InstallMethod(IsMetacyclicPGroup,
  "Is metacyclic p – group",
  [IsGroup],
  function(G)
    local p;
    p := Factors(Size(G))[1];
    if p = 2 then
      if Maximum(List(List(MaximalSubgroups(G),
MinimalGeneratingSet), Size)) <= 2
        then return true;
      fi;
    else
      if Size(FactorGroup(G, Agemo(G, p))) <= p2 then
        return true;
      fi;
    fi;
    return false;
  end);
```

6.3.3. EndoOrbitsOfGroup

EndoOrbitsOfGroup(G) (операція)

Повертає: список

Аргументом є група G . Виводить список ендоециклічних орбіт групи G .

Приклад.

D — група з бібліотеки *AllSmallGroups* з $IdGroup = [81, 2]$.

```
gap> D := SmallGroup(81,2);
```

```
<pc group of size 81 with 4 generators>
```

T — список ендоециклічних орбіт групи D .

```
gap> T := EndoOrbitsOfGroup(D);;
```

```
gap> Length(T);
```

```
1
```

```
gap> Size(T[1][2]);
```

```
81
```

Наведемо програмну реалізацію цієї функції на мові GAP, що міститься в пакеті LocalNR.

```
# EndoOrbitsOfGroup(< G >)
```

```
InstallMethod(EndoOrbitsOfGroup,
```

```
  "Compute endo — orbits of group",
```

```
  [IsGroup],
```

```
  function(G)
```

```
    local A, En, F, H, M, m, Or, T, x, y;
```

Група A — група автоморфізмів групи G .

```
A := AutomorphismGroup(G);
```

Список En — список ендоморфізмів групи G .

```
En := Endomorphisms(G);
```

Знаходимо m — експоненту групи G .

$m := \text{Exponent}(G);$

Список M —список елементів групи G , порядок яких дорівнює m .

$M := \text{Filtered}(G, x \rightarrow \text{Order}(x) = m);$

Далі, знаходимо список ендоеиклічних орбіт групи G .

if $\text{Size}(M) = 0$ *then*

return M ;

else

Знаходимо список орбіт A на області визначення M .

$Or := \text{OrbitsDomain}(A, M);$

Знаходимо масив T представників із списку Or .

$T := [];$

for x *in* Or *do*

$\text{Add}(T, \text{Representative}(x));$

od;

$F := [];$

for x *in* T *do*

$H := [];$

for y *in* En *do*

$\text{Add}(H, x^y);$

Список H новий змінний список, записи якого є елементами списку H з видаленими дублікатами.

$H := \text{Unique}(H);$

od;

$\text{Add}(F, H);$

od;

Повертаємо масив F .

return F ;

fi;

end);

6.3.4. IsEndoCyclicGroup

IsEndoCyclicGroup(G) (властивість)

Повертає: логічний оператор

Аргументом є група G . Вивід має значення **true**, якщо G є ендоециклічною групою, інакше — значення **false**.

Приклад.

D — група з бібліотеки *AllSmallGroups* з $IdGroup = [81, 2]$.

```
gap> D := SmallGroup(81,2);
```

```
<pc group of size 81 with 4 generators>
```

Перевірка, чи група G є ендоециклічною групою.

```
gap> IsEndoCyclicGroup(D);
```

```
true
```

Наведемо програмну реалізацію цієї функції на мові GAP, що міститься в пакеті LocalNR.

```
# IsEndoCyclicGroup(< G >)
InstallMethod(IsEndoCyclicGroup,
  "Is endo — cyclic group",
  [IsGroup],
  function(G)
    local Fe;
```

Список Fe — список ендоециклічних орбіт групи G .

```
Fe := EndoOrbitsOfGroup(G);
```

Якщо розмір списку Fe ендоециклічних орбіт групи G не нульовий та максимальна значення розміру списку Fe дорівнює порядку групи G , то повертаємо **true**, інакше — **false**.

```

    if Size( $Fe$ ) > 0 and
Maximum(List( $Fe$ , Size)) = Size( $G$ ) then
    return true;
else return false; fi;
end);

```

Висновки до розділу 6

У даному розділі:

- отримано алгоритм побудови скінченних локальних майже-кілець;
- наведено функції для локальних майже-кілець з пакету LocalNR, а саме:
 - TheAdditiveGroupsOfLibraryOfLNRsOfOrder,
 - TheLibraryOfLNRsOnGroup,
 - LocalNearRing,
 - AllLocalNearRings,
 - IsAdditiveGroupOfLibraryOfLNRs,
 - InfoLocalNearRing;
- наведено функції для груп з пакету LocalNR, а саме:
 - IsMinimalNonAbelianGroup,
 - IsMetacyclicPGroup,
 - EndoOrbitsOfGroup,
 - IsEndoCyclicGroup;

Основні результати даного розділу опубліковано у працях [1, 3, 17, 18, 19] зі списку публікацій і, відповідно, [101], [115], [99], [100], [98] зі списку використаних джерел, а також опубліковано у тезах конференцій [23, 33, 39] і, відповідно, [91], [75], [72].

Розділ 7

Класифікація локальних майже-кілець малих порядків та ендоеиклічні групи

В розділі наведено класифікація локальних майже-кілець малих порядків. Також вивчаються ендоеиклічні групи та локальні майже-кілець.

7.1. Класифікація локальних майже-кілець малих порядків

Протягом 10 років наша дослідницька група використовувала обчислювальний кластер SCIT3 в Інституті кібернетики імені В. Глушкова Національної академії наук України. Він мав 127 вузлів (75 вузлів з дво-ядерними процесорами Intel Xeon 5160 та 52 вузли з чотириядерними процесорами Xeon 5345 з частотою 3,0 ГГц та 2,2 ГГц відповідно, з 8 або 16 ГБ оперативної пам'яті. Кількість ядер на вузол становила 4 або 8; загалом він мав 716 ядер.

7.1.1. Локальні майже-кілець порядку 64

Існує 267 неізоморфних груп порядку $64 = 2^6$, з яких 53 є 2-породженими групами, і лише 24 з цих груп є адитивними групами локальних майже-кілець та класифіковано ці майже-кільця.

Нехай $[n, i]$ — i -та група порядку n у бібліотеці SmallGroups у GAP, $n(G)$ — кількість неізоморфних локальних майже-кілець.

Наведемо класифікацію 2-породжених груп, які є адитивними групами локальних майже-кілець порядку 64.

Теорема 7.1. *Наступні 2-породженні групи є адитивними групами локальних майже-кілець порядку 64:*

- $IdGroup(G) = [64, 2]$, група $G \cong C_8 \times C_8$ та $n(G) = 1683$;
- $IdGroup(G) = [64, 3]$, група $G \cong C_8 \rtimes C_8$ та $n(G) = 1628$;
- $IdGroup(G) = [64, 4]$, група $G \cong ((C_8 \times C_2) \rtimes C_2) \rtimes C_2$ та $n(G) = 167245$;
- $IdGroup(G) = [64, 5]$, група $G \cong (C_4 \times C_2) \rtimes C_8$ та $n(G) = 118190$;
- $IdGroup(G) = [64, 10]$, група $G \cong (C_8 \rtimes C_4) \rtimes C_2$ та $n(G) = 7424$;
- $IdGroup(G) = [64, 12]$, група $G \cong (C_4 \rtimes C_8) \rtimes C_2$ та $n(G) = 5633$;
- $IdGroup(G) = [64, 14]$, група $G \cong (C_2 \times C_2).((C_4 \times C_2) \rtimes C_2)$ та $n(G) = 5520$;
- $IdGroup(G) = [64, 15]$, група $G \cong C_8 \rtimes C_8$ та $n(G) = 2384$;
- $IdGroup(G) = [64, 16]$, група $G \cong C_8 \rtimes C_8$ та $n(G) = 2384$;
- $IdGroup(G) = [64, 17]$, група $G \cong (C_8 \times C_2) \rtimes C_4$ та $n(G) = 433060$;
- $IdGroup(G) = [64, 23]$, група $G \cong (C_4 \times C_2 \times C_2) \rtimes C_4$ та $n(G) = 111758$;
- $IdGroup(G) = [64, 24]$, група $G \cong (C_8 \rtimes C_2) \rtimes C_4$ та $n(G) = 109189$;

- $IdGroup(G) = [64, 26]$, група $G \cong C_{16} \times C_4$ та $n(G) = 11467$;
- $IdGroup(G) = [64, 27]$, група $G \cong C_{16} \rtimes C_4$ та $n(G) = 11467$;
- $IdGroup(G) = [64, 29]$, група $G \cong (C_{16} \times C_2) \rtimes C_2$ та $n(G) = 28185$;
- $IdGroup(G) = [64, 30]$, група $G \cong (C_{16} \rtimes C_2) \rtimes C_2$ та $n(G) = 4433$;
- $IdGroup(G) = [64, 34]$, група $G \cong (((C_4 \times C_2) \rtimes C_2) \rtimes C_2) \rtimes C_2$ та $n(G) = 16177$;
- $IdGroup(G) = [64, 35]$, група $G \cong (C_4 \times C_4) \rtimes C_4$ та $n(G) = 15504$;
- $IdGroup(G) = [64, 36]$, група $G \cong (C_2 \cdot ((C_4 \times C_2) \rtimes C_2))$ та $n(G) = 15761$;
- $IdGroup(G) = [64, 37]$, група $G \cong C_2 \cdot (((C_4 \times C_2) \rtimes C_2) \rtimes C_2)$ та $n(G) = 15920$;
- $IdGroup(G) = [64, 44]$, група $G \cong C_4 \rtimes C_{16}$ та $n(G) = 28500$;
- $IdGroup(G) = [64, 45]$, група $G \cong C_8.D_8 = C_4 \cdot (C_8 \times C_2)$ та $n(G) = 1920$;
- $IdGroup(G) = [64, 50]$, група $G \cong C_{32} \times C_2$ та $n(G) = 257$;
- $IdGroup(G) = [64, 51]$, група $G \cong C_{32} \rtimes C_2$ та $n(G) = 257$.

Серед 267 неізоморфних груп порядку $64 = 2^6$ них лише 2 групи експоненти 32 та 8 груп експоненти 16 є адитивними групами локальних майже-кілець.

Як прямий наслідок теореми 7.1, маємо наступне твердження.

Теорема 7.2. *Наступні групи експоненти 32 є адитивними групами локальних майже-кілець порядку 64:*

- $IdGroup(G) = [64, 50]$, група $G \cong C_{32} \times C_2$ та $n(G) = 257$;

- $IdGroup(G) = [64, 51]$, група $G \cong C_{32} \rtimes C_2$ та $n(G) = 257$;

Знайдені всі неізоморфні групи порядку 64 з експонентою 16, які є адитивними групами локальних майже-кілець.

Теорема 7.3. *Наступні групи експоненти 16 є адитивними групами локальних майже-кілець порядку 64:*

- $IdGroup(G) = [64, 26]$, група $G \cong C_{16} \times C_4$ та $n(G) = 11467$;
- $IdGroup(G) = [64, 27]$, група $G \cong C_{16} \rtimes C_4$ та $n(G) = 11467$;
- $IdGroup(G) = [64, 29]$, група $G \cong (C_{16} \times C_2) \rtimes C_2$ та $n(G) = 28185$;
- $IdGroup(G) = [64, 30]$, група $G \cong (C_{16} \rtimes C_2) \rtimes C_2$ та $n(G) = 4433$;
- $IdGroup(G) = [64, 44]$, група $G \cong C_4 \rtimes C_{16}$ та $n(G) = 28500$;
- $IdGroup(G) = [64, 45]$, група $G \cong C_8.D_8 = C_4.(C_8 \times C_2)$ та $n(G) = 1920$;
- $IdGroup(G) = [64, 183]$, група $G \cong C_{16} \times C_2 \times C_2$;
- $IdGroup(G) = [64, 184]$, група $G \cong C_2 \times (C_{16} \rtimes C_2)$.

7.1.2. Локальні майже-кілець порядку 81

Наприклад, існують 14 неізоморфних груп порядку $16 = 2^4$, з яких 9 є адитивними групами локальних майже-кілець. Наступна теорема описує такі групи порядку $81 = 3^4$. Зокрема, серед 15 неізоморфних груп цього порядку лише 9 є такими групами.

Наведено класифікацію локальних майже-кілець порядку 81 та їх адитивних груп.

Теорема 7.4. *Наступні групи, і тільки вони, є адитивними групами локальних майже-кілець порядку 81.*

- $IdGroup(G) = [81, 1]$, група $G \cong C_{81}$ та $n(G) = 1$;
- $IdGroup(G) = [81, 2]$, група $G \cong C_9 \times C_9$ та $n(G) = 268$;
- $IdGroup(G) = [81, 3]$, група $G \cong (C_9 \times C_3) \rtimes C_3$ та $n(G) = 46$;
- $IdGroup(G) = [81, 5]$, група $G \cong C_{27} \times C_3$ та $n(G) = 388$;
- $IdGroup(G) = [81, 6]$, група $G \cong C_{27} \rtimes C_3$ та $n(G) = 10$;
- $IdGroup(G) = [81, 11]$, група $G \cong C_9 \times C_3 \times C_3$ та $n(G) = 22989$;
- $IdGroup(G) = [81, 12]$, група $G \cong C_3 \times ((C_3 \times C_3) \rtimes C_3)$ та $n(G) = 807$;
- $IdGroup(G) = [81, 13]$, група $G \cong C_3 \times (C_9 \rtimes C_3)$ та $n(G) = 337$;
- $IdGroup(G) = [81, 15]$, група $G \cong C_3 \times C_3 \times C_3 \times C_3$ та $n(G) = 12322$.

7.1.3. Локальні майже-кілеця порядку 243

Зазначимо, що існують 15 неізоморфних груп порядку $81 = 3^4$, з яких 9 є адитивними групами локальних майже-кілець. Наступна теорема описує 2-породжені групи порядку $243 = 3^5$ з цією властивістю. Зокрема, серед 29 неізоморфних 2-породжених груп цього порядку лише 10 є такими адитивними групами.

Наведено класифікацію 2-породжених груп порядку 243, які є адитивними групами локальних майже-кілець. Більш того, вказано їх підгрупи необоротних елементів.

Теорема 7.5. *Нехай R — локальне майже-кілеце порядку 243, R^* мультиплікативна група в R і L адитивна підгрупа необоротних елементів*

адитивної групи R^+ в R . Якщо R^+ є 2-породженою, то пара R^+ і L є однією з наступних:

[243, 2]	$(C_9 \times C_3) \rtimes C_9$	i	[81, 11]	$C_9 \times C_3 \times C_3$;
[243, 10]	$C_{27} \times C_9$	i	[81, 2]	$C_9 \times C_9$;
[243, 11]	$C_{27} \rtimes C_9$	i	[81, 2]	$C_9 \times C_9$;
[243, 12]	$(C_{27} \times C_3) \rtimes C_3$	i	[81, 11]	$C_9 \times C_3 \times C_3$;
[243, 13]	$((C_9 \times C_3) \rtimes C_3) \rtimes C_3$	i	[81, 15]	$C_3 \times C_3 \times C_3 \times C_3$;
[243, 14]	$(C_9 \times C_3) \rtimes C_9$	i	[81, 11]	$C_9 \times C_3 \times C_3$;
[243, 15]	$(C_9 \times C_3) \rtimes C_9$	i	[81, 11]	$C_9 \times C_3 \times C_3$;
[243, 16]	$(C_{27} \rtimes C_3) \rtimes C_3$	i	[81, 11]	$C_9 \times C_3 \times C_3$;
[243, 23]	$C_{81} \times C_3$	i	[81, 5]	$C_{27} \times C_3$;
[243, 24]	$C_{81} \rtimes C_3$	i	[81, 5]	$C_{27} \times C_3$.

В наступній теоремі наведено кількість усіх неізоморфних локальних майже-кілець із заданими адитивними з теореми 7.5 та наведено їх мультиплікативні групи.

Теорема 7.6. Нехай $n(G)$ кількість усіх неізоморфних локальних майже-кілець R адитивна група R^+ яких ізоморфна групі G . Якщо $n(R^*)$ є кількістю цих майже-кілець, для яких $IdGroup(R^*)$ є фіксованим, то має місце наступне.

- $IdGroup(G) = [243, 2]$, група $G \cong (C_9 \times C_3) \rtimes C_9$ та $n(G) = 119629$:
 - $IdGroup(R^*) = [162, 32]$, група $R^* \cong C_3 \times C_3 \times D_{18}$ та $n(R^*) = 12879$;
 - $IdGroup(R^*) = [162, 33]$, група $R^* \cong C_3 \times C_9 \times S_3$ та $n(R^*) = 3351$;
 - $IdGroup(R^*) = [162, 35]$, група $R^* \cong ((C_3 \times C_3) \rtimes C_3) \times S_3$ та $n(R^*) = 87$;

- $IdGroup(R^*) = [162, 36]$, $zpyyna R^* \cong C_3 \times ((C_9 \rtimes C_3) \rtimes C_2)$ $ma n(R^*) = 96472$;
- $IdGroup(R^*) = [162, 37]$, $zpyyna R^* \cong (C_9 \rtimes C_3) \times S_3$ $ma n(R^*) = 6810$;
- $IdGroup(R^*) = [162, 51]$, $zpyyna R^* \cong C_3 \times C_3 \times C_3 \times S_3$ $ma n(R^*) = 30$;
- $IdGroup(G) = [243, 10]$, $zpyyna G \cong C_{27} \times C_9$ $ma n(G) = 119298$:
 - $IdGroup(R^*) = [162, 3]$, $zpyyna R^* \cong C_9 \times D_{18}$ $ma n(R^*) = 477$;
 - $IdGroup(R^*) = [162, 6]$, $zpyyna R^* \cong (C_9 \rtimes C_9) \rtimes C_2$ $ma n(R^*) = 811$;
 - $IdGroup(R^*) = [162, 23]$, $zpyyna R^* \cong C_{18} \times C_9$ $ma n(R^*) = 21372$;
 - $IdGroup(R^*) = [162, 25]$, $zpyyna R^* \cong C_2 \times (C_9 \rtimes C_9)$ $ma n(R^*) = 96531$;
 - $IdGroup(R^*) = [162, 30]$, $zpyyna R^* \cong C_2 \times ((C_9 \times C_3) \rtimes C_3)$ $ma n(R^*) = 36$;
 - $IdGroup(R^*) = [162, 31]$, $zpyyna R^* \cong C_2 \times (C_3 \cdot ((C_3 \times C_3) \rtimes C_3) = (C_3 \times C_3) \cdot (C_3 \times C_3))$ $ma n(R^*) = 27$;
 - $IdGroup(R^*) = [162, 47]$, $zpyyna R^* \cong C_{18} \times C_3 \times C_3$ $ma n(R^*) = 6$;
 - $IdGroup(R^*) = [162, 49]$, $zpyyna R^* \cong C_6 \times (C_9 \rtimes C_3)$ $ma n(R^*) = 6$;
 - $IdGroup(R^*) = [162, 50]$, $zpyyna R^* \cong C_2 \times ((C_9 \times C_3) \rtimes C_3)$ $ma n(R^*) = 32$;
- $IdGroup(G) = [243, 11]$, $zpyyna G \cong C_{27} \rtimes C_9$ $ma n(G) = 1288$:
 - $IdGroup(R^*) = [162, 3]$, $zpyyna R^* \cong C_9 \times D_{18}$ $ma n(R^*) = 477$;

- $IdGroup(R^*) = [162, 6]$, $zpyna R^* \cong (C_9 \rtimes C_9) \rtimes C_2$ $ma n(R^*) = 811$;
- $IdGroup(G) = [243, 12]$, $zpyna G \cong (C_{27} \times C_3) \rtimes C_3$ $ma n(G) = 29989$:
 - $IdGroup(R^*) = [162, 33]$, $zpyna R^* \cong C_3 \times C_9 \times S_3$ $ma n(R^*) = 10306$;
 - $IdGroup(R^*) = [162, 37]$, $zpyna R^* \cong (C_9 \rtimes C_3) \times S_3$ $ma n(R^*) = 19683$;
- $IdGroup(G) = [243, 13]$, $zpyna G \cong ((C_9 \times C_3) \rtimes C_3) \rtimes C_3$ $ma n(G) = 139672$:
 - $IdGroup(R^*) = [162, 32]$, $zpyna R^* \cong C_3 \times C_3 \times D_{18}$ $ma n(R^*) = 2430$;
 - $IdGroup(R^*) = [162, 33]$, $zpyna R^* \cong C_3 \times C_9 \times S_3$ $ma n(R^*) = 90$;
 - $IdGroup(R^*) = [162, 34]$, $zpyna R^* \cong C_3 \times (((C_3 \times C_3) \rtimes C_3) \rtimes C_2)$ $ma n(R^*) = 81811$;
 - $IdGroup(R^*) = [162, 35]$, $zpyna R^* \cong ((C_3 \times C_3) \rtimes C_3) \times S_3$ $ma n(R^*) = 6723$;
 - $IdGroup(R^*) = [162, 36]$, $zpyna R^* \cong C_3 \times ((C_9 \rtimes C_3) \rtimes C_2)$ $ma n(R^*) = 32076$;
 - $IdGroup(R^*) = [162, 37]$, $zpyna R^* \cong (C_9 \rtimes C_3) \times S_3$ $ma n(R^*) = 342$;
 - $IdGroup(R^*) = [162, 51]$, $zpyna R^* \cong C_3 \times C_3 \times C_3 \times S_3$ $ma n(R^*) = 3321$;
 - $IdGroup(R^*) = [162, 52]$, $zpyna R^* \cong C_3 \times C_3 \times ((C_3 \times C_3) \rtimes C_2)$ $ma n(R^*) = 12879$;

- $IdGroup(G) = [243, 14]$, $epyna\ G \cong (C_9 \times C_3) \rtimes C_9$ $ma\ n(G) = 115020$:
 - $IdGroup(R^*) = [162, 32]$, $R^* \cong C_3 \times C_3 \times D_{18}$ $ma\ n(R^*) = 12393$;
 - $IdGroup(R^*) = [162, 33]$, $R^* \cong C_3 \times C_9 \times S_3$ $ma\ n(R^*) = 3321$;
 - $IdGroup(R^*) = [162, 36]$, $R^* \cong C_3 \times ((C_9 \rtimes C_3) \rtimes C_2)$ $ma\ n(R^*) = 92583$;
 - $IdGroup(R^*) = [162, 37]$, $R^* \cong (C_9 \rtimes C_3) \times S_3$ $ma\ n(R^*) = 6723$;
- $IdGroup(G) = [243, 15]$, $epyna\ G \cong (C_9 \times C_3) \rtimes C_9$ $ma\ n(G) = 117783$:
 - $IdGroup(R^*) = [162, 32]$, $epyna\ R^* \cong C_3 \times C_3 \times D_{18}$ $ma\ n(R^*) = 11961$;
 - $IdGroup(R^*) = [162, 33]$, $epyna\ R^* \cong C_3 \times C_9 \times S_3$ $ma\ n(R^*) = 3432$;
 - $IdGroup(R^*) = [162, 34]$, $epyna\ R^* \cong C_3 \times (((C_3 \times C_3) \rtimes C_3) \rtimes C_2)$ $ma\ n(R^*) = 5832$;
 - $IdGroup(R^*) = [162, 36]$, $epyna\ R^* \cong C_3 \times ((C_9 \rtimes C_3) \rtimes C_2)$ $ma\ n(R^*) = 89127$;
 - $IdGroup(R^*) = [162, 37]$, $epyna\ R^* \cong (C_9 \rtimes C_3) \times S_3$ $ma\ n(R^*) = 6702$;
 - $IdGroup(R^*) = [162, 52]$, $epyna\ R^* \cong C_3 \times C_3 \times ((C_3 \times C_3) \rtimes C_2)$ $ma\ n(R^*) = 729$;
- $IdGroup(G) = [243, 16]$, $epyna\ G \cong (C_{27} \rtimes C_3) \rtimes C_3$ $ma\ n(G) = 59049$:
 - $IdGroup(R^*) = [162, 33]$, $epyna\ R^* \cong C_3 \times C_9 \times S_3$ $ma\ n(R^*) = 19683$;
 - $IdGroup(R^*) = [162, 37]$, $epyna\ R^* \cong (C_9 \rtimes C_3) \times S_3$ $ma\ n(R^*) = 39366$;
- $IdGroup(G) = [243, 23]$, $epyna\ G \cong C_{81} \times C_3$ $ma\ n(G) = 3349$:

- $IdGroup(R^*) = [162, 8]$, група $R^* \cong C_{27} \times S_3$ та $n(R^*) = 28$;
- $IdGroup(R^*) = [162, 26]$, група $R^* \cong C_{54} \times C_3$ та $n(R^*) = 1134$;
- $IdGroup(R^*) = [162, 27]$, група $R^* \cong C_2 \times (C_{27} \rtimes C_3)$ та $n(R^*) = 2187$;
- $IdGroup(G) = [243, 24]$, група $G \cong C_{81} \rtimes C_3$, $n(G) = 28$ та $IdGroup(R^*) = [162, 8]$, група $R^* \cong C_{27} \times S_3$, $n(R^*) = 28$.

7.1.4. Локальні майже-кілець порядків 343

Відомо, що існує 5 неізоморфних груп порядку $7^3 = 343$. Виявляється, що всі вони є адитивними групами локальних майже-кілець. Наступна таблиця містить список усіх неізоморфних майже-кілець цього порядку, які не є майже-полями.

Наведено класифікацію локальних майже-кілець порядку 343.

Теорема 7.7. *Нехай $n(G)$ кількість усіх неізоморфних локальних майже-кілець R адитивна група R^+ яких ізоморфна групі G . Існує 88 локальних майже-кілець R порядку 343:*

- $IdGroup(G) = [343, 1]$, група $G \cong C_{343}$ та $n(G) = 1$;
- $IdGroup(G) = [343, 2]$, група $G \cong C_{49} \times C_7$ та $n(G) = 31$;
- $IdGroup(G) = [343, 3]$, група $G \cong (C_7 \times C_7) \rtimes C_7$ та $n(G) = 8$;
- $IdGroup(G) = [343, 4]$, група $G \cong C_{49} \rtimes C_7$ та $n(G) = 2$;
- $IdGroup(G) = [343, 5]$, група $G \cong C_7 \times C_7 \times C_7$ та $n(G) = 46$.

7.1.5. Локальні майже-кілець порядків 1331

Відомо, що існує 5 неізоморфних груп порядку $11^3 = 1331$. Виявляється, що всі вони є адитивними групами локальних майже-кілець. Наступна теорема містить список усіх неізоморфних майже-кілець цього порядку.

Далі, наведено класифікацію локальних майже-кілець порядку 1331.

Теорема 7.8. *Існує 158 локальних майже-кілець порядку 1331:*

- $IdGroup(G) = [1331, 1]$, група $G \cong C_{81}$ та $n(G) = 1$;
- $IdGroup(G) = [1331, 2]$, група $G \cong C_{121} \times C_{11}$ та $n(G) = 47$;
- $IdGroup(G) = [1331, 3]$, група $G \cong (C_{11} \times C_{11}) \rtimes C_{11}$ та $n(G) = 12$;
- $IdGroup(G) = [1331, 4]$, група $G \cong C_{121} \rtimes C_{11}$ та $n(G) = 2$;
- $IdGroup(G) = [1331, 5]$, група $G \cong C_{11} \times C_{11} \times C_{11}$ та $n(G) = 96$.

7.2. Ендоциклічні групи та локальні майже-кілець

Нехай G — група та $\text{End } G$ — множина всіх її ендоморфізмів, яку можна розглядати як напівгрупу відносно операції композиції ендоморфізмів. Для кожного $g \in G$ позначимо через $g^{\text{End } G}$ множину $\{g^\alpha \mid \alpha \in \text{End } G\}$ всіх образів елемента g відносно ендоморфізмів із $\text{End } G$.

Нагадаємо означення ендоморфно циклічної групи.

Означення 7.9. Групу G назвемо ендоморфно циклічною, коли в ній існує елемент g , для якого $G = g^{\text{End } G}$.

Пакет SONATA містить бібліотеку майже-кілець з одиницею *AllLibraryNearRingsWithOne*. У цій бібліотеці майже-кілець впорядковані відповідно до їхніх адитивних груп G , наприклад, команда

$$N := \text{AllLibraryNearRingsWithOne}(G)$$

визначає список локальних майже-кілець N .

Ми використовуємо функцію *IsEndoCyclicGroup* з пакету LocalNR для перевірки, чи є G ендоциклічною групою.

Нехай $[n, i]$ — i -та група порядку n у бібліотеці SmallGroups в GAP. Позначимо через C_n , D_n та Q_n циклічну групу, групу діедра та групу кватерніонів порядку n , відповідно.

7.2.1. Локальні майже-кілець та ендоциклічні 2-породжені групи порядку 64

Існує 267 неізоморфних груп порядку $64 = 2^6$, з яких 53 є 2-породженими групами, і лише 39 з цих груп є ендоциклічними. Більш того, 24 з цих груп є адитивними групами локальних майже-кілець.

Наступну лему отримано за допомогою GAP, пакетів LocalNR та SONATA, де наведено список ендоциклічних 2-породжених груп порядку 64.

Лема 7.10. *Наступні 2-породженні групи G порядку 64 є ендоциклічними. Більш того, якщо G є адитивною групою локального майже-кілець R , то виконується наступне.*

- $IdGroup(G) = [64, 2]$, група $G \cong C_8 \times C_8$ та $n(G) = 1683$;
- $IdGroup(G) = [64, 3]$, група $G \cong C_8 \rtimes C_8$ та $n(G) = 1628$;
- $IdGroup(G) = [64, 4]$, група $G \cong ((C_8 \times C_2) \rtimes C_2) \rtimes C_2$ та $n(G) = 167245$;
- $IdGroup(G) = [64, 5]$, група $G \cong (C_4 \times C_2) \rtimes C_8$ та $n(G) = 118190$;
- $IdGroup(G) = [64, 6]$, група $G \cong (C_8 \times C_4) \rtimes C_2$ та $n(G) = 0$;
- $IdGroup(G) = [64, 7]$, група $G \cong Q_8 \rtimes C_8$ та $n(G) = 0$;

- $IdGroup(G) = [64, 8]$, $zpyna\ G \cong ((C_8 \times C_2) \rtimes C_2) \rtimes C_2$ $ma\ n(G) = 0$;
- $IdGroup(G) = [64, 9]$, $zpyna\ G \cong (C_2 \times Q_8) \rtimes C_4$ $ma\ n(G) = 0$;
- $IdGroup(G) = [64, 10]$, $zpyna\ G \cong (C_8 \rtimes C_4) \rtimes C_2$ $ma\ n(G) = 7424$;
- $IdGroup(G) = [64, 11]$, $zpyna\ G \cong (C_2 \times C_2).((C_4 \times C_2) \rtimes C_2) = (C_4 \times C_2).(C_4 \times C_2)$ $ma\ n(G) = 0$;
- $IdGroup(G) = [64, 12]$, $zpyna\ G \cong (C_4 \rtimes C_8) \rtimes C_2$ $ma\ n(G) = 5633$;
- $IdGroup(G) = [64, 14]$, $zpyna\ G \cong (C_2 \times C_2).((C_4 \times C_2) \rtimes C_2) = (C_4 \times C_2).(C_4 \times C_2)$ $ma\ n(G) = 5520$;
- $IdGroup(G) = [64, 15]$, $zpyna\ G \cong C_8 \rtimes C_8$ $ma\ n(G) = 2384$;
- $IdGroup(G) = [64, 16]$, $zpyna\ G \cong C_8 \rtimes C_8$ $ma\ n(G) = 2384$;
- $IdGroup(G) = [64, 17]$, $zpyna\ G \cong (C_8 \times C_2) \rtimes C_4$ $ma\ n(G) = 433060$;
- $IdGroup(G) = [64, 18]$, $zpyna\ G \cong (C_8 \times C_2) \rtimes C_4$ $ma\ n(G) = 0$;
- $IdGroup(G) = [64, 19]$, $zpyna\ G \cong C_4.(C_4 \times C_4)$ $ma\ n(G) = 0$;
- $IdGroup(G) = [64, 20]$, $zpyna\ G \cong (C_4 \times C_4) \rtimes C_4$ $ma\ n(G) = 0$;
- $IdGroup(G) = [64, 21]$, $zpyna\ G \cong (C_8 \times C_2) \rtimes C_4$ $ma\ n(G) = 0$;
- $IdGroup(G) = [64, 23]$, $zpyna\ G \cong (C_4 \times C_2 \times C_2) \rtimes C_4$ $ma\ n(G) = 111758$;
- $IdGroup(G) = [64, 24]$, $zpyna\ G \cong (C_8 \rtimes C_2) \rtimes C_4$ $ma\ n(G) = 109189$;
- $IdGroup(G) = [64, 26]$, $zpyna\ G \cong C_{16} \times C_4$ $ma\ n(G) = 11467$;
- $IdGroup(G) = [64, 27]$, $zpyna\ G \cong C_{16} \rtimes C_4$ $ma\ n(G) = 11467$;
- $IdGroup(G) = [64, 28]$, $zpyna\ G \cong C_{16} \rtimes C_4$ $ma\ n(G) = 0$;

- $IdGroup(G) = [64, 29]$, *група* $G \cong (C_{16} \times C_2) \rtimes C_2$ *та* $n(G) = 28185$;
- $IdGroup(G) = [64, 30]$, *група* $G \cong (C_{16} \rtimes C_2) \rtimes C_2$ *та* $n(G) = 4433$;
- $IdGroup(G) = [64, 32]$, *група* $G \cong ((C_8 \rtimes C_2) \rtimes C_2) \rtimes C_2$ *та* $n(G) = 0$;
- $IdGroup(G) = [64, 33]$, *група* $G \cong (C_4 \times C_2 \times C_2) \rtimes C_4$ *та* $n(G) =$;
- $IdGroup(G) = [64, 34]$, *група* $G \cong (((C_4 \times C_2) \rtimes C_2) \rtimes C_2) \rtimes C_2$ *та* $n(G) = 16177$;
- $IdGroup(G) = [64, 35]$, *група* $G \cong (C_4 \times C_4) \rtimes C_4$ *та* $n(G) = 15504$;
- $IdGroup(G) = [64, 36]$, *група* $G \cong (C_2 \cdot ((C_4 \times C_2) \rtimes C_2) = (C_2 \times C_2) \cdot (C_4 \times C_2)) \rtimes C_2$ *та* $n(G) = 15761$;
- $IdGroup(G) = [64, 37]$, *група* $G \cong C_2 \cdot (((C_4 \times C_2) \rtimes C_2) \rtimes C_2) = (C_4 \times C_2) \cdot (C_4 \times C_2)$ *та* $n(G) = 15920$;
- $IdGroup(G) = [64, 38]$, *група* $G \cong (C_{16} \times C_2) \rtimes C_2$ *та* $n(G) = 0$;
- $IdGroup(G) = [64, 41]$, *група* $G \cong (C_{16} \rtimes C_2) \rtimes C_2$ *та* $n(G) = 0$;
- $IdGroup(G) = [64, 44]$, *група* $G \cong C_4 \rtimes C_{16}$ *та* $n(G) = 28500$;
- $IdGroup(G) = [64, 45]$, *група* $G \cong C_8.D_8 = C_4 \cdot (C_8 \times C_2)$ *та* $n(G) = 1920$;
- $IdGroup(G) = [64, 50]$, *група* $G \cong C_{32} \times C_2$ *та* $n(G) = 257$;
- $IdGroup(G) = [64, 51]$, *група* $G \cong C_{32} \rtimes C_2$ *та* $n(G) = 257$;
- $IdGroup(G) = [64, 52]$, *група* $G \cong D_{64}$ *та* $n(G) = 0$.

З леми 7.10 випливає наступний результат.

Теорема 7.11. *Нехай G — 2-породжена група порядку 64. Якщо G — адитивна група локального майже-кільця R , то G є ендоциклічною.*

7.2.2. 2-Породжені ендоциклічні групи порядку 256

Нагадаємо, що експонентою групи є найменше спільне кратне порядків її елементів. Зокрема, експонентою скінченної p -групи є максимальний порядок її елементів.

Наступна лема визначає експоненту адитивної групи скінченного майже-кілля з одиницею.

Лема 7.12. *Експонента адитивної групи скінченного майже-кілля R з одиницею дорівнює адитивному порядку його одиниці, який співпадає з адитивним порядком кожного елементу його мультиплікативної групи R^* .*

Лема 7.13. *Нехай R — локальне майже-кілля порядку p^n . Тоді $|R^*| = p^n - p^k$, де $\lfloor \frac{n}{2} \rfloor \leq k < n$.*

Позначимо через $U(G)$ множину всіх елементів групи G , порядок яких дорівнює експоненті цієї групи.

Безпосередній наслідок леми 7.13.

Наслідок 7.14. *Якщо група G є адитивною групою локального майже-кілля R порядку p^n , тоді $U(G)$ не менше $p^n - p^{n-1}$.*

Існує 56092 неізоморфних груп порядку $256 = 2^8$, з яких 540 є 2-породженими групами: 3 групи мають експоненту 128, 9 груп мають експоненту 64, 30 груп мають експоненту 32, 107 груп мають експоненту 16, 84 групи мають експоненту 8, та 3 групи мають експоненту 4.

Застосовуючи систему комп'ютерної алгебри GAP, пакети SONATA та LocalNR, ми визначили всі ендоциклічні 2-породжені групи G порядку 256 експоненти 16 та порядок множини всіх елементів групи G , порядок яких дорівнює експоненті цієї групи.

В наступній лемі наведено ендоциклічні 2-породжені групи порядку 256 та експоненти 4.

Лема 7.15. *Наступні 2-породжені групи G порядку 256 та експоненти 4 є ендоциклічними, та вказано порядок $U(G)$ для кожної групи G :*

- $IdGroup(G) = [256, 295]$, група $G \cong (C_2 \times ((C_2 \times C_2 \times C_2) \rtimes C_4)) \rtimes C_4$ та $|U(G)| = 208$;
- $IdGroup(G) = [256, 298]$, група $G \cong (C_2 \times ((C_2 \times C_2 \times C_2) \rtimes C_4)) \rtimes C_4$ та $|U(G)| = 208$;
- $IdGroup(G) = [256, 306]$, група $G \cong (((C_4 \times C_2) \rtimes C_4) \rtimes C_2) \rtimes C_4$ та $|U(G)| = 224$.

В наступній лемі наведено ендоциклічні 2-породжені групи порядку 256 та експоненти 8.

Лема 7.16. *Наступні 2-породжені групи G порядку 256 та експоненти 8 є ендоциклічними, та вказано порядок $U(G)$ для кожної групи G :*

- $IdGroup(G) = [256, 2]$, група $G \cong (C_8 \times C_4) \rtimes C_8$ та $|U(G)| = 192$;
- $IdGroup(G) = [256, 3]$, група $G \cong (C_4 \rtimes C_8) \rtimes C_8$ та $|U(G)| = 192$;
- $IdGroup(G) = [256, 4]$, група $G \cong ((C_8 \times C_2) \rtimes C_2) \rtimes C_8$ та $|U(G)| = 192$;
- $IdGroup(G) = [256, 5]$, група $G \cong ((C_8 \times C_2) \rtimes C_4) \rtimes C_4$ та $|U(G)| = 128$;
- $IdGroup(G) = [256, 6]$, група $G \cong (C_8 \times C_4) \rtimes C_8$ та $|U(G)| = 192$;
- $IdGroup(G) = [256, 7]$, група $G \cong (C_8 \times C_4) \rtimes C_8$ та $|U(G)| = 192$;
- $IdGroup(G) = [256, 8]$, група $G \cong (C_8 \times C_2 \times C_2) \rtimes C_8$ та $|U(G)| = 192$;
- $IdGroup(G) = [256, 9]$, група $G \cong ((C_8 \times C_2) \rtimes C_2) \rtimes C_8$ та $|U(G)| = 192$;

- $IdGroup(G) = [256, 10]$, $zpyna\ G \cong (C_4 \rtimes C_8) \rtimes C_8$ $ma\ |U(G)| = 192$;
- $IdGroup(G) = [256, 11]$, $zpyna\ G \cong (C_8 \rtimes C_4) \rtimes C_8$ $ma\ |U(G)| = 192$;
- $IdGroup(G) = [256, 12]$, $zpyna\ G \cong ((C_8 \times C_2) \rtimes C_4) \rtimes C_4$ $ma\ |U(G)| = 128$;
- $IdGroup(G) = [256, 13]$, $zpyna\ G \cong ((C_8 \times C_2) \rtimes C_4) \rtimes C_4$ $ma\ |U(G)| = 128$;
- $IdGroup(G) = [256, 14]$, $zpyna\ G \cong (C_2 \times (C_8 \rtimes C_2)) \rtimes C_8$ $ma\ |U(G)| = 192$;
- $IdGroup(G) = [256, 15]$, $zpyna\ G \cong (C_4 \rtimes C_8) \rtimes C_8$ $ma\ |U(G)| = 192$;
- $IdGroup(G) = [256, 16]$, $zpyna\ G \cong (C_2 \times (C_4 \rtimes C_8)) \rtimes C_4$ $ma\ |U(G)| = 128$;
- $IdGroup(G) = [256, 17]$, $zpyna\ G \cong ((C_8 \times C_2) \rtimes C_2) \rtimes C_8$ $ma\ |U(G)| = 192$;
- $IdGroup(G) = [256, 18]$, $zpyna\ G \cong (C_8 \rtimes C_4) \rtimes C_8$ $ma\ |U(G)| = 192$;
- $IdGroup(G) = [256, 19]$, $zpyna\ G \cong (C_4 \rtimes C_8) \rtimes C_8$ $ma\ |U(G)| = 192$;
- $IdGroup(G) = [256, 20]$, $zpyna\ G \cong (C_2 \times ((C_8 \times C_2) \rtimes C_2)) \rtimes C_4$ $ma\ |U(G)| = 128$;
- $IdGroup(G) = [256, 21]$, $zpyna\ G \cong ((C_8 \times C_2) \rtimes C_2) \rtimes C_8$ $ma\ |U(G)| = 192$;
- $IdGroup(G) = [256, 22]$, $zpyna\ G \cong (C_2 \times ((C_4 \times C_2) \rtimes C_4)) \rtimes C_4$ $ma\ |U(G)| = 192$;
- $IdGroup(G) = [256, 23]$, $zpyna\ G \cong ((C_8 \times C_2) \rtimes C_2) \rtimes C_8$ $ma\ |U(G)| = 64$;

- $IdGroup(G) = [256, 35]$, $zpyna\ G \cong (C_2 \times C_2 \times C_2).((C_4 \times C_2) \rtimes C_4) = (C_4 \times C_2 \times C_2).(C_4 \times C_4)$ $ma\ |U(G)| = 192$;
- $IdGroup(G) = [256, 36]$, $zpyna\ G \cong (C_2 \times C_2 \times C_2).((C_4 \times C_2) \rtimes C_4) = (C_4 \times C_2 \times C_2).(C_4 \times C_4)$ $ma\ |U(G)| = 192$;
- $IdGroup(G) = [256, 38]$, $zpyna\ G \cong (C_2 \times C_2 \times C_2).((C_4 \times C_2) \rtimes C_4) = (C_4 \times C_2 \times C_2).(C_4 \times C_4)$ $ma\ |U(G)| = 192$;
- $IdGroup(G) = [256, 91]$, $zpyna\ G \cong ((C_4 \times C_2 \times C_2) \rtimes C_8) \rtimes C_2$ $ma\ |U(G)| = 128$;
- $IdGroup(G) = [256, 92]$, $zpyna\ G \cong (C_2 \times (C_4 \rtimes C_4)) \rtimes C_8$ $ma\ |U(G)| = 128$;
- $IdGroup(G) = [256, 94]$, $zpyna\ G \cong ((C_4 \times C_4) \rtimes C_8) \rtimes C_2$ $ma\ |U(G)| = 160$;
- $IdGroup(G) = [256, 103]$, $zpyna\ G \cong ((C_4 \times C_4) \rtimes C_8) \rtimes C_2$ $ma\ |U(G)| = 160$;
- $IdGroup(G) = [256, 110]$, $zpyna\ G \cong ((C_4 \times C_2) \rtimes C_4) \rtimes C_8$ $ma\ |U(G)| = 160$;
- $IdGroup(G) = [256, 111]$, $zpyna\ G \cong ((C_4 \times C_2) \rtimes C_4) \rtimes C_8$ $ma\ |U(G)| = 128$;
- $IdGroup(G) = [256, 117]$, $zpyna\ G \cong ((C_2 \times C_2).(C_2 \times C_2 \times C_2)) \rtimes C_8$ $ma\ |U(G)| = 160$;
- $IdGroup(G) = [256, 119]$, $zpyna\ G \cong (C_2 \times C_2 \times Q_8) \rtimes C_8$ $ma\ |U(G)| = 128$;
- $IdGroup(G) = [256, 120]$, $zpyna\ G \cong (C_2 \times (C_4 \rtimes C_4)) \rtimes C_8$ $ma\ |U(G)| = 128$;

- $IdGroup(G) = [256, 122]$, $zpyna\ G \cong ((C_2 \times C_2).(C_2 \times C_2 \times C_2)) \rtimes C_8$
 $ma\ |U(G)| = 160$;
- $IdGroup(G) = [256, 175]$, $zpyna\ G \cong (((C_8 \times C_2) \rtimes C_2) \rtimes C_2) \rtimes C_4$
 $ma\ |U(G)| = 192$;
- $IdGroup(G) = [256, 176]$, $zpyna\ G \cong (C_8 \times C_2 \times C_2) \rtimes C_8$ $ma\ |U(G)| = 192$;
- $IdGroup(G) = [256, 177]$, $zpyna\ G \cong ((C_4 \times C_2) \rtimes C_8) \rtimes C_4$ $ma\ |U(G)| = 128$;
- $IdGroup(G) = [256, 178]$, $zpyna\ G \cong (C_8 \times C_2 \times C_2) \rtimes C_8$ $ma\ |U(G)| = 192$;
- $IdGroup(G) = [256, 191]$, $zpyna\ G \cong ((C_8 \rtimes C_2) \rtimes C_2) \rtimes C_8$ $ma\ |U(G)| = 192$;
- $IdGroup(G) = [256, 192]$, $zpyna\ G \cong (((C_8 \times C_2) \rtimes C_2) \rtimes C_2) \rtimes C_4$
 $ma\ |U(G)| = 128$;
- $IdGroup(G) = [256, 193]$, $zpyna\ G \cong ((C_4 \times C_2) \rtimes C_8) \rtimes C_4$ $ma\ |U(G)| = 128$;
- $IdGroup(G) = [256, 194]$, $zpyna\ G \cong (C_2.(C_4 \times C_2) \rtimes C_2) = (C_2 \times C_2).(C_4 \times C_2)) \rtimes C_8$ $ma\ |U(G)| = 192$;
- $IdGroup(G) = [256, 201]$, $zpyna\ G \cong (((C_4 \times C_2) \rtimes C_2) \rtimes C_4) \rtimes C_4$
 $ma\ |U(G)| = 64$;
- $IdGroup(G) = [256, 238]$, $zpyna\ G \cong (C_2 \times C_2 \times (C_4 \rtimes C_4)) \rtimes C_4$ $ma\ |U(G)| = 64$;
- $IdGroup(G) = [256, 292]$, $zpyna\ G \cong (C_2 \times ((C_2 \times C_2 \times C_2) \rtimes C_4)) \rtimes C_4$
 $ma\ |U(G)| = 64$;

- $IdGroup(G) = [256, 293]$, $zpyna\ G \cong (C_2 \times ((C_2 \times C_2 \times C_2) \rtimes C_4)) \rtimes C_4$
 $ma\ |U(G)| = 64$;
- $IdGroup(G) = [256, 296]$, $zpyna\ G \cong (C_2 \times (C_2 \cdot ((C_4 \times C_2) \rtimes C_2) =$
 $(C_2 \times C_2) \cdot (C_4 \times C_2))) \rtimes C_4\ ma\ |U(G)| = 128$;
- $IdGroup(G) = [256, 299]$, $zpyna\ G \cong (C_2 \times ((C_8 \rtimes C_2) \rtimes C_2)) \rtimes C_4$
 $ma\ |U(G)| = 128$;
- $IdGroup(G) = [256, 301]$, $zpyna\ G \cong (C_2 \times ((C_2 \times C_2 \times C_2) \rtimes C_4)) \rtimes C_4$
 $ma\ |U(G)| = 64$;
- $IdGroup(G) = [256, 302]$, $zpyna\ G \cong (C_2 \times ((C_2 \times C_2 \times C_2) \rtimes C_4)) \rtimes C_4$
 $ma\ |U(G)| = 64$;
- $IdGroup(G) = [256, 304]$, $zpyna\ G \cong ((C_2 \times ((C_4 \times C_2) \rtimes C_2)) \rtimes C_2) \rtimes C_4$
 $ma\ |U(G)| = 64$;
- $IdGroup(G) = [256, 305]$, $zpyna\ G \cong C_2 \cdot ((C_2 \times ((C_4 \times C_2) \rtimes C_2)) \rtimes$
 $C_4) = (C_2 \times C_2 \times C_2 \times C_2) \cdot (C_4 \times C_4)\ ma\ |U(G)| = 192$;
- $IdGroup(G) = [256, 307]$, $zpyna\ G \cong ((C_2 \times (C_8 \rtimes C_2)) \rtimes C_2) \rtimes C_4$
 $ma\ |U(G)| = 128$;
- $IdGroup(G) = [256, 312]$, $zpyna\ G \cong (((C_8 \times C_2) \rtimes C_2) \rtimes C_2) \rtimes C_4$
 $ma\ |U(G)| = 128$;
- $IdGroup(G) = [256, 318]$, $zpyna\ G \cong ((C_4 \times C_2) \rtimes C_8) \rtimes C_4\ ma$
 $|U(G)| = 128$;
- $IdGroup(G) = [256, 326]$, $zpyna\ G \cong (((((C_8 \times C_2) \rtimes C_2) \rtimes C_2) \rtimes C_2) \rtimes C_2) \rtimes C_2$
 $ma\ |U(G)| = 128$;
- $IdGroup(G) = [256, 327]$, $zpyna\ G \cong (((((C_8 \times C_2) \rtimes C_2) \rtimes C_2) \rtimes C_2) \rtimes C_2) \rtimes C_2$
 $ma\ |U(G)| = 128$;

- $IdGroup(G) = [256, 332]$, група $G \cong (((C_4 \times C_2) \rtimes C_8) \rtimes C_2) \rtimes C_2$ та $|U(G)| = 160$;
- $IdGroup(G) = [256, 333]$, група $G \cong ((C_2 \times Q_8) \rtimes C_8) \rtimes C_2$ та $|U(G)| = 160$;
- $IdGroup(G) = [256, 336]$, група $G \cong (C_4 \times C_4 \times C_2) \rtimes C_8$ та $|U(G)| = 128$;
- $IdGroup(G) = [256, 337]$, група $G \cong (C_2 \times ((C_4 \times C_2) \rtimes C_2)) \rtimes C_8$ та $|U(G)| = 128$;
- $IdGroup(G) = [256, 340]$, група $G \cong ((C_4 \times C_4) \rtimes C_8) \rtimes C_2$ та $|U(G)| = 160$;
- $IdGroup(G) = [256, 341]$, група $G \cong (C_4 \rtimes Q_8) \rtimes C_8$ та $|U(G)| = 160$;
- $IdGroup(G) = [256, 342]$, група $G \cong ((C_4 \times C_4) \rtimes C_8) \rtimes C_2$ та $|U(G)| = 160$;
- $IdGroup(G) = [256, 343]$, група $G \cong (C_4 \rtimes Q_8) \rtimes C_8$ та $|U(G)| = 160$;
- $IdGroup(G) = [256, 346]$, група $G \cong ((C_2 \times C_2) \cdot (C_2 \times C_2 \times C_2)) \rtimes C_8$ та $|U(G)| = 160$;
- $IdGroup(G) = [256, 347]$, група $G \cong ((C_2 \times C_2) \cdot (C_2 \times C_2 \times C_2)) \rtimes C_8$ та $|U(G)| = 160$.

В наступному твердженні класифіковано ендосиклічні 2-породжені групи порядку 256 та експоненти 16

(https://github.com/raemarina/256_exp_16).

Лема 7.17. Наступні 2-породжені групи G порядку 256 та експоненти 16 є ендосиклічними, та вказано порядок $U(G)$ для кожної групи G :

- $IdGroup(G) = [256, 39]$, група $G \cong C_{16} \times C_{16}$ та $|U(G)| = 192$;

- $IdGroup(G) = [256, 40]$, *zpyna* $G \cong C_{16} \rtimes C_{16}$ *ma* $|U(G)| = 192$;
- $IdGroup(G) = [256, 41]$, *zpyna* $G \cong C_{16} \rtimes C_{16}$ *ma* $|U(G)| = 192$;
- $IdGroup(G) = [256, 42]$, *zpyna* $G \cong (((C_{16} \times C_2) \rtimes C_2) \rtimes C_2) \rtimes C_2$
ma $|U(G)| = 128$;
- $IdGroup(G) = [256, 43]$, *zpyna* $G \cong (C_4 \times C_2 \times C_2) \rtimes C_{16}$ *ma* $|U(G)| = 128$;
- $IdGroup(G) = [256, 44]$, *zpyna* $G \cong ((C_4 \times C_2) \rtimes C_{16}) \rtimes C_2$ *ma*
 $|U(G)| = 128$;
- $IdGroup(G) = [256, 45]$, *zpyna* $G \cong (C_2 \times Q_8) \rtimes C_{16}$ *ma* $|U(G)| = 128$;
- $IdGroup(G) = [256, 46]$, *zpyna* $G \cong (((C_{16} \times C_2) \rtimes C_2) \rtimes C_2) \rtimes C_2$
ma $|U(G)| = 128$;
- $IdGroup(G) = [256, 47]$, *zpyna* $G \cong (C_4 \times C_2).((C_2 \times C_2 \times C_2) \rtimes C_4) = (C_4 \times C_2 \times C_2).(C_8 \times C_2)$ *ma* $|U(G)| = 128$;
- $IdGroup(G) = [256, 48]$, *zpyna* $G \cong ((C_4 \times C_2) \rtimes C_{16}) \rtimes C_2$ *ma*
 $|U(G)| = 128$;
- $IdGroup(G) = [256, 49]$, *zpyna* $G \cong (C_4 \times C_2).((C_2 \times C_2 \times C_2) \rtimes C_4) = (C_4 \times C_2 \times C_2).(C_8 \times C_2)$ *ma* $|U(G)| = 128$;
- $IdGroup(G) = [256, 50]$, *zpyna* $G \cong (C_4 \times C_4) \rtimes C_{16}$ *ma* $|U(G)| = 128$;
- $IdGroup(G) = [256, 51]$, *zpyna* $G \cong (C_4 \times C_4) \rtimes C_{16}$ *ma* $|U(G)| = 128$;
- $IdGroup(G) = [256, 52]$, *zpyna* $G \cong ((C_4 \times C_2) \rtimes C_2) \rtimes C_{16}$ *ma*
 $|U(G)| = 128$;
- $IdGroup(G) = [256, 53]$, *zpyna* $G \cong (C_4 \times C_2).((C_2 \times C_2 \times C_2) \rtimes C_4) = (C_4 \times C_2 \times C_2).(C_8 \times C_2)$ *ma* $|U(G)| = 128$;

- $IdGroup(G) = [256, 54]$, $zpyna\ G \cong (C_4 \times C_2).((C_2 \times C_2 \times C_2) \rtimes C_4) = (C_4 \times C_2 \times C_2).(C_8 \times C_2)\ ma\ |U(G)| = 128$;
- $IdGroup(G) = [256, 56]$, $zpyna\ G \cong (C_{16} \times C_8) \rtimes C_2\ ma\ |U(G)| = 128$;
- $IdGroup(G) = [256, 57]$, $zpyna\ G \cong Q_{16} \rtimes C_{16}\ ma\ |U(G)| = 128$;
- $IdGroup(G) = [256, 58]$, $zpyna\ G \cong (C_8 \rtimes C_{16}) \rtimes C_2\ ma\ |U(G)| = 128$;
- $IdGroup(G) = [256, 59]$, $zpyna\ G \cong Q_{16} \rtimes C_{16}\ ma\ |U(G)| = 128$;
- $IdGroup(G) = [256, 64]$, $zpyna\ G \cong (((C_{16} \times C_2) \rtimes C_2) \rtimes C_2) \rtimes C_2\ ma\ |U(G)| = 64$;
- $IdGroup(G) = [256, 80]$, $zpyna\ G \cong (C_8 \rtimes C_{16}) \rtimes C_2\ ma\ |U(G)| = 128$;
- $IdGroup(G) = [256, 84]$, $zpyna\ G \cong (C_8 \rtimes C_{16}) \rtimes C_2\ ma\ |U(G)| = 128$;
- $IdGroup(G) = [256, 87]$, $zpyna\ G \cong C_{16} \rtimes C_{16}\ ma\ |U(G)| = 192$;
- $IdGroup(G) = [256, 88]$, $zpyna\ G \cong C_{16} \rtimes C_{16}\ ma\ |U(G)| = 192$;
- $IdGroup(G) = [256, 89]$, $zpyna\ G \cong C_{16} \rtimes C_{16}\ ma\ |U(G)| = 192$;
- $IdGroup(G) = [256, 90]$, $zpyna\ G \cong ((C_{16} \times C_2) \rtimes C_4) \rtimes C_2\ ma\ |U(G)| = 128$;
- $IdGroup(G) = [256, 93]$, $zpyna\ G \cong ((C_{16} \rtimes C_2) \rtimes C_4) \rtimes C_2\ ma\ |U(G)| = 128$;
- $IdGroup(G) = [256, 95]$, $zpyna\ G \cong ((C_{16} \rtimes C_2) \rtimes C_4) \rtimes C_2\ ma\ |U(G)| = 128$;
- $IdGroup(G) = [256, 96]$, $zpyna\ G \cong (C_2 \times C_2).((C_4 \rtimes C_8) \rtimes C_2) = (C_4 \times C_4).(C_8 \times C_2)\ ma\ |U(G)| = 128$;
- $IdGroup(G) = [256, 97]$, $zpyna\ G \cong ((C_{16} \times C_2) \rtimes C_4) \rtimes C_2\ ma\ |U(G)| = 64$;

- $IdGroup(G) = [256, 98]$, $zpyna\ G \cong ((C_8 \times C_2) \rtimes C_8) \rtimes C_2$ $ma\ |U(G)| = 64$;
- $IdGroup(G) = [256, 99]$, $zpyna\ G \cong (C_2 \times Q_{16}) \rtimes C_8$ $ma\ |U(G)| = 64$;
- $IdGroup(G) = [256, 100]$, $zpyna\ G \cong ((C_{16} \times C_2) \rtimes C_4) \rtimes C_2$ $ma\ |U(G)| = 64$;
- $IdGroup(G) = [256, 101]$, $zpyna\ G \cong (C_2 \times Q_{16}) \rtimes C_8$ $ma\ |U(G)| = 64$;
- $IdGroup(G) = [256, 102]$, $zpyna\ G \cong ((C_8 \times C_2) \rtimes C_8) \rtimes C_2$ $ma\ |U(G)| = 102$;
- $IdGroup(G) = [256, 104]$, $zpyna\ G \cong ((C_{16} \times C_2) \rtimes C_4) \rtimes C_2$ $ma\ |U(G)| = 128$;
- $IdGroup(G) = [256, 105]$, $zpyna\ G \cong (C_2 \times C_2).((C_8 \rtimes C_4) \rtimes C_2) = (C_4 \times C_4).(C_8 \times C_2)$ $ma\ |U(G)| = 128$;
- $IdGroup(G) = [256, 106]$, $zpyna\ G \cong (C_4 \rtimes C_4) \rtimes C_{16}$ $ma\ |U(G)| = 128$;
- $IdGroup(G) = [256, 107]$, $zpyna\ G \cong (C_8 \rtimes C_4) \rtimes C_8$ $ma\ |U(G)| = 64$;
- $IdGroup(G) = [256, 109]$, $zpyna\ G \cong (C_8 \rtimes C_4) \rtimes C_8$ $ma\ |U(G)| = 64$;
- $IdGroup(G) = [256, 113]$, $zpyna\ G \cong (C_8 \rtimes C_4) \rtimes C_8$ $ma\ |U(G)| = 64$;
- $IdGroup(G) = [256, 114]$, $zpyna\ G \cong (C_8 \rtimes C_4) \rtimes C_8$ $ma\ |U(G)| = 64$;
- $IdGroup(G) = [256, 115]$, $zpyna\ G \cong (C_8 \rtimes C_4) \rtimes C_8$ $ma\ |U(G)| = 64$;
- $IdGroup(G) = [256, 116]$, $zpyna\ G \cong (C_8 \rtimes C_4) \rtimes C_8$ $ma\ |U(G)| = 128$;
- $IdGroup(G) = [256, 121]$, $zpyna\ G \cong (C_2 \times Q_8) \rtimes C_{16}$ $ma\ |U(G)| = 128$;

- $IdGroup(G) = [256, 124]$, *zpyna* $G \cong ((C_2 \times C_2).(C_2 \times C_2 \times C_2)) \rtimes C_8$
ma $|U(G)| = 128$;
- $IdGroup(G) = [256, 125]$, *zpyna* $G \cong (C_4 \times C_2).((C_2 \times C_2 \times C_2) \rtimes C_4) = (C_4 \times C_2 \times C_2).(C_8 \times C_2)$ *ma* $|U(G)| = 128$;
- $IdGroup(G) = [256, 126]$, *zpyna* $G \cong (C_{16} \times C_2) \rtimes C_8$ *ma* $|U(G)| = 128$;
- $IdGroup(G) = [256, 127]$, *zpyna* $G \cong (C_{16} \times C_2) \rtimes C_8$ *ma* $|U(G)| = 128$;
- $IdGroup(G) = [256, 130]$, *zpyna* $G \cong (C_{16} \rtimes C_2) \rtimes C_8$ *ma* $|U(G)| = 128$;
- $IdGroup(G) = [256, 131]$, *zpyna* $G \cong (C_{16} \rtimes C_2) \rtimes C_8$ *ma* $|U(G)| = 128$;
- $IdGroup(G) = [256, 133]$, *zpyna* $G \cong (C_{16} \times C_4) \rtimes C_4$ *ma* $|U(G)| = 128$;
- $IdGroup(G) = [256, 134]$, *zpyna* $G \cong (C_{16} \rtimes C_4) \rtimes C_4$ *ma* $|U(G)| = 128$;
- $IdGroup(G) = [256, 136]$, *zpyna* $G \cong (C_8 \times C_2) \rtimes C_{16}$ *ma* $|U(G)| = 128$;
- $IdGroup(G) = [256, 137]$, *zpyna* $G \cong (C_4 \times C_2).((C_4 \times C_2) \rtimes C_4) = (C_4 \times C_2).(C_8 \times C_4)$ *ma* $|U(G)| = 128$;
- $IdGroup(G) = [256, 139]$, *zpyna* $G \cong (C_4 \rtimes C_{16}) \rtimes C_4$ *ma* $|U(G)| = 128$;
- $IdGroup(G) = [256, 140]$, *zpyna* $G \cong (C_8 \times C_2) \rtimes C_{16}$ *ma* $|U(G)| = 128$;

- $IdGroup(G) = [256, 151]$, $zpyna\ G \cong (C_4 \times C_2).((C_4 \times C_2) \rtimes C_4) = (C_4 \times C_2).(C_8 \times C_4)\ ma\ |U(G)| = 128$;
- $IdGroup(G) = [256, 155]$, $zpyna\ G \cong (C_8 \rtimes C_2) \rtimes C_{16}\ ma\ |U(G)| = 128$;
- $IdGroup(G) = [256, 159]$, $zpyna\ G \cong (C_8 \rtimes C_8) \rtimes C_4\ ma\ |U(G)| = 64$;
- $IdGroup(G) = [256, 160]$, $zpyna\ G \cong (C_4.D_8 = C_4.(C_4 \times C_2)) \rtimes C_8\ ma\ |U(G)| = 64$;
- $IdGroup(G) = [256, 161]$, $zpyna\ G \cong (C_4.D_8 = C_4.(C_4 \times C_2)) \rtimes C_8\ ma\ |U(G)| = 64$;
- $IdGroup(G) = [256, 162]$, $zpyna\ G \cong (C_8 \rtimes C_8) \rtimes C_4\ ma\ |U(G)| = 64$;
- $IdGroup(G) = [256, 163]$, $zpyna\ G \cong (C_8 \rtimes C_8) \rtimes C_4\ ma\ |U(G)| = 64$;
- $IdGroup(G) = [256, 164]$, $zpyna\ G \cong (C_4.D_8 = C_4.(C_4 \times C_2)) \rtimes C_8\ ma\ |U(G)| = 64$;
- $IdGroup(G) = [256, 165]$, $zpyna\ G \cong (C_4.D_8 = C_4.(C_4 \times C_2)) \rtimes C_8\ ma\ |U(G)| = 64$;
- $IdGroup(G) = [256, 166]$, $zpyna\ G \cong (C_8 \rtimes C_8) \rtimes C_4\ ma\ |U(G)| = 64$;
- $IdGroup(G) = [256, 167]$, $zpyna\ G \cong (C_8.D_8 = C_4.(C_8 \times C_2)) \rtimes C_4\ ma\ |U(G)| = 64$;
- $IdGroup(G) = [256, 168]$, $zpyna\ G \cong (C_8.D_8 = C_4.(C_8 \times C_2)) \rtimes C_4\ ma\ |U(G)| = 64$;
- $IdGroup(G) = [256, 169]$, $zpyna\ G \cong (C_8.D_8 = C_4.(C_8 \times C_2)) \rtimes C_4\ ma\ |U(G)| = 64$;
- $IdGroup(G) = [256, 170]$, $zpyna\ G \cong (C_8.D_8 = C_4.(C_8 \times C_2)) \rtimes C_4\ ma\ |U(G)| = 64$;

- $IdGroup(G) = [256, 171]$, *эпына* $G \cong ((C_{16} \times C_2) \rtimes C_2) \rtimes C_4$ *ма* $|U(G)| =$;
- $IdGroup(G) = [256, 172]$, *эпына* $G \cong ((C_{16} \times C_2) \rtimes C_2) \rtimes C_4$ *ма* $|U(G)| = 128$;
- $IdGroup(G) = [256, 173]$, *эпына* $G \cong ((C_{16} \times C_2) \rtimes C_2) \rtimes C_4$ *ма* $|U(G)| = 128$;
- $IdGroup(G) = [256, 174]$, *эпына* $G \cong ((C_{16} \times C_2) \rtimes C_2) \rtimes C_4$ *ма* $|U(G)| = 128$;
- $IdGroup(G) = [256, 179]$, *эпына* $G \cong ((C_{16} \rtimes C_2) \rtimes C_2) \rtimes C_4$ *ма* $|U(G)| = 128$;
- $IdGroup(G) = [256, 180]$, *эпына* $G \cong ((C_{16} \rtimes C_2) \rtimes C_2) \rtimes C_4$ *ма* $|U(G)| = 128$;
- $IdGroup(G) = [256, 181]$, *эпына* $G \cong ((C_{16} \rtimes C_2) \rtimes C_2) \rtimes C_4$ *ма* $|U(G)| = 128$;
- $IdGroup(G) = [256, 182]$, *эпына* $G \cong (C_8 \times C_2) \rtimes C_{16}$ *ма* $|U(G)| = 128$;
- $IdGroup(G) = [256, 183]$, *эпына* $G \cong (C_4 \times C_2).((C_4 \times C_2) \rtimes C_4) = (C_4 \times C_2).(C_8 \times C_4)$ *ма* $|U(G)| = 128$;
- $IdGroup(G) = [256, 184]$, *эпына* $G \cong (C_4 \times C_2).((C_4 \times C_2) \rtimes C_4) = (C_2 \times C_2 \times C_2).(C_8 \times C_4)$ *ма* $|U(G)| = 128$;
- $IdGroup(G) = [256, 185]$, *эпына* $G \cong (C_4 \times C_4).((C_4 \times C_2) \rtimes C_2) = (C_4 \times C_2).(C_8 \times C_4)$ *ма* $|U(G)| = 128$;
- $IdGroup(G) = [256, 186]$, *эпына* $G \cong ((C_{16} \times C_2) \rtimes C_2) \rtimes C_4$ *ма* $|U(G)| = 128$;

- $IdGroup(G) = [256, 187]$, *zpyyna* $G \cong (C_8 \rtimes C_2) \rtimes C_{16}$ *ma* $|U(G)| = 128$;
- $IdGroup(G) = [256, 197]$, *zpyyna* $G \cong ((C_4 \rtimes C_4) \rtimes C_4) \rtimes C_4$ *ma* $|U(G)| = 128$;
- $IdGroup(G) = [256, 218]$, *zpyyna* $G \cong ((C_4 \rtimes C_4) \rtimes C_4) \rtimes C_4$ *ma* $|U(G)| = 64$;
- $IdGroup(G) = [256, 221]$, *zpyyna* $G \cong (C_2 \times (C_8 \rtimes C_4)) \rtimes C_4$ *ma* $|U(G)| = 64$;
- $IdGroup(G) = [256, 242]$, *zpyyna* $G \cong (C_2 \times (C_8 \rtimes C_4)) \rtimes C_4$ *ma* $|U(G)| = 64$;
- $IdGroup(G) = [256, 246]$, *zpyyna* $G \cong (C_2 \times (C_8 \rtimes C_4)) \rtimes C_4$ *ma* $|U(G)| = 64$;
- $IdGroup(G) = [256, 250]$, *zpyyna* $G \cong (C_2 \times (C_8 \rtimes C_4)) \rtimes C_4$ *ma* $|U(G)| = 64$;
- $IdGroup(G) = [256, 256]$, *zpyyna* $G \cong (C_8.D_8 = C_4.(C_8 \times C_2)) \rtimes C_4$ *ma* $|U(G)| = 128$;
- $IdGroup(G) = [256, 257]$, *zpyyna* $G \cong (C_8.D_8 = C_4.(C_8 \times C_2)) \rtimes C_4$ *ma* $|U(G)| = 128$;
- $IdGroup(G) = [256, 328]$, *zpyyna* $G \cong (((C_{16} \rtimes C_2) \rtimes C_2) \rtimes C_2) \rtimes C_2$ *ma* $|U(G)| = 128$;
- $IdGroup(G) = [256, 329]$, *zpyyna* $G \cong C_2.((((C_8 \times C_2) \rtimes C_2) \rtimes C_2) \rtimes C_2) = (C_2 \times C_2 \times C_2 \times C_2).(C_8 \times C_2)$ *ma* $|U(G)| = 128$;
- $IdGroup(G) = [256, 330]$, $G \cong (((C_{16} \rtimes C_2) \rtimes C_2) \rtimes C_2) \rtimes C_2$ *ma* $|U(G)| = 128$;

- $IdGroup(G) = [256, 331]$, $G \cong C_2.((((C_8 \times C_2) \rtimes C_2) \rtimes C_2) \rtimes C_2) = (C_4 \times C_2 \times C_2).(C_8 \times C_2) \text{ ма } |U(G)| = 128$;
- $IdGroup(G) = [256, 344]$, $G \cong (C_4.((C_2 \times C_2 \times C_2) \rtimes C_4) = (C_4 \times C_2).(C_8 \times C_2)) \rtimes C_2 \text{ ма } |U(G)| = 128$;
- $IdGroup(G) = [256, 345]$, $G \cong (C_4.((C_2 \times C_2 \times C_2) \rtimes C_4) = (C_4 \times C_2).(C_8 \times C_2)) \rtimes C_2 \text{ ма } |U(G)| = 128$;
- $IdGroup(G) = [256, 348]$, $G \cong C_4.((C_2 \times Q_8) \rtimes C_4) = (C_4 \times C_4).(C_8 \times C_2) \text{ ма } |U(G)| = 128$;
- $IdGroup(G) = [256, 349]$, $G \cong C_4.((C_2 \times Q_8) \rtimes C_4) = (C_4 \times C_4).(C_8 \times C_2) \text{ ма } |U(G)| = 128$;
- $IdGroup(G) = [256, 356]$, $G \cong C_4.((C_4 \times C_4) \rtimes C_4) = (C_4 \times C_4).(C_8 \times C_2) \text{ ма } |U(G)| = 128$;
- $IdGroup(G) = [256, 357]$, $G \cong C_4.((C_4 \times C_4) \rtimes C_4) = (C_4 \times C_4).(C_8 \times C_2) \text{ ма } |U(G)| = 128$;
- $IdGroup(G) = [256, 361]$, $G \cong C_4.(((C_2 \times C_2 \times C_2) \rtimes C_4) \rtimes C_2) = (C_4 \times C_4).(C_8 \times C_2) \text{ ма } |U(G)| = 128$;
- $IdGroup(G) = [256, 362]$, $G \cong C_4.(((C_2 \times C_2 \times C_2) \rtimes C_4) \rtimes C_2) = (C_4 \times C_4).(C_8 \times C_2) \text{ ма } |U(G)| = 128$;
- $IdGroup(G) = [256, 384]$, $G \cong (((C_{16} \rtimes C_2) \rtimes C_2) \rtimes C_2) \rtimes C_2 \text{ ма } |U(G)| = 64$.

Далі, наведено список ендоциклічних 2-породжених груп порядку 256 та експоненти 32.

Лема 7.18. *Наступні 2-породжені групи G порядку 256 та експоненти 32 є ендоциклічними, та вказано порядок $U(G)$ для кожної групи G :*

- $IdGroup(G) = [256, 316]$, *zpyna* $G \cong C_{32} \times C_8$ *ma* $|U(G)| = 128$;
- $IdGroup(G) = [256, 317]$, *zpyna* $G \cong C_{32} \rtimes C_8$ *ma* $|U(G)| = 128$;
- $IdGroup(G) = [256, 318]$, *zpyna* $G \cong C_{32} \rtimes C_8$ *ma* $|U(G)| = 128$;
- $IdGroup(G) = [256, 319]$, *zpyna* $G \cong C_8 \rtimes C_{32}$ *ma* $|U(G)| = 128$;
- $IdGroup(G) = [256, 320]$, *zpyna* $G \cong (C_8 \times C_2).(C_4 \times C_4) = C_4.(C_{16} \times C_4)$ *ma* $|U(G)| = 128$;
- $IdGroup(G) = [256, 322]$, *zpyna* $G \cong C_{32} \rtimes C_8$ *ma* $|U(G)| = 128$;
- $IdGroup(G) = [256, 323]$, *zpyna* $G \cong ((C_{32} \times C_2) \rtimes C_2) \rtimes C_2$ *ma* $|U(G)| = 128$;
- $IdGroup(G) = [256, 324]$, *zpyna* $G \cong ((C_{32} \times C_2) \rtimes C_2) \rtimes C_2$ *ma* $|U(G)| = 128$;
- $IdGroup(G) = [256, 325]$, *zpyna* $G \cong ((C_{32} \rtimes C_2) \rtimes C_2) \rtimes C_2$ *ma* $|U(G)| = 128$;
- $IdGroup(G) = [256, 350]$, *zpyna* $G \cong ((C_{32} \rtimes C_2) \rtimes C_2) \rtimes C_2$ *ma* $|U(G)| = 128$;
- $IdGroup(G) = [256, 351]$, *zpyna* $G \cong (C_4 \times C_2) \rtimes C_{32}$ *ma* $|U(G)| = 128$;
- $IdGroup(G) = [256, 352]$, *zpyna* $G \cong (C_8 \times C_2).((C_4 \times C_2) \rtimes C_2) = (C_4 \times C_2).(C_{16} \times C_2)$ *ma* $|U(G)| = 128$;
- $IdGroup(G) = [256, 353]$, *zpyna* $G \cong C_8.((C_2 \times C_2 \times C_2) \rtimes C_4) = (C_4 \times C_2).(C_{16} \times C_2)$ *ma* $|U(G)| = 128$;
- $IdGroup(G) = [256, 367]$, *zpyna* $G \cong C_8.((C_2 \times C_2 \times C_2) \rtimes C_4) = (C_2 \times C_2 \times C_2).(C_{16} \times C_2)$ *ma* $|U(G)| = 128$;

- $IdGroup(G) = [256, 371]$, $zpyna\ G \cong (C_{32} \times C_4) \rtimes C_2$ $ma\ |U(G)| = 64$;
- $IdGroup(G) = [256, 373]$, $zpyna\ G \cong (C_{32} \times C_4) \rtimes C_2$ $ma\ |U(G)| = 64$;
- $IdGroup(G) = [256, 380]$, $zpyna\ G \cong (C_{32} \rtimes C_4) \rtimes C_2$ $ma\ |U(G)| = 128$;
- $IdGroup(G) = [256, 406]$, $zpyna\ G \cong Q_8 \rtimes C_{32}$ $ma\ |U(G)| = 64$;
- $IdGroup(G) = [256, 410]$, $zpyna\ G \cong ((C_{32} \times C_2) \rtimes C_2) \rtimes C_2$ $ma\ |U(G)| = 64$;
- $IdGroup(G) = [256, 443]$, $zpyna\ G \cong ((C_{32} \rtimes C_2) \rtimes C_2) \rtimes C_2$ $ma\ |U(G)| = 128$;
- $IdGroup(G) = [256, 444]$, $zpyna\ G \cong C_8 \rtimes C_{32}$ $ma\ |U(G)| = 128$;
- $IdGroup(G) = [256, 446]$, $zpyna\ G \cong C_8.(C_8 \rtimes C_4) = C_8.(C_{16} \times C_2)$ $ma\ |U(G)| = 128$;
- $IdGroup(G) = [256, 447]$, $zpyna\ G \cong C_8 \rtimes C_{32}$ $ma\ |U(G)| = 128$;
- $IdGroup(G) = [256, 453]$, $zpyna\ G \cong C_{16}.D_{16} = C_8.(C_{16} \times C_2)$ $ma\ |U(G)| = 128$;
- $IdGroup(G) = [256, 454]$, $zpyna\ G \cong (C_{32} \times C_2) \rtimes C_4$ $ma\ |U(G)| = 128$;
- $IdGroup(G) = [256, 455]$, $zpyna\ G \cong (C_{32} \rtimes C_2) \rtimes C_4$ $ma\ |U(G)| = 128$;
- $IdGroup(G) = [256, 456]$, $zpyna\ G \cong (C_{32} \rtimes C_2) \rtimes C_4$ $ma\ |U(G)| = 128$;
- $IdGroup(G) = [256, 459]$, $zpyna\ G \cong (C_{16} \rtimes C_4) \rtimes C_4$ $ma\ |U(G)| = 64$;
- $IdGroup(G) = [256, 463]$, $zpyna\ G \cong (C_{16} \rtimes C_4) \rtimes C_4$ $ma\ |U(G)| = 64$;

- $IdGroup(G) = [256, 465]$, група $G \cong (C_{16} \rtimes C_4) \rtimes C_4$ та $|U(G)| = 64$.

Наведено список ендоциклічних 2-породжених груп порядку 256 та експоненти 64.

Лема 7.19. *Наступні 2-породжені групи G порядку 256 та експоненти 64 є ендоциклічними, та вказано порядок $U(G)$ для кожної групи G :*

- $IdGroup(G) = [256, 497]$, група $G \cong C_{64} \times C_4$ та $|U(G)| = 128$;
- $IdGroup(G) = [256, 498]$, група $G \cong C_{64} \rtimes C_4$ та $|U(G)| = 128$;
- $IdGroup(G) = [256, 499]$, група $G \cong C_{64} \rtimes C_4$ та $|U(G)| = 64$;
- $IdGroup(G) = [256, 500]$, група $G \cong (C_{64} \times C_2) \rtimes C_2$ та $|U(G)| = 64$;
- $IdGroup(G) = [256, 501]$, група $G \cong (C_{64} \rtimes C_2) \rtimes C_2$ та $|U(G)| = 64$;
- $IdGroup(G) = [256, 525]$, група $G \cong (C_{64} \times C_2) \rtimes C_2$ та $|U(G)| = 64$;
- $IdGroup(G) = [256, 528]$, група $G \cong (C_{64} \rtimes C_2) \rtimes C_2$ та $|U(G)| = 64$;
- $IdGroup(G) = [256, 531]$, група $G \cong C_4 \rtimes C_{64}$ та $|U(G)| = 64$;
- $IdGroup(G) = [256, 532]$, група $G \cong C_{32}.D_8 = C_4.(C_{32} \times C_2)$ та $|U(G)| = 64$.

Наведено список ендоциклічних 2-породжених груп порядку 256 та експоненти 128.

Лема 7.20. *Наступні 2-породжені групи G порядку 256 та експоненти 128 є ендоциклічними, та вказано порядок $U(G)$ для кожної групи G :*

- $IdGroup(G) = [256, 537]$, група $G \cong C_{128} \times C_2$ та $|U(G)| = 128$;
- $IdGroup(G) = [256, 538]$, група $G \cong C_{128} \rtimes C_2$ та $|U(G)| = 128$;
- $IdGroup(G) = [256, 539]$, група $G \cong D_{256}$ та $|U(G)| = 64$.

Висновки до розділу 7

У даному розділі:

- класифіковано локальні майже-кільця на 2-породжених групах порядків 64 та 243;
- наведено класифікацію локальних майже-кілець порядків 81 та 1331;
- вивчено локальні майже-кільця та ендоеиклічні 2-породжені групи порядків 64 та 256.

Основні результати даного розділу опубліковано у працях [2, 4, 15] зі списку публікацій і, відповідно, [6], [87], [96] зі списку використаних джерел, а також опубліковано у тезах конференцій [24, 25, 26, 28, 29, 32, 35] і, відповідно, [81], [82], [80] [14], [77], [95], [93].

Основні результати та висновки

Основні результати дисертації можна сформулювати таким чином:

- Встановлений зв'язок між нільпотентною мультиплікативною групою та адитивною групою в локальному майже-кілці.
- Класифіковано локальні майже-кілця, які не є полями та мультиплікативна група яких є групою Шмідта.
- Знайдені адитивні групи локальних майже-кілець порядку 32 та 128 з мультиплікативними групами Міллера–Морено.
- Вивчені скінченні p -групи з циклічною підгрупою індексу p як адитивні групи локальних майже-кілець.
- Отримано локальні майже-кілця з бібліотеки пакету SONATA системи комп'ютерної алгебри GAP.
- Проаналізовано скінченні неабелеві 2-породженні p -групи з циклічним комутантом.
- Показано, що не існує майже-кілець з одиницею, адитивна група якого ізоморфна групі $G(p^m, p^n)$ з $p > 2$ і $2 \leq m \leq n$.
- Вивчено скінченні локальні майже-кілця з розщепленою метациклічною адитивною групою.
- Отримано необхідні і достатні умови існування локальних майже-кілець на групах типу (B.1). Доведено, що індекс підгрупи всіх необоротних елементів таких майже-кілець в адитивній групі дорівнює p . А також, показано, що кожна група типу (B.1) є адитивною групою майже-кілця з одиницею.

- Введено та досліджено напівдистрибутивні майже-кільця з одиницею.
- Вивчено напівгрупу необоротних елементів локальних майже-кільць, адитивна група якого ізоморфна абелевій групі типу $(2^m, 2^n)$ з $m \geq n > 1$.
- Використовуючи пакет YangBaxter, надано класифікації брейсів (до порядку 32) та косих брейсів (до порядку 16) відповідно до адитивних або мультиплікативних груп, які є p -групами Міллера–Морено.
- Наведено деяку інформацію щодо майже-кільцевих брейсів, що стосуються, пакету LocalNR.
- Отримано алгоритм побудови скінченних локальних майже-кільць.
- Наведено функції для локальних майже-кільць з пакету LocalNR, а саме:
 - TheAdditiveGroupsOfLibraryOfLNRSOfOrder,
 - TheLibraryOfLNRSOnGroup,
 - LocalNearRing,
 - AllLocalNearRings,
 - IsAdditiveGroupOfLibraryOfLNRS,
 - InfoLocalNearRing.
- Наведено функції для груп з пакету LocalNR, а саме:
 - IsMinimalNonAbelianGroup,
 - IsMetacyclicPGroup,
 - EndoOrbitsOfGroup,
 - IsEndoCyclicGroup.

- Класифіковано локальні майже-кільця на 2-породжених групах порядків 64 та 243.
- Наведено класифікацію локальних майже-кілець порядків 81 та 1331.
- Вивчено локальні майже-кільця та ендоеиклічні 2-породжені групи порядків 64 та 256.

Список використаних джерел

1. Раєвська І. Ю., Раєвська М. Ю. Майже-поля з неабелево спадковими мультиплікативними групами, *Математичні Студії*, **34** (2010), № 1, 38–43.
2. Раєвська І. Ю., Раєвська М. Ю. Локальні майже-кільця з обмеженнями на мультиплікативні групи та підгрупи необоротних елементів, *Науковий часопис НПУ імені М. П. Драгоманова. Серія 1. Фізико-математичні науки*. — Київ: НПУ імені М. П. Драгоманова, № 14 (2013), 134–145.
3. Раєвська І. Ю., Раєвська М. Ю. Локальні майже-кільця на скінченних неабелевих p -групах. Тези доповідей міжнародної конференції “Сучасні проблеми механіки та математики” присвяченої 90-річчю від дня народження академіка НАН України Ярослава Степановича Підстригача та 40-річчю створеного ним Інституту прикладних проблем механіки і математики НАН України, 22–25 травня 2018 р., Інститут прикладних проблем механіки і математики ім. Я. С. Підстригача НАН України, Львів, Т. 3, С. 230,
http://www.iapmm.lviv.ua/mpmm2018/Volume_3.pdf
4. Раєвська І. Ю., Раєвська М. Ю. Скінченні локальні майже-кільця, *Могілянський математичний журнал*, **1** (2018), 38–48.
5. Раєвська І. Ю., Раєвська М. Ю. Локальні майже-кільця на елементарних абелевих групах порядку p^3 , *Науковий вісник Ужгородського університету. Серія “Математика і інформатика”*, **38**(1) (2021), 85–93.

6. Раєвська І., Раєвська М. Про ендоциклічні 2-породжені групи порядку 256 та експоненти 16. *Буковинський матем. журнал*, 2025, 13 (2), 161–169.
7. Раєвська І. Ю., Раєвська М. Ю., Сисак Я. П. Локальні майже-кільця на неметациклічних групах Міллера–Морено, *Вісник Київського університету. Серія: фіз.-мат. науки*, **3** (2012), 39–46.
8. Раєвська М. Ю. Локальні майже-кільця з мультиплікативною групою Міллера–Морено, *Вісн. Київ. Ун-ту. Математика, Механіка*, **25** (2011), 45–48.
9. Раєвська М. Ю., Сисак Я. П. Про локальні майже-кільця з мультиплікативною групою Міллера–Морено, *Укр. мат. журн.*, **64** (2012), по. 6, 811–818.
10. Раєвська М. Мультиплікативні групи скінченних локальних майже-кілець, канд. дис... фіз.-мат. наук: 01.01.06; Інститут математики НАН України. — К., 2012. — 116 с.
11. Раєвська М. Про локальні майже-кільця з нільпотентною мультиплікативною групою. *Науковий вісник Ужгородського університету. Серія «Математика і інформатика»*, 2025, **46** (1), 89–92, [https://doi.org/10.24144/2616-7700.2025.46\(1\).89-92](https://doi.org/10.24144/2616-7700.2025.46(1).89-92)
12. Раєвська М. Про локальні майже-кільця з нільпотентною мультиплікативною групою. The conference of young scientists “Pidstryhach Readings — 2025”, Lviv, Ukraine, May 27–29, 2025, http://iapmm.lviv.ua/chyt2025/abstracts/Raievska_Iryna.pdf
13. Холл М. Теорія груп, М.: Видавництво іноземної літератури, 1962.
14. Abramov A. V., Raievska I. Yu., Raievska M. Yu., Sysak Ya. P., Yurashev V. G. Local nearrings of order 1331. Abstracts of the

conference dedicated to the 60th anniversary of the algebra department of Kyiv University. Kyiv, Ukraine, July 14–17, 2020, P. 11;

[https://drive.google.com/file/d/](https://drive.google.com/file/d/1gyNWN20TC6V09mP3uRXw7uG9bg-3S_E7/view)

[1gyNWN20TC6V09mP3uRXw7uG9bg-3S_E7/view](https://drive.google.com/file/d/1gyNWN20TC6V09mP3uRXw7uG9bg-3S_E7/view)

15. Abramov A. V., Raievska I. Yu., Raievska M. Yu., Sysak Ya. P., Yurashev V. G. Miller-Moreno groups as multiplicative groups of local nearrings of order 64. 13th International Algebraic Conference in Ukraine. Kyiv, Ukraine, July 6–9, 2021 (in the form of webinars)
[https://drive.google.com/file/d/](https://drive.google.com/file/d/1wdZLWtj9jeFLH9BjSb7ZX5RFnTfTpstE/view)
[1wdZLWtj9jeFLH9BjSb7ZX5RFnTfTpstE/view](https://drive.google.com/file/d/1wdZLWtj9jeFLH9BjSb7ZX5RFnTfTpstE/view)
16. Aichinger E., Binder F., Ecker Ju., Mayr P. and Noebauer C. *SONATA – System of Nearrings and their Applications*, Version 2.9.6, Johannes Kepler Universitaet Linz, 2022,
<https://gap-packages.github.io/sonata/>
17. Al-Hasanat B. N., Almazaydeh A. On classification of groups of order p^4 , where p is an odd prime, *International Journal of Mathematics and Computer Science*, **17** (2022), no. 4, 1569–1593.
18. Amberg B., Hubert P., Sysak Ya. Local near-rings with dihedral multiplicative group, *J. Algebra*, **273** (2004), 700–717.
19. Beidleman J. C. Distributively generated near-rings with descending chain condition, *Math. Zeitschr*, **91** (1966), 65–69.
20. On the theory of radicals of distributively generated near-rings. I. The Primitive-Radical, *Math. Ann*, **173** (1967), 89.
21. Beidleman J. C. On the Theory of Radicals of Distributively Generated Near-Rings. II. The Nil-Radical, *Math. Annalen*, **173** (1967), 200–218.

22. Berman G., Silverman R. J. Simplicity of near-rings of transformations, *Proc. Amer. Math. Soc.*, **10** (1959), 456–459.
23. Berman G., Silverman R. J. Near-Rings, *The American Mathematical Monthly*, **66** (1959), no. 1, 23–34.
24. Betsch G. Ein Radikal für Fastringe, *Math. Z.*, **78** (1962), 86–90.
25. Bidwell J. N. S., Curran M. J. The automorphism group of a split metacyclic p -group, *Arch. Math.*, **87** (2006), 488–497.
26. Blackett D. W. Simple and semi-simple near-rings, *Proc. American Math. Soc.*, **4** (1953), 772–785.
27. Burnside W. Theory of groups of finite order, Cambridge: At the University press, 1897, 430 p.
28. Clay J. R. Research in near-ring theory using a digital computer, *BIT*, **10** (1970), 249–265.
29. Clay J. R. Nearrings. Geneses and Applications, New York: Clarendon Press, Oxford University Press, 1992.
30. Clay J. R., Doi D., Near-rings with identity on alternating groups, *Math. Scand.*, **23** (1968), 54–56.
31. Clay J. R., Malone Jr. The near-rings with identities on certain finite groups, *Math. Scand.*, **19** (1966), 146–150.
32. Clay J. R., Maxson C. J. The near-rings with identities on generalized quaternion groups, *Ist. Lombardo Accad. Sci. Lett. Rend. A*, **104** (1970), 525–530.
33. Curran M. J. The automorphism group of a split metacyclic 2-group, *Arch. Math.*, **89** (2007), 10–23.

34. Dixon L. Definitions of a group and a field by independent postulates, *Trans. Amer. Math. Soc.*, **6** (1905), 198–204.
35. Feigelstock S. Additive groups of local near-rings, *Comm. Algebra*, **34** (2006), 743–747.
36. Feit W., Thompson J. Solvability of groups of odd order, *Pacific J. Math.*, **18** (1963), 771–1029.
37. Ferrero C. C., Ferrero G., Nearrings. Some developments linked to semigroups and groups, Kluwer Academic Publishers, Dordrecht, 2002, 609 p.
38. Frohlich A. Distributively generated near-rings (I. Ideal theory), *Proc. London Math. Soc.*, **8** (1958), no. 3, 76–94.
39. Frohlich A. Distributively generated near-rings (II. Representation theory), *Proc. London Math. Soc.*, **8** (1958), no. 3, 95–108.
40. The GAP Group, Aachen, St Andrews. *GAP — Groups, Algorithms and Programming*, Version 4.13.0, 2024, <https://www.gap-system.org/>
41. Gorenstein D. Finite groups. New York: Harper & Row, 1968, 527 p.
42. Gorodnik A. Local near-rings with commutative groups of units, *Houston J. Math.*, **25** (1999), 223–234.
43. Holcombe W. M. L. Categorical representations of endomorphism near-rings, *J. Lond. Math. Soc. (2)*, **16** (1977), no. 1, 21–37.
44. Hopkins C. Rings with minimum condition for left ideals, *Annals of Math.*, **40** (1939), 712–730.
45. Hubert P. Nearrings and a construction of triply factorized groups, Doctoral dissertation, Mainz, 2005, 146 p.

46. Huppert B. Endliche Gruppen I. Berlin, Heidelberg, New York: Springer-Verlag, 1967.
47. King B. W. Presentations of metacyclic groups, *Bul. Austral. Math. Soc.*, **8** (1973), 103–131.
48. Krimmel J. E. A condition on near-rings with identity, *Monatsh. Math.*, **77** (1973), 52–54.
49. Kurosh A. G. Course of higher algebra. Moscow: Nauka, 1967 [in Russian].
50. Johnson M. J. Near-rings with identities on dihedral groups, *Proc. Edinburgh Math. Soc. (2)*, **18** (1972/73), 219–228.
51. Laxton R. R., Lockhart R. The near-rings hosted by a class of groups, *Proc. Edinb. Math. Soc.*, **23** 1980, 69–86.
52. Ligh S. A generalization of a theorem of Zassenhaus, *Canadian Mathematical Bulletin*, **12** (October 1969), no. 5, 677–678,
<https://doi.org/10.4153/CMB-1969-089-2>
53. Ligh S. Near rings with identities on certain groups, *Monatsh. Math.*, **75** (1971), 38–43.
54. Ligh S. D. g. near rings on certain groups, *Monatsh. Math.*, **75** (1971), 244–249.
55. Ligh S. Finite hereditary near-field groups, *Mh. Math.*, **86** (1978), no. 1, 7–11.
56. Lockhart R. The theory of near-rings, *Lecture Notes in Math.*, **2295**, Springer, Cham, 2021, 537 p.

57. Mahmood S. J., Mansouri M. F. Tensor product of near-ring modules, *Math. Appl.*, Kluwer Academic Publishers, Dordrecht, **426** (1997), 335–342.
58. Malone J. J., Lyons C. G. Finite dihedral groups and d.g. near rings. I, *Compositio Math.* **24** (1972), 305–312.
59. Malone J. J., Lyons C. G. Finite dihedral groups and d.g. near rings. II, *Compositio Math.* **26** (1973), 249–259.
60. Malone J. J. DG near rings on the infinite dihedral group, *Proc. Roy. Soc. Edinburgh Sect. A*, **78** (1977/78), no. 1–2, 67–70.
61. Maxson C. J. On local near-rings, *Math. Z.*, **106** (1968), 197–205.
62. Maxson C. J. Local near-rings of cardinality p^2 , *Canad. Math. Bull.*, **11** (1968), no. 4, 555–561.
63. Maxson C. J. On the construction of finite local near-rings (I): on non-cyclic abelian p -groups, *Quart. J. Math. Oxford (2)*, **21** (1970), 449–457.
64. Maxson C. J. On the construction of finite local near-rings (II): on non-abelian p -groups, *Quart. J. Math. Oxford (2)*, **22** (1971), 65–72.
65. Meldrum J. D. P. Near-rings and their links with groups, London: Pitman Publishing Limited, 1985 — 273 p.
66. Menegazzo F. Automorphisms of p -groups with cyclic commutator subgroup, *Rend. Sem. Mat. Univ. Padova*, **90** (1993), 81–101.
67. Miech R. J. On p -groups with a cyclic commutator, *J. Austral. Math. Soc.*, **20** (1975), 178–198.
68. Neumann B. H. On the commutativity of addition, *J. London Math. Soc.*, **15** (1940), 203–208.

69. Neumann H. On varieties of groups and their associated near-rings, *Math. Z.*, **65** (1956), 36–69.
70. Pilz G. Near-rings. The theory and its applications, North Holland, Amsterdam, 1977.
71. Raievska I. Yu., Raievska M. Yu. Finite nearrings with identity on Miller-Moreno groups. *Mat. Stud.*, 2014, **42** (1), 15–20,
http://matstud.org.ua/texts/2014/42_1/15-20.pdf
72. Raievska I., Raievska M. On finite one-sided distributive structures. Abstracts of Humboldt Kolleg “Education and science and their role in social and industrial progress of society”. Kyiv, Ukraine, June 12–15, 2014, P. 45.
73. Raievska I., Raievska M. Finite local nearrings on split metacyclic additive group. Тези доповідей Міжнародної конференції молодих математиків, 3–6 червня 2015 р., Ін-т математики НАН України, Київ, Україна, С. 42.
74. Raievska I., Raievska M. Local nearrings on finite 2-generated non-abelian non-metacyclic p -groups. Abstracts of Scientific Conference dedicated to 100th anniversary of K. M. Fishman and M. K. Fage. Chernivtsi, Ukraine, July 1–4, 2015, P. 103.
75. Raievska I. Yu., Raievska M. Yu. Finite one-sided distributive structures. Тези доповідей XI Літньої школи “Алгебра, Топологія, Аналіз”, 1–14 серпня 2016 р., Одеса, Україна,
http://www.imath.kiev.ua/~topology/ata11/ata11_theses.pdf
76. Raievska I. Yu., Raievska M. Yu. Some special p -groups and nearrings with identity. Тези доповідей до XII Міжнародної алгебраїчної

- конференції в Україні, присвяченій 215-й річниці з дня народження В. Буняковського, 02—06 липня 2019 р., Донецький національний університет імені Василя Стуса, Вінниця, Україна, С. 92–93,
<https://jiac.donnu.edu.ua/article/view/6991>
77. Raievska I., Raievska M., The additive groups of local nearrings of order 64. Тези доповідей конференції молодих учених “Підстригачівські читання — 2020”. Львів, Україна, 26–28 травня, 2020,
<http://iapmm.lviv.ua/chyt2020/abstracts/Raievska.pdf>
78. Raievska I. Yu., Raievska M. Yu. Local nearrings on finite non-abelian 2-generated p-groups. *Carpathian Math. Publ.*, **12** (1) (2020), 199–207,
 URL: <https://journals.pnu.edu.ua/index.php/cmp/article/view/3905/4478>
79. Raievska I. Yu., Raievska M. Yu. Local near-rings with a multiplicative Schmidt group. *Ukr. Math. J.*, **71** (2020), No. 10, 1643–1649, <https://doi.org/10.1007/s11253-020-01737-6>; перекладено з *Ukr. Mat. Zh.*, 2019, **71**, No. 10, 1435–1440. (in Ukrainian);
<http://umj.imath.kiev.ua/index.php/umj/article/view/1526/509>
80. Raievska I., Raievska M., Local nearrings of order 343. International Algebraic Conference “At the End of the Year 2021”, (2021, December 27–28, Kyiv, Ukraine) (in the form of webinars)
<https://www.imath.kiev.ua/~algebra/algebra2021/abstracts>
81. Raievska I., Raievska M. Finite local nearrings and their classification, International conference-workshop “GAP Days Summer 2022”, RWTH Aachen University, Aachen, Germany, October 17–21, 2022,
<https://www.gapdays.de/gapdays2022-summer/abstracts/raievska>

82. Raievska I., Raievska M., Local nearrings and their classification, International Conference “On the Trail of Women in Mathematics “Contemporary Women in Mathematics”, Gdansk, Poland, September 15–17, 2022,
https://otowim22.ptkwm.pl/Abstract_Book.pdf
83. Raievska I., Raievska M. Lower bounds for the number of local nearrings on groups of order p^3 , *Math. Commun.*, **29** (2024), 177–191.
84. Raievska I., Raievska M. Groups of order p^4 as additive groups of local nearrings. *Ukrainian Math. J.*, 2024, **76** (6), 1005–1024, translation of *Ukrain. Mat. Zh.*, 2024, **76** (6), 890–906. **76** (6), 890–906
85. Raievska I., Raievska M. Groups of nilpotency class 2 of order p^4 as additive groups of local nearrings. *Algebra Discrete Math.*, 2024, 38 (1), 93–114.
86. Raievska I., Raievska M. Groups of the nilpotency class 3 of order p^4 as additive groups of local nearrings *Carpathian Math. Publ.*, **17** (2025), no. 1, 292–301.
87. Raievska I., Raievska M. Local nearrings and endocyclic groups of small order. *Scientific Bulletin of Uzhhorod University. Series of Mathematics and Informatics*, 2025, **47** (2), 65–71,
[https://doi.org/10.24144/2616-7700.2025.47\(2\).65-71](https://doi.org/10.24144/2616-7700.2025.47(2).65-71)
88. Raievska I., Raievska M. Braces and skew-braces via gap: YangBaxter and LocalNR packages. *Journal of Mathematical Sciences*, 2025, **294**, 230–241,
<https://link.springer.com/article/10.1007/s10958-025-08097-1>
89. Raievska I., Raievska M. Local nearrings, their structure, and the GAP system. *Ukrainian Math. J.*, 2025, **76** (11), 1831–

- 1848, <https://doi.org/10.1007/s11253-025-02426-y>; translation of *Ukrain. Mat. Zh.*, 2024, **76** (11), 1629–1644.
90. Raievska I. Yu., Raievska M. Yu. Braces, skew-braces, local nearrings via GAP: the YangBaxter and LocalNR packages. Тези доповідей конференції молодих учених “Підстригачівські читання — 2024”. Львів, Україна, 27–29 травня, 2024,
<http://www.iapmm.lviv.ua/chyt2024/abstracts/Raievska.pdf>
 91. Raievska I., Raievska M. LocalNR package and its applications, GAP Days Spring 2024, University of Kaiserslautern-Landau, Kaiserslautern, March 11–15, 2024,
<https://www.gapdays.de/gapdays2024-spring/abstracts/raievska>
 92. Raievska I., Raievska M., Sysak Ya. Finite local nearrings with multiplicative Miller–Moreno group. Abstracts of 9-th International Algebraic Conference in Ukraine. Lviv, Ukraine, July 8–13, 2013, P. 154.
 93. Raievska I. Yu., Raievska M. Yu., Sysak Ya. P. Local nearrings of order 81. Abstracts of X International Algebraic Conference in Ukraine dedicated to the 70th anniversary of Yu. A. Drozd, Odessa, Ukraine, August 20–27, 2015, P. 94.
 94. Raievska I. Yu., Raievska M. Yu., Sysak Ya. P. Finite local nearrings with split metacyclic additive group. *Algebra and Discrete Mathematics*, (2016), **22** (1), 129–152,
<http://admjournal.luguniv.edu.ua/index.php/adm/article/view/293/pdf>
 95. Raievska I. Yu., Raievska M. Yu., Sysak Ya. P. Local nearrings of order 64. Abstracts of the International mathematical conference “Groups and

- Actions: Geometry and Dynamics, dedicated to the memory of professor Vitaly Sushchansky". Kyiv, Ukraine, December 19–22, 2016, P. 43.
96. Raievska I. Yu., Raievska M. Yu., Sysak Ya. P. Local nearrings of order 243. *Proceedings CMSM* 4, June 28 — July 2, 2017, Chisinau / ed.: Mitrofan Choban [et al.]. Chisinau: Institute of Mathematics and Computer Science, 2017 (CEP USM), 149–152.
 97. Raievska I., Raievska M., Sysak Ya. Semidistributive nearrings with identity. *Algebra Discrete Math.*, 36(2) (2023), 217–224,
<https://admjournal.luguniv.edu.ua/index.php/adm/article/view/2207/pdf>
 98. Raievska I., Raievska M., Sysak Ya. LocalNR, Package of local nearrings, Version 1.0.4 (2024) (GAP package),
<https://gap-packages.github.io/LocalNR/>
 99. Raievska I., Raievska M., Sysak Ya. DatabaseEndom64: (v1.0.1) [Data set] (2024). Zenodo,
<https://doi.org/10.5281/zenodo.10820320>
 100. Raievska I., Raievska M., Sysak Ya. DatabaseEndom243: (v1.0.1) [Data set] (2024). Zenodo,
<https://doi.org/10.5281/zenodo.10820318>
 101. Raievska I., Raievska M., Sysak Ya. LocalNR package and some of its applications. *Algebra Discrete Math.*, 2025, **40** (2), 215–225,
<https://doi.org/10.12958/adm2449>
 102. Raievska I. Yu., Sysak Ya. P. Finite local nearrings on metacyclic Miller-Moreno p -groups, *Algebra Discrete Math.*, **13** (2012), no. 1, 111–127.
 103. Raievska M. On multiplicative groups of finite local nearrings. Abstracts of AAA89: Workshop on General Algebra, Dresden, Germany, February

- 26 – March 1, 2015,
<http://at.yorku.ca/cgi-bin/abstract/cbkb-72>
104. Raievska M. Finite local nearrings on non-abelian p -groups with cyclic commutator subgroups. Abstracts of conference “Groups and their actions”. Bedlewo (near Poznan), Poland, June 22–26, 2015,
<http://mat.polsl.pl/groups/bedlewo-2015.pdf>
105. Raievska M. On semidistributive local nearrings. *Науковий вісник Ужгородського університету. Серія “Математика і інформатика”*, **43**(2) (2023), 67–71,
[https://doi.org/10.24144/2616-7700.2023.43\(2\).67-71](https://doi.org/10.24144/2616-7700.2023.43(2).67-71)
106. Raievska M. p -groups with cyclic subgroup of index p and local nearrings. *Прикл. проблеми мех. і мат.*, **22** 2024, 117–122.
107. Raievska M. p -Groups with cyclic subgroup of index p and local nearrings. 15th Ukraine Algebra Conference, Lviv, Ukraine, July 8–12, 2025. P. 87,
<https://xvuac.mmf.com.ua/index.php/abstracts>
108. Raievska M. Yu., Sysak Ya. P. On local nearrings with Miller-Moreno multiplicative group. *Ukr. Mat. Zh.*, **64** 2012, no. 6, 811–818 (in Ukrainian).
109. Redei L. Das “schiefe Produkt” in der Gruppentheorie mit Anwendung auf die endlichen nichtkommutativen Gruppen mit lauter kommutativen echten Untergruppen und die Ordnungszahlen, zu denen nur kommutative Gruppen gehören, *Comment. Math. Helv.*, **20** 1947, 225–264.
110. Rump W. Classification of cyclic braces, *J. Pure Appl. Algebra*, **209** 2007, no. 3, 671–685.

111. Rump W. Set-theoretic solutions to the Yang-Baxter equation, skew-braces, and related near-rings. *J. Algebra Appl.*, **18** 2019, no. 8, Article ID 1950145, 22 p.
112. Rump W. Classification of the affine structures of a generalized quaternion group of order, *J. Group Theory*, **23** 2020, no. 5, 847–869.
113. Shmidt O. Iu. Groups, all subgroups of which are special. *Math. col.*, **31** 1924, 366–372 [in Russian].
114. Sysak Ya. P. Products of groups and local nearrings, *Note di Mat.*, **28** (2008), no. 2, 179–213.
115. Sysak Ya., Raievska I., Raievska M. Construction of local nearrings using GAP. *Algebra Discrete Math.*, 2025, **40** (1), 133–144, <https://doi.org/10.12958/adm2427>
116. Sysak Ya. P., Di Termini S. Local nearrings with generalized quaternion multiplicative group, *Ricerche Mat.*, **56** (2007), 61–72.
117. Taussky-Todd O. Rings with non-commutative addition, *Bull. Calcutta Math. Soc.*, **28** (1936), 245–246.
118. Veblen O., Wedderburn J. H. Non-desarguesian and non-pascalian geometrie, *Trans. Amer. Math. Soc.*, **8** (1907), 379–388.
119. Vendramin L., Konovalov O. YangBaxter — Combinatorial Solutions for the Yang-Baxter equation, GAP package, Version 0.10.1, 2022, <https://gap-packages.github.io/YangBaxter/>
120. Wähling H. Theorie der Fastkörper, Essen: Thales Verlag, 1987.
121. Zassenhaus H. Über endliche Fastkörper, *Abh. Math. Sem., Univ. Hamburg*, **11** (1935/36), 187–220.

Додаток А

Список публікацій і апробація результатів

Цей додаток містить список публікацій здобувача по темі дисертації, а також відомості про апробацію результатів дисертаційної роботи.

Результати дисертації висвітлено у 14 наукових публікаціях. Основні результати опубліковано у наукових фахових виданнях України і наукових періодичних виданнях інших держав, пороіндексованих у міжнародних наукометричних базах Scopus або Web of Science [12, 2, 1, 5, 7, 9, 11, 16]. Результати дисертації додатково відображено у 21 тезах доповідей і матеріалах міжнародних наукових конференцій.

Наукові праці, у яких опубліковані наукові результати дисертації:

1. Sysak Ya., Raievska I., Raievska M. Construction of local nearrings using GAP. *Algebra Discrete Math.*, 2025, **40** (1), 133–144, <https://doi.org/10.12958/adm2427> (SJR — **Q3**).
2. Raievska I., Raievska M., Sysak Ya. LocalNR package and some of its applications. *Algebra Discrete Math.*, 2025, **40** (2), 215–225, <https://doi.org/10.12958/adm2449> (SJR — **Q3**)
3. Раєвська І., Раєвська М. Про ендоциклічні 2-породжені групи порядку 256 та експоненти 16. *Буковинський матем. журнал*, 2025, 13 (2), 161–169 (Категорія Б)

4. Raievska I., Raievska M. Local nearrings and endocyclic groups of small order. *Scientific Bulletin of Uzhhorod University. Series of Mathematics and Informatics*, 2025, **47** (2), 65–71,
[https://doi.org/10.24144/2616-7700.2025.47\(2\).65-71](https://doi.org/10.24144/2616-7700.2025.47(2).65-71) (Категорія Б)
5. Raievska I., Raievska M. Braces and skew-braces via gap: YangBaxter and LocalNR packages. *Journal of Mathematical Sciences*, 2025, **294**, 230–241,
<https://link.springer.com/article/10.1007/s10958-025-08097-1> (SJR — **Q3**)
6. Raievska M. p -groups with cyclic subgroup of index p and local nearrings. *Прикл. проблеми мех. і мат.*, 2024, **22**, 117–122 (Категорія Б)
7. Raievska I., Raievska M. Local nearrings, their structure, and the GAP system. *Ukrainian Math. J.*, 2025, **76** (11), 1831–1848, <https://doi.org/10.1007/s11253-025-02426-y>; translation of *Ukrain. Mat. Zh.*, 2024, **76** (11), 1629–1644 (SJR — **Q3**)
8. Раєвська М. Про локальні майже-кільця з нільпотентною мультиплікативною групою. *Науковий вісник Ужгородського університету. Серія «Математика і інформатика»*, 2025, **46** (1), 89–92,
[https://doi.org/10.24144/2616-7700.2025.46\(1\).89-92](https://doi.org/10.24144/2616-7700.2025.46(1).89-92) (Категорія Б)
9. Raievska I., Raievska M., Sysak Ya. Semidistributive nearrings with identity. *Algebra Discrete Math.*, 36(2) (2023), 217–224,
<https://admjournal.luguniv.edu.ua/index.php/adm/article/view/2207/pdf> (SJR — **Q3**)
10. Raievska M. On semidistributive local nearrings. *Науковий вісник*

Ужгородського університету. Серія “Математика і інформатика”, **43**(2) (2023), 67–71,

[https://doi.org/10.24144/2616-7700.2023.43\(2\).67-71](https://doi.org/10.24144/2616-7700.2023.43(2).67-71) (Категорія Б)

11. Raievska I. Yu., Raievska M. Yu. Local near-rings with a multiplicative Schmidt group. *Ukr. Math. J.*, **71** (2020), No. 10, P. 1643–1649, <https://doi.org/10.1007/s11253-020-01737-6>; перекладено з *Ukr. Mat. Zh.*, 2019, **71**, No. 10, 1435–1440. (in Ukrainian), <http://umj.imath.kiev.ua/index.php/umj/article/view/1526/509> (SJR — **Q3**)
12. Raievska I. Yu., Raievska M. Yu. Local nearrings on finite non-abelian 2-generated p-groups. *Carpathian Math. Publ.*, **12** (1) (2020), 199–207, URL: <https://journals.pnu.edu.ua/index.php/cmp/article/view/3905/4478> (SJR — **Q2**)
13. Raievska I. Yu., Raievska M. Yu. Finite nearrings with identity on Miller-Moreno groups. *Mat. Stud.*, 2014, **42** (1), 15–20, http://matstud.org.ua/texts/2014/42_1/15-20.pdf (Фахове видання)
14. Раєвська І. Ю., Раєвська М. Ю. Локальні майже-кільця з обмеженнями на мультиплікативні групи та підгрупи необоротних елементів. *Науковий часопис НПУ імені М. П. Драгоманова. Серія 1. Фізико-математичні науки*, Київ: НПУ імені М. П. Драгоманова, 2013, **14**, 134–145 (Фахове видання)
15. Raievska I. Yu., Raievska M. Yu., Sysak Ya. P. Local nearrings of order 243. *Proceedings CMSM 4*, June 28 — July 2, 2017, Chisinau / ed.: Mitrofan Choban [et al.]. Chisinau: Institute of Mathematics and Computer Science, 2017 (СЕР USM), 149–152.

16. Raievska I. Yu., Raievska M. Yu., Sysak Ya. P. Finite local nearrings with split metacyclic additive group. *Algebra and Discrete Mathematics*, (2016), **22** (1), 129–152,
<http://admjournal.luguniv.edu.ua/index.php/adm/article/view/293/pdf> (SJR — **Q4**)
17. Raievska I., Raievska M., Sysak Ya. DatabaseEndom64: (v1.0.1) [Data set] (2024). Zenodo,
<https://doi.org/10.5281/zenodo.10820320>
18. Raievska I., Raievska M., Sysak Ya. DatabaseEndom243: (v1.0.1) [Data set] (2024). Zenodo,
<https://doi.org/10.5281/zenodo.10820318>
19. Raievska I., Raievska M., Sysak Ya. LocalNR, Package of local nearrings, Version 1.0.4 (2024) (GAP package),
<https://gap-packages.github.io/LocalNR/>

**Наукові праці, які засвідчують апробацію
матеріалів дисертації:**

1. Raievska M. p -Groups with cyclic subgroup of index p and local nearrings. 15th Ukraine Algebra Conference, Lviv, Ukraine, July 8–12, 2025. P. 87,
<https://xvuac.mmf.com.ua/index.php/abstracts>
Форма участі — online, доповідь.
2. Раєвська М. Про локальні майже-кільця з нільпотентною мультиплікативною групою. The conference of young scientists “Pidstryhach Readings — 2025”, Lviv, Ukraine, May 27–29, 2025,
http://iapmm.lviv.ua/chyt2025/abstracts/Raievska_Iryna.pdf
Форма участі — online, доповідь.

3. Raievska I. Yu., Raievska M. Yu. Braces, skew-braces, local nearrings via GAP: the YangBaxter and LocalNR packages. Тези доповідей конференції молодих учених “Підстригачівські читання — 2024”. Львів, Україна, 27–29 травня, 2024,
<http://www.iapmm.lviv.ua/chyt2024/abstracts/Raievska.pdf>
 Форма участі — online, доповідь.
4. Raievska I., Raievska M. LocalNR package and its applications, GAP Days Spring 2024, University of Kaiserslautern-Landau, Kaiserslautern, March 11–15, 2024,
<https://www.gapdays.de/gapdays2024-spring/abstracts/raievska>
 Форма участі — очно, доповідь.
5. Raievska I., Raievska M. Finite local nearrings and their classification, International conference-workshop “GAP Days Summer 2022”, RWTH Aachen University, Aachen, Germany, October 17–21, 2022,
<https://www.gapdays.de/gapdays2022-summer/abstracts/raievska>
 Форма участі — очно, доповідь.
6. Raievska I., Raievska M., Local nearrings and their classification, International Conference “On the Trail of Women in Mathematics “Contemporary Women in Mathematics”, Gdansk, Poland, September 15–17, 2022,
https://otowim22.ptkwm.pl/Abstract_Book.pdf
 Форма участі — очно, доповідь.
7. Raievska I., Raievska M., Local nearrings of order 343. International Algebraic Conference “At the End of the Year 2021”. Kyiv, Ukraine,

December 27–28, 2021 (in the form of webinars)

<https://www.imath.kiev.ua/~algebra/algebra2021/abstracts>

Форма участі — online, доповідь.

8. Abramov A. V., Raievska I. Yu., Raievska M. Yu., Sysak Ya. P., Yurashev V. G. Miller-Moreno groups as multiplicative groups of local nearrings of order 64. 13th International Algebraic Conference in Ukraine. Kyiv, Ukraine, July 6–9, 2021 (in the form of webinars)

[https://drive.google.com/file/d/](https://drive.google.com/file/d/1wdZLWtj9jeFLH9BjSb7ZX5RFnTfTpstE/view)

[1wdZLWtj9jeFLH9BjSb7ZX5RFnTfTpstE/view](https://drive.google.com/file/d/1wdZLWtj9jeFLH9BjSb7ZX5RFnTfTpstE/view)

Форма участі — online, доповідь.

9. Abramov A. V., Raievska I. Yu., Raievska M. Yu., Sysak Ya. P., Yurashev V. G. Local nearrings of order 1331. Abstracts of the conference dedicated to the 60th anniversary of the algebra department of Kyiv University. Kyiv, Ukraine, July 14–17, 2020, P. 11;

[https://drive.google.com/file/d/](https://drive.google.com/file/d/1gyNWN20TC6V09mP3uRXw7uG9bg-3S_E7/view)

[1gyNWN20TC6V09mP3uRXw7uG9bg-3S_E7/view](https://drive.google.com/file/d/1gyNWN20TC6V09mP3uRXw7uG9bg-3S_E7/view)

Форма участі — online, доповідь.

10. Raievska I., Raievska M., The additive groups of local nearrings of order 64. Тези доповідей конференції молодих учених “Підстригачівські читання — 2020”. Львів, Україна, 26–28 травня, 2020,

<http://iapmm.lviv.ua/chyt2020/abstracts/Raievska.pdf>

Форма участі — online, доповідь.

11. Raievska I. Yu., Raievska M. Yu. Some special p -groups and nearrings with identity. Тези доповідей до XII Міжнародної алгебраїчної конференції в Україні, присвяченій 215-й річниці з дня народження В. Буняковського, 02–06 липня 2019 р., Донецький національний

університет імені Василя Стуса, Вінниця, Україна, С. 92–93,
<https://jiac.donnu.edu.ua/article/view/6991>

Форма участі — заочно.

12. Раєвська І. Ю., Раєвська М. Ю. Локальні майже-кільця на скінченних неабелевих p -групах. Тези доповідей міжнародної конференції “Сучасні проблеми механіки та математики” присвяченої 90-річчю від дня народження академіка НАН України Ярослава Степановича Підстригача та 40-річчю створеного ним Інституту прикладних проблем механіки і математики НАН України, 22–25 травня 2018 р., Інститут прикладних проблем механіки і математики ім. Я. С. Підстригача НАН України, Львів, Т. 3, С. 230,
http://www.iapmm.lviv.ua/mpmm2018/Volume_3.pdf

Форма участі — очно, доповідь.

13. Raievska I. Yu., Raievska M. Yu., Sysak Ya. P. Local nearrings of order 64. Abstracts of the International mathematical conference “Groups and Actions: Geometry and Dynamics, dedicated to the memory of professor Vitaly Sushchansky”. Kyiv, Ukraine, December 19–22, 2016, P. 43.

Форма участі — очно, доповідь.

14. Raievska I. Yu., Raievska M. Yu. Finite one-sided distributive structures. Тези доповідей XI Літньої школи “Алгебра, Топологія, Аналіз”, 1–14 серпня 2016 р., Одеса, Україна,
http://www.imath.kiev.ua/~topology/ata11/ata11_theses.pdf

Форма участі — очно, доповідь.

15. Raievska I., Raievska M. Local nearrings on finite 2-generated non-abelian non-metacyclic p -groups. Abstracts of Scientific Conference

dedicated to 100th anniversary of K. M. Fishman and M. K. Fage. Chernivtsi, Ukraine, July 1–4, 2015, P. 103.

Форма участі — очно, доповідь.

16. Raievska I. Yu., Raievska M. Yu., Sysak Ya. P. Local nearrings of order 81. Abstracts of X International Algebraic Conference in Ukraine dedicated to the 70th anniversary of Yu. A. Drozd, Odessa, Ukraine, August 20–27, 2015, P. 94.

Форма участі — очно, доповідь.

17. Raievska M. Finite local nearrings on non-abelian p -groups with cyclic commutator subgroups. Abstracts of conference “Groups and their actions”. Bedlewo (near Poznan), Poland, June 22–26, 2015,
<http://mat.polsl.pl/groups/bedlewo-2015.pdf>

Форма участі — очно, доповідь.

18. Raievska I., Raievska M. Finite local nearrings on split metacyclic additive group. Тези доповідей Міжнародної конференції молодих математиків, 3–6 червня 2015 р., Ін-т математики НАН України, Київ, Україна, С. 42.

Форма участі — очно, доповідь.

19. Raievska M. On multiplicative groups of finite local nearrings. Abstracts of AAA89: Workshop on General Algebra, Dresden, Germany, February 26 – March 1, 2015,
<http://at.yorku.ca/cgi-bin/abstract/cbkb-72>

Форма участі — очно, доповідь.

20. Raievska I., Raievska M. On finite one-sided distributive structures. Abstracts of Humboldt Kolleg “Education and science and their role

in social and industrial progress of society”. Kyiv, Ukraine, June 12–15, 2014, P. 45.

Форма участі — очно, доповідь.

21. Raievska I., Raievska M., Sysak Ya. Finite local nearrings with multiplicative Miller–Moreno group. Abstracts of 9-th International Algebraic Conference in Ukraine. Lviv, Ukraine, July 8–13, 2013, P. 154.

Форма участі — очно, доповідь.

Відомості про апробацію результатів дисертації

Основні результати дисертації доповідалися й обговорювалися на:

- Воркшоп, присвячений 70-річчю Юрія Вікторовича Боднарчука, 23 грудня 2025 року, Національний університет “Києво-Могилянська академія”, Київ, Україна;
- Ukraine Mathematics Conference “At the End of the Year 2025”, December 18–19, 2025, Taras Shevchenko National University of Kyiv, Kyiv, Ukraine,
<https://sites.google.com/knu.ua/umc-2025/>
- 15th Ukraine Algebra Conference, July 8–12, 2025, Lviv, Ukraine,
<https://xvuac.mmf.com.ua/index.php/abstracts>
- The conference of young scientists “Pidstryhach Readings — 2025”, May 27–29, 2025, Lviv, Ukraine,
http://iapmm.lviv.ua/chyt2025/abstracts/Raievska_Maryna.pdf
- Конференція молодих учених “Підстригачівські читання – 2024”, 27–29 травня 2024 року, Львів, Україна,
<http://www.iapmm.lviv.ua/chyt2024/index.html>

- GAP Days Spring 2024, March 11–15, 2024, University of Kaiserslautern-Landau, Kaiserslautern, Germany,
<https://www.gapdays.de/gapdays2024-spring/abstracts/raievska>
- The 14th International Algebraic Conference in Ukraine (online), July 3–7, 2023, Sumy, Ukraine,
<https://sites.google.com/view/iacu2023/home>
- Online Twinning Conference (online), March 27–30, 2023, Digital Theme UK-Ukraine Twinning Initiative, Great Britain,
<https://irp.cdn-website.com/ee30e730/files/uploaded/Final\%20Programme\%20UA-DIGITAL\%202023.pdf>
- International conference-workshop “GAP Days Summer 2022”, October 17–21, 2022, RWTH Aachen University, Aachen, Germany,
<https://www.gapdays.de/gapdays2022-summer/abstracts/raievska>
- International Conference “On the Trail of Women in Mathematics “Contemporary Women in Mathematics”, September 15–17, 2022, Gdansk, Poland,
<https://otowim22.ptkwm.pl/>
- International Algebraic Conference “At the End of the Year 2021” (online), December 27–28, 2021, Kyiv, Ukraine,
<https://www.imath.kiev.ua/~algebra/algebra2021/>
- 3rd TA visitors meeting (TAM) (online), November 3–4, 2021, Amsterdam, Netherlands, <https://www.hpc-europa.org/3rdTAM>
- The 13th International Algebraic Conference in Ukraine, July 6–9, 2021, Kyiv, Ukraine,
<https://drive.google.com/file/d/1wdZLWtj9jeFLH9BjSb7ZX5RFnTfTpstE/view>

- Міжнародна конференція молодих математиків (online), 3–5 червня 2021 року, Київ, Україна,
https://www.imath.kiev.ua/~young/youngconf2021/Abstracts_2021.pdf
- The conference dedicated to the 60th anniversary of the algebra department of Kyiv University, July 14–17, 2020, Kyiv, Ukraine,
<https://sites.google.com/view/kyiv-algebra60/home>
- GAP-Singular-Meeting as part of the OpenDreamKit project, August 15–23, 2019, PfalzAkademie, Lambrecht, Germany,
<https://opendreamkit.org/meetings/2019-04-02-GAPsingularMeeting/>
- XII International Algebraic Conference in Ukraine dedicated to the 215th anniversary of V. Bunyakovsky, July 02–06, 2019, Vinnytsia, Ukraine,
<https://xvuac.mmf.com.ua/index.php/history/all-history/90-xii-iacu>
- 4th Conference of Mathematical Society of Moldova CMSM4'2017, June 28 – July 2, 2017, Chisinau, Republic of Moldova,
<http://cmsm4.math.md/>
- International mathematical conference “Groups and Actions: Geometry and Dynamics, dedicated to the memory of professor Vitaly Sushchanskyy”, December 19–22, 2016, Kyiv, Ukraine,
<https://www.ukma.edu.ua/eng/index.php/news/667-international-conference-groups-and-actions-geometry-and-dynamics>
- XI Літня школа “Алгебра, Топологія, Аналіз”, 1–14 серпня 2016 року,

Одеса, Україна,

<https://www.imath.kiev.ua/~topology/ata11/>

- Summer School on Algebra, Statistics and Combinatorics, June 27 – July 2, 2016, Espoo, Finland,
<https://www.aalto.fi/en/news/summer-school-on-algebra-statistics-and-combinatorics>
- XVII Міжнародна наукова конференція ім. акад. Михайла Кравчука, 19–20 травня 2016 року, Київ, Україна,
<https://matan.kpi.ua/uk/kravchuk-conf2016.html>
- X Міжнародна алгебраїчна конференція в Україні присвячена 70-річчю Ю. А. Дрозда, 20–27 серпня 2015 року, Одеса, Україна
- X Літня школа “Алгебра, Топологія, Аналіз”, 3–15 серпня 2015 року, Одеса, Україна,
<https://imath.kiev.ua/~topology/xata/>
- Наукова конференція, присвячена 100-річчю від дня народження К. М. Фішмана та М. К. Фаге, 1–4 липня 2015 року, Чернівці, Україна
- Conference “Groups and their actions”, June 22–26, 2015, Bedlewo (near Poznan), Poland
- Міжнародна конференція молодих математиків, 3–6 червня 2015 року, Київ, Україна
- AAA89: Workshop on General Algebra, February 26 – March 01, 2015, Dresden, Germany,
<https://tu-dresden.de/mn/math/algebra/forschung/tagungen/aaaseries/aaa89>

- IX-а Літня школа “Алгебра, топологія і аналіз”, 7–18 липня 2014 року, Поляниця, Україна,
https://imath.kiev.ua/~topology/xata/xata_program.pdf
- Humboldt Kolleg “Education and Science and their Role in Social and Industrial Progress of Society”, June 12–15, 2014, Kyiv, Ukraine,
<http://hk2014.humboldt.org.ua/>
- 9th International Algebraic Conference in Ukraine, July 08–13, 2013, Lviv, Ukraine,
<http://iapmm.lviv.ua/iacu2013/>
- засіданнях Вченої ради Інституту математики НАН України (20 червня 2023 р. — онлайн, 24 червня 2025 р. — онлайн)
- семінарі лабораторії топології Інституту математики НАН України (керівник: чл.-кор. С. І. Максименко, Київ, Україна) (19 квітня 2023 р. — онлайн) <https://www.imath.kiev.ua/events/index.php?seminarId=34&archiv=1>
- семінарах “Алгебра” Варшавського університету (керівник: проф. Ян Окнінський, Варшава, Польща) (21 квітня 2022 р., 9 березня 2023 р., 18 січня 2024 р.) <https://www.mimuw.edu.pl/en/seminars/seminar-algebra/>
- семінарі “Secant group” в ІМ ПАН (керівник: проф. Ярослав Бучинський, Варшава, Польща) (31 січня 2023 р.)
- семінарі “Algebra and Discrete Mathematics” в Університеті міста Лінц (керівник: проф. Мануель Кауерс, Лінц, Австрія) (18 квітня 2024 р.) <http://www.algebra.uni-linz.ac.at/teaching/seminar/schedule.php?term=ss2024>

- Алгебраїчних семінарах Інституту математики НАН України (керівники: чл.-кор. Ю. А. Дрозд, чл.-кор. С. І. Максименко, Київ, Україна) (6 жовтня 2015 р., 18 грудня 2018 р., 26 червня 2024 р. — онлайн, 12.11.2025 р.) <https://www.imath.kiev.ua/events/index.php?seminarId=22&archiv=1>
- розширене засідання “Під кінець року” Алгебраїчного семінару Київського національного університету імені Тараса Шевченка (керівник: проф. А. П. Петравчук) (26 грудня 2017 р.)
- семінарі молодих вчених Інституту математики НАН України (організатор: Рада молодих вчених ІМ НАНУ, Київ, Україна) (29 вересня 2016 р.) <https://www.imath.kiev.ua/events/index.php?seminarId=85>
- Scientific Seminar “Geometry, Topology, Applications” (керівник: проф. Т. О. Банах, Львів, Україна) (9 березня 2026 р.) <http://www.math.lviv.ua/seminar/past.php>