

На правах рукопису
Національна академія наук України
Інститут математики

РАЄВСЬКА Ірина Юріївна

УДК 512.6

**Скінченні майже-кільця з одиницею
та локальні майже-кільця
з деякими обмеженнями на адитивні
групи**

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. І. Ю. Раєвська



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

Київ — 2026

Анотація

Раєвська І. Ю. Скінченні майже-кільця з одиницею та локальні майже-кільця з деякими обмеженнями на адитивні групи. — 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 дослідженню майже-кілець з одиницею та локальних майже-кілець, та їх побудові за допомогою системи комп’ютерної алгебри GAP.

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

Розділ 1 складається з трьох підрозділів 1.1, 1.2 та 1.3. У розділі 1 наведено огляд літератури за темою дисертації. Підрозділ 1.1 присвячено огляду відомих результатів про скінченні майже-кільця з одиницею. Очевидно, що кожне асоціативне кільце є майже-кільцем, і кожна група є адитивною групою майже-кільця, але не обов’язково майже-кільця з одиницею. Клей ввів механізм, необхідний і достатній для побудови всіх майже-кілець, адитивна група яких є скінченною та циклічною. Мексон довів, що якщо таке майже-кільце має мультиплікативну одиницю, то це майже-кільце є кільцем. Питання про те, які групи можуть бути адитивними групами майже-кілець з одиницею, досліджується з кінця 1960-х років. Один з перших результатів в цьому напрямку був отриманий Клейом і Малон, які показали, що з точністю до ізоморфізму існує єдине майже-кільце з одиницею, адитивна група якого циклічна, і яке фактично є комутативним кільцем. Також було встановлено, що адитивна група скінченного майже-кільця з одиницею є простою тоді і тільки тоді, коли це майже-кільце є полем простого порядку. Більш того, доведе-

но, що кожна нециклічна група, порядок якої є добутком різних простих чисел, та симетрична група S_n при $n \geq 3$ не можуть бути адитивними групами майже-кілець з одиницею. Клей показав, що не існує майже-кілець з одиницею, адитивна група якого ізоморфна групі кватерніонів Q_8 та встановив, що існує сім неізоморфних класів майже-кілець з одиницею на групі діедра D_4 порядку 8. Ці сім класів майже-кілець перелічені в таблиці 3. Клей і Мексон довели, що узагальнені групи кватерніонів Q_{2^n} при $n > 3$ не можуть бути адитивними групами майже-кілець з одиницею. Групи діедра D_n порядку $2n$ як адитивні групи майже-кілець з одиницею були досліджені Джонсоном та встановлено, що для непарного n група D_n не може бути адитивною групою майже-кілець з одиницею, та доведено, що з точністю до ізоморфізму існує єдине таке майже-кілець на групі D_n при $n = 2p$, де p — просте число. Бойкетт та Нибауер класифікували всі майже-кілець з одиницею на групах порядку, що не перевищує 31, використовуючи систему комп'ютерної алгебри GAP. Зокрема, визначили всі неабелеві групи вказаних порядків, які не можуть бути адитивними групами майже-кілець з одиницею. Якщо адитивна група R^+ деякого майже-кілець R з одиницею є метациклічною групою Міллера–Морено, то вона є p -групою. Очевидно, що кожне дистрибутивне майже-кілець є напівдистрибутивним, але не навпаки. Наприклад, майже-кілець $\text{Map}(G)$ всіх функцій на групі G порядку 2 є напівдистрибутивним, а не дистрибутивним. Відомо, що адитивна група будь-якого дистрибутивного майже-кілець з одиницею є абелевою. У підрозділі 1.2 наведені результати, що стосуються скінченних локальних майже-кілець. Дослідження локальних майже-кілець було ініційовано Мексоном, який визначив ряд їх основних властивостей і, зокрема, довів, що адитивна група нуль-симетричного локального майже-кілець є p -групою. Цим автором було описано усі неізоморфні нуль-симетричні локальні майже-кілець з нециклічною адитивною групою порядку p^2 , які

не є майже-полями. Зазначимо, що залишається відкритим питання, які неабелеві p -групи можуть бути адитивними групами локальних майже-кілець. У підрозділі 1.3 дано огляд системи комп'ютерної алгебри GAP, назва якої розшифровується як “Groups, Algorithms and Programming”. Разом із системою розповсюджується багато пакетів для неї, наприклад, пакет “Systems of nearrings and their applications” (SONATA) — це пакет для побудови та дослідження скінченних майже-кілець та майже-кілець з одиницею. В цьому пакеті міститься бібліотека всіх 68659 майже-кілець порядку менших за 16, та всіх майже-кілець з одиницею порядку меншого за 32. А також, різноманітні функції для аналізу структури та елементів скінченних майже-кілець.

Розділ 2 складається з чотирьох підрозділів 2.1, 2.2, 2.3 та 2.4. В цьому розділі наведено основні означення та результати, що стосуються майже-кілець з одиницею та груп порядку p^3 . У підрозділах 2.1 та 2.2 наведено результати про групи порядку p^3 та майже-кілець з одиницею, відповідно, які буде використано в подальших дослідженнях. Підрозділ 2.3 присвячено вивченню майже-кілець з одиницею на абелевих групах порядку p^3 . Отримані необхідні умови існування майже-кілець з одиницею на таких групах. У підрозділ 2.4 доведено необхідні умови існування майже-кілець з одиницею на неабелевих групах порядку p^3 . Цей розділ складається з двох підпунктів 2.4.1 та 2.4.2, в яких вивчаються майже-кілець з одиницею, адитивна група яких ізоморфна G_1 та G_3 , відповідно.

Розділ 3 складається з трьох підрозділів 3.1, 3.2 та 3.3. Цей розділ присвячено вивченню локальних майже-кілець порядку p^3 . У підрозділі 3.1 наведено означення локальних майже-кілець та їх основні властивості. Підрозділ 3.2 присвячено вивченню локальних майже-кілець на елементарних абелевих групах порядку p^3 . Цей розділ складається з одного підпункту 3.2.1, в якому побудовано приклади локальних майже-кілець з елементарною абелевою адитивною групою порядку p^3 . У підрозділі 3.3

вивчаються локальні майже-кільця на неабелевих групах порядку p^3 . В трьох підпунктах 3.3.1, 3.3.2 та 3.3.3 цього розділу отримані необхідні та достатні умови існування локальні майже-кільця, адитивні групи яких ізоморфні G_1 , G_2 та G_3 , відповідно.

Розділ 4 складається з трьох підрозділів 4.1, 4.2 та 4.3. В цьому розділі вивчаються майже-кільця з одиницею порядків p^4 . У підрозділі 4.1 наведено класифікацію груп порядку p^4 . Підрозділах 4.2 та 4.3 отримано необхідні умови існування майже-кілець з одиницею на групах класу нільпотентності 2 та класу нільпотентності 3, відповідно.

Розділ 5 складається з двох підрозділів 5.1 та 5.2. В цьому розділі описано локальні майже-кільця порядку p^4 . Підрозділ 5.1 присвячено дослідженню локальні майже-кільця на групах порядку p^4 та класу нільпотентності 2. А саме, показано, що для непарних p із 6 таких груп 4 є адитивними групами локальних майже-кілець. Деякі приклади таких майже-кілець явно побудовані. У підрозділі 5.2 досліджуються групи класу нільпотентності 3 порядку p^4 , які є адитивними групами локальних майже-кілець. В трьох підрозділах 5.2.1, 5.2.2 та 5.2.3 цього розділу отримані необхідні та достатні умови існування локальні майже-кілець, адитивні групи яких ізоморфні H_1 та H_2 . У підрозділі 5.2.4 сформульовано гіпотезу щодо груп H_3 та H_4 .

Розділ 6 складається з п'яти підрозділів 6.1, 6.2, 6.3, 6.4 та 6.5. У цьому розділі вивчаються майже-кільцям з одиницею на деяких неабелевих групах. У підрозділі 6.1 дано означення та опис груп Міллера–Морено та груп Шмідт. У підрозділі 6.2 описано всі можливі типи груп Міллера–Морено, які є адитивними групами майже-кілець з одиницею. У підрозділі 6.3 показано, що не існує майже-кілець з одиницею, адитивна група яких ізоморфна групі Шмідта. Підрозділ 6.4 складається з трьох підпунктів 6.4.1, 6.4.2 та 6.4.3. У цьому підрозділі досліджуються прямі добутки метациклічних p -груп Міллера–Морено та циклічних p -груп як адитив-

ні групи майже-кілець з одиницею та локальних майже-кілець. Більш того, визначено формули множення для таких майже-кілець та описано функції, що їх задають. У підрозділі 6.5 вивчаються прямі добутки неметациклічних p -груп Міллера–Морено та циклічних p -груп як адитивні групи майже-кілець з одиницею та локальних майже-кілець. Цей підрозділ складається з трьох підпунктів 6.5.1, 6.5.2 та 6.5.3. В першому підпункті 6.5.1 наведено попередні результати. В підпункті 6.5.2 досліджуються майже-кілець з одиницею на групах $F(p^m, p^n, p, p^k)$. В підпункті 6.5.3 визначено формули множення для локальних майже-кілець на групах $F(p^m, p^n, p, p^k)$ та описано функції, що їх задають.

Розділ 7 складається з п'яти підрозділів 7.1, 7.2, 7.3, 7.4 та 7.5. Цей розділ присвячено застосуванню системи GAP для дослідження та класифікації локальних майже-кілець. В перших двох підрозділах 7.1 та 7.2 вивчається побудова майже-кілець з одиницею та класифікація локальних майже-кілець. В підрозділі 7.3 описано деякі функції з пакету LocalNR, а саме, UnitsOfNearRing 7.3.1, IsLocalNearRing 7.3.2, IsLocalRing 7.3.3, NearRingNonUnits 7.3.4 та NonUnitsAsAdditiveSubgroup 7.3.5. В підрозділі 7.4 досліджено майже-кілець з одиницею і локальні майже-кілець, та ендоециклічні групи. Підрозділ 7.5 присвячено класифікації локальних майже-кілець малих порядків, а саме, локальних майже-кілець порядку 32 7.5.1 та 128 7.5.2 та 7.5.3.

Ключові слова: Майже-кілець з одиницею, локальні майже-кілець, адитивна група, групи Міллера–Морено, групи Шмідта, GAP, SONATA, LocalNR.

Abstract

Raievska I. Iu. Finite nearrings with identity and local nearrings with some restrictions on additive groups. — 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 nearrings with identity and local nearrings, and their construction using the computer algebra system GAP.

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.

Chapter 1 of the thesis consists of three subsections 1.1, 1.2 and 1.3. Section 1 provides a review of the literature on the topic of the dissertation. Subsection 1.1 is devoted to a review of known results on finite nearrings with identity. It is obvious that every associative ring is a nearring, and every group is the additive group of a nearring, but not necessarily of a nearring with identity. Clay introduced a mechanism necessary and sufficient to construct all nearrings whose additive group is finite and cyclic. Maxson proved that if such a nearring has a multiplicative identity, then this nearring is a ring. The question of which groups can be additive groups of nearrings with identity has been studied since the late 1960s. One of the first results in this direction was obtained by Clay and Malone, who showed that up to isomorphism there exists a unique nearring with unity whose additive group is cyclic and which is in fact a commutative ring. It was also established that the additive group of a finite nearring with unity is prime if and only if this nearring is a field of prime order. Moreover, it was proved that every non-cyclic group whose order is the product of distinct primes and the

symmetric group S_n for $n \geq 3$ cannot be additive groups of nearrings with identity. Clay showed that there is no nearring with unity whose additive group is isomorphic to the quaternion group Q_8 and established that there are seven non-isomorphic classes of nearrings with unity on the dihedral group D_4 of order 8. These seven classes of nearrings are listed in Table 3. Clay and Maxson proved that the generalized quaternion groups Q_{2^n} for $n > 3$ cannot be additive groups of nearrings with identity. The dihedral groups D_n of order $2n$ as additive groups of nearrings with identity were studied by Johnson and it was established that for odd n the group D_n cannot be an additive group of nearrings with identity, and it was proved that up to isomorphism there exists a unique such nearring on the group D_n for $n = 2p$, where p is a prime number. Boykett and Noebauer classified all nearrings with identity on groups of order not exceeding 31 using the GAP computer algebra system. In particular, they defined all non-Abelian groups of the specified orders that cannot be additive groups of nearrings with identity. Groups with wide systems of Abelian subgroups have been studied by many authors. In particular, minimal non-Abelian groups, i.e., such non-Abelian groups in which all proper subgroups are Abelian, have been called Miller–Moreno groups, in honor of the authors who first considered finite groups with this property a century ago and proved their solvability. These groups were first studied by Miller and Moreno. If the additive group R^+ of some nearring R with identity is a metacyclic Miller–Moreno group, then it is a p -group. Moreover, as proved by Clay, the group of quaternions Q_8 cannot be the additive group of such a nearring R either. Therefore, the group R^+ can be isomorphic only to the group $G(p^m, p^n)$ for suitable primes p and natural numbers m and n . It is obvious that every distributive nearring is semidistributive, but not vice versa. For example, the nearring $\text{Map}(G)$ of all functions on the group G of order 2 is semidistributive, not distributive. It is known that the additive group of any distributive nearring with identi-

ty is abelian. Subsection 1.2 gives results concerning finite local nearrings. The study of local nearrings was initiated by Maxson, who determined a number of their basic properties and, in particular, proved that the additive group of a zero-symmetric local nearring is a p -group. This author described all non-isomorphic zero-symmetric local nearrings with a non-cyclic additive group of order p^2 that are not nearfields. Note that it remains an open question which non-abelian p -groups can be additive groups of local nearrings. In subsection 1.3, an overview of the GAP computer algebra system, whose name stands for “Groups, Algorithms and Programming”, is given. Many packages for it are distributed together with the system, for example, the “Systems of nearrings and their applications” (SONATA) package — this is a package for constructing and studying finite nearrings and nearrings with identity. This package contains a library of all 68659 nearrings of order less than 16, and all nearrings with identity order less than 32. Also, various functions for analyzing the structure and elements of finite nearrings.

Chapter 2 consists of four subsections 2.1, 2.2, 2.3, and 2.4. This section presents the main definitions and results concerning nearrings with identity and groups of order p^3 . Subsections 2.1 and 2.2 present results on groups of order p^3 and nearrings with identity, respectively, which will be used in further research. Subsection 2.3 is devoted to the study of nearrings with identity on abelian groups of order p^3 . Necessary conditions for the existence of nearrings with identity on such groups are obtained. Subsection 2.4 proves necessary conditions for the existence of nearrings with identity on non-abelian groups of order p^3 . This section consists of two subsections 2.4.1 and 2.4.2, which studies nearrings with identity whose additive group is isomorphic to G_1 and G_3 , respectively.

Chapter 3 consists of three subsections 3.1, 3.2, and 3.3. This section is devoted to the study of local nearrings of order p^3 . Subsection 3.1 gives the definition of local nearrings and their basic properties. Subsection 3.2

is devoted to the study of local nearrings on elementary abelian groups of order p^3 . This section consists of one subsection 3.2.1, in which examples of local nearrings with an elementary abelian additive group of order p^3 are constructed. Subsection 3.3 studies local nearrings on non-abelian groups of order p^3 . In three subsections 3.3.1, 3.3.2 and 3.3.3 of this section, necessary and sufficient conditions for the existence of local nearrings whose additive groups are isomorphic to G_1 , G_2 and G_3 , respectively, are obtained.

Chapter 4 consists of three subsections 4.1, 4.2, and 4.3. This section studies nearrings with identity of orders p^4 . In subsection 4.1, a classification of groups of order p^4 is given. In subsections 4.2 and 4.3, necessary conditions for the existence of nearrings with identity on groups of nilpotency class 2 and nilpotency class 3, respectively, are obtained.

Chapter 5 consists of two subsections 5.1 and 5.2. This section describes local nearrings of order p^4 . Subsection 5.1 is devoted to the study of local nearrings on groups of order p^4 and nilpotency class 2. Namely, it is shown that for odd p out of 6 such groups 4 are additive groups of local nearrings. Some examples of such nearrings are explicitly constructed. In subsection 5.2 groups of nilpotency class 3 of order p^4 , which are additive groups of local nearrings, are studied. In three subsections 5.2.1, 5.2.2 and 5.2.3 of this section, necessary and sufficient conditions for the existence of local nearrings whose additive groups are isomorphic to H_1 and H_2 are obtained. In subsection 5.2.4, a hypothesis is formulated regarding the groups H_3 and H_4 .

Chapter 6 consists of five subsections 6.1, 6.2, 6.3, 6.4, and 6.5. This section studies nearrings with identity on some non-Abelian groups. In subsection 6.1, the definition and description of Miller–Moreno groups and Schmidt groups are given. In subsection 6.2, all possible types of Miller–Moreno groups, which are additive groups of nearrings with identity, are described. In subsection 6.3, it is shown that there are no nearrings with identity whose

additive group is isomorphic to the Schmidt group. Subsection 6.4 consists of three subsections 6.4.1, 6.4.2 and 6.4.3. In this subsection, direct products of metacyclic Miller–Moreno p -groups and cyclic p -groups as additive groups of nearrings with identity and local nearrings are studied. Moreover, multiplication formulas for such nearrings are defined and the functions that define them are described. In subsection 6.5, direct products of non-metacyclic Miller–Moreno p -groups and cyclic p -groups as additive groups of nearrings with identity and local nearrings are studied. This subsection consists of three subsections 6.5.1, 6.5.2 and 6.5.3. The first subsection 6.5.1 presents preliminary results. Subsection 6.5.2 investigates nearrings with unity on the groups $F(p^m, p^n, p, p^k)$. Subsection 6.5.3 defines multiplication formulas for local nearrings on the groups $F(p^m, p^n, p, p^k)$ and describes the functions that define them.

Chapter 7 consists of five subsections 7.1, 7.2, 7.3, 7.4 and 7.5. This section is devoted to the application of the GAP system to the study and classification of local nearrings. The first two subsections 7.1 and 7.2 study the construction nearrings with identity and classification of local nearrings. Section 7.3 describes some functions from the LocalNR package, namely, UnitsOfNearRing 7.3.1, IsLocalNearRing 7.3.2, IsLocalRing 7.3.3, NearRingNonUnits 7.3.4 and NonUnitsAsAdditiveSubgroup 7.3.5. In subsection 7.4, nearrings with identity and local nearrings, and endocyclic groups are studied. Subsection 7.5 is devoted to the classification of local nearrings of small orders, namely, local nearrings of order 32 7.5.1 and 128 7.5.2 and 7.5.3.

Key words: Nearrings, local nearrings, additive group, Miller–Moreno groups, Schmidt group, GAP, SONATA, LocalNR.

Список публікацій

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,
https://bmj.chnu.edu.ua/media/gbdhv1v1/161-169-raievska-raievska_cor.pdf (Категорія Б)
4. Раєвська І. Про прямі добутки неметациклічних p -груп Міллера–Морено та циклічних p -груп як адитивні групи локальних майже-кілець. *Науковий вісник Ужгородського університету. Серія «Математика і інформатика»*, 2025, **46** (1), 79–88,
[https://doi.org/10.24144/2616-7700.2025.46\(1\).79-88](https://doi.org/10.24144/2616-7700.2025.46(1).79-88) (Категорія Б)
5. Raievska I., Raievska M. Groups of the nilpotency class 3 of order p^4 as additive groups of local nearrings. *Carpathian Math. Publ.*, 2025, **17** (1), 292–301,
<https://doi.org/10.15330/cmp.17.1.292-301> (SJR — **Q1**)
6. 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. **76** (11), 1629–1644 (SJR — **Q3**)

7. 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)
8. Raievska I. On direct products of metacyclic Miller–Moreno p -groups and cyclic p -groups as additive groups of local nearrings. *Прикл. проблеми мех. і мат.*, 2024, **22**, 123–130. (Категорія Б)
9. Raievska I., Raievska M. Groups of order p^4 as additive groups of local nearrings. *Ukrainian Math. J.*, 2024, **76** (6), 1005–1024, <https://doi.org/10.1007/s11253-024-02369-w>; translation of *Ukrain. Mat. Zh.*, 2024, **76** (6), 890–906. **76** (6), 890–906 (SJR — **Q3**)
10. 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,
<http://dx.doi.org/10.12958/adm2269> (SJR — **Q3**)
11. Raievska I. Yu. Local nearrings with additive groups of order 128, *Науковий вісник Ужгородського університету. Серія “Математика і інформатика”*, 2024, **44** (1), 46–50,
[https://doi.org/10.24144/2616-7700.2024.45\(2\).110-114](https://doi.org/10.24144/2616-7700.2024.45(2).110-114) (Категорія Б)
12. Raievska I., Raievska M. Lower bounds for the number of local nearrings on groups of order p^3 . *Math. Commun.*, 2024, **29** (2), 177–191,
<https://www.mathos.unios.hr/mc/index.php/mc/issue/view/35> (SJR — **Q4**)
13. Раєвська І. Ю., Раєвська М. Ю. Локальні майже-кільця на елементарних абелевих групах порядку p^3 . Науковий вісник Ужгородсько-

- го університету. Серія “Математика і інформатика”, 2021, **38**(1), 85–93,
[https://doi.org/10.24144/2616-7700.2021.38\(1\).85-93](https://doi.org/10.24144/2616-7700.2021.38(1).85-93) (Категорія Б)
14. 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> (SJR — **Q3**)
 15. 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)
 16. Раєвська І. Ю., Раєвська М. Ю. Скінченні локальні майже-кільця. *Могиллянський математичний журнал*, 2018, **1**, 38–48,
<http://mmj.ukma.edu.ua/article/view/152611/151700>
 17. Raievska I., Raievska M., Sysak Ya. DatabaseEndom32: (v1.0.2) [Data set] (2024). Zenodo,
<https://doi.org/10.5281/zenodo.10820301>
 18. Raievska I., Raievska M., Sysak Ya. DatabaseEndom128: (v0.2) [Data set] (2022). Zenodo,
<https://doi.org/10.5281/zenodo.7225377>
 19. Raievska I., Raievska M., Sysak Ya. DatabaseEndom625: (v0.2) [Data set] (2023). Zenodo,
<https://doi.org/10.5281/zenodo.7613145>
 20. Raievska I., Raievska M., Sysak Ya. LocalNR, Package of local nearrings,

- Version 1.0.4 (2024) (GAP package),
<https://gap-packages.github.io/LocalNR/>
21. Sysak Ya., Raievska I., Raievska M. Construction of local nearrings using GAP, Ukraine Mathematics Conference “At the End of the Year 2025”, December 18–19, 2025, Taras Shevchenko National University of Kyiv, Kyiv, Ukraine, P. 54,
<https://drive.google.com/file/d/1LGUD-of4DUq2LiKYbN233claruwbGIj4/view>
 22. Raievska I., Raievska M., Sysak Ya. Local nearrings with additive groups of order 128 and exponent 8. II, Міжнародна конференція, присвячена 75-й річниці від дня народження Володимира Маслюченка, Чернівецький національний університет імені Юрія Федьковича, 25–27 вересня 2025 року, Чернівці, Україна, С. 159,
<https://drive.google.com/file/d/1Clufy2S3NPcxiNvsyQLnBD035EKDZQsV/view>
 23. Raievska I. On direct products of metacyclic Miller–Moreno p -groups and cyclic p -groups as additive groups of local nearrings, 15th Ukraine Algebra Conference, Lviv, Ukraine, July 8–12, 2025. P. 86,
<https://xvuac.mmf.com.ua/index.php/abstracts>
 24. Раєвська І. Про прямі добутки неметациклічних p -груп Міллера–Морено та циклічних p -груп як адитивні групи локальних майже-кілець, The conference of young scientists “Pidstryhach Readings — 2025”, Lviv, Ukraine, May 27–29, 2025,
http://iapmm.lviv.ua/chyt2025/abstracts/Raievska_Iryna.pdf
 25. 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

26. Raievska I., Raievska M. Groups of order p^4 as additive groups of local nearrings, Ukraine Algebra Conference “At the End of the Year 2023”, Kyiv, Ukraine, December 26–27, 2023 (online),
<https://sites.google.com/view/aey2023/home?authuser=0>
27. Raievska I., Raievska M. Groups of nilpotency class 3 of order p^4 as additive groups of local nearrings, XIX International Scientific Mykhailo Kravchuk Conference, dedicated to the 125th anniversary of Igor Sikorsky Kyiv Polytechnic Institute, Igor Sikorsky Kyiv Polytechnic Institute, October 11–12, 2023 (online),
<https://matan.kpi.ua/en/kravchuk-conf-2023/>
28. Raievska I., Raievska M. Groups of the nilpotency class 2 of order p^4 as additive groups of local nearrings, The 103rd Workshop on General Algebra, Tartu, Estonia, June 9–11, 2023,
https://kodu.ut.ee/~vlaan/AAA103abstracts/abstract_Raievska.pdf
29. Raievska I., Raievska M., Finite one-sided distributive structures and GAP, International Algebraic Conference “At the End of the Year 2022” (online), Kyiv, Ukraine, December 27–28, 2022,
<https://www.imath.kiev.ua/~algebra/algebra2022/abstracts>
30. 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>
31. 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
32. Раєвська І. Ю., Раєвська М. Ю., Локальні майже-кільця на елементарних абелевих групах порядку p^3 , Тези доповідей конференції молодих учених “Підстригачівські читання — 2021”, Львів, Україна, 26–28 травня, 2021,
<http://www.iapmm.lviv.ua/chyt2021/abstracts/Raievska.pdf>
33. Raievskaya I., Raievskaya M., On local nearrings of order p^3 , Abstracts of 11th International Skorobohatko Mathematical Conference, Lviv, Ukraine, October 26–30, 2020, P. 97,
http://www.iapmm.lviv.ua/conf_skorob2020/documents/2020tezy.pdf
34. Raievskaya I. Yu., Raievskaya M. Yu. Local nearrings of order p^3 . Abstracts of 11th International Algebraic Conference in Ukraine dedicated to the 75th anniversary of V. V. Kirichenko, July 3–7, 2017, Institute of Mathematics of NAS of Ukraine, Kyiv, Ukraine, P. 113.
35. Раєвська І. Ю., Раєвська М. Ю. Адитивні групи скінченних майже-кільць з одиницею. Тези доповідей Міжнародної конференції молодих математиків, присвяченої 100-річчю з дня народження академіка НАН України Ю. О. Митропольського (1917–2008), 7–10 червня 2017 р., Ін-т математики НАН України, Київ, С. 20.
36. Raievskaya I. Yu., Raievskaya 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

37. Raievska I. On additive groups of finite local nearrings. Abstracts of AAA89: Workshop on General Algebra, Dresden, Germany, February 26–March 01, 2015,
<https://tu-dresden.de/mn/math/algebra/forschung/tagungen/aaaseries/aaa89>
38. Raievska I., Raievska M. Using the computer algebra system GAP for constructing and studying of algebraic structures. Abstracts of IXth Summer School “Algebra, Topology and Analysis”, Polianytsia, Ukraine, July 7–18, 2014, P. 68–69.
39. Raievska I. Yu., Raievska M. Yu., Sysak Ya. P. Small groups as the additive groups of local nearrings. Abstracts of the International Algebraic Conference dedicated to 100-th anniversary of L. A. Kaluzhnin, Taras Shevchenko Nat. Univ., Kyiv, Ukraine, July 7–12, 2014, P. 70.
40. Raievska I., Raievska M. Finite nearrings with identity on Miller-Moreno groups. Abstracts of IV International Hahn conference dedicated to the 135-th anniversary of Hans Hahn, Chernivtsi, Ukraine, June 30–July 5, 2014, P. 253–255.
41. Raievska I., Raievska M. Nearrings with identity on Miller-Moreno groups. Abstracts of II Ukrainian Scientific Conference “Applying of mathematics methods in science and technics”. Lutsk, Ukraine, November 22–23, 2013, P. 104–109
42. Raievska I. Yu., Raievska M. Yu. Local nearrings of order at most 31. Abstracts of 2nd EUMLS Conference Mathematics for Life Sciences. Olenivka, Crimea, Ukraine, September 5–10, 2013, P. 27.

Зміст

Перелік умовних позначень	24
Вступ	26
Розділ 1	
Огляд літератури та попередні відомості	60
1.1. Скінченні майже-кільця з одиницею	60
1.2. Скінченні локальні майже-кільця	68
1.3. Система комп'ютерної алгебри GAP	82
Висновки до розділу 1	95
Розділ 2	
Майже-кільця з одиницею порядків p^3	96
2.1. Групи порядку p^3	96
2.2. Майже-кільця з одиницею	97
2.3. Майже-кільця з одиницею на абелевих групах порядку p^3 .	99
2.4. Майже-кільця з одиницею на неабелевих групах порядку p^3	102
2.4.1. Майже-кільця з одиницею, адитивна група яких ізо- морфна G_1	102
2.4.2. Майже-кільця з одиницею, адитивна група яких ізо- морфна G_3	108
Висновки до розділу 2	110
Розділ 3	
Локальні майже-кільця порядку p^3	111
3.1. Про локальні майже-кільця	111

3.2. Локальні майже-кільця на елементарних абелевих групах порядку p^3	112
3.2.1. Приклади локальних майже-кілець з елементарною абелевою адитивною групою порядку p^3	117
3.3. Локальні майже-кільця на неабелевих групах порядку p^3	119
3.3.1. Локальні майже-кільця, адитивні групи яких ізоморфні G_1	119
3.3.2. Локальні майже-кільця, адитивні групи яких ізоморфні G_2	129
3.3.3. Локальні майже-кільця, адитивні групи яких ізоморфні G_3	130
Висновки до розділу 3	136

Розділ 4

Майже-кільця з одиницею порядків p^4	138
4.1. Групи порядку p^4	138
4.2. Майже-кільця на групах класу нільпотентності 2	139
4.2.1. Група G_4	140
4.2.2. Майже-кільця з одиницею, адитивні групи яких ізоморфні G_4	141
4.2.3. Група G_5	147
4.2.4. Майже-кільця з одиницею адитивна група яких ізоморфна групі G_5	148
4.3. Майже-кільця на групах класу нільпотентності 3	153
4.3.1. Групи H_1	154
4.3.2. Майже-кільця з одиницею, адитивні групи яких ізоморфні H_1	157

4.3.3. Про групу H_2	163
4.3.4. Майже-кільця з одиницею, адитивні групи яких ізо- морфні H_2	167
Висновки до розділу 4	173

Розділ 5

Локальні майже-кільця порядку p^4	174
5.1. Локальні майже-кільця на групах порядку p^4 та класу нільпотентності 2	174
5.1.1. Групи класу нільпотентності 2 порядку 16 та ло- кальні майже-кільця	174
5.1.2. Групи G_1 , G_2 та G_3 і локальні майже-кільця	175
5.1.3. Локальні майже-кільця, адитивні групи яких ізо- морфні G_4	182
5.1.4. Локальні майже-кільця, адитивні групи яких ізо- морфні G_5	192
5.1.5. Групи G_6	197
5.2. Локальні майже-кільця на групах порядку p^4 та класу нільпотентності 3	198
5.2.1. Локальні майже-кільця, адитивні групи яких ізо- морфні H_1	198
5.2.2. Локальні майже-кільця, адитивні групи яких ізо- морфні H_2	204
5.2.3. Групи H_2 як адитивні групи локальних майже-кілець	207
5.2.4. Групи H_3 та H_4	218
Висновки до розділу 5	218

Розділ 6

Майже-кільця з одиницею на деяких неабелевих

групах	220
6.1. Групи Міллера–Морено та Шмідта	220
6.2. Майже-кільця з одиницею на групах Міллера–Морено . . .	221
6.3. Майже-кільця з одиницею та групи Шмідта	228
6.4. Прямі добутки метациклічних p -груп Міллера–Морено та циклічних p -груп як адитивні групи локальних майже-кілець	229
6.4.1. Групи $F(p^m, p^n, p^k)$	229
6.4.2. Майже-кільця з одиницею на групах $F(p^m, p^n, p^k)$.	230
6.4.3. Локальні майже-кільця, адитивні групи яких ізо- морфні $F(p^m, p^n, p^k)$	236
6.5. Прямі добутки неметациклічних p -груп Міллера–Морено та циклічних p -груп як адитивні групи локальних майже- кілець	240
6.5.1. Попередні результати	240
6.5.2. Майже-кільця з одиницею на групах $F(p^m, p^n, p, p^k)$	242
6.5.3. Локальні майже-кільця на групах $F(p^m, p^n, p, p^k)$. .	248
Висновки до розділу 6	252

Розділ 7

Застосування системи GAP для дослідження та класифікації локальних майже-кілець	254
7.1. Побудова майже-кілець з одиницею	254
7.2. Локальні майже-кільця пакету SONATA	255
7.3. LocalNR package: функції для майже-кілець	258
7.3.1. UnitsOfNearRing	258
7.3.2. IsLocalNearRing	260
7.3.3. IsLocalRing	262
7.3.4. NearRingNonUnits	263

7.3.5. NonUnitsAsAdditiveSubgroup	265
7.4. Майже-кільця з одиницею і локальні майже-кільця, та ендоциклічні групи	266
7.4.1. Локальні майже-кільця та ендоциклічні групи порядку 32	271
7.4.2. Локальні майже-кільця та ендоциклічні групи порядку 256	273
7.5. Класифікація локальних майже-кілець малих порядків	275
7.5.1. Локальні майже-кільця порядку 32	279
7.5.2. Локальні майже-кільця порядку 128	287
7.5.3. 2-Породжені групи експоненти 8 як адитивні групи нуль-симетричних локальних майже-кілець порядку 128	291
Висновки до розділу 7	292
Основні результати та висновки	294
Список використаних джерел	297
Додаток А	
Список публікацій і апробація результатів	313

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
$\text{End}(G)$	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
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 правих обернених в R
R^*	Група оборотних елементів майже-кільця R
$\Phi(G)$	Підгрупа Фраттіні групи G

Вступ

Роботу присвячено вивченню скінченних майже-кілець з одиницею та локальних майже-кілець з обмеженнями на адитивні групи.

Обґрунтування вибору теми дослідження.

Характерною рисою сучасного етапу розвитку алгебри є підвищення активності досліджень в областях, що узагальнюють теорії класичних алгебраїчних систем, наприклад, теорія майже-кілець. Майже-кільця виникають природним чином при вивченні систем нелінійних відображень і вивчаються протягом багатьох десятиліть.

Основи аксіоматики теорії майже-кілець були закладені в роботах Оре [70], Фуртванглера–Таусскі [42] та Таусскі–Тодд [127].

Дослідження майже-кілець пов’язане з роботами Бейдлемана [23, 24], Бетша [25], Блекетта [27], Вендта [129], Мейсона [58], Х. Нойман [69], Петерсона [71], Хезерлі [46] та інші.

Однією з перших робіт в Україні, в якій розглядаються майже-кільця, є стаття Калужніна та Суцанського [50], опубліковано в 1978 році. Першою дисертацією в Україні, в якій розглядаються майже-кільця, є докторська дисертація Усенка [15] захищена у 1999 році.

Відомо, що будь-яка скінченна абелева група A є прямою сумою примарних циклічних підгруп, кожна з яких можна розглядати як адитивну групу деякого кільця лишків $\mathbb{Z}/p^i\mathbb{Z}$. Звідси A є адитивною групою прямої суми цих кілець. Отже, кожна скінченна абелева група є адитивною групою асоціативного (і навіть комутативного) кільця з одиницею. Однак, у випадку майже-кілець з одиницею аналогічний результат для скінченних неабелевих груп не виконується.

Питання про те, які групи можуть бути адитивними групами майже-кілець з одиницею, досліджується з кінця 1960-х років. Над вирішенням цього питання працювали Бойкетт, Джонсон, Дой, Клей, Кріммел, Лай, Лекстон, Локхарт, Малон, Мексон, Нибауер, Раєвська М., Сисак та інші.

В дисертації розглянуто майже-кілець на групах Міллера–Морено, Шмідта.

Монографії Пільца [72], Мелдрума [64], Клея [32], К. Ферреро та Г. Ферреро [41], Локхарта [56] присвячені загальній теорії майже-кілець.

Нагадаємо, що кільце R з одиницею, множина L всіх необоротних елементів якого утворює ідеал в R (а отже, фактор-кільце R/L є тілом), називається локальним кільцем. Як легко переконатися, в означенні локального кільця достатньо насправді припускати, що L є тільки підгрупою адитивної групи кільця R . Замінивши в ньому слово “кільце” на “майже-кільце”, отримуємо означення локальних майже-кілець, вивчення яких розпочав Мексон [60]. Відомо, що скінченна група є адитивною групою деякого локального кільця тоді і тільки тоді, коли вона є абелевою p -групою. Як було показано Мексоном, адитивна група R^+ скінченного локального майже кільця R є p -групою, а його підгрупа L необоротних елементів є ідеалом в R . Звідси випливає, зокрема, що фактор-група R/L є елементарною абелевою. Більш того, ним було встановлено, що кожна абелева p -група, відмінна від циклічної групи та групи порядку 4, є адитивною групою локального майже-кільця, що не є кільцем, а також описані всі неізоморфні нуль-симетричні локальні майже-кілець з елементарною абелевою адитивною групою порядку p^2 , які не є майже-полями.

Однак, задача класифікації скінченних неабелевих p -груп, що є адитивними групами локальних майже-кілець, залишається далекою від розв’язання. Прямі добутки метациклічних p -груп Міллера–Морено та циклічних p -груп, прямі добутки неметациклічних p -груп Міллера–

Морено та циклічних p -груп досліджуються в даному рукописі.

Відомо, наприклад, що узагальнені групи кватерніонів та група дієдра порядку 8 не можуть бути адитивними групами локальних майже-кілець. Крім того, як показав Фейгельсток [40], для кожного простого числа p та цілого $n > p$ існує група порядку p^n , яка не є адитивною групою локального майже-кілля. В зв'язку з цим в роботах [12, 102] вивчалися локальні майже-кілля, адитивна група яких є мінімальною неабелевою або, в іншій термінології, групою Міллера–Морено (див. [118]). Узагальнення в цьому напрямку дослідження є актуальними.

Вивченню локальних майже-кілець присвячені роботи Амберга, Городніка, Губерта, Мексона, Раєвської М., Сисака, Фейгелстока та інших.

Оскільки повністю описані усі нуль-симетричні локальні майже-кілля порядку p^2 , то наступним кроком є характеристика локальних майже-кілець на абелевих та неабелевих групах порядку p^3 та на групах порядку p^4 класу нільпотентності 2 та класу нільпотентності 3.

Список усіх 698 неізоморфних локальних майже-кілець порядку не більше 31 містяться в пакеті SONATA [19] системи комп'ютерної алгебри GAP [43]. Однак класифікація майже-кілець порядку 32 і вище вимагає набагато складніших обчислень. Для локальних майже-кілець вони були реалізовані в новому GAP-пакеті LocalNR [111].

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 еволю-

ційних 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 майже-кілець з одиницею та пов’язаних з ними груп.

Об’єктом дослідження є скінченні майже-кілець з одиницею та локальні майже-кілець.

Предметом дослідження є адитивні групи скінченних майже-кілець з одиницею та локальних майже-кілець, класифікація скінченних локальних майже-кілець.

Завдання дослідження:

- Описати майже-кілець з одиницею на групах порядку p^3 .
- Отримати необхідні умови існування майже-кілець з одиницею на абелевих групах порядку p^3 .
- Отримати необхідні умови існування майже-кілець з одиницею на неабелевих групах порядку p^3 .
- Описати локальні майже-кілець з адитивними групами порядку p^3 . Визначити формули множення для таких майже-кілець та описано функції, що їх задають.
- Навести приклад локальних майже-кілець з адитивною групою порядку p^3 .

- Дати оцінку нижньої межі кількості локальних майже-кілець на групах порядку p^3 .
- Навести алгоритм побудови локального майже-кілця з елементарною абелевою адитивною групою порядку 5^3 , що реалізовано в системі комп'ютерної алгебри GAP.
- Проаналізувати існування та кількість неізоморфних локальних майже-кілець на групах порядку p^3 .
- Навести деякі структурні результати стосовно груп порядку p^4 .
- Отримати необхідні умови існування майже-кілець з одиницею на групах порядку p^4 . Визначити формули множення для таких майже-кілець та описано функції, що їх задають.
- Описати локальні майже-кілця з адитивними групами порядку p^4 . Вказати формули множення для таких майже-кілець та описано функції, що їх задають.
- Навести приклад локального майже-кілця порядку $5^4 = 625$.
- Дати алгоритм побудови локального майже-кілця з неабелевою адитивною групою порядку 5^4 , що реалізовано в системі комп'ютерної алгебри GAP.
- Навести необхідні та достатні умови існування майже-кілець з одиницею на групах Міллера–Морено.
- Показати, що не існує майже-кілець з одиницею, адитивна група яких ізоморфна групі Шмідта.
- Дослідити прямі добутки p -груп Міллера–Морено та циклічних p -груп як адитивні групи майже-кілець з одиницею та локальних

майже-кілець. Визначити формули множення для таких майже-кілець та описано функції, що їх задають.

- Описати побудову майже-кілець з одиницею;
- Навести деякі функції для локальних майже-кілець з пакету LocalNR, а саме:
 - UnitsOfNearRing(R) (вивід: список оборотних елементів майже-кілець, якщо R є майже-кілем з одиницею, інакше вивід має вигляд `Error, no units exist`),
 - IsLocalNearRing(R) (вивід: значення `true`, якщо R є локальним майже-кілем, інакше вивід має значення `false`),
 - IsLocalRing(R) (вивід: значення `true`, якщо R є локальним кільцем, інакше вивід має значення `false`),
 - NearRingNonUnits(R) (вивід: список необоротних елементів R),
 - NonUnitsAsAdditiveSubgroup(R) (вивід: адитивна підгрупа необоротних елементів R);
- Описати майже-кілець з одиницею пакету SONATA та ендоециклічні групи.
- Проаналізувати локальні майже-кілець порядку 32.
- Навести часткову класифікацію локальних майже-кілець порядку 128.
- Знайти 2-породжені ендоециклічні групи порядку 256 та експоненти 16, які не є адитивними групами локальних майже-кілець.

Методи дослідження.

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

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

Наукова новизна одержаних результатів.

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

- Описано майже-кілець з одиницею на групах порядку p^3 .
- Наведено необхідні умови існування майже-кілець з одиницею на абелевих групах порядку p^3 .
- Наведено необхідні умови існування майже-кілець з одиницею на неабелевих групах порядку p^3 .
- Описано локальні майже-кілець з адитивними групами порядку p^3 . Визначено формули множення для таких майже-кілець та описано функції, що їх задають.

- Наведено приклад локального майже-кільця з адитивною групою порядку p^3 .
- Дано оцінку нижньої межі кількості локальних майже-кілець на групах порядку p^3 .
- Наведено алгоритм побудови локального майже-кільця з елементарною абелевою адитивною групою порядку 5^3 , що реалізовано в системі комп'ютерної алгебри GAP.
- Проаналізовано існування та кількість неізоморфних локальних майже-кілець на групах порядку p^3 .
- Наведено деякі структурні результати стосовно груп порядку p^4 .
- Отримано необхідні умови існування майже-кілець з одиницею на групах порядку p^4 .
- Визначено формули множення для таких майже-кілець та описано функції, що їх задають.
- Описано локальні майже-кільця з адитивними групами порядку p^4 . Вказано формули множення для таких майже-кілець та описано функції, що їх задають.
- Наведено приклад локального майже-кільця порядку $5^4 = 625$.
- Дано алгоритм побудови локального майже-кільця з неабелевою адитивною групою порядку 5^4 , що реалізовано в системі комп'ютерної алгебри GAP.
- Наведено необхідні та достатні умови існування майже-кілець з одиницею на групах Міллера–Морено.
- Показано, що не існує майже-кілець з одиницею, адитивна група яких ізоморфна групі Шмідта.

- Описано прямі добутки p -груп Міллера–Морено та циклічних p -груп як адитивні групи майже-кілець з одиницею та локальних майже-кілець. Визначено формули множення для таких майже-кілець та описано функції, що їх задають.
- Описано побудову майже-кілець з одиницею.
- Наведено деякі функції для локальних майже-кілець з пакету LocalNR, а саме:
 - UnitsOfNearRing(R) (вивід: список оборотних елементів майже-кілець, якщо R є майже-кілем з одиницею, інакше вивід має вигляд `Error, no units exist`),
 - IsLocalNearRing(R) (вивід: значення `true`, якщо R є локальним майже-кілем, інакше вивід має значення `false`),
 - IsLocalRing(R) (вивід: значення `true`, якщо R є локальним кілем, інакше вивід має значення `false`),
 - NearRingNonUnits(R) (вивід: список необоротних елементів R),
 - NonUnitsAsAdditiveSubgroup(R) (вивід: адитивна підгрупа необоротних елементів R).
- Описано майже-кілець з одиницею пакету SONATA та ендоециклічні групи.
- Проаналізовано локальні майже-кілець порядку 32.
- Наведено часткову класифікацію локальних майже-кілець порядку 128.
- Знайдено 2-породжені ендоециклічні групи порядку 256 та експоненти 16, які не є адитивними групами локальних майже-кілець.

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, системи GAP, і у деяких інших галузях науки, зокрема, теорії кодування.

Особистий внесок здобувача.

Основні результати дисертації, які виносяться на захист, отримані автором особисто. Три статті опублікована без співавторів. У спільних з науковим консультантом та М. Ю. Раєвською публікаціях за темою дисертації розподіл особистих внесків такий:

- у роботах [1, 2, 17, 18, 19, 20] — визначення напрямку досліджень, постановка задач, ідеї відносно вибору методик розв’язування, побудова алгоритму, брав участь у написанні функцій, обговоренні результатів, контроль якості викладення результатів належить науковому консультанту Я. П. Сисаку.
- у статті [1] — в дисертацію включено теорему 1. Здобувачка брала участь в обговоренні алгоритму.
- у статті [2] — здобувачка брала участь у написанні функцій для майже-кілець: `UnitsOfNearRing`, `IsLocalNearRing`, `IsLocalRing`, `NearRingNonUnits`, `NonUnitsAsAdditiveSubgroup`. В дисертацію включено твердження 1 та гіпотезу.
- у статті [3] — внесок авторів рівноцінний. В дисертацію включено лему 4.
- у статтях [5, 9, 10, 12, 13, 16, 17, 18, 19] — співавторка М. Ю. Раєвська перевіряла результати та брала участь в обговоренні результатів, постановці гіпотез та фінальному оформленні результатів.

- у статті [6] — внесок авторів рівноцінний. В дисертацію включено теорему 13.
- у статті [7] — внесок авторів рівноцінний. В дисертацію включено лему 1, теорему 1, лему 2, теорему 2.
- у статті [14] — внесок авторів рівноцінний. В дисертацію включено лему 5, лему 6, теорему 4.
- у статті [15] — внесок авторів рівноцінний. В дисертацію включено лему 5, теорему 3.
- у пакеті [20] — здобувачка та М. 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/>
- Міжнародна конференція, присвячена 75-й річниці від дня народження Володимира Маслюченка, 25–27 вересня 2025 року, Чернівецький національний університет імені Юрія Федьковича, Чернівці, Україна,

<https://drive.google.com/file/d/1Clufy2S3NPcxiNvsyQLnBD035EKDZQsV/view>

- 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_Iryna.pdf
- GAP Days Spring 2024, March 11–15, 2024, University of Kaiserslautern-Landau, Kaiserslautern, Germany,
<https://www.gapdays.de/gapdays2024-spring/abstracts/raievska>
- Ukraine Algebra Conference “At the End of the Year 2023” (online), December 26–27, 2023, Kyiv, Ukraine,
<https://sites.google.com/view/ae2023/home>
- XIX Міжнародна наукова конференція імені академіка Михайла Кравчука, присвячена 125-річчю КПІ ім. Ігоря Сікорського (онлайн), 11–12 жовтня 2023 року, Київ, Україна,
<https://matan.kpi.ua/en/kravchuk-conf-2023/>
- AAA103, The 103rd Workshop on General Algebra, June 9–11, 2023, University of Tartu, Tartu, Estonia,
<https://aaa103.ut.ee/>
- 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 Algebraic Conference “At the End of the Year 2022” (online), December 27–28, 2022, Kyiv, Ukraine,

<https://www.imath.kiev.ua/~algebra/algebra2022/abstracts>

- 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/>
- Підстригачівські читання – 2021 (онлайн), 26–28 травня 2021 року, Львів, Україна,
<http://www.iapmm.lviv.ua/chyt2021/abstracts/Raievska.pdf>
- 11th International Skorobohatko Mathematical Conference, October 26–30, 2020, Lviv, Ukraine,
http://www.iapmm.lviv.ua/conf_skorob2020/index.html
- Конференція молодих учених “Підстригачівські читання – 2020”, 26–28 травня 2020 року, Львів, Україна,
<http://iapmm.lviv.ua/chyt2020/index.html>
- 11th International Skorobohatko Mathematical Conference, October 26–30, 2020, Lviv, Ukraine,
http://www.iapmm.lviv.ua/conf_skorob2020/
- GAP-Singular-Meeting as part of the OpenDreamKit project, August 15–23, 2019, PfalzAkademie, Lambrecht, Germany,
<https://opendreamkit.org/meetings/2019-04-02-GAPSingularMeeting/>
- Міжнародної наукової конференції “Сучасні проблеми механіки та математики”, яка присвячена 90-річчю від дня народження акаде-

міка НАН України Ярослава Степановича Підстригача та 40-річчю створеного ним Інституту прикладних проблем механіки і математики НАН України, 22–25 травня 2018 року, Львів, Україна,
<http://www.iapmm.lviv.ua/mpmm2018/>

- 11th International Algebraic Conference in Ukraine dedicated to the 75th anniversary of V. V. Kirichenko, July 03–07, 2017, Kyiv, Ukraine,
<https://www.imath.kiev.ua/~algebra/iacu2017/>
- XI Літня школа “Алгебра, Топологія, Аналіз”, 1–14 серпня 2016 року, Одеса, Україна,
<https://www.imath.kiev.ua/~topology/ata11/>
- Міжнародна конференція молодих математиків присвячена 100-річчю з дня народження академіка НАН України Юрія Олексійовича Митропольського (1917–2008), 7–10 червня 2017 року, Київ, Україна,
<https://www.imath.kiev.ua/~young/conf2/>
- 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>
- AAA89: Workshop on General Algebra, February 26 – March 01, 2015, Dresden, Germany,
<https://tu-dresden.de/mn/math/algebra/forschung/tagungen/aaaseries/aaa89>
- The International Algebraic Conference dedicated to 100-th anniversary of L. A. Kaluzhnin, 07–12 July, 2014, Kyiv, Ukraine;

- IX-а Літня школа “Алгебра, топологія і аналіз”, 7–18 липня 2014 року, Поляниця, Україна,
https://imath.kiev.ua/~topology/xata/xata_program.pdf
- IV Міжнародна Ганська конференція, 30 червня – 1 липня 2014 року, Чернівці, Україна;
- 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/>
- II Всеукраїнська наукова конференція “Застосування математичних методів в науці і техніці”, 22–23 листопада 2013 року, Луцьк, Україна;
- 2nd EUMLS Conference Mathematics for Life Sciences, September 05–10, 2013, Olenivka, Crimea, Ukraine,
<http://eumls2013.humboldt.org.ua/>

Семінарах:

- засіданнях Вченої ради Інституту математики НАН України (20 червня 2023 р. — онлайн, 24 червня 2025 р. — онлайн);
- Алгебраїчний семінар Інституту математики НАН України (керівник: чл.-кор. Ю. А. Дрозд, академік С. І. Максименко, Київ, Україна) (6 жовтня 2015 р., 18 грудня 2018 р., 26 червня 2024 р. — онлайн, 12.11.2025 р.);
- лабораторії топології Інституту математики НАН України (керівник: академік С. І. Максименко, Київ, Україна) (19 квітня 2023 р.);
- “Алгебра” Варшавського університету (керівник: проф. Ян Окнінський, Варшава, Польща) (21 квітня 2022 р., 9 березня 2023 р., 18 січня 2024 р.);

- “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.);
- Scientific Seminar “Geometry, Topology, Applications” (керівник: проф. Т. О. Банах, Львів, Україна) (9 березня 2026 р.);
- розширене засідання “Під кінець року” Алгебраїчного семінару Київського національного університету імені Тараса Шевченка (керівник: проф. А. П. Петравчук, Київ, Україна) (26 грудня 2017 р.);
- Семінар молодих вчених Інституту математики НАН України (організатор: Рада молодих вчених ІМ НАНУ, Київ, Україна) (22 вересня 2016 р.).

Публікації.

Результати дисертації висвітлено у 42 наукових публікаціях (див. список публікацій здобувача на с. 12–18), з них 15 — статті у наукових виданнях, внесених до переліку наукових фахових видань України та закордонних виданнях, а також 22 публікації у тезах доповідей і матеріалах міжнародних та вітчизняних конференцій. Статті [5, 1, 2, 6, 9, 10, 14, 12] проіндексовані у міжнародних наукометричних базах Scopus або Web of Science. Статтю [5] опубліковано у виданні з квартиля Q1 відповідно до класифікації SCImago Journal and Country Rank, статті [1, 2, 6, 9, 10, 14] у виданнях з квартиля Q3, статтю [12] у виданні з квартиля Q4. Відповідно до п. 2 Наказу № 1220 МОН України від 23.09.2019 вказані 15 статей зараховуються як 23 наукові публікації. Роботи [1, 2, 5–7, 9–16, 20] проіндексовано у базі Zentrablatt Math, а роботи [1, 5, 6, 9, 10, 12, 14, 15] проіндексовано у базі MathSciNet. Статті [4, 8, 11] одноосібні.

Структура й об'єм дисертації.

Дисертація складається з переліку умовних позначень, вступу, семи розділів, висновків, списку використаних джерел, що містить 130 найменувань та додатку зі списком публікацій і апробацією результатів. Повний обсяг роботи становить 325 сторінок друкованого тексту із них список використаних джерел міститься на 16 сторінках, а додаток — на 13 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 3 статті, а саме статті [14–16] зі списку публікацій.

Стипендія.

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

Гранти.

1. Проєкт “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 та завдання дослідження, наукову новизну одержаних результатів.

У розділі 1 наведено огляд літератури за темою дисертації.

В розділі 2 наведено основні означення та результати, що стосуються майже-кілець з одиницею та груп порядку p^3 . У підрозділах 2.1 та 2.2 наведено результати про групи порядку p^3 та майже-кілець з одиницею, відповідно, які буде використано в подальших дослідженнях.

Наступне твердження містить класифікацію груп порядку p^3 (див. [16]).

Твердження 2.1. *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 дієдра, $a^4 = 1, b^2 = 1, a^{-1}b = ba;$

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

Наведемо основні означення (див., наприклад, [72], [64], [32], [41], [122]).

Означення 2.4. Непорожня множина R з двома бінарними операціями “+” та “ $\cdot$ ” називається майже-кільцем, якщо:

1) $(R, +)$ — група з нейтральним елементом 0;

2) $(R, \cdot)$ — напівгрупа;

3) $x \cdot (y + z) = x \cdot y + x \cdot z$ для всіх $x, y, z \in R$.

Таке майже-кільце називається лівим майже-кільцем. Якщо ж аксіомі 3) замінити аксіомою $(x + y) \cdot z = x \cdot z + y \cdot z$ для всіх $x, y, z \in R$, то отримаємо праве майже-кільце.

Група $(R, +)$ позначається через R^+ та називається адитивною групою, а її нейтральний елемент 0 — нулем майже-кільця R .

Майже-кільце R , в якому напівгрупа $(R, \cdot)$ є моноїдом з одиничним елементом i , називається майже-кільцем з одиницею i .

Підрозділ 2.3 присвячено вивченню майже-кільць з одиницею на абелевих групах порядку p^3 . Отримані необхідні умови існування майже-кільць з одиницею на таких групах.

Нехай $G(p, p, p)$ — група зі співвідношеннями 3) з твердження 2.1.

Нехай R — майже-кільце з одиницею, адитивна група R^+ якого ізоморфна групі $G(p, p, p)$. Тоді $R^+ = \langle a \rangle + \langle b \rangle + \langle c \rangle$ для деяких $a, b, c \in R$, що задовольняють співвідношення $ap = bp = cp = 1$, $a + b = b + a$, $a + c = c + a$, $c + b = b + c$. Зокрема, кожний елемент $x \in R$ єдиним чином записується у вигляді $x = ax_1 + bx_2 + cx_3$ з коефіцієнтами $0 \leq x_1 < p$, $0 \leq x_2 < p$ та $0 \leq x_3 < p$.

Без втрати загальності, можна припустити, що a є одиницею в R , тобто $ax = xa = x$ для кожного $x \in R$. Більш того, для кожного $x \in R$ існують такі коефіцієнти $\alpha(x)$, $\beta(x)$, $\gamma(x)$, $\lambda(x)$, $\mu(x)$ та $\nu(x)$, що

$$xb = a\alpha(x) + b\beta(x) + c\gamma(x)$$

та

$$xc = a\lambda(x) + b\mu(x) + c\nu(x).$$

Зрозуміло, що вони єдиним чином визначені за модулем p , тому деякі відображення $\alpha : R \rightarrow Z_p$, $\beta : R \rightarrow Z_p$, $\gamma : R \rightarrow Z_p$, $\lambda : R \rightarrow Z_p$, $\mu : R \rightarrow Z_p$, $\nu : R \rightarrow Z_p$.

Теорема 2.7. *Якщо $x, y = ay_1 + by_2 + cy_3 \in R$, то*

$$\begin{aligned} xy = & a(x_1y_1 + \alpha(x)y_2 + \lambda(x)y_3) + b(x_2y_1 + \beta(x)y_2 + \mu(x)y_3) + \\ & + c(x_3y_1 + \gamma(x)y_2 + \nu(x)y_3), \end{aligned}$$

причому виконуються наступні твердження:

- (0) $\alpha(0) \equiv 0 \pmod{p}$, $\beta(0) \equiv 0 \pmod{p}$, $\gamma(0) \equiv 0 \pmod{p}$,
 $\lambda(0) \equiv 0 \pmod{p}$, $\mu(0) \equiv 0 \pmod{p}$ та $\nu(0) \equiv 0 \pmod{p}$ тоді і тільки тоді, коли майже-кільце R є нуль-симетричним;
- (1) $\alpha(a) = 0$, $\beta(a) = 1$, $\gamma(a) = 0$, $\lambda(a) = 0$, $\mu(a) = 0$, $\nu(a) = 1 \pmod{p}$;

$$(2) \alpha(xy) \equiv x_1\alpha(y) + \alpha(x)\beta(y) + \lambda(x)\gamma(y) \pmod{p};$$

$$(3) \beta(xy) \equiv x_2\alpha(y) + \beta(x)\beta(y) + \mu(x)\gamma(y) \pmod{p};$$

$$(4) \gamma(xy) \equiv x_3\alpha(y) + \gamma(x)\beta(y) + \nu(x)\gamma(y) \pmod{p};$$

$$(5) \lambda(xy) \equiv x_1\lambda(y) + \alpha(x)\mu(y) + \lambda(x)\nu(y) \pmod{p};$$

$$(6) \mu(xy) \equiv x_2\lambda(y) + \beta(x)\mu(y) + \mu(x)\nu(y) \pmod{p};$$

$$(7) \nu(xy) \equiv x_3\lambda(y) + \gamma(x)\mu(y) + \nu(x)\nu(y) \pmod{p}.$$

Підрозділ 2.3 присвячено вивченню майже-кілець з одиницею на абелевих групах порядку p^3 . Отримані необхідні умови існування майже-кілець з одиницею на таких групах.

Нехай $G(p, p, p)$ — група зі співвідношеннями 3) з леми 2.1.

Нехай R — майже-кілець з одиницею, адитивна група R^+ якого ізоморфна групі $G(p, p, p)$. Тоді $R^+ = \langle a \rangle + \langle b \rangle + \langle c \rangle$ для деяких $a, b, c \in R$, що задовольняють співвідношення $ap = bp = cp = 1$, $a + b = b + a$, $a + c = c + a$, $c + b = b + c$. Зокрема, кожний елемент $x \in R$ єдиним чином записується у вигляді $x = ax_1 + bx_2 + cx_3$ з коефіцієнтами $0 \leq x_1 < p$, $0 \leq x_2 < p$ та $0 \leq x_3 < p$.

Без втрати загальності, можна припустити, що a є одиницею в R , тобто $ax = xa = x$ для кожного $x \in R$. Більш того, для кожного $x \in R$ існують такі коефіцієнти $\alpha(x), \beta(x), \gamma(x), \lambda(x), \mu(x)$ та $\nu(x)$, що

$$xb = a\alpha(x) + b\beta(x) + c\gamma(x)$$

та

$$xc = a\lambda(x) + b\mu(x) + c\nu(x).$$

Зрозуміло, що вони єдиним чином визначені за модулем p , тому деякі відображення $\alpha : R \rightarrow Z_p$, $\beta : R \rightarrow Z_p$, $\gamma : R \rightarrow Z_p$, $\lambda : R \rightarrow Z_p$, $\mu : R \rightarrow Z_p$, $\nu : R \rightarrow Z_p$.

Теорема 2.7. *Якщо $x, y = ay_1 + by_2 + cy_3 \in R$, то*

$$xy = a(x_1y_1 + \alpha(x)y_2 + \lambda(x)y_3) + b(x_2y_1 + \beta(x)y_2 + \mu(x)y_3) + \\ + c(x_3y_1 + \gamma(x)y_2 + \nu(x)y_3),$$

причому виконуються наступні твердження:

- (0) $\alpha(0) \equiv 0 \pmod{p}$, $\beta(0) \equiv 0 \pmod{p}$, $\gamma(0) \equiv 0 \pmod{p}$,
 $\lambda(0) \equiv 0 \pmod{p}$, $\mu(0) \equiv 0 \pmod{p}$ та $\nu(0) \equiv 0 \pmod{p}$ тоді і
 тільки тоді, коли майже-кілець R є нуль-симетричним;
- (1) $\alpha(a) = 0$, $\beta(a) = 1$, $\gamma(a) = 0$, $\lambda(a) = 0$, $\mu(a) = 0$, $\nu(a) = 1$
 $\pmod{p}$;
- (2) $\alpha(xy) \equiv x_1\alpha(y) + \alpha(x)\beta(y) + \lambda(x)\gamma(y) \pmod{p}$;
- (3) $\beta(xy) \equiv x_2\alpha(y) + \beta(x)\beta(y) + \mu(x)\gamma(y) \pmod{p}$;
- (4) $\gamma(xy) \equiv x_3\alpha(y) + \gamma(x)\beta(y) + \nu(x)\gamma(y) \pmod{p}$;
- (5) $\lambda(xy) \equiv x_1\lambda(y) + \alpha(x)\mu(y) + \lambda(x)\nu(y) \pmod{p}$;
- (6) $\mu(xy) \equiv x_2\lambda(y) + \beta(x)\mu(y) + \mu(x)\nu(y) \pmod{p}$;
- (7) $\nu(xy) \equiv x_3\lambda(y) + \gamma(x)\mu(y) + \nu(x)\nu(y) \pmod{p}$.

Розділ 3 присвячено вивченню локальних майже-кілець порядку p^3 . У підрозділі 3.1 наведене означення локальних майже-кілець та їх основні властивості. Підрозділ 3.2 присвячено вивченню локальних майже-кілець на абелевих групах порядку p^3 . Цей розділ складається з одного підпункту 3.2.1, в якому побудовано приклади локальних майже-кілець з елементарною абелевою адитивною групою порядку p^3 . У підрозділі 3.3 вивчаються локальні майже-кілеця на неабелевих групах порядку p^3 . В трьох підпунктах 3.3.1, 3.3.2 та 3.3.3 цього розділу отримані необхідні та

достатні умови існування локальні майже-кільця, адитивні групи яких ізоморфні G_1 , G_2 та G_3 , відповідно.

Означення 3.1. *Майже-кільце R з одиницею називається локальним, якщо множина L всіх необоротних елементів із R утворює підгрупу адитивної групи R^+ . В цьому випадку L будемо називати підгрупою необоротних елементів майже-кільця R .*

Маємо наступну теорему.

Теорема 3.11. *Існує щонайменше p неізоморфних локальних майже-кільць на елементарній абелевій групі порядку p^3 .*

Позначимо через G_1 групу зі співвідношеннями 5*) твердження 2.1, G_2 групу зі співвідношеннями 4*) твердження 2.1, G_3 групу зі співвідношеннями 2) твердження 2.1.

Нехай R — локальне майже-кільце, адитивна група якого R^+ ізоморфна G_1 . Тоді $R^+ = \langle a \rangle + \langle b \rangle + \langle c \rangle$ для деяких елементів a , b і c з R , що задовольняють співвідношення $ap = 0$, $bp = 0$, $cp = 0$, $a + b = b + a + c$, $a + c = c + a$ і $b + c = c + b$. Зокрема, кожен елемент $x \in R$ однозначно записується у вигляді $x = ax_1 + bx_2 + cx_3$ з коефіцієнтами $0 \leq x_1 < p$, $0 \leq x_2 < p$ і $0 \leq x_3 < p$.

Оскільки порядок елемента a дорівнює експоненті групи G , то за лемою 2.2 можна вважати, 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 $\alpha(x)$, $\beta(x)$ і $\gamma(x)$, що

$$xb = a\alpha(x) + b\beta(x) + c\gamma(x).$$

Зрозуміло, що вони так однозначно визначені за модулем p , що визначені деякі відображення $\alpha : R \rightarrow \mathbb{Z}_p$, $\beta : R \rightarrow \mathbb{Z}_p$ і $\gamma : R \rightarrow \mathbb{Z}_p$.

Отже, маємо приклади $p+1$ майже-кільцевих добутків і формулюємо наступний результат.

Теорема 3.15. *На кожній неметациклічній неабелевій групі поряд-*

ку p^3 існує щонайменше $p + 1$ неізоморфних локальних майже-кілець.

На всіх абелевих групах існують локальні майже-кільця. Також, згідно з [12] і [54], існують локальні майже-кільця на G_1 і G_2 , відповідно. Отже, маємо наступний результат.

Твердження 3.17. *На кожній групі порядку p^3 з $p > 2$ існує локальне майже-кільце.*

Нехай R — локальне майже-кільце, яке не є майже-полем, адитивна група якого R^+ ізоморфна G_3 . Тоді $R^+ = \langle a \rangle + \langle b \rangle$ для деяких елементів a і b з R , що задовольняють відношення $ap^2 = 0$, $bp = 0$ та $b + a = a + b$.

Отже, формулюємо наступний результат.

Теорема 3.21. *На кожній метациклічній абелевій групі порядку p^3 існує щонайменше $p + 1$ неізоморфних локальних майже-кілець.*

Розділ 4 складається з трьох підрозділів 4.1, 4.2 та 4.3. В цьому розділі вивчаються майже-кільця з одиницею порядків p^4 . У підрозділі 4.1 наведено класифікацію груп порядку p^4 . Підрозділах 4.2 та 4.3 отримано необхідні умови існування майже-кілець з одиницею на групах класу нільпотентності 2 та класу нільпотентності 3, відповідно.

Групи порядку p^4 з $p > 3$ описано в такій теоремі (див., наприклад, [20], [28]).

Теорема 4.1. *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:

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

Розглянемо групи класу нільпотентності 2 порядку p^4 .

Нехай G_4 — адитивно записана група з теореми 4.1. Тоді $G_4 = \langle a \rangle + \langle b \rangle + \langle c \rangle + \langle d \rangle$ для деяких елементів a, b, c і d з R , що задовольняють співвідношення $ap = 0, bp = 0, cp = 0, dp = 0, a+b = b+a+c, a+c = c+a, b+c = c+b, a+d = d+a, b+d = d+b$ і $c+d = d+c$.

Нехай R — майже-кільце з одиницею адитивна група R^+ якого ізоморфна групі G_4 . Тоді

$$R^+ = \langle a \rangle + \langle b \rangle + \langle c \rangle + \langle d \rangle$$

для деяких елементів a, b, c і d з R задовольняють співвідношення $ap = 0, bp = 0, cp = 0, dp = 0, a+b = b+a+c, a+c = c+a, b+c = c+b, a+d = d+a, b+d = d+b$ і $c+d = d+c$. Зокрема, кожен елемент

$x \in R$ єдиним чином записаний у вигляді $x = ax_1 + bx_2 + cx_3 + dx_4$ з коефіцієнтами $0 \leq x_1 < p$, $0 \leq x_2 < p$, $0 \leq x_3 < p$ і $0 \leq x_4 < p$.

Оскільки порядок елемента a рівний експоненті групи G , то за лемою 2.2 можна 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 $\alpha(x)$, $\beta(x)$, $\gamma(x)$, $\varphi(x)$, $\lambda(x)$, $\mu(x)$, $\nu(x)$ і $\psi(x)$, що

$$xb = a\alpha(x) + b\beta(x) + c\gamma(x) + d\varphi(x)$$

і

$$xd = a\lambda(x) + b\mu(x) + c\nu(x) + d\psi(x).$$

Зрозуміло, що вони однозначно визначені так по модулю p , що визначені деякі відображення $\alpha: R \rightarrow \mathbb{Z}_p$, $\beta: R \rightarrow \mathbb{Z}_p$, $\gamma: R \rightarrow \mathbb{Z}_p$, $\varphi: R \rightarrow \mathbb{Z}_p$, $\lambda: R \rightarrow \mathbb{Z}_p$, $\mu: R \rightarrow \mathbb{Z}_p$, $\nu: R \rightarrow \mathbb{Z}_p$ і $\psi: R \rightarrow \mathbb{Z}_p$.

Лема 4.5. *Нехай R — майже-кільце з одиницею адитивна група R^+ якого ізоморфна групі G_4 . Якщо a співпадає з одиничним елементом в R , $x = ax_1 + bx_2 + cx_3 + dx_4$, $y = ay_1 + by_2 + cy_3 + dy_4 \in R$,*

$$xb = a\alpha(x) + b\beta(x) + c\gamma(x) + d\varphi(x)$$

і

$$xd = a\lambda(x) + b\mu(x) + c\nu(x) + d\psi(x),$$

то

$$\begin{aligned} xy = & a(x_1y_1 + \alpha(x)y_2 + \lambda(x)y_4) + b(x_2y_1 + \beta(x)y_2 + \mu(x)y_4) + \\ & + c(-x_1x_2 \binom{y_1}{2} - \alpha(x)\beta(x) \binom{y_2}{2} - x_2\alpha(x)y_1y_2 - \lambda(x)\mu(x) \binom{y_4}{2} - \\ & - x_2\alpha(x)y_3 + x_3y_1 + \gamma(x)y_2 + x_1\beta(x)y_3 + \nu(x)y_4) + d(x_4y_1 + \\ & + \varphi(x)y_2 + \psi(x)y_4). \end{aligned}$$

Більш того, для відображень

$\alpha: R \rightarrow \mathbb{Z}_p$, $\beta: R \rightarrow \mathbb{Z}_p$, $\gamma: R \rightarrow \mathbb{Z}_p$, $\varphi: R \rightarrow \mathbb{Z}_p$, $\lambda: R \rightarrow \mathbb{Z}_p$, $\mu: R \rightarrow \mathbb{Z}_p$, $\nu: R \rightarrow \mathbb{Z}_p$ і $\psi: R \rightarrow \mathbb{Z}_p$ виконуються наступні твердження:

$$(0) \quad \alpha(0) \equiv 0 \pmod{p}, \beta(0) \equiv 0 \pmod{p}, \gamma(0) \equiv 0 \pmod{p};$$

$$\varphi(0) \equiv 0 \pmod{p}, \lambda(0) \equiv 0 \pmod{p}, \mu(0) \equiv 0 \pmod{p},$$

$\nu(0) \equiv 0 \pmod{p}$ і $\psi(0) \equiv 0 \pmod{p}$ тоді й лише тоді, коли майже-кільце R є нуль-симетричним;

$$(1) \quad \alpha(xy) \equiv x_1\alpha(y) + \alpha(x)\beta(y) + \lambda(x)\varphi(y) \pmod{p};$$

$$(2) \quad \beta(xy) \equiv x_2\alpha(y) + \beta(x)\beta(y) + \mu(x)\varphi(y) \pmod{p};$$

$$(3) \quad \gamma(xy) \equiv -x_1x_2\binom{\alpha(y)}{2} - \alpha(x)\beta(x)\binom{\beta(y)}{2} - x_2\alpha(x)\alpha(y)\beta(y) - \\ - \lambda(x)\mu(x)\binom{\varphi(y)}{2} - x_2\alpha(x)\gamma(y) + x_3\alpha(y) + \gamma(x)\beta(y) + \\ + x_1\beta(x)\gamma(y) + \nu(x)\varphi(y) \pmod{p};$$

$$(4) \quad \varphi(xy) \equiv x_4\alpha(y) + \varphi(x)\beta(y) + \psi(x)\varphi(y) \pmod{p};$$

$$(5) \quad \lambda(xy) \equiv x_1\lambda(y) + \alpha(x)\mu(y) + \lambda(x)\psi(y) \pmod{p};$$

$$(6) \quad \mu(xy) \equiv x_2\lambda(y) + \beta(x)\mu(y) + \mu(x)\psi(y) \pmod{p};$$

$$(7) \quad \nu(xy) \equiv -x_1x_2\binom{\lambda(y)}{2} - \alpha(x)\beta(x)\binom{\mu(y)}{2} - x_2\alpha(x)\lambda(y)\mu(y) - \\ - \lambda(x)\mu(x)\binom{\psi(y)}{2} - x_2\alpha(x)\nu(y) + x_3\lambda(y) + \gamma(x)\mu(y) + \\ + x_1\beta(x)\nu(y) + \nu(x)\psi(y) \pmod{p};$$

$$(8) \quad \psi(xy) \equiv x_4\lambda(y) + \varphi(x)\mu(y) + \psi(x)\psi(y) \pmod{p}.$$

Ми розглянемо групи класу нільпотентності 3 порядку p^4 .

Нехай H_1 — адитивно записана група з теореми 4.1. Тоді $H_1 = \langle a \rangle + \langle b \rangle + \langle c \rangle + \langle d \rangle$ для деяких елементів a, b, c і d з R задовольня-

ють співвідношення $ap = bp = cp = dp = 0$, $b + c = c + b$, $a + d = d + a$, $b + d = d + b$, де $c = -a - b + a + b$ і $d = -a - c + a + c$.

Нехай R — майже-кільце з одиницею, адитивна група якого R^+ ізоморфна H_1 . Тоді $R^+ = \langle a \rangle + \langle b \rangle + \langle c \rangle + \langle d \rangle$ для деяких елементів a , b , c і d of R задовольняють співвідношення $ap = bp = cp = dp = 0$, $b + c = c + b$, $a + d = d + a$, $b + d = d + b$, де $c = -a - b + a + b$ і $d = -a - c + a + c$. Зокрема, кожен елемент $x \in R$ однозначно записується у формі $x = ax_1 + bx_2 + cx_3 + dx_4$ з коефіцієнтами $0 \leq x_1 < p$, $0 \leq x_2 < p$, $0 \leq x_3 < p$ і $0 \leq x_4 < p$.

Оскільки порядок елемента a дорівнює експоненті групи G , тобто p , з цього випливає, що ми можемо 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 $\alpha(x)$, $\beta(x)$, $\gamma(x)$, $\phi(x)$, що

$$xb = a\alpha(x) + b\beta(x) + c\gamma(x) + d\phi(x).$$

Зрозуміло, що вони однозначно визначені за модулем p , тому визначені деякі відображення $\alpha: R \rightarrow \mathbb{Z}_p$, $\beta: R \rightarrow \mathbb{Z}_p$, $\gamma: R \rightarrow \mathbb{Z}_p$, $\phi: R \rightarrow \mathbb{Z}_p$.

Лема 4.17. *Нехай R — майже-кільце з одиницею, адитивна група якого R^+ ізоморфна H_1 . Якщо a збігається з одиничним елементом R , $x = ax_1 + bx_2 + cx_3 + dx_4$, $y = ay_1 + by_2 + cy_3 + dy_4 \in R$,*

$$xb = a\alpha(x) + b\beta(x) + c\gamma(x) + d\phi(x),$$

тоді

$$\begin{aligned} xy = & a(x_1y_1 + \alpha(x)y_2) + b(x_2y_1 + \beta(x)y_2) + c(x_3y_1 - x_1x_2 \binom{y_1}{2}) - \\ & - x_2\alpha(x)y_1y_2 + \gamma(x)y_2) - \alpha(x)\beta(x) \binom{y_2}{2} + x_1\beta(x)y_3 - \\ & - x_2\alpha(x)y_3) + d(x_4y_1 + x_2 \binom{x_1}{2} \binom{y_1}{2} - x_1x_3 \binom{y_1}{2}) + \end{aligned}$$

$$\begin{aligned}
& +x_1^2x_2\binom{y_1}{y_1-3} + x_2y_1\binom{\alpha(x)y_2}{2} - \alpha(x)x_3y_1y_2+ \\
& +x_1x_2\alpha(x)\binom{y_1}{2}y_2 + \phi(x)y_2 + \beta(x)\binom{\alpha(x)}{2}\binom{y_2}{2}- \\
& -\alpha(x)\gamma(x)\binom{y_2}{2} + \alpha(x)^2\beta(x)\binom{y_2}{y_2-3} + x_1\gamma(x)y_3- \\
& -\beta(x)\binom{x_1}{2}y_3 + x_2\binom{\alpha(x)}{2}y_3 - x_3\alpha(x)y_3 + x_1^2\beta(x)y_4- \\
& -x_1x_2\alpha(x)y_4).
\end{aligned}$$

Крім того, для відображень

$\alpha: R \rightarrow \mathbb{Z}_p$, $\beta: R \rightarrow \mathbb{Z}_p$, $\gamma: R \rightarrow \mathbb{Z}_p$, $\phi: R \rightarrow \mathbb{Z}_p$ справедливі наступні твердження:

$$(0) \quad \alpha(0) \equiv 0 \pmod{p}, \beta(0) \equiv 0 \pmod{p}, \gamma(0) \equiv 0 \pmod{p};$$

та $\phi(0) \equiv 0 \pmod{p}$ тоді і тільки тоді, коли майже-кілець R є нуль-симетричним;

$$(1) \quad xc = c(x_1\beta(x) - x_2\alpha(x)) + d(x_1\gamma(x) - \beta(x)\binom{x_1}{2} + x_2\binom{\alpha(x)}{2} - x_3\alpha(x));$$

$$(2) \quad xd = d(x_1^2\beta(x) - x_1x_2\alpha(x));$$

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

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

$$(5) \quad \gamma(xy) \equiv x_3\alpha(y) - x_1x_2\binom{\alpha(y)}{2} - x_2\alpha(x)\alpha(y)\beta(y) + \gamma(x)\beta(y) -$$

$$- \alpha(x)\beta(x)\binom{\beta(y)}{2} + x_1\beta(x)\gamma(y) - x_2\alpha(x)\gamma(y) \pmod{p};$$

$$(6) \quad \phi(xy) \equiv x_4\alpha(y) + x_2\binom{x_1}{2}\binom{\alpha(y)}{2} - x_1x_3\binom{\alpha(y)}{2} + x_1^2x_2\binom{\alpha(y)}{\alpha(y)-3} +$$

$$+ x_2\alpha(y)\binom{\alpha(x)\beta(y)}{2} - \alpha(x)x_3\alpha(y)\beta(y) + x_1x_2\alpha(x)\binom{\alpha(y)}{2}y_2 +$$

$$\begin{aligned}
& + \phi(x)\beta(y) + \beta(x)\binom{\alpha(x)}{2}\binom{\beta(y)}{2} - \alpha(x)\gamma(x)\binom{\beta(y)}{2} + \\
& + \alpha(x)^2\beta(x)\binom{\beta(y)}{\beta(y)-3} + x_1\gamma(x)\gamma(y) - \beta(x)\binom{x_1}{2}\gamma(y) + \\
& + x_2\binom{\alpha(x)}{2}\gamma(y) - x_3\alpha(x)\gamma(y) + x_1^2\beta(x)\phi(y) - x_1x_2\alpha(x)\phi(y) \pmod{p}.
\end{aligned}$$

У розділі 5 описано локальні майже-кільця порядку p^4 . Підрозділ 5.1 присвячено дослідженню локальних майже-кільця на групах порядку p^4 та класу нільпотентності 2. А саме, показано, що для непарних p із 6 таких груп 4 є адитивними групами локальних майже-кільць. Деякі приклади таких майже-кільць явно побудовані. У підрозділі 5.2 досліджуються групи класу нільпотентності 3 порядку p^4 , які є адитивними групами локальних майже-кільць. В трьох підрозділах 5.2.1, 5.2.2 та 5.2.3 цього розділу отримані необхідні та достатні умови існування локальних майже-кільць, адитивні групи яких ізоморфні H_1 та H_2 . У підрозділі 5.2.4 сформульовано гіпотезу щодо груп H_3 та H_4 .

Групи G_1 , G_2 та G_3 з теореми 4.1 є групами Міллера–Морено.

Згідно з [102] G_2 та G_3 є групами $G(p^2, p^2)$ і $G(p^3, p)$, відповідно (див., наприклад, лема 2 [102]). Тому, за теоремою 2 [102] існує локальне майже-кільце R , адитивна група R^+ якого ізоморфна групі G_3 . Як наслідок, на адитивній групі не існує локального майже-кільця G_2 .

Нехай R — локальне майже-кільце, адитивна група R^+ якого ізоморфна групі G_3 . Тоді $R^+ = \langle a \rangle + \langle b \rangle$ для деяких елементів a і b з R задовольняючи співвідношення $ap^3 = 0$, $bp = 0$ і $-b + a + b = a(1 - p^2)$. Зокрема, кожен елемент $x \in R$ однозначно записується у вигляді $x = ax_1 + bx_2$ з коефіцієнтами $0 \leq x_1 < p^3$ і $0 \leq x_2 < p$.

Формула для множення елементів локальних майже-кільць на метациклічних групах Міллера–Морено визначена в [102]. Формула множен-

ня довільних елементів нуль-симетричного локального майже-кільця на G_3 наведена в доведенні [102, Theorem 2], а саме:

$$x \cdot y = a(x_1y_1 + p^2x_1x_2\binom{y_1}{2}) + b(x_2y_1 + \beta(x)y_2),$$

де

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

Аналогічно, G_1 — це група $G(p^2, p, p)$ згідно з [12]. Отже, за теоремою 3 [12] існує локальне майже-кільце, адитивна група якого ізоморфна G_1 . Оскільки G_1 є неметациклічною групою Міллера–Морено, використовуючи [12, Theorem 3], для довільних елементів $x = ax_1 + bx_2 + cx_3$ і $y = ay_1 + by_2 + cy_3$ з G_1 отримуємо наступну формулу множення:

$$\begin{aligned} x \cdot y = & a(x_1y_1 + p^kx_2y_2) + b(x_2y_1 + x_1y_2) + \\ & + c(-x_1x_2\binom{y_1}{2} + x_3y_1 + x_1^2y_3), \end{aligned}$$

де $k = 1, 2$.

Легко побачити, що $R = (G_1, +, \cdot)$ є ненуль-симетричним локальним майже-кільцем.

Нехай R — локальне майже-кільце, адитивна група якого R^+ ізоморфна G_4 . Тоді $R^+ = \langle a \rangle + \langle b \rangle + \langle c \rangle + \langle d \rangle$ для деяких елементів a, b, c та d з R , що задовольняють співвідношення $ap = 0, bp = 0, cp = 0, dp = 0$, $a + b = b + a + c, a + c = c + a, b + c = c + b, d + c = c + d, a + d = d + a$ і $b + d = d + b$.

Маємо наступний результат.

Теорема 5.6. *Для кожного непарного простого числа p існує локальне майже-кільце R , адитивна група якого R^+ ізоморфна G_4 .*

Нехай G_6 — адитивно записана група з теореми 4.1. Тоді $G_6 = \langle a \rangle + \langle b \rangle + \langle c \rangle$ для деяких елементів a, b та c з R , що задовольняють

співвідношення $ap^2 = 0$, $bp = 0$, $cp = 0$, $a + b = b + a$, $a + c = c + a$, $c + b = b + c + ap$.

Лема 5.12. G_6 не є ендоциклічною.

Гіпотеза 5.13. Не існує локального майже-кілля, адитивна група якого ізоморфна G_6 .

Нехай R — локальне майже-кілля, адитивна група якого R^+ ізоморфна H_1 . Тоді $R^+ = \langle a \rangle + \langle b \rangle + \langle c \rangle + \langle d \rangle$ для деяких елементів a, b, c і d з R задовольняючи співвідношення $ap = bp = cp = dp = 0$, $b + c = c + b$, $a + d = d + a$, $b + d = d + b$, де $c = -a - b + a + b$ і $d = -a - c + a + c$.

Маємо наступний результат.

Теорема 5.17. Для кожного простого числа $p > 3$ існує локальне майже-кілля R , адитивна група якого R^+ ізоморфна H_1 .

Проаналізувавши групи H_3 та H_4 порядку 625 за допомогою GAP, з'ясували, що не існує локальних майже-кілля на цих групах. Це дозволяє зробити наступне припущення.

Гіпотеза 5.23. Не існує локального майже-кілля, адитивна група якого ізоморфна H_3 чи H_4 .

У розділі 6 вивчаються майже-кілля з одиницею на деяких неабелевих групах. У підрозділі 6.1 дано означення та опис груп Міллера–Морено та груп Шмідт. У підрозділі 6.2 описано всі можливі типи груп Міллера–Морено, які є адитивними групами майже-кілля з одиницею. У підрозділі 6.3 показано, що не існує майже-кілля з одиницею, адитивна група яких ізоморфна групі Шмідта. Підрозділ 6.4 складається з трьох підпунктів 6.4.1, 6.4.2 та 6.4.3. У цьому підрозділі досліджуються прямі добутки метациклічних p -груп Міллера–Морено та циклічних p -груп як адитивні групи майже-кілля з одиницею та локальних майже-кілля. Більш того, визначено формули множення для таких майже-кілля та описано функції, що їх задають. У підрозділі 6.5 вивчаються прямі добутки неметациклічних p -груп Міллера–Морено та циклічних p -груп як

адитивні групи майже-кілець з одиницею та локальних майже-кілець. Цей підрозділ складається з трьох підпунктів 6.5.1, 6.5.2 та 6.5.3. В першому підпункті 6.5.1 наведено попередні результати. В підпункті 6.5.2 досліджуються майже-кілець з одиницею на групах $F(p^m, p^n, p, p^k)$. В підпункті 6.5.3 визначено формули множення для локальних майже-кілець на групах $F(p^m, p^n, p, p^k)$ та описано функції, що їх задають.

Нагадаємо, що групою Шмідта або мінімальною ненільпотентною називається скінченна ненільпотентна група, будь-яка власна підгрупа якої нільпотентна.

Маємо наступне твердження.

Теорема 6.12. *Не існує майже-кілець з одиницею, адитивна група яких ізоморфна групі Шмідта.*

Нехай R — локальне майже-кілець, адитивна група якого R^+ ізоморфна $F(p^m, p^n, p^k)$. Тоді $R^+ = \langle a \rangle + \langle b \rangle + \langle c \rangle$ з елементами a , b та c , де a співпадає з одиничним елементом R та виконуються співвідношення $a^{p^m} = b^{p^n} = c^{p^k} = 1$, $b^{-1}ab = a^{1+p^{m-1}}$, $ca = ac$ та $cb = bc$, де $m \geq 2$, $n \geq 1$ та $k \geq 1$.

Теорема 6.18. *Для кожного непарного простого числа p , $m \geq n$ та $m \geq k$ існує локальне майже-кілець R , адитивна група якого R^+ ізоморфна $F(p^m, p^n, p^k)$.*

Розділ 7 присвячено застосуванню системи GAP для дослідження та класифікації локальних майже-кілець. В перших двох підрозділах 7.1 та 7.2 вивчається побудова та класифікація майже-кілець з одиницею. В підрозділі 7.3 описано деякі функції з пакету LocalNR, а саме, UnitsOfNearRing 7.3.1, IsLocalNearRing 7.3.2, IsLocalRing 7.3.3, NearRingNonUnits 7.3.4 та NonUnitsAsAdditiveSubgroup 7.3.5. В підрозділі 7.4 досліджено майже-кілець з одиницею і локальні майже-кілець, та ендоециклічні групи. Підрозділ 7.5 присвячено класифікації локальних майже-кілець малих порядків, а саме, локальних майже-кілець порядку

32 7.5.1 та 128 7.5.2 та 7.5.3.

Алгоритм побудови майже-кілець з одиницею базується на наступній теоремі.

Теорема 7.1. *Нехай G — група, і нехай множина $\text{End } G$ усіх ендоморфізмів G розглядається як моноїд щодо композиції ендоморфізмів. Тоді G — адитивна група майже-кілля з одиницею тоді і тільки тоді, коли існують елемент $g \in G$ та підмоноїд F з $\text{End } G$ такі, що $G = g^F$ та $g^\phi = g^\psi$ лише тоді, коли $\phi = \psi$ для будь-яких $\phi, \psi \in F$.*

Пакет LocalNR містить бібліотеку локальних майже-кілець до порядку 361 та деякі функції для аналізу скінченних майже-кілець. Поточна версія цього пакету — 1.0.4, випущена 15.03.2024.

Розділ 1

Огляд літератури та попередні відомості

1.1. Скінченні майже-кілець з одиницею

Майже-кілець виникають природним чином при вивченні систем нелінійних відображень і вивчаються протягом багатьох десятиліть. Основні визначення та багато результатів стосовно майже-кілець можна знайти, наприклад, у книзі Пільца [72].

Майже-кілець — це узагальнення кілець в тому сенсі, що додавання не обов'язково є комутативним і передбачається лише один дистрибутивний закон. Очевидно, що кожне асоціативне кільце є майже-кілцем, і кожна група є адитивною групою майже-кілець, але не обов'язково майже-кілець з одиницею. Питання про те, яка група може бути адитивною групою майже-кілець з одиницею, далеко від вирішення.

Клей [30] ввів механізм, необхідний і достатній для побудови всіх майже-кілець, адитивна група яких є скінченною та циклічною.

Теорема 1.1 (Theorem 1, [30]). *Нехай $*$ — бінарна операція на Z_n . Операція $*$ є лівою дистрибутивною над $+$ тоді і тільки тоді, коли існує функція π така, що для всіх $p, q \in Z_n$, $p * q = \pi(p) \cdot q$.*

Мексон [59] довів, що якщо таке майже-кілець має мультиплікативну одиницю, то це майже-кілець є кільцем.

Твердження 1.2 (Proposition 1, [59]). *Якщо $(N, +, *)$ є майже-кільцем з одиницею і та $(N, +) \cong (Z_n, +)$ для деякого додатного цілого числа n , $n \geq 2$, то $(N, +, *)$ є кільцем.*

Також показав, що якщо потужність множини N є добутком різних простих чисел, то майже-кільце з одиницею є кільцем.

Твердження 1.3 (Proposition 3, [59]). *Якщо $(N, +, *)$ є майже-кільцем з одиницею і та $|N| = \prod_{k=1}^m P_k$, де P_k є простим числом і $P_k \neq P_l$ якщо $k \neq l$, то N є кільцем.*

Прикладом майже-кільця є множина $M(G)$ всіх відображень довільної групи G в себе, якщо операцію додавання відображень визначити як по-елементну операцію їх образів в групі G , тобто $g^{\alpha+\beta} = g^\alpha g^\beta$ для всіх $g \in G$ та $\alpha, \beta \in M(G)$, а операцію множення відображень як їх композицію, тобто $g^{\alpha \cdot \beta} = (g^\alpha)^\beta$. Зауважимо, що навіть якщо G є абелевою групою, то при такому визначенні операцій в $M(G)$ правий дистрибутивний закон не виконується.

Якщо операція в групі G записується адитивно з нейтральним елементом 0 , то легко бачити, що наступні підмножини із $M(G)$ також є майже-кільцями відносно вказаних вище операцій:

- множина $M_0(G) = \{\alpha : G \rightarrow G \mid 0^\alpha = 0\}$ всіх відображень, що переводять 0 в 0 ;
- множина $M_c(G) = \{\alpha : G \rightarrow G \mid g^\alpha = 0^\alpha, g \in G\}$ всіх відображень, значення яких для будь-якого елемента групи G є сталим.

Майже-кільця першого виду називаються нуль-симетричними, а другого — константними.

Відомо, що будь-яка скінченна абелева група A є прямою сумою примарних циклічних підгруп, кожену з яких можна розглядати як адитивну групу деякого кільця лишків $\mathbb{Z}/p^i\mathbb{Z}$. Звідси A є адитивною групою

прямої суми цих кілець. Отже, кожна скінченна абелева група є адитивною групою асоціативного (і навіть комутативного) кільця з одиницею. Однак, у випадку майже-кілець з одиницею аналогічний результат для скінченних неабелевих груп не виконується.

Питання про те, які групи можуть бути адитивними групами майже-кілець з одиницею, досліджується з кінця 1960-х років. Один з перших результатів в цьому напрямку був отриманий Клейом і Малон [34], які показали, що з точністю до ізоморфізму існує єдине майже-кілець з одиницею, адитивна група якого циклічна, і яке фактично є комутативним кільцем.

Теорема 1.4 (Theorem 1, [34]). *Нехай $(G, +)$ — циклічна група. Якщо $(G, +, *)$ є майже-кілцем з одиницею, то $(G, +, *)$ є комутативний кілцем з одиницею.*

Наслідок 1.5 (Corollary, [34]). *Нехай $(G, +)$ — циклічна група. Існує, з точністю до ізоморфізму, єдине майже-кілець (кілець) з одиницею, адитивна група якого є $(G, +)$.*

Також було встановлено, що адитивна група скінченного майже-кіля з одиницею є простою тоді і тільки тоді, коли це майже-кілець є полем простого порядку.

Теорема 1.6 (Theorem 2, [34]). *Нехай $(G, +)$ — проста (нетривіальна) група скінченного порядку. Якщо $(G, +, *)$ є майже-кілцем з одиницею, то $(G, +, *)$ є полем.*

Більш того, доведено, що кожна нециклічна група, порядок якої є добутком різних простих чисел, та симетрична група S_n при $n \geq 3$ не можуть бути адитивними групами майже-кілець з одиницею.

Наслідок 1.7 (Corollary, [34]). *Проста група складеного порядку не може бути адитивною групою майже-кіля з одиницею.*

Теорема 1.8 (Theorem 4, [34]). *Нехай $(S_n, +)$ — симетрична група на n символах. Не існує майже-кільця з одиницею адитивна група якого $(S_n, +)$ при $n \geq 3$.*

Результати статті [34] були узагальнені Лайом [55], де доведено, що скінченні неабелеві групи з точно однією власною нормальною підгрупою не можуть бути адитивними групами майже-кільця з одиницею.

Теорема 1.9 (Theorem 1, [55]). *Нехай $(G, +)$ — скінченна некомутативна група з рівно однією власною нормальною підгрупою. Тоді $(G, +)$ не може бути адитивною групою майже-кільця з одиницею i .*

Більш того, цим же автором було встановлено, що кожне майже-кільце з одиницею на неабелевій групі з точно однією власною нормальною підгрупою є комутативним кільцем порядку p^2 для деякого простого числа p . Клей та Дой [33] довели, що знакозмінна група A_4 також не може бути адитивною групою майже-кільця з одиницею.

Теорема 1.10 (Theorem A, [33]). *Для $n \geq 4$, знакозмінна група $(A_4, +)$ не може бути адитивною групою майже-кільця з одиницею.*

Наведені вище результати були узагальнені Кріммелом [53] та доведено, що кожна скінченна група непростого порядку, ґратка нормальних підгруп якої лінійно впорядкована, не може бути адитивною групою майже-кільця з одиницею.

Теорема 1.11 (Theorem, [53]). *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-кільця з одиницею.*

Клей [31] показав, що не існує майже-кільця з одиницею, адитивна група якого ізоморфна групі кватерніонів Q_8 та встановив, що існує сім неізоморфних класів майже-кільця з одиницею на групі дієдра D_4 порядку 8. Ці сім класів майже-кільця перелічені в таблиці 3 у статті [31]. Клей

і Мексон [35] довели, що узагальнені групи кватерніонів Q_{2^n} при $n > 3$ не можуть бути адитивними групами майже-кілець з одиницею. Групи діедра D_n порядку $2n$ як адитивні групи майже-кілець з одиницею були дослідженні Джонсоном [49] та встановлено, що для непарного n група D_n не може бути адитивною групою майже-кілець з одиницею, та доведено, що з точністю до ізоморфізму існує єдине таке майже-кілець на групі D_n при $n = 2p$, де p — просте число.

Теорема 1.12 (Theorem 5.4, [49]). *Існує, з точністю до ізоморфізму, єдине майже-кілець з мультиплікативною одиницею і на $(D_n, +)$, $n = 2q$.*

Лекстон, Локхарт [54] дослідили структуру майже-кілець на елементах класу $\mathfrak{K}$ з більш алгебраїчної точки зору і тим самим завершили та розширили програму Кріммела [52].

Клас $\mathfrak{K}$ складається з тих груп H зі скінченним представленням вигляду

$$H = \langle e, \mu: \mu t - ei, en, -\mu + e + \mu - ej \rangle, \quad (1.1)$$

де i, j — додатні цілі числа, $1 < j < n$, $0 \leq i < n$, а t — просте число.

У своїй дисертації Кріммел [52] розглянув групу H з представленням у вигляді (1.1) та обчислив $[H : W_1; \text{з одиницею } e]$, та $[H : N_1; \text{з одиницею } e]$ лише для певних випадків.

У [54] дослідження було зосереджено на майже-кілецях з одиницею на групах з представленням вигляду

$$H = \langle a, b \mid a^{p^{n-1}} = 1, b^p = 1, a^b = a^{1+p^{n-2}} \rangle, \quad p \text{ — просте число, } n \geq 3. \quad (1.2)$$

Наступна теорема містить кількість всіх майже-кілець з одиницею на групах H представлення (1.2).

Теорема 1.13 (Theorem 7.1, [54]). (i) *Якщо $p = 2$ і $n = 4$, то $n(H) = 32$.*

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

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

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

Бойкетт та Нибауер [29] класифікували всі майже-кілець з одиницею на групах порядку, що не перевищує 31, використовуючи систему комп'ютерної алгебри GAP [43]. Зокрема, визначили всі неабелеві групи вказаних порядків, які не можуть бути адитивними групами майже-кілець з одиницею.

Групи з широкими системами абелевих підгруп вивчалися багатьма авторами. Зокрема, мінімальні неабелеві групи, тобто такі неабелеві групи, у яких всі власні підгрупи абелеві, отримали назву груп Міллера–Морено, в честь авторів, які століття тому вперше розглянули скінченні групи з цією властивістю та довели їх розв'язність. Ці групи вперше вивчалися Міллером та Морено [67]. Детальна класифікація цих груп була отримана Редєї [118] лише всередині минулого століття. Будова таких груп добре відома і повністю описується наступною теоремою (див. [118, Chapter XII]).

Теорема 1.14. *Скінченні групи Міллера–Морено вичерпуються групами наступних типів:*

- 1) група кватерніонів Q_8 ;
- 2) група $G = \langle a \rangle \rtimes \langle b \rangle$ порядку p^{m+n} (p — просте число) з $|a| = p^m$, $|b| = p^n$, $b^{-1}ab = a^{1+p^{m-1}}$, де $m \geq 2$, $n \geq 1$;
- 3) група $G = (\langle a \rangle \times \langle c \rangle) \rtimes \langle b \rangle$ порядку p^{m+n+1} (p — просте число) з $|a| = p^m$, $|b| = p^n$, $|c| = p$, $b^{-1}ab = ac$, $b^{-1}cb = c$, де $m \geq n \geq 1$ та $m + n > 2$ при $p = 2$;

- 4) група $G = P \rtimes \langle b \rangle$ порядку $p^r q^s$ з елементарною абелевою підгрупою P порядку p^r , на якій елемент b індукує незвідний автоморфізм простого порядку q , причому $b^{q^s} = 1$ та $\langle b^q \rangle = Z(G)$, де p, q — різні прості та r, s — натуральні числа.

Нагадаємо, що група G називається *метациклічною*, якщо існує така циклічна нормальна підгрупа $\langle a \rangle$, що фактор-група $G/\langle a \rangle$ є циклічною.

В статті [102] для кожного простого числа p та натуральних чисел m, n з $m \geq 2$ позначимо через $G(p^m, p^n)$ напівпрямий добуток $\langle a \rangle \rtimes \langle b \rangle$ двох циклічних груп $\langle a \rangle$ та $\langle b \rangle$ порядків p^m і p^n відповідно, в якому $b^{-1}ab = a^{1+p^{m-1}}$. Як випливає з теореми 6.1, кожна метациклічна p -група Міллера-Морено ізоморфна або групі кватерніонів Q_8 , або групі $G(p^m, p^n)$.

Таким чином, якщо адитивна група R^+ деякого майже-кільця R з одиницею є метациклічною групою Міллера-Морено, то вона є p -групою. Крім того, як доведено в [31], група кватерніонів Q_8 також не може бути адитивною групою такого майже-кільця R . Звідси та з теореми 6.1 випливає, що група R^+ може бути ізоморфна лише групі $G(p^m, p^n)$ для підходящих простих p та натуральних чисел m та n .

В роботі [12] для кожного простого числа p та натуральних чисел m, n з $m \geq n \geq 1$ позначимо через $G(p^m, p^n, p)$ напівпрямий добуток $(\langle a \rangle \times \langle c \rangle) \rtimes \langle b \rangle$ з циклічними підгрупами $\langle a \rangle$, $\langle b \rangle$ та $\langle c \rangle$ порядків p^m , p^n та p , відповідно, в якому $b^{-1}ab = ac$ та $b^{-1}cb = c$. Як випливає з теореми 6.1, кожна неметациклічна p -група Міллера-Морено ізоморфна групі $G(p^m, p^n, p)$.

В моїй кандидатській дисертації [2] доведено наступну теорему.

Теорема 1.15. *Нехай R — майже-кільце з одиницею i , адитивна група R^+ якого є групою Міллера-Морено. Тоді R^+ є p -групою та виконується одне з наступних тверджень:*

- 1) група R^+ ізоморфна групі $G(p^m, p^n)$ з $m \geq n$ та і породжує в R^+ циклічну нормальну підгрупу порядку p^m ;
- 2) група R^+ ізоморфна групі $G(2^m, 2^n)$ з $m \leq n$ та і породжує циклічну підгрупу порядку 2^n , яка не є нормальною в R^+ ;
- 3) група R^+ ізоморфна групі $G(p^m, p^n, p)$ та і породжує в R^+ циклічну нормальну підгрупу порядку p^m .

Як безпосередній наслідок, з теореми 6.7 випливає наступний результат.

Наслідок 1.16. *Не існує майже-кілець з одиницею, адитивна група яких ізоморфна групі $G(p^m, p^n)$ з $p > 2$ та $2 \leq m < n$.*

У статті [110] отримано структурний опис напівдистрибутивних майже-кілець з одиницею.

Означення 1.17 ([110]). (Ліве) майже-кілець R називається напівдистрибутивним, якщо таким є множення справа відносно його додавання. Іншими словами, для будь-яких елементів $r, s, t \in R$ має місце рівність $(r + s + r)t = rt + st + rt$.

Очевидно, що кожне дистрибутивне майже-кілець є напівдистрибутивним, але не навпаки. Наприклад, майже-кілець $\text{Map}(G)$ всіх функцій на групі G порядку 2 є напівдистрибутивним, а не дистрибутивним.

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

Лема 1.18 (Lemma 4, [110]). *Адитивна група кожного напівдистрибутивного майже-кілеця R з одиницею є абелевою.*

Теорема 1.19 (Theorem 1, [110]). *Напівдистрибутивне майже-кілець R з одиницею є простим як майже-кілець тоді і тільки тоді, коли R є простим асоціативним кільцем.*

Також побудовано приклад напівдистрибутивного майже-кільця без одиниці на неабелевій адитивній групі.

Приклад 1.20 (Example, [110]). Нехай N — майже-кільце, адитивна група якого N^+ ізоморфна симетричній групі степеня 3. Тоді $N^+ = \langle a \rangle + \langle b \rangle$, де $a \cdot 3 = b \cdot 2 = 0$ та $b + a + b = a \cdot 2$. Зокрема, кожен елемент N^+ можна однозначно записати у вигляді $a \cdot m + b \cdot n$, де $0 \leq m \leq 2$ та $0 \leq n \leq 1$. Ми визначаємо множення $*$ на N^+ за 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 цю таблицю, легко побачити, що $(N, +, *)$ — це майже-кільце, яке є напівдистрибутивним та нуль-симетричним.

Монографії Пільца [72], Мелдрума [64], Клея [32], К. Ферреро та Г. Ферреро [41], Локхарта [56] присвячені загальній теорії майже-кілець.

1.2. Скінченні локальні майже-кільця

Майже-кільце R з одиницею називається локальним, якщо підгрупа усіх необоротних елементів із R утворює підгрупу адитивної групи R .

Очевидно, що кожне локальне кільце R є нуль-симетричним локальним майже-кільцем, підгрупа L якого співпадає з радикалом Джекобсона кільця R .

Нагадаємо, що якщо G — адитивна група, то множина всіх відображень групи G в себе відносно операцій додавання відображень та їх композиції утворює майже-кільце $M(G)$, нулем якого є відображення $0 : G \rightarrow \{0\}$, а одиницею — тотожне відображення ι на групі G .

Наступне твердження є прикладом локального майже-кільця найменшого порядку, що не є кільцем.

Твердження 1.21 ([5]). *Майже-кільце $M(G)$ тоді і тільки тоді є локальним, коли G — група порядку 2. В цьому випадку $M(G)$ — локальне майже-кільце порядку 4, яке не є нуль-симетричним, а отже, не є локальним кільцем.*

Дослідження локальних майже-кільць було ініційовано Мексоном [60], який визначив ряд їх основних властивостей і, зокрема, довів, що адитивна група нуль-симетричного локального майже-кільця є p -групою.

Наслідок 1.22 (Corollary 7.6, [60]). *Адитивна група скінченного локального кільця є p -групою.*

Локальні майже-кільця були досліджені в роботах Амберга, Губерта, Сисака [21], Городніка [45], Губерта [47], Мексона ([60], [61], [62], [63]), Раєвської І., Раєвської М. та Сисака ([103], [107], [110]), Фейгелстока [40] та інших.

Мексон [61] описав усі неізоморфні нуль-симетричні локальні майже-кільця з нециклічною адитивною групою порядку p^2 , які не є майже-полями.

Теорема 1.23 (Theorem 1.6, [61]). *Кожне локальне майже-кільце з потужністю p^2 визначає відображення $\rho : C(p) \rightarrow C(p)$, яке задовольняє*

$$(i) \quad \rho(x) = 0 \Leftrightarrow x = 0, x \in C(p), \quad (1.3)$$

$$(ii) \quad \rho \text{ є груповим ендоморфізмом в } (C(p) \rightarrow C(p), \cdot).$$

Навпаки, припустимо, що нам дано відображення $\rho: C(p) \rightarrow C(p)$, яке задовольняє умови 1.3 вищезазначеної теореми. Використовуючи ρ , визначаємо множення $*$ на $(N, +) \equiv (C(p) \times C(p), +)$ наступним чином [61]:

$$(x_1, x_2) * (y_1, y_2) = (x_1, x_2) \begin{pmatrix} y_1 & y_2 \\ 0 & \rho(y_1) \end{pmatrix} \quad (1.4)$$

Теорема 1.24 (Theorem 1.7, [61]). *Якщо $\rho: C(p) \rightarrow C(p)$ задовольняє умови 1.3 Теорему 1.23, то $N = (C(p) \times C(p), +, *)$ — локальне майже-кільце, де “+” — по-точкове додавання, а “*” задається як 1.4.*

Мексон [61] показав, що з точністю до ізоморфізму існує $p-1$ локальне майже-кільце 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 1.25 (Corollary 1.11, [61]). *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 [130] про майже-поля й роботою Клея та Малоне [34], ця стаття дає повний опис усіх нуль-симетричних локальних майже-кілець порядку p^2 .

Мексон у статті [62] також показав, що кожна нециклічна абелева p -група порядку $p^n > 4$ є адитивною групою нуль-симетричного локального майже-кілця, яке не є кільцем. Мексоном сформульовано проблему пошуку єдиного набору відображень, що визначають всі неізоморфні локальні майже-кільця на цих групах. Ця проблема й досі залишається відкритою, як і проблема визначення кількості неізоморфних локальних майже-кілець на даній групі.

Теорема 1.26 ([62]). *Для кожної скінченної нециклічної абелевої p -групи $(G, +)$ порядку $|G| > 4$ існує локальне майже-кільце $N \equiv (N, +, \cdot)$ з $(N, +) = (G, +)$ таке, що N не є кільцем.*

А в статті [63] ним же було показано, що група діедра D_4 не може бути адитивною групою локального майже-кілця, та побудовані приклади локальних майже-кілець на неабелевих групах порядку p^n та експоненти p^{n-1} для $n \geq 3$ при $p \neq 2$ та для $n \geq 4$ при $p = 2$.

Теорема 1.27 (Theorem, [63]). *Для кожного простого числа p та кожного додатного цілого числа n , де $n \geq 3$, якщо p непарне та $n \geq 4$, якщо $p = 2$, існує локальне майже-кілце N порядку p^n таке, що $(N, +)$ є неабелевою групою.*

Наступна лема (див. [21]), характеризує основні властивості довільних скінченних локальних майже-кілець.

Лема 1.28. *Нехай R — скінченне локальне майже-кілце з одиницею i та L — підгрупа в R^+ всіх необоротних елементів із R . Тоді R^+ — p -група для деякого простого p , експонента якої збігається з порядком елемента i в R^+ , та виконуються наступні твердження:*

- 1) L — ідеал та (R, R) -підгрупа в R ;
- 2) кожна власна R^* -інваріантна підгрупа із R^+ та кожний правий ідеал із R міститься в L ;
- 3) множина $i + L$ утворює нормальну силовську p -підгрупу мультиплікативної групи R^* .

Зазначимо, що залишається відкритим питання, які неабелеві p -групи можуть бути адитивними групами локальних майже-кілець.

Як було показано Файгелстоком [40], для кожного простого числа p та кожного цілого n з $n > p$ існує група G порядку p^n , яка не може бути адитивною групою локального майже-кілця.

Теорема 1.29 (Theorem 8, [40]). *Для кожного простого числа p та кожного цілого числа $n > p$ існує така група G порядку p^n , що G не є адитивною групою локального майже-кілця.*

Оскільки кожна скінченна абелева p -група є адитивною групою локального майже-кільця, то наступним кроком є характеристизація локальних майже-кілець на мінімальних неабелевих p -групах.

Раєвська І., Сисак [102] класифікували метациклічні p -групи Міллера–Морено, які виступають як адитивні групи скінченних локальних майже-кілець.

Отримано необхідні умови, при яких група $G(p^m, p^n)$ є адитивною групою деякого локального майже-кільця.

Теорема 1.30 (Theorem 1, [102]). *Нехай R — локальне майже-кільце, адитивна група R^+ якого ізоморфна групі $G(p^m, p^n)$. Тоді $R^+ = \langle a \rangle + \langle b \rangle$, один із елементів a, b є одиничним елементом в R та виконуються наступні твердження:*

$$1) ap^m = bp^n = 0 \text{ та } a + b = b + a(1 + p^{m-1});$$

$$2) \text{ якщо } a \text{ — одиничний елемент в } R, \text{ то } p^{m+n} > 8 \text{ з } m > n,$$

$$L = \langle a \cdot p \rangle + \langle b \rangle \quad \text{та} \quad R^* = \{ax_1 + bx_2 \mid x_1 \not\equiv 0 \pmod{p}\};$$

$$3) \text{ якщо } b \text{ — одиничний елемент в } R, \text{ то } p = 2 \text{ з } m \leq n,$$

$$L = \langle a \rangle + \langle b \cdot 2 \rangle \quad \text{та} \quad R^* = \{ax_1 + bx_2 \mid x_2 \equiv 1 \pmod{2}\}.$$

Раєвська І., Сисак [102] одержали наступні формули для добутку xy довільних елементів $x = ax_1 + bx_2$ та $y = ay_1 + by_2$ майже-кільця R з теореми 1.30.

Наслідок 1.31 (Corollary 2, [102]). *Якщо a — одиничний елемент в R та $xb = a\alpha(x) + b\beta(x)$, то*

$$xy = a(x_1y_1 + \alpha(x)y_2 - x_1x_2 \binom{y_1}{2} p^{m-1}) + b(x_2y_1 + \beta(x)y_2),$$

де відображення $\alpha : R \rightarrow \mathbb{Z}_{p^m}$ та $\beta : R \rightarrow \mathbb{Z}_{p^n}$ задовольняють умовам:

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

(1) $\alpha(a) \equiv 0 \pmod{p^m}$ та $\beta(a) \equiv 1 \pmod{p^n}$;

(2) $\alpha(x) \equiv 0 \pmod{p^{m-n}}$;

(3) $x_1(\beta(x) - 1) \equiv 0 \pmod{p}$;

(4) $\alpha(xy) \equiv x_1\alpha(y) + \alpha(x)\beta(y) - x_1x_2\binom{\alpha(y)}{2}p^{m-1} \pmod{p^m}$;

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

Наслідок 1.32 (Corollary 3, [102]). Якщо b — одиничний елемент в R та $xa = a\alpha(x) + b\beta(x)$, то

$$xy = a(\alpha(x)y_1 + x_1y_2 - x_1x_2\binom{y_2}{2}2^{m-1}) + b(\beta(x)y_1 + x_2y_2),$$

де відображення $\alpha : R \rightarrow \mathbb{Z}_{2^m}$ та $\beta : R \rightarrow \mathbb{Z}_{2^n}$ задовольняють умовам:

(0) $\alpha(0) \equiv 0 \pmod{2^m}$ та $\beta(0) \equiv 0 \pmod{2^n}$ тоді і тільки тоді, коли майже-кілець R є нуль-симетричним;

(1) $\alpha(b) \equiv 1 \pmod{2^m}$ та $\beta(b) \equiv 0 \pmod{2^n}$;

(2) $\beta(x) \equiv 0 \pmod{2^{n-m+1}}$;

(3) $\alpha(x) \equiv 0 \pmod{2}$ тоді і тільки тоді, коли $x_2 \equiv 0 \pmod{2}$;

(4) $\alpha(xy) \equiv \alpha(x)\alpha(y) + x_1\beta(y) - x_1x_2\binom{\beta(y)}{2}2^{m-1} \pmod{2^m}$;

(5) $\beta(xy) \equiv \beta(x)\alpha(y) + x_2\beta(y) \pmod{2^n}$.

Наступна теорема показує, що наведені в теоремі 1.30 необхідні умови існування скінченного локального майже-кілця з адитивною групою, ізоморфною групі $G(p^m, p^n)$, є і достатніми. Це завершує класифікацію всіх метациклічних груп Міллера–Морено, які є адитивними групами локальних майже-кілець.

Теорема 1.33 (Theorem 2, [102]). Для довільного простого числа p та натуральних чисел m, n таких, що або $p^{m+n} > 8$ та $m > n$ або $p = 2$ та $1 < m \leq n$, існує локальне майже-кільце R , адитивна група R^+ якого ізоморфна групі $G(p^m, p^n)$.

Раєвська І., Раєвська М., Сисак [12] довели, що довільна неметациклічна p -група Міллера–Морено порядку $p^n > 8$ є адитивною групою деякого локального майже-кільця, причому мультиплікативна група кожного такого майже-кільця має порядок $p^{n-1}(p-1)$. Також досліджено властивості адитивної підгрупи L необоротних елементів локального майже-кільця R з неметациклічною адитивною групою Міллера–Морено. Адитивна група R^+ майже-кільця R ізоморфна групі $G(p^m, p^n, p)$ для підходящих простого p та натуральних чисел m та n . Тому $R^+ = \langle a \rangle + \langle b \rangle + \langle c \rangle$ з елементом a , який співпадає з одиничним елементом майже-кільця R , та елементами b, c , що задовольняють співвідношенням $ap^m = bp^n = 0$, $-b + a + b = a + c$ та $-b + c + b = c$.

Теорема 1.34 (Теорема 2, [12]). Мають місце наступні твердження:

1. $L = \langle a \cdot p \rangle + \langle b \rangle + \langle c \rangle$ і, зокрема, L — підгрупа індексу p в R^+ ;
2. елемент $x = ax_1 + bx_2 + cx_3$ тоді і тільки тоді є оборотним в R , коли $x_1 \not\equiv 0 \pmod{p}$.

Більш того, отримано наступну формулу для добутку xy довільних елементів $x = ax_1 + bx_2 + cx_3$ та $y = ay_1 + by_2 + cy_3$ локального майже-кільця R .

Наслідок 1.35 (Наслідок 2, [12]). Якщо $x, y \in R$ та

$$xb = a\alpha(x) + b\beta(x) + c\gamma(x),$$

то

$$xy = a(x_1y_1 + \alpha(x)y_2) + b(x_2y_1 + \beta(x)y_2) +$$

$$+c(-x_1x_2\binom{y_1}{2}) + x_3y_1 + \gamma(x)y_2 + x_1\beta(x)y_3),$$

причому для відображень $\alpha : R \rightarrow \mathbb{Z}_{p^m}$, $\beta : R \rightarrow \mathbb{Z}_{p^n}$ та $\gamma : R \rightarrow \mathbb{Z}_p$ виконуються наступні твердження:

(0) $\alpha(0) \equiv 0 \pmod{p^m}$, $\beta(0) \equiv 0 \pmod{p^n}$ та $\gamma(0) \equiv 0 \pmod{p}$ 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) $\gamma(xy) \equiv \gamma(x)\beta(y) + x_1\beta(x)\gamma(y) - x_1x_2\binom{\alpha(y)}{2} \pmod{p}$.

Зокрема, якщо $\alpha(x) \equiv p^kx_2 \pmod{p^m}$, $\beta(x) \equiv x_1 \pmod{p^n}$ та $\gamma(x) \equiv 0 \pmod{p}$ з $m - n < k \leq m$, то отримуємо наступний результат.

Теорема 1.36 (Теорема 3, [12]). В адитивно записаній групі $G = G(p^m, p^n, p)$ операція “ $\cdot$ ”, задана як

$$x \cdot y = a(x_1y_1 + p^kx_2y_2) + b(x_2y_1 + x_1y_2) + \\ + c(-x_1x_2\binom{y_1}{2}) + x_3y_1 + x_1^2y_3)$$

є асоціативною та ліво-дистрибутивною по відношенню до операції “ $+$ ” групи G та визначає деяке нуль-симетричне локальне майже-кілець $(G, +, \cdot)$ з одиничним елементом a .

Для кожного простого p , метациклічна p -group 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 $\langle b \rangle$.

У статті [103] класифіковано розщеплювані метациклічні групи, які є адитивними групами скінченних локальних майже-кілець.

Наступна корисна характеристика неабелевих розщеплюваних метациклічних p -груп згідно Б. Кінг (див. [51], Theorem 3.2 та Proposition 4.10).

Твердження 1.37 (Proposition 1, [103]). *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 1.37 будемо позначати через $G(p^m, p^n, r)$ або $G(2^m, 2^n, -r)$, відповідно.

Теорема 1.38 (Theorem 1, [103]). *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:*

$$1) \ ap^m = bp^n = 0 \text{ та } a + b = b + a(1 + p^{m-r}) \text{ з}$$

$$1 \leq r < \min\{m, n+1\} \text{ та } r < m-1 \text{ для } p=2;$$

$$2) \text{ якщо } a \text{ є одиницею в } R, \text{ тоді } m \geq n+r \geq 2r, L = \langle ap \rangle + \langle b \rangle \text{ та } R^* = \{ax_1 + bx_2 \mid x_1 \not\equiv 0 \pmod{p}\};$$

$$3) \text{ якщо } b \text{ є одиницею в } R, \text{ тоді } p=2 < m \leq n, r=1, L = \langle a \rangle + \langle b2 \rangle \text{ та } R^* = \{ax_1 + bx_2 \mid x_2 \equiv 1 \pmod{2}\}.$$

Раєвська І., Раєвська М., Сисак [102] отримали 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 1.39 (Corollary 2, [103]). 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 1.40 (Corollary 3, [103]). 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) $\alpha(b) = 1$ та $\beta(b) = 0$;

(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) $\beta(xy) = \beta(x)\alpha(y) + x_2\beta(y)$.

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 1.38 та 1.42 це завершує нашу класифікацію всіх розщеплюваних метациклічних груп, які є адитивними групами локальних майже-кілець.

Теорема 1.41 (Theorem 4, [103]). *Якщо m, n і r є такими цілими числами $r + 1 < m \leq n$ та $0 \leq r \leq 1$, що існує локальне майже-кілець R , адитивна група якого R^+ ізоморфна групі $G(2^m, 2^n, -r)$.*

Теорема 1.42 (Theorem 2, [103]). *Нехай R є локальним майже-кілецем, 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 $R^* = \{ax_1 + bx_2 \mid x_2 \equiv 1 \pmod{2}\}$.

Маємо таку формулу для множення будь-яких двох елементів у локальному майже-кілеці R , адитивна група якого ізоморфна $G(2^m, 2^n, -r)$ в [103].

Наслідок 1.43 (Corollary 4, [103]). *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 $\beta(b) = 0$;

$$(2) \beta(x) \equiv 0 \pmod{2^{n-1}};$$

$$(3) \alpha(xy) = \begin{cases} \alpha(x)\alpha(y) + x_1\beta(y), & \text{якщо } m = n \text{ та } x_2 \equiv 0 \pmod{2}, \text{ та} \\ \alpha(x)\alpha(y), & \text{інакше;} \end{cases}$$

$$(4) \beta(xy) = \beta(x)\alpha(y) + x_2\beta(y).$$

Теорема 1.44 (Theorem 3, [103]). Для кожного простого числа p та таких додатних цілих m, n , що або $m \geq n + r \geq 2r + [\frac{2}{p}]$, або $p = 2$, $2 < m \leq n$ та $r = 1$ існує локальне майже-кільце R , адитивна група якого R^+ ізоморфна групі $G(p^m, p^n, r)$.

В [88] доведено, що для $p > 2$ кожна скінченна неметациклічна 2-породжена p -група нільпотентності класу 2 з циклічною комутаторною підгрупою є адитивною групою локального майже-кільця та, зокрема, майже-кільця з одиницею. Також показано, що підгрупа всіх необоротних елементів цього майже-кільця має індекс p у своїй адитивній групі.

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 $G(p^m, p^n, p^d)$.

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 $0 \leq x_3 < p^d$.

Показано в [88], що множина L усіх необоротних елементів R є підгрупою індексу p в R^+ .

Теорема 1.45 (Theorem 2, [88]). *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-кільці R .

Наслідок 1.46 (Corollary 2, [88]). *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*

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

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

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

$$(5) \quad \gamma(xy) \equiv -x_1x_2\binom{\alpha(y)}{2} - \alpha(x)\beta(x)\binom{\beta(y)}{2} - x_2\alpha(x)\alpha(y)\beta(y) \\ + x_3\alpha(y) + \gamma(x)\beta(y) + x_1\beta(x)\gamma(y) - x_2\alpha(x)\gamma(y) \pmod{p^d}.$$

Наступна теорема показує, що умови, наведені в теоремі 1.45, 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-кілця з одиницею.

Теорема 1.47 (Theorem 3, [88]). *Для кожного простого числа p та додатних цілих чисел m, n та d з $1 \leq d \leq n \leq m$ існує локальне майже-кілце R , адитивна група якого R^+ ізоморфна групі $G(p^m, p^n, p^d)$.*

Як наслідок маємо наступне твердження.

Наслідок 1.48 (Corollary 6, [88]). *Кожна група $G(p^m, p^n, p^d)$ є адитивною групою майже-кілця з одиницею.*

Основні результати, що стосуються локальних майже-кілець, підсумовані в оглядах [122], [7] та [100].

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

Теорема 1.49 (Theorem 2, [115]). *Нехай група G , її елемент g та підмоноїд F з $\text{End } G$ задовольняють Теорему 7.1 і нехай $A = F \cap \text{Aut } G$. Майже-кілце $Nr = (G, \cdot, \star_F)$ є локальним тоді й тільки тоді, коли існує підгрупа L групи G така, що $G = g^A \cup L$ та $g^A \cap L = \emptyset$.*

Результати з теорії майже-кілець, зокрема, локальних майже-кілець, можуть мати застосування в побудові криптографічних схем і кодуванні (див., наприклад, [38], [39], [22], [68]).

1.3. Система комп'ютерної алгебри GAP

Розробка системи комп'ютерної алгебри GAP [43], назва якої розшифровується як “Groups, Algorithms and Programming”, була розпочата в 1986 році в місті Аахен, Німеччина. Поточна версія системи — GAP 4.13.0. Система GAP є вільно розповсюджувальною, відкритою та розширюваною.

Структура GAP (див., наприклад, [18])

GAP має ядро, написане на мові програмування C. Ядро реалізує

- мову GAP,
- інтерактивне середовище для розробки та використання програм GAP,
- керування пам'яттю та
- швидкі версії критично важливих операцій для різних типів даних.

В ядрі програми міститься бібліотека SmallGroup груп порядку до 2000 (див., наприклад, [120]). Групи відсортовані за порядком і перелічені до ізоморфізму; тобто для кожного з доступних порядків надається список представників груп типу ізоморфізму. Бібліотека містить такі групи:

- ті, що мають порядок не більше 2000, крім 1024 (423164062 групи);
- ті, що мають порядок вільний від кубів не більше 50000 (395703 групи);
- ті, що мають порядок p^7 для простих чисел $p = 3, 5, 7, 11$ (907489 груп);

- ті, що мають порядок p^n для $n \leq 6$ та всі прості числа p ;
- ті, що мають порядок $q^n \cdot p$ для q^n , що ділять 2^8 , 3^6 , 5^5 або 7^4 та всі прості числа p з $p \neq q$;
- ті, що мають порядок вільний від квадратів;
- ті, порядок яких розкладається на множники не більше ніж на 3 прості числа.

Перші три елементи у цьому списку охоплюють явний діапазон порядків; останні чотири надають доступ до нескінченних сімейств груп, що мають порядки певних типів.

Разом із системою розповсюджується багато пакетів для неї, наприклад (див., [44]):

- AutoDoc (Генерація документації з вихідного коду GAP),
- AutomGrp (Групи автоматів),
- CAP (Категорії, Алгоритми, Програмування),
- Circle (Спряжені групи скінченних кілець),
- Cryst (Обчислення з кристалографічними групами),
- Digraphs (Графи, диграфи та мультидиграфи в GAP),
- Polycyclic (Обчислення з поліциклічними групами),
- Semigroups (Пакет для напівгруп та моноїдів),
- SONATA (Система майже кілець та їх застосування),
- YangBaxter (Комбінаторні розв'язки для рівняння Янга–Бакстера), тощо.

Пакети переважно написані мовою GAP, але деякі також містять автономні модулі. Деякі пакети надають посилання на інші системи, наприклад:

- JupyterKernel (ядро Jupyter, написане на GAP),
- JupyterViz (інструменти візуалізації для Jupyter та GAP REPL).

Функціонал програми GAP містить багато функцій для аналізу структури та елементів груп, напівгруп, кілець, тощо. Наведемо деякі з цих функцій (див., [43]):

- AllEndomorphisms(G) (повертає всі гомоморфізми з G на себе),
- AllSubgroups(G) (для скінченної групи G функція AllSubgroups повертає список усіх підгруп G , призначений переважно для використання в класі для невеликих прикладів),
- AutomorphismGroup(G) (повертає повну групу автоморфізмів групи G . Автоморфізми діють на G оператором),
- ConjugacyClassesSubgroups(G , U) (цей атрибут повертає список усіх класів спряженості підгруп групи G . Порядок, у якому перераховані класи, залежить від методу, обраного GAP),
- DerivedSubgroup(G) (комутатор G' групи G — це підгрупа, породжена всіма комутаторами пар елементів G . Вона є нормальною в G , а фактор-група G/G' є найбільшою абелевою фактор-групою G),
- FrattiniSubgroup(G) (підгрупа Фраттіні групи G — це перетин усіх максимальних підгруп G),
- FreeGroup([wfilt], name1, name2, ...) (якщо викликати функцію FreeGroup з додатним цілим числом *rank*, вона повертає вільну групу на твірних *rank*. Якщо вказано необов'язковий аргумент name,

то твірні друкуються як *name1*, *name2* тощо, тобто кожне *name* є конкатенацією рядка *name* та цілого числа від 1 до *rank*. За замовчуванням для *name* використовується рядок “f”),

- `GroupByGenerators(gens, id)` (`GroupByGenerators` повертає групу G , згенеровану списком *gens*. Якщо присутній другий аргумент *id*, то він зберігається як елемент ідентифікації групи),
- `IdealByGenerators(R, gens)` (функція `TwoSidedIdealByGenerators` повертає кільце, згенероване елементами колекції *gens* під час додавання, множення та множення з елементами кільця R зліва та справа),
- `IsCommutative(M)` (магма M є комутативною, якщо для всіх елементів $a, b \in M$ виконується рівність $a * b = b * a$. `IsAbelian` є синонімом `IsCommutative`),
- `IsCyclic(G)` (група називається циклічною, якщо її можна породити одним елементом. Для циклічної групи можна обчислити породжуючу множину, що складається лише з одного елемента, використовуючи `MinimalGeneratingSet`),
- `IsSemigroup(D)` (повертає значення `true`, якщо об’єкт D є напівгрупою. Напівгрупа — це магма з асоціативним множенням),
- `IsSolvableGroup(G)` (група є розв’язною, якщо похідний ряд досягає тривіальної підгрупи за скінченну кількість кроків),
- `IsSubgroup(G, U)` (`IsSubgroup` повертає значення `true`, якщо U є групою, яка є підмножиною домену G),
- `MinimalGeneratingSet(G)` (повертає породжуючу множину G мінімальної можливої довжини),
- `SemigroupByGenerators(gens)` (є базовою операцією `Semigroup`),

- `SubgroupsSolvableGroup(G)` (Ця функція (що реалізує алгоритм, опублікований у [48]) обчислює підгрупи розв’язної групи G , використовуючи принцип гомоморфізму. Вона повертає список представників до G -спряженості).

Айчингер, Біндер, Еккер, Майер і Нибауер розробили пакет “Systems of nearrings and their applications” (SONATA) версія 2.9.7 [19] — це пакет для побудови та дослідження скінченних майже-кілець та майже-кілець з одиницею. В цьому пакеті міститься бібліотека всіх 68659 майже-кілець порядку менших за 16, та всіх майже-кілець з одиницею порядку меншого за 32. А також, різноманітні функції для аналізу структури та елементів скінченних майже-кілець, а саме (див., [19]):

- 1) методи для знаходження всіх ендоморфізмів заданої групи, а саме, `Endomorphisms(nr)`;
- 2) методи для побудови майже-кілець функцій на групі G таких як:
 - майже-кілець поліноміальних функцій на групі G (у сенсі Лауша–Нибауера): `PolynomialNearRing(G)`;
 - майже-кілець, породжені моноїдом ендоморфізмів $EndG$, групою автоморфізмів $AutG$ чи групою внутрішніх автоморфізмів $InnG$, а саме, `EndomorphismNearRing(G)`, `AutomorphismNearRing(G)`, `InnerAutomorphismNearRing(G)`;
 - майже-кілець трансформацій, а саме, `TransformationNearRing(G)`; `TransformationNearRingByAdditiveGenerators(G, endomaplist)`, `TransformationNearRingByGenerators(G, endomaplist)`;
 - централізаторні майже-кілець, а саме, `CentralizerNearRing(G, endos)`;
- 3) різноманітні функції для вивчення будови майже-кілець (його поряд-

ку, адитивних підгруп, ідеалів, оборотних елементів, ...), наприклад:

- `Size(nr)` (повертає кількість елементів у майже-кільці nr),
- `GroupReduct(nr)` (повертає майже-кільце nr як (мультиплікативну) групу),
- `NearRingIdealByGenerators(nr, gens)` (приймає як аргументи майже кільце nr та список $gens$ з довільної кількості елементів nr . Вона повертає найменший ідеал nr , що містить усі елементи $gens$),
- `NearRingLeftIdealByGenerators(nr, gens)` (приймає як аргументи майже кільце nr та список $gens$ з довільної кількості елементів nr . Вона повертає найменший лівий ідеал nr , що містить усі елементи $gens$),
- `NearRingIdeals(nr)` (обчислює всі ідеали майже-кільця nr . Повернене значення — це список ідеалів nr),
- `IsNearRingLeftIdeal(I)` (можна застосувати до будь-якого ідеалу майже-кільця. Ця функція повертає значення `true`, якщо I є лівим ідеалом у своєму “батьківському” майже-кільці),
- `FactorNearRing(nr, I)` (для майже-кільця nr та ідеалу I майже-кільця nr повертає фактор-кільце майже-кільця nr за модулем ідеалу I),
- `NearRingUnits(nr)` (повертає одиниці майже-кільця nr або у вигляді мультиплікативної групи, або у вигляді списку);

4) визначення властивостей елементів майже-кільця, наприклад,

- `Distributors(nr)` (елемент x майже-кільця $(N, +, \cdot)$ називається

дистрибутивним, якщо

$$x = (n_1 + n_2) \cdot n_3 - (n_1 \cdot n_3 + n_2 \cdot n_3)$$

для деяких елементів n_1, n_2, n_3 з N . Функція **Distributors** повертає список, що містить дистрибутивні елементи майже-кільця nr),

- **ZeroSymmetricElements(nr)** (нехай $(N, +, \cdot)$ — ліве майже-кільце, і позначимо через 0 нейтральний елемент $(N, +)$). Елемент n з N називається нульсиметричним елементом, якщо $0 \cdot n = 0$. Функція **ZeroSymmetricElements** повертає список, що містить нульсиметричні елементи майже-кільця nr),
- **IdempotentElements(nr)** (повертає список, що містить ідемпотентні елементи мультиплікативної напівгрупи майже-кільця nr),
- **NilpotentElements(nr)** (нехай $(N, +, \cdot)$ — майже-кільце з нулем 0 . Елемент n з N називається нільпотентним, якщо існує додатне ціле число k таке, що $nk = 0$. Функція **NilpotentElements** повертає список підписків довжини 2, де перший елемент — нільпотентний елемент n , а другий елемент — найменше k таке, що $nk = 0$),
- **RegularElements(nr)** (нехай $(N, +, \cdot)$ — майже-кільце. Елемент n з N називається регулярним, якщо існує елемент x такий, що $n \cdot x \cdot n = n$. Функція **RegularElements** повертає список усіх регулярних елементів майже-кільця nr);

5) визначення чи є два майже-кільця ізоморфними, наприклад, **IsIsomorphicNearRing**;

6) функції для визначення властивостей майже-кільця, наприклад,

- `IsAbelianNearRing(nr)` (майже-кільце називається абелевим, якщо його адитивна група є абелевою. Функція `IsAbelianNearRing` повертає відповідне логічне значення `true` або `false`),
- `IsCommutative(nr)` (майже-кільце $(N, +, \cdot)$ називається комутативним, якщо його мультиплікативна напівгрупа є комутативною. Функція `IsCommutative` повертає відповідне значення `true` або `false`),
- `IsNilpotentNearRing(nr)` (майже-кільце N називається нільпотентним, якщо існує додатне ціле число k , тобто $N^k = \{0\}$. Функція `IsNilpotentNearRing` перевіряє, чи є майже-кільце nr нільпотентним, і повертає відповідне логічне значення `true` або `false`), тощо.

7) функції для роботи з бібліотекою майже-кілець та майже-кілець з одиницею, наприклад:

- `LibraryNearRing(G, num)` (отримує майже кільце з файлів бібліотеки майже-кілець. G має бути групою порядку ≤ 15 . num має бути цілим числом, яке вказує номер класу майже кілець у вказаній групі)
- `AllLibraryNearRings(G)` (повертає список усіх майже-кілець (у бібліотеці), які мають групу G як вказану групу),
- `LibraryNearRingWithOne(G, num)` (отримує майже кільце з файлів бібліотеки майже-кілець. G має бути однією з попередньо визначених груп порядку ≤ 31 . num має бути цілим числом, яке вказує номер класу майже кілець з одиницею у вказаній групі),
- `AllLibraryNearRingsWithOne(G)` (повертає список усіх майже-кілець з одиницею (у бібліотеці), які мають групу G як вказану групу)

- `IdLibraryNearRing(nr)` (повертає пару $[G, n]$ таку, що майже-кільце nr ізоморфне n -му майже-кільцю бібліотеки на групі G),
- `IdLibraryNearRingWithOne(nr)` (повертає пару $[G, n]$ таку, що майже-кільце nr ізоморфне n -му майже-кільцю бібліотеки з одиницею на групі G . Цю функцію можна застосувати лише до майже-кілець, які мають одиницю),
- `IsLibraryNearRing(nr)` (повертає значення `true`, якщо номер `nearring` було прочитано з бібліотеки `nearring`, та `false` в іншому випадку).

Список усіх 698 неізоморфних локальних майже-кілець порядку не більше 31 містяться в пакеті SONATA. Однак класифікація майже-кілець порядку 32 і вище вимагає набагато складніших обчислень. Для локальних майже-кілець вони були реалізовані в новому GAP-пакеті LocalNR. Поточна версія пакета LocalNR [111] (ще не розповсюджена з GAP) містить усі 37441 локальне майже-кільце порядку щонайбільше 361, за винятком порядків 32, 64, 128, 243 і 256.

Наприклад, існує 267 неізоморфних груп порядку $64 = 2^5$, з яких 53 є 2-породженими групами, і лише 24 з цих груп є адитивними групами локальних майже-кілець та класифіковано ці майже-кільця (див. [100, 106]).

Нехай $[n, i]$ — i -та група порядку n у бібліотеці SmallGroups у GAP.

Позначимо через $n(G)$ — кількість усіх неізоморфних локальних майже-кілець R , адитивна група яких R^+ ізоморфна групі G .

Теорема 1.50 (Theorem 25, [100]). *Наступні 2-породженні групи G є адитивними групами локальних майже-кілець порядку 64:*

- $IdGroup(G) = [64, 2]$, $G \cong C_8 \times C_8$ та $n(G) = 1683$;
- $IdGroup(G) = [64, 3]$, $G \cong C_8 \rtimes C_8$ та $n(G) = 1628$;

- $IdGroup(G) = [64, 4], G \cong ((C_8 \times C_2) \rtimes C_2) \rtimes C_2 \text{ } ma \text{ } n(G) = 167245;$
- $IdGroup(G) = [64, 5], G \cong (C_4 \times C_2) \rtimes C_8 \text{ } ma \text{ } n(G) = 118190;$
- $IdGroup(G) = [64, 10], G \cong (C_8 \rtimes C_4) \rtimes C_2 \text{ } ma \text{ } n(G) = 7424;$
- $IdGroup(G) = [64, 12], G \cong (C_4 \rtimes C_8) \rtimes C_2 \text{ } ma \text{ } n(G) = 5633;$
- $IdGroup(G) = [64, 14], G \cong (C_2 \times C_2).((C_4 \times C_2) \rtimes C_2) \text{ } ma \text{ } n(G) = 5520;$
- $IdGroup(G) = [64, 15], G \cong C_8 \rtimes C_8 \text{ } ma \text{ } n(G) = 2384;$
- $IdGroup(G) = [64, 16], G \cong C_8 \rtimes C_8 \text{ } ma \text{ } n(G) = 2384;$
- $IdGroup(G) = [64, 17], G \cong (C_8 \times C_2) \rtimes C_4 \text{ } ma \text{ } n(G) = 433060;$
- $IdGroup(G) = [64, 23], G \cong (C_4 \times C_2 \times C_2) \rtimes C_4 \text{ } ma \text{ } n(G) = 111758;$
- $IdGroup(G) = [64, 24], G \cong (C_8 \rtimes C_2) \rtimes C_4 \text{ } ma \text{ } n(G) = 109189;$
- $IdGroup(G) = [64, 26], G \cong C_{16} \times C_4 \text{ } ma \text{ } n(G) = 11467;$
- $IdGroup(G) = [64, 27], G \cong C_{16} \rtimes C_4 \text{ } ma \text{ } n(G) = 11467;$
- $IdGroup(G) = [64, 29], G \cong (C_{16} \times C_2) \rtimes C_2 \text{ } ma \text{ } n(G) = 28185;$
- $IdGroup(G) = [64, 30], G \cong (C_{16} \rtimes C_2) \rtimes C_2 \text{ } ma \text{ } n(G) = 4433;$
- $IdGroup(G) = [64, 34], G \cong (((C_4 \times C_2) \rtimes C_2) \rtimes C_2) \rtimes C_2 \text{ } ma \text{ } n(G) = 16177;$
- $IdGroup(G) = [64, 35], G \cong (C_4 \times C_4) \rtimes C_4 \text{ } ma \text{ } n(G) = 15504;$
- $IdGroup(G) = [64, 36], G \cong (C_2).((C_4 \times C_2) \rtimes C_2) \text{ } ma \text{ } n(G) = 15761;$
- $IdGroup(G) = [64, 37], G \cong C_2.(((C_4 \times C_2) \rtimes C_2) \rtimes C_2) \text{ } ma \text{ } n(G) = 15920;$

- $IdGroup(G) = [64, 44]$, $G \cong C_4 \rtimes C_{16}$ та $n(G) = 28500$;
- $IdGroup(G) = [64, 45]$, $G \cong C_8.D_8 = C_4.(C_8 \times C_2)$ та $n(G) = 1920$;
- $IdGroup(G) = [64, 50]$, $G \cong C_{32} \times C_2$ та $n(G) = 257$;
- $IdGroup(G) = [64, 51]$, $G \cong C_{32} \rtimes C_2$ та $n(G) = 257$.

Існує 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.

Теорема 1.51 (Theorem 2, [107]). *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.*

- $IdGroup(G) = [243, 2]$, $G \cong (C_9 \times C_3) \rtimes C_9$ та $n(G) = 119629$:
 - $IdGroup(R^*) = [162, 32]$, $R^* \cong C_3 \times C_3 \times D_{18}$ та $n(R^*) = 12879$;
 - $IdGroup(R^*) = [162, 33]$, $R^* \cong C_3 \times C_9 \times S_3$ та $n(R^*) = 3351$;
 - $IdGroup(R^*) = [162, 35]$, $R^* \cong ((C_3 \times C_3) \rtimes C_3) \times S_3$ та $n(R^*) = 87$;
 - $IdGroup(R^*) = [162, 36]$, $R^* \cong C_3 \times ((C_9 \rtimes C_3) \rtimes C_2)$ та $n(R^*) = 96472$;
 - $IdGroup(R^*) = [162, 37]$, $R^* \cong (C_9 \rtimes C_3) \times S_3$ та $n(R^*) = 6810$;
 - $IdGroup(R^*) = [162, 51]$, $R^* \cong C_3 \times C_3 \times C_3 \times S_3$ та $n(R^*) = 30$;
- $IdGroup(G) = [243, 10]$, $G \cong C_{27} \times C_9$ та $n(G) = 119298$:
 - $IdGroup(R^*) = [162, 3]$, $R^* \cong C_9 \times D_{18}$ та $n(R^*) = 477$;

- $IdGroup(R^*) = [162, 6], R^* \cong (C_9 \rtimes C_9) \rtimes C_2 \text{ } ma \text{ } n(R^*) = 811;$
- $IdGroup(R^*) = [162, 23], R^* \cong C_{18} \times C_9 \text{ } ma \text{ } n(R^*) = 21372;$
- $IdGroup(R^*) = [162, 25], R^* \cong C_2 \times (C_9 \rtimes C_9) \text{ } ma \text{ } n(R^*) = 96531;$
- $IdGroup(R^*) = [162, 30], R^* \cong C_2 \times ((C_9 \times C_3) \rtimes C_3) \text{ } ma \text{ } n(R^*) = 36;$
- $IdGroup(R^*) = [162, 31], R^* \cong C_2 \times (C_3 \cdot ((C_3 \times C_3) \rtimes C_3) = (C_3 \times C_3) \cdot (C_3 \times C_3)) \text{ } ma \text{ } n(R^*) = 27;$
- $IdGroup(R^*) = [162, 47], R^* \cong C_{18} \times C_3 \times C_3 \text{ } ma \text{ } n(R^*) = 6;$
- $IdGroup(R^*) = [162, 49], R^* \cong C_6 \times (C_9 \rtimes C_3) \text{ } ma \text{ } n(R^*) = 6;$
- $IdGroup(R^*) = [162, 50], R^* \cong C_2 \times ((C_9 \times C_3) \rtimes C_3) \text{ } ma \text{ } n(R^*) = 32;$
- $IdGroup(G) = [243, 11], G \cong C_{27} \rtimes C_9 \text{ } ma \text{ } n(G) = 1288:$
 - $IdGroup(R^*) = [162, 3], R^* \cong C_9 \times D_{18} \text{ } ma \text{ } n(R^*) = 477;$
 - $IdGroup(R^*) = [162, 6], R^* \cong (C_9 \rtimes C_9) \rtimes C_2 \text{ } ma \text{ } n(R^*) = 811;$
- $IdGroup(G) = [243, 12], G \cong (C_{27} \times C_3) \rtimes C_3 \text{ } ma \text{ } n(G) = 29989:$
 - $IdGroup(R^*) = [162, 33], R^* \cong C_3 \times C_9 \times S_3 \text{ } ma \text{ } n(R^*) = 10306;$
 - $IdGroup(R^*) = [162, 37], R^* \cong (C_9 \rtimes C_3) \times S_3 \text{ } ma \text{ } n(R^*) = 19683;$
- $IdGroup(G) = [243, 13], G \cong ((C_9 \times C_3) \rtimes C_3) \rtimes C_3 \text{ } ma \text{ } n(G) = 139672:$
 - $IdGroup(R^*) = [162, 32], R^* \cong C_3 \times C_3 \times D_{18} \text{ } ma \text{ } n(R^*) = 2430;$
 - $IdGroup(R^*) = [162, 33], R^* \cong C_3 \times C_9 \times S_3 \text{ } ma \text{ } n(R^*) = 90;$
 - $IdGroup(R^*) = [162, 34], R^* \cong C_3 \times (((C_3 \times C_3) \rtimes C_3) \rtimes C_2) \text{ } ma \text{ } n(R^*) = 81811;$
 - $IdGroup(R^*) = [162, 35], R^* \cong ((C_3 \times C_3) \rtimes C_3) \times S_3 \text{ } ma \text{ } n(R^*) = 6723;$

- $IdGroup(R^*) = [162, 36]$, $R^* \cong C_3 \times ((C_9 \rtimes C_3) \rtimes C_2)$ $ma\ n(R^*) = 32076$;
- $IdGroup(R^*) = [162, 37]$, $R^* \cong (C_9 \rtimes C_3) \times S_3$ $ma\ n(R^*) = 342$;
- $IdGroup(R^*) = [162, 51]$, $R^* \cong C_3 \times C_3 \times C_3 \times S_3$ $ma\ n(R^*) = 3321$;
- $IdGroup(R^*) = [162, 52]$, $R^* \cong C_3 \times C_3 \times ((C_3 \times C_3) \rtimes C_2)$ $ma\ n(R^*) = 12879$;
- $IdGroup(G) = [243, 14]$, $G \cong (C_9 \times C_3) \rtimes C_9$ $ma\ n(G) = 115020$:
 - $IdGroup(R^*) = [162, 32]$, $R^* \cong C_3 \times C_3 \times D_{18}$ $ma\ n(R^*) = 12393$;
 - $IdGroup(R^*) = [162, 33]$, $R^* \cong C_3 \times C_9 \times S_3$ $ma\ n(R^*) = 3321$;
 - $IdGroup(R^*) = [162, 36]$, $R^* \cong C_3 \times ((C_9 \rtimes C_3) \rtimes C_2)$ $ma\ n(R^*) = 92583$;
 - $IdGroup(R^*) = [162, 37]$, $R^* \cong (C_9 \rtimes C_3) \times S_3$ $ma\ n(R^*) = 6723$;
- $IdGroup(G) = [243, 15]$, $G \cong (C_9 \times C_3) \rtimes C_9$ $ma\ n(G) = 117783$:
 - $IdGroup(R^*) = [162, 32]$, $R^* \cong C_3 \times C_3 \times D_{18}$ $ma\ n(R^*) = 11961$;
 - $IdGroup(R^*) = [162, 33]$, $R^* \cong C_3 \times C_9 \times S_3$ $ma\ n(R^*) = 3432$;
 - $IdGroup(R^*) = [162, 34]$, $R^* \cong C_3 \times (((C_3 \times C_3) \rtimes C_3) \rtimes C_2)$ $ma\ n(R^*) = 5832$;
 - $IdGroup(R^*) = [162, 36]$, $R^* \cong C_3 \times ((C_9 \rtimes C_3) \rtimes C_2)$ $ma\ n(R^*) = 89127$;
 - $IdGroup(R^*) = [162, 37]$, $R^* \cong (C_9 \rtimes C_3) \times S_3$ $ma\ n(R^*) = 6702$;
 - $IdGroup(R^*) = [162, 52]$, $R^* \cong C_3 \times C_3 \times ((C_3 \times C_3) \rtimes C_2)$ $ma\ n(R^*) = 729$;
- $IdGroup(G) = [243, 16]$, $G \cong (C_{27} \rtimes C_3) \rtimes C_3$ $ma\ n(G) = 59049$:

- $IdGroup(R^*) = [162, 33]$, $R^* \cong C_3 \times C_9 \times S_3$ *ma* $n(R^*) = 19683$;
- $IdGroup(R^*) = [162, 37]$, $R^* \cong (C_9 \rtimes C_3) \times S_3$ *ma* $n(R^*) = 39366$;
- $IdGroup(G) = [243, 23]$, $G \cong C_{81} \times C_3$ *ma* $n(G) = 3349$:
 - $IdGroup(R^*) = [162, 8]$, $R^* \cong C_{27} \times S_3$ *ma* $n(R^*) = 28$;
 - $IdGroup(R^*) = [162, 26]$, $R^* \cong C_{54} \times C_3$ *ma* $n(R^*) = 1134$;
 - $IdGroup(R^*) = [162, 27]$, $R^* \cong C_2 \times (C_{27} \rtimes C_3)$ *ma* $n(R^*) = 2187$;
- $IdGroup(G) = [243, 24]$, $G \cong C_{81} \rtimes C_3$, $n(G) = 28$ *ma* $IdGroup(R^*) = [162, 8]$, $R^* \cong C_{27} \times S_3$, $n(R^*) = 28$.

Висновки до розділу 1

У розділі зроблено огляд літератури за темою дисертації. Основна увага в ньому приділена роботам та результатам, що стосуються дослідженню та класифікації скінченних майже-кілець з одиницею та локальних майже-кілець з обмеженнями на адитивні групи. Наведено інформацію про систему комп'ютерної алгебри GAP та її пакету SONATA.

Питання дослідження адитивних груп майже-кілець з одиницею та локальних майже-кілець, і їх класифікація є актуальною задачею.

Розділ 2

Майже-кільця з одиницею порядків p^3

У даному розділі вивчаються скінченні майже-кільця з одиницею порядків p^3 .

2.1. Групи порядку p^3

Наступне твердження містить класифікацію груп порядку p^3 (див. [16]).

Твердження 2.1. *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 дієдра*, $a^4 = 1, b^2 = 1, a^{-1}b = ba$;
- 5) *група кватерніонів*, $a^4 = 1, b^2 = a^2, a^{-1}b = ba$.

Неабелеві групи порядку p^3 , p — непарне:

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

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

Нагадаємо, що експонентою групи є найменше спільне кратне порядків її елементів. Зокрема, експонентою скінченної p -групи є максимальний порядок її елементів.

Наступне твердження є добре відомим (див., наприклад, [34], теорема 3).

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

Нехай G — група, а $\text{End } G$ — 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 $\{g^\alpha | \alpha \in \text{End } G\}$ усіх образів елемента g відносно ендоморфізмів $\text{End } G$.

Означення 2.3. Група G називається ендоциклічною, якщо вона містить елемент g з $G = g^{\text{End } G}$.

2.2. Майже-кільця з одиницею

Наведемо основні означення (див., наприклад, [72], [64], [32], [41], [122]).

Означення 2.4. Непорожня множина R з двома бінарними операціями “+” та “·” називається майже-кільцем, якщо:

1) $(R, +)$ — група з нейтральним елементом 0;

2) $(R, \cdot)$ — напівгрупа;

3) $x \cdot (y + z) = x \cdot y + x \cdot z$ для всіх $x, y, z \in R$.

Таке майже-кільце називається лівим майже-кільцем. Якщо ж аксіому 3) замінити аксіомою $(x + y) \cdot z = x \cdot z + y \cdot z$ для всіх $x, y, z \in R$, то отримаємо праве майже-кільце.

Група $(R, +)$ позначається через R^+ та називається *адитивною групою*, а її нейтральний елемент 0 — *нулем* майже-кільця R . З аксіоми 3) випливає, що

$$r \cdot 0 = r \cdot (0 + 0) = r \cdot 0 + r \cdot 0,$$

звідки отримуємо $r \cdot 0 = 0$. З цієї ж аксіоми випливає, що $r \cdot (-s) = -(r \cdot s)$. Майже-кільце R називається *нуль-симетричним*, якщо також $0 \cdot x = 0$.

Майже-кільце R , в якому напівгрупа $(R, \cdot)$ є моноїдом з одиничним елементом i , називається *майже-кільцем з одиницею i* . Група всіх оборотних елементів цього моноїда позначається через R^* та називається *мультиплікативною групою* майже-кільця R , а її доповнення $R \setminus R^*$ — множиною необоротних елементів із R .

Наступна лема визначає експоненту адитивної групи скінченного майже-кільця з одиницею [102, Lemma 5].

Лема 2.5. *Експонента адитивної групи скінченного майже-кільця R з одиницею дорівнює адитивному порядку його одиниці, який співпадає з адитивним порядком кожного елементу його мультиплікативної групи R^* .*

Наступна лема характеризує основні властивості скінчених локальних майже-кільць (див. [21], Lemma 3.2).

Лема 2.6. *Нехай R — локальне майже-кільце з одиницею i , а L — підгрупа всіх необоротних елементів R . Тоді справедливі такі твердження:*

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

2.3. Майже-кільця з одиницею на абелевих групах порядку p^3

Нехай $G(p, p, p)$ — група зі співвідношеннями 3) з леми 2.1.

Нехай R — майже-кільце з одиницею, адитивна група R^+ якого ізоморфна групі $G(p, p, p)$. Тоді $R^+ = \langle a \rangle + \langle b \rangle + \langle c \rangle$ для деяких $a, b, c \in R$, що задовольняють співвідношення $ap = bp = cp = 1$, $a + b = b + a$, $a + c = c + a$, $c + b = b + c$. Зокрема, кожний елемент $x \in R$ єдиним чином записується у вигляді $x = ax_1 + bx_2 + cx_3$ з коефіцієнтами $0 \leq x_1 < p$, $0 \leq x_2 < p$ та $0 \leq x_3 < p$.

Без втрати загальності, можна припустити, що a є одиницею в R , тобто $ax = xa = x$ для кожного $x \in R$. Більш того, для кожного $x \in R$ існують такі коефіцієнти $\alpha(x), \beta(x), \gamma(x), \lambda(x), \mu(x)$ та $\nu(x)$, що

$$xb = a\alpha(x) + b\beta(x) + c\gamma(x)$$

та

$$xc = a\lambda(x) + b\mu(x) + c\nu(x).$$

Зрозуміло, що вони єдиним чином визначені за модулем p , тому деякі відображення $\alpha : R \rightarrow Z_p$, $\beta : R \rightarrow Z_p$, $\gamma : R \rightarrow Z_p$, $\lambda : R \rightarrow Z_p$, $\mu : R \rightarrow Z_p$, $\nu : R \rightarrow Z_p$.

Теорема 2.7. Якщо $x, y = ay_1 + by_2 + cy_3 \in R$, то

$$xy = a(x_1y_1 + \alpha(x)y_2 + \lambda(x)y_3) + b(x_2y_1 + \beta(x)y_2 + \mu(x)y_3) +$$

$$+c(x_3y_1 + \gamma(x)y_2 + \nu(x)y_3),$$

причому виконуються наступні твердження:

$$(0) \quad \alpha(0) \equiv 0 \pmod{p}, \quad \beta(0) \equiv 0 \pmod{p}, \quad \gamma(0) \equiv 0 \pmod{p}, \\ \lambda(0) \equiv 0 \pmod{p}, \quad \mu(0) \equiv 0 \pmod{p} \text{ та } \nu(0) \equiv 0 \pmod{p} \text{ тоді і} \\ \text{тільки тоді, коли майже-кільце } R \text{ є нуль-симетричним;}$$

$$(1) \quad \alpha(a) = 0, \quad \beta(a) = 1, \quad \gamma(a) = 0, \quad \lambda(a) = 0, \quad \mu(a) = 0, \quad \nu(a) = 1 \\ \pmod{p};$$

$$(2) \quad \alpha(xy) \equiv x_1\alpha(y) + \alpha(x)\beta(y) + \lambda(x)\gamma(y) \pmod{p};$$

$$(3) \quad \beta(xy) \equiv x_2\alpha(y) + \beta(x)\beta(y) + \mu(x)\gamma(y) \pmod{p};$$

$$(4) \quad \gamma(xy) \equiv x_3\alpha(y) + \gamma(x)\beta(y) + \nu(x)\gamma(y) \pmod{p};$$

$$(5) \quad \lambda(xy) \equiv x_1\lambda(y) + \alpha(x)\mu(y) + \lambda(x)\nu(y) \pmod{p};$$

$$(6) \quad \mu(xy) \equiv x_2\lambda(y) + \beta(x)\mu(y) + \mu(x)\nu(y) \pmod{p};$$

$$(7) \quad \nu(xy) \equiv x_3\lambda(y) + \gamma(x)\mu(y) + \nu(x)\nu(y) \pmod{p}.$$

Доведення. Оскільки

$$0 \cdot a = a \cdot 0 = 0,$$

то R є нуль-симетричним майже-кільцем, якщо і тільки якщо

$$0 = 0 \cdot b = a\alpha(0) + b\beta(0) + c\gamma(0)$$

або

$$\alpha(0) = \beta(0) = \gamma(0) = 0,$$

та

$$0 = 0 \cdot c = a\lambda(0) + b\mu(0) + c\nu(0)$$

або

$$\lambda(0) = \mu(0) = \nu(0) = 0.$$

Більш того,

$$b = ab = a\alpha(a) + b\beta(a) + c\gamma(a)$$

та

$$c = ac = a\lambda(a) + b\mu(a) + c\nu(a),$$

маємо $\alpha(a) = 0$, $\beta(a) = 1$, $\gamma(a) = 0$, $\lambda(a) = 0$, $\mu(a) = 0$, $\nu(a) = 1$. Тому твердження (0) та (1) мають місце.

Далі, з лівої дистрибутивності, отримаємо

$$\begin{aligned} xy &= (xa)y_1 + (xb)y_2 + (xc)y_3 = (ax_1 + bx_2 + cx_3)y_1 + \\ &+ (a\alpha(x) + b\beta(x) + c\gamma(x))y_2 + \\ &+ (a\lambda(x) + b\mu(x) + c\nu(x))y_3. \end{aligned}$$

Користуючись комутативністю додавання, маємо

$$\begin{aligned} (ax_1 + bx_2 + cx_3)y_1 &= ax_1y_1 + bx_2y_1 + cx_3y_1, \\ (a\alpha(x) + b\beta(x) + c\gamma(x))y_2 &= a\alpha(x)y_2 + b\beta(x)y_2 + c\gamma(x)y_2 \end{aligned}$$

та

$$(a\lambda(x) + b\mu(x) + c\nu(x))y_3 = a\lambda(x)y_3 + b\mu(x)y_3 + c\nu(x)y_3.$$

Тому

$$\begin{aligned} xy &= a(x_1y_1 + \alpha(x)y_2 + \lambda(x)y_3) + b(x_2y_1 + \beta(x)y_2 + \mu(x)y_3) + \\ &+ c(x_3y_1 + \gamma(x)y_2 + \nu(x)y_3). \end{aligned}$$

З асоціативності множення маємо $(xy)b = x(yb)$. Оскільки

$$(xy)b = a\alpha(xy) + b\beta(xy) + c\gamma(xy)$$

та

$$\begin{aligned} x(yb) &= a(x_1\alpha(y) + \alpha(x)\beta(y) + \lambda(x)\gamma(y)) + \\ &+ b(x_2\alpha(y) + \beta(x)\beta(y) + \mu(x)\gamma(y)) + \end{aligned}$$

$$+c(x_3\alpha(y) + \gamma(x)\beta(y) + \nu(x)\gamma(y)),$$

то прирівнюючи відповідні коефіцієнти отримаємо рівності (2)–(4).

Аналогічно з асоціативності множення маємо $(xy)c = x(yc)$. Оскільки

$$(xy)c = a\lambda(xy) + b\mu(xy) + c\nu(xy)$$

та

$$\begin{aligned} x(yc) = & a(x_1\lambda(y) + \alpha(x)\mu(y) + \lambda(x)\nu(y)) + \\ & + b(x_2\lambda(y) + \beta(x)\mu(y) + \mu(x)\nu(y)) + \\ & + c(x_3\lambda(y) + \gamma(x)\mu(y) + \nu(x)\nu(y)), \end{aligned}$$

то прирівнюючи відповідні коефіцієнти отримаємо рівності (5)–(7). $\square$

2.4. Майже-кільця з одиницею на неабелевих групах порядку p^3

2.4.1. Майже-кільця з одиницею, адитивна група яких ізоморфна G_1

Далі позначимо через G_1 групу зі співвідношеннями 5*) твердження 2.1.

Ми визначаємо групу G_1 як адитивно записану групу, породжену a, b, c з урахуванням співвідношень $ap = bp = cp = 0$, $a + b = b + a + c$, $a + c = c + a$, $b + c = c + b$.

Наступні дві леми доведено в [12].

Лема 2.8. *Нехай $k, l \in \mathbb{N}$. Тоді в G_1 виконуються рівності*

$$-ak - bl + ak + bl = c(kl)$$

та

$$bl + ak = -c(kl) + ak + bl.$$

Доведення. Оскільки $-b + a + b = a + c$, маємо $-bl + a + bl = a + cl$. Тоді

$$-bl + ak + bl = (a + cl)k = ak + ckl.$$

Отже, $-ak - bl + ak + bl = ckl$. □

Лема 2.9. *Нехай $k, l, r \in \mathbb{N}$. Тоді в G_1 маємо*

$$(ak + bl)r = akr + blr - ckl \binom{r}{2}.$$

Доведення. Доведення буде проведено індукцією за r . Для $r = 1$ виконується рівність. Нехай для r виконується рівність, тобто

$$(ak + bl)r = akr + blr - ckl \binom{r}{2}.$$

Доведемо рівність для $r + 1$:

$$\begin{aligned} (ak + bl)(r + 1) &= akr + blr + ak + bl - ckl \binom{r}{2} = \\ &= ak(r + 1) + bl(r + 1) - cklr - ckl \binom{r}{2} = \\ &= ak(r + 1) + bl(r + 1) - ckl(r + \binom{r}{2}) = \\ &= ak(r + 1) + bl(r + 1) - ckl \binom{r + 1}{2}. \end{aligned}$$

Отже, рівність справедлива для будь-якого r . □

Нехай R — майже-кільце з одиницею, адитивна група R^+ якого ізоморфна групі G_1 . Тоді

$$R^+ = \langle a \rangle + \langle b \rangle + \langle c \rangle$$

для деяких елементів a, b і c з R задовольняють співвідношення $ap = 0$, $bp = 0$, $cp = 0$, $a + b = b + a + c$, $a + c = c + a$ і $b + c = c + b$. Зокрема, кожен елемент $x \in R$ єдиним чином записаний у вигляді $x = ax_1 + bx_2 + cx_3$ з коефіцієнтами $0 \leq x_1 < p$, $0 \leq x_2 < p$ і $0 \leq x_3 < p$.

Покажемо, що не існує майже-кільця, в якому одиниця знаходиться в центрі адитивної групи G_1 . Відзначимо, що підгрупа $\langle c \rangle$ є центром групи G_1 .

Зауваження 2.10. Нехай c — одиниця майже-кільця R , тобто $xc = cx = x$ для кожного $x \in R$. Тоді для кожного $x \in R$ існують такі коефіцієнти $\alpha(x)$, $\beta(x)$, $\gamma(x)$, $\lambda(x)$, $\mu(x)$ і $\nu(x)$, що

$$xb = a\alpha(x) + b\beta(x) + c\gamma(x)$$

і

$$xa = a\lambda(x) + b\mu(x) + c\nu(x).$$

Зрозуміло, що вони однозначно визначені по модулю p , тому деякі відображення $\alpha : R \rightarrow \mathbb{Z}_p$, $\beta : R \rightarrow \mathbb{Z}_p$, $\gamma : R \rightarrow \mathbb{Z}_p$, $\lambda : R \rightarrow \mathbb{Z}_p$, $\mu : R \rightarrow \mathbb{Z}_p$ і $\nu : R \rightarrow \mathbb{Z}_p$ є визначеними.

Далі, використовуючи лему 2.8, ми отримуємо

$$\begin{aligned} xc &= -xa - xb + xa + xb = -c\nu(x) - b\mu(x) - a\lambda(x) - \\ &\quad - c\gamma(x) - b\beta(x) - a\alpha(x) + a\lambda(x) + b\mu(x) + \\ &\quad + c\nu(x) + a\alpha(x) + b\beta(x) + c\gamma(x) = -b\mu(x) - a\lambda(x) - \\ &\quad - b\beta(x) - a\alpha(x) + a\lambda(x) + b\mu(x) + a\alpha(x) + b\beta(x) = \\ &= -b\mu(x) + c\lambda(x)\beta(x) - b\beta(x) - a\lambda(x) - a(\alpha(x) - \\ &\quad - \lambda(x)) + b\mu(x) + a\alpha(x) + b\beta(x) = c\lambda(x)\beta(x) - \\ &\quad - b(\mu(x) + \beta(x)) - a\alpha(x) + b\mu(x) + a\alpha(x) + b\beta(x) = \\ &= c\lambda(x)\beta(x) - b(\mu(x) + \beta(x)) - a\alpha(x) - \\ &\quad - c\mu(x)\alpha(x) + a\alpha(x) + b\mu(x) + b\beta(x) = \\ &= c(\lambda(x)\beta(x) - \mu(x)\alpha(x)) - b(\mu(x) + \beta(x)) + \\ &\quad + b\mu(x) + b\beta(x) = c(\lambda(x)\beta(x) - \mu(x)\alpha(x)) \neq x. \end{aligned}$$

Тому не існує майже-кільця, в якому одиниця знаходиться в центрі адитивної групи G_1 .

Оскільки порядок елемента a дорівнює експоненті групи G_1 , то за лемою 2.2 ми можемо 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 $\alpha(x)$, $\beta(x)$ і $\gamma(x)$, що

$$xb = a\alpha(x) + b\beta(x) + c\gamma(x).$$

Зрозуміло, що вони однозначно визначені по модулю p , тому і визначені відображення $\alpha: R \rightarrow \mathbb{Z}_p$, $\beta: R \rightarrow \mathbb{Z}_p$ і $\gamma: R \rightarrow \mathbb{Z}_p$.

Майже-кільця з одиницею на неметациклічних групах Міллера–Морено були вивчені в статтях [12] і [73]. Лема 2.11 базуються на результатах цих робіт.

Лема 2.11. *Нехай R — майже-кільце з одиницею a , адитивна група якого є G_1 . Якщо $x = ax_1 + bx_2 + cx_3$, $y = ay_1 + by_2 + cy_3 \in R$,*

$$xb = a\alpha(x) + b\beta(x) + c\gamma(x),$$

то

$$\begin{aligned} xy &= a(x_1y_1 + \alpha(x)y_2) + b(x_2y_1 + \beta(x)y_2) + \\ &+ c(-x_1x_2\binom{y_1}{2} - \alpha(x)\beta(x)\binom{y_2}{2} - x_2\alpha(x)y_1y_2 + \\ &+ x_3y_1 + \gamma(x)y_2 + x_1\beta(x)y_3 - x_2\alpha(x)y_3). \end{aligned}$$

Більш того, для відображень виконуються наступні твердження $\alpha: R \rightarrow \mathbb{Z}_p$, $\beta: R \rightarrow \mathbb{Z}_p$ і $\gamma: R \rightarrow \mathbb{Z}_p$:

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

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

$$(2) \quad \beta(xy) \equiv x_2\alpha(y) + \beta(x)\beta(y) \pmod{p};$$

$$(3) \quad \gamma(xy) \equiv -x_1x_2\binom{\alpha(y)}{2} - \alpha(x)\beta(x)\binom{\beta(y)}{2} - x_2\alpha(x)\alpha(y)\beta(y) + \\ + x_3\alpha(y) + \gamma(x)\beta(y) + x_1\beta(x)\gamma(y) - x_2\alpha(x)\gamma(y) \pmod{p}.$$

Доведення. Оскільки $0 \cdot a = a \cdot 0 = 0$, то R є нуль-симетричним майже-кільцем тоді і тільки тоді, коли

$$0 = 0 \cdot b = a\alpha(0) + b\beta(0) + c\gamma(0)$$

або еквівалентно $\alpha(0) \equiv 0 \pmod{p}$, $\beta(0) \equiv 0 \pmod{p}$ і $\gamma(0) \equiv 0 \pmod{p}$. Крім того, оскільки $c = -a - b + a + b$ і з лівого дистрибутивного закону, ми маємо

$$0 \cdot c = -0 \cdot a - 0 \cdot b + 0 \cdot a + 0 \cdot b = 0,$$

звідки

$$0 \cdot x = 0 \cdot (ax_1 + bx_2 + cx_3) = \\ = (0 \cdot a)x_1 + (0 \cdot b)x_2 + (0 \cdot c)x_3 = 0.$$

Отже, виконується твердження (0).

Далі, використовуючи лему 2.8, отримуємо

$$xc = -xa - xb + xa + xb = -cx_3 - bx_2 - ax_1 - c\gamma(x) - \\ - b\beta(x) - a\alpha(x) + ax_1 + bx_2 + cx_3 + a\alpha(x) + \\ + b\beta(x) + c\gamma(x) = -bx_2 - ax_1 - b\beta(x) - a\alpha(x) + \\ + ax_1 + bx_2 + a\alpha(x) + b\beta(x) = -bx_2 + cx_1\beta(x) - \\ - b\beta(x) - ax_1 - a(\alpha(x) - x_1) + bx_2 + a\alpha(x) + b\beta(x) = \\ = cx_1\beta(x) - b(x_2 + \beta(x)) - a\alpha(x) + bx_2 + a\alpha(x) + b\beta(x) = \\ = cx_1\beta(x) - b(x_2 + \beta(x)) - a\alpha(x) - cx_2\alpha(x) + a\alpha(x) + \\ + bx_2 + b\beta(x) = c(x_1\beta(x) - x_2\alpha(x)) - b(x_2 + \beta(x)) +$$

$$+bx_2 + b\beta(x) = c(x_1\beta(x) - x_2\alpha(x)).$$

Використовуючи лівий дистрибутивний закон, маємо:

$$xy = (ax_1 + bx_2 + cx_3)y_1 + (a\alpha(x) + b\beta(x) + c\gamma(x))y_2 + (cx_1\beta(x) - x_2\alpha(x))y_3.$$

За лемою 2.9, маємо

$$\begin{aligned} (ax_1 + bx_2)y_1 &= ax_1y_1 + bx_2y_1 - cx_1x_2\binom{y_1}{2}, \\ (a\alpha(x) + b\beta(x))y_2 &= a\alpha(x)y_2 + b\beta(x)y_2 - \\ &\quad - c\alpha(x)\beta(x)\binom{y_2}{2} \end{aligned}$$

і

$$bx_2y_1 + a\alpha(x)y_2 = a\alpha(x)y_2 + bx_2y_1 - cx_2\alpha(x)y_1y_2.$$

Отже, використовуючи лівий дистрибутивний закон, отримуємо:

$$\begin{aligned} xy &= a(x_1y_1 + \alpha(x)y_2) + b(x_2y_1 + \beta(x)y_2) + c(-x_1x_2\binom{y_1}{2} - \\ &\quad - \alpha(x)\beta(x)\binom{y_2}{2} - x_2\alpha(x)y_1y_2 + x_3y_1 + \\ &\quad + \gamma(x)y_2 + x_1\beta(x)y_3 - x_2\alpha(x)y_3). \end{aligned}$$

З асоціативності множення в R випливає, що для всіх $x, y \in R$

$$(xy)b = x(yb). \quad (2.1)$$

Згідно з

$$xb = a\alpha(x) + b\beta(x) + c\gamma(x),$$

маємо

$$(xy)b = a\alpha(xy) + b\beta(xy) + c\gamma(xy) \quad (2.2)$$

і

$$yb = a\alpha(y) + b\beta(y) + c\gamma(y).$$

Підставляючи останнє рівняння в праву частину рівності 1), ми також маємо:

$$\begin{aligned}
 x(yb) = & a(x_1\alpha(y) + \alpha(x)\beta(y)) + b(x_2\alpha(y) + \beta(x)\beta(y)) + \\
 & + c(-x_1x_2\binom{\alpha(y)}{2} - \alpha(x)\beta(x)\binom{\beta(y)}{2} - \\
 & - x_2\alpha(x)\alpha(y)\beta(y) + x_3\alpha(y) + \gamma(x)\beta(y) + \\
 & + x_1\beta(x)\gamma(y) - x_2\alpha(x)\gamma(y)).
 \end{aligned} \tag{2.3}$$

Оскільки з рівності (2.1) випливає конгруентність відповідних коефіцієнтів у формулах (2.2) і (2.3), то отримуємо твердження (1)–(3). $\square$

2.4.2. Майже-кільця з одиницею, адитивна група яких ізоморфна G_3

Нехай R — майже-кільце з одиницею, яке не є майже-полем, адитивна група якого R^+ ізоморфна G_3 . Тоді $R^+ = \langle a \rangle + \langle b \rangle$ для деяких елементів a і b з R , що задовольняють відношення $ap^2 = 0$, $bp = 0$ та $b + a = a + b$. Зокрема, кожен елемент $x \in R$ однозначно записується у вигляді $x = ax_1 + bx_2$ з коефіцієнтами $0 \leq x_1 < p^2$ і $0 \leq x_2 < p$.

Без обмеження загальності можна 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 за модулями p^2 та p відповідно, що визначені такі відображення $\alpha : R \rightarrow \mathbb{Z}_{p^2}$ і $\beta : R \rightarrow \mathbb{Z}_p$.

Лема 2.12. *Нехай R — майже-кільце з одиницею, яке не є майже-полем, адитивна група якого R^+ ізоморфна G_3 . Якщо a співпадає з одиничним елементом R , $x = ax_1 + bx_2$, $y = ay_1 + by_2 \in R$, $xb = a\alpha(x) + b\beta(x)$, то*

$$xy = a(x_1y_1 + \alpha(x)y_2) + b(x_2y_1 + \beta(x)y_2). \tag{2.4}$$

Більш того, для відображень $\alpha: R \rightarrow \mathbb{Z}_{p^2}$ та $\beta: R \rightarrow \mathbb{Z}_p$ справедливі такі твердження:

- (0) $\alpha(0) = \beta(0) = 0$ тоді і тільки тоді, коли R є нуль-симетричним;
- (1) $\alpha(a) = 0$ і $\beta(a) = 1$;
- (2) $\alpha(xy) \equiv x_1\alpha(y) + \alpha(x)\beta(y) \pmod{p^2}$;
- (3) $\beta(xy) \equiv x_2\alpha(y) + \beta(x)\beta(y) \pmod{p}$.

Доведення. Оскільки $0 \cdot a = an \cdot 0 = 0$, то R є нуль-симетричним майже-кільцем 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 $b = ab = a\alpha(a) + b\beta(a)$, маємо $\alpha(a) = 0$ та $\beta(a) = 1$, тому мають місце твердження (0) та (1).

Далі, використовуючи лівий дистрибутивний закон, отримуємо

$$xy = (xa)y_1 + (xb)y_2 = (ax_1 + bx_2)y_1 + (a\alpha(x) + b\beta(x))y_2.$$

Також маємо

$$(ax_1 + bx_2)y_1 = ax_1y_1 + bx_2y_1$$

і

$$(a\alpha(x) + b\beta(x))y_2 = a\alpha(x)y_2 + b\beta(x)y_2.$$

Тому

$$xy = a(x_1y_1 + \alpha(x)y_2) + b(x_2y_1 + \beta(x)y_2)$$

і тому виконується твердження (2).

Нарешті, асоціативність множення в R означає, що

$$(xy)b = x(yb) = a\alpha(xy) + b\beta(xy).$$

Крім того, підставляючи $yb = a\alpha(y) + b\beta(y)$ замість y у формулу (2.4), також маємо

$$x(yb) = a(x_1\alpha(y) + \alpha(x)\beta(y)) + b(x_2\alpha(y) + \beta(x)\beta(y)).$$

Порівнюючи коефіцієнти при a та b у двох виразах, отриманих для $x(yb)$, отримуємо твердження (2) та (3) леми. $\square$

Висновки до розділу 2

У даному розділі:

- описано майже-кілець з одиницею на групах порядку p^3 ;
- наведено необхідні умови існування майже-кілець з одиницею на абелевих групах порядку p^3 ;
- наведено необхідні умови існування майже-кілець з одиницею на неабелевих групах порядку p^3 .

Основні результати даного розділу опубліковано у працях [12] зі списку публікацій і, відповідно, [95] зі списку використаних джерел, а також опубліковано у тезах конференцій [36, 29] і, відповідно, [83, 89].

Розділ 3

Локальні майже-кільця порядку p^3

В цьому розділі наведено основні означення та результати по локальним майже-кільцям. Отримано необхідні та достатні умови існування локальних майже-кілець з одиницею на групах порядку p^3 .

3.1. Про локальні майже-кільця

Означення 3.1. Майже-кільце R з одиницею називається локальним, якщо множина L всіх необоротних елементів із R утворює підгрупу адитивної групи R^+ . В цьому випадку L будемо називати підгрупою необоротних елементів майже-кільця R .

Скінченні локальні майже-кільця з циклічною підгрупою необоротних елементів описані в [5, теорема 1].

Теорема 3.2. 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 напівапрямому добутку двох циклічних підгруп порядків p та $p - 1$.

Як безпосередній наслідок теореми 3.2 маємо наступний результат.

Наслідок 3.3. *Нехай R є локальним майже-кільцем порядку p^3 , яке не є ізоморфним $\mathbb{Z}/p^3\mathbb{Z}$ або не є майже-полем. Тоді підгрупа необоротних елементів L є елементарною абелевою групою порядку p^2 .*

Наступна лема характеризує основні властивості скінченних локальних майже-кілець (див. [21], Lemma 3.2).

Лема 3.4. *Нехай R — локальне майже-кільце з одиницею i , а L — підгрупа всіх необоротних елементів R . Тоді справедливі такі твердження:*

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

В наступному твердженні встановлено порядки підгрупи необоротних елементів L [98, Corollary 1].

Лема 3.5. *Нехай R — локальне майже-кільце порядку p^4 з неабелевою адитивною групою та не є майже-полем. Тоді підгрупа необоротних елементів L є нециклічною групою порядку p^3 або p^2 .*

Визначимо біноміальний коефіцієнт $\binom{n}{k}$ цілих чисел n і k за формулою:

$$\binom{n}{k} = \begin{cases} \frac{n!}{k!(n-k)!}, & 0 \leq k \leq n; \\ 0, & k > n \text{ або } k < 0. \end{cases} \quad (3.1)$$

3.2. Локальні майже-кільця на елементарних абелевих групах порядку p^3

В статті [34] майже-кільця з одиницею, а тому і локальні, з циклічною адитивною групою повністю вивчені. Розглянемо елементарні абелеві групи порядку p^3 у якості адитивних груп локальних майже-кілець.

Наступне твердження містить класифікацію абелевих груп порядку p^3 (див. [16]).

Лема 3.6. *Нехай G — абелева група порядку p^3 . Далі наведено визначальні співвідношення всіх неізоморфних груп G .*

- 1) $a^{p^3} = 1$.
- 2) $a^{p^2} = 1, b^p = 1, ab = ba$.
- 3) $a^p = b^p = c^p = 1, ab = ba, ac = ca, cb = bc$.

Нехай $G(p, p, p)$ — група зі співвідношеннями 2) з леми 3.6.

Нехай R — локальне майже-кільце з адитивною групою R^+ , що ізоморфна групі $G(p, p, p)$, і не є майже-полем.

Зауважимо, що за наслідком 3.13 підгрупа необоротних елементів L адитивної групи R^+ локального майже-кільця R є елементарною абелевою порядку p^2 , тобто $|R : L| = p$.

Теорема 3.7. *Нехай R — локальне майже-кільце з адитивною групою R^+ , що ізоморфна групі $G(p, p, p)$, і не є майже-полем. Тоді*

$$R^+ = \langle a \rangle + \langle b \rangle + \langle c \rangle$$

для деяких $a, b, c \in R$, що задовольняють співвідношення $ap = bp = cp = 1, a + b = b + a, a + c = c + a, c + b = b + c$. Якщо a є одиницею в R , то $L = \langle b \rangle + \langle c \rangle$ та

$$R^* = \{ax_1 + bx_2 + cx_3 \mid x_1 \not\equiv 0 \pmod{p}\}.$$

Доведення. Якщо a є одиницею в R , то b та $c \in L$ за наслідком 3.13. Тоді $L = \langle b \rangle + \langle c \rangle$. Оскільки $R^* = R \setminus L$, та елемент

$$x = ax_1 + bx_2 + cx_3 \in R^*,$$

якщо і тільки якщо, $x_1 \not\equiv 0 \pmod{p}$. $\square$

Застосовуючи теорему 3.7, отримаємо наступну формулу множення для будь-яких двох елементів $x = ax_1 + bx_2 + cx_3$ та $y = ay_1 + by_2 + cy_3$ локального майже-кільця R .

Наслідок 3.8. *Якщо $x, y \in R$ $xb = b\beta(x) + c\gamma(x)$ та $xc = b\mu(x) + c\nu(x)$, то*

$$xy = ax_1y_1 + b(x_2y_1 + \beta(x)y_2 + \mu(x)y_3) + \\ + c(x_3y_1 + \gamma(x)y_2 + \nu(x)y_3),$$

причому для відображень $\alpha: R \rightarrow \mathbb{Z}_p$, $\beta: R \rightarrow \mathbb{Z}_p$, $\gamma: R \rightarrow \mathbb{Z}_p$, $\lambda: R \rightarrow \mathbb{Z}_p$, $\mu: R \rightarrow \mathbb{Z}_p$ та $\nu: R \rightarrow \mathbb{Z}_p$ виконуються наступні твердження:

- (0) $\beta(0) \equiv 0 \pmod{p}$, $\gamma(0) \equiv 0 \pmod{p}$, $\mu(0) \equiv 0 \pmod{p}$ та $\nu(0) \equiv 0 \pmod{p}$ тоді і тільки тоді, коли майже-кільце R є нуль-симетричним;
- (1) $\beta(a) = 1$, $\gamma(a) = 0$, $\mu(a) = 0$, $\nu(a) = 1 \pmod{p}$;
- (2) якщо $\beta(x) \equiv 0 \pmod{p}$ та $\mu(x) \equiv 0 \pmod{p}$, то $x_1 \equiv 0 \pmod{p}$;
- (3) $\beta(xy) \equiv \beta(x)\beta(y) + \mu(x)\gamma(y) \pmod{p}$;
- (4) $\gamma(xy) \equiv \gamma(x)\beta(y) + \nu(x)\gamma(y) \pmod{p}$;
- (6) $\mu(xy) \equiv \beta(x)\mu(y) + \mu(x)\nu(y) \pmod{p}$;
- (7) $\nu(xy) \equiv \gamma(x)\mu(y) + \nu(x)\nu(y) \pmod{p}$.

Очевидно, що функції $\beta(x)$ та $\mu(x)$ не залежать від коефіцієнта x_3 .

Маємо наступне твердження.

Лема 3.9. *Підгрупа $\langle c \rangle$ є ідеалом в локальному майже-кільці R .*

Доведення. Нехай $x = ax_1 + bx_2 + cx_3$, $y = ay_1 + by_2 + cy_3 \in R$, $z = cz_3 \in \langle c \rangle$. Перевіримо, чи буде $\langle c \rangle$ ідеалом в R , тобто

$$(z + x)y - xy \in \langle c \rangle.$$

Для цього скористаємося формулою множення елементів в R з наслідку 3.8,

$$\begin{aligned} xy &= ax_1y_1 + b(x_2y_1 + \beta(x)y_2 + \\ &+ \mu(x)y_3) + c(x_3y_1 + \gamma(x)y_2 + \nu(x)y_3). \end{aligned}$$

Маємо

$$\begin{aligned} (z + x)y - xy &= (cz_3 + ax_1 + bx_2 + cx_3)(ay_1 + by_2 + cy_3) - \\ &- (ax_1 + bx_2 + cx_3)(ay_1 + by_2 + cy_3) = (ax_1 + bx_2 + c(x_3 + \\ &+ z_3))(ay_1 + by_2 + cy_3) - (ax_1 + bx_2 + cx_3)(ay_1 + by_2 + cy_3) = \\ &= ax_1y_1 + b(x_2y_1 + \beta(z + x)y_2 + \mu(z + x)y_3) + c(x_3y_1 + \\ &+ \gamma(z + x)y_2 + \nu(z + x)y_3) - ax_1y_1 - b(x_2y_1 + \beta(x)y_2 + \\ &+ \mu(x)y_3) - c(x_3y_1 + \gamma(x)y_2 + \nu(x)y_3) = \\ &= c(y_2(\gamma(z + x) - \gamma(x)) + y_3(\nu(z + x) - \nu(x))) \in \langle c \rangle. \end{aligned}$$

Отже, $\langle c \rangle$ є ідеалом в R . □

Далі, наведемо приклади майже-кільцевого множення.

Лема 3.10. *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-кілець $R = (G, +, \cdot)$.

Маємо наступну теорему.

Теорема 3.11. *Існує щонайменше p неізоморфних локальних майже-кілець на елементарній абелевій групі порядку p^3 .*

Доведення. Оскільки нуль-симетричні локальні майже-кілеця порядку p^2 класифіковані в роботі [61], то й описані всі неізоморфні фактор-майже-кілеця $N = R / \langle c \rangle$. Тобто можна застосувати формулу множення з вказаної роботи, попередньо адаптувавши її для лівих локальних майже-кілець. Зрозуміло, що $N^+ = \langle a \rangle + \langle b \rangle$. А саме, нехай $x = ax_1 + bx_2$ та $y = ay_1 + by_2$ елементи майже-кілеця N , тоді

$$xy = ax_1y_1 + b(x_2y_1 + \rho(x_1)y_2),$$

де ρ приймає $p - 1$ значення для нуль-симетричних майже-кілець за [61, Theorem 1.6].

З іншого боку, за наслідком 3.8 маємо:

$$xy = ax_1y_1 + b(x_2y_1 + x_1\beta(x)y_2).$$

Прирівнявши коефіцієнти при твірних, отримаємо: $x_1\beta(x)y_2 = \rho(x_1)y_2$. Якщо $y_2 \not\equiv 0 \pmod{p}$, то $x_1\beta(x) = \rho(x_1)$. Звідки $\beta(x) = \rho(x_1)x_1^{-1}$. Якщо $y_2 \equiv 0 \pmod{p}$, то $xy = ax_1y_1 + bx_2y_1$.

Отже, існує $p - 1$ таких різних функцій $\beta(x)$.

Очевидно, що множення з леми 3.10 з функціями $\beta(x) = 1$ та $\nu(x) = 1$ є майже-кілецевим і визначає константне локальне майже-кілець, що завершує доведення. $\square$

3.2.1. Приклади локальних майже-кілець з елементарною абелевою адитивною групою порядку p^3

Дамо алгоритм побудови локального майже-кілеця з елементарною абелевою адитивною групою порядку 5^3 , що реалізовано в системі комп'ютерної алгебри GAP.

```
# В середовищі системи GAP завантажуюємо пакет LocalNR.
LoadPackage("LocalNR");
#  $G$  — група з IdGroup [125, 5].
 $G := SmallGroup(125, 5);$ 
#  $gen$  — список, що містить мінімальну систему твірних.
 $gen := MinimalGeneratingSet(G);$ 
# Повертаємо список з порядками твірних зі списку  $gen$ .
List( $gen$ , Order);
#  $a$  — перший елемент зі списку  $gen$ .
 $a := gen[1];$ 
#  $b$  — другий елемент зі списку  $gen$ .
 $b := gen[2];$ 
#  $c$  — третій елемент зі списку  $gen$ .
 $c := gen[3];$ 
#  $beta$  — функція, яка повертає значення  $x^2$  по  $mod\ 5$ .
 $beta := function(x)$ 
  return  $x^2 mod\ 5$ ; end;
 $nu := function(x)$ 
  return  $x^2 mod\ 5$ ; end;
#  $mulGR$  — функція майже-кілецевого добутку.
 $mulGR := function(x, y)$ 
  local  $x1, x2, x3, y1, y2, y3$ ;
```

```

for x1 in [0..4] do
for x2 in [0..4] do
for x3 in [0..4] do
for y1 in [0..4] do
for y2 in [0..4] do
for y3 in [0..4] do
if x = a^x1 * b^x2 * c^x3 and y = a^y1 * b^y2 * c^y3 then return
a^(x1 * y1) * b^(x2 * y1 + beta(x1) * y2) * c^(x3 * y1 + nu(x1) * y3); fi;
od; od; od; od; od; od; end;
# n — майже-кільце на групі G та з множенням mulGR (без перевірки).
n := ExplicitMultiplicationNearRingNC(G, mulGR);
# M — таблиця множення майже-кільця n.
M := MultiplicationTable(n);
# mul — майже-кільцеве множення, що отримано за допомогою таблиці M.
mul :=
NearRingMultiplicationByOperationTable(G, M, AsSortedList(G));
# n — майже-кільце на групі G та з множенням mul (з перевіркою).
n := ExplicitMultiplicationNearRing(G, mul);

```

З побудованих прикладів з пакетів SONATA та LocalNR маємо наступну кількість локальних майже-кілець з досліджуваними характеристиками, що не є майже-поллями:

Адитивна група	Кількість неізоморфних локальних майже-кілець
$C_2 \times C_2 \times C_2$	6
$C_3 \times C_3 \times C_3$	12
$C_5 \times C_5 \times C_5$	29
$C_7 \times C_7 \times C_7$	46
$C_{11} \times C_{11} \times C_{11}$	96

3.3. Локальні майже-кілеця на неабелевих групах порядку p^3

Далі позначимо через G_1 групу зі співвідношеннями 5*) твердження 2.1, G_2 групу зі співвідношеннями 4*) твердження 2.1, G_3 групу зі співвідношеннями 2) твердження 2.1.

Позначимо через $n(G)$ кількість усіх неізоморфних локальних майже-кілець на групі G .

3.3.1. Локальні майже-кілеця, адитивні групи яких ізоморфні G_1

Нехай R — локальне майже-кілеце, адитивна група якого R^+ ізоморфна G_1 . Тоді $R^+ = \langle a \rangle + \langle b \rangle + \langle c \rangle$ для деяких елементів a, b і c з R , що задовольняють співвідношення $ap = 0$, $bp = 0$, $cp = 0$, $a + b = b + a + c$, $a + c = c + a$ і $b + c = c + b$. Зокрема, кожен елемент $x \in R$ однозначно записується у вигляді $x = ax_1 + bx_2 + cx_3$ з коефіцієнтами $0 \leq x_1 < p$, $0 \leq x_2 < p$ і $0 \leq x_3 < p$.

Оскільки порядок елемента a дорівнює експоненті групи G , то за ле-

мою 2.2 можна вважати, 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 $\alpha(x)$, $\beta(x)$ і $\gamma(x)$, що

$$xb = a\alpha(x) + b\beta(x) + c\gamma(x).$$

Зрозуміло, що вони так однозначно визначені за модулем p , що визначені деякі відображення $\alpha : R \rightarrow \mathbb{Z}_p$, $\beta : R \rightarrow \mathbb{Z}_p$ і $\gamma : R \rightarrow \mathbb{Z}_p$.

Згідно з наслідком 3.5, L є нормальною підгрупою порядку p^2 в R . Оскільки L містить комутатор R^+ , то випливає, що $L = \langle b \rangle + \langle c \rangle$ і підгрупа $\langle c \rangle$ є центром в R^+ . Оскільки $R^* = R \setminus L$, то випливає

$$R^* = \{ax_1 + bx_2 + cx_3 \mid x_1 \not\equiv 0 \pmod{p}\}$$

і $x = ax_1 + bx_2 + cx_3$ є оборотним тоді і тільки тоді, коли $x_1 \not\equiv 0 \pmod{p}$.

Локальні майже-кільця на неметациклічних групах Міллера–Морено були вивчені в статтях [12] і [73]. Леми 3.12 та 3.18 базуються на результатах цих робіт.

Лема 3.12. *Нехай R — локальне майже-кільце, адитивна група якого дорівнює G_1 з одиницею a . Якщо $x = ax_1 + bx_2 + cx_3$, $y = ay_1 + by_2 + cy_3 \in R$,*

$$xb = a\alpha(x) + b\beta(x) + c\gamma(x),$$

то

$$\begin{aligned} x \cdot y = & ax_1y_1 + b(x_2y_1 + \beta(x)y_2) + \\ & + c(-x_1x_2\binom{y_1}{2} + x_3y_1 + \gamma(x)y_2 + x_1\beta(x)y_3). \end{aligned} \quad (3.2)$$

Більш того, для відображень $\beta : R \rightarrow \mathbb{Z}_p$ і $\gamma : R \rightarrow \mathbb{Z}_p$ мають місце наступні твердження:

(0) $\alpha(0) \equiv 0 \pmod{p}$, $\beta(0) \equiv 0 \pmod{p}$ і $\gamma(0) \equiv 0 \pmod{p}$ *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) $\beta(xy) \equiv \beta(x)\beta(y) \pmod{p}$;
- (4) $\gamma(xy) \equiv \gamma(x)\beta(y) + x_1\beta(x)\gamma(y) \pmod{p}$.

Доведення. Оскільки $L = \langle b \rangle + \langle c \rangle$ і $L \in (R, R)$ -підгрупою в R^+ згідно з твердженням 1) леми 3.4 випливає, що $xb \in L$, отже, $a\alpha(x) \in L$ для кожного $x \in R$. Таким чином $\alpha(x) \equiv 0 \pmod{p}$ і маємо твердження (1). Підставляючи отримане значення $\alpha(x) \equiv 0 \pmod{p}$ у формули з леми 2.11 отримуємо твердження (3) та (4) леми та формулу для добутку xy . Покладемо $y = c$, маємо $xc = c(x_1\beta(x))$. Отже, якщо $\beta(x) \equiv 0 \pmod{p}$, тоді $xc = 0$, і так $x \in L$. Отже, $x_1 \equiv 0 \pmod{p}$, як вказано в твердженні (2). Дійсно, твердження (0) повторює твердження (0) леми 2.11. $\square$

Відомо, що для таких груп комутатор $D(R^+)$ збігається з центром $Z(R^+)$ та має порядок p .

Лема 3.13. *Комутатор $D(R^+)$ є ідеалом у локальному майже-кільці R .*

Доведення. Нехай $x = ax_1 + bx_2 + cx_3$, $y = ay_1 + by_2 + cy_3 \in R$, $z = cz_3 \in D(R^+)$. Перевіримо, чи є $D(R^+)$ ідеалом у R , тобто

$$(z + x)y - xy \in D(R^+).$$

Для цього ми використовуємо формулу (3.2) для множення елементів з R . Отримуємо

$$\begin{aligned} (z + x)y - xy &= (cz_3 + ax_1 + bx_2 + cx_3)(ay_1 + by_2 + cy_3) - \\ &- (ax_1 + bx_2 + cx_3)(ay_1 + by_2 + cy_3) = (ax_1 + bx_2 + c(x_3 + z_3))(ay_1 + \end{aligned}$$

$$\begin{aligned}
& +by_2 + cy_3) - (ax_1 + bx_2 + cx_3)(ay_1 + by_2 + cy_3) = ax_1y_1 + \\
& +b(x_2y_1 + \beta(x)y_2) + c(-x_1x_2\binom{y_1}{2} + x_3y_1 + z_3y_1 + \gamma(z+x)y_2 + \\
& +x_1\beta(x)y_3) - ax_1y_1 - b(x_2y_1 + \beta(x)y_2) - c(-x_1x_2\binom{y_1}{2} + x_3y_1 + \\
& +\gamma(x)y_2 + x_1\beta(x)y_3) = ax_1y_1 + b(x_2y_1 + \beta(x)y_2) - ax_1y_1 - b(x_2y_1 + \\
& +\beta(x)y_2) + c(z_3y_1 + (\gamma(z+x) - \gamma(x))y_2) = ax_1y_1 - ax_1y_1 + b(x_2y_1 + \\
& +\beta(x)y_2) - c(x_1y_1(x_2y_1 + \beta(x)y_2)) - b(x_2y_1 + \beta(x)y_2) + c(z_3y_1 + \\
& +(\gamma(z+x) - \gamma(x))y_2) = c(z_3y_1 + (\gamma(z+x) - \gamma(x))y_2 - x_1x_2y_1^2 - \\
& -x_1y_1y_2\beta(x)) \in D(R^+).
\end{aligned}$$

Отже, $D(R^+)$ є ідеалом R . □

Лема 3.14. *Нехай R — локальне майже-кільце, адитивна група якого R^+ ізоморфна G_1 . Якщо $x = ax_1 + bx_2 + cx_3$, $y = ay_1 + by_2 + cy_3 \in R$, то відображення $\beta: R \rightarrow \mathbb{Z}_{p^2}$ і $\gamma: R \rightarrow \mathbb{Z}_p$ з (3.2) може бути одним із наступних:*

- 1) $\beta(x) = x_1^i$ і $\gamma(x) = 0$ ($0 < i < p$);
- 2) $\beta(x) = 1$ і $\gamma(x) = 0$;
- 3) $\beta(x) = x_1^2$ і $\gamma(x) = x_1x_2$.

Доведення. 1) Оскільки нуль-симетричні локальні майже-кільця порядку p^2 класифіковано в [61], то описано всі неізоморфні фактор-майже-кільця по комутаторній підгрупі $N = R/D(R^+)$. Тобто, можна застосувати формулу множення із зазначеної роботи, попередньо адаптувавши її для лівих локальних майже-кілець. Зрозуміло, що $N^+ = \langle a \rangle + \langle b \rangle$. А саме, нехай $x = ax_1 + bx_2$ і $y = ay_1 + by_2$ є елементами N , тоді

$$xy = ax_1y_1 + b(x_2y_1 + \rho(x_1)y_2).$$

Більш того, у [61, Theorem 1.6] і [61, Corollary 1.11] було показано, що існують, з точністю до ізоморфізму, $p - 1$ локальні майже-кільця (які не є майже-поллями) з адитивною групою порядку p^2 та експонентою p . Ці локальні майже-кільця повністю визначаються такими відображеннями $\rho: \mathbb{Z}_p \rightarrow \mathbb{Z}_p$, що (i) $\rho(x) = 0$ тоді і тільки тоді, коли $x = 0$ і (ii) ρ є груповим ендоморфізмом $(\mathbb{Z}_p - \{0\}, \cdot)$ [57]. Отже, ρ приймає одне з $p - 1$ значень для нуль-симетричних майже-кілець.

З іншого боку, за формулою (3.2) маємо:

$$xy = ax_1y_1 + b(x_2y_1 + \beta(x)y_2).$$

Прирівнюючи коефіцієнти для твірних, отримуємо: $\beta(x)y_2 = \rho(x_1)y_2$. Звідси, $\beta(x) = \rho(x_1)$. Отже, існує $p - 1$ різних нуль-симетричних майже-кілець.

2) Очевидно, що множення (3.2) з функціями $\beta(x) = 1$ та $\gamma(x) = 0$ є константним майже-кільцевим множенням.

3) Далі покажемо, що для $\beta(x) = x_1^2$ та $\gamma(x) = x_1x_2$ множення (3.2), тобто

$$\begin{aligned} x * y = & ax_1y_1 + b(x_2y_1 + x_1^2y_2) + c(-x_1x_2 \binom{y_1}{2} + \\ & + x_3y_1 + x_1x_2y_2 + x_1^3y_3) \end{aligned}$$

є майже-кільцевим множенням. За лемою 3.12 (3) і (4), функції $\beta(x)$ та $\gamma(x)$ повинні задовольняти такі умови: $\beta(xy) = \beta(x)\beta(y)$ і

$$\gamma(xy) = \beta(y)\gamma(x) + x_1\beta(x)\gamma(y).$$

Перевіряємо, що

$$\beta(xy) = (x_1y_1)^2 = x_1^2y_1^2 = \beta(x)\beta(y)$$

і

$$\gamma(xy) = x_1y_1(x_2y_1 + x_1y_2) = x_1x_2y_1^2 + x_1^2y_1y_2 =$$

$$= \beta(y)\gamma(x) + x_1\beta(x)\gamma(y).$$

Отже, $\beta(x)$ і $\gamma(x)$ задовольняють умови (3) та (4) леми 3.12.

Легко побачити, що елемент a є мультиплікативною одиницею для $(R, *)$ і $x * b = bx_1^2 + cx_1x_2$ для кожного $x \in R$. Покажемо, що відносно операцій “+” and “*” система $(R, +, *)$ є майже-кільцем з одиничним елементом a . Очевидно, що достатньо перевірити, що якщо $z = az_1 + bz_2 + cz_3$ є довільним елементом R , тоді $x * (y + z) = x * y + x * z$ і $(x * y) * b = x * (y * b)$.

Дійсно, маємо

$$\begin{aligned} x * z &= ax_1z_1 + b(x_2z_1 + x_1^2z_2) + c(-x_1x_2\binom{z_1}{2} + \\ &\quad + x_3z_1 + x_1x_2z_2 + x_1^3z_3) \end{aligned}$$

і

$$\begin{aligned} &b(x_2y_1 + x_1^2y_2) + a(x_1z_1) = a(x_1z_1) + \\ &+ b(x_2y_1 + x_1^2y_2) - c(x_1z_1(x_2y_1 + x_1^2y_2)) \end{aligned}$$

за лемою 2.8. Отримуємо

$$\begin{aligned} x * y + x * z &= \\ &a(x_1y_1 + x_1z_1) + b(x_2y_1 + x_1^2y_2 + x_2z_1 + x_1^2z_2) + \\ &+ c(-x_1x_2\binom{y_1}{2}) + x_3y_1 + x_1x_2y_2 + x_1^3y_3 - \\ &- x_1x_2\binom{z_1}{2} + x_3z_1 + x_1x_2z_2 + x_1^3z_3 - x_1z_1(x_2y_1 + x_1^2y_2) = \\ &= ax_1(y_1 + z_1) + b(x_2(y_1 + z_1) + x_1^2(y_2 + z_2)) + \\ &+ c(-x_1x_2\binom{(y_1 + z_1)}{2}) + x_3(y_1 + z_1) + \\ &+ x_1x_2(y_2 + z_2) + x_1^3(y_3 + z_3 - z_1y_2)). \end{aligned}$$

З іншого боку,

$$\begin{aligned} y + z &= (ay_1 + by_2 + cy_3) + (az_1 + bz_2 + cz_3) = \\ &= a(y_1 + z_1) + b(y_2 + z_2) + c(y_3 + z_3 - z_1y_2) \end{aligned}$$

тому, що

$$by_2 + az_1 = az_1 + by_2 - cz_1y_2$$

за лемою 2.8. Тому

$$\begin{aligned} x * (y + z) &= ax_1(y_1 + z_1) + b(x_2(y_1 + z_1) + x_1^2(y_2 + z_2)) + \\ &+ c(-x_1x_2 \binom{(y_1 + z_1)}{2} + x_3(y_1 + z_1) + x_1x_2(y_2 + \\ &+ z_2) + x_1^3(y_3 + z_3 - z_1y_2)). \end{aligned}$$

Отже, $x * (y + z) = x * y + x * z$, як і вимагалось.

Далі, $y * b = by_1^2 + cy_1y_2$ і тому

$$\begin{aligned} x * (y * b) &= b(x_1^2y_1^2) + c(x_1x_2y_1^2 + x_1^3y_1y_2) = \\ &= b(x_1y_1)^2 + c(x_1x_2(x_2y_1 + x_1^2y_2)). \end{aligned}$$

З іншого боку,

$$\begin{aligned} (x * y) * b &= (ax_1y_1 + b(x_2y_1 + x_1^2y_2) + c(-x_1x_2 \binom{y_1}{2} + \\ &+ x_3y_1 + x_1x_2y_2 + x_1^3y_3)) * b = b(x_1y_1)^2 + \\ &+ c(x_1x_2(x_2y_1 + x_1^2y_2)) = x * (y * b). \end{aligned}$$

Таким чином, система $(R, +, *)$ є майже-кільцевим множенням з одиничним елементом a , а отже, множення “ $*$ ” є майже-кільцевим множенням, як і стверджувалося. $\square$

Отже, маємо приклади $p+1$ майже-кільцевих добутоків і формулюємо наступний результат.

Теорема 3.15. *На кожній неметациклічній неабелевій групі порядку p^3 існує щонайменше $p + 1$ неізоморфних локальних майже-кілець.*

Доведення. Майже-кілець $R = (R, +, \cdot)$ з функціями $\beta(x) = x_1^i$ та $\gamma(x) = 0$ ($0 < i < p$) є неізоморфними нуль-симетричними локальними майже-кілецями згідно з вищезазначеним та статтею [61]. Легко перевірити, що локальні майже-кілець $R = (R, +, \cdot)$ з функціями $\beta(x) = 1$ та $\gamma(x) = 0$ є ненуль-симетричними. Очевидно, що $R = (R, +, \cdot)$ з функціями $\beta(x) = x_1^2$ та $\gamma(x) = x_1x_2$ є нуль-симетричними та неізоморфними майже-кілецям, розглянутим вище. Отже, існує щонайменше $p + 1$ неізоморфних локальних майже-кілець на кожній неметациклічній неабелевій групі порядку p^3 . $\square$

Приклад 3.16. Нехай $G \cong (C_5 \times C_5) \rtimes C_5$. Якщо $x = ax_1 + bx_2 + cx_3$ і $y = ay_1 + by_2 + cy_3 \in G$, та $(G, +, \cdot)$ є локальним майже-кілецем, тоді за лемою 6.15 “ $\cdot$ ” є одним із наступних добутків.

- (1) $x \cdot y = ax_1y_1 + b(x_2y_1 + y_2) + c(-x_1x_2\binom{y_1}{2} + x_3y_1 + x_1y_3);$
- (2) $x \cdot y = ax_1y_1 + b(x_2y_1 + x_1^3(x)y_2) + c(-x_1x_2\binom{y_1}{2} + x_3y_1 + x_1x_2y_2 + x_1^4y_3);$
- (3) $x \cdot y = ax_1y_1 + b(x_2y_1 + x_1y_2) + c(-x_1x_2\binom{y_1}{2} + x_3y_1 + x_1^2y_3);$
- (4) $x \cdot y = ax_1y_1 + b(x_2y_1 + x_1^2y_2) + c(-x_1x_2\binom{y_1}{2} + x_3y_1 + x_1^3y_3);$
- (5) $x \cdot y = ax_1y_1 + b(x_2y_1 + x_1^3(x)y_2) + c(-x_1x_2\binom{y_1}{2} + x_3y_1 + x_1^4y_3);$
- (6) $x \cdot y = ax_1y_1 + b(x_2y_1 + x_1^4y_2) + c(-x_1x_2\binom{y_1}{2} + x_3y_1 + x_1^5y_3).$

Комп’ютерна програма, яка підтвердила, що для $p = 5$ майже-кілець, отримане в Lemma 6.15 (3), справді є локальним майже-кілецем (див. приклад 3.16 (2)), розміщена на GitHub:

https://github.com/raemarina/Examples/blob/main/LNR_125-3.txt

Далі, наведемо цю програму.

```

# В середовищі системи GAP завантажуюємо пакет LocalNR.
LoadPackage("LocalNR");
#  $G$  — група з IdGroup [125, 3].
 $G := SmallGroup(125, 3)$ ;
#  $gen$  — список, що містить мінімальну систему твірних.
 $gen := MinimalGeneratingSet(G)$ ;
# Повертаємо список з порядками твірних зі списку  $gen$ .
List( $gen$ , Order);
#  $a$  — перший елемент зі списку  $gen$ .
 $a := gen[1]$ ;
#  $b$  — другий елемент зі списку  $gen$ .
 $b := gen[2]$ ;
#  $c$  — комутатор елементів  $a$  та  $b$ .
 $c := a^{\wedge} - 1 * b^{\wedge} - 1 * a * b$ ;
#  $gamma$  — функція, яка повертає значення  $2 * x * y$ .
 $gamma := function(x, y)$ 
  return  $2 * x * y$ ; end;
#  $beta$  — функція, яка повертає значення  $x^{\wedge}2$ .
 $beta := function(x)$ 
  return  $x^{\wedge}2$ ; end;
#  $mulGR$  — функція майже-кільцевого добутку.
 $mulGR := function(x, y)$ 
  local  $x1, x2, x3, y1, y2, y3$ ;
  for  $x1$  in [0..4] do
    for  $x2$  in [0..4] do
      for  $x3$  in [0..4] do
        for  $y1$  in [0..4] do
          for  $y2$  in [0..4] do
            for  $y3$  in [0..4] do

```

```

    if  $x = a^{\wedge}x1 * b^{\wedge}x2 * c^{\wedge}x3$  and  $y = a^{\wedge}y1 * b^{\wedge}y2 * c^{\wedge}y3$  then return
     $a^{\wedge}(x1 * y1) * b^{\wedge}(x2 * y1 + \text{beta}(x1) * y2) * c^{\wedge}(\text{gamma}(x1, x2) * y2 - x1 * x2 * \text{Binomial}(y1, 2) + x3 * y1 + x1 * \text{beta}(x1) * y3); fi;$ 
    od; od; od; od; od; od; end;

    #  $n$  — майже-кільце на групі  $G$  та з множенням  $mulGR$  (без перевірки).
     $n := \text{ExplicitMultiplicationNearRingNC}(G, mulGR);$ 
    #  $M$  — таблиця множення майже-кільця  $n$ .
     $M := \text{MultiplicationTable}(n);;$ 
    #  $mul$  — майже-кільцеве множення, що отримано за допомогою таблиці  $M$ .
     $mu_N R :=$ 
     $\text{NearRingMultiplicationByOperationTable}(G, M, \text{AsSortedList}(G));$ 
    #  $n$  — майже-кільце на групі  $G$  та з множенням  $mul$  (з перевіркою).
     $n := \text{ExplicitMultiplicationNearRing}(G, mu_N R);$ 
    # Перевірка, чи є майже-кільце  $n$  локальним.
     $\text{IsLocalNearRing}(n);$ 

```

З пакетів SONATA та LocalNR маємо наступну кількість неізоморфних локальних майже-кілець.

$StructureDescription(R^+)$	$n(R^+)$
$(C_3 \times C_3) \rtimes C_3$	4
$(C_5 \times C_5) \rtimes C_5$	6
$(C_7 \times C_7) \rtimes C_7$	8
$(C_{11} \times C_{11}) \rtimes C_{11}$	12

3.3.2. Локальні майже-кільця, адитивні групи яких ізоморфні G_2

Нехай R — локальне майже-кільце, адитивна група якого R^+ ізоморфна G_2 . Тоді $R^+ = \langle a \rangle + \langle b \rangle$ для деяких елементів a та b множини R , що задовольняють співвідношення $ap^2 = 0$, $bp = 0$ та $-b + a + b = a(1 + p)$. Зокрема, кожен елемент $x \in R$ однозначно записується у вигляді $x = ax_1 + bx_2$ з коефіцієнтами $0 \leq x_1 < p^2$ і $0 \leq x_2 < p$.

Згідно з [54, Теорема 7.1] для $p = 3$ існують три нуль-симетричні майже-кільця з одиницею на G_2 , а для $p > 3$ одне. Водночас, згідно з [54, Теорема 4.2], існує одне ненуль-симетричне майже-кільце з одиницею на G_2 . З іншого боку, в [63] було показано, що для кожної групи G_2 існує нуль-симетричне локальне майже-кільце. За допомогою бібліотеки майже-кільць SONATA легко переконатися, що всі майже-кільця з одиницею на G_2 порядку 27 є локальними. Формула для множення елементів локальних майже-кільць на метациклічних групах Міллера–Морено визначена в [102]. Оскільки G_2 є метациклічною групою Міллера–Морено, використовуючи [102, Collary 2], для довільних елементів $x = ax_1 + bx_2$ та $y = ay_1 + by_2$ групи G_2 та покладаючи $\alpha(x) = 0$ та $\beta(x) = 1$, отримуємо наступну формулу множення:

$$x \cdot y = a(x_1y_1 - x_1x_2 \binom{y_1}{2} p) + b(x_2y_1 + y_2). \quad (3.3)$$

Легко бачити, що $R = (G_2, +, \cdot)$ є ненуль-симетричним локальним майже-кільцем.

Формула множення довільних елементів нуль-симетричного локального майже-кільця на G_2 наведена при доведенні [102, Theorem 2], а саме:

$$x \cdot y = a(x_1y_1 - x_1x_2 \binom{y_1}{2} p) + b(x_2y_1 + \beta(x)y_2), \quad (3.4)$$

де

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

Отже, з результатів, представлених у цьому розділі, маємо:

- 1) $n(G_2) = 4$ для $p = 3$;
- 2) $n(G_2) = 2$ для $p > 3$. Більш того, формули множення в таких майже-кільцях визначаються формулами (3.3) чи (3.4).

Нехай адитивно записані групи типу H мають скінченне представлення у вигляді

$$\langle a, b | ap^k, bp, -b + a + b - a(1 + p^{k-1}) \rangle,$$

де $k \geq 2$ і p є простим (див. [54]).

Кількість неізоморфних майже-кілець з одиницею на групах типу H наведено в [54]. Очевидно, що для $k = 2$ та $p > 2$ група типу H буде ізоморфною групі G_2 .

Як зазначалося вище, на всіх абелевих групах існують локальні майже-кільця. Також, згідно з [12] і [54], існують локальні майже-кільця на G_1 і G_2 , відповідно. Отже, маємо наступний результат.

Твердження 3.17. *На кожній групі порядку p^3 з $p > 2$ існує локальне майже-кільце.*

3.3.3. Локальні майже-кільця, адитивні групи яких ізоморфні G_3

Нехай R — локальне майже-кільце, яке не є майже-полем, адитивна група якого R^+ ізоморфна G_3 . Тоді $R^+ = \langle a \rangle + \langle b \rangle$ для деяких елементів a і b з R , що задовольняють відношення $ap^2 = 0$, $bp = 0$ та $b + a = a + b$.

Зокрема, кожен елемент $x \in R$ однозначно записується у вигляді $x = ax_1 + bx_2$ з коефіцієнтами $0 \leq x_1 < p^2$ і $0 \leq x_2 < p$.

Без обмеження загальності можна 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 за модулями p^2 та p відповідно, що визначені такі відображення $\alpha : R \rightarrow \mathbb{Z}_{p^2}$ і $\beta : R \rightarrow \mathbb{Z}_p$.

Лема 3.18. *Нехай R — локальне майже-кільце, яке не є майже-полем, адитивна група якого R^+ ізоморфна G_3 . Якщо a співпадає з одиничним елементом R , $x = ax_1 + bx_2$, $y = ay_1 + by_2 \in R$, $xb = a\alpha(x) + b\beta(x)$, то*

$$xy = a(x_1y_1 + \alpha(x)y_2) + b(x_2y_1 + \beta(x)y_2). \quad (3.5)$$

Більш того, для відображень $\alpha : R \rightarrow \mathbb{Z}_{p^2}$ та $\beta : R \rightarrow \mathbb{Z}_p$ справедливі такі твердження:

- (0) $\alpha(0) = \beta(0) = 0$ тоді і тільки тоді, коли R є нуль-симетричним;
- (1) $\alpha(a) = 0$ і $\beta(a) = 1$;
- (2) $\alpha(x) \equiv 0 \pmod{p}$;
- (3) $\alpha(xy) \equiv x_1\alpha(y) + \alpha(x)\beta(y) \pmod{p^2}$;
- (4) $\beta(xy) \equiv \beta(x)\beta(y) \pmod{p}$.

Доведення. Оскільки $0 \cdot a = ap \cdot 0 = 0$, то R є нуль-симетричним майже-кільцем 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 $b = ab = a\alpha(a) + b\beta(a)$, маємо $\alpha(a) = 0$ та $\beta(a) = 1$, тому мають місце твердження (0) та (1).

Далі, використовуючи лівий дистрибутивний закон, отримуємо

$$xy = (xa)y_1 + (xb)y_2 = (ax_1 + bx_2)y_1 + (a\alpha(x) + b\beta(x))y_2.$$

Також маємо

$$(ax_1 + bx_2)y_1 = ax_1y_1 + bx_2y_1$$

і

$$(a\alpha(x) + b\beta(x))y_2 = a\alpha(x)y_2 + b\beta(x)y_2.$$

Тому

$$xy = a(x_1y_1 + \alpha(x)y_2) + b(x_2y_1 + \beta(x)y_2)$$

і тому виконується твердження (2).

Згідно з наслідком 3.5 $L = \langle ap \rangle + \langle b \rangle$. Оскільки $xL \subseteq L$ для кожного $x \in R$ за лемою 3.4, маємо

$$xb = a\alpha(x) + b\beta(x) \in L,$$

звідки $\alpha(x) \equiv 0 \pmod{p}$ для кожного $x \in R$.

Нарешті, асоціативність множення в R означає, що

$$(xy)b = x(yb) = a\alpha(xy) + b\beta(xy).$$

Крім того, підставляючи $yb = a\alpha(y) + b\beta(y)$ замість y у формулу (3.5), також маємо

$$x(yb) = a(x_1\alpha(y) + \alpha(x)\beta(y)) + b(x_2\alpha(y) + \beta(x)\beta(y)).$$

Оскільки $\alpha(y) \equiv 0 \pmod{p}$, то

$$x(yb) = a(x_1\alpha(y) + \alpha(x)\beta(y)) + b(\beta(x)\beta(y)).$$

Порівнюючи коефіцієнти при a та b у двох виразах, отриманих для $x(yb)$, отримуємо твердження (3) та (4) леми. $\square$

Лема 3.19. $\langle ap \rangle$ є ідеалом в R .

Доведення. Нехай $x = ax_1 + bx_2$, $y = ay_1 + by_2 \in R$, $z = apz_1 \in \langle ap \rangle$.
Перевіримо, чи є $\langle ap \rangle$ ідеалом в R , тобто

$$(z + x)y - xy \in \langle ap \rangle.$$

Використавши формулу (3.5), маємо

$$\begin{aligned} (z + x)y - xy &= (apz_1 + ax_1 + bx_2)(ay_1 + by_2) - \\ &- (ax_1 + bx_2)(ay_1 + by_2) = (a(pz_1 + x_1) + bx_2)(ay_1 + \\ &+ by_2) - (ax_1 + bx_2)(ay_1 + by_2) = a((pz_1 + x_1)y_1 + \\ &+ \alpha(z + x)y_2) + b(x_2y_1 + \beta(z + x)y_2) - \\ &- (a(z_1y_1 + \alpha(x)y_2) + b(x_2y_1 + \beta(x)y_2)) = \\ &= a(pz_1y_1 + (\alpha(z + x) - \alpha(x))y_2) + b(\beta(z + x) - \beta(x))y_2 = \\ &= a(pz_1y_1 + (\alpha(z + x) - \alpha(x))y_2) \in \langle ap \rangle, \end{aligned}$$

оскільки $\beta(z + x) - \beta(x) = 0$.

Отже, $\langle ap \rangle$ є ідеалом в R . □

Лема 3.20. Нехай R — локальне майже-кільце, яке не є майже-полем, адитивна група якого R^+ ізоморфна G_3 . Якщо $x = ax_1 + bx_2$, $y = ay_1 + by_2 \in R$, то відображення $\alpha: R \rightarrow \mathbb{Z}_{p^2}$ і $\beta: R \rightarrow \mathbb{Z}_p$ з (3.5) може бути одним із наступних:

- (1) $\alpha(x) = 0$ і $\beta(x) = x_1^i \pmod{p}$ ($0 < i < p$);
- (2) $\alpha(x) = 0$ і $\beta(x) = 1$;
- (3) $\alpha(x) = px_2$ і $\beta(x) \equiv x_1 \pmod{p}$.

Доведення. 1) Оскільки нуль-симетричні локальні майже-кільця порядку p^2 класифіковано в [61], то описано всі неізоморфні фактор-майже-кільця з комутаторною підгрупою $N = R/\langle ap \rangle$. Тобто, можна застосувати формулу множення із зазначеної роботи, попередньо адаптувавши

її для лівих локальних майже-кілець. Зрозуміло, що $N^+ = \langle \bar{a} \rangle + \langle \bar{b} \rangle$. А саме, нехай $\bar{x} = \bar{a}x_1 + \bar{b}x_2$ і $\bar{y} = \bar{a}y_1 + \bar{b}y_2$ є елементами в N , тоді

$$\overline{xy} = \bar{a}x_1y_1 + \bar{b}(x_2y_1 + \rho(x_1)y_2).$$

Більш того, згідно з [61, Теорема 1.6] ρ приймає одне з $p - 1$ значень для нуль-симетричних майже-кілець.

З іншого боку, за формулою (3.5) маємо

$$\overline{xy} = \bar{a}x_1y_1 + \bar{b}(x_2y_1 + \beta(x)y_2).$$

Прирівнюючи коефіцієнти для твірних, отримуємо: $\beta(x)y_2 = \rho(x_1)y_2$. Звідси, $\beta(x) = \rho(x_1)$. Отже, існує $p - 1$ різних нуль-симетричних майже-кілець.

2) Очевидно, що множення (3.5) з функціями $\alpha(x) = 0$ і $\beta(x) = 1$ є константним майже-кільцевим множенням.

3) Прямою перевіркою умов (3) та (4) леми 3.18 для $\alpha(x) = px_2$ і $\beta(x) \equiv x_1 \pmod{p}$ множення (3.5), доводимо лему. $\square$

Отже, маємо приклади $p + 1$ майже-кільцевих добутоків і формулюємо наступний результат.

Теорема 3.21. *На кожній метациклічній абелевій групі порядку p^3 існує щонайменше $p + 1$ неізоморфних локальних майже-кілець.*

Доведення. Майже-кільця $R = (R, +, \cdot)$ з функціями $\alpha(x) = 0$ та $\beta(x) = x_1^i \pmod{p}$ ($0 < i < p$) є неізоморфними нуль-симетричними локальними майже-кільцями згідно з вищезазначеним та статтею [61]. Легко перевірити, що локальне майже-кільце $R = (R, +, \cdot)$ з функціями $\alpha(x) = 0$ and $\beta(x) = 1$ є ненуль-симетричним.

Давайте розглянемо $R = (R, +, \cdot)$ з функціями $\alpha(x) = px_2$ і $\beta(x) \equiv x_1 \pmod{p}$. У цьому випадку маємо

$$|\{xb = apx_2 + bx_1 | x \in R\}| = p^2$$

і R є нуль-симетричним. Наприклад, у вищезгаданому випадку з $\alpha(x) = 0$ і $\beta(x) = x_1 \pmod{p}$ отримуємо $|\{xb = bx_1 | x \in R\}| = p$, і тому R є неізоморфними майже-кільцям, розглянутим вище. Отже, на кожній метациклічній абелевій групі порядку p^3 існує щонайменше $p + 1$ неізоморфних локальних майже-кілець. $\square$

З пакетів SONATA та LocalNR маємо наступну кількість неізоморфних локальних майже-кілець.

$StructureDescription(R^+)$	$n(R^+)$
$C_9 \times C_3$	13
$C_{25} \times C_5$	31
$C_{49} \times C_7$	31
$C_{121} \times C_{11}$	47

Сформулюємо теорему, в якій проаналізовано існування та кількість неізоморфних локальних майже-кілець на групах порядку p^3 .

Теорема 3.22. *Мають місце наступні твердження.*

1. *Існує одне неізоморфне локальне майже-кільце на циклічній групі (типу 1)) порядку p^3 , яку є комутативним кільцем.*
2. *Існує щонайменше $p + 1$ неізоморфних локальних майже-кілець на кожній метациклічній абелевій групі (типу 2)) порядку p^3 .*
3. *Існує щонайменше p неізоморфних локальних майже-кілець на елементарній абелевій групі (типу 3)) порядку p^3 .*
4. *Не існує локальних майже-кілець на групі діедра порядку 8.*
5. *Не існує локальних майже-кілець на групі кватерніонів порядку 8.*

- 4*.** 1) Існує 4 неізоморфних локальних майже-кілець на метациклічній неабелевій групі порядку p^3 з $p = 3$;
- 2) існує 2 неізоморфних локальних майже-кілець на метациклічній неабелевій групі порядку p^3 з $p > 3$.
- 5*.** Існує щонайменше $p + 1$ неізоморфних локальних майже-кілець на кожній неметациклічній неабелевій групі (типу 5*) порядку p^3 .

Доведення. 1. Як наслідок того, що з точністю до ізоморфізму існує єдине майже-кілець з одиницею, адитивна група якого циклічна, і яке фактично є комутативним кільцем (див. [34, Theorem 1 and Corollary]).

2. Доведено в [95, Theorem 3].
3. Доведено в [9, Теорема 4].
4. Показано в [63, Introduction].
5. Як наслідок того, що не існує майже-кілець з одиницею на групі кватерніонів порядку 8 (див. [31, Subsection 5.1]).
- 4*. Доведено в [54, Theorem 7.1] і підрозділі 5 статті [95].
- 5*. Доведено в [95, Theorem 2].

□

Висновки до розділу 3

У даному розділі:

- досліджено локальні майже-кілець з адитивними групами порядку p^3 ;
- визначено формули множення для таких майже-кілець та описано функції, що їх задають;

- описано приклад локального майже-кілля з адитивною групою порядку p^3 ;
- дано оцінку нижньої межі кількості локальних майже-кілля на групах порядку p^3 ;
- наведено алгоритм побудови локального майже-кілля з елементарною абелевою адитивною групою порядку 5^3 , що реалізовано в системі комп'ютерної алгебри GAP;
- проаналізовано існування та кількість неізоморфних локальних майже-кілля на групах порядку p^3 .

Основні результати даного розділу опубліковано у працях [13, 12] зі списку публікацій і, відповідно, [9, 95] зі списку використаних джерел, а також опубліковано у тезах конференцій [37, 34, 33, 32] і, відповідно, [10, 74, 84, 87].

Розділ 4

Майже-кільця з одиницею порядків p^4

У даному розділі вивчаються майже-кільця з одиницею порядків p^4 .

4.1. Групи порядку p^4

Групи порядку p^4 з $p > 3$ описано в такій теоремі (див., наприклад, [20], [28]).

Теорема 4.1. *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:

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

4.2. Майже-кільця на групах класу нільпотентності 2

Розглянемо групи класу нільпотентності 2 порядку p^4 .

Нехай $[n, i]$ — i -та група порядку n в бібліотеці SmallGroups library системи комп'ютерної алгебри GAP. Позначимо через C_n циклічну групу порядку n .

За допомогою GAP можна отримати таке твердження.

Зауваження 4.2. Існують групи 6 класу нільпотентності 2 порядку $2^4 = 16$, а саме:

1. $(C_4 \times C_2) \rtimes C_2$ [16, 3];
2. $C_4 \rtimes C_4$ [16, 4];

3. $C_8 \rtimes C_2$ [16, 6];
4. $C_2 \times D_8$ [16, 11];
5. $C_2 \times Q_8$ [16, 12];
6. $(C_4 \times C_2) \rtimes C_2$ [16, 13].

4.2.1. Група G_4

Нехай G_4 — адитивно записана група з теореми 4.1. Тоді $G_4 = \langle a \rangle + \langle b \rangle + \langle c \rangle + \langle d \rangle$ для деяких елементів a, b, c і d з R , що задовольняють співвідношення $ap = 0, bp = 0, cp = 0, dp = 0, a+b = b+a+c, a+c = c+a, b+c = c+b, a+d = d+a, b+d = d+b$ і $c+d = d+c$.

Лема 4.3. Для довільних цілих чисел k і l з групи G_4 мають місце рівності $-ak - bl + ak + bl = c(kl)$ і $bl + ak = -c(kl) + ak + bl$.

Доведення. Оскільки $-a - b + a + b = c$, маємо $-b + a + b = a + c$. Тоді

$$-bl + ak + bl = (a + cl)k = ak + c(kl).$$

Отже, $-ak - bl + ak + bl = c(kl)$, і тому $bl + ak = -c(kl) + ak + bl$. $\square$

Лема 4.4. Для будь-яких натуральних чисел k, l, n, m і r з групи G_4 має місце рівність

$$(ak + bl + cm + dn)r = a(kr) + b(lr) + c(mr - kl \binom{r}{2}) + d(nr).$$

Доведення. Доведення проведемо індукцією по r . Для $r = 1$ виконується рівність. Нехай для r виконується рівність, тобто

$$(ak + bl + cm + dn)r = a(kr) + b(lr) + c(mr - kl \binom{r}{2}) + d(nr).$$

Доведемо рівність для $r + 1$:

$$\begin{aligned}
 & (ak + bl + cm + dn)(r + 1) = \\
 & = a(kr) + b(lr) + ak + bl + c(kl \binom{r}{2}) + c(m(r + 1)) + \\
 & + d(n(r + 1)) = a(k(r + 1)) + b(l(r + 1)) + c(-klr) + \\
 & + c(-kl \binom{r}{2}) + c(m(r + 1)) + d(n(r + 1)) = a(k(r + 1)) + \\
 & + b(l(r + 1)) + c(m(r + 1) - kl(r + \binom{r}{2})) + d(n(r + 1)) = \\
 & = a(k(r + 1)) + b(l(r + 1)) + c(m(r + 1) - kl \binom{r + 1}{2}) + \\
 & + dn(r + 1).
 \end{aligned}$$

Отже, рівність справедлива для будь-якого r . □

4.2.2. Майже-кільця з одиницею, адитивні групи яких ізоморфні G_4

Нехай R — майже-кільце з одиницею адитивна група R^+ якого ізоморфна групі G_4 . Тоді

$$R^+ = \langle a \rangle + \langle b \rangle + \langle c \rangle + \langle d \rangle$$

для деяких елементів a, b, c і d з R задовольняють співвідношення $ap = 0$, $bp = 0$, $cp = 0$, $dp = 0$, $a + b = b + a + c$, $a + c = c + a$, $b + c = c + b$, $a + d = d + a$, $b + d = d + b$ і $c + d = d + c$. Зокрема, кожен елемент $x \in R$ єдиним чином записаний у вигляді $x = ax_1 + bx_2 + cx_3 + dx_4$ з коефіцієнтами $0 \leq x_1 < p$, $0 \leq x_2 < p$, $0 \leq x_3 < p$ і $0 \leq x_4 < p$.

Оскільки порядок елемента a рівний експоненті групи G , то за ле-
мою 2.2 можна 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
 $\alpha(x)$, $\beta(x)$, $\gamma(x)$, $\varphi(x)$, $\lambda(x)$, $\mu(x)$, $\nu(x)$ і $\psi(x)$, що

$$xb = a\alpha(x) + b\beta(x) + c\gamma(x) + d\varphi(x)$$

і

$$xd = a\lambda(x) + b\mu(x) + c\nu(x) + d\psi(x).$$

Зрозуміло, що вони однозначно визначені так по модулю p , що визначе-
ні деякі відображення $\alpha: R \rightarrow \mathbb{Z}_p$, $\beta: R \rightarrow \mathbb{Z}_p$, $\gamma: R \rightarrow \mathbb{Z}_p$, $\varphi: R \rightarrow \mathbb{Z}_p$,
 $\lambda: R \rightarrow \mathbb{Z}_p$, $\mu: R \rightarrow \mathbb{Z}_p$, $\nu: R \rightarrow \mathbb{Z}_p$ і $\psi: R \rightarrow \mathbb{Z}_p$.

Лема 4.5. *Нехай R — майже-кільце з одиницею адитивна група R^+
якого ізоморфна групі G_4 . Якщо a співпадає з одиничним елементом в
 R , $x = ax_1 + bx_2 + cx_3 + dx_4$, $y = ay_1 + by_2 + cy_3 + dy_4 \in R$,*

$$xb = a\alpha(x) + b\beta(x) + c\gamma(x) + d\varphi(x)$$

і

$$xd = a\lambda(x) + b\mu(x) + c\nu(x) + d\psi(x),$$

то

$$\begin{aligned} xy = & a(x_1y_1 + \alpha(x)y_2 + \lambda(x)y_4) + b(x_2y_1 + \beta(x)y_2 + \mu(x)y_4) + \\ & + c(-x_1x_2\binom{y_1}{2} - \alpha(x)\beta(x)\binom{y_2}{2} - x_2\alpha(x)y_1y_2 - \lambda(x)\mu(x)\binom{y_4}{2} - \\ & - x_2\alpha(x)y_3 + x_3y_1 + \gamma(x)y_2 + x_1\beta(x)y_3 + \nu(x)y_4) + d(x_4y_1 + \\ & + \varphi(x)y_2 + \psi(x)y_4). \end{aligned}$$

Більш того, для відображень

$\alpha: R \rightarrow \mathbb{Z}_p$, $\beta: R \rightarrow \mathbb{Z}_p$, $\gamma: R \rightarrow \mathbb{Z}_p$, $\varphi: R \rightarrow \mathbb{Z}_p$, $\lambda: R \rightarrow \mathbb{Z}_p$, $\mu: R \rightarrow \mathbb{Z}_p$,
 $\nu: R \rightarrow \mathbb{Z}_p$ і $\psi: R \rightarrow \mathbb{Z}_p$ виконуються наступні твердження:

$$(0) \quad \alpha(0) \equiv 0 \pmod{p}, \beta(0) \equiv 0 \pmod{p}, \gamma(0) \equiv 0 \pmod{p};$$

$$\varphi(0) \equiv 0 \pmod{p}, \lambda(0) \equiv 0 \pmod{p}, \mu(0) \equiv 0 \pmod{p},$$

$\nu(0) \equiv 0 \pmod{p}$ і $\psi(0) \equiv 0 \pmod{p}$ тоді й лише тоді, коли майже-кільце R є нуль-симетричним;

$$(1) \quad \alpha(xy) \equiv x_1\alpha(y) + \alpha(x)\beta(y) + \lambda(x)\varphi(y) \pmod{p};$$

$$(2) \quad \beta(xy) \equiv x_2\alpha(y) + \beta(x)\beta(y) + \mu(x)\varphi(y) \pmod{p};$$

$$(3) \quad \gamma(xy) \equiv -x_1x_2\binom{\alpha(y)}{2} - \alpha(x)\beta(x)\binom{\beta(y)}{2} - x_2\alpha(x)\alpha(y)\beta(y) - \\ - \lambda(x)\mu(x)\binom{\varphi(y)}{2} - x_2\alpha(x)\gamma(y) + x_3\alpha(y) + \gamma(x)\beta(y) + \\ + x_1\beta(x)\gamma(y) + \nu(x)\varphi(y) \pmod{p};$$

$$(4) \quad \varphi(xy) \equiv x_4\alpha(y) + \varphi(x)\beta(y) + \psi(x)\varphi(y) \pmod{p};$$

$$(5) \quad \lambda(xy) \equiv x_1\lambda(y) + \alpha(x)\mu(y) + \lambda(x)\psi(y) \pmod{p};$$

$$(6) \quad \mu(xy) \equiv x_2\lambda(y) + \beta(x)\mu(y) + \mu(x)\psi(y) \pmod{p};$$

$$(7) \quad \nu(xy) \equiv -x_1x_2\binom{\lambda(y)}{2} - \alpha(x)\beta(x)\binom{\mu(y)}{2} - x_2\alpha(x)\lambda(y)\mu(y) - \\ - \lambda(x)\mu(x)\binom{\psi(y)}{2} - x_2\alpha(x)\nu(y) + x_3\lambda(y) + \gamma(x)\mu(y) + \\ + x_1\beta(x)\nu(y) + \nu(x)\psi(y) \pmod{p};$$

$$(8) \quad \psi(xy) \equiv x_4\lambda(y) + \varphi(x)\mu(y) + \psi(x)\psi(y) \pmod{p}.$$

Доведення. Оскільки $0 \cdot a = a \cdot 0 = 0$, звідси випливає, що R є нуль-симетричним майже-кільцем тоді й лише тоді, коли

$$0 = 0 \cdot b = a\alpha(0) + b\beta(0) + c\gamma(0) + d\varphi(0)$$

i

$$0 = 0 \cdot d = a\lambda(0) + b\mu(0) + c\nu(0) + d\psi(0).$$

Еквівалентно маємо $\alpha(0) \equiv 0 \pmod{p}$, $\beta(0) \equiv 0 \pmod{p}$, $\gamma(0) \equiv 0 \pmod{p}$, $\varphi(0) \equiv 0 \pmod{p}$, $\lambda(0) \equiv 0 \pmod{p}$, $\mu(0) \equiv 0 \pmod{p}$, $\nu(0) \equiv 0 \pmod{p}$ і $\psi(0) \equiv 0 \pmod{p}$.

Навіть більше, якщо $c = -a - b + a + b$ і ліво-дистрибутивний закон маємо

$$0 \cdot c = -0 \cdot a - 0 \cdot b + 0 \cdot a + 0 \cdot b = 0,$$

звідки

$$\begin{aligned} 0 \cdot x &= 0 \cdot (ax_1 + bx_2 + cx_3 + dx_4) = \\ &= (0 \cdot a)x_1 + (0 \cdot b)x_2 + (0 \cdot c)x_3 + (0 \cdot d)x_4 = 0. \end{aligned}$$

Отже, виконується це твердження (0).

Далі, використовуючи лему 4.3, отримуємо

$$\begin{aligned} xc &= -xa - xb + xa + xb = -cx_3 - bx_2 - ax_1 - c\gamma(x) - \\ &- b\beta(x) - a\alpha(x) + ax_1 + bx_2 + cx_3 + a\alpha(x) + b\beta(x) + c\gamma(x) = \\ &= -bx_2 - ax_1 - b\beta(x) - a\alpha(x) + ax_1 + bx_2 + a\alpha(x) + b\beta(x) = \\ &= -bx_2 + cx_1\beta(x) - b\beta(x) - ax_1 - a(\alpha(x) - x_1) + bx_2 + a\alpha(x) + \\ &+ b\beta(x) = cx_1\beta(x) - b(x_2 + \beta(x)) - a\alpha(x) + bx_2 + a\alpha(x) + \\ &+ b\beta(x) = cx_1\beta(x) - b(x_2 + \beta(x)) - a\alpha(x) - cx_2\alpha(x) + \\ &+ a\alpha(x) + bx_2 + b\beta(x) = c(x_1\beta(x) - x_2\alpha(x)) - b(x_2 + \beta(x)) + \\ &+ bx_2 + b\beta(x) = c(x_1\beta(x) - x_2\alpha(x)). \end{aligned}$$

Далі, використовуючи ліво-дистрибутивний закон маємо

$$\begin{aligned} xy &= (ax_1 + bx_2 + cx_3 + dx_4)y_1 + (a\alpha(x) + b\beta(x) + c\gamma(x) + \\ &+ d\varphi(x))y_2 + (c(x_1\beta(x) - x_2\alpha(x)))y_3 + \end{aligned}$$

$$+(a\lambda(x) + b\mu(x) + c\nu(x) + d\psi(x))y_4.$$

За лемою 4.4, отримуємо

$$\begin{aligned} (ax_1 + bx_2 + cx_3 + dx_4)y_1 &= ax_1y_1 + bx_2y_1 + \\ &+ c(x_3y_1 - x_1x_2\binom{y_1}{2}) + dx_4y_1, \\ (a\alpha(x) + b\beta(x) + c\gamma(x) + d\varphi(x))y_2 &= a\alpha(x)y_2 + b\beta(x)y_2 + \\ &+ c(\gamma(x)y_2 - \alpha(x)\beta(x)\binom{y_2}{2}) + d\varphi(x)y_2, \\ (a\lambda(x) + b\mu(x) + c\nu(x) + d\psi(x))y_4 &= a\lambda(x)y_4 + b\mu(x)y_4 + \\ &+ c(\nu(x)y_4 - \lambda(x)\mu(x)\binom{y_4}{2}) + d\psi(x)y_4. \end{aligned}$$

За лемою 4.4, маємо

$$bx_2y_1 + a\alpha(x)y_2 = a\alpha(x)y_2 + bx_2y_1 - cx_2\alpha(x)y_1y_2,$$

і

$$b\beta(x)y_2 + a\lambda(x)y_4 = a\lambda(x)y_4 + b\beta(x)y_2 - c\lambda(x)\beta(x)y_2y_4.$$

Звідси і використовуючи ліво-дистрибутивний закон маємо

$$\begin{aligned} xy &= a(x_1y_1 + \alpha(x)y_2 + \lambda(x)y_4) + b(x_2y_1 + \beta(x)y_2 + \mu(x)y_4) + \\ &+ c(-x_1x_2\binom{y_1}{2} - \alpha(x)\beta(x)\binom{y_2}{2} - x_2\alpha(x)y_1y_2 - \lambda(x)\mu(x)\binom{y_4}{2}) - \\ &- x_2\alpha(x)y_3 + x_3y_1 + \gamma(x)y_2 + x_1\beta(x)y_3 + \nu(x)y_4 + d(x_4y_1 + \\ &+ \varphi(x)y_2 + \psi(x)y_4). \end{aligned}$$

З асоціативності множення в R випливає, що для всіх $x, y \in R$

$$(xy)b = x(yb) \tag{4.1}$$

і

$$(xy)d = x(yd). \tag{4.2}$$

Згідно з

$$xb = a\alpha(x) + b\beta(x) + c\gamma(x) + d\varphi(x),$$

отримуємо

$$(xy)b = a\alpha(xy) + b\beta(xy) + c\gamma(xy) + d\varphi(xy) \quad (4.3)$$

і

$$yb = a\alpha(y) + b\beta(y) + c\gamma(y) + d\varphi(y).$$

Підстановка останнього рівняння в праву частину рівності 1), також маємо

$$\begin{aligned} x(yb) = & a(x_1\alpha(y) + \alpha(x)\beta(y) + \lambda(x)\varphi(y)) + b(x_2\alpha(y) + \\ & + \beta(x)\beta(y) + \mu(x)\varphi(y)) + c(-x_1x_2\binom{\alpha(y)}{2} - \\ & - \alpha(x)\beta(x)\binom{\beta(y)}{2} - x_2\alpha(x)\alpha(y)\beta(y) - \lambda(x)\mu(x)\binom{\varphi(y)}{2} - \\ & - x_2\alpha(x)\gamma(y) + x_3\alpha(y) + \gamma(x)\beta(y) + x_1\beta(x)\gamma(y) + \nu(x)\varphi(y)) + \\ & + d(x_4\alpha(y) + \varphi(x)\beta(y) + \psi(x)\varphi(y)). \end{aligned} \quad (4.4)$$

Оскільки з рівності (4.1) випливає конгруентність відповідних коефіцієнтів у формулах (4.3) і (4.4), отримуємо твердження (1)–(4).

Далі, згідно з

$$xd = a\lambda(x) + b\mu(x) + c\nu(x) + d\psi(x)$$

замість y в рівності (4.2), отримуємо

$$(xy)d = a\lambda(xy) + b\mu(xy) + c\nu(xy) + d\psi(xy) \quad (4.5)$$

і

$$yd = a\lambda(y) + b\mu(y) + c\nu(y) + d\psi(y).$$

Підстановка останнього рівняння в праву частину рівності 2), також маємо

$$x(yd) = a(x_1\lambda(y) + \alpha(x)\mu(y) + \lambda(x)\psi(y)) + b(x_2\lambda(y) + \quad (4.6)$$

$$\begin{aligned}
& +\beta(x)\mu(y) + \mu(x)\psi(y)) + c(-x_1x_2\binom{\lambda(y)}{2} - \\
& -\alpha(x)\beta(x)\binom{\mu(y)}{2} - x_2\alpha(x)\lambda(y)\mu(y) - \lambda(x)\mu(x)\binom{\psi(y)}{2} - \\
& -x_2\alpha(x)\nu(y) + x_3\lambda(y) + \gamma(x)\mu(y) + x_1\beta(x)\nu(y) + \\
& +\nu(x)\psi(y)) + d(x_4\lambda(y) + \varphi(x)\mu(y) + \psi(x)\psi(y)).
\end{aligned}$$

Нарешті, порівнюючи коефіцієнти біля a , b , c і d в формулах (4.5) і (4.6), отримуємо твердження (5)–(8) з леми. $\square$

4.2.3. Група G_5

Нехай G_5 — адитивно записана група з теореми 4.1. Тоді $G_5 = \langle a \rangle + \langle b \rangle + \langle c \rangle$ для деяких елементів a , b і c з R задовольняють співвідношення $ap^2 = bp = cp = 0$, $a + b = b + a(1 - p)$, $a + c = c + a$ і $b + c = c + b$.

Нагадаємо, що експонентою скінченної p -групи є максимальний порядок її елементів. Легко перевірити наступне твердження.

Лема 4.6. *Якщо x елемент максимального порядку G_5 , то існують такі твірні a , b і c цієї групи, що $a = x$ і виконуються співвідношення $ap^2 = bp = cp = 0$, $-b + a + b = a(1 - p)$, $a + c = c + a$, $b + c = c + b$.*

Лема 4.7. *Для будь-яких натуральних чисел k , r , s і t групи G_5 виконуються рівності*

$$ck + bs + ar = ar(1 + sp) + bs + ck$$

і

$$(ar + bs + ck)t = ar(t + s\binom{t}{2}p) + bst + ckt.$$

Доведення. Нехай $q = 1 + p$. Оскільки $-b + a + b = a(1 - p)$, $a + c = c + a$ і $b + c = c + b$ з цього випливає, що $c + b + a = aq + b + c$, тому

$$ck + bs + ar = arq^s + bs + ck$$

для довільних цілих чисел $k \geq 0$, $r \geq 0$ і $s \geq 0$. Беручи до уваги, що

$$q^s = (1 + p)^s \equiv 1 + sp \pmod{p^2}$$

за формулою бінома, що дає

$$ck + bs + ar = ar(1 + sp) + bs + ck.$$

Далі,

$$(ar + bs + ck)t = ar(1 + q^s + \dots + q^{s(t-1)}) + bst + ckt$$

за індукцією по t . Тому,

$$\begin{aligned} 1 + q^s + \dots + q^{s(t-1)} &\equiv 1 + (1 + sp) + \dots + (1 + s(t-1)p) = \\ &= t + s \binom{t}{2} p \pmod{p^2}, \end{aligned}$$

а, отже,

$$(ar + bs + ckt)t = ar(t + s \binom{t}{2} p) + bst + ckt.$$

□

4.2.4. Майже-кільця з одиницею адитивна група яких ізоморфна групі G_5

Нехай R майже-кільце з одиницею адитивна група R^+ якого ізоморфна групі G_5 . Тоді $R^+ = \langle a \rangle + \langle b \rangle + \langle c \rangle$ з елементами a , b і c , де a співпадає з одиничним елементом в R і виконуються співвідношення

$ap^2 = bp = cp = 0$, $a + b = b + a(1 - p)$, $a + c = c + a$, $b + c = c + b$.
Навіть більше, кожен елемент $x \in R$ однозначно записується у вигляді $x = ax_1 + bx_2 + cx_3$ з коефіцієнтами $0 \leq x_1 < p^2$, $0 \leq x_2 < p$ і $0 \leq x_3 < p$.

Розглянемо, що a співпадає з одиничним елементом R , так що $xa = ax = x$ для кожного $x \in R$. Крім того, для кожного $x \in R$ існують такі цілі числа $\alpha(x)$, $\beta(x)$, $\gamma(x)$, $\nu(x)$, $\mu(x)$ і $\phi(x)$, що

$$xb = a\alpha(x) + b\beta(x) + c\gamma(x)$$

і

$$xc = a\nu(x) + b\mu(x) + c\phi(x).$$

Зрозуміло, що за модулем p^2 , p , p і p^2 , p , p , відповідно, ці цілі однозначно визначаються x і тому визначені деякі відображення $\alpha: R \rightarrow \mathbb{Z}_{p^2}$, $\beta: R \rightarrow \mathbb{Z}_p$, $\gamma: R \rightarrow \mathbb{Z}_p$, $\nu: R \rightarrow \mathbb{Z}_{p^2}$, $\mu: R \rightarrow \mathbb{Z}_p$ і $\phi: R \rightarrow \mathbb{Z}_p$.

Лема 4.8. *Нехай $x = ax_1 + bx_2 + cx_3$ і $y = ay_1 + by_2 + cy_3$ елементи з R . Якщо a збігається з одиницею R , то*

$$\begin{aligned} xy = & a(x_1y_1 + \alpha(x)y_2 + x_1x_2\binom{y_1}{2}p + \nu(x)y_3) + \\ & + b(x_2y_1 + \beta(x)y_2 + \mu(x)y_3) + c(x_3y_1 + \gamma(x)y_2 + \phi(x)y_3). \end{aligned} \quad (4.7)$$

Більш того, для відображень

$\alpha: R \rightarrow \mathbb{Z}_{p^2}$, $\beta: R \rightarrow \mathbb{Z}_p$, $\gamma: R \rightarrow \mathbb{Z}_p$, $\nu: R \rightarrow \mathbb{Z}_{p^2}$, $\mu: R \rightarrow \mathbb{Z}_p$ та $\phi: R \rightarrow \mathbb{Z}_p$ мають місце наступні твердження:

(0) $\alpha(0) = \beta(0) = \gamma(0) = \nu(0) = \mu(0) = \phi(0) = 0$ тоді і тільки тоді, коли майже-кілець R є нуль-симетричним;

(1) $\alpha(a) = 0$, $\beta(a) = 1$, $\gamma(a) = 0$, $\nu(c) = 0$, $\mu(c) = 0$ і $\phi(c) = 1$;

(2) $\alpha(x) \equiv 0 \pmod{p}$ та $\nu(x) \equiv 0 \pmod{p}$;

(3) $\alpha(xy) = x_1\alpha(y) + \alpha(x)\beta(y) + x_1x_2\binom{\alpha(y)}{2}p + \nu(x)\gamma(y) \pmod{p^2}$;

$$(4) \quad \beta(xy) = x_2\alpha(y) + \beta(x)\beta(y) + \mu(x)\gamma(y) \pmod{p};$$

$$(5) \quad \gamma(xy) = x_3\alpha(y) + \gamma(x)\beta(y) + \phi(x)\gamma(y) \pmod{p};$$

$$(6) \quad \nu(xy) = x_1\nu(y) + \alpha(x)\mu(y) + x_1x_2\binom{\mu(y)}{2}p + \nu(x)\phi(y) \pmod{p^2};$$

$$(7) \quad \mu(xy) = x_2\nu(y) + \beta(x)\mu(y) + \mu(x)\phi(y) \pmod{p};$$

$$(8) \quad \phi(xy) = x_3\nu(y) + \gamma(x)\mu(y) + \phi(x)\phi(y) \pmod{p}.$$

Доведення. За ліво-дистрибутивним законом маємо

$$\begin{aligned} xy &= (xa)y_1 + (xb)y_2 + (xc)y_3 = (ax_1 + bx_2 + cx_3)y_1 + (a\alpha(x) + \\ &\quad + b\beta(x) + c\gamma(x))y_2 + (a\nu(x) + b\mu(x) + c\phi(x))y_3. \end{aligned}$$

Крім того, з леми 4.7 випливає, що

$$\begin{aligned} (ax_1 + bx_2 + cx_3)y_1 &= ax_1(y_1 + x_2\binom{y_1}{2}p) + bx_2y_1 + cx_3y_1, \\ (a\alpha(x) + b\beta(x) + c\gamma(x))y_2 &= \\ &= a\alpha(x)(y_2 + \beta(x)\binom{y_2}{2}p) + b\beta(x)y_2 + c\gamma(x)y_2, \end{aligned}$$

i

$$\begin{aligned} (a\nu(x) + b\mu(x) + c\phi(x))y_3 &= \\ &= a\nu(x)(y_3 + \mu(x)\binom{y_3}{2}p) + b\mu(x)y_3 + c\phi(x)y_3. \end{aligned}$$

За лемою 4.7 маємо

$$\begin{aligned} bx_2y_1 + a\alpha(x)(y_2 + \beta(x)\binom{y_2}{2}p) &= \\ &= a\alpha(x)(y_2 - \beta(x)\binom{y_2}{2}p)(1 - x_2y_1p) + bx_2y_1 \end{aligned}$$

i

$$b\beta(x)y_2 + a\nu(x)(y_3 + \mu(x)\binom{y_3}{2}p) =$$

$$= a\nu(x)(y_2 - \mu(x)\binom{y_2}{2}p)(1 - \beta(x)y_2) + b\beta(x)y_2.$$

Таким чином, ми отримуємо

$$\begin{aligned} xy = & a((x_1y_1 + \alpha(x)y_2) + (x_1x_2\binom{y_1}{2} + \alpha(x)y_2 + \alpha(x)x_2y_1y_2p + \\ & + \alpha(x)\beta(x)\binom{y_2}{2})p + \nu(x)y_3 + \nu(x)x_2y_1y_2p + \nu(x)\beta(x)y_2y_3p + \\ & + \nu(x)\mu(x)\binom{y_3}{2}p) + b(x_2y_1 + \beta(x)y_2 + \mu(x)y_3) + \\ & + c(x_3y_1 + \gamma(x)y_2 + \phi(x)y_3). \end{aligned}$$

Оскільки $0 \cdot a = a \cdot 0 = 0$, майже-кільце R є нуль-симетричним тоді і тільки тоді, коли

$$0 = 0 \cdot b = a\alpha(0) + b\beta(0) + c\gamma(0)$$

і

$$0 = 0 \cdot c = a\nu(0) + b\mu(0) + c\phi(0).$$

Звідки

$$\alpha(0) = \beta(0) = \gamma(0) = \nu(0) = \mu(0) = \phi(0) = 0.$$

Так само, з рівностей

$$b = ab = a\alpha(a) + b\beta(a)$$

і

$$c = ac = a\nu(c) + b\mu(c) + c\phi(c)$$

випливає, що $\alpha(a) = 0$, $\beta(a) = 1$, $\gamma(a) = 0$, $\nu(c) = 0$, $\mu(c) = 0$ і $\phi(c) = 1$, отримуємо твердження (1). Оскільки $(xb)p = x(bp) = 0$ і

$$xb = a\alpha(x) + b\beta(x) + c\gamma(x),$$

маємо

$$0 = (a\alpha(x) + b\beta(x) + c\gamma(x))p = a\alpha(x)(p + \beta(x)\binom{p}{2}p) = a\alpha(x)p$$

за лемою 4.7 і, отже, $\alpha(x) \equiv 0 \pmod{p}$. Більш того, $(xc)p = x(cp) = 0$ і

$$xc = a\nu(x) + b\mu(x) + c\phi(x),$$

маємо

$$0 = (a\nu(x) + b\mu(x) + c\phi(x))p = a\nu(x)(p + \mu(x)\binom{p}{2}) = a\nu(x)p$$

за лемою 4.7 і, отже, $\nu(x) \equiv 0 \pmod{p}$, і тому твердження (2). Тому отримуємо

$$\begin{aligned} xy &= a(x_1y_1 + \alpha(x)y_2 + x_1x_2\binom{y_1}{2}p + \nu(x)y_3) + \\ &+ b(x_2y_1 + \beta(x)y_2 + \mu(x)y_3) + c(x_3y_1 + \gamma(x)y_2 + \phi(x)y_3), \end{aligned}$$

як вимагалось в (4.7).

Нарешті, асоціативність множення в R означає, що

$$x(yb) = (xy)b = a\alpha(xy) + b\beta(xy) + c\gamma(xy)$$

і

$$x(yc) = (xy)c = a\nu(xy) + b\mu(xy) + c\phi(xy).$$

Крім того, заміна

$$yb = a\alpha(y) + b\beta(y) + c\gamma(y)$$

замість y в формулі (4.7), також маємо

$$\begin{aligned} x(yb) &= a(x_1\alpha(y) + \alpha(x)\beta(y) + x_1x_2\binom{\alpha(y)}{2}p + \nu(x)\gamma(y)) + \\ &+ b(x_2\alpha(y) + \beta(x)\beta(y) + \mu(x)\gamma(y)) + c(x_3\alpha(y) + \\ &+ \gamma(x)\beta(y) + \phi(x)\gamma(y)). \end{aligned}$$

Порівнюючи коефіцієнти при a і b у двох виразах, отриманих для $x(yb)$, отримуємо твердження (3)–(5) леми.

Далі, підстановка

$$yc = a\nu(y) + b\mu(y) + c\phi(y)$$

замість y в формулі (4.7), отримуємо

$$\begin{aligned} x(yc) = & a((x_1\nu(y) + \alpha(x)\mu(y) + x_1x_2\binom{\mu(y)}{2}p + \nu(x)\phi(y)) + \\ & + b(x_2\nu(y) + \beta(x)\mu(y) + \mu(x)\phi(y)) + c(x_3\nu(y) + \\ & + \gamma(x)\mu(y) + \phi(x)\phi(y)). \end{aligned}$$

Нарешті, порівнюючи коефіцієнти під a і b у двох виразах, отриманих для $x(yc)$, отримуємо твердження (6)–(8) леми. $\square$

4.3. Майже-кільця на групах класу нільпотентності 3

Ми розглянемо групи класу нільпотентності 3 порядку p^4 .

Це легка вправа, наприклад, у GAP, щоб отримати наступні твердження.

Зауваження 4.9. Існують 3 неізоморфні групи класу нільпотентності 3 порядку $2^4 = 16$, які є:

1. D_{16} [16, 7];
2. QD_{16} [16, 8];
3. Q_{16} [16, 9].

Зауваження 4.10. Існують 4 неізоморфні групи класу нільпотентності 3 порядку $3^4 = 81$, які є:

1. $(C_3 \times C_3 \times C_3) \rtimes C_3$ [81, 7];
2. $(C_9 \times C_3) \rtimes C_3$ [81, 8];
3. $(C_9 \rtimes C_3) \rtimes C_3$ [81, 9];
4. $(C_9 \rtimes C_3) \rtimes C_3$ [81, 10].

За допомогою пакетів SONATA та LocalNR можна перевірити наступне твердження (див., наприклад, [29]).

Теорема 4.11. *Не існує локальних майже-кілець на групах класу нільпотентності 3 порядків 16 і 81.*

4.3.1. Групи H_1

Нехай H_1 — адитивно записана група з теореми 4.1. Тоді $H_1 = \langle a \rangle + \langle b \rangle + \langle c \rangle + \langle d \rangle$ для деяких елементів a, b, c і d з R задовольняють співвідношення $ap = bp = cp = dp = 0$, $b + c = c + b$, $a + d = d + a$, $b + d = d + b$, де $c = -a - b + a + b$ і $d = -a - c + a + c$.

Лема 4.12. *Для довільних цілих чисел k і m в групі H_1 виконуються рівності*

$$-ak - cm + ak + cm = dkm$$

і

$$cm + ak = ak + cm - dkm.$$

Доведення. Оскільки $-a - c + a + c = d$, отримуємо $-c + a + c = a + d$. Тоді

$$-cm + ak + cm = (a + dm)k = ak + dkm.$$

Тому, $-ak - cm + ak + cm = dkm$ і, отже, $cm + ak = ak + cm - dkm$. $\square$

Наслідок 4.13. Для довільних цілих чисел k і m в групі H_1 виконуються рівності

$$-cm + ak = ak - cm + dkm$$

і

$$-cm - ak = -ak - cm - dkm.$$

Лема 4.14. Для довільних цілих чисел k і l в групі H_1 виконуються рівності

$$-ak - bl + ak + bl = ckl + dl \binom{k}{2}$$

і

$$bl + ak = ak + bl - ckl + dl \binom{k}{2}.$$

Доведення. Нехай $k = 1$. Оскільки $-a - b + a + b = c$, отримуємо $-b + a + b = a + c$. Тоді

$$-bl + a + bl = a + cl = a + cl - dl \binom{1}{2},$$

де $dl \binom{1}{2} = 0$ згідно з (3.1). Тому, $-a - bl + a + bl = cl - dl \binom{1}{2}$ і, отже, $bl + a = a + bl - cl + dl \binom{1}{2}$.

Доведення проведемо індукцією по k . Для $k = 1$ справедлива рівність. Нехай для k виконується рівність, тобто

$$-bl + ak + bl = ak + cl - dl \binom{k}{2}.$$

Доведемо рівність для $k + 1$:

$$\begin{aligned} -bl + a(k+1) + bl &= -bl + ak + a + bl = \\ &= -bl + ak + bl + a + cl = ak + cl - dl \binom{k}{2} + a + cl = \\ &= ak + a + cl - dl \binom{k}{2} - dl \binom{k}{2} = \end{aligned}$$

$$\begin{aligned}
a(k+1) + cl(k+1) - dl\left(\binom{k}{2} + k\right) &= \\
&= a(k+1) + cl(k+1) - dl\left(\binom{k+1}{2}\right).
\end{aligned}$$

□

Наслідок 4.15. Для довільних цілих чисел k і l в групі H_1 виконуються рівності

$$\begin{aligned}
-bl + ak &= ak - bl + ckl - dl\left(\binom{k}{2}\right) \\
i \\
-bl - ak &= -ak - bl - ckl - dl\left(\binom{-k}{2}\right).
\end{aligned}$$

Лема 4.16. Для будь-яких натуральних чисел k, l, n, m і r в групі H_1 виконується наступна рівність

$$\begin{aligned}
(ak + bl + cm + dn)r &= akr + blr + c(mr - kl\binom{r}{2}) + \\
&+ d(nr + l\binom{k}{2}\binom{r}{2} - km\binom{r}{2} + k^2l\binom{r}{r-3}).
\end{aligned}$$

Доведення. Доведення проведемо індукцією по r . Для $r = 1$ рівність справедлива. Нехай для r рівність виконується, тобто

$$\begin{aligned}
(ak + bl + cm + dn)r &= akr + blr + c(mr - kl\binom{r}{2}) + \\
&+ d(nr + l\binom{k}{2}\binom{r}{2} - km\binom{r}{2} + k^2l\binom{r}{r-3}).
\end{aligned}$$

Використовуючи леми 4.12 і 4.14, доведемо рівність для $r + 1$:

$$\begin{aligned}
&(ak + bl + cm + dn)(r + 1) = \\
&= akr + blr + c(mr - kl\binom{r}{2}) + d(nr + l\binom{k}{2}\binom{r}{2} - \\
&- km\binom{r}{2} + k^2l\binom{r}{r-3}) + ak + bl + cm + dn =
\end{aligned}$$

$$\begin{aligned}
&= akr + blr + ak + c(m(r+1) - kl\binom{r}{2}) - d(kmr - k^2l\binom{r}{2}) + \\
&\quad + bl + d(n(r+1) + l\binom{k}{2}\binom{r}{2} - km\binom{r}{2}) + \\
&\quad + k^2l\binom{r}{r-3}) = akr + ak + blr + bl - cklr + dlr\binom{k}{2} + \\
&\quad + c(m(r+1) - kl\binom{r}{2}) - d(kmr - k^2l\binom{r}{2}) + d(n(r+1) + \\
&\quad + l\binom{k}{2}\binom{r}{2} - km\binom{r}{2} + k^2l\binom{r}{r-3}) = \\
&= a(k(r+1)) + b(l(r+1)) + c(m(r+1) - kl\binom{r+1}{2}) + \\
&\quad + d(n(r+1) + l\binom{k}{2}\binom{r+1}{2} - km\binom{r+1}{2}) + \\
&\quad + k^2l\binom{r+1}{r-2}).
\end{aligned}$$

Отже, рівність справедлива для будь-якого r . □

4.3.2. Майже-кільця з одиницею, адитивні групи яких ізоморфні H_1

Нехай R — майже-кільце з одиницею, адитивна група якого R^+ ізоморфна H_1 . Тоді $R^+ = \langle a \rangle + \langle b \rangle + \langle c \rangle + \langle d \rangle$ для деяких елементів a, b, c і d of R задовольняють співвідношення $ap = bp = cp = dp = 0$, $b + c = c + b$, $a + d = d + a$, $b + d = d + b$, де $c = -a - b + a + b$ і $d = -a - c + a + c$. Зокрема, кожен елемент $x \in R$ однозначно записується у формі $x = ax_1 + bx_2 + cx_3 + dx_4$ з коефіцієнтами $0 \leq x_1 < p$, $0 \leq x_2 < p$, $0 \leq x_3 < p$ і $0 \leq x_4 < p$.

Оскільки порядок елемента a дорівнює експоненті групи G , тобто p , з цього випливає, що ми можемо 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 $\alpha(x)$, $\beta(x)$, $\gamma(x)$, $\phi(x)$, що

$$xb = a\alpha(x) + b\beta(x) + c\gamma(x) + d\phi(x).$$

Зрозуміло, що вони однозначно визначені за модулем p , тому визначені деякі відображення $\alpha: R \rightarrow \mathbb{Z}_p$, $\beta: R \rightarrow \mathbb{Z}_p$, $\gamma: R \rightarrow \mathbb{Z}_p$, $\phi: R \rightarrow \mathbb{Z}_p$.

Лема 4.17. *Нехай R — майже-кільце з одиницею, адитивна група якого R^+ ізоморфна H_1 . Якщо a збігається з одиничним елементом R , $x = ax_1 + bx_2 + cx_3 + dx_4$, $y = ay_1 + by_2 + cy_3 + dy_4 \in R$,*

$$xb = a\alpha(x) + b\beta(x) + c\gamma(x) + d\phi(x),$$

тоді

$$\begin{aligned} xy = & a(x_1y_1 + \alpha(x)y_2) + b(x_2y_1 + \beta(x)y_2) + c(x_3y_1 - x_1x_2 \binom{y_1}{2}) - \quad (4.8) \\ & - x_2\alpha(x)y_1y_2 + \gamma(x)y_2) - \alpha(x)\beta(x) \binom{y_2}{2} + x_1\beta(x)y_3 - \\ & - x_2\alpha(x)y_3) + d(x_4y_1 + x_2 \binom{x_1}{2} \binom{y_1}{2} - x_1x_3 \binom{y_1}{2}) + \\ & + x_1^2x_2 \binom{y_1}{y_1-3} + x_2y_1 \binom{\alpha(x)y_2}{2} - \alpha(x)x_3y_1y_2 + \\ & + x_1x_2\alpha(x) \binom{y_1}{2} y_2 + \phi(x)y_2 + \beta(x) \binom{\alpha(x)}{2} \binom{y_2}{2} - \\ & - \alpha(x)\gamma(x) \binom{y_2}{2} + \alpha(x)^2\beta(x) \binom{y_2}{y_2-3} + x_1\gamma(x)y_3 - \\ & - \beta(x) \binom{x_1}{2} y_3 + x_2 \binom{\alpha(x)}{2} y_3 - x_3\alpha(x)y_3 + x_1^2\beta(x)y_4 - \\ & - x_1x_2\alpha(x)y_4). \end{aligned}$$

Крім того, для відображень

$\alpha: R \rightarrow \mathbb{Z}_p$, $\beta: R \rightarrow \mathbb{Z}_p$, $\gamma: R \rightarrow \mathbb{Z}_p$, $\phi: R \rightarrow \mathbb{Z}_p$ справедливі наступні твердження:

$$(0) \quad \alpha(0) \equiv 0 \pmod{p}, \beta(0) \equiv 0 \pmod{p}, \gamma(0) \equiv 0 \pmod{p};$$

та $\phi(0) \equiv 0 \pmod{p}$ тоді і тільки тоді, коли майже-кільце R є нуль-симетричним;

$$(1) \quad xc = c(x_1\beta(x) - x_2\alpha(x)) + d(x_1\gamma(x) - \beta(x)\binom{x_1}{2} + x_2\binom{\alpha(x)}{2} - x_3\alpha(x));$$

$$(2) \quad xd = d(x_1^2\beta(x) - x_1x_2\alpha(x));$$

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

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

$$(5) \quad \gamma(xy) \equiv x_3\alpha(y) - x_1x_2\binom{\alpha(y)}{2} - x_2\alpha(x)\alpha(y)\beta(y) + \gamma(x)\beta(y) -$$

$$- \alpha(x)\beta(x)\binom{\beta(y)}{2} + x_1\beta(x)\gamma(y) - x_2\alpha(x)\gamma(y) \pmod{p};$$

$$(6) \quad \phi(xy) \equiv x_4\alpha(y) + x_2\binom{x_1}{2}\binom{\alpha(y)}{2} - x_1x_3\binom{\alpha(y)}{2} + x_1^2x_2\binom{\alpha(y)}{\alpha(y)-3} +$$

$$+ x_2\alpha(y)\binom{\alpha(x)\beta(y)}{2} - \alpha(x)x_3\alpha(y)\beta(y) + x_1x_2\alpha(x)\binom{\alpha(y)}{2}y_2 +$$

$$+ \phi(x)\beta(y) + \beta(x)\binom{\alpha(x)}{2}\binom{\beta(y)}{2} - \alpha(x)\gamma(x)\binom{\beta(y)}{2} +$$

$$+ \alpha(x)^2\beta(x)\binom{\beta(y)}{\beta(y)-3} + x_1\gamma(x)\gamma(y) - \beta(x)\binom{x_1}{2}\gamma(y) +$$

$$+ x_2\binom{\alpha(x)}{2}\gamma(y) - x_3\alpha(x)\gamma(y) + x_1^2\beta(x)\phi(y) - x_1x_2\alpha(x)\phi(y) \pmod{p}.$$

Доведення. Оскільки $0 \cdot a = a \cdot 0 = 0$, з цього випливає, що R є нуль-симетричним майже-кільцем тоді і тільки тоді, коли

$$0 = 0 \cdot b = a\alpha(0) + b\beta(0) + c\gamma(0) + d\phi(0).$$

Рівнозначно маємо

$$\alpha(0) \equiv 0 \pmod{p}, \beta(0) \equiv 0 \pmod{p},$$

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

Крім того, оскільки $c = -a - b + a + b$, $d = -a - c + a + c$ і ліво-дистрибутивний закон маємо

$$0 \cdot c = -0 \cdot a - 0 \cdot b + 0 \cdot a + 0 \cdot b = 0$$

і

$$0 \cdot d = -0 \cdot a - 0 \cdot c + 0 \cdot a + 0 \cdot c = 0,$$

звідки

$$\begin{aligned} 0 \cdot x &= 0 \cdot (ax_1 + bx_2 + cx_3 + dx_4) = \\ &= (0 \cdot a)x_1 + (0 \cdot b)x_2 + (0 \cdot c)x_3 + (0 \cdot d)x_4 = 0. \end{aligned}$$

Отже, виконується твердження (0).

Далі, використовуючи леми [4.12](#) і [4.14](#), отримуємо

$$\begin{aligned} xc &= x(-a - b + a + b) = -xa - xb + xa + xb = \\ &= -dx_4 - cx_3 - bx_2 - ax_1 - d\phi(x) - c\gamma(x) - b\beta(x) - a\alpha(x) + \\ &+ ax_1 + bx_2 + cx_3 + dx_4 + a\alpha(x) + b\beta(x) + c\gamma(x) + d\varphi(x) = \\ &= -cx_3 - bx_2 - c\gamma(x) - ax_1 + dx_1\gamma(x) - b\beta(x) - a\alpha(x) + \\ &+ ax_1 + bx_2 + a\alpha(x) + cx_3 - dx_3\alpha(x) + b\beta(x) + c\gamma(x) = \\ &= -cx_3 - bx_2 - c\gamma(x) + dx_1\gamma(x) - b\beta(x) - ax_1 + \\ &+ cx_1\beta(x) + d\beta(x) \binom{-x_1}{2} - a\alpha(x) + a\alpha(x) + \\ &+ bx_2 - cx_2\alpha(x) + dx_2 \binom{\alpha(x)}{2} + cx_3 - dx_3\alpha(x) + \\ &+ b\beta(x) + c\gamma(x) = -cx_3 - bx_2 - c\gamma(x) + dx_1\gamma(x) - \\ &- b\beta(x) + cx_1\beta(x) - ax_1 - dx_1^2\beta(x) + d\beta(x) \binom{-x_1}{2} + \\ &+ ax_1 + bx_2 - cx_2\alpha(x) + dx_2 \binom{\alpha(x)}{2} + cx_3 - dx_3\alpha(x) + \end{aligned}$$

$$+b\beta(x) + c\gamma(x) = c(x_1\beta(x) - x_2\alpha(x)) + d(x_1\gamma(x) - \beta(x)\binom{x_1}{2} + x_2\binom{\alpha(x)}{2} - x_3\alpha(x)).$$

Використовуючи леми 4.12 і 4.14, отримуємо

$$\begin{aligned} xd &= x(-a - c + a + c) = -xa - xc + xa + xc = \\ &= -dx_4 - cx_3 - bx_2 - ax_1 - d(x_1\gamma(x) - \beta(x)\binom{x_1}{2} + \\ &\quad + x_2\binom{\alpha(x)}{2} - x_3\alpha(x)) - c(x_1\beta(x) - x_2\alpha(x)) + \\ &\quad + ax_1 + bx_2 + cx_3 + dx_4 + c(x_1\beta(x) - x_2\alpha(x)) + d(x_1\gamma(x) - \\ &\quad - \beta(x)\binom{x_1}{2} + x_2\binom{\alpha(x)}{2} - x_3\alpha(x)) = \\ &= -cx_3 - bx_2 - c(x_1\beta(x) - x_2\alpha(x)) - ax_1 + d(x_1^2\beta(x) - x_1x_2\alpha(x)) + \\ &\quad ax_1 + bx_2 + cx_3 + c(x_1\beta(x) - x_2\alpha(x)) = d(x_1^2\beta(x) - x_1x_2\alpha(x)). \end{aligned}$$

Отримуємо твердження (1)–(2) леми.

За ліво-дистрибутивним законом і (1)–(2) леми, маємо

$$\begin{aligned} xy &= x(ay_1) + x(by_2) + x(cy_3) + x(dy_4) = \\ &= (ax_1 + bx_2 + cx_3 + dx_4)y_1 + (a\alpha(x) + b\beta(x) + c\gamma(x) + d(\phi(x)))y_2 + \\ &\quad + (c(x_1\beta(x) - x_2\alpha(x)) + d(x_1\gamma(x) - \beta(x)\binom{x_1}{2}))y_3 \\ &\quad + d(x_1^2\beta(x) - x_1x_2\alpha(x))y_4. \end{aligned}$$

Крім того, лема 4.16 означає, що

$$\begin{aligned} (ax_1 + bx_2 + cx_3 + dx_4)y_1 &= ax_1y_1 + bx_2y_1 + \\ &+ c(x_3y_1 - x_1x_2\binom{y_1}{2}) + d(x_4y_1 + x_2\binom{x_1}{2}\binom{y_1}{2} - \\ &\quad - x_1x_3\binom{y_1}{2} + \binom{y_1}{y_1-3}x_1^2x_2), \end{aligned}$$

$$(a\alpha(x) + b\beta(x) + c\gamma(x) + d\phi(x))y_2 = a\alpha(x)y_2 + b\beta(x)y_2 + \\ + c(\gamma(x)y_2 + \alpha(x)\beta(x)\binom{y_2}{2}) + d(\phi(x)y_2 + \beta(x)\binom{\alpha(x)}{2})\binom{y_2}{2} - \\ - \alpha(x)\gamma(x)\binom{y_2}{2} + \alpha(x)^2\beta(x)\binom{y_2}{y_2-3},$$

$$(c(x_1b(x) - x_2\alpha(x)) + d(x_1\gamma(x) - \beta(x)\binom{x_1}{2}) + \\ + x_2\binom{\alpha(x)}{2} - x_3\alpha(x))y_3 = c(x_1\beta(x)y_3 - x_2\alpha(x)y_3) + \\ + d(x_1\gamma(x)y_3 - \beta(x)\binom{x_1}{2}y_3 + x_2\binom{\alpha(x)}{2}y_3 - x_3\alpha(x)y_3)$$

i

$$d(x_1^2\beta(x) - x_1x_2\alpha(x))y_4 = d(x_1^2\beta(x)y_4 - x_1x_2\alpha(x)y_4).$$

За лемами 4.12 і 4.14, маємо

$$xy = a(x_1y_1 + \alpha(x)y_2) + b(x_2y_1 + \beta(x)y_2) + \\ + c(x_3y_1 - x_1x_2\binom{y_1}{2} - x_2\alpha(x)y_1y_2 + \gamma(x)y_2 - \\ - \alpha(x)\beta(x)\binom{y_2}{2} + x_1\beta(x)y_3 - x_2\alpha(x)y_3) + d(x_4y_1 + \\ + x_2\binom{x_1}{2}\binom{y_1}{2} - x_1x_3\binom{y_1}{2} + x_1^2x_2\binom{y_1}{y_1-3} + x_2y_1\binom{\alpha(x)y_2}{2} - \\ - \alpha(x)x_3y_1y_2 + x_1x_2\alpha(x)\binom{y_1}{2}y_2 + \phi(x)y_2 + \beta(x)\binom{\alpha(x)}{2}\binom{y_2}{2} - \\ - \alpha(x)\gamma(x)\binom{y_2}{2} + \alpha(x)^2\beta(x)\binom{y_2}{y_2-3} + x_1\gamma(x)y_3 - \\ - \beta(x)\binom{x_1}{2}y_3 + x_2\binom{\alpha(x)}{2}y_3 - x_3\alpha(x)y_3 + \\ + x_1^2\beta(x)y_4 - x_1x_2\alpha(x)y_4).$$

Нарешті, асоціативність множення в R означає, що

$$x(yb) = (xy)b = a\alpha(xy) + b\beta(xy) + c\gamma(xy) + d\phi(xy).$$

Крім того, заміна

$$yb = a\alpha(y) + b\beta(y) + c\gamma(y) + d\phi(y)$$

замість y в формулі (**), також маємо

$$\begin{aligned} x(yb) = & a(x_1\alpha(y) + \alpha(x)\beta(y)) + b(x_2\alpha(y) + \beta(x)\beta(y)) + \\ & + c(x_3\alpha(y) - x_1x_2\binom{\alpha(y)}{2} - x_2\alpha(x)\alpha(y)\beta(y) + \gamma(x)\beta(y) - \\ & - \alpha(x)\beta(x)\binom{\beta(y)}{2} + x_1\beta(x)\gamma(y) - x_2\alpha(x)\gamma(y)) + d(x_4\alpha(y) + \\ & + x_2\binom{x_1}{2}\binom{\alpha(y)}{2} - x_1x_3\binom{\alpha(y)}{2} + x_1^2x_2\binom{\alpha(y)}{\alpha(y)-3} + \\ & + x_2\alpha(y)\binom{\alpha(x)\beta(y)}{2} - \alpha(x)x_3\alpha(y)\beta(y) + x_1x_2\alpha(x)\binom{\alpha(y)}{2}y_2 + \\ & + \phi(x)\beta(y) + \beta(x)\binom{\alpha(x)}{2}\binom{\beta(y)}{2} - \alpha(x)\gamma(x)\binom{\beta(y)}{2} + \\ & + \alpha(x)^2\beta(x)\binom{\beta(y)}{\beta(y)-3} + x_1\gamma(x)\gamma(y) - \beta(x)\binom{x_1}{2}\gamma(y) + \\ & x_2\binom{\alpha(x)}{2}\gamma(y) - x_3\alpha(x)\gamma(y) + x_1^2\beta(x)\phi(y) - x_1x_2\alpha(x)\phi(y)). \end{aligned}$$

Порівнюючи коефіцієнти a , b , c і d у двох виразах, отриманих для $x(yb)$, ми отримуємо твердження (3)–(6) леми. $\square$

4.3.3. Про групу H_2

Нехай H_2 — адитивно записана група з теореми 4.1. Тоді $H_2 = \langle a \rangle + \langle b \rangle + \langle c \rangle$ для деяких елементів a , b та c з R , які задовольняють співвідношення $ap^2 = bp = cp = 0$, $b + c = c + b$, $-a - c + a + c = ap$, де $c = -a - b + a + b$.

Лема 4.18. Для довільних цілих k та m в групі H_2 виконуються рівності

$$-am - ck + am + ck = aktp$$

та

$$ck + am = am(1 - kp) + ck.$$

Доведення. Оскільки $-a - c + a + c = ap$, то отримаємо $-c + a + c = a(1 + p)$.
Тоді

$$-ck + am + ck = am(1 + kp).$$

Отже, $-ak - cm + ak + cm = aktp$ та $ck + am = am(1 - kp) + ck$. $\square$

Лема 4.19. Для довільних цілих n та m в групі H_2 виконуються рівності

$$-bn + am + bn = a(m - \binom{m}{2}np) + cmn$$

та

$$bn + am = a(m + \binom{m}{2}np) + bn - cmn.$$

Доведення. Доведення проведемо індукцією по m .

Нехай $m = 1$. Оскільки $-a - b + a + b = c$, то маємо $-b + a + b = a + c$.

Із співвідношень групи та за лемою 4.18, маємо

$$-bn + a + bn = a(1 - n\binom{1}{2}p) + cn$$

і тому

$$bn + a = a(1 + \binom{1}{2}np) + bn - cn,$$

тобто для $m = 1$ виконується рівність.

Нехай для m виконується рівність, тобто

$$-bn + am + bn = a(m - \binom{m}{2}np) + cmn.$$

Доведемо рівність для $m + 1$:

$$\begin{aligned}
 -bn + a(m + 1) + bn &= -bn + am + a + bn = \\
 &= -bn + am + bn + a + cn = -bn + bn + a(m - \binom{m}{2}np) + \\
 + cmn + a + cn &= a(m - \binom{m}{2}np) + a(1 - mnp) + cmn + cn = \\
 &= a((m + 1) - \binom{m+1}{2}np) + cm(n + 1).
 \end{aligned}$$

Отже,

$$-bn + am + bn = a(m - \binom{m}{2}np) + cmn$$

та

$$bn + am = a(m + \binom{m}{2}np) + bn - cmn.$$

□

Лема 4.20. Для будь-яких невід'ємних цілих k, l, m та натурального r в H_2 має місце рівність

$$\begin{aligned}
 (ak + bl + cm)r &= a(kr + (\binom{k}{2}\binom{r}{2}l - km\binom{r}{2}) + \\
 &+ k^2l\binom{r}{r-3})p + blr + c(mr - kl\binom{r}{2}).
 \end{aligned}$$

Доведення. Доведення проведемо індукцією по r .

Нехай $r = 1$. Тоді маємо

$$\begin{aligned}
 (ak + bl + cm)1 &= a(k + (\binom{k}{2}\binom{1}{2}l - km\binom{1}{2}) + k^2l\binom{1}{-2})p + \\
 &bl + c(m - \binom{1}{2}kl) = ak + bl + cm.
 \end{aligned}$$

Отже, для $r = 1$ виконується рівність.

Нехай для r виконується рівність, тобто

$$(ak + bl + cm)r = a(kr + (\binom{k}{2}\binom{r}{2}l - km\binom{r}{2}) + k^2l\binom{r}{r-3})p +$$

$$blr + c(mr - kl\binom{r}{2}).$$

Використовуючи леми 4.18 та 4.19, доведемо рівність для $r + 1$:

$$\begin{aligned}
& (ak + bl + cm)(r + 1) = (ak + bl + cm)r + ak + bl + cm = \\
& = a(kr + (\binom{k}{2}\binom{r}{2}l - km\binom{r}{2} + k^2l\binom{r}{r-3})p) + blr + \\
& + c(mr - kl\binom{r}{2}) + ak + bl + cm = a(kr + \\
& + (\binom{k}{2}\binom{r}{2}l - lm\binom{r}{2} + k^2l\binom{r}{r-3})p) + \\
& + brl + ak - ak(mr - kl\binom{r}{2})p + c(mr - kl\binom{r}{2}) + bl + cm = \\
& = a(kr + (\binom{k}{2}\binom{r}{2}l - km\binom{r}{2} + k^2l\binom{r}{r-3})p) + \\
& + a(k - kmrp + k^2l\binom{r}{2}p + \binom{k}{2}lrp) + blr - clr(k - kmrp + \\
& + k^2l\binom{r}{2}p) + c(mr - kl\binom{r}{2}) + bl + cm = \\
& = a(kr + \binom{k}{2}\binom{r}{2}lp - km\binom{r}{2}p + k^2l\binom{r}{r-3}p + k - \\
& - kmrp + k^2l\binom{r}{2}p + \binom{k}{2}lrp) + bl(r + 1) + c(m(r + 1) - \\
& - kl\binom{r}{2} - klr) = a(k(r + 1) + (\binom{k}{2}\binom{r+1}{2}l - \\
& - km\binom{r+1}{2} + k^2l\binom{r+1}{r-2})p) + bl(r + 1) + \\
& + c(m(r + 1) - kl\binom{r+1}{2}).
\end{aligned}$$

Отже, рівність справедлива для будь-якого r . □

Враховуючи властивість симетричності біноміальних коефіцієнтів, тобто $\binom{r}{r-3} = \binom{r}{3}$, та лему 4.20, маємо наступне твердження.

Наслідок 4.21. Для будь-яких невід'ємних цілих k, l, m та натурального r в H_2 має місце рівність

$$(ak + bl + cm)r = a(kr + \binom{k}{2}\binom{r}{2}l - km\binom{r}{2} + \\ + k^2l\binom{r}{3})p + blr + c(mr - kl\binom{r}{2}).$$

4.3.4. Майже-кільця з одиницею, адитивні групи яких ізоморфні H_2

Наступна лема описує множення в майже-кільці R , адитивна група якого R^+ є ізоморфною групі H_2 . Тоді $R^+ = \langle a \rangle + \langle b \rangle + \langle c \rangle$ для деяких елементів a, b, c з R , які задовольняють співвідношення $ap^2 = bp = cp = 0$, $b + c = c + b$, $-a - c + a + c = ap$, де $c = -a - b + a + b$. Зокрема, кожен елемент $x \in R$ однозначно записується у вигляді $x = ax_1 + bx_2 + cx_3$ з коефіцієнтами $0 \leq x_1 < p^2$, $0 \leq x_2 < p$ і $0 \leq x_3 < p$.

Лема 4.22. Нехай R — майже-кільце з одиницею, адитивна група якого R^+ ізоморфна H_2 . Якщо a збігається з одиничним елементом R , $x = ax_1 + bx_2 + cx_3$, $y = ay_1 + by_2 + cy_3 \in R$ та

$$xb = a\alpha(x) + b\beta(x) + c\gamma(x),$$

то

$$xy = a(x_1y_1 + \alpha(x)y_2 + \binom{x_1}{2}\binom{y_1}{2}x_2 - x_1x_3\binom{y_1}{2} + \\ + x_1^2x_2\binom{y_1}{3} + \binom{\alpha(x)y_2}{2}x_2y_1 - \alpha(x)x_3y_1y_2 - \\ - x_1x_2\alpha(x)y_2\binom{y_1}{2} + \binom{\alpha(x)}{2}\beta(x)\binom{y_2}{2} - \\ \alpha(x)\gamma(x)\binom{y_2}{2} + \alpha(x)^2\beta(x)\binom{y_2}{3} - \binom{x_1}{2}\beta(x)y_3 + \quad (4.9)$$

$$\begin{aligned}
& + \binom{\alpha(x)}{2} x_2 y_3 - x_3 \alpha(x) y_3) p) + b(x_2 y_1 + \beta(x) y_2) + \\
& + c(x_3 y_1 - x_2 \alpha(x) y_1 y_2 - x_1 x_2 \binom{y_1}{2}) + \gamma(x) y_2 - \\
& - \alpha(x) \beta(x) \binom{y_2}{2} + x_1 \beta(x) y_3 - x_2 \alpha(x) y_3).
\end{aligned}$$

Більш того, для відображень

$\alpha: R \rightarrow \mathbb{Z}_{p^2}, \beta: R \rightarrow \mathbb{Z}_p, \gamma: R \rightarrow \mathbb{Z}_p$ виконуються наступні твердження:

(0) $\alpha(0) \equiv 0 \pmod{p^2}, \beta(0) \equiv 0 \pmod{p}, \gamma(0) \equiv 0 \pmod{p}$ тоді і тільки тоді, коли майже-кільце R є нуль-симетричним;

(1) $\alpha(a) \equiv 0 \pmod{p^2}, \beta(a) \equiv 1 \pmod{p}, \gamma(a) \equiv 0 \pmod{p}$;

(2) якщо $x_1 \not\equiv 0 \pmod{p}$, то $x_1 \beta(x) - x_2 \alpha(x) \equiv 1 \pmod{p}$;

(3) $xc = a(-\binom{x_1}{2} \beta(x) + \binom{\alpha(x)}{2} x_2 - x_3 \alpha(x)) p + c(x_1 \beta(x) - x_2 \alpha(x))$;

(4) $\alpha(xy) \equiv x_1 \alpha(y) + \alpha(x) \beta(y) + (\binom{x_1}{2} \binom{\alpha(y)}{2} x_2 - x_1 x_3 \binom{\alpha(y)}{2}) +$

$$x_1^2 x_2 \binom{\alpha(y)}{3} + \binom{\alpha(x) \beta(y)}{2} x_2 \alpha(y) - \alpha(x) x_3 \alpha(y) \beta(y) +$$

$$x_1 x_2 \alpha(x) \beta(y) \binom{\alpha(y)}{2} + \binom{\alpha(x)}{2} \beta(x) \binom{\beta(y)}{2} - \alpha(x) \gamma(x) \binom{\beta(y)}{2} +$$

$$\alpha(x)^2 \beta(x) \binom{\beta(y)}{3} + \binom{x_1}{2} \beta(x) \gamma(y) + \binom{\alpha(x)}{2} x_2 \gamma(y) - x_3 \alpha(x) \gamma(y)) p \pmod{p^2};$$

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

(6) $\gamma(xy) \equiv x_3 \alpha(y) - x_2 \alpha(x) \alpha(y) \beta(y) - x_1 x_2 \binom{\alpha(y)}{2} + \gamma(x) \beta(y) -$

$$\alpha(x) \beta(x) \binom{\beta(y)}{2} + x_1 \beta(x) \gamma(y) - x_2 \alpha(x) \gamma(y) \pmod{p}.$$

Доведення. Оскільки $0 \cdot a = a \cdot 0 = 0$, звідси випливає R є нуль-симетричним майже-кільцем тоді і тільки тоді, коли

$$0 = 0 \cdot b = a\alpha(0) + b\beta(0) + c\gamma(0)$$

або еквівалентно $\alpha(0) \equiv 0 \pmod{p^2}$, $\beta(0) \equiv 0 \pmod{p}$, $\gamma(0) \equiv 0 \pmod{p}$. Більш того, оскільки

$$b = ab = a\alpha(a) + b\beta(a) + c\gamma(a),$$

маємо $\alpha(a) \equiv 0 \pmod{p^2}$, $\beta(a) \equiv 1 \pmod{p}$ і $\gamma(a) \equiv 0 \pmod{p}$, а отже, виконуються твердження (0) і (1).

Далі, використовуючи леми 4.18 і 4.19, маємо

$$\begin{aligned} xc &= x(-a - b + a + b) = -xa - xb + xa + xb = \\ &= -cx_3 - bx_2 - ax_1 - c\gamma(x) - b\beta(x) - a\alpha(x) + \\ &+ ax_1 + bx_2 + cx_3 + a\alpha(x) + b\beta(x) + c\gamma(x) = \\ &= -cx_3 - bx_2 - c\gamma(x) - ax_1 + ax_1\gamma(x)p - b\beta(x) - a\alpha(x) + \\ &+ ax_1 + bx_2 + a\alpha(x) - ax_3\alpha(x)p + cx_3 + b\beta(x) + c\gamma(x) = \\ &= -cx_3 - bx_2 - c\gamma(x) - a\binom{x_1}{2}\beta(x)p - b\beta(x) + cx_1\beta(x) - \\ &+ ax_1 + ax_1\gamma(x)p - a\alpha(x) + ax_1 + a\alpha(x) + a\binom{\alpha(x)}{2}x_2p + \\ &+ bx_2 - cx_2\alpha(x) - ax_3\alpha(x)p + cx_3 + b\beta(x) + c\gamma(x) = \\ &= a\left(-\binom{x_1}{2}\beta(x) + \binom{\alpha(x)}{2}x_2 - x_3\alpha(x)\right)p + c(x_1\beta(x) - x_2\alpha(x)). \end{aligned}$$

Отримали рівність (3) леми.

Далі, користуючись лівою дистрибутивністю та за лемами 4.18–4.20 і наслідком 4.21.

$$\begin{aligned} xy &= x(ay_1) + x(by_2) + x(cy_3) = \\ &= (ax_1 + bx_2 + cx_3)y_1 + (a\alpha(x) + b\beta(x) + c\gamma(x))y_2 + \end{aligned}$$

$$\begin{aligned}
& + (a(-\binom{x_1}{2}\beta(x) + \binom{\alpha(x)}{2}x_2 - x_3\alpha(x)p + c(x_1\beta(x) - \\
& - x_2\alpha(x)))y_3 = a(x_1y_1 + \binom{x_1}{2}\binom{y_1}{2}x_2p - x_1x_3\binom{y_1}{2}p + \\
& + x_1^2x_2\binom{y_1}{3}p) + bx_2y_1 + c(x_3y_1 - x_1x_2\binom{y_1}{2}) + \\
& + a(\alpha(x)y_2 + \binom{\alpha(x)}{2}\beta(x)\binom{y_2}{2}p - \alpha(x)\gamma(x)\binom{y_2}{2}p + \\
& + \alpha(x)^2\beta(x)\binom{y_2}{3}p) + b\beta(x)y_2 + c(\gamma(x)y_2 - \alpha(x)\beta(x)\binom{y_2}{2}) + \\
& + a(-\binom{x_1}{2}\beta(x) + \binom{\alpha(x)}{2}x_2 - x_3\alpha(x))y_3p + \\
& + c(x_1\beta(x) - x_2\alpha(x))y_3 = a(x_1y_1 + \binom{x_1}{2}\binom{y_1}{2}x_2p - \\
& - x_1x_3\binom{y_1}{2}p + x_1^2x_2\binom{y_1}{3}p) + bx_2y_1 + a\alpha(x)y_2 - \\
& - a\alpha(x)y_2(x_3y_1 - x_1x_2\binom{y_1}{2})p + c(x_3y_1 - x_1x_2\binom{y_1}{2}) + \\
& + a(\binom{\alpha(x)}{2}\beta(x)\binom{y_2}{2} - \alpha(x)\gamma(x)\binom{y_2}{2} + \alpha(x)^2\beta(x)\binom{y_2}{3})p + \\
& + b\beta(x)y_2 + c(\gamma(x)y_2 - \alpha(x)\beta(x)\binom{y_2}{2}) + a(-\binom{x_1}{2}\beta(x) + \\
& + \binom{\alpha(x)}{2}x_2 - x_3\alpha(x))y_3p + c(x_1\beta(x) - x_2\alpha(x))y_3 \\
& = a(x_1y_1 + \binom{x_1}{2}\binom{y_1}{2}x_2p - x_1x_3\binom{y_1}{2}p + x_1^2x_2\binom{y_1}{3}p + \alpha(x)y_2 + \\
& + \binom{\alpha(x)y_2}{2}x_2y_1p) + bx_2y_1 - cx_2\alpha(x)y_1y_2 - a(\alpha(x)x_3y_1y_2p + \\
& + x_1x_2\alpha(x)y_2\binom{y_1}{2}p) + c(x_3y_1 - x_1x_2\binom{y_1}{2}) + a(\binom{\alpha(x)}{2}\beta(x)\binom{y_2}{2}p - \\
& + \alpha(x)\gamma(x)\binom{y_2}{2}p + \alpha(x)^2\beta(x)\binom{y_2}{3}p) + b\beta(x)y_2 + c(\gamma(x)y_2 -
\end{aligned}$$

$$\begin{aligned}
& -\alpha(x)\beta(x)\binom{y_2}{2}) + a(-\binom{x_1}{2}\beta(x) + \binom{\alpha(x)}{2}x_2 - \\
& \quad -x_3\alpha(x))y_3p + c(x_1\beta(x) - x_2\alpha(x))y_3 \\
& = a(x_1y_1 + \alpha(x)y_2 + (\binom{x_1}{2}\binom{y_1}{2}x_2 - x_1x_3\binom{y_1}{2}) + \\
& + x_1^2x_2\binom{y_1}{3} + \binom{\alpha(x)y_2}{2}x_2y_1 - \alpha(x)x_3y_1y_2 - x_1x_2\alpha(x)y_2\binom{y_1}{2}) + \\
& + \binom{\alpha(x)}{2}\beta(x)\binom{y_2}{2} - -\alpha(x)\gamma(x)\binom{y_2}{2} + \alpha(x)^2\beta(x)\binom{y_2}{3} - \\
& \quad -\binom{x_1}{2}\beta(x)y_3 + \binom{\alpha(x)}{2}x_2y_3 - x_3\alpha(x)y_3)p + \\
& + b(x_2y_1 + \beta(x)y_2) + c(x_3y_1 - x_2\alpha(x)y_1y_2 - x_1x_2\binom{y_1}{2}) \\
& \quad + \gamma(x)y_2 - \alpha(x)\beta(x)\binom{y_2}{2} + x_1\beta(x)y_3 - x_2\alpha(x)y_3).
\end{aligned}$$

Далі, нехай $y = a(1 - p) + c$, тоді

$$\begin{aligned}
xy & = a(x_1(1 - p) + (-\binom{x_1}{2}\beta(x) + \binom{\alpha(x)}{2}x_2 - x_3\alpha(x))p + \\
& \quad + bx_2 + c(x_3 + x_1\beta(x) - x_2\alpha(x))
\end{aligned}$$

за формулою (4.9). З іншого боку, $y = c + a$ і тому

$$\begin{aligned}
xy & = xc + x = a(x_1(1 - (x_1\beta(x) - x_2\alpha(x))p) + \\
& \quad + (-\binom{x_1}{2}\beta(x) + \binom{\alpha(x)}{2}x_2 - x_3\alpha(x))p + \\
& \quad + bx_2 + c(x_3 + x_1\beta(x) - x_2\alpha(x))
\end{aligned}$$

за лемою 4.18.

Порівнюючи обидва результати для xy , отримаємо

$$x_1(1 - p) \equiv x_1(1 - (x_1\beta(x) - x_2\alpha(x))p) \pmod{p^2}.$$

Якщо $x_1 \not\equiv 0 \pmod{p}$, то

$$x_1\beta(x) - x_2\alpha(x))p \equiv p \pmod{p^2}.$$

Тому

$$x_1\beta(x) - x_2\alpha(x) \equiv 1 \pmod{p},$$

що доводить твердження (2) леми.

Нарешті, асоціативність множення в R означає, що $(xy)b = x(yb)$. З одного боку маємо

$$x(yb) = a\alpha(xy) + b\beta(xy) + c\gamma(xy).$$

З іншого боку,

$$\begin{aligned} x(yb) = & a(x_1\alpha(y) + \alpha(x)\beta(y) + \binom{x_1}{2}\binom{\alpha(y)}{2}x_2 - \\ & - x_1x_3\binom{\alpha(y)}{2} + x_1^2x_2\binom{\alpha(y)}{3} + \binom{\alpha(x)\alpha(y)}{2}x_2\alpha(y) - \\ & - \alpha(x)x_3\alpha(y)\beta(y) + x_1x_2\alpha(x)\beta(y)\binom{\alpha(y)}{2} + \\ & + \binom{\alpha(x)}{2}\beta(x)\binom{\beta(y)}{2} - \alpha(x)\gamma(x)\binom{\beta(y)}{2} + \alpha(x)^2\beta(x)\binom{\beta(y)}{3} - \\ & + \binom{\alpha(x)}{2}x_2\gamma(y) - x_3\alpha(x)\gamma(y))p + b(x_2\alpha(y) + \beta(x)\beta(y)) + \\ & - \binom{x_1}{2}\beta(x)\gamma(y) + c(x_3\alpha(y) - x_2\alpha(x)\alpha(y)\beta(y) - x_1x_2\binom{\alpha(y)}{2} + \\ & + \gamma(x)\beta(y) - \alpha(x)\beta(x)\binom{\beta(y)}{2} + x_1\beta(x)\gamma(y) - x_2\alpha(x)\gamma(y)). \end{aligned}$$

Порівнюючи коефіцієнти біля a , b і c в двох останніх виразах для xy , отримаємо конгруентності (4)–(6) леми. $\square$

Висновки до розділу 4

У даному розділі:

- наведено деякі структурні результати стосовно груп порядку p^4 ;
- отримано необхідні умови існування майже-кілець з одиницею на групах порядку p^4 ;
- визначено формули множення для таких майже-кілець та описано функції, що їх задають.

Основні результати даного розділу опубліковано у працях [9, 10, 5] зі списку публікацій і, відповідно, [96–98] зі списку використаних джерел, а також опубліковано у тезах конференцій [26, 27, 28] і, відповідно, [92–94].

Розділ 5

Локальні майже-кілець порядку p^4

В цьому розділі розглядаються групи класу нільпотентності 2 порядку p^4 , які є адитивними групами локальних майже-кілець. Показано, що для непарних p із 6 таких груп 4 є адитивними групами локальних майже-кілець. Деякі приклади таких майже-кілець явно побудовані. Досліджуються групи класу нільпотентності 3 порядку p^4 , які є адитивними групами локальних майже-кілець. Базуючись на системі комп'ютерної алгебри GAP, побудовано приклади локальних майже-кілець на вказаних групах.

5.1. Локальні майже-кілець на групах порядку p^4 та класу нільпотентності 2

5.1.1. Групи класу нільпотентності 2 порядку 16 та локальні майже-кілець

Як згадувалося вище, бібліотека всіх неізоморфних майже-кілець з одиницею порядку до 31 міститься в пакеті SONATA, і тому всі неізоморфні локальні майже-кілець порядку 16 (див. [29]).

Лема 5.1. *Наступні групи класу нільпотентності 2, і тільки вони, є адитивними групами локальних майже-кілець порядку 16:*

1. $(C_4 \times C_2) \rtimes C_2$ [16, 3];
2. $C_4 \rtimes C_4$ [16, 4];
3. $C_8 \rtimes C_2$ [16, 6];
4. $C_2 \times Q_8$ [16, 12].

Нехай $n(G)$ — кількість усіх неізоморфних локальних майже-кілець R , адитивна група R^+ яких ізоморфна групі G .

$StructureDescription(R^+)$	$n(R^+)$
$(C_4 \times C_2) \rtimes C_2$	37
$C_4 \rtimes C_4$	24
$C_8 \rtimes C_2$	33
$C_2 \times Q_8$	2

5.1.2. Групи G_1 , G_2 та G_3 і локальні майже-кілець

Групи G_1 , G_2 та G_3 з теореми 4.1 є групами Міллера–Морено.

Згідно з [102] G_2 та G_3 є групами $G(p^2, p^2)$ і $G(p^3, p)$, відповідно (див., наприклад, лема 2 [102]). Тому, за теоремою 2 [102] існує локальне майже-кілець R , адитивна група R^+ якого ізоморфна групі G_3 . Як наслідок, на адитивній групі не існує локального майже-кілець G_2 .

Нехай R — локальне майже-кілець, адитивна група R^+ якого ізоморфна групі G_3 . Тоді $R^+ = \langle a \rangle + \langle b \rangle$ для деяких елементів a і b з R задовольняючи співвідношення $ap^3 = 0$, $bp = 0$ і $-b + a + b = a(1 - p^2)$. Зокрема,

кожен елемент $x \in R$ однозначно записується у вигляді $x = ax_1 + bx_2$ з коефіцієнтами $0 \leq x_1 < p^3$ і $0 \leq x_2 < p$.

Формула для множення елементів локальних майже-кілець на метациклічних групах Міллера–Морено визначена в [102]. Формула множення довільних елементів нуль-симетричного локального майже-кілець на G_3 наведена в доведенні [102, Theorem 2], а саме:

$$x \cdot y = a(x_1y_1 + p^2x_1x_2 \binom{y_1}{2}) + b(x_2y_1 + \beta(x)y_2),$$

де

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

Приклад 5.2. Нехай $G \cong C_{27} \rtimes C_3$. Якщо $x = ax_1 + bx_2$ і $y = ay_1 + by_2 \in G$ та $(G, +, \cdot)$ є локальним майже-кілецем, тоді, як і вище, “ $\cdot$ ” може бути наступним множенням:

$$x \cdot y = a(x_1y_1 + 9x_1x_2 \binom{y_1}{2}) + b(x_2y_1 + \beta(x)y_2),$$

де

$$\beta(x) = \begin{cases} 1, & x_1 \not\equiv 0 \pmod{3}; \\ 0, & x_1 \equiv 0 \pmod{3}. \end{cases}$$

Комп’ютерна програма, для перевірки, що майже-кілець, отримане в прикладі 5.2, справді є локальним майже кілецем, збережено на GitHub:

https://github.com/raemarina/Examples/blob/main/LNR_81-6.txt

Далі, наведемо цю програму.

В середовищі системи GAP завантажуюємо пакет LocalNR.

LoadPackage(“*LocalNR*”);

G — група з *IdGroup* [81, 6].

$G := \text{SmallGroup}(81, 6);$

gen — список, що містить мінімальну систему твірних.

gen := MinimalGeneratingSet(G);

```

# Повертаємо список з порядками твірних зі списку gen.
List(gen, Order);

# a — перший елемент зі списку gen.
a := gen[1];

# b — другий елемент зі списку gen.
b := gen[2];

# beta — функція, яка повертає значення 0 або 1 по mod 3.
beta := function(x)
  if x mod 3 <> 0 then return 1;
  else return 0; fi; end;

# mulGR — функція майже-кільцевого добутку.
mulGR := function(x, y)
  local x1, x2, y1, y2;
  for x1 in [0..26] do
    for x2 in [0..2] do
      for y1 in [0..26] do
        for y2 in [0..2] do
          if x = a^x1 * b^x2 and y = a^y1 * b^y2 then return
            a^(x1*y1+9*x1*x2*Binomial(y1, 2)) * b^(x2*y1+beta(x1)*y2); fi;
          od; od; od; od; end;
        end
      end
    end
  end

# n — майже-кільце на групі G та з множенням mulGR (без перевірки).
n := ExplicitMultiplicationNearRingNC(G, mulGR);

# M — таблиця множення майже-кільця n.
M := MultiplicationTable(n);;

# mul — майже-кільцеве множення, що отримано за допомогою таблиці M.
muNR :=
NearRingMultiplicationByOperationTable(G, M, AsSortedList(G));

```

n — майже-кільце на групі G та з множенням mul (з перевіркою).
 $n := ExplicitMultiplicationNearRing(G, mu_N R);$
 # Перевірка, чи є майже-кільце n локальним.
 $IsLocalNearRing(n);$

З пакету LocalNR та [109] ми маємо наступну кількість усіх неізоморфних нуль-симетричних локальних майже-кільць на G_3 порядків 81 та 625.

$StructureDescription(R^+)$	$n(R^+)$
$C_{27} \rtimes C_3$	10
$C_{125} \rtimes C_5$	5

Аналогічно, G_1 — це група $G(p^2, p, p)$ згідно з [12]. Отже, за теоремою 3 [12] існує локальне майже-кільце, адитивна група якого ізоморфна G_1 . Оскільки G_1 є неметациклічною групою Міллера–Морено, використовуючи [12, Theorem 3], для довільних елементів $x = ax_1 + bx_2 + cx_3$ і $y = ay_1 + by_2 + cy_3$ з G_1 отримуємо наступну формулу множення:

$$x \cdot y = a(x_1y_1 + p^k x_2y_2) + b(x_2y_1 + x_1y_2) + \\ + c(-x_1x_2 \binom{y_1}{2} + x_3y_1 + x_1^2y_3),$$

де $k = 1, 2$.

Легко побачити, що $R = (G_1, +, \cdot)$ є ненуль-симетричним локальним майже-кільцем.

Приклад 5.3. Нехай $G \cong (C_9 \times C_3) \rtimes C_3$. Якщо $x = ax_1 + bx_2 + cx_3$ і $y = ay_1 + by_2 + cy_3 \in G$, та $(G, +, \cdot)$ є локальним майже-кільцем, тоді, як і вище, “ $\cdot$ ” може бути одним із наступних:

$$(1) \ x \cdot y = a(x_1y_1 + 3x_2y_2) + b(x_2y_1 + x_1y_2) + c(-x_1x_2 \binom{y_1}{2} + x_3y_1 + x_1^2y_3);$$

$$(2) \ x \cdot y = a(x_1y_1) + b(x_2y_1 + x_1y_2) + c(-x_1x_2\binom{y_1}{2} + x_3y_1 + x_1^2y_3).$$

Комп'ютерна програма, яка підтвердила, що майже-кільця, отримані в прикладі 5.3, справді є локальними майже-кільцями, розміщена на GitHub.:

https://github.com/raemarina/Examples/blob/main/LNR_81-3.txt

Далі, наведемо ці програми. Спочатку дамо алгоритм для побудови майже-кільця з множенням (1) з прикладу 5.3.

```
# В середовищі системи GAP завантажуюмо пакет LocalNR.
LoadPackage("LocalNR");
# G — група з IdGroup [81, 3].
G := SmallGroup(81, 3);
# gen — список, що містить мінімальну систему твірних.
gen := MinimalGeneratingSet(G);
# Повертаємо список з порядками твірних зі списку gen.
List(gen, Order);
# a — перший елемент зі списку gen.
a := gen[1];
# b — другий елемент зі списку gen.
b := gen[2];
# c — комутатор елементів a та b.
c := a^2 - 1 * b^2 - 1 * a * b;
# mulGR — функція майже-кільцевого добутку.
mulGR := function(x, y)
local x1, x2, x3, y1, y2, y3;
for x1 in [0..8] do
for x2 in [0..2] do
for x3 in [0..2] do
for y1 in [0..8] do
```

```

for y2 in [0..2] do
for y3 in [0..2] do
if  $x = a^{x1} * b^{x2} * c^{x3}$  and  $y = a^{y1} * b^{y2} * c^{y3}$  then return
 $a^{(x1*y1+3*x2*y2)*b^{(x2*y1+x1*y2)*c^{(-x1*x2*Binomial(y1,2)+$ 
 $x3 * y1 + x1^2 * y3); fi;$ 
od; od; od; od; od; od; end;

#  $n$  — майже-кільце на групі  $G$  та з множенням  $mulGR$  (без перевірки).

 $n := ExplicitMultiplicationNearRingNC(G, mulGR);$ 
#  $M$  — таблиця множення майже-кільця  $n$ .
 $M := MultiplicationTable(n);;$ 
#  $mul$  — майже-кільцеве множення, що отримано за допомогою таблиці  $M$ .
 $mu_N R :=$ 
 $NearRingMultiplicationByOperationTable(G, M, AsSortedList(G));$ 
#  $n$  — майже-кільце на групі  $G$  та з множенням  $mul$  (з перевіркою).
 $n := ExplicitMultiplicationNearRing(G, mu_N R);$ 
# Перевірка, чи є майже-кільце  $n$  локальним.
 $IsLocalNearRing(n);$ 

```

Це алгоритм для побудови майже-кільця з множенням (2) з прикладу 5.3.

```

# В середовищі системи GAP завантажуюємо пакет LocalNR.
LoadPackage("LocalNR");
#  $G$  — група з  $IdGroup$  [81, 3].
 $G := SmallGroup(81, 3);$ 
#  $gen$  — список, що містить мінімальну систему твірних.
 $gen := MinimalGeneratingSet(G);$ 
# Повертаємо список з порядками твірних зі списку  $gen$ .

```

```

List(gen, Order);
# a — перший елемент зі списку gen.
a := gen[1];
# b — другий елемент зі списку gen.
b := gen[2];
# c — комутатор елементів a та b.
c := a^ - 1 * b^ - 1 * a * b;
# mulGR — функція майже-кільцевого добутку.
mulGR := function(x, y)
local x1, x2, x3, y1, y2, y3;
for x1 in [0..8] do
for x2 in [0..2] do
for x3 in [0..2] do
for y1 in [0..8] do
for y2 in [0..2] do
for y3 in [0..2] do
if x = a^x1 * b^x2 * c^x3 and y = a^y1 * b^y2 * c^y3 then return
a^(x1 * y1) * b^(x2 * y1 + x1 * y2) * c^(-x1 * x2 * Binomial(y1, 2) + x3 *
y1 + x1^2 * y3); fi;
od; od; od; od; od; od; end;
# n — майже-кільце на групі G та з множенням mulGR (без перевірки).
n := ExplicitMultiplicationNearRingNC(G, mulGR);
# M — таблиця множення майже-кільця n.
M := MultiplicationTable(n);
# mul — майже-кільцеве множення, що отримано за допомогою таблиці M.
mu_NR :=
NearRingMultiplicationByOperationTable(G, M, AsSortedList(G));

```

n — майже-кільце на групі G та з множенням mul (з перевіркою).
 $n := ExplicitMultiplicationNearRing(G, mu_N R);$
 # Перевірка, чи є майже-кільце n локальним.
 $IsLocalNearRing(n);$

З пакету LocalNR та [109] ми маємо наступну кількість усіх неізоморфних нуль-симетричних локальних майже-кілець на G_1 порядків 81 та 625.

$StructureDescription(R^+)$	$n(R^+)$
$(C_9 \times C_3) \rtimes C_3$	46
$(C_{25} \times C_5) \rtimes C_5$	154

5.1.3. Локальні майже-кільця, адитивні групи яких ізоморфні G_4

Нехай R — локальне майже-кільце, адитивна група якого R^+ ізоморфна G_4 . Тоді $R^+ = \langle a \rangle + \langle b \rangle + \langle c \rangle + \langle d \rangle$ для деяких елементів a, b, c та d з R , що задовольняють співвідношення $ap = 0, bp = 0, cp = 0, dp = 0$, $a + b = b + a + c, a + c = c + a, b + c = c + b, d + c = c + d, a + d = d + a$ і $b + d = d + b$. Зокрема, кожен елемент $x \in R$ однозначно записується у вигляді $x = ax_1 + bx_2 + cx_3 + dx_4$ з коефіцієнтами $0 \leq x_1 < p, 0 \leq x_2 < p, 0 \leq x_3 < p$ і $0 \leq x_4 < p$.

Оскільки порядок елемента a дорівнює експоненті групи G , тобто p , то за лемою 2.2 можна вважати, що a є одиницею R , тобто $ax = xa = x$ для кожного $x \in R$. Крім того, для кожного $x \in R$ існують такі коефіцієнти $\alpha(x), \beta(x), \gamma(x), \varphi(x), \lambda(x), \mu(x), \nu(x)$ і $\psi(x)$, що

$$xb = a\alpha(x) + b\beta(x) + c\gamma(x) + d\varphi(x)$$

та

$$xd = a\lambda(x) + b\mu(x) + c\nu(x) + d\psi(x).$$

Зрозуміло, що вони так однозначно визначені за модулем p , що визначено деякі відображення $\alpha: R \rightarrow \mathbb{Z}_p$, $\beta: R \rightarrow \mathbb{Z}_p$, $\gamma: R \rightarrow \mathbb{Z}_p$, $\varphi: R \rightarrow \mathbb{Z}_p$, $\lambda: R \rightarrow \mathbb{Z}_p$, $\mu: R \rightarrow \mathbb{Z}_p$, $\nu: R \rightarrow \mathbb{Z}_p$ та $\psi: R \rightarrow \mathbb{Z}_p$.

Згідно з наслідком 3.5, L є нормальною підгрупою порядку p^3 або p^2 в R . Оскільки L складається з комутаторної підгрупи R^+ , то твірні b та c можна вибрати такими, що $c = -a - b + a + b$. Якщо $|L| = p^3$, то $L = \langle b \rangle + \langle c \rangle + \langle d \rangle$. Оскільки $R^* = R \setminus L$, то впливає

$$R^* = \{ax_1 + bx_2 + cx_3 + dx_4 \mid x_1 \not\equiv 0 \pmod{p}\}$$

і $x = ax_1 + bx_2 + cx_3 + dx_4$ є оборотним тоді і тільки тоді, коли $x_1 \not\equiv 0 \pmod{p}$.

У цьому розділі нехай R буде локальним майже-кільцем з $|R : L| = p$.

Лема 5.4. *Якщо a співпадає з одиничним елементом R , $x = ax_1 + bx_2 + cx_3 + dx_4$, $y = ay_1 + by_2 + cy_3 + dy_4 \in R$, $|R : L| = p$,*

$$xb = a\alpha(x) + b\beta(x) + c\gamma(x) + d\varphi(x)$$

і

$$xd = a\lambda(x) + b\mu(x) + c\nu(x) + d\psi(x),$$

то

$$\begin{aligned} xy = & a(x_1y_1) + b(x_2y_1 + \beta(x)y_2 + \mu(x)y_4) + \\ & + c(-x_1x_2\binom{y_1}{2} + x_3y_1 + \gamma(x)y_2 + x_1\beta(x)y_3 + \nu(x)y_4) + \\ & + d(x_4y_1 + \varphi(x)y_2 + \psi(x)y_4). \end{aligned} \quad (5.1)$$

Більш того, для відображень

$\alpha: R \rightarrow \mathbb{Z}_p$, $\beta: R \rightarrow \mathbb{Z}_p$, $\gamma: R \rightarrow \mathbb{Z}_p$, $\varphi: R \rightarrow \mathbb{Z}_p$, $\lambda: R \rightarrow \mathbb{Z}_p$, $\mu: R \rightarrow \mathbb{Z}_p$, $\nu: R \rightarrow \mathbb{Z}_p$ і $\psi: R \rightarrow \mathbb{Z}_p$ мають місце наступні твердження:

- (0) $\beta(0) \equiv 0 \pmod{p}$, $\gamma(0) \equiv 0 \pmod{p}$, $\varphi(0) \equiv 0 \pmod{p}$,
 $\lambda(0) \equiv 0 \pmod{p}$, $\mu(0) \equiv 0 \pmod{p}$, $\nu(0) \equiv 0 \pmod{p}$ і
 $\psi(0) \equiv 0 \pmod{p}$ тоді і тільки тоді, коли майже-кілець R є нуль-
симетричним;
- (1) $\alpha(x) \equiv 0 \pmod{p}$ and $\lambda(x) \equiv 0 \pmod{p}$;
- (2) якщо $\beta(x) \equiv 0 \pmod{p}$, то $x_1 \equiv 0 \pmod{p}$;
- (3) $\beta(xy) \equiv \beta(x)\beta(y) + \mu(x)\varphi(y) \pmod{p}$;
- (4) $\gamma(xy) \equiv \gamma(x)\beta(y) + x_1\beta(x)\gamma(y) + \nu(x)\varphi(y) \pmod{p}$;
- (5) $\varphi(xy) \equiv \varphi(x)\beta(y) + \psi(x)\varphi(y) \pmod{p}$;
- (6) $\mu(xy) \equiv \beta(x)\mu(y) + \mu(x)\psi(y) \pmod{p}$;
- (7) $\nu(xy) \equiv \gamma(x)\mu(y) + x_1\beta(x)\gamma(y) + \nu(x)\psi(y) \pmod{p}$;
- (8) $\psi(xy) \equiv \varphi(x)\mu(y) + \psi(x)\psi(y) \pmod{p}$.

Доведення. Якщо $|L| = p^3$, то $L = \langle b \rangle + \langle c \rangle + \langle d \rangle$. Оскільки $L \in (R, R)$ -підгрупою в R^+ згідно з твердженням 1) леми 3.4 випливає, що $xb \in L$ і $xd \in L$, звідси $a\alpha(x) \in L$ і $a\lambda(x) \in L$ для кожного $x \in R$. Отже, $\alpha(x) \equiv 0 \pmod{p}$ та $\lambda(x) \equiv 0 \pmod{p}$, тому отримуємо твердження (1). Підставляючи отримане значення $\alpha(x) \equiv 0 \pmod{p}$ і $\lambda(x) \equiv 0 \pmod{p}$ у твердженнях (2)–(4) та (6)–(8) з леми 4.5, отримуємо твердження (3)–(8) леми та формулу множення (5.1). Покладаючи $y = c$, отримуємо $xc = c(x_1\beta(x))$. Отже, якщо $\beta(x) \equiv 0 \pmod{p}$, то $xc = 0$, і тому $x \in L$. Отже, $x_1 \equiv 0 \pmod{p}$, як зазначено в твердженні (2). Дійсно, твердження (0) повторює твердження (0) леми 4.5. $\square$

Далі, ми наведемо приклади локальних майже-кілець.

Лема 5.5. Нехай R — локальне майже-кільце, 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 $\psi: R \rightarrow \mathbb{Z}_p$ з множення $(*)$ може бути одним із наступних:

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

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

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

Доведення. Легко перевірити, що функції з тверджень 1) та 2) задовольняють умови 2)–8) теореми 5.4. $\square$

Як наслідок леми 5.5 маємо наступний результат.

Теорема 5.6. Для кожного непарного простого числа p існує локальне майже-кільце R , адитивна група якого R^+ ізоморфна G_4 .

Приклад 5.7. Нехай $G \cong C_3 \times ((C_3 \times C_3) \rtimes C_3)$. Якщо $x = ax_1 + bx_2 + cx_3 + dx_4$ і $y = ay_1 + by_2 + cy_3 + dy_4 \in G$, та $(G, +, \cdot)$ є локальним майже-кільцем, тоді за лемою 5.5 “ $\cdot$ ” може бути одним із наступних:

$$(1) \ x \cdot y = ax_1y_1 + b(x_2y_1 + x_1y_2) + c(-x_1x_2\binom{y_1}{2} + x_3y_1 + x_1^2y_3) + d(x_4y_1 + x_1y_4);$$

$$(2) \ x \cdot y = ax_1y_1 + b(x_2y_1 + x_1^2y_2) + c(-x_1x_2\binom{y_1}{2} + x_3y_1 + y_3) + d(x_4y_1 + x_1^2y_4);$$

$$(3) \ x \cdot y = ax_1y_1 + b(x_2y_1 + y_2) + c(-x_1x_2\binom{y_1}{2} + x_3y_1 + x_1y_3) + d(x_4y_1 + y_4).$$

Комп’ютерна програма підтвердила, що для $p = 3$ майже-кільце, отримане в лемі 5.5, справді є локальним майже-кільцем, розміщена на GitHub:

https://github.com/raemarina/Examples/blob/main/LNR_81-12.txt

Далі, наведемо ці програми. Спочатку дамо алгоритм для побудови майже-кільця з множенням (1) з прикладу 5.7.

```

# В середовищі системи GAP завантажуюємо пакет LocalNR.
LoadPackage("LocalNR");
#  $G$  — група з IdGroup [81, 12].
 $G := SmallGroup(81, 12)$ ;
#  $gen$  — список, що містить мінімальну систему твірних.
 $gen := MinimalGeneratingSet(G)$ ;
# Повертаємо список з порядками твірних зі списку  $gen$ .
List( $gen$ , Order);
#  $a$  — перший елемент зі списку  $gen$ .
 $a := gen[1]$ ;
#  $b$  — другий елемент зі списку  $gen$ .
 $b := gen[2]$ ;
#  $d$  — третій елемент зі списку  $gen$ .
 $d := gen[3]$ ;
#  $c$  — комутатор елементів  $a$  та  $b$ .
 $c := a^{\wedge} - 1 * b^{\wedge} - 1 * a * b$ ;
#  $psi$  та  $beta$  — функції, які повертають значення  $x$ .
 $psi := function(x)$ 
  return  $x$ ; end;
 $beta := function(x)$ 
  return  $x$ ; end;
#  $mulGR$  — функція майже-кільцевого добутку.
 $mulGR := function(x, y)$ 
  local  $x1, x2, x3, x4, y1, y2, y3, y4$ ;
  for  $x1$  in [0..2] do
  for  $x2$  in [0..2] do
  for  $x3$  in [0..2] do
  for  $x4$  in [0..2] do
  for  $y1$  in [0..2] do

```

```

for y2 in [0..2] do
for y3 in [0..2] do
for y4 in [0..2] do
if x = a^x1 * b^x2 * c^x3 * d^x4 and y = a^y1 * b^y2 * c^y3 *
d^y4 then return
a^(x1*y1)*b^(x2*y1+beta(x1)*y2)*c^(-x1*x2*Binomial(y1,2)+
x3*y1+x1*beta(x1)*y3)*d^(x4*y1+psi(x1)*y4); fi;
od; od; od; od; od; od; od; od; end;
# n — майже-кільце на групі G та з множенням mulGR (без перевірки).
n := ExplicitMultiplicationNearRingNC(G, mulGR);
# M — таблиця множення майже-кільця n.
M := MultiplicationTable(n);
# mul — майже-кільцеве множення, що отримано за допомогою таблиці M.
mu_NR :=
NearRingMultiplicationByOperationTable(G, M, AsSortedList(G));
# n — майже-кільце на групі G та з множенням mul (з перевіркою).
n := ExplicitMultiplicationNearRing(G, mu_NR);
# Перевірка, чи є майже-кільце n локальним.
IsLocalNearRing(n);

```

Це алгоритм для побудови майже-кільця з множенням (2) з прикладу 5.7.

```

# В середовищі системи GAP завантажуюємо пакет LocalNR.
LoadPackage("LocalNR");
# G — група з IdGroup [81, 12].
G := SmallGroup(81, 12);
# gen — список, що містить мінімальну систему твірних.

```

```

gen := MinimalGeneratingSet(G);
# Повертаємо список з порядками твірних зі списку gen.
List(gen, Order);
# a — перший елемент зі списку gen.
a := gen[1];
# b — другий елемент зі списку gen.
b := gen[2];
# d — третій елемент зі списку gen.
d := gen[3];
# c — комутатор елементів a та b.
c :=  $a^{\wedge} - 1 * b^{\wedge} - 1 * a * b$ ;
# psi та beta — функції, які повертають значення  $x^{\wedge}2$ .
psi := function(x)
  return  $x^{\wedge}2$ ; end;
beta := function(x)
  return  $x^{\wedge}2$ ; end;
# mulGR — функція майже-кільцевого добутку.
mulGR := function(x, y)
  local x1, x2, x3, x4, y1, y2, y3, y4;
  for x1 in [0..2] do
    for x2 in [0..2] do
      for x3 in [0..2] do
        for x4 in [0..2] do
          for y1 in [0..2] do
            for y2 in [0..2] do
              for y3 in [0..2] do
                for y4 in [0..2] do
                  if  $x = a^{\wedge}x1 * b^{\wedge}x2 * c^{\wedge}x3 * d^{\wedge}x4$  and  $y = a^{\wedge}y1 * b^{\wedge}y2 * c^{\wedge}y3 * d^{\wedge}y4$  then return

```

```

 $a^{(x1 * y1)} * b^{(x2 * y1 + \text{beta}(x1) * y2)} * c^{(-x1 * x2 * \text{Binomial}(y1, 2) + x3 * y1 + x1 * \text{beta}(x1) * y3)} * d^{(x4 * y1 + \text{psi}(x1) * y4)}; fi;$ 
    od; od; od; od; od; od; od; end;
#  $n$  — майже-кільце на групі  $G$  та з множенням  $mulGR$  (без перевірки).
 $n := \text{ExplicitMultiplicationNearRingNC}(G, mulGR);$ 
#  $M$  — таблиця множення майже-кільця  $n$ .
 $M := \text{MultiplicationTable}(n);;$ 
#  $mul$  — майже-кільцеве множення, що отримано за допомогою таблиці  $M$ .
 $mu_N R :=$ 
 $\text{NearRingMultiplicationByOperationTable}(G, M, \text{AsSortedList}(G));$ 
#  $n$  — майже-кільце на групі  $G$  та з множенням  $mul$  (з перевіркою).
 $n := \text{ExplicitMultiplicationNearRing}(G, mu_N R);$ 
# Перевірка, чи є майже-кільце  $n$  локальним.
 $\text{IsLocalNearRing}(n);$ 

```

Це алгоритм для побудови майже-кільця з множенням (3) з прикладу 5.7.

```

# В середовищі системи GAP завантажуюємо пакет LocalNR.
LoadPackage("LocalNR");
#  $G$  — група з  $\text{IdGroup}$  [81, 12].
 $G := \text{SmallGroup}(81, 12);$ 
#  $gen$  — список, що містить мінімальну систему твірних.
 $gen := \text{MinimalGeneratingSet}(G);$ 
# Повертаємо список з порядками твірних зі списку  $gen$ .
 $\text{List}(gen, \text{Order});$ 
#  $a$  — перший елемент зі списку  $gen$ .

```

```

a := gen[1];
# b — другий елемент зі списку gen.
b := gen[2];
# d — третій елемент зі списку gen.
d := gen[3];
# c — комутатор елементів a та b.
c :=  $a^{\wedge} - 1 * b^{\wedge} - 1 * a * b$ ;
# psi — функція, яка повертає значення 1.
psi := function(x)
  return 1; end;
# beta — функція, яка повертає значення 1.
beta := function(x)
  return 1; end;
# mulGR — функція майже-кільцевого добутку.
mulGR := function(x, y)
  local x1, x2, x3, x4, y1, y2, y3, y4;
  for x1 in [0..2] do
    for x2 in [0..2] do
      for x3 in [0..2] do
        for x4 in [0..2] do
          for y1 in [0..2] do
            for y2 in [0..2] do
              for y3 in [0..2] do
                for y4 in [0..2] do
                  if  $x = a^{\wedge}x1 * b^{\wedge}x2 * c^{\wedge}x3 * d^{\wedge}x4$  and  $y = a^{\wedge}y1 * b^{\wedge}y2 * c^{\wedge}y3 * d^{\wedge}y4$  then return
                     $a^{\wedge}(x1*y1) * b^{\wedge}(x2*y1 + beta(x1)*y2) * c^{\wedge}(-x1*x2*Binomial(y1, 2) +$ 
 $x3*y1 + x1*beta(x1)*y3) * d^{\wedge}(x4*y1 + psi(x1)*y4);$  fi;
                  od; od; od; od; od; od; od; od; od; end;
                od;
              od;
            od;
          od;
        od;
      od;
    od;
  od;

```

n — майже-кільце на групі G та з множенням $mulGR$ (без перевірки).

$n := ExplicitMultiplicationNearRingNC(G, mulGR);$

M — таблиця множення майже-кільця n .

$M := MultiplicationTable(n);;$

mul — майже-кільцеве множення, що отримано за допомогою таблиці M .

$mu_N R :=$

$NearRingMultiplicationByOperationTable(G, M, AsSortedList(G));$

n — майже-кільце на групі G та з множенням mul (з перевіркою).

$n := ExplicitMultiplicationNearRing(G, mu_N R);$

Перевірка, чи є майже-кільце n локальним.

$IsLocalNearRing(n);$

З пакету LocalNR та [109] маємо наступну кількість усіх неізоморфних нуль-симетричних локальних майже-кільць на G_4 порядків 81 та 625.

$StructureDescription(R^+)$	$n(R^+)$
$C_3 \times ((C_3 \times C_3) \rtimes C_3)$	794
$ R : L = 3$	782
$ R : L = 9$	12
$C_5 \times ((C_5 \times C_5) \rtimes C_5)$	2090
$ R : L = 5$	2078
$ R : L = 25$	12

5.1.4. Локальні майже-кільця, адитивні групи яких ізоморфні G_5

Нехай R — локальне майже-кільце, адитивна група якого R^+ ізоморфна G_5 . Тоді $R^+ = \langle a \rangle + \langle b \rangle + \langle c \rangle$ з елементами a, b і c , де a співпадає з одиничним елементом R та справедливі співвідношення $ap^2 = bp = cp = 0$, $a + b = b + a(1 - p)$, $a + c = c + a$ та $b + c = c + b$. Більш того, кожен елемент $x \in R$ однозначно записується у вигляді $x = ax_1 + bx_2 + cx_3$ з коефіцієнтами $0 \leq x_1 < p^2$, $0 \leq x_2 < p$ і $0 \leq x_3 < p$.

Розглянемо, що a так співпадає з одиничним елементом R , що $xa = ax = x$ для кожного $x \in R$. Крім того, для кожного $x \in R$ існують такі цілі числа $\alpha(x)$, $\beta(x)$, $\gamma(x)$, $\nu(x)$, $\mu(x)$ і $\phi(x)$, що

$$xb = a\alpha(x) + b\beta(x) + c\gamma(x)$$

та

$$xc = a\nu(x) + b\mu(x) + c\phi(x).$$

Зрозуміло, що за модулем p^2 , p , p та p^2 , p , p відповідно ці цілі числа однозначно визначаються x , тому визначаються деякі 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 $\phi: R \rightarrow \mathbb{Z}_p$.

Згідно з наслідком 3.5, L є нормальною підгрупою порядку p^3 або p^2 в R . Нехай у цьому розділі R буде локальним майже-кільцем з $|R : L| = p$.

Якщо $|L| = p^3$, то $L = \langle ap \rangle + \langle b \rangle + \langle c \rangle$. Оскільки $R^* = R \setminus L$, то випливає, що

$$R^* = \{ax_1 + bx_2 + cx_3 \mid x_1 \not\equiv 0 \pmod{p}\}$$

та $x = ax_1 + bx_2 + cx_3$ є оборотним тоді і тільки тоді, коли $x_1 \not\equiv 0 \pmod{p}$. Оскільки $L \in (R, R)$ -підгрупою в R^+ згідно з твердженням 1)

леми 3.4, то $xb \in L$ та $xc \in L$, отже, $a\alpha(x) \in L$ та $a\nu(x) \in L$ для кожного $x \in R$. Отже, $\alpha(x) \equiv 0 \pmod{p}$ та $\nu(x) \equiv 0 \pmod{p}$, як у твердженні (2) леми 4.8. Отже, для локальних майже-кілець R маємо таке ж множення, як і для майже-кілець з одиницею, тобто множення (4.7).

Лема 5.8. *Нехай $x = ax_1 + bx_2 + cx_3$ і $y = ay_1 + by_2 + cy_3$ є елементами R та $|R : L| = p$. Якщо a збігається з одиничним елементом R , то множення (4.7) виконується для відображень з леми 4.8.*

Далі, наведемо приклади локальних майже-кілець.

Лема 5.9. *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:*

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

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

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

Доведення. Легко перевірити, що функції з тверджень 1) та 2) задовольняють умови 1)–8) леми 4.8. □

Як наслідок леми 5.9 маємо наступний результат.

Теорема 5.10. *Для кожного непарного простого числа p існує локальне майже-кілець R , адитивна група якого R^+ ізоморфна G_5 .*

Приклад 5.11. Нехай $G \cong (C_9 \rtimes C_3) \times C_3$. Якщо $x = ax_1 + bx_2 + cx_3$ і $y = ay_1 + by_2 + cy_3 \in G$, та $(G, +, \cdot)$ є локальним майже-кілецем, тоді за лемою 5.5 “ $\cdot$ ” може бути одним із наступних:

$$(1) \ x \cdot y = a(x_1y_1 + 3x_1x_2\binom{y_1}{2}) + b(x_2y_1 + \beta(x)y_2) + c(x_3y_1 + \phi(x)y_3), \text{ де}$$

$$\beta(x) = \phi(x) = \begin{cases} 1, & x_1 \not\equiv 0 \pmod{3}; \\ 0, & x_1 \equiv 0 \pmod{3}, \end{cases}$$

$$(2) \ x \cdot y = a(x_1y_1 + 3x_1x_2\binom{y_1}{2}) + b(x_2y_1 + y_2) + c(x_3y_1 + y_3).$$

Комп'ютерна програма підтвердила, що для $p = 3$ майже-кільце, отримане в лемі 5.9, справді є локальним майже-кільцем, розміщена на GitHub:

https://github.com/raemarina/Examples/blob/main/LNR_81-13.txt

Це алгоритм для побудови майже-кільця з множенням 1) з прикладу 5.11.

```
# В середовищі системи GAP завантажуюмо пакет LocalNR.
LoadPackage("LocalNR");
# G — група з IdGroup [81, 13].
G := SmallGroup(81, 13);
# gen — список, що містить мінімальну систему твірних.
gen := MinimalGeneratingSet(G);
# Повертаємо список з порядками твірних зі списку gen.
List(gen, Order);
# a — перший елемент зі списку gen.
a := gen[1];
# b — другий елемент зі списку gen.
b := gen[2];
# c — третій елемент зі списку gen.
c := gen[3];
# mulGR — функція майже-кільцевого добутку.
mulGR := function(x, y)
```

```

local x1, x2, x3, y1, y2, y3;
for x1 in [0..8] do
for x2 in [0..2] do
for x3 in [0..2] do
for y1 in [0..8] do
for y2 in [0..2] do
for y3 in [0..2] do
if  $x = a^{x1} * b^{x2} * c^{x3}$  and  $y = a^{y1} * b^{y2} * c^{y3}$  then return
 $a^{(x1 * y1 + x1 * x2 * \text{Binomial}(y1, 2) * 3) * b^{(x2 * y1 + y2) * c^{(x3 * y1 + y3)}}$ ; fi;
od; od; od; od; od; od; end;
#  $n$  — майже-кільце на групі  $G$  та з множенням  $mulGR$  (без перевірки).
 $n := \text{ExplicitMultiplicationNearRingNC}(G, mulGR);$ 
#  $M$  — таблиця множення майже-кільця  $n$ .
 $M := \text{MultiplicationTable}(n);;$ 
#  $mul$  — майже-кільцеве множення, що отримано за допомогою таблиці  $M$ .
 $mu_N R :=$ 
 $\text{NearRingMultiplicationByOperationTable}(G, M, \text{AsSortedList}(G));$ 
#  $n$  — майже-кільце на групі  $G$  та з множенням  $mul$  (з перевіркою).
 $n := \text{ExplicitMultiplicationNearRing}(G, mu_N R);$ 
# Перевірка, чи є майже-кільце  $n$  локальним.
 $\text{IsLocalNearRing}(n);$ 

```

Це алгоритм для побудови майже-кільця з множенням 2) з прикладу 5.11.

В середовищі системи GAP завантажуюємо пакет LocalNR.

```

LoadPackage("LocalNR");
#  $G$  — група з IdGroup [81, 13].
 $G := \text{SmallGroup}(81, 13)$ ;
#  $gen$  — список, що містить мінімальну систему твірних.
 $gen := \text{MinimalGeneratingSet}(G)$ ;
# Повертаємо список з порядками твірних зі списку  $gen$ .
List( $gen$ , Order);
#  $a$  — перший елемент зі списку  $gen$ .
 $a := gen[1]$ ;
#  $b$  — другий елемент зі списку  $gen$ .
 $b := gen[2]$ ;
#  $c$  — третій елемент зі списку  $gen$ .
 $c := gen[3]$ ;
#  $phi$  та  $beta$  — функції, які повертають значення 1 або 0.
 $phi := \text{function}(x)$ 
if  $x \bmod 3 \neq 0$  then return 1;
else return 0; fi; end;
 $beta := \text{function}(x)$ 
if  $x \bmod 3 \neq 0$  then return 1;
else return 0; fi; end;
#  $mulGR$  — функція майже-кільцевого добутку.
 $mulGR := \text{function}(x, y)$ 
local  $x1, x2, x3, y1, y2, y3$ ;
for  $x1$  in [0..8] do
for  $x2$  in [0..2] do
for  $x3$  in [0..2] do
for  $y1$  in [0..8] do
for  $y2$  in [0..2] do
for  $y3$  in [0..2] do

```

```

    if  $x = a^{\wedge}x1 * b^{\wedge}x2 * c^{\wedge}x3$  and  $y = a^{\wedge}y1 * b^{\wedge}y2 * c^{\wedge}y3$  then return
     $a^{\wedge}(x1 * y1 + x1 * x2 * \text{Binomial}(y1, 2) * 3) * b^{\wedge}(x2 * y1 + \text{beta}(x1) * y2) * c^{\wedge}(x3 * y1 + \text{phi}(x1) * y3); fi;$ 
    od; od; od; od; od; od; end;
    #  $n$  — майже-кільце на групі  $G$  та з множенням  $mulGR$  (без перевірки).
     $n := \text{ExplicitMultiplicationNearRingNC}(G, mulGR);$ 
    #  $M$  — таблиця множення майже-кільця  $n$ .
     $M := \text{MultiplicationTable}(n);;$ 
    #  $mul$  — майже-кільцеве множення, що отримано за допомогою таблиці  $M$ .
     $mu_N R :=$ 
     $\text{NearRingMultiplicationByOperationTable}(G, M, \text{AsSortedList}(G));$ 
    #  $n$  — майже-кільце на групі  $G$  та з множенням  $mul$  (з перевіркою).
     $n := \text{ExplicitMultiplicationNearRing}(G, mu_N R);$ 
    # Перевірка, чи є майже-кільце  $n$  локальним.
     $\text{IsLocalNearRing}(n);$ 
    З пакету LocalNR та [109] маємо таку кількість усіх неізоморфних локальних майже-кілець на групах  $G_5$  порядків 81 та 625.

```

$StructureDescription(R^+)$	$n(R^+)$
$(C_9 \times C_3) \rtimes C_3$	337
$(C_{25} \times C_5) \rtimes C_5$	630

5.1.5. Групи G_6

Нехай G_6 — адитивно записана група з теореми 4.1. Тоді $G_6 = \langle a \rangle + \langle b \rangle + \langle c \rangle$ для деяких елементів a, b та c з R , що задовольняють

співвідношення $ap^2 = 0$, $bp = 0$, $cp = 0$, $a + b = b + a$, $a + c = c + a$, $c + b = b + c + ap$.

Лема 5.12. G_6 не є ендоциклічним.

Доведення. Розглянемо групу $G_6 = \langle a, b, c : ap^2 = bp = cp = 0, a + b = b + a, a + c = c + a, c + b = b + c + ap \rangle$. Оскільки підгрупа $\langle ap \rangle$ є єдиною підгрупою порядку p^2 , то $\langle ap \rangle$ є фіксованою під дією $\text{End } G_6$. Отже, G_6 не є ендоциклічним за означенням 2.3. $\square$

Гіпотеза 5.13. Не існує локального майже-кільця, адитивна група якого ізоморфна G_6 .

5.2. Локальні майже-кільця на групах порядку p^4 та класу нільпотентності 3

5.2.1. Локальні майже-кільця, адитивні групи яких ізоморфні H_1

Нехай R — локальне майже-кільце, адитивна група якого R^+ ізоморфна H_1 . Тоді $R^+ = \langle a \rangle + \langle b \rangle + \langle c \rangle + \langle d \rangle$ для деяких елементів a, b, c і d з R задовольняючи співвідношення $ap = bp = cp = dp = 0$, $b + c = c + b$, $a + d = d + a$, $b + d = d + b$, де $c = -a - b + a + b$ і $d = -a - c + a + c$. Зокрема, кожен елемент $x \in R$ однозначно записується у вигляді $x = ax_1 + bx_2 + cx_3 + dx_4$ з коефіцієнтами $0 \leq x_1 < p$, $0 \leq x_2 < p$, $0 \leq x_3 < p$ і $0 \leq x_4 < p$.

Оскільки порядок елемента a дорівнює експоненті групи G , тобто p , звідси випливає, що ми можемо припустити, що a є одиницею R , тобто

$ax = xa = x$ для кожного $x \in R$. Крім того, для кожного $x \in R$ існують такі коефіцієнти $\alpha(x)$, $\beta(x)$, $\gamma(x)$, $\phi(x)$, що

$$xb = a\alpha(x) + b\beta(x) + c\gamma(x) + d\phi(x).$$

Зрозуміло, що вони однозначно визначені за модулем p , так що визначені деякі відображення $\alpha: R \rightarrow \mathbb{Z}_p$, $\beta: R \rightarrow \mathbb{Z}_p$, $\gamma: R \rightarrow \mathbb{Z}_p$, $\phi: R \rightarrow \mathbb{Z}_p$.

Згідно з наслідком 3.5, L є нормальною підгрупою порядку p^3 або p^2 в R .

У цьому розділі нехай R буде локальним майже-кільцем з $|R : L| = p$.

Теорема 5.14. *Нехай R — локальне майже-кільце, адитивна група якого R^+ ізоморфна групі H_1 , та $|R : L| = p$. Тоді $R^+ = \langle a \rangle + \langle b \rangle + \langle c \rangle + \langle d \rangle$, $ap = bp = cp = dp = 0$, $b+c = c+b$, $a+d = d+a$, $b+d = d+b$, де $c = -a - b + a + b$, $d = -a - c + a + c$. Якщо a співпадає з одиничним елементом R , тоді виконуються наступні твердження:*

- 1) $L = \langle b \rangle + \langle c \rangle + \langle d \rangle$ і $R^* = \{ax_1 + bx_2 + cx_3 + cx_4 \mid x_1 \not\equiv 0 \pmod{p}\}$;
- 2) $xb = b\beta(x) + c\gamma(x) + d\phi(x)$;
- 3) $xc = cx_1\beta(x) + d(x_1\gamma(x) - \beta(x)\binom{x_1}{2})$;
- 4) $xd = dx_1^2\beta(x)$.

Доведення. Оскільки L складається з комутаторної підгрупи R^+ , то твірні b , d та c можна вибрати такими, що $c = -a - b + a + b$ і $d = -a - c + a + c$. Якщо $|L| = p^3$, то $L = \langle b \rangle + \langle c \rangle + \langle d \rangle$ і $L \in (R, R)$ -підгрупою в R^+ згідно з твердженням 1) леми 3.4, $xb \in L$, отже, $a\alpha(x) \in L$ для кожного $x \in R$. Тому $\alpha(x) \equiv 0 \pmod{p}$, і так

$$xb = b\beta(x) + c\gamma(x) + d\phi(x)$$

і твердження 2) виконується. Оскільки $R^* = R \setminus L$, то випливає

$$R^* = \{ax_1 + bx_2 + cx_3 + cx_4 \mid x_1 \not\equiv 0 \pmod{p}\}$$

і $x = ax_1 + bx_2 + cx_3 + dx_4 \in$ оборотним тоді і тільки тоді, коли $x_1 \not\equiv 0 \pmod{p}$, як зазначено в твердженні 1).

Якщо, замінюючи $\alpha(x) \equiv 0 \pmod{p}$ на 1) і 2) теореми 4.17, ми отримуємо

$$xc = cx_1\beta(x) + d(x_1\gamma(x) - \beta(x)\binom{x_1}{2})$$

і $xd = dx_1^2\beta(x)$. □

Як наслідок леми 4.17 та теореми 5.14 маємо наступне твердження.

Наслідок 5.15. *Якщо a співпадає з одиничним елементом R , $x = ax_1 + bx_2 + cx_3 + dx_4$, $y = ay_1 + by_2 + cy_3 + dy_4 \in R$ і $|R : L| = p$, тоді*

$$\begin{aligned} xy = & a(x_1y_1) + b(x_2y_1 + \beta(x)y_2) + c(x_3y_1 - x_1x_2\binom{y_1}{2}) + \\ & + x_1\beta(x)y_3 + \gamma(x)y_2) + d(x_4y_1 + x_2\binom{x_1}{2}\binom{y_1}{2} - \\ & - x_1x_3\binom{y_1}{2} + x_1^2x_2\binom{y_1}{y_1-3}) + \phi(x)y_2 + x_1\gamma(x)y_3 - \\ & - \beta(x)\binom{x_1}{2}y_3 + x_1^2\beta(x)y_4). \end{aligned} \quad (5.2)$$

Більш того, для відображень $\beta: R \rightarrow \mathbb{Z}_p$, $\gamma: R \rightarrow \mathbb{Z}_p$, $\phi: R \rightarrow \mathbb{Z}_p$ мають місце наступні твердження:

(0) $\beta(0) \equiv 0 \pmod{p}$, $\gamma(0) \equiv 0 \pmod{p}$, $\phi(0) \equiv 0 \pmod{p}$ тоді і тільки тоді, коли майже-кілець R є нуль-симетричним;

(1) $\beta(xy) \equiv \beta(x)\beta(y) \pmod{p}$;

(2) $\gamma(xy) \equiv x_1\beta(x)\gamma(y) \pmod{p}$;

(3) $\phi(xy) \equiv \phi(x)\beta(y) + x_1\gamma(x)\gamma(y) - \beta(x)\binom{x_1}{2}\gamma(y) + x_1^2\beta(x)\phi(y) \pmod{p}$.

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

Лема 5.16. 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 $\phi: R \rightarrow \mathbb{Z}_p$ з множення (5.2) може бути $\beta(x) \equiv x_1^2 \pmod{p}$ та

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

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

Доведення. Легко перевірити, що функції β та γ задовольняють умови 1)–2) наслідку 5.15. Оскільки $\gamma(x) \equiv 0 \pmod{p}$, то випливає, що

$$\phi(xy) = \phi(x)\beta(y) + x_1^2\beta(x)\phi(y).$$

Якщо $x_1y_1 \not\equiv 0 \pmod{p}$, то $\phi(xy) = 0 = \phi(x)\beta(y)$. Для $x_1y_1 \equiv 0 \pmod{p}$ нам потрібно перевірити три випадки.

1) якщо $x_1 \equiv 0 \pmod{p}$ і $y_1 \not\equiv 0 \pmod{p}$, то

$$\phi(xy) = (x_2y_1)^2 = x_2^2y_1^2 = \phi(x)\beta(y);$$

2) якщо $x_1 \not\equiv 0 \pmod{p}$ і $y_1 \equiv 0 \pmod{p}$, то

$$\phi(xy) = (x_2^2y_1)^2 = x_2^4y_1^3 = \phi(x)\beta(y);$$

3) якщо $x_1 \equiv 0 \pmod{p}$ і $y_1 \equiv 0 \pmod{p}$, то

$$\phi(xy) = 0 = \phi(x)\beta(y).$$

Виводимо умови 3) наслідку 5.15. □

Як наслідок леми 5.16 маємо наступний результат.

Теорема 5.17. Для кожного простого числа $p > 3$ існує локальне майже-кільце R , адитивна група якого R^+ ізоморфна H_1 .

Приклад 5.18. Нехай $G \cong (C_5 \times C_5 \times C_5) \rtimes C_5$. Якщо $x = ax_1 + bx_2 + cx_3 + dx_4$ і $y = ay_1 + by_2 + cy_3 + dy_4 \in G$, та $(G, +, \cdot)$ є локальним майже-кільцем, тоді за лемою 5.16 “ $\cdot$ ” може бути наступним:

$$\begin{aligned} x \cdot y = & a(x_1y_1) + b(x_2y_1 + \beta(x)y_2) + c(x_3y_1 - \\ & - x_1x_2 \binom{y_1}{2} + x_1\beta(x)y_3) + d(x_4y_1 + \\ & + x_2 \binom{x_1}{2} \binom{y_1}{2} - x_1x_3 \binom{y_1}{2} + \\ & + x_1^2x_2 \binom{y_1}{y_1-3}) + \phi(x)y_2 - \beta(x) \binom{x_1}{2} y_3 + x_1^2\beta(x)y_4, \end{aligned}$$

де $\beta(x) \equiv x_1^2 \pmod{5}$ і

$$\phi(x) = \begin{cases} x_2^2, & x_1 \equiv 0 \pmod{5}; \\ 0, & x_1 \not\equiv 0 \pmod{5}. \end{cases}$$

Комп’ютерна програма підтвердила, що для $p = 5$ майже-кільце, отримане в лемі 5.16, справді є локальним майже-кільцем, розміщена на GitHub:

https://github.com/raemarina/Examples/blob/main/LNR_625-7.txt

Це алгоритм для побудови майже-кільця з множенням з прикладу 5.18.

```
# В середовищі системи GAP завантажуюємо пакет LocalNR.
LoadPackage("LocalNR");
# G — група з IdGroup [625, 7].
G := SmallGroup(625, 7);
# gen — список, що містить мінімальну систему твірних.
gen := MinimalGeneratingSet(G);
# Повертаємо список з порядками твірних зі списку gen.
List(gen, Order);
```

```

# a — перший елемент зі списку gen.
a := gen[1];
# b — другий елемент зі списку gen.
b := gen[2];
# c — комутатор елементів a та b.
c := a^ - 1 * b^ - 1 * a * b;
# d — комутатор елементів a та c.
d := a^ - 1 * c^ - 1 * a * c;
# beta — функція, яка повертає значення  $x^2$  по mod 5.
beta := function(x)
return x^2 mod 5; end;
# phi — функція, яка повертає значення  $y^2$  по mod 5 або 0.
phi := function(x, y)
if x = 0 mod 5 then return y^2 mod 5;
else return 0; fi; end;
# mulGR — функція майже-кільцевого добутку.
mulGR := function(x, y)
local x1, x2, x3, x4, y1, y2, y3, y4;
for x1 in [0..4] do
for x2 in [0..4] do
for x3 in [0..4] do
for x4 in [0..4] do
for y1 in [0..4] do
for y2 in [0..4] do
for y3 in [0..4] do
for y4 in [0..4] do
if x = a^x1 * b^x2 * c^x3 * d^x4 and y = a^y1 * b^y2 * c^y3 * d^y4
then return a^(x1*y1) * b^(x2*y1 + beta(x1)*y2) * c^(x3*y1 - x1*x2 *
Binomial(y1, 2) + x1*beta(x1)*y3) * d^(x4*y1 - x1*x3 * Binomial(y1, 2) +

```

$x2 * \text{Binomial}(y1, 2) * \text{Binomial}(x1, 2) + x1^2 * x2 * (\text{Binomial}(y1, y1 - 3) \bmod 5) + \text{phi}(x1, x2) * y2 - \text{beta}(x1) * \text{Binomial}(x1, 2) * y3 + x1^2 * \text{beta}(x1) * y4); fi;$

od; od; od; od; od; od; od; end;

n — майже-кільце на групі G та з множенням $mulGR$ (без перевірки).

$n := \text{ExplicitMultiplicationNearRingNC}(G, mulGR);$

M — таблиця множення майже-кільця n .

$M := \text{MultiplicationTable}(n);;$

mul — майже-кільцеве множення, що отримано за допомогою таблиці M .

$mu_N R :=$

$\text{NearRingMultiplicationByOperationTable}(G, M, \text{AsSortedList}(G));$

n — майже-кільце на групі G та з множенням mul (з перевіркою).

$n := \text{ExplicitMultiplicationNearRing}(G, mu_N R);$

Перевірка, чи є майже-кільце n локальним.

$\text{IsLocalNearRing}(n);$

З пакету LocalNR та [109] ми маємо наступну кількість усіх неізоморфних нуль-симетричних локальних майже-кілець на H_1 порядку 625.

$\text{IdGroup}(R^+)$	$\text{IdGroup}(R^*)$	$\text{StructureDescription}(R^*)$	$n(R^*)$
[625, 7]	[500, 21]	$((C_5 \times C_5) \rtimes C_5) \rtimes C_4$	45
103	[500, 42]	$C_5 \times ((C_5 \times C_5) \rtimes C_4)$	34
	[500, 44]	$C_5 \times ((C_5 \times C_5) \rtimes C_4)$	6
	[500, 46]	$(C_5 \times C_5 \times C_5) \rtimes C_4$	18

5.2.2. Локальні майже-кільця, адитивні групи яких ізоморфні H_2

Нехай R — локальне майже-кільце, адитивна група якого R^+ ізоморфна H_2 . Тоді $R^+ = \langle a \rangle + \langle b \rangle + \langle c \rangle$ для деяких елементів $a, b, c \in R$, які задовольняють відношення $ap^2 = bp = cp = 0$, $b+c = c+b$, $-a-c+a+c = ap$, де $c = -a-b+a+b$. Зокрема, кожен елемент $x \in R$ однозначно записується у вигляді $x = ax_1 + bx_2 + cx_3$ з коефіцієнтами $0 \leq x_1 < p^2$, $0 \leq x_2 < p$ і $0 \leq x_3 < p$.

Оскільки порядок елемента a дорівнює експоненті групи G , тобто p^2 , то можна вважати, що a є одиничним елементом в R , тобто $ax = xa = x$ для кожного $x \in R$. Крім того, для кожного $x \in R$ існують такі коефіцієнти $\alpha(x)$, $\beta(x)$, $\gamma(x)$, що

$$xb = a\alpha(x) + b\beta(x) + c\gamma(x).$$

Зрозуміло, що вони однозначно визначені по модулю p^2 , p та p , тому визначені відображення $\alpha: R \rightarrow \mathbb{Z}_{p^2}$, $\beta: R \rightarrow \mathbb{Z}_p$ та $\gamma: R \rightarrow \mathbb{Z}_p$.

За наслідком 3.5, L є нормальною підгрупою порядку p^3 або p^2 в R .

У цьому розділі нехай R — локальне майже-кільце з $|R : L| = p$.

Теорема 5.19. *Нехай R — локальне майже-кільце, адитивна група якого R^+ ізоморфна H_2 та $|R : L| = p$. Тоді $R^+ = \langle a \rangle + \langle b \rangle + \langle c \rangle$ для деяких елементів $a, b, c \in R$, які задовольняють співвідношення $ap^2 = bp = cp = 0$, $b+c = c+b$, $-a-c+a+c = ap$, де $c = -a-b+a+b$. Якщо a збігається з одиницею в R , то справедливі такі твердження:*

1)

$$L = \langle ap \rangle + \langle b \rangle + \langle c \rangle$$

та

$$R^* = \{ax_1 + bx_2 + cx_3 \mid x_1 \not\equiv 0 \pmod{p}\};$$

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

3) $xc = a(-\binom{x_1}{2}\beta(x))p + c(x_1\beta(x))$.

Доведення. Якщо $|L| = p^3$, то $L = \langle ap \rangle + \langle b \rangle + \langle c \rangle$ та $L \in (R, R)$ -підгрупою R^+ із твердження 1) леми 3.4 випливає, що

$$xb = a\alpha(x) + b\beta(x) + c\gamma(x) \in L,$$

звідки $a\alpha(x) \in L$ для кожного $x \in R$. Тоді $\alpha(x) \equiv 0 \pmod{p}$, і тому виконується твердження 2). Оскільки $R^* = R \setminus L$, то

$$R^* = \{ax_1 + bx_2 + cx_3 \mid x_1 \not\equiv 0 \pmod{p}\}$$

та $x = ax_1 + bx_2 + cx_3$ є оберненим тоді і тільки тоді, коли $x_1 \not\equiv 0 \pmod{p}$, як стверджується в умові 1).

Далі, підставляючи $\alpha(x) \equiv 0 \pmod{p}$ в умову 3) леми 4.22, отримаємо

$$xc = a\left(-\binom{x_1}{2}\beta(x)\right)p + c(x_1\beta(x)).$$

□

Як наслідок леми 4.22 і теореми 5.19 маємо наступне твердження.

Наслідок 5.20. *Нехай R — локальне майже-кільце, адитивна група якого R^+ ізоморфна H_2 та $|R : L| = p$. Якщо a збігається з одиничним елементом R , $x = ax_1 + bx_2 + cx_3$, $y = ay_1 + by_2 + cy_3 \in R$, то*

$$\begin{aligned} xy = & a(x_1y_1 + \alpha(x)y_2 + \left(\binom{x_1}{2}\binom{y_1}{2}\right)x_2 - \\ & - x_1x_3\binom{y_1}{2} + x_1^2x_2\binom{y_1}{3} - \\ & - \left(\binom{x_1}{2}\beta(x)y_3\right)p) + b(x_2y_1 + \beta(x)y_2) + \\ & + c(x_3y_1 - x_1x_2\binom{y_1}{2} + \gamma(x)y_2 + x_1\beta(x)y_3). \end{aligned} \quad (5.3)$$

Більш того, для відображень

$\alpha: R \rightarrow \mathbb{Z}_{p^2}$, $\beta: R \rightarrow \mathbb{Z}_p$ та $\gamma: R \rightarrow \mathbb{Z}_p$ виконуються наступні твердження:

- (0) $\alpha(0) \equiv 0 \pmod{p^2}$, $\beta(0) \equiv 0 \pmod{p}$ та $\gamma(0) \equiv 0 \pmod{p}$ тоді і тільки тоді, коли майже-кільце R є нуль-симетричним;
- (1) $\alpha(a) \equiv 0 \pmod{p^2}$, $\beta(a) \equiv 1 \pmod{p}$, $\gamma(a) \equiv 0 \pmod{p}$;
- (2) $\alpha(x) \equiv 0 \pmod{p}$;
- (3) якщо $x_1 \not\equiv 0 \pmod{p}$, то $\beta(x) \equiv 1 \pmod{p}$;
- (4) $\alpha(xy) \equiv x_1\alpha(y) + \alpha(x)\beta(y) - \binom{x_1}{2}\beta(x)\gamma(y)p \pmod{p^2}$;
- (5) $\beta(xy) \equiv \beta(x)\beta(y) \pmod{p}$;
- (6) $\gamma(xy) \equiv \gamma(x)\beta(y) + x_1\beta(x)\gamma(y) \pmod{p}$.

5.2.3. Групи H_2 як адитивні групи локальних майже-кільць

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

Теорема 5.21. Для кожного простого $p > 3$ існує локальне майже-кільце R , адитивна група якого R^+ ізоморфна H_2 .

Доведення. Нехай G — адитивно записана група H_2 з твірними a, b, c , що задовольняють співвідношення $ap^2 = bp = cp = 0$, $b + c = c + b$, $-a - c + a + c = ap$, де $c = -a - b + a + b$. Тоді $G = \langle a \rangle + \langle b \rangle + \langle c \rangle$ і кожен елемент $x \in G$ однозначно записується у вигляді $x = ax_1 + bx_2 + cx_3$ з коефіцієнтами $0 \leq x_1 < p^2$, $0 \leq x_2 < p$ і $0 \leq x_3 < p$. Визначимо таке множення “ $\cdot$ ” на G , щоб $R = (G, +, \cdot)$ було локальним майже-кільцем.

Визначаємо множення $x \cdot y$ за (5.3), де $\alpha(x) \equiv 0 \pmod{p^2}$, $\beta(x) \equiv x_1^{p-2} \pmod{p}$ та $\gamma(x) \equiv 0 \pmod{p}$. Позначимо $x_1 \pmod{p}$ через $\bar{x}_1$. Тоді маємо

$$x \cdot y = a(x_1y_1 + \left(\binom{x_1}{2}\binom{y_1}{2}x_2 - x_1x_3\binom{y_1}{2}\right) + \quad (5.4)$$

$$+x_1^2x_2\binom{y_1}{3}-\binom{x_1}{2}\bar{x}_1^{p-2}y_3)p)+b(x_2y_1+\\ +\bar{x}_1^{p-2}y_2)+c(x_3y_1-x_1x_2\binom{y_1}{2}+\bar{x}_1^{p-2}x_1y_3).$$

Очевидно, що існує таке k , для якого має місце $x_1 \equiv \bar{x}_1 + kp \pmod{p^2}$, де $0 \leq k \leq p-1$. Звідси та малої теореми Ферма маємо

$$\bar{x}_1^{p-2}x_1 \equiv \bar{x}_1^{p-1} \equiv 1 \pmod{p}.$$

Тоді $px_1 \equiv p\bar{x}_1 \pmod{p^2}$ та $x_1 \equiv \bar{x}_1 \pmod{p}$. Зрозуміло, що

$$p\bar{x}_1^{p-1} \equiv p \pmod{p^2}.$$

Легко перевірити, що функції α , β і γ задовольняють умови (2), (3), (5)–(7) наслідку 5.20.

Нехай елемент a є мультиплікативною одиницею в $(G, \cdot)$ і

$$xb = a\alpha(x) + b\beta(x) + c\gamma(x)$$

для кожного $x \in G$. Покажемо, що відносно операцій “+” і “ $\cdot$ ” система $R = (G, +, \cdot)$ є майже-кільцем з одиничним елементом a . Очевидно, що достатньо перевірити, що

$$x \cdot (y + z) = x \cdot y + x \cdot z$$

для довільних $z = az_1 + bz_2 + cz_3$ з R і

$$(x \cdot y) \cdot z = x \cdot (y \cdot z).$$

Дійсно, за формулою (5.4) маємо

$$x \cdot z = a(x_1z_1 + (\binom{x_1}{2}\binom{z_1}{2}x_2 - x_1x_3\binom{z_1}{2}) + \\ + x_1^2x_2\binom{z_1}{3} - \binom{x_1}{2}\bar{x}_1^{p-2}z_3)p) +$$

$$+b(x_2z_1 + \bar{x}_1^{p-2}z_2) + c(x_3z_1 - x_1x_2\binom{z_1}{2} + \bar{x}_1^{p-2}x_1z_3).$$

Оскільки

$$y + z = ay_1 + by_2 + cy_3 + az_1 + bz_2 + cz_3 = ay_1 + by_2 +$$

$$az_1(1 - y_3p)cy_3 + bz_2 + cz_3 = a(y_1 + z_1 + \\ + (\binom{z_1}{2}y_2 - z_1y_3)p) + b(y_2 + z_2) + c(y_3 + z_3 - y_2z_1),$$

то

$$\begin{aligned} x \cdot (y + z) &= a(x_1(y_1 + z_1 + (\binom{z_1}{2}y_2 - z_1y_3)p) + \\ &+ (\binom{x_1}{2}\binom{y_1 + z_1}{2}x_2 - x_1x_3\binom{y_1 + z_1}{2} + \\ &+ x_1^2x_2\binom{y_1 + z_1}{3} - \binom{x_1}{2}\bar{x}_1^{p-2}(y_3 + z_3 - y_2z_1))p) + \\ &+ b(x_2(y_1 + z_1) + \bar{x}_1^{p-2}(y_2 + z_2)) + c(x_3(y_1 + z_1) - \\ &- x_1x_2\binom{y_1 + z_1}{2} + \bar{x}_1^{p-1}(y_3 + z_3 - y_2z_1)) = \\ &= a(x_1(y_1 + z_1) + (x_1\binom{z_1}{2}y_2 - x_1y_3z_1 + \\ &+ \binom{x_1}{2}x_2\binom{y_1 + z_1}{2} - x_1x_3\binom{y_1 + z_1}{2} + x_1^2x_2\binom{y_1 + z_1}{3} - \\ &- \binom{x_1}{2}\bar{x}_1^{p-2}(y_3 + z_3) + \binom{x_1}{2}\bar{x}_1^{p-2}y_2z_1)p) + b(x_2(y_1 + z_1) + \\ &+ \bar{x}_1^{p-2}(y_2 + z_2)) + c(x_3(y_1 + z_1) - x_1x_2\binom{y_1 + z_1}{2} + \\ &+ (y_3 + z_3) - y_2z_1). \end{aligned}$$

З іншого боку,

$$x \cdot y + x \cdot z = a(x_1y_1 + (\binom{x_1}{2}\binom{y_1}{2}x_2 - x_1x_3\binom{y_1}{2} +$$

$$\begin{aligned}
& +x_1^2x_2\binom{y_1}{3} - \binom{x_1}{2}\bar{x}_1^{p-2}y_3)p) + b(x_2y_1 + \bar{x}_1^{p-2}y_2) + \\
& +c(x_3y_1 - x_1x_2\binom{y_1}{2} + \bar{x}_1^{p-1}y_3) + a(x_1z_1 + (\binom{x_1}{2}\binom{z_1}{2}x_2 - \\
& - x_1x_3\binom{z_1}{2} + x_1^2x_2\binom{z_1}{3} - \binom{x_1}{2}\bar{x}_1^{p-2}z_3)p) + \\
& +b(x_2z_1 + \bar{x}_1^{p-2}z_2) + c(x_3z_1 - x_1x_2\binom{z_1}{2} + \bar{x}_1^{p-1}z_3) = \\
& = a(x_1y_1 + (\binom{x_1}{2}\binom{y_1}{2}x_2 - x_1x_3\binom{y_1}{2} + x_1^2x_2\binom{y_1}{3} - \\
& - \binom{x_1}{2}\bar{x}_1^{p-2}y_3)p) + b(x_2y_1 + \bar{x}_1^{p-2}y_2) + a(x_1z_1 + \\
& + (\binom{x_1}{2}\binom{z_1}{2}x_2 - x_1x_3\binom{z_1}{2} + x_1^2x_2\binom{z_1}{3} - \\
& - \binom{x_1}{2}\bar{x}_1^{p-2}z_3)p)(1 - (x_3y_1 - x_1x_2\binom{y_1}{2} + \bar{x}_1^{p-1}y_3)p) + \\
& +c(x_3y_1 - x_1x_2\binom{y_1}{2} + \bar{x}_1^{p-1}y_3) + b(x_2z_1 + \\
& + \bar{x}_1^{p-2}z_2) + c(x_3z_1 - x_1x_2\binom{z_1}{2} + \bar{x}_1^{p-1}z_3).
\end{aligned}$$

За лемами 4.18–4.20, маємо

$$\begin{aligned}
& = a(x_1y_1 + (\binom{x_1}{2}\binom{y_1}{2}x_2 - x_1x_3\binom{y_1}{2} + x_1^2x_2\binom{y_1}{3} - \\
& - \binom{x_1}{2}\bar{x}_1^{p-2}y_3)p) + b(x_2y_1 + \bar{x}_1^{p-2}y_2) + a(x_1z_1 + \\
& + (\binom{x_1}{2}\binom{z_1}{2}x_2 - x_1x_3\binom{z_1}{2} + x_1^2x_2\binom{z_1}{3} - \\
& - \binom{x_1}{2}\bar{x}_1^{p-2}z_3 - x_1x_3y_1z_1 + x_1^2x_2\binom{y_1}{2}z_1 - \bar{x}_1^py_3z_1)p) + \\
& +c(x_3y_1 - x_1x_2\binom{y_1}{2} + \bar{x}_1^{p-1}y_3) + b(x_2z_1 + \bar{x}_1^{p-2}z_2) +
\end{aligned}$$

$$+c(x_3z_1 - x_1x_2\binom{z_1}{2} + \bar{x}_1^{p-1}z_3).$$

Далі,

$$\begin{aligned} &= a(x_1y_1 + (\binom{x_1}{2}\binom{y_1}{2}x_2 - x_1x_3\binom{y_1}{2} + x_1^2x_2\binom{y_1}{3} - \\ &\quad - \binom{x_1}{2}\bar{x}_1^{p-2}y_3)p) + a(x_1z_1 + (\binom{x_1}{2}\binom{z_1}{2}x_2 - \\ &\quad - x_1x_3\binom{z_1}{2} + x_1^2x_2\binom{z_1}{3} - \binom{x_1}{2}\bar{x}_1^{p-2}z_3 - \\ &\quad - x_1x_3y_1z_1 + x_1^2x_2\binom{y_1}{2}z_1 - \bar{x}_1^py_3z_1)p) + \\ &\quad + \binom{x_1z_1}{2}(x_2y_1 + x_1^{p-2}y_2)p) + b(x_2y_1 + \bar{x}_1^{p-2}y_2) - \\ &\quad - cx_1z_1(x_2y_1 + \bar{x}_1^{p-2}y_2) + c(x_3y_1 - x_1x_2\binom{y_1}{2} + \bar{x}_1^{p-1}y_3) + \\ &\quad + b(x_2z_1 + \bar{x}_1^{p-2}z_2) + c(x_3z_1 - x_1x_2\binom{z_1}{2} + \bar{x}_1^{p-1}z_3). \end{aligned}$$

В результаті, отримуємо

$$\begin{aligned} &a(x_1(y_1 + z_1) + (\binom{x_1}{2}x_2(\binom{y_1}{2} + \binom{z_1}{2})) - x_1x_3(\binom{y_1}{2} + \\ &\quad + \binom{z_1}{2})) + x_1^2x_2(\binom{y_1}{3} + \binom{z_1}{3}) - \binom{x_1}{2}\bar{x}_1^{p-2}(y_3 + z_3) - \\ &\quad - x_1x_3y_1z_1 + x_1^2x_2(\binom{y_1}{2}z_1 - \bar{x}_1y_3z_1 + \binom{x_1z_1}{2}x_2y_1 + \\ &\quad + \binom{x_1z_1}{2}\bar{x}_1^{p-2}y_2)p) + b(x_2(y_1 + z_1) + \bar{x}_1^{p-2}(y_2 + z_2)) + \\ &\quad + c(x_3(y_1 + z_1) - x_1x_2(\binom{y_1}{2} + \binom{z_1}{2}) + y_1z_1) + \\ &\quad + (y_3 + z_2) - y_2z_1). \end{aligned}$$

Відмітимо наступні конгруентності та тотожності, які використаємо при доведенні лівої дистрибутивності.

По-перше,

$$\begin{aligned} \binom{x_1 z_1}{2} \bar{x}_1^{p-2} y_2 &= \frac{1}{2} (x_1^2 z_1^2 - x_1 z_1) \bar{x}_1^{p-2} y_2 = \\ &= \frac{1}{2} (\bar{x}_1^p y_2 z_1^2 - \bar{x}_1^{p-1} y_2 z_1) \equiv \frac{1}{2} (\bar{x}_1 z_1^2 y_2 - y_2 z_1) \pmod{p^2} \end{aligned}$$

та

$$x_1 \binom{z_1}{2} y_2 + \binom{x_1}{2} \bar{x}_1^{p-2} y_2 z_1 \equiv \frac{1}{2} (\bar{x}_1 z_1^2 y_2 - y_2 z_1) \pmod{p^2}.$$

Тому

$$\binom{x_1 z_1}{2} \bar{x}_1^{p-2} y_2 \equiv x_1 \binom{z_1}{2} y_2 + \binom{x_1}{2} \bar{x}_1^{p-2} y_2 z_1 \pmod{p^2}.$$

По-друге,

$$\binom{x_1}{2} x_2 \binom{y_1 + z_1}{2} = \binom{x_1}{2} x_2 \left(\binom{y_1}{2} + \binom{z_1}{2} + y_1 z_1 \right).$$

Прирівнюючи коефіцієнти при твірній a у результатах для $x \cdot (y + z)$ та $x \cdot y + x \cdot z$, отримаємо

$$\begin{aligned} \binom{x_1}{2} x_2 y_1 z_1 + x_1^2 x_2 \binom{y_1 + z_1}{2} &\equiv x_1^2 x_2 \left(\binom{y_1}{3} + \binom{z_1}{3} \right) + \\ &+ x_1^2 x_2 \binom{y_1}{2} z_1 - \binom{x_1 z_1}{2} x_2 y_1 \pmod{p^2}. \end{aligned}$$

Далі,

$$\begin{aligned} &\frac{1}{2} (x_1^2 x_2 y_1 z_1 - x_1 x_2 y_1 z_1) + \frac{1}{6} x_1^2 x_2 (y_1^3 + \\ &+ 3y_1^2 z_1 + 3y_1 z_1^2 + z_1^3 - 3y_1^2 - 6y_1 z_1 - 3z_1^2 + 2y_1 + 2z_1) \equiv \\ &\frac{1}{6} x_1^2 x_2 (y_1^3 - 3y_1^2 + 2y_1 + z_1^3 - 3z_1^2 + 2z_1) + \frac{1}{2} (x_1^2 x_2 y_1^2 z_1 - \\ &- x_1^2 x_2 y_1 z_1 + x_1^2 x_2 y_1 z_1^2 - x_1 x_2 y_1 z_1) \pmod{p^2}. \end{aligned}$$

Спростивши, маємо:

$$-x_1^2 x_2 y_1 z_1 + \frac{1}{2} x_1^2 x_2 y_1 z_1 \equiv -\frac{1}{2} x_1^2 x_2 y_1 z_1 \pmod{p^2}.$$

Звідси та прирівнявши коефіцієнти при твірних b та c , маємо

$$x \cdot (y + z) = x \cdot y + x \cdot z.$$

Далі, перевіримо асоціативність множення.

З одного боку, маємо

$$\begin{aligned}
 (x \cdot y) \cdot z &= a(x_1 y_1 z_1 + \binom{x_1}{2} \binom{y_1}{2} x_2 - x_1 x_3 \binom{y_1}{2} + \\
 &+ x_1^2 x_2 \binom{y_1}{3} - \binom{x_1}{2} \bar{x}_1^{p-2} y_3) z_1 + \binom{x_1 y_1}{2} \binom{z_1}{2} (x_2 y_1 + \\
 &+ \bar{x}_1^{p-2} y_2) - x_1 y_1 (x_3 y_1 - x_1 x_2 \binom{y_1}{2} + \bar{x}_1^{p-1} y_3) \binom{z_1}{2} + \\
 &+ x_1^2 y_1^2 (x_2 y_1 + \bar{x}_1^{p-2} y_2) \binom{z_1}{3} - \binom{x_1 y_1}{2} \bar{x}_1^{p-2} \bar{y}_1^{p-2} z_3) p) + \\
 &+ b((x_2 y_1 + \bar{x}_1^{p-2} y_2) z_1 + \bar{x}_1^{p-2} \bar{y}_1^{p-2} z_2) + c((x_3 y_1 - x_1 x_2 \binom{y_1}{2} + \\
 &+ \bar{x}_1^{p-1} y_3) z_1 - x_1 y_1 (x_2 y_1 + \bar{x}_1^{p-2} y_2) \binom{z_1}{2} + \bar{x}_1^{p-1} \bar{y}_1^{p-1} z_3) = \\
 &= a(x_1 y_1 z_1 + \binom{x_1}{2} \binom{y_1}{2} x_2 z_1 - x_1 x_3 \binom{y_1}{2} z_1 + x_1^2 x_2 \binom{y_1}{3} z_1 - \\
 &- \binom{x_1}{2} \bar{x}_1^{p-2} y_3 z_1 + \binom{x_1 y_1}{2} \binom{z_1}{2} x_2 y_1 + \binom{x_1 y_1}{2} \binom{z_1}{2} \bar{x}_1^{p-2} y_2 - \\
 &- x_1 x_3 y_1^2 \binom{z_1}{2} + x_1^2 x_2 y_1 \binom{y_1}{2} \binom{z_1}{2} - x_1 y_1 y_3 \binom{z_1}{2} + \\
 &+ x_1^2 y_1^3 x_2 \binom{z_1}{3} + \bar{x}_1^p y_1^2 y_2 \binom{z_1}{3} - \binom{x_1 y_1}{2} \bar{x}_1^{p-2} \bar{y}_1^{p-2} z_3) p) + \\
 &+ b(x_2 y_1 z_1 + \bar{x}_1^{p-2} y_2 z_1 + \bar{x}_1^{p-2} \bar{y}_1^{p-2} z_2) + c(x_3 y_1 z_1 - \\
 &- x_1 x_2 \binom{y_1}{2} z_1 + \bar{x}_1^{p-1} y_3 z_1 - x_1 x_2 y_1^2 - \\
 &- \bar{x}_1^{p-1} y_1 y_2 \binom{z_1}{2} + \bar{x}_1^{p-1} \bar{y}_1^{p-1} z_3).
 \end{aligned}$$

З іншого боку, маємо

$$\begin{aligned}
x \cdot (y \cdot z) &= a(x_1(y_1z_1 + (\binom{y_1}{2} \binom{z_1}{2} y_2 - y_1y_3 \binom{z_1}{2}) + \\
&+ y_1^2y_2 \binom{z_1}{3} - \binom{y_1}{2} \bar{y}_1^{p-2} z_3)p) + (\binom{x_1}{2} \binom{y_1z_1}{2} x_2 - \\
&- x_1x_2 \binom{y_1z_1}{2} + x_1^2x_2 \binom{y_1z_1}{3} - \binom{x_1}{2} \bar{x}_1^{p-2} (y_3z_1 - \\
&- y_1y_2 \binom{z_1}{2} + \bar{y}_1^{p-1} z_3)p) + b(x_2y_1z_1 + \bar{x}_1^{p-2} (y_2z_1 + \\
&+ \bar{y}_1^{p-2} z_2)) + c(x_3y_1z_1 - x_1x_2 \binom{y_1z_1}{2} + \bar{x}_1^{p-1} (y_3z_1 - \\
&- y_1y_2 \binom{z_1}{2} + \bar{y}_1^{p-1} z_3) = a(x_1y_1z_1 + (x_1 \binom{y_1}{2} \binom{z_1}{2} y_2 - \\
&- x_1y_1y_3 \binom{z_1}{2} + x_1y_1^2y_2 \binom{z_1}{3} - x_1 \binom{y_1}{2} \bar{y}_1^{p-2} z_3 + \\
&+ \binom{x_1}{2} \binom{y_1z_1}{2} x_2 - x_1x_2 \binom{y_1z_1}{2} + x_1^2x_2 \binom{y_1z_1}{3} - \\
&- \binom{x_1}{2} \bar{x}_1^{p-2} y_3z_1 + \binom{x_1}{2} \bar{x}_1^{p-2} y_1y_2 \binom{z_1}{2} - \\
&- \binom{x_1}{2} \bar{x}_1^{p-2} \bar{y}_1^{p-2} z_3)p) + b(x_2y_1z_1 + \bar{x}_1^{p-2} y_2z_1 + \\
&+ \bar{x}_1^{p-2} \bar{y}_1^{p-2} z_2) + c(x_3y_1z_1 - x_1x_2 \binom{y_1z_1}{2} + y_3z_1 - \\
&- y_1y_2 \binom{z_1}{2} + z_3).
\end{aligned}$$

Отже,

$$x \cdot (y \cdot z) = (x \cdot y) \cdot z.$$

Тому $R = (G, +, \cdot)$ є майже-кільце з одиничним елементом a .

Для завершення доведення залишається показати, що множина всіх необоротних елементів $R = (G, +, \cdot)$ збігається з $L = \langle ap \rangle + \langle b \rangle + \langle c \rangle$. Тому

достатньо довести, що елемент $x = ax_1 + bx_2 + cx_3$ оборотний справа тоді і тільки тоді, коли $x_1 \not\equiv 0 \pmod{p}$.

Справді, якщо існує такий елемент $y = ay_1 + by_2 + cy_3$, що $x \cdot y = a$, то

$$x_1y_1 + \left(\binom{x_1}{2} \binom{y_1}{2} x_2 - x_1x_3 \binom{y_1}{2} + x_1^2x_2 \binom{y_1}{3} - \right. \\ \left. - \binom{x_1}{2} \bar{x}_1^{p-2}y_3 \right)p \equiv 1 \pmod{p^2}$$

за нашим визначенням $x \cdot y$. Звідки $x_1y_1 \equiv 1 \pmod{p^2}$, а отже, $x_1 \equiv 1 \pmod{p}$.

І навпаки, якщо виконується остання конгруенція, то $\beta(x) \equiv 1 \pmod{p}$ за (3) наслідку 5.20. Тому існують такі натуральні числа y_1 , y_2 та y_3 , що $x_1y_1 \equiv 1 \pmod{p^2}$,

$$x_2y_1 + \bar{x}_1^{p-2}y_2 \equiv 0 \pmod{p}$$

та

$$x_3z_1 - x_1x_2 \binom{z_1}{2} + \bar{x}_1^{p-2}x_1z_3 \equiv 0 \pmod{p}.$$

Покладемо $y = ay_1 + by_2 + cy_3$ та

$$z_1 = 1 + \left(\binom{x_1}{2} \binom{y_1}{2} x_2 - x_1x_3 \binom{y_1}{2} + \right. \\ \left. + x_1^2x_2 \binom{y_1}{3} - \binom{x_1}{2} \bar{x}_1^{p-2}y_3 \right)p.$$

Але тоді $x \cdot y = az_1$. Оскільки $\alpha(x) \equiv 0 \pmod{p}$, то існує таке натуральне число s , що $z_1s \equiv 1 \pmod{p^2}$, звідки

$$x \cdot (ys) = (x \cdot y)s = (az_1)s = a.$$

Тому елемент x оборотний справа. Таким чином, майже-кільце R є локальним, і це завершує доведення. $\square$

Наведемо приклад локального майже-кільця порядку $5^4 = 625$, адитивна група якого R^+ ізоморфна H_2 .

Приклад 5.22. Нехай $G \cong (C_{25} \rtimes C_5) \rtimes C_5$. Якщо $x = ax_1 + bx_2 + cx_3$, $y = ay_1 + by_2 + cy_3 \in G$ та $(G, +, \cdot)$ є локальне майже-кільце, тоді згідно прикладу з теореми 5.21 функції α , β і γ можуть бути наступними: $\alpha(x) \equiv 0 \pmod{25}$, $\beta(x) \equiv x_1^3 \pmod{5}$ та $\gamma(x) \equiv 0 \pmod{5}$. Підставивши ці функції у формулу (5.4) маємо:

$$\begin{aligned} x \cdot y = & a(x_1y_1 + \left(\binom{x_1}{2}\binom{y_1}{2}x_2 - x_1x_3\binom{y_1}{2} + \right. \\ & \left. + x_1^2x_2\binom{y_1}{y_1-3} - \binom{x_1}{2}\bar{x}_1^3y_3)p) + \\ & + b(x_2y_1 + \bar{x}_1^3y_2) + c(x_3y_1 - x_1x_2\binom{y_1}{2} + x_1\bar{x}_1^3y_3). \end{aligned}$$

Комп'ютерна програма, яка будує майже-кільце з прикладу 5.22, наведено нижче, а також розміщено на GitHub:

https://github.com/raemarina/Examples/blob/main/LNR_625-8.txt

```
# В середовищі системи GAP завантажуюмо пакет LocalNR.
LoadPackage("LocalNR");
# G — група з IdGroup [625, 8].
G := SmallGroup(625, 8);
# gen — список, що містить мінімальну систему твірних.
gen := MinimalGeneratingSet(G);
# Повертаємо список з порядками твірних зі списку gen.
List(gen, Order);
# a — перший елемент зі списку gen.
a := gen[1];
# b — другий елемент зі списку gen.
b := gen[2];
```

```

# c — комутатор елементів a та b.
c := a^1 - 1 * b^1 - 1 * a * b;
# alpha та gamma — функції, які повертають значення 0.
alpha := function(x, y, z)
return 0; fi; end;
gamma := function(x)
return 0; end;
# beta — функція, яка повертає значення  $x^3$  по mod 5.
beta := function(x)
return x^3 mod 5; end;
# mulGR — функція майже-кільцевого добутку.
mulGR := function(x, y)
local x1, x2, x3, y1, y2, y3;
for x1 in [0..24] do
for x2 in [0..4] do
for x3 in [0..4] do
for y1 in [0..24] do
for y2 in [0..4] do
for y3 in [0..4] do
if x = a^x1 * b^x2 * c^x3 and y = a^y1 * b^y2 * c^y3 then return
a^(x1*y1 + alpha(x1, x2, x3)*y2 + (Binomial(x1, 2)*Binomial(y1, 2)*
x2 - x1 * x3 * Binomial(y1, 2) + x1^2 * x2 * Binomial(y1, y1 - 3) -
Binomial(x1, 2)*beta(x1)*y3)*5)*b^(x2*y1 + beta(x1)*y2)*c^(x3*y1 -
x1 * x2 * Binomial(y1, 2) + gamma(x1) * y2 + x1 * beta(x1) * y3); fi;
od; od; od; od; od; od; end;
# n — майже-кільце на групі G та з множенням mulGR (без перевірки).
n := ExplicitMultiplicationNearRingNC(G, mulGR);
# M — таблиця множення майже-кільця n.

```

```

M := MultiplicationTable(n);;
# mul — майже-кільцеве множення, що отримано за допомогою та-
блиці M.
mu_NR :=
NearRingMultiplicationByOperationTable(G, M, AsSortedList(G));
# n — майже-кільце на групі G та з множенням mul (з перевіркою).
N := ExplicitMultiplicationNearRing(G, mu_NR);
# Перевірка, чи є майже-кільце n локальним.
IsLocalNearRing(n);

```

З пакету LocalNR та [109] маємо наступну кількість усіх неізоморфних нуль-симетричних локальних майже-кілець на групі H_2 порядку 625.

$IdGroup(R^+)$	$IdGroup(R^*)$	$StructureDescription(R^*)$	$n(R^*)$
[625, 8]	[500, 42]	$C_5 \times ((C_5 \times C_5) \rtimes C_4)$	125

5.2.4. Групи H_3 та H_4

Проаналізувавши групи H_3 та H_4 порядку 625 за допомогою GAP, з'ясували, що не існує локальних майже-кілець на цих групах. Це дозволяє зробити наступне припущення.

Гіпотеза 5.23. Не існує локального майже-кільця, адитивна група якого ізоморфна H_3 чи H_4 .

Висновки до розділу 5

У даному розділі:

- описано локальні майже-кільця з адитивними групами порядку p^4 ;
- вказано формули множення для таких майже-кілець та описано функції, що їх задають;
- наведено приклад локального майже-кільця порядку $5^4 = 625$;
- дано алгоритм побудови локального майже-кільця з неабелевою адитивною групою порядку 5^4 , що реалізовано в системі комп'ютерної алгебри GAP.

Основні результати даного розділу опубліковано у працях [9, 10, 5] зі списку публікацій і, відповідно, [96–98] зі списку використаних джерел, а також опубліковано у тезах конференцій [26, 27, 28] і, відповідно, [92–94].

Розділ 6

Майже-кілець з одиницею на деяких неабелевих групах

У даному розділі описано всі можливі типи груп Міллера–Морено, які можуть бути адитивними групами майже-кілець з одиницею. Показано, що не існує майже-кілець з одиницею, адитивна група яких ізоморфна групі Шмідта. Досліджуються прямі добутки p -груп Міллера–Морено та циклічних p -груп як адитивні групи майже-кілець з одиницею та локальних майже-кілець.

6.1. Групи Міллера–Морено та Шмідта

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 Редеї (див., [118]).

Теорема 6.1. *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.

Нагадаємо, що групою Шмідта або мінімальною ненільпотентною називається скінченна ненільпотентна група, будь-яка власна підгрупа якої нільпотентна.

Наступна теорема описує будову груп Шмідта та доведена в статті [17].

Теорема 6.2. *Скінченна група G тоді і лише тоді являється групою Шмідта, коли вона розкладається в напівпрямий добуток $G = S \rtimes T$ своєї нормальної силовської s -підгрупи S порядку s^α , $\alpha \geq 1$, та силовської t -підгрупи $T = \langle b \rangle$ порядку t^β , $\beta \geq 1$, та задовольняє наступним умовам:*

- 1) $Z(G) = \Phi(G) = \Phi(S) \times \langle b^t \rangle$, де $\Phi(G)$ підгрупа Фраттіні групи G ;
- 2) $G' = S$, $S' = \Phi(S)$, $G'' = S'$ експонента S' не перевищує число s ;
- 3) якщо S — неабелева, то $Z(S) = S' = \Phi(S)$.

6.2. Майже-кільця з одиницею на групах Міллера–Морено

Будь-яка група Міллера–Морено типу 4) теореми 6.1 не має елемента, порядок якого співпадає з її експонентою. Звідси та з леми 2.2 випливає таке твердження.

Лема 6.3. *Не існує майже-кільця з одиницею, адитивна група якого ізоморфна групі типу 4) теореми 6.1.*

Доведення. Нехай R — майже-кільце з одиницею, адитивна група R^+ якого ізоморфна групі G . Оскільки експонента групи G дорівнює pq^s , то за лемою 2.2 група R^+ містить елемент g порядку pq^s . Але тоді $G = P < g >$ і тому перетин $P \cap < g >$ є нормальною підгрупою порядку p в G . В силу того, що P — мінімальна нормальна підгрупа в G , звідси випливає $P = P \cap < g >$, отже, $G = < g >$. Отримане протиріччя завершує доведення леми. $\square$

Далі ми використовуємо такі позначення:

- 1) $G(p^m, p^n)$ позначає адитивно записану групу типу 2) теореми 6.1 з такими твірними a і b порядків p^m і p^n , відповідно, що $-b + a + b = a(1 + p^{m-1})$;
- 2) $G(p^m, p^n, p)$ позначає адитивно записану групу типу 3) теореми 6.1 з такими твірними a , b і c порядків p^m , p^n і p , відповідно, що $-b + a + b = a + c$ і $-b + c + b = c$.

Леми 6.4 і 6.5 легко отримати простими обчисленнями.

Лема 6.4. *У групі $G(p^m, p^n)$ для будь-яких натуральних чисел r , s та t , виконуються рівності*

$$bs + ar = ar(1 - sp^{m-1}) + bs$$

i

$$(ar + bs)t = ar\left(t - s\binom{t}{2}p^{m-1}\right) + bst.$$

Лема 6.5. *Експонента групи $G(p^m, p^n)$ дорівнює p^m для $m > n$ і p^n для $m \leq n$. Більш того, якщо x є елементом максимального порядку в $G(p^m, p^n)$, то існують такі твірні a , b цієї групи, що або $x = a$, або*

$x = b$ та виконуються співвідношення $ap^m = bp^n = 0$ і $-b + a + b = a(1 + p^{m-1})$.

Нехай адитивна група майже-кільця R з одиницею ізоморфна групі $G(p^m, p^n)$. З леми 6.5 випливає, що $R^+ = \langle a \rangle + \langle b \rangle$ з елементами a, b один з яких збігається з одиницею R та виконуються співвідношення $ap^m = bp^n = 0$ і $a + b = b + a(1 + p^{m-1})$. Більш того, кожен елемент $x \in R$ однозначно записується у вигляді $x = ax_1 + bx_2$ з коефіцієнтами $0 \leq x_1 < p^m$ і $0 \leq x_2 < p^n$.

Розглянемо випадок, коли a збігається з одиницею R так, що $xa = ax = x$ для кожного $x \in R$. Тоді R^+ має експоненту p^m згідно з лемою 6.5, тому $m \geq n$. Крім того, для кожного $x \in R$ існують такі цілі числа $\alpha(x)$ і $\beta(x)$, що $xb = a\alpha(x) + b\beta(x)$. Зрозуміло, що за модулем p^m і p^n , відповідно, ці цілі числа однозначно визначаються x , і тому визначаються деякі відображення $\alpha : R \rightarrow \mathbb{Z}_{p^m}$ і $\beta : R \rightarrow \mathbb{Z}_{p^n}$.

Лема 6.6. *Нехай $x = ax_1 + bx_2$ і $y = ay_1 + by_2$ є елементами в R . Якщо a збігається з одиницею R , то $m \geq n + 1$ і*

$$\begin{aligned} xy = a[(x_1y_1 + \alpha(x)y_2) - (x_1x_2 \binom{y_1}{2} + \alpha(x)x_2y_1y_2 + \\ + \alpha(x)\beta(x) \binom{y_2}{2})p^{m-1}] + b(x_2y_1 + \beta(x)y_2). \end{aligned}$$

Більш того, для відображень $\alpha : R \rightarrow \mathbb{Z}_{p^m}$ і $\beta : R \rightarrow \mathbb{Z}_{p^n}$ справедливі наступні 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) $\alpha(x) \equiv 0 \pmod{p^{m-n}}$, крім випадку $p = 2 = m$ і $n = 1$;
- (3) $x_1(\beta(x) - 1) \equiv x_2\alpha(x) \pmod{p}$;

$$(4) \quad \alpha(xy) = x_1\alpha(y) + \alpha(x)\beta(y) - \\ - [x_1x_2\binom{\alpha(y)}{2} + \alpha(x)x_2\alpha(y)\beta(y) + \alpha(x)\beta(x)\binom{\beta(y)}{2}]p^{m-1};$$

$$(5) \quad \beta(xy) = x_2\alpha(y) + \beta(x)\beta(y).$$

Доведення. За лівим дистрибутивним законом, маємо

$$xy = (xa)y_1 + (xb)y_2 = (ax_1 + bx_2)y_1 + (a\alpha(x) + b\beta(x))y_2.$$

Крім того, лема 6.4 означає, що

$$(ax_1 + bx_2)y_1 = ax_1(y_1 - x_2\binom{y_1}{2}p^{m-1}) + bx_2y_1,$$

$$(a\alpha(x) + b\beta(x))y_2 = a\alpha(x)(y_2 - \beta(x)\binom{y_2}{2}p^{m-1}) + b\beta(x)y_2$$

і

$$bx_2y_1 + a\alpha(x)(y_2 - \beta(x)\binom{y_2}{2}p^{m-1}) = \\ = a\alpha(x)(y_2 - \beta(x)\binom{y_2}{2}p^{m-1})(1 - x_2y_1p^{m-1}) + bx_2y_1.$$

Отже,

$$xy = a[(x_1y_1 + \alpha(x)y_2) - (x_1x_2\binom{y_1}{2} + \alpha(x)x_2y_1y_2 + \\ + \alpha(x)\beta(x)\binom{y_2}{2})p^{m-1}] + b(x_2y_1 + \beta(x)y_2), \quad (6.1)$$

як вимагалось.

Як $0 \cdot a = a \cdot 0 = 0$, майже-кільце R є нуль-симетричним тоді і тільки тоді, коли

$$0 = 0 \cdot b = a\alpha(0) + b\beta(0),$$

звідки $\alpha(0) = \beta(0) = 0$. Так само з рівності $b = ab = a\alpha(a) + b\beta(a)$ з цього випливає, що $\alpha(a) = 0$ і $\beta(a) = 1$. Оскільки $(xb)p^n = x(bp^n) = 0$ і $xb = a\alpha(x) + b\beta(x)$, маємо

$$0 = (a\alpha(x) + b\beta(x))p^n = a\alpha(x)(p^n - \beta(x)\binom{p^n}{2}p^{m-1})$$

за лемою 6.4 і, отже, $\alpha(x) \equiv 0 \pmod{p^{m-n}}$, крім випадку $p = 2 = m$ і $n = 1$, в якій група R^+ є групою діедра порядку 8. Далі, якщо $y = a(1 - p^{m-1}) + b$, то

$$xy = a[\alpha(x) + x_1 - (x_1 + \alpha(x)x_2)p^{m-1}] + b(x_2(1 - p^{m-1}) + \beta(x))$$

за формулою (6.1). З іншого боку, $y = b + a$ і так

$$xy = xb + x = a(\alpha(x) + x_1 - x_1\beta(x)p^{m-1}) + b(x_2 + \beta(x))$$

за лемою 6.4. Порівнюючи обидва результати для xy , отримуємо

$$(x_1 + \alpha(x)x_2)p^{m-1} \equiv x_1\beta(x)p^{m-1} \pmod{p^m}$$

і

$$x_2(1 - p^{m-1}) + \beta(x) \equiv x_2 + \beta(x) \pmod{p^n}.$$

Отже, $m \geq n + 1$ і

$$x_1(\beta(x) - 1) \equiv x_2\alpha(x) \pmod{p},$$

тому виконується твердження (3).

Нарешті, асоціативність множення в R означає, що

$$x(yb) = (xy)b = a\alpha(xy) + b\beta(xy).$$

Крім того, заміна $yb = a\alpha(y) + b\beta(y)$ замість y в формулі (6.1), також маємо

$$\begin{aligned} x(yb) = & a[(x_1\alpha(y) + \alpha(x)\beta(y)) - (x_1x_2\binom{\alpha(y)}{2} + \alpha(x)x_2\alpha(y)\beta(y) + \\ & + \alpha(x)\beta(x)\binom{\beta(y)}{2})p^{m-1}] + b(x_2\alpha(y) + \beta(x)\beta(y)). \end{aligned}$$

Порівнюючи коефіцієнти при a і b у двох виразах, отриманих для $x(yb)$, отримуємо твердження (4) і (5) леми. Лему доведено. $\square$

Як висновок узагальнимо результати, отримані в [12] і [102].

Теорема 6.7. 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-кілля з одиницею.

Теорема 6.8. 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 6.7, або групою $G(4, 2)$.

Доведення. Нехай існує майже-кілля R з одиницею i , адитивною групою якого є G . Оскільки G не може бути ізоморфним Q_8 за результатом Клея [31], то з теореми 6.1 і леми 6.3 випливає, що G ізоморфна одній із груп $G(p^m, p^n)$ чи $G(p^m, p^n, p)$ для відповідного простого p і натуральних чисел m, n . Найменшою з цих груп є дієдральна група $G(4, 2)$, на якій існує майже-кілля R з одиницею за іншим результатом Клея, згаданим у вступі.

Далі, групи $G(p^m, p^n)$ з $p^{m+n} > 8$ і $m > n$, $G(2^m, 2^n)$ з $m \leq n$ і $G(p^m, p^n, p)$ з $m + n > 2$ для $p = 2$ є групи з теореми 6.7. Тому залишається розглянути лише випадок, коли G ізоморфна $G(p^m, p^n)$ з $m \leq n$ і $p > 2$.

Оскільки i є елементом максимального порядку G за лемою 2.2, то з леми 6.5 що існують такі твірні a порядку p^m і b порядку p^n цієї групи,

що

$$-b + a + b = a(1 + p^{m-1})$$

і $a = i$ або $b = i$. Якщо $a = i$, то $m = n$, що неможливо за лемою 6.6. Покажемо, що випадок $b = i$ також неможливий.

Припустимо протилежне, так що для кожного $x \in R$ маємо $xb = x$. Оскільки x однозначно записується у вигляді $x = ax_1 + bx_2$ з коефіцієнтами $0 \leq x_1 < p^m$ і $0 \leq x_2 < p^n$, існують коефіцієнти $\alpha(x)$ і $\beta(x)$ такий як $xa = a\alpha(x) + b\beta(x)$. Більш того, це випливає з [102], лема 8, що вони задовольняють наступним умовам:

$$(1) \quad \alpha(b) \equiv 1 \pmod{p^m} \text{ і } \beta(b) \equiv 0 \pmod{p^n};$$

$$(2) \quad \alpha(x)(1 - x_2) \equiv 0 \pmod{p};$$

$$(3) \quad \alpha(xy) \equiv \alpha(x)\alpha(y) + x_1\beta(y) - x_1x_2\binom{\beta(y)}{2}p^{m-1} \pmod{p^m}.$$

Покладемо $x = y = -b$, так що $x_1 = y_1 = 0$ і $x_2 = y_2 = -1$. Тоді $2\alpha(-b) \equiv 0 \pmod{p}$ за твердженням (2) випливає, що $\alpha(-b) \equiv 0 \pmod{p}$. З іншого боку, $b = (-b)^2$ і

$$\alpha((-b)^2) \equiv \alpha(-b)^2 \pmod{p^m}$$

за твердженням (3). Тому

$$\alpha(b) = \alpha((-b)^2) \equiv 0 \pmod{p}.$$

Оскільки $\alpha(b) \equiv 1 \pmod{p^m}$ за твердженням (1), маємо протиріччя. Таким чином, випадок $b = i$ неможливий, як і вимагалось. $\square$

Наступне твердження є прямим наслідком теореми 6.8.

Наслідок 6.9 (Corollary 1, [80]). *Не існує майже-кілля з одиницею, адитивна група якого ізоморфна групі $G(p^m, p^n)$ з $p > 2$ і $2 \leq m \leq n$.*

6.3. Майже-кільця з одиницею та групи Шмідта

Нехай G — непримарна група Міллера–Морено, тобто $G = P \rtimes \langle b \rangle$ з нормальною елементарною абелевою підгрупою P порядку p^r , на якій елемент b порядку q^s індукує незвідний автоморфізм простого порядку q , де p, q — прості, q ділить $p^r - 1$ та r, s — натуральні числа.

Лема 6.10. *В групі G не існує елемента, порядок якого співпадає з її експонентою.*

Доведення. Припустимо, що існує елемент $g \in G$, порядок якого співпадає з її експонентою pq^s . Тоді $G = P \langle g \rangle$ і тому перетин $P \cap \langle g \rangle$ є нормальною підгрупою порядку p в G . В силу того, що P — мінімальна нормальна підгрупа в G , маємо $P = P \cap \langle g \rangle$ і, таким чином, $G = \langle g \rangle$. Отримане протиріччя завершує доведення леми. $\square$

Нагадаємо, що *цілком характеристичною підгрупою* називається підгрупа групи G , яка інваріантна відносно всіх ендоморфізмів групи G .

Наступна лема є безпосереднім наслідком [29, Lemma 1].

Лема 6.11. *Нехай R — майже-кільце з одиницею i , адитивна група R^+ якого ізоморфна групі G . Тоді для кожного елемента $y \in G$ існує такий ендоморфізм φ групи G , що $i^\varphi = y$.*

Маємо наступне твердження.

Теорема 6.12. *Не існує майже-кільця з одиницею, адитивна група яких ізоморфна групі Шмідта.*

Доведення. За [80, Lemma 2] не існує майже-кільця з одиницею, адитивна група яких ізоморфна непримарній групі Міллера–Морено.

Нехай тепер G ізоморфна групі Шмідта, яка не є групою Міллера–Морено. Припустимо, що група G є адитивною групою деякого майже-кільця з одиницею. Тоді за лемою 6.11 для кожного елемента $y \in G$ існує

такий ендоморфізм φ групи G , що $i^\varphi = y$. Оскільки $\Phi(G)$ є цілком характеристичною підгрупою, то $\bar{i}^\varphi = \bar{y}$ для всіх $\bar{y} \in G/\Phi(G)$. Враховуючи, що $G/\Phi(G)$ — група Міллера–Морено, маємо протиріччя в силу лем 2.2 та 6.10. $\square$

6.4. Прямі добутки метациклічних p -груп Міллера–Морено та циклічних p -груп як адитивні групи локальних майже-кілець

6.4.1. Групи $F(p^m, p^n, p^k)$

Нагадаємо, що скінченна група називається мінімальною неабелевою групою або групою Міллера–Морено, якщо вона неабелева, а всі її власні підгрупи є абелевими. Ці групи вперше вивчалися Міллером та Мореном в 1903 році [67]. Будова таких груп добре відома і повністю описується в [118].

Наступне твердження легко перевіряється.

Лема 6.13. *Експонента групи $F(p^m, p^n, p^k)$ дорівнює p^m для $m \geq n$ та $m \geq k$, p^n для $n > m$ та $n > k$, та p^k для $k > m$ та $k > n$. Якщо x — елемент максимального порядку в $F(p^m, p^n, p^k)$, то існують такі твірні a, b, c цієї групи, що або $a = x$, $b = x$, або $c = x$, і виконуються співвідношення $a^{p^m} = b^{p^n} = c^{p^k} = 1$, $b^{-1}ab = a^{1+p^{m-1}}$, $ca = ac$ та $cb = bc$, де $m \geq 2$, $n \geq 1$ та $k \geq 1$.*

Лема 6.14. *Нехай група G ізоморфна $F(p^m, p^n, p^k)$. Тоді для будь-яких натуральних чисел r, s, t , u виконуються рівності*

$$cu + bs + ar = ar(1 + sp^{m-1}) + bs + cu$$

i

$$(ar + bs + cu)t = ar(t + s \binom{t}{2} p^{m-1}) + bst + cut.$$

Доведення. Нехай $q = 1 + p^{m-1}$. Оскільки $-b + a + b = a(1 - p^{m-1})$, $a + c = c + a$ та $b + c = c + b$, тоді $b + a = aq + b$, отже, $bs + ar = arq^s + bs$ для довільних цілих чисел $r \geq 0$ та $s \geq 0$. Беручи до уваги, що

$$q^s = (1 + p^{m-1})^s \equiv 1 + sp^{m-1} \pmod{p^{m-1}}$$

за біноміальною формулою, маємо

$$cu + bs + ar = ar(1 + sp^{m-1}) + bs + cu.$$

Далі,

$$(ar + bs + cu)t = ar(1 + q^s + \dots + q^{s(t-1)}) + bst + cut$$

за індукцією t . Отже,

$$\begin{aligned} 1 + q^s + \dots + q^{s(t-1)} &= (1 + sp^{m-1}) + \dots + (1 + s(t-1)p^{m-1}) \equiv \\ &\equiv t + s \binom{t}{2} p^{m-1} \pmod{p^m}, \end{aligned}$$

тому

$$(ar + bs + cu)t = ar(t + s \binom{t}{2} p^{m-1}) + bst + cut.$$

□

6.4.2. Майже-кільця з одиницею на групах $F(p^m, p^n, p^k)$

Зрозуміло, що групи $F(p^m, p^n, p^k)$ є прямим добутком метациклічних груп Міллера–Морено порядку p^{mn} та циклічних груп порядку p^k . Очевидно, що прямий добуток майже-кілець з одиницею є майже-кілцем з одиницею. Отже, далі адитивна група R ізоморфна групі $F(p^m, p^n, p^k)$.

Нехай адитивна група майже-кільця R з одиницею ізоморфна групі $F(p^m, p^n, p^k)$. Отже, $R^+ = \langle a \rangle + \langle b \rangle + \langle c \rangle$ з елементами a, b, c , один з яких співпадає з одиничним елементом R , та справедливі співвідношення $ap^m = bp^n = cp^k = 0$, $a + b = b + a(1 + p^{m-1})$, $a + c = c + a$ та $b + c = c + b$, де $m \geq 2$, $n \geq 1$ і $k \geq 1$. Більш того, 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 $0 \leq x_3 < p^k$.

Розглядається випадок, коли a співпадає з одиничним елементом R , тобто $xa = ax = x$ для кожного $x \in R$, та $p > 2$. Отже, R^+ має експоненту p^m та $m \geq n$, а також $m \geq k$. Крім того, для кожного $x \in R$ існують такі цілі числа $\alpha(x)$, $\beta(x)$, $\gamma(x)$, $\phi(x)$, $\psi(x)$ і $\xi(x)$, що

$$xb = a\alpha(x) + b\beta(x) + c\gamma(x)$$

та

$$xc = a\phi(x) + b\psi(x) + c\xi(x),$$

відповідно. Зрозуміло, що за модулями p^m , p^n , p^k , p^m , p^n та p^k відповідно ці цілі числа однозначно визначаються x , і тому визначені деякі відображення $\alpha: R \rightarrow Z_{p^m}$, $\beta: R \rightarrow Z_{p^n}$, $\gamma: R \rightarrow Z_{p^k}$, $\phi: R \rightarrow Z_{p^m}$, $\psi: R \rightarrow Z_{p^n}$ та $\xi: R \rightarrow Z_{p^k}$.

Лема 6.15. *Нехай $x = ax_1 + bx_2 + cx_3$ та $y = ay_1 + by_2 + cy_3$ — елементи з R . Якщо a співпадає з одиничним елементом R , то*

$$\begin{aligned} xy = & a(x_1y_1 + \alpha(x)y_2 + \phi(x)y_3 + (x_1x_2 \binom{y_1}{2} + \\ & + \alpha(x)x_1y_1y_2 + \alpha(x)\beta(x) \binom{y_2}{2} + x_2\phi(x)y_1y_3 + \\ & + \beta(x)\phi(x)y_2y_3 + \phi(x)\psi(x) \binom{y_3}{2})p^{m-1}) + b(x_2y_1 + \beta(x)y_2 + \\ & + \psi(x)y_3) + c(x_3y_1 + \gamma(x)y_2 + \xi(x)y_3). \end{aligned} \quad (6.2)$$

Більш того, для відображень $\alpha: R \rightarrow Z_{p^m}$, $\beta: R \rightarrow Z_{p^n}$, $\gamma: R \rightarrow Z_{p^k}$, $\phi: R \rightarrow Z_{p^m}$, $\psi: R \rightarrow Z_{p^n}$ та $\xi: R \rightarrow Z_{p^k}$ мають місце такі твердження:

(0) $\alpha(0) = \beta(0) = \gamma(0) = \phi(0) = \psi(0) = \xi(0) = 0$ тоді і тільки тоді, коли майже-кільце R є нуль-симетричним;

(1) $\alpha(a) = 0$, $\beta(a) = 1$, $\gamma(a) = 0$, $\phi(c) = 0$, $\psi(c) = 0$ і $\xi(c) = 1$;

(2) $\alpha(xy) = x\alpha(y) + \alpha(x)\beta(y) + \phi(x)\gamma(y) + (x_1x_2\binom{\alpha(y)}{2} + \alpha(x)x_1\alpha(y)\beta(y) +$
 $+ \alpha(x)\beta(x)\binom{\beta(y)}{2} + x_2\phi(x)\alpha(y)\gamma(y) +$
 $+ \beta(x)\phi(x)\beta(y)\gamma(y) + \phi(x)\psi(x)\binom{\gamma(y)}{2})p^{m-1}$;

(3) $\beta(xy) = x_2\alpha(y) + \beta(x)\beta(y) + \psi(x)\gamma(y)$;

(4) $\gamma(xy) = x_3\alpha(y) + \gamma(x)\beta(y) + \xi(x)\gamma(y)$;

(5) $\phi(xy) = x_1\phi(y) + \alpha(x)\psi(y) + \phi(x)\xi(y) + (x_1x_2\binom{\phi(y)}{2} + \alpha(x)x_1\phi(y)\psi(y) +$
 $+ \alpha(x)\beta(x)\binom{\psi(y)}{2} + x_2\phi(x)\phi(y)\xi(y) +$
 $+ \beta(x)\phi(x)\psi(y)\xi(y) + \phi(x)\psi(x)\binom{\xi(y)}{2})p^{m-1}$;

(6) $\psi(xy) = x_2\phi(y) + \beta(x)\psi(y) + \psi(x)\xi(y)$;

(7) $\xi(xy) = x_3\phi(y) + \gamma(x)\psi(y) + \xi(x)\xi(y)$.

Доведення. Згідно з лівим дистрибутивним законом, маємо

$$xy = (xa)y_1 + (xb)y_2 + (xc)y_3 = (ax_1 + bx_2 + cx_3)y_1 +$$

$$+ ((a\alpha(x) + b\beta(x) + c\gamma(x))y_2 + (a\phi(x) + b\psi(x) + c\xi(x))y_3.$$

Крім того, з леми 6.14 випливає, що

$$(ax_1 + bx_2 + cx_3)y_1 = ax_1(y_1 + x_2 \binom{y_1}{2} p^{m-1}) + bx_2y_1 + cx_3y_1,$$

$$\begin{aligned} & ((a\alpha(x) + b\beta(x) + c\gamma(x))y_2 = \\ & = a\alpha(x)(y_2 + \beta(x) \binom{y_2}{2} p^{m-1}) + b\beta(x)y_2 + c\gamma(x)y_2 \end{aligned}$$

і

$$\begin{aligned} & (a\phi(x) + b\psi(x) + c\xi(x))y_3 = \\ & = a\phi(x)(y_3 + \psi(x) \binom{y_3}{2} p^{m-1}) + b\psi(x)y_3 + c\xi(x)y_3. \end{aligned}$$

Отже,

$$\begin{aligned} xy &= ax_1(y_1 + x_2 \binom{y_1}{2} p^{m-1}) + a\alpha(x)(y_2 + \\ & + \beta(x) \binom{y_2}{2} p^{m-1})(1 + x_2y_1p^{m-1}) + b(x_2y_1 + \\ & + \beta(x)y_2) + a\phi(x)(y_3 + \psi(x) \binom{y_3}{2} p^{m-1}) + b\psi(x)y_3 + \\ & + c(x_2y_1 + \gamma(x)y_2 + \xi(x)y_3) = a(x_1y_1 + x_1x_2 \binom{y_1}{2} p^{m-1}) + \\ & + a\alpha(x)(y_2 + x_1y_1y_2p^{m-1} + \beta(x) \binom{y_2}{2} p^{m-1}) + a\phi(x)(y_3 + \\ & + \psi(x) \binom{y_3}{2} p^{m-1})(1 + (x_2y_1 + \beta(x)y_2)p^{m-1}) + b(x_2y_1 + \\ & + \beta(x)y_2) + b\psi(x)y_3 + c(x_3y_1 + \gamma(x)y_2 + \xi(x)y_3) = a(x_1y_1 + \\ & + x_1x_2 \binom{y_1}{2} p^{m-1}) + a\alpha(x)(y_2 + x_1y_1y_2p^{m-1} + \\ & + \beta(x) \binom{y_2}{2} p^{m-1}) + a(\phi(x)y_3 + \phi(x)\psi(x) \binom{y_3}{2} p^{m-1})(1 + \\ & + x_2y_1p^{m-1} + \beta(x)y_2p^{m-1}) + b(x_2y_1 + \beta(x)y_2) + b\psi(x)y_3 + c(x_3y_1 + \\ & + \gamma(x)y_2 + \xi(x)y_3) = a(x_1y_1 + x_1x_2 \binom{y_1}{2} p^{m-1}) + a\alpha(x)(y_2 + \end{aligned}$$

$$\begin{aligned}
& +x_1y_1y_2p^{m-1} + \beta(x)\binom{y_2}{2}p^{m-1}) + a(\phi(x)y_3 + x_2\phi(x)y_1y_3p^{m-1} + \\
& +\beta(x)\phi(x)y_2y_3p^{m-1} + \phi(x)\psi(x)\binom{y_3}{2}p^{m-1}) + b(x_2y_1 + \\
& +\beta(x)y_2) + b\psi(x)y_3 + c(x_3y_1 + \gamma(x)y_2 + \xi(x)y_3).
\end{aligned}$$

Наприкінці,

$$\begin{aligned}
& a(x_1y_1 + \alpha(x)y_2 + \phi(x)y_3 + (x_1x_2\binom{y_1}{2} + \alpha(x)x_1y_1y_2 + \\
& +\alpha(x)\beta(x)\binom{y_2}{2} + x_2\phi(x)y_1y_3 + \beta(x)\phi(x)y_2y_3 + \\
& \phi(x)\psi(x)\binom{y_3}{2})p^{m-1}) + b(x_2y_1 + \beta(x)y_2 + \psi(x)y_3) + \\
& +c(x_3y_1 + \gamma(x)y_2 + \xi(x)y_3).
\end{aligned}$$

Оскільки $0 \cdot a = a \cdot 0 = 0$, то R є нуль-симетричним майже-кільцем тоді і тільки тоді, коли

$$0 = 0 \cdot b = a\alpha(0) + b\beta(0) + c\gamma(0)$$

і

$$0 = 0 \cdot c = a\phi(0) + b\psi(0) + c\xi(0).$$

Еквівалентно маємо $\alpha(0) \equiv 0 \pmod{p^m}$, $\beta(0) \equiv 0 \pmod{p^n}$, $\gamma(0) \equiv 0 \pmod{p^k}$, $\phi(0) \equiv 0 \pmod{p^m}$, $\psi(0) \equiv 0 \pmod{p^n}$, $\xi(0) \equiv 0 \pmod{p^k}$.

Асоціативність множення в R означає, що для всіх $x, y \in R$,

$$(xy)b = (x(yb)) \tag{6.3}$$

і

$$(xy)c = x(yc). \tag{6.4}$$

Згідно з $xb = a\alpha(x) + b\beta(x) + c\gamma(x)$, отримуємо

$$(xy)b = a\alpha(xy) + b\beta(xy) + c\gamma(xy) \tag{6.5}$$

і $yb = a\alpha(y) + b\beta(y) + c\gamma(y)$. Підставляючи останнє рівняння в праву частину рівності (6.3), також маємо

$$\begin{aligned} x(yb) = & a(x_1\alpha(y) + \alpha(x)\beta(y) + \phi(x)\gamma(y) + (x_1x_2\binom{\alpha(y)}{2}) + \\ & + \alpha(x)x_1\alpha(y)\beta(y) + \alpha(x)\beta(x)\binom{\beta(y)}{2} + x_2\phi(x)\alpha(y)\gamma(y) + \\ & + \beta(x)\phi(x)\beta(y)\gamma(y) + \phi(x)\psi(x)\binom{\gamma(y)}{2})p^{m-1} + b(x_2\alpha(y) + \\ & + \beta(x)\beta(y) + \psi(x)\gamma(y)) + c(x_3\alpha(y) + \gamma(x)\beta(y) + \xi(x)\gamma(y)). \end{aligned} \quad (6.6)$$

Оскільки рівність (6.3) передбачає конгруентність відповідних коефіцієнтів у формулах (6.5) та (6.6), отримуємо твердження (2)–(4).

$$\begin{aligned} \alpha(xy) = & x\alpha(y) + \alpha(x)\beta(y) + \phi(x)\gamma(y) + (x_1x_2\binom{\alpha(y)}{2}) + \\ & + \alpha(x)x_1\alpha(y)\beta(y) + \alpha(x)\beta(x)\binom{\beta(y)}{2} + x_2\phi(x)\alpha(y)\gamma(y) + \\ & + \beta(x)\phi(x)\beta(y)\gamma(y) + \phi(x)\psi(x)\binom{\gamma(y)}{2})p^{m-1}; \\ \beta(xy) = & x_2\alpha(y) + \beta(x)\beta(y) + \psi(x)\gamma(y); \\ \gamma(xy) = & x_3\alpha(y) + \gamma(x)\beta(y) + \xi(x)\gamma(y). \end{aligned}$$

Далі, згідно з $xc = a\phi(x) + b\psi(x) + c\xi(x)$ замість y у рівності (6.4), отримуємо

$$(xy)c = a\phi(xy) + b\psi(xy) + c\xi(xy) \quad (6.7)$$

і $yc = a\phi(y) + b\psi(y) + c\xi(y)$. Підставляючи останнє рівняння в праву частину рівності (6.4), також маємо

$$\begin{aligned} x(yc) = & a(x_1\phi(y) + \alpha(x)\psi(y) + \phi(x)\xi(y) + (x_1x_2\binom{\phi(y)}{2}) + \\ & + \alpha(x)x_1\phi(y)\psi(y) + \alpha(x)\beta(x)\binom{\psi(y)}{2} + x_2\phi(x)\phi(y)\xi(y) + \end{aligned} \quad (6.8)$$

$$\begin{aligned}
& +\beta(x)\phi(x)\psi(y)\xi(y) + \phi(x)\psi(x)\binom{\xi(y)}{2}p^{m-1})+ \\
& +b(x_2\phi(y) + \beta(x)\psi(y) + \psi(x)\xi(y)) + c(x_3\phi(y) + \gamma(x)\psi(y) + \xi(x)\xi(y)).
\end{aligned}$$

Нарешті, порівнюючи коефіцієнти при a , b та c у формулах (6.7) та (6.8), ми отримуємо твердження (5)–(7) леми.

$$\begin{aligned}
\phi(xy) &= x_1\phi(y) + \alpha(x)\psi(y) + \phi(x)\xi(y) + (x_1x_2\binom{\phi(y)}{2} + \\
& +\alpha(x)x_1\phi(y)\psi(y) + \alpha(x)\beta(x)\binom{\psi(y)}{2} + x_2\phi(x)\phi(y)\xi(y) + \\
& +\beta(x)\phi(x)\psi(y)\xi(y) + \phi(x)\psi(x)\binom{\xi(y)}{2})p^{m-1}; \\
\psi(xy) &= x_2\phi(y) + \beta(x)\psi(y) + \psi(x)\xi(y); \\
\xi(xy) &= x_3\phi(y) + \gamma(x)\psi(y) + \xi(x)\xi(y).
\end{aligned}$$

□

6.4.3. Локальні майже-кільця, адитивні групи яких ізоморфні $F(p^m, p^n, p^k)$

Нехай R — локальне майже-кільце, адитивна група якого R^+ ізоморфна $F(p^m, p^n, p^k)$. Тоді $R^+ = \langle a \rangle + \langle b \rangle + \langle c \rangle$ з елементами a , b та c , де a співпадає з одиничним елементом R та виконуються співвідношення $a^{p^m} = b^{p^n} = c^{p^k} = 1$, $b^{-1}ab = a^{1+p^{m-1}}$, $ca = ac$ та $cb = bc$, де $m \geq 2$, $n \geq 1$ та $k \geq 1$. Moreover, each element $x \in R$ is uniquely written in the form $x = ax_1 + bx_2 + cx_3$ with coefficients $0 \leq x_1 < p^m$, $0 \leq x_2 < p^n$ and $0 \leq x_3 < p^k$.

Нехай у цьому розділі R буде локальним майже-кільцем з $|R : L| = p$.

Розглянемо, що a співпадає з одиничним елементом R , так що $xa = ax = x$ для кожного $x \in R$, $m \geq n$ та $m \geq k$. Крім того, для кожного

$x \in R$ існують такі цілі числа $\alpha(x)$, $\beta(x)$, $\gamma(x)$, $\phi(x)$, $\psi(x)$ та $\xi(x)$, що

$$xb = a\alpha(x) + b\beta(x) + c\gamma(x)$$

і

$$xc = a\phi(x) + b\psi(x) + c\xi(x),$$

відповідно. Зрозуміло, що за модулями p^m , p^n , p^k , p^m , p^n та p^k , відповідно, ці цілі числа однозначно визначаються x , і тому визначені деякі відображення $\alpha: R \rightarrow Z_{p^m}$, $\beta: R \rightarrow Z_{p^n}$, $\gamma: R \rightarrow Z_{p^k}$, $\phi: R \rightarrow Z_{p^m}$, $\psi: R \rightarrow Z_{p^n}$ та $\xi: R \rightarrow Z_{p^k}$.

Якщо $|R : L| = p$, то $L = \langle ap \rangle + \langle b \rangle + \langle c \rangle$. Оскільки $R^* = R \setminus L$, то випливає, що

$$R^* = ax_1 + bx_2 + cx_3 | x_1 \not\equiv 0 \pmod{p^m}$$

і $x = ax_1 + bx_2 + cx_3$ є оборотним тоді і тільки тоді, коли $x_1 \not\equiv 0 \pmod{p^m}$. Оскільки $L \in (R, R)$ -підгрупою в R^+ згідно з твердженням 1) леми 3.4, то $xb \in L$ та $xc \in L$, отже $a\alpha(x) \in L$ та $a\phi(x) \in L$ для кожного $x \in R$. Таким чином, $\alpha(x) \equiv 0 \pmod{p}$ та $\phi(x) \equiv 0 \pmod{p}$. Отже, для локальних майже-кілець R маємо таке ж множення, як і для майже-кілець з одиницею, тобто множення (6.2).

Лема 6.16. *Нехай $x = ax_1 + bx_2 + cx_3$ та $y = ay_1 + by_2 + cy_3$ — елементи R та $|R : L| = p$. Якщо a співпадає з одиничним елементом R , то $m \geq n$, $m \geq k$ та множення (6.2) виконується для відображень з леми 6.15.*

Далі, наведемо приклади локальних майже-кілець.

Лема 6.17. *Нехай R — локальне майже-кілець, адитивна група якого R^+ ізоморфна $F(p^m, p^n, p^k)$, $|R : L| = p$, $m \geq n$ та $m \geq k$. Якщо $x = ax_1 + bx_2 + cx_3$, $y = ay_1 + by_2 + cy_3$, то відображення $\alpha: R \rightarrow Z_{p^m}$, $\beta: R \rightarrow Z_{p^n}$, $\gamma: R \rightarrow Z_{p^k}$, $\phi: R \rightarrow Z_{p^m}$, $\psi: R \rightarrow Z_{p^n}$ та $\xi: R \rightarrow Z_{p^k}$*

можуть бути наступними: $\phi(x) \equiv 0 \pmod{p^m}$, $\psi(x) \equiv 0 \pmod{p^m}$, $\alpha(x) \equiv 0 \pmod{p^m}$, $\gamma(x) \equiv 0 \pmod{p^k}$, $\xi(x) \equiv 0 \pmod{p^k}$,

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

Доведення. Легко перевірити, що функції з твердження леми задовольняють умову леми 6.16. $\square$

Як наслідок леми 6.17 маємо наступний результат.

Теорема 6.18. Для кожного непарного простого числа p , $m \geq n$ та $m \geq k$ існує локальне майже-кільце R , адитивна група якого R^+ ізоморфна $F(p^m, p^n, p^k)$.

Наведемо приклад локального майже-кільця на групі $F(25, 5, 5)$.

Приклад 6.19. Нехай $G \cong (C_{25} \rtimes C_5) \times C_5$ [625,13]. Якщо $x = ax_1 + bx_2 + cx_3$ і $y = ay_1 + by_2 + cy_3 \in G$, та $(G, +, \cdot)$ є локальним майже-кільцем, тоді як вище “ $\cdot$ ” може бути наступним:

$$x \cdot y = a(x_1y_1 + \beta(x)x_1x_2 \binom{y_1}{2} * 5) + b(x_2y_1 + \beta(x)y_2) + c(x_3y_1 + y_3),$$

де

$$\beta(x) = \begin{cases} 1, & \text{якщо } x_1 \not\equiv 0 \pmod{5}; \\ 0, & \text{якщо } x_1 \equiv 0 \pmod{5}. \end{cases}$$

Наступна комп’ютерна програма перевіряє, що майже-кільце отримана в прикладі 6.19 є дійсно локальним майже-кільцем.

В середовищі системи GAP завантажуюємо пакет LocalNR.

`LoadPackage("LocalNR");`

G — група з `IdGroup` [625, 13].

`G := SmallGroup(625, 13);`

`gen` — список, що містить мінімальну систему твірних.

`gen := MinimalGeneratingSet(G);`

```

# Повертаємо список з порядками твірних зі списку gen.
List(gen, Order);

# a — перший елемент зі списку gen.
a := gen[1];

# b — другий елемент зі списку gen.
b := gen[2];

# c — третій елемент зі списку gen.
c := gen[3];

# mulGR — функція майже-кільцевого добутку.
mulGR := function(x, y)
  local x1, x2, x3, y1, y2, y3;
  for x1 in [0..24] do
    for x2 in [0..4] do
      for x3 in [0..4] do
        for y1 in [0..25] do
          for y2 in [0..4] do
            for y3 in [0..4] do
              if x = a^x1 * b^x2 * c^x3 and y = a^y1 * b^y2 * c^y3 then return
                a^(x1 * y1 + x1 * x2 * Binomial(y1, 2) * 5) * b^(x2 * y1 + y2) * c^(x3 *
y1 + y3); fi;
            od; od; od; od; od; od; end;
          end;
        end;
      end;
    end;
  end;

# n — майже-кільце на групі G та з множенням mulGR (без перевірки).
n := ExplicitMultiplicationNearRingNC(G, mulGR);

# M — таблиця множення майже-кільця n.
M := MultiplicationTable(n);

# mulNR — майже-кільцеве множення, що отримано за допомогою
таблиці M.

```

$mul_N R :=$
 $NearRingMultiplicationByOperationTable(G, M, AsSortedList(G));$
 $\#$ n — майже-кілець на групі G та з множенням $mul_N R$ (з перевіркою).
 $n := ExplicitMultiplicationNearRing(G, mul_N R);$
 $\#$ Перевірка, чи є майже-кілець n локальним.
 $IsLocalNearRing(n);$

З [19], [111] і [109] маємо наступну кількість всіх неізоморфних нуль-симетричних локальних майже-кілець на групі G з прикладу 6.19.

$IdGroup(R^+)$	$StructureDescription(R^+)$	$n(R^+)$
[625, 13]	$(C_{25} \rtimes C_5) \times C_5$	630

6.5. Прямі добутки неметациклічних p -груп Міллера–Морено та циклічних p -груп як адитивні групи локальних майже-кілець

6.5.1. Попередні результати

Лема 6.20. *Неметациклічні p -групи Міллера–Морено ізоморфні групі $G = (\langle a \rangle \times \langle c \rangle) \rtimes \langle b \rangle$ порядку p^{m+n+1} (p — просте число) з $|a| = p^m$, $|b| = p^n$, $|c| = p$, $b^{-1}ab = ac$, $b^{-1}cb = c$, де $m \geq n \geq 1$ та $m + n > 2$ при $p = 2$.*

Розглянемо прямий добуток неметациклічної p -групи Міллера–Морено та циклічної p -групи. Як безпосередній наслідок леми 6.20, маємо наступну лему.

Лема 6.21. Нехай G прямий добуток неметациклічної p -групи Міллера–Морено та циклічної p -групи. Тоді G є групою наступного типу: група $G = ((\langle a \rangle \times \langle c \rangle) \rtimes \langle b \rangle) \times \langle d \rangle$ порядку $p^{m+n+k+1}$ з $a^{p^m} = b^{p^n} = c^p = d^{p^k} = 1$, $b^{-1}ab = ac$, $b^{-1}cb = c$, $d^{-1}ad = a$, $d^{-1}bd = b$, $d^{-1}cd = c$, де $m \geq n \geq 1$ та $m + n > 2$ при $p = 2$.

Позначимо через $F(p^m, p^n, p, p^k)$ адитивно записану групу з леми 6.21 з такими твірними a, b, c та d порядків p^m, p^n, p та p^k , відповідно, що $-b + a + b = a + c$, $-b + c + b = c$, $-d + a + d = a$, $-d + b + d = b$, $-d + c + d = c$, де $m \geq n \geq 1$ та $m + n > 2$ при $p = 2$.

Лема 6.22. Для довільних цілих чисел r та s в групі $F(p^m, p^n, p, p^k)$ виконуються співвідношення:

$$-ar - bs + ar + bs = crs, \quad bs + ar = -crs + ar + bs.$$

Доведення. Оскільки $-b + a + b = a + c$, то $-bs + a + bs = a + cs$. Тоді $-bs + ar + bs = (a + cs)r = ar + crs$. Звідси $bs + ar = -crs + ar + bs$. $\square$

Лема 6.23. Для будь-яких натуральних чисел r, t, s в групі $F(p^m, p^n, p, p^k)$ справедливе співвідношення:

$$(ar + bs)t = art + bst - crs \binom{t}{2}. \quad (6.9)$$

Доведення. Доведення проведемо індукцією по t . При $t = 1$ рівність вірна. Нехай при t виконується рівність, тобто

$$(ar + bs)t = art + bst - crs \binom{t}{2}.$$

Покажемо справедливість рівності при $t + 1$:

$$\begin{aligned} (ar + bs)(t + 1) &= art + bst + ar + bs - crs \binom{t}{2} = \\ &= ar(t + 1) + bs(t + 1) - crst - crs \binom{t}{2} = \end{aligned}$$

$$\begin{aligned}
&= ar(t+1) + bs(t+1) - crs\left(t + \binom{t}{2}\right) = \\
&= ar(t+1) + bs(t+1) - crs\binom{t+1}{2}.
\end{aligned}$$

Отже, рівність (6.9) справедлива при будь-якому t . $\square$

Лема 6.24. Якщо $m \geq n \geq 1$, $m \geq k$ та $m > 1$ при $p = 2$, то експонента групи $F(p^m, p^n, p, p^k)$ дорівнює p^m .

Доведення. Дійсно, для кожного $x \in F(p^m, p^n, p, p^k)$ існують такі цілі числа $\alpha, \beta, \gamma, \phi$, що $x = a^\alpha b^\beta c^\gamma d^\phi$.

$$\begin{aligned}
x^{p^m} &= (a^\alpha b^\beta c^\gamma d^\phi)^{p^m} = (a^\alpha b^\beta)^{p^m} c^{\gamma p^m} d^{\phi p^m} = \\
&= a^{\alpha p^m} b^{\beta p^m} c^{-\alpha\beta \binom{p^m}{2}} = a^{\alpha p^m} b^{\beta p^m} c^{-\alpha\beta \frac{p^m(p^m-1)}{2}} = 1.
\end{aligned}$$

Оскільки $|a| = p^m$ та $m \geq n \geq 1$ з $m > 1$ при $p = 2$, то p^m експонента групи $F(p^m, p^n, p, p^k)$. $\square$

6.5.2. Майже-кільця з одиницею на групах $F(p^m, p^n, p, p^k)$

Нехай адитивною групою майже-кільця R з одиницею є прямий добуток деяких неметациклічних p -груп Міллера–Морено та деяких циклічних p -груп. А отже, ізоморфна групі $F(p^m, p^n, p, p^k)$.

Розглянемо групи $F(p^m, p^n, p, p^k)$ з $m \geq n \geq 1$, $m \geq k$ та $n > 1$, при $p = 2$.

Лема 6.25. Нехай R — майже-кільце з одиницею i , адитивна група R^+ якого ізоморфна групі $F(p^m, p^n, p, p^k)$ з $m \geq n \geq 1$, $m \geq k$ та $n > 1$ при $p = 2$. Тоді $R^+ = \langle a \rangle + \langle b \rangle + \langle c \rangle + \langle d \rangle$ з елементами a, b, c та d , що задовольняють співвідношенням $ap^m = bp^n = cp = dp^k = 0$,

$-b+a+b = a+c$, $-b+c+b = c$, $-d+a+d = a$, $-d+b+d = b$, $-d+c+d = c$.
 Причому $a = i$ та кожний елемент $x \in R$ однозначно записується у вигляді $x = ax_1 + bx_2 + cx_3 + dx_4$ з коефіцієнтами $0 \leq x_1 < p^m$, $0 \leq x_2 < p^n$, $0 \leq x_3 < p$ та $0 \leq x_4 < p^k$.

Доведення. Оскільки за лемою 2.2 одиниця i є елементом максимального порядку в групі R^+ , то твірний елемент a цієї групи можна вибрати так, щоб він співпадав з i . Решта впливає з означення групи $F(p^m, p^n, p, p^k)$. $\square$

Зокрема, з леми 6.25 випливає, що для кожного $x \in R$ виконується рівність $xa = ax = x$ та існують однозначно визначені відображення $\alpha_b : R \rightarrow \mathbb{Z}_{p^m}$, $\beta_b : R \rightarrow \mathbb{Z}_{p^n}$, $\gamma_b : R \rightarrow \mathbb{Z}_p$, $\phi_b : R \rightarrow \mathbb{Z}_{p^k}$ та $\alpha_d : R \rightarrow \mathbb{Z}_{p^m}$, $\beta_d : R \rightarrow \mathbb{Z}_{p^n}$, $\gamma_d : R \rightarrow \mathbb{Z}_p$, $\phi_d : R \rightarrow \mathbb{Z}_{p^k}$, для яких

$$xb = a\alpha_b(x) + b\beta_b(x) + c\gamma_b(x) + d\phi_b(x), \quad (6.10)$$

та

$$xd = a\alpha_d(x) + b\beta_d(x) + c\gamma_d(x) + d\phi_d(x). \quad (6.11)$$

Теорема 6.26. *Якщо $x = ax_1 + bx_2 + cx_3 + dx_4$ та $y = ay_1 + by_2 + cy_3 + dy_4$ — довільні елементи із R , то*

$$\begin{aligned} xy = & a(x_1y_1 + \alpha_b(x)y_2 + \alpha_d(x)y_4) + b(x_2y_1 + \beta_b(x)y_2 + \\ & + \beta_d(x)y_4) + c(x_3y_1 + \gamma_b(x)y_2 + x_1\beta_b(x)y_3 - \\ & - x_2\alpha_b(x)y_3 + \gamma_d(x)y_4 - x_1x_2\binom{y_1}{2} - \\ & - \alpha_b(x)\beta_b(x)\binom{y_2}{2} - \alpha_d(x)\beta_d(x)\binom{y_4}{2} - \\ & - x_2\alpha_b(x)y_1y_2 - x_2\alpha_d(x)y_1y_2 - \alpha_d(x)\beta_b(x)y_2^2) + \\ & + d(x_4y_1 + \phi_b(x)y_2 + \phi_d(x)y_4), \end{aligned} \quad (6.12)$$

причому для відображень $\alpha_b : R \rightarrow \mathbb{Z}_{p^m}$, $\beta_b : R \rightarrow \mathbb{Z}_{p^n}$, $\gamma_b : R \rightarrow \mathbb{Z}_p$, $\phi_b : R \rightarrow \mathbb{Z}_{p^k}$ та $\alpha_d : R \rightarrow \mathbb{Z}_{p^m}$, $\beta_d : R \rightarrow \mathbb{Z}_{p^n}$, $\gamma_d : R \rightarrow \mathbb{Z}_p$, $\phi_d : R \rightarrow \mathbb{Z}_{p^k}$ виконуються наступні твердження:

(0) $\alpha_b(0) \equiv 0 \pmod{p^m}$, $\beta_b(0) \equiv 0 \pmod{p^n}$, $\gamma_b(0) \equiv 0 \pmod{p}$, $\phi_b(0) \equiv 0 \pmod{p^k}$, $\alpha_d(0) \equiv 0 \pmod{p^m}$, $\beta_d(0) \equiv 0 \pmod{p^n}$, $\gamma_d(0) \equiv 0 \pmod{p}$, $\phi_d(0) \equiv 0 \pmod{p^k}$ тоді і тільки тоді, коли майже-кільце R є нуль-симетричним;

(1) $\alpha_b(xy) \equiv x_1\alpha_b(y) + \alpha_b(x)\beta_b(y) + \alpha_d(x)\phi_b(y) \pmod{p^m}$;

(2) $\beta_b(xy) \equiv x_2\alpha_b(y) + \beta_b(x)\beta_b(y) + \beta_d(x)\phi_b(y) \pmod{p^n}$;

(3) $\gamma_b(xy) \equiv x_3\alpha_b(y) + \gamma_b(x)\beta_b(y) + x_1\beta_b(x)\gamma_b(y) - x_2\alpha_b(x)\gamma_b(y) +$
 $+ \gamma_d(x)\phi_b(y) - x_1x_2\binom{\alpha_b(y)}{2} - \alpha_b(x)\beta_b(x)\binom{\beta_b(y)}{2} -$
 $- \alpha_d(x)\beta_d(x)\binom{\phi_b(y)}{2} - x_2\alpha_b(x)\alpha_b(y)\beta_b(y) - x_2\alpha_d(x)\alpha_b(y)\beta_b(y) -$
 $- \alpha_d(x)\beta_b(x)\beta_b(y)^2 \pmod{p}$;

(4) $\phi_b(xy) \equiv x_4\alpha_b(y) + \phi_b(x)\beta_b(y) + \phi_d(x)\phi_b(y) \pmod{p^k}$;

(5) $\alpha_d(xy) \equiv x_1\alpha_d(y) + \alpha_b(x)\beta_d(y) + \alpha_d(x)\phi_d(y) \pmod{p^m}$;

(6) $\beta_d(xy) \equiv x_2\alpha_d(y) + \beta_b(x)\beta_d(y) + \beta_d(x)\phi_d(y) \pmod{p^n}$;

(7) $\gamma_d(xy) \equiv x_3\alpha_d(y) + \gamma_b(x)\beta_d(y) + x_1\beta_b(x)\gamma_d(y) - x_2\alpha_b(x)\gamma_d(y) +$
 $+ \gamma_d(x)\phi_d(y) - x_1x_2\binom{\alpha_d(y)}{2} - \alpha_b(x)\beta_b(x)\binom{\beta_d(y)}{2} -$
 $- \alpha_d(x)\beta_d(x)\binom{\phi_d(y)}{2} - x_2\alpha_b(x)\alpha_d(y)\beta_d(y) - x_2\alpha_d(x)\alpha_d(y)\beta_d(y) -$
 $- \alpha_d(x)\beta_b(x)\beta_d(y)^2 \pmod{p}$;

(8) $\phi_d(xy) \equiv x_4\alpha_d(y) + \phi_b(x)\beta_d(y) + \phi_d(x)\phi_d(y) \pmod{p^k}$.

Доведення. Якщо майже-кільце R є нуль-симетричним, то

$$0 = 0 \cdot b = a\alpha_b(0) + b\beta_b(0) + c\gamma_b(0) + d\phi_b(0),$$

та

$$0 = 0 \cdot d = a\alpha_d(0) + b\beta_d(0) + c\gamma_d(0) + d\phi_d(0).$$

Звідси $\alpha_b(0) \equiv 0 \pmod{p^m}$, $\beta_b(0) \equiv 0 \pmod{p^n}$, $\gamma_b(0) \equiv 0 \pmod{p}$, $\phi_b(0) \equiv 0 \pmod{p^k}$, $\alpha_d(0) \equiv 0 \pmod{p^m}$, $\beta_d(0) \equiv 0 \pmod{p^n}$, $\gamma_d(0) \equiv 0 \pmod{p}$, $\phi_d(0) \equiv 0 \pmod{p^k}$. Навпаки, якщо мають місце вказані конгруентності, то

$$0 \cdot b = a \cdot 0 + b \cdot 0 + c \cdot 0 + d \cdot 0 = 0.$$

Також $0 \cdot a = a \cdot 0 = 0$, оскільки a — мультиплікативна одиниця в R . Крім того, з рівності $c = -a - b + a + b$ та лівої дистрибутивності множення випливає

$$0 \cdot c = -0 \cdot a - 0 \cdot b + 0 \cdot a + 0 \cdot b = 0,$$

звідки

$$\begin{aligned} 0 \cdot x &= 0 \cdot (ax_1 + bx_2 + cx_3d + x_4) = \\ &= (0 \cdot a)x_1 + (0 \cdot b)x_2 + (0 \cdot c)x_3 + (0 \cdot d)x_4 = 0. \end{aligned}$$

Отже, майже-кільце R є нуль-симетричним, що доводить твердження (0).

Далі, враховуючи рівність (6.10) та лему 6.22, маємо

$$\begin{aligned} xc &= -xa - xb + xa + xb = -cx_3 - bx_2 - ax_1 - c\gamma_b(x) - \\ &\quad - b\beta_b(x) - a\alpha_b(x) + ax_1 + bx_2 + cx_3 + a\alpha_b(x) + \\ &\quad + b\beta_b(x) + c\gamma_b(x) = -bx_2 - ax_1 - b\beta_b(x) - a\alpha_b(x) + \\ &\quad + ax_1 + bx_2 + a\alpha_b(x) + b\beta_b(x) = -bx_2 + cx_1\beta_b(x) - \\ &\quad - b\beta_b(x) - ax_1 - a(\alpha_b(x) - x_1) + bx_2 + a\alpha_b(x) + b\beta_b(x) = \\ &\quad = cx_1\beta_b(x) - b(x_2 + \beta_b(x)) - a\alpha_b(x) + bx_2 + a\alpha_b(x) + \end{aligned}$$

$$\begin{aligned}
& +b\beta_b(x) = cx_1\beta_b(x) - b(x_2 + \beta_b(x)) - a\alpha_b(x) - \\
& -cx_2\alpha_b(x) + a\alpha_b(x) + bx_2 + b\beta_b(x) = c(x_1\beta_b(x) - \\
& -x_2\alpha_b(x)) - b(x_2 + \beta_b(x)) + bx_2 + b\beta_b(x) = \\
& = c(x_1\beta_b(x) - x_2\alpha_b(x)).
\end{aligned}$$

Отже,

$$\begin{aligned}
xy = & (ax_1 + bx_2 + cx_3 + dx_4)y_1 + (a\alpha_b(x) + b\beta_b(x) + c\gamma_b(x) + \\
& + d\phi_b(x))y_2 + (cx_1\beta_b(x) - x_2\alpha_b(x))y_3 + (a\alpha_d(x) + \\
& + b\beta_d(x) + c\gamma_d(x) + d\phi_d(x))y_4.
\end{aligned}$$

За лемою 6.23, отримуємо

- $(ax_1 + bx_2)y_1 = ax_1y_1 + bx_2y_1 - cx_1x_2\binom{y_1}{2};$
- $(a\alpha_b(x) + b\beta_b(x))y_2 = a\alpha_b(x)y_2 + b\beta_b(x)y_2 - c\alpha_b(x)\beta_b(x)\binom{y_2}{2};$
- $(a\alpha_d(x) + b\beta_d(x))y_4 = a\alpha_d(x)y_4 + b\beta_d(x)y_4 - c\alpha_d(x)\beta_d(x)\binom{y_4}{2};$
- $bx_2y_1 + a\alpha_b(x)y_2 = a\alpha_b(x)y_2 + bx_2y_1 - cx_2\alpha_b(x)y_1y_2;$
- $b(x_2y_1 + \beta_b(x)y_2) + a\alpha_d(x)y_4 = a\alpha_d(x)y_2 + b(x_2y_1 + \beta_b(x)y_2) -$
 $-c\alpha_d(x)y_2(x_2y_1 + \beta_b(x)y_2) = a\alpha_d(x)y_2 + b(x_2y_1 + \beta_b(x)y_2) -$
 $-c(x_2\alpha_d(x)y_1y_2 + \alpha_d(x)\beta_b(x)y_2^2).$

Звідси, враховуючи ліву дистрибутивність, одержуємо

$$\begin{aligned}
xy = & a(x_1y_1 + \alpha_b(x)y_2 + \alpha_d(x)y_4) + b(x_2y_1 + \beta_b(x)y_2 + \beta_d(x)y_4) + \\
& + c(x_3y_1 + \gamma_b(x)y_2 + x_1\beta_b(x)y_3 - x_2\alpha_b(x)y_3 + \gamma_d(x)y_4 - \\
& - x_1x_2\binom{y_1}{2} - \alpha_b(x)\beta_b(x)\binom{y_2}{2} - \alpha_d(x)\beta_d(x)\binom{y_4}{2} - \\
& - x_2\alpha_b(x)y_1y_2 - x_2\alpha_d(x)y_1y_2 - \alpha_d(x)\beta_b(x)y_2^2) +
\end{aligned}$$

$$+d(x_4y_1 + \phi_b(x)y_2 + \phi_d(x)y_4).$$

Крім того, в силу закону асоціативності, для всіх $x, y \in R$ справедливі рівності

$$(xy)b = x(yb), \quad (6.13)$$

та

$$(xy)d = x(yd). \quad (6.14)$$

Згідно з рівності (6.10), маємо

$$(xy)b = a\alpha_b(xy) + b\beta_b(xy) + c\gamma_b(xy) + d\phi_b(xy), \quad (6.15)$$

та

$$yb = a\alpha_b(y) + b\beta_b(y) + c\gamma_b(y) + d\phi_b(y).$$

Підставивши останній вираз в праву частину рівності (6.13), виводимо

$$\begin{aligned} x(yb) &= a(x_1\alpha_b(y) + \alpha_b(x)\beta_b(y) + \alpha_d(x)\phi_b(y)) + b(x_2\alpha_b(y) + \\ &+ \beta_b(x)\beta_b(y) + \beta_d(x)\phi_b(y)) + c(x_3\alpha_b(y) + \gamma_b(x)\beta_b(y) + \\ &+ x_1\beta_b(x)\gamma_b(y) - x_2\alpha_b(x)\gamma_b(y) + \gamma_d(x)\phi_b(y) - x_1x_2\binom{\alpha_b(y)}{2} - \\ &- \alpha_b(x)\beta_b(x)\binom{\beta_b(y)}{2} - \alpha_d(x)\beta_d(x)\binom{\phi_b(y)}{2} - \\ &- x_2\alpha_b(x)\alpha_b(y)\beta_b(y) - x_2\alpha_d(x)\alpha_b(y)\beta_b(y) - \\ &- \alpha_d(x)\beta_b(x)\beta_b(y)^2) + d(x_4\alpha_b(y) + \\ &+ \phi_b(x)\beta_b(y) + \phi_d(x)\phi_b(y)). \end{aligned} \quad (6.16)$$

Оскільки з рівності (6.13) випливає конгруентність відповідних коефіцієнтів в формулах (6.15) та (6.16), то звідси отримуємо твердження (1)–(4). Згідно з рівності (6.11) маємо:

$$(xy)d = a\alpha_d(xy) + b\beta_d(xy) + c\gamma_d(xy) + d\phi_d(xy) \quad (6.17)$$

та

$$yd = a\alpha_d(y) + b\beta_d(y) + c\gamma_d(y) + d\phi_d(y).$$

Підставимо отриманий вираз в праву частину рівності (6.14), отримаємо

$$\begin{aligned} x(yd) = & a(x_1\alpha_d(y) + \alpha_b(x)\beta_d(y) + \alpha_d(x)\phi_d(y)) + b(x_2\alpha_b(y) + \\ & + \beta_b(x)\beta_d(y) + \beta_d(x)\phi_d(y)) + c(x_3\alpha_d(y) + \gamma_b(x)\beta_d(y) + \\ & + x_1\beta_b(x)\gamma_d(y) - x_2\alpha_b(x)\gamma_d(y) + \gamma_d(x)\phi_d(y) - x_1x_2\binom{\alpha_d(y)}{2} - \\ & - \alpha_b(x)\beta_b(x)\binom{\beta_d(y)}{2} - \alpha_d(x)\beta_d(x)\binom{\phi_d(y)}{2} - \\ & - x_2\alpha_b(x)\alpha_d(y)\beta_d(y) - x_2\alpha_d(x)\alpha_d(y)\beta_d(y) - \\ & - \alpha_d(x)\beta_b(x)\beta_d(y)^2) + d(x_4\alpha_d(y) + \\ & + \phi_b(x)\beta_d(y) + \phi_d(x)\phi_d(y)). \end{aligned} \quad (6.18)$$

Оскільки з рівності (6.14) випливає конгруентність відповідних коефіцієнтів в формулах (6.17) та (6.18), то звідси маємо твердження (5)–(8).

Лему доведено. $\square$

6.5.3. Локальні майже-кільця на групах $F(p^m, p^n, p, p^k)$

Нехай адитивною групою локального майже-кільця R є прямий добуток деякої неметациклічної p -групи Міллера–Морено та деякої циклічної p -групи. А отже, R^+ ізоморфна групі $F(p^m, p^n, p, p^k)$. Тоді $R^+ = \langle a \rangle + \langle b \rangle + \langle c \rangle + \langle d \rangle$ з елементами a, b, c та d , що задовольняють співвідношенням $ap^m = bp^n = cp = dp^k = 0$, $-b + a + b = a + c$, $-b + c + b = c$, $-d + a + d = a$, $-d + b + d = b$, $-d + c + d = c$. Причому a є одиничним

елементом в R та кожний елемент $x \in R$ однозначно записується у вигляді $x = ax_1 + bx_2 + cx_3 + dx_4$ з коефіцієнтами $0 \leq x_1 < p^m$, $0 \leq x_2 < p^n$, $0 \leq x_3 < p$ та $0 \leq x_4 < p^k$. Зокрема, для кожного $x \in R$ виконується рівність $xa = ax = x$ та існують однозначно визначені відображення $\alpha_b : R \rightarrow \mathbb{Z}_{p^m}$, $\beta_b : R \rightarrow \mathbb{Z}_{p^n}$, $\gamma_b : R \rightarrow \mathbb{Z}_p$, $\phi_b : R \rightarrow \mathbb{Z}_{p^k}$ та $\alpha_d : R \rightarrow \mathbb{Z}_{p^m}$, $\beta_d : R \rightarrow \mathbb{Z}_{p^n}$, $\gamma_d : R \rightarrow \mathbb{Z}_p$, $\phi_d : R \rightarrow \mathbb{Z}_{p^k}$, для яких виконуються рівності (6.10) та (6.11).

Нехай далі множина L всіх необоротних елементів майже-кільця R є підгрупою індексу p в R^+ .

Лема 6.27. *Якщо $|R : L| = p$ та a — одиниця в R , то мають місце наступні твердження:*

1. $L = \langle a \cdot p \rangle + \langle b \rangle + \langle c \rangle + \langle d \rangle$;
2. елемент $x = ax_1 + bx_2 + cx_3 + dx_4$ є оборотним тоді і тільки тоді, коли $x_1 \not\equiv 0 \pmod{p}$.

Доведення. Оскільки $a \notin L$ та $ap \in L$, то

$$L = \langle a \cdot p \rangle + \langle b \rangle + \langle c \rangle + \langle d \rangle.$$

З того, що $R^* = R \setminus L$ випливає, що

$$R^* = \{ax_1 + bx_2 + cx_3 + dx_4 | x_1 \not\equiv 0 \pmod{p}\}.$$

□

Застосовуючи твердження 1) леми 6.27 до теореми 6.26, отримуємо наступну формулу для добутку xu довільних елементів $x = ax_1 + bx_2 + cx_3 + dx_4$ та $y = ay_1 + by_2 + cy_3 + dy_4$ локального майже-кільця R .

Наслідок 6.28. *Якщо $x, y \in R$, $|R : L| = p$,*

$$xb = a\alpha_b(x) + b\beta_b(x) + c\gamma_b(x) + d\phi_b(x)$$

та

$$xd = a\alpha_d(x) + b\beta_d(x) + c\gamma_d(x) + d\phi_d(x),$$

то

$$\begin{aligned} xy = & a(x_1y_1 + \alpha_b(x)y_2 + \alpha_d(x)y_4) + b(x_2y_1 + \\ & + \beta_b(x)y_2 + \beta_d(x)y_4) + c\left(x_3y_1 + \gamma_b(x)y_2 + x_1\beta_b(x)y_3 + \right. \\ & \left. + \gamma_d(x)y_4 - x_1x_2\binom{y_1}{2}\right) + d(x_4y_1 + \phi_b(x)y_2 + \phi_d(x)y_4), \end{aligned} \quad (6.19)$$

причому для відображень $\alpha_b : R \rightarrow \mathbb{Z}_{p^m}$, $\beta_b : R \rightarrow \mathbb{Z}_{p^n}$, $\gamma_b : R \rightarrow \mathbb{Z}_p$, $\phi_b : R \rightarrow \mathbb{Z}_{p^k}$ та $\alpha_d : R \rightarrow \mathbb{Z}_{p^m}$, $\beta_d : R \rightarrow \mathbb{Z}_{p^n}$, $\gamma_d : R \rightarrow \mathbb{Z}_p$, $\phi_d : R \rightarrow \mathbb{Z}_{p^k}$ виконуються наступні твердження:

0) $\alpha_b(0) \equiv 0 \pmod{p^m}$, $\beta_b(0) \equiv 0 \pmod{p^n}$, $\gamma_b(0) \equiv 0 \pmod{p}$, $\phi_b(0) \equiv 0 \pmod{p^k}$, $\alpha_d(0) \equiv 0 \pmod{p^m}$, $\beta_d(0) \equiv 0 \pmod{p^n}$, $\gamma_d(0) \equiv 0 \pmod{p}$, $\phi_d(0) \equiv 0 \pmod{p^k}$ тоді і тільки тоді, коли майже-кільце R є нуль-симетричним;

- 1) $\alpha_b(x) \equiv 0 \pmod{p}$;
- 2) якщо $\beta_b(x) \equiv 0 \pmod{p}$, то $x_1 \equiv 0 \pmod{p}$;
- 3) $\alpha_b(xy) \equiv x_1\alpha_b(y) + \alpha_b(x)\beta_b(y) + \alpha_d(x)\phi_b(y) \pmod{p^m}$;
- 4) $\beta_b(xy) \equiv x_2\alpha_b(y) + \beta_b(x)\beta_b(y) + \beta_d(x)\phi_b(y) \pmod{p^n}$;
- 5) $\gamma_b(xy) \equiv \gamma_b(x)\beta_b(y) + x_1\beta_b(x)\gamma_b(y) + \gamma_d(x)\phi_b(y) \pmod{p}$;
- 6) $\phi_b(xy) \equiv x_4\alpha_b(y) + \phi_b(x)\beta_b(y) + \phi_d(x)\phi_b(y) \pmod{p^k}$;
- 7) $\alpha_d(xy) \equiv x_1\alpha_d(y) + \alpha_b(x)\beta_d(y) + \alpha_d(x)\phi_d(y) \pmod{p^m}$;
- 8) $\beta_d(xy) \equiv x_2\alpha_d(y) + \beta_b(x)\beta_d(y) + \beta_d(x)\phi_d(y) \pmod{p^n}$;
- 9) $\gamma_d(xy) \equiv \gamma_b(x)\beta_d(y) + x_1\beta_b(x)\gamma_d(y) + \gamma_d(x)\phi_d(y) \pmod{p}$;
- 10) $\phi_d(xy) \equiv x_4\alpha_d(y) + \phi_b(x)\beta_d(y) + \phi_d(x)\phi_d(y) \pmod{p^k}$.

Доведення. Дійсно, твердження 0), 3), 4), 6)–8), 10) повторюють твердження 0)–2), 4)–6), 8) теореми 6.26. Оскільки

$$L = \langle a \cdot p \rangle + \langle b \rangle + \langle c \rangle + \langle d \rangle$$

за твердженням 1) леми 6.27 та $L \in (R, R)$ -підгрупою в R^+ за твердженням 1) леми 3.4, то $xb \in L$ та $xd \in L$, звідки $a\alpha_b(x) \in L$ та $a\alpha_d(x) \in L$ для кожного $x \in R$. Отже, $\alpha_b(x) \equiv 0 \pmod{p}$ та $\alpha_d(x) \equiv 0 \pmod{p}$, що доводить твердження 1). Підставляючи отримане значення $a\alpha_b(x)$ та $a\alpha_d(x)$ в конгруентності 1)–8) теореми 6.26, одержуємо твердження 3)–10) наслідку та формулу множення (6.19). Поклавши в формулі (6.19) $y = c$, отримаємо $xc = c(x_1\beta_b(x))$. Отже, якщо $\beta_b(x) \equiv 0 \pmod{p}$, то $xc = 0$, і тому $x \in L$. За твердженням 2) леми 6.27 випливає, що $x_1 \equiv 0 \pmod{p}$ та доводить твердження 2). $\square$

Покажемо тепер, що для довільного простого числа p та натуральних чисел $m \geq n$ та $m \geq k$ з $m > 1$ при $p = 2$ існує локальне майже-кілеце R , адитивна група R^+ якого ізоморфна групі $F(p^m, p^n, p, p^k)$.

Лема 6.29. *Нехай R — локальне майже-кілеце, адитивна група якого ізоморфна групі $F(p^m, p^n, p, p^k)$, $|R : L| = p$, $m \geq n \geq 1$, $m \geq k$ та $m > 1$ при $p = 2$. Якщо $x = ax_1 + bx_2 + cx_3 + dx_4$ та $y = ay_1 + by_2 + cy_3 + dy_4$ — довільні елементи із R , то відображення $\alpha_b : R \rightarrow \mathbb{Z}_{p^m}$, $\beta_b : R \rightarrow \mathbb{Z}_{p^n}$, $\gamma_b : R \rightarrow \mathbb{Z}_p$, $\phi_b : R \rightarrow \mathbb{Z}_{p^k}$ та $\alpha_d : R \rightarrow \mathbb{Z}_{p^m}$, $\beta_d : R \rightarrow \mathbb{Z}_{p^n}$, $\gamma_d : R \rightarrow \mathbb{Z}_p$, $\phi_d : R \rightarrow \mathbb{Z}_{p^k}$ можуть бути наступними:*

$$\begin{aligned} \alpha_b(x) &= 0 \pmod{p^m}, \quad \gamma_b(x) = 0 \pmod{p}, \quad \phi_b(x) = 0 \pmod{p^k}, \\ \alpha_d(x) &= 0 \pmod{p^m}, \quad \beta_d(x) = 0 \pmod{p^n}, \quad \gamma_d(x) = 0 \pmod{p}, \quad \phi_d(x) = 1 \pmod{p^k}, \end{aligned}$$

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

Нехай $[n, i]$ є i -ою групою порядку n в бібліотеці SmallGroups системи комп'ютерної алгебри GAP.

Приклад 6.30. Нехай $G \cong ((C_5 \times C_5) \rtimes C_5) \times C_5$ [625, 12]. Якщо $x = ax_1 + bx_2 + cx_3 + dx_4$, $y = ay_1 + by_2 + cy_3 + dy_4 \in G$ та $(G, +, \cdot)$ є локальним майже-кільцем, то « $\cdot$ » може бути наступним:

$$x \cdot y = a(x_1y_1) + b(x_2y_1 + \beta_b(x)y_2) + c\left(x_3y_1 + x_1\beta_b(x)y_3 - x_1x_2\binom{y_1}{2}\right) + d(x_4y_1 + y_4),$$

де

$$\beta_b(x) = \begin{cases} 1, & x_1 \not\equiv 0 \pmod{5}; \\ 0, & x_1 \equiv 0 \pmod{5}. \end{cases}$$

Висновки до розділу 6

У даному розділі:

- наведено необхідні та достатні умови існування майже-кілець з одиницею на групах Міллера–Морено;
- показано, що не існує майже-кілець з одиницею, адитивна група яких ізоморфна групі Шмідта;
- описано прямі добутки p -груп Міллера–Морено та циклічних p -груп як адитивні групи майже-кілець з одиницею та локальних майже-кілець;
- визначено формули множення для таких майже-кілець та описано функції, що їх задають.

Основні результати даного розділу опубліковано у працях [15, 14, 8, 4] зі списку публікацій і, відповідно, [3, 76, 80, 86] зі списку використаних

джерел, а також опубліковано у тезах конференцій [41, 40, 35, 23, 24] і, відповідно, [4, 6, 77, 79, 82].

Розділ 7

Застосування системи GAP для дослідження та класифікації локальних майже-кілець

У даному розділі досліджується побудова майже-кілець з одиницею та класифікація локальні майже-кілець за допомогою системи GAP. Наведено функції для дослідження локальних майже-кілець пакету LocalNR.

7.1. Побудова майже-кілець з одиницею

Список усіх локальних майже-кілець порядку не більше 31 можна отримати з бібліотек пакету SONATA систем GAP. Зокрема, існує 9 неізоморфних груп порядку 16, які є адитивними групами локальних майже-кілець. Використовуючи мову програмування GAP, побудовано загальний алгоритм, який дозволяє класифікувати локальні майже-кілець порядку 32 і більше.

Алгоритм побудови майже-кілець з одиницею базується на наступній теоремі.

Теорема 7.1. *Нехай G — група, і нехай множина $\text{End } G$ усіх ендоморфізмів G розглядається як моноїд щодо композиції ендоморфізмів. Тоді G — адитивна група майже-кілець 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 $\phi, \psi \in F$.

Доведення. Дійсно, якщо покласти $g^\phi \star g^\psi = g^{\phi\psi}$, то $Nr = (G, \cdot, \star_F)$ — це ліве майже-кільце з одиницею g , а мультиплікативний моноїд Nr ізоморфний F . Зокрема, у цьому випадку показник степеня G збігається з порядком g . $\square$

Більш того, якщо F_1 та F_2 є підмоноїдами $\text{End } G$, що задовольняють теорему 7.1, то (ліві) майже-кільця $Nr_1 = (G, \cdot, \star_{F_1})$ та $Nr_2 = (G, \cdot, \star_{F_2})$ є ізоморфними тоді і тільки тоді, коли існує такий автоморфізм α для G , що $F_1^\alpha = F_2$.

Таким чином, щоб визначити всі неізоморфні майже-кільця з одиницею на групі G , необхідно знайти всі підмоноїди $\text{End } G$, що задовольняють висновок останньої теореми. Очевидно, що це можливо лише тоді, коли моноїд $\text{End } G$ малий у певному сенсі. Наприклад, якщо G має порядок не більше 31, то всі такі майже-кільця можна знайти.

Якщо G — проста група, то $\text{End } G = \text{Aut } G \cup \{0\}$, і тому $F \setminus \{0\}$ — група автоморфізмів, що діють кратнотранзитивно на G . Відомо, що в цьому випадку G є абелевою групою простого порядку.

7.2. Локальні майже-кільця пакету SONATA

Щоб визначити, чи буде вибране майже-кільце R локальним, за допомогою команди

$$u := \text{Size}(\text{NearRingUnits}(R));$$

знаходимо порядок u мультиплікативної групи R^* цього майже-кільця.

Далі, за допомогою команди

$$Id := NearRingIdeals(R);$$

визначаємо список всіх ідеалів майже-кільця R , а командою

$$Ord := List(Id, Size);$$

повертаємо відповідний список їх порядків. Найбільший з цих порядків — порядок $t := Size(R)$. Якщо число $t - u$ міститься в списку Ord , то майже-кільце R є локальним, в іншому разі — ні.

Позначимо через C_n циклічну групу порядку n , $I(R^+)$ тип групи G в бібліотеці *AllSmallGroups* системи GAP.

Наступне твердження легко отримати з результатів статті [5].

Твердження 7.2. *Нехай R — локальне майже-кільце порядку не вище 31, яке не є майже-полем. Тоді група R^+ та її підгрупа L є наступними:*

- $IdGroup(R^+) = [4, 1]$, $R^+ \cong C_4$ та $IdGroup(L) = [2, 1]$, $L \cong C_2$;
- $IdGroup(R^+) = [4, 2]$, $R^+ \cong C_2 \times C_2$ та $IdGroup(L) = [2, 1]$, $L \cong C_2$;
- $IdGroup(R^+) = [8, 1]$, $R^+ \cong C_8$ та $IdGroup(L) = [4, 1]$, $L \cong C_4$;
- $IdGroup(R^+) = [8, 2]$, $R^+ \cong C_4 \times C_2$ та $IdGroup(L) = [4, 2]$, $L \cong C_2 \times C_2$;
- $IdGroup(R^+) = [8, 5]$, $R^+ \cong C_2 \times C_2 \times C_2$ та $IdGroup(L) = [4, 2]$, $L \cong C_2 \times C_2$;
- $IdGroup(R^+) = [9, 1]$, $R^+ \cong C_9$ та $IdGroup(L) = [3, 1]$, $L \cong C_3$;

- $IdGroup(R^+) = [9, 2], R^+ \cong C_3 \times C_3$ *ma* $IdGroup(L) = [3, 1], L \cong C_3$;
- $IdGroup(R^+) = [16, 1], R^+ \cong C_{16}$ *ma* $IdGroup(L) = [8, 1], L \cong C_4 \times C_2$;
- $IdGroup(R^+) = [16, 2], R^+ \cong C_4 \times C_4$ *ma* $IdGroup(L) = [8, 2], L \cong C_4 \times C_2$;
- $IdGroup(R^+) = [16, 3], R^+ \cong (C_4 \times C_2) \rtimes C_2$ *ma* $IdGroup(L) = [8, 5], L \cong C_2 \times C_2 \times C_2$;
- $IdGroup(R^+) = [16, 4], R^+ \cong C_4 \rtimes C_4$ *ma* $IdGroup(L) = [8, 2], L \cong C_4 \times C_2$;
- $IdGroup(R^+) = [16, 5], R^+ \cong C_8 \times C_2$ *ma* $IdGroup(L) = [8, 2], L \cong C_4 \times C_2$;
- $IdGroup(R^+) = [16, 6], R^+ \cong C_8 \times C_2$ *ma* $IdGroup(L) = [8, 2], L \cong C_4 \times C_2$;
- $IdGroup(R^+) = [16, 10], R^+ \cong C_4 \times C_2 \times C_2$ *ma* $IdGroup(L) = [8, 5], L \cong C_2 \times C_2 \times C_2$;
- $IdGroup(R^+) = [16, 12], R^+ \cong C_2 \times Q_8$ *ma* $IdGroup(L) = [4, 2], L \cong C_2 \times C_2$;
- $IdGroup(R^+) = [16, 14], R^+ \cong C_2 \times C_2 \times C_2 \times C_2$:
 - $IdGroup(L) = [8, 5], L \cong C_2 \times C_2 \times C_2$;
 - $IdGroup(L) = [4, 2], L \cong C_2 \times C_2$;
- $IdGroup(R^+) = [25, 1], R^+ \cong C_{25}$ *ma* $IdGroup(L) = [5, 1], L \cong C_5$;
- $IdGroup(R^+) = [25, 2], R^+ \cong C_5 \times C_5$ *ma* $IdGroup(L) = [5, 1], L \cong C_5$;

- $IdGroup(R^+) = [27, 1]$, $R^+ \cong C_{27}$ *ma* $IdGroup(L) = [9, 1]$, $L \cong C_9$;
- $IdGroup(R^+) = [27, 2]$, $R^+ \cong C_9 \times C_3$ *ma* $IdGroup(L) = [9, 2]$,
 $L \cong C_3 \times C_3$;
- $IdGroup(R^+) = [27, 3]$, $R^+ \cong (C_3 \times C_3) \rtimes C_3$ *ma* $IdGroup(L) = [,]$,
 $L \cong C_3 \times C_3$;
- $IdGroup(R^+) = [27, 4]$, $R^+ \cong C_9 \rtimes C_3$ *ma* $IdGroup(L) = [9, 2]$,
 $L \cong C_3 \times C_3$;
- $IdGroup(R^+) = [27, 5]$, $R^+ \cong C_3 \times C_3 \times C_3$ *ma* $IdGroup(L) = [9, 2]$,
 $L \cong C_3 \times C_3$.

7.3. LocalNR package: функції для майже-кілець

Пакет LocalNR містить бібліотеку локальних майже-кілець до порядку 361 та деякі функції для аналізу скінченних майже-кілець. Поточна версія цього пакету — 1.0.4, випущена 15.03.2024. Наведемо деякі функції для локальних майже-кілець з пакету LocalNR.

7.3.1. UnitsOfNearRing

UnitsOfNearRing(R) (атрибут)

Повертає: множина

Аргументом є майже-кілець R . Вивід список оборотних елементів майже-кілеця, якщо R є майже-кілцем з одиницею, інакше вивід має вигляд `Error, no units exist.`

Приклад.

N — локальне майже-кілець з адитивною групою $[32, 5]$ та мультиплікативною групою $[16, 3]$, яке є 8 у каталогу майже-кілець в бібліотеці.

```
gap> N := LocalNearRing(32,5,16,3,8);
```

```
ExplicitMultiplicationNearRing ( <pc group of size 32 with  
5 generators> , multiplication )
```

U — список оборотних елементів майже-кілець N .

```
gap> U := UnitsOfNearRing(N);
```

```
[ (f1), (f1*f5), (f1*f4), (f1*f4*f5), (f1*f3), (f1*f3*f5),  
(f1*f3*f4), (f1*f3*f4*f5), (f1*f2), (f1*f2*f5), (f1*f2*f4),  
(f1*f2*f4*f5), (f1*f2*f3), (f1*f2*f3*f5), (f1*f2*f3*f4),  
(f1*f2*f3*f4*f5) ]
```

```
gap> Un := NearRingUnits(N);;
```

```
gap> U = Un;
```

```
true
```

Наведемо програмну реалізацію цієї функції на мові GAP, що міститься в пакеті LocalNR.

```
# UnitsOfNearRing(< R >)
```

```
InstallMethod(UnitsOfNearRing,
```

```
“Compute all units of nearring”,
```

```
true,
```

```
[IsNearRing], 0,
```

```
function(R)
```

```
local A, G, one, x;
```

```
# one — одиниця майже-кілець  $R$ .
```

```
one := Identity(R);
```

```
if one = fail then
```

```

return [];
else
#  $G$  — адитивна група майже-кільця  $R$ .
 $G := \text{GroupReduct}(R)$ ;
#  $A$  — група автоморфізмів групи  $G$ .
 $A := \text{AutomorphismGroup}(G)$ ;
# Повертаємо список оборотних елементів з  $R$ .
return  $\text{Filtered}(R, x \rightarrow x^{\wedge} \text{Size}(A) = \text{one})$ ;
fi;
end);

```

7.3.2. IsLocalNearRing

IsLocalNearRing(R) (властивість)

Повертає: логічний оператор

Аргументом є майже-кільце R . Вивід має значення **true**, якщо R є локальним майже-кільцем, інакше вивід має значення **false**.

Приклад.

```

#  $H$  — група з бібліотеки AllSmallGroups з  $\text{IdGroup} = [16, 6]$ .
gap> H := SmallGroup(16,6);
<pc group of size 16 with 4 generators>
#  $A$  — майже-кільце, породжене автоморфізмами групи  $H$ .
gap> A := AutomorphismNearRing(H);
AutomorphismNearRing( <pc group of size 16 with 4 generators> )
# Порядок майже-кільця  $A$ .
gap> Size(A);

```

```

# Перевірка, чи є локальним майже-кільце  $A$ .
gap> IsLocalNearRing(A);
true

#  $K$  — майже-кільце з одиницею на групі з бібліотеки AllSmallGroups
з  $IdGroup = [8, 2]$  та типом ізоморфізму 1.
gap> K := LibraryNearRingWithOne(SmallGroup(8,2),1);
#I using isomorphic copy of the group LibraryNearRing(8/2, 814)
# Перевірка, чи є локальним майже-кільце  $K$ .
gap> IsLocalNearRing(K);
false

```

Наведемо програмну реалізацію цієї функції на мові GAP, що міститься в пакеті LocalNR.

```

# IsLocalNearRing(<  $R$  >)
InstallMethod(IsLocalNearRing,
  “Is local nearring”,
  true,
  [IsNearRing],
  0,
  function( $R$ )
    local  $h, f, ff, k, l, i$ ;
    if IsNearRingWithIdentity( $R$ ) then
       $h := \text{NearRingUnits}(R)$ ;
       $f := []$ ;
      for  $i$  in  $h$  do
         $ff := \text{AsGroupReductElement}(i)$ ;
        Add( $f, ff$ );
      od;
    end;
  end;

```

```

k := Difference(GroupReduct(R), f);;
l := Subgroup(GroupReduct(R), k);
if Size(l) = Size(k) then
  return true;
else return false;
fi;
else return false;
fi;
end);

```

7.3.3. IsLocalRing

IsLocalRing(*R*) (властивість)

Повертає: логічний оператор

Аргументом є локальне майже-кілець *R*. Вивід має значення **true**, якщо *R* є локальним кільцем, інакше вивід має значення **false**.

Приклад.

L — список локальних майже-кілець з адитивною групою [16, 14] та мультиплікативною групою [8, 4] з бібліотеці.

```
gap> L := AllLocalNearRings(16,14,8,4);;
```

Знаходимо розмір списку *L*.

```
gap> Size(L);
```

24

Фільтруємо всі локальні кільця зі списку *L*.

```
gap> F := Filtered(L, x->IsLocalRing(x));;
```

Знаходимо розмір списку *F*.

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

1

Наведемо програмну реалізацію цієї функції на мові GAP, що міститься в пакеті LocalNR.

```
# IsLocalRing(< R >)
InstallMethod(IsLocalRing,
  "Is local ring",
  [IsNearRing],
  function(R)
    if IsLocalNearRing(R) then
      if IsAbelian(GroupReduct(R)) and
        IsDistributiveNearRing(R) then
        return true;
      else return false;
    fi;
  else return false;
  fi;
end);
```

7.3.4. NearRingNonUnits

NearRingNonUnits(R) (атрибут)

Повертає: множина

Аргументом є майже-кільце R . Вихідним результатом є список необоротних елементів R .

Приклад.

T — локальне майже-кілець з адитивною групою $[49, 2]$ та мультиплікативною групою $[42, 1]$, яке є 1 у каталогі майже-кілець в бібліотеці.

```
gap> T := LocalNearRing(49,2,42,1,1);
      ExplicitMultiplicationNearRing ( <pc group of size 49 with
2 generators> , multiplication )
```

Nu — список необоротних елементів з T .

```
gap> Nu := NearRingNonUnits(T);
[ (<identity> of ...), (f2), (f2^2), (f2^3), (f2^4), (f2^5), (f2^6) ]
```

Знаходимо розмір списку Nu .

```
gap> Size(Nu);
```

7

R — майже-кілець на групі з бібліотеки *AllSmallGroups* з $IdGroup = [8, 4]$ та типом ізоморфізму 3.

```
gap> R := LibraryNearRing(SmallGroup(8,4),3);
```

I using isomorphic copy of the group LibraryNearRing(8/5, 3)

N — список необоротних елементів з R .

```
gap> N := NearRingNonUnits(R);
[ (), ((1,2,3,4)(5,6,7,8)), ((1,3)(2,4)(5,7)(6,8)), ((1,4,3,2)(5,8,7,6)),
((1,5,3,7)(2,8,4,6)), ((1,6,3,8)(2,5,4,7)), ((1,7,3,5)(2,6,4,8)),
((1,8,3,6)(2,7,4,5)) ]
```

Наведемо програмну реалізацію цієї функції на мові GAP, що міститься в пакеті LocalNR.

```
# NearRingNonUnits(< R >)
InstallMethod(NearRingNonUnits,
  "Compute nearring non — units",
  [IsNearRing],
  function(R)
```

```

# Перевірка, чи майже-кільце  $R$  з одиницею.
if Identity( $R$ ) = fail then
return  $R$ ;
# Повертаємо список необоротних елементів з  $R$ .
else return
Difference( $R$ , NearRingUnits( $R$ ));
fi;
end);

```

7.3.5. NonUnitsAsAdditiveSubgroup

NonUnitsAsAdditiveSubgroup(R) (атрибут)

Повертає: підгрупа

Аргументом є локальне майже-кільце R . Вихідним результатом є адитивна підгрупа необоротних елементів R .

Приклад.

T — локальне майже-кільце з адитивною групою $[125, 4]$ та мультиплікативною групою $[100, 9]$, яке є 1 у каталогу майже-кілець в бібліотеці.

```
gap> T := LocalNearRing(125,4,100,9,1);
```

```
ExplicitMultiplicationNearRing ( <pc group of size 125 with
3 generators> , multiplication )
```

L — підгрупа необоротних елементів з T .

```
gap> L := NonUnitsAsAdditiveSubgroup(T);
```

```
Group([ <identity> of ..., f2, f3, f2^2, f2*f3, f3^2, f2^3, f2^2*f3, f2*f3^2,
f3^3, f2^4, f2^3*f3, f2^2*f3^2, f2*f3^3, f3^4, f2^4*f3, f2^3*f3^2, f2^2*f3^3,
f2*f3^4, f2^4*f3^2, f2^3*f3^3, f2^2*f3^4, f2^4*f3^3, f2^3*f3^4, f2^4*f3^4 ])
```

Знаходимо ідентифікатор групи L в бібліотеці *AllSmallGroups*.

```
gap> IdGroup(L);
```

[25, 2]

Наведемо програмну реалізацію цієї функції на мові GAP, що міститься в пакеті LocalNR.

```
# NonUnitsAsAdditiveSubgroup(< R >)
InstallMethod(NonUnitsAsAdditiveSubgroup,
  "Compute non – units as additive subgroup",
  [IsNearRing],
  function(R)
    local a, N, g, L;
    if IsLocalNearRing(R) then
      N := NearRingNonUnits(R);
      g := [];
      for a in N do
        Add(g, AsGroupReductElement(a));
      od;
      L := Subgroup(GroupReduct(R), g);
      return L;
    else return fail;
  fi;
end);
```

7.4. Майже-кільця з одиницею і локальні майже-кільця, та ендоециклічні групи

Пакет SONATA містить базу даних майже-кілець з одиницею *AllLibraryNearRingsWithOne*. У цій бібліотеці майже-кілець впорядковані відповідно до їхніх адитивних груп G , наприклад, команда

$$N := \text{AllLibraryNearRingsWithOne}(G)$$

визначає списки локальних майже-кілець N .

Використовуючи функцію *IsEndoCyclicGroup* з пакету LocalNR для перевірки, чи є G ендоциклічною групою.

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

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

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

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

Лема 7.3. *Наступні групи G порядку менше 32 є ендоциклічними. Більш того, якщо G є адитивною групою майже-кілець з одиницею R , то виконується наступне.*

- $\text{IdGroup}(G) = [4, 1]$, $G \cong C_4$ та $m(G) = 1$;
- $\text{IdGroup}(G) = [4, 2]$, $G \cong C_2 \times C_2$ та $m(G) = 5$;
- $\text{IdGroup}(G) = [5, 1]$, $G \cong C_5$ та $m(G) = 1$;
- $\text{IdGroup}(G) = [6, 2]$, $G \cong C_6$ та $m(G) = 1$;
- $\text{IdGroup}(G) = [7, 1]$, $G \cong C_7$ та $m(G) = 1$;
- $\text{IdGroup}(G) = [8, 1]$, $G \cong C_8$ та $m(G) = 1$;

- $IdGroup(G) = [8, 2], G \cong C_4 \times C_2 \text{ } ma \text{ } m(G) = 10;$
- $IdGroup(G) = [8, 3], G \cong D_8 \text{ } ma \text{ } m(G) = 7;$
- $IdGroup(G) = [8, 4], G \cong Q_8 \text{ } ma \text{ } m(G) = 0;$
- $IdGroup(G) = [8, 5], G \cong C_2 \times C_2 \times C_2 \text{ } ma \text{ } m(G) = 35;$
- $IdGroup(G) = [9, 1], G \cong C_9 \text{ } ma \text{ } m(G) = 1;$
- $IdGroup(G) = [9, 2], G \cong C_3 \times C_3 \text{ } ma \text{ } m(G) = 10;$
- $IdGroup(G) = [10, 2], G \cong C_{10} \text{ } ma \text{ } m(G) = 1;$
- $IdGroup(G) = [11, 1], G \cong C_{11} \text{ } ma \text{ } m(G) = 1;$
- $IdGroup(G) = [12, 2], G \cong C_{12} \text{ } ma \text{ } m(G) = 1;$
- $IdGroup(G) = [12, 4], G \cong D_{12} \text{ } ma \text{ } m(G) = 1;$
- $IdGroup(G) = [12, 5], G \cong C_6 \times C_2 \text{ } ma \text{ } m(G) = 9;$
- $IdGroup(G) = [13, 1], G \cong C_{13} \text{ } ma \text{ } m(G) = 1;$
- $IdGroup(G) = [14, 2], G \cong C_{14} \text{ } ma \text{ } m(G) = 1;$
- $IdGroup(G) = [15, 1], G \cong C_{15} \text{ } ma \text{ } m(G) = 1;$
- $IdGroup(G) = [16, 1], G \cong C_{16} \text{ } ma \text{ } m(G) = 1;$
- $IdGroup(G) = [16, 2], G \cong C_4 \times C_4 \text{ } ma \text{ } m(G) = 51;$
- $IdGroup(G) = [16, 3], G \cong (C_4 \times C_2) \rtimes C_2 \text{ } ma \text{ } m(G) = 132;$
- $IdGroup(G) = [16, 4], G \cong C_4 \rtimes C_4 \text{ } ma \text{ } m(G) = 40;$
- $IdGroup(G) = [16, 5], G \cong C_8 \times C_2 \text{ } ma \text{ } m(G) = 37;$
- $IdGroup(G) = [16, 6], G \cong C_8 \rtimes C_2 \text{ } ma \text{ } m(G) = 33;$

- $IdGroup(G) = [16, 7], G \cong D_{16} \text{ } ma \text{ } m(G) = 0;$
- $IdGroup(G) = [16, 10], G \cong C_4 \times C_2 \times C_2 \text{ } ma \text{ } m(G) = 470;$
- $IdGroup(G) = [16, 11], G \cong C_2 \times D_8 \text{ } ma \text{ } m(G) = 708;$
- $IdGroup(G) = [16, 12], G \cong C_2 \times Q_8 \text{ } ma \text{ } m(G) = 4;$
- $IdGroup(G) = [16, 14], G \cong C_2 \times C_2 \times C_2 \times C_2 \text{ } ma \text{ } m(G) = 2798;$
- $IdGroup(G) = [17, 1], G \cong C_{17} \text{ } ma \text{ } m(G) = 1;$
- $IdGroup(G) = [18, 2], G \cong C_{18} \text{ } ma \text{ } m(G) = 1;$
- $IdGroup(G) = [18, 3], G \cong C_3 \times S_3 \text{ } ma \text{ } m(G) = 8;$
- $IdGroup(G) = [18, 5], G \cong C_6 \times C_3 \text{ } ma \text{ } m(G) = 17;$
- $IdGroup(G) = [19, 1], G \cong C_{19} \text{ } ma \text{ } m(G) = 1;$
- $IdGroup(G) = [20, 2], G \cong C_{20} \text{ } ma \text{ } m(G) = 1;$
- $IdGroup(G) = [20, 4], G \cong D_{20} \text{ } ma \text{ } m(G) = 1;$
- $IdGroup(G) = [20, 5], G \cong C_{10} \times C_2 \text{ } ma \text{ } m(G) = 9;$
- $IdGroup(G) = [21, 2], G \cong C_{21} \text{ } ma \text{ } m(G) = 1;$
- $IdGroup(G) = [22, 2], G \cong C_{22} \text{ } ma \text{ } m(G) = 1;$
- $IdGroup(G) = [23, 1], G \cong C_{23} \text{ } ma \text{ } m(G) = 1;$
- $IdGroup(G) = [24, 2], G \cong C_{24} \text{ } ma \text{ } m(G) = 1;$
- $IdGroup(G) = [24, 5], G \cong \text{ } ma \text{ } m(G) = 1;$
- $IdGroup(G) = [24, 6], G \cong D_{24} \text{ } ma \text{ } m(G) = 0;$
- $IdGroup(G) = [24, 9], G \cong C_{12} \times C_2 \text{ } ma \text{ } m(G) = 14;$

- $IdGroup(G) = [24, 10]$, $G \cong C_3 \times D_8$ та $m(G) = 7$;
- $IdGroup(G) = [24, 11]$, $G \cong C_3 \times Q_8$ та $m(G) = 0$;
- $IdGroup(G) = [24, 13]$, $G \cong C_2 \times A_4$ та $m(G) = 8$;
- $IdGroup(G) = [24, 14]$, $G \cong C_2 \times C_2 \times S_3$ та $m(G) = 10$;
- $IdGroup(G) = [24, 15]$, $G \cong C_6 \times C_2 \times C_2$ та $m(G) = 136$;
- $IdGroup(G) = [25, 1]$, $G \cong C_{25}$ та $m(G) = 1$;
- $IdGroup(G) = [25, 2]$, $G \cong C_5 \times C_5$ та $m(G) = 16$;
- $IdGroup(G) = [26, 2]$, $G \cong C_{26}$ та $m(G) = 1$;
- $IdGroup(G) = [27, 1]$, $G \cong C_{27}$ та $m(G) = 1$;
- $IdGroup(G) = [27, 2]$, $G \cong C_9 \times C_3$ та $m(G) = 20$;
- $IdGroup(G) = [27, 3]$, $G \cong (C_3 \times C_3) \rtimes C_3$ та $m(G) = 22$;
- $IdGroup(G) = [27, 4]$, $G \cong C_9 \rtimes C_3$ та $m(G) = 4$;
- $IdGroup(G) = [27, 5]$, $G \cong C_3 \times C_3 \times C_3$ та $m(G) = 202$;
- $IdGroup(G) = [28, 2]$, $G \cong C_{28}$ та $m(G) = 1$;
- $IdGroup(G) = [28, 3]$, $G \cong D_{28}$ та $m(G) = 1$;
- $IdGroup(G) = [28, 4]$, $G \cong C_{14} \times C_2$ та $m(G) = 9$;
- $IdGroup(G) = [29, 1]$, $G \cong C_{29}$ та $m(G) = 1$;
- $IdGroup(G) = [30, 4]$, $G \cong C_{30}$ та $m(G) = 1$;
- $IdGroup(G) = [31, 1]$, $G \cong C_{31}$ та $m(G) = 1$.

З леми 7.3 випливає наступна теорема.

Теорема 7.4. *Нехай G — група порядку менше 32. Якщо G — адитивна група майже-кільця з одиницею R , то G є ендоециклічною.*

7.4.1. Локальні майже-кілець та ендоциклічні групи порядку 32

Пакет LocalNR надає функціональність для дослідження майже-кілець з одиницею та локальних майже-кілець. Пакет також включає базу даних *AllLocalNearRings* локальних майже-кілець малих порядків. У цій бібліотеці локальні майже-кілець упорядковані відповідно до їх адитивних та мультиплікативних груп, наприклад, команда

$$N := \text{AllLocalNearRings}(k, l, m, n)$$

визначає списки локальних майже-кілець N . Аргументи k, l, m, n взяті з IdGroup адитивної групи та мультиплікативної групи відповідно.

Далі, позначимо через $n(G)$ — кількість усіх неізоморфних локальних майже-кілець R , адитивна група яких R^+ ізоморфна групі G .

Існує 51 неізоморфна група порядку $32 = 2^5$, з яких 35 є ендоциклічними групами, і лише 19 з цих груп є адитивними групами локальних майже-кілець.

Лема 7.5. *Наступні групи G порядку 32 є ендоциклічними. Більш того, якщо G є адитивною групою локального майже-кілець R , то виконується наступне.*

- $\text{IdGroup}(G) = [32, 1]$, $G \cong C_{32}$ та $n(G) = 1$.
- $\text{IdGroup}(G) = [32, 2]$, $G \cong (C_4 \times C_2) \rtimes C_4$ та $n(G) = 1397$.
- $\text{IdGroup}(G) = [32, 3]$, $G \cong C_8 \times C_4$ та $n(G) = 880$.
- $\text{IdGroup}(G) = [32, 4]$, $G \cong C_8 \rtimes C_4$ та $n(G) = 798$.
- $\text{IdGroup}(G) = [32, 5]$, $G \cong (C_8 \times C_2) \rtimes C_2$ та $n(G) = 1945$.

- $IdGroup(G) = [32, 6], G \cong ((C_4 \times C_2) \rtimes C_2) \rtimes C_2 \text{ } ma \text{ } n(G) = 433.$
- $IdGroup(G) = [32, 7], G \cong (C_8 \rtimes C_2) \rtimes C_2 \text{ } ma \text{ } n(G) = 225.$
- $IdGroup(G) = [32, 8], G \cong C_2 \cdot ((C_4 \times C_2) \rtimes C_2) = (C_2 \times C_2) \cdot (C_4 \times C_2) \text{ } ma \text{ } n(G) = 208.$
- $IdGroup(G) = [32, 9], G \cong (C_8 \times C_2) \rtimes C_2 \text{ } ma \text{ } n(G) = 0.$
- $IdGroup(G) = [32, 10], G \cong Q_8 \rtimes C_4 \text{ } ma \text{ } n(G) = 0.$
- $IdGroup(G) = [32, 11], G \cong (C_4 \times C_4) \rtimes C_2 \text{ } ma \text{ } n(G) = 0.$
- $IdGroup(G) = [32, 12], G \cong C_4 \rtimes C_8 \text{ } ma \text{ } n(G) = 2406.$
- $IdGroup(G) = [32, 16], G \cong C_{16} \times C_2 \text{ } ma \text{ } n(G) = 129.$
- $IdGroup(G) = [32, 17], G \cong C_{16} \rtimes C_2 \text{ } ma \text{ } n(G) = 129.$
- $IdGroup(G) = [32, 18], G \cong D_{32} \text{ } ma \text{ } n(G) = 0.$
- $IdGroup(G) = [32, 21], G \cong C_4 \times C_4 \times C_2 \text{ } ma \text{ } n(G) = 135558.$
- $IdGroup(G) = [32, 22], G \cong C_2 \times ((C_4 \times C_2) \rtimes C_2) \text{ } ma \text{ } n(G) = 149374.$
- $IdGroup(G) = [32, 23], G \cong C_2 \times (C_4 \rtimes C_4) \text{ } ma \text{ } n(G) = 157905.$
- $IdGroup(G) = [32, 24], G \cong (C_4 \times C_4) \rtimes C_2 \text{ } ma \text{ } n(G) = 262544.$
- $IdGroup(G) = [32, 25], G \cong C_4 \times D_8 \text{ } ma \text{ } n(G) = 0.$
- $IdGroup(G) = [32, 26], G \cong C_4 \times Q_8 \text{ } ma \text{ } n(G) = 0.$
- $IdGroup(G) = [32, 27], G \cong (C_2 \times C_2 \times C_2 \times C_2) \rtimes C_2 \text{ } ma \text{ } n(G) = 0.$
- $IdGroup(G) = [32, 28], G \cong (C_4 \times C_2 \times C_2) \rtimes C_2 \text{ } ma \text{ } n(G) = 0.$
- $IdGroup(G) = [32, 34], G \cong (C_4 \times C_4) \rtimes C_2 \text{ } ma \text{ } n(G) = 0.$
- $IdGroup(G) = [32, 35], G \cong C_4 \rtimes Q_8 \text{ } ma \text{ } n(G) = 0.$

- $IdGroup(G) = [32, 36]$, $G \cong C_8 \times C_2 \times C_2$ та $n(G) = 177175$.
- $IdGroup(G) = [32, 37]$, $G \cong C_2 \times (C_8 \rtimes C_2)$ та $n(G) = 527419$.
- $IdGroup(G) = [32, 39]$, $G \cong C_2 \times D_{16}$ та $n(G) = 0$.
- $IdGroup(G) = [32, 43]$, $G \cong (C_2 \times D_8) \rtimes C_2$ та $n(G) = 0$.
- $IdGroup(G) = [32, 45]$, $G \cong C_4 \times C_2 \times C_2 \times C_2$ та $n(G) > 6684533$.
- $IdGroup(G) = [32, 46]$, $G \cong C_2 \times C_2 \times D_8$ та $n(G) = 0$.
- $IdGroup(G) = [32, 47]$, $G \cong C_2 \times C_2 \times Q_8$ та $n(G) = 0$.
- $IdGroup(G) = [32, 49]$, $G \cong (C_2 \times D_8) \rtimes C_2$ та $n(G) = 0$.
- $IdGroup(G) = [32, 50]$, $G \cong (C_2 \times Q_8) \rtimes C_2$ та $n(G) =$.
- $IdGroup(G) = [32, 51]$, $G \cong C_2 \times C_2 \times C_2 \times C_2 \times C_2$ та $n(G) > 7007053$.

Як наслідок леми 7.5 маємо наступний результат.

Теорема 7.6. *Нехай G — група порядку 32. Якщо G — адитивна група локального майже-кільця R , то G є ендоциклічною.*

7.4.2. Локальні майже-кільця та ендоциклічні групи порядку 256

Маємо наступне твердження.

Лема 7.7. *Наступні 2-породжені ендоциклічні групи G порядку 256 та експоненти 16 не є адитивними групами локальних майже-кільць:*

- $IdGroup(G) = [256, 64]$ та $G \cong (((C_{16} \times C_2) \rtimes C_2) \rtimes C_2) \rtimes C_2$;
- $IdGroup(G) = [256, 97]$ та $G \cong ((C_{16} \times C_2) \rtimes C_4) \rtimes C_2$;

- $IdGroup(G) = [256, 98]$ ma $G \cong ((C_8 \times C_2) \rtimes C_8) \rtimes C_2$;
- $IdGroup(G) = [256, 99]$ ma $G \cong (C_2 \times Q_{16}) \rtimes C_8$;
- $IdGroup(G) = [256, 100]$ ma $G \cong ((C_{16} \times C_2) \rtimes C_4) \rtimes C_2$;
- $IdGroup(G) = [256, 101]$ ma $G \cong (C_2 \times Q_{16}) \rtimes C_8$;
- $IdGroup(G) = [256, 102]$ ma $G \cong ((C_8 \times C_2) \rtimes C_8) \rtimes C_2$;
- $IdGroup(G) = [256, 107]$ ma $G \cong (C_8 \rtimes C_4) \rtimes C_8$;
- $IdGroup(G) = [256, 109]$ ma $G \cong (C_8 \rtimes C_4) \rtimes C_8$;
- $IdGroup(G) = [256, 113]$ ma $G \cong (C_8 \rtimes C_4) \rtimes C_8$;
- $IdGroup(G) = [256, 114]$ ma $G \cong (C_8 \rtimes C_4) \rtimes C_8$;
- $IdGroup(G) = [256, 115]$ ma $G \cong (C_8 \rtimes C_4) \rtimes C_8$;
- $IdGroup(G) = [256, 159]$ ma $G \cong (C_8 \rtimes C_8) \rtimes C_4$;
- $IdGroup(G) = [256, 160]$ ma $G \cong (C_4.D_8 = C_4.(C_4 \times C_2)) \rtimes C_8$;
- $IdGroup(G) = [256, 161]$ ma $G \cong (C_4.D_8 = C_4.(C_4 \times C_2)) \rtimes C_8$;
- $IdGroup(G) = [256, 162]$ ma $G \cong (C_8 \rtimes C_8) \rtimes C_4$;
- $IdGroup(G) = [256, 163]$ ma $G \cong (C_8 \rtimes C_8) \rtimes C_4$;
- $IdGroup(G) = [256, 164]$ ma $G \cong (C_4.D_8 = C_4.(C_4 \times C_2)) \rtimes C_8$;
- $IdGroup(G) = [256, 165]$ ma $G \cong (C_4.D_8 = C_4.(C_4 \times C_2)) \rtimes C_8$;
- $IdGroup(G) = [256, 166]$ ma $G \cong (C_8 \rtimes C_8) \rtimes C_4$;
- $IdGroup(G) = [256, 167]$ ma $G \cong (C_8.D_8 = C_4.(C_8 \times C_2)) \rtimes C_4$;
- $IdGroup(G) = [256, 168]$ ma $G \cong (C_8.D_8 = C_4.(C_8 \times C_2)) \rtimes C_4$;

- $IdGroup(G) = [256, 169]$ та $G \cong (C_8.D_8 = C_4.(C_8 \times C_2)) \rtimes C_4$;
- $IdGroup(G) = [256, 170]$ та $G \cong (C_8.D_8 = C_4.(C_8 \times C_2)) \rtimes C_4$;
- $IdGroup(G) = [256, 218]$ та $G \cong ((C_4 \rtimes C_4) \rtimes C_4) \rtimes C_4$;
- $IdGroup(G) = [256, 221]$ та $G \cong (C_2 \times (C_8 \rtimes C_4)) \rtimes C_4$;
- $IdGroup(G) = [256, 242]$ та $G \cong (C_2 \times (C_8 \rtimes C_4)) \rtimes C_4$;
- $IdGroup(G) = [256, 246]$ та $G \cong (C_2 \times (C_8 \rtimes C_4)) \rtimes C_4$;
- $IdGroup(G) = [256, 250]$ та $G \cong (C_2 \times (C_8 \rtimes C_4)) \rtimes C_4$;
- $IdGroup(G) = [256, 384]$ та $G \cong (((C_{16} \rtimes C_2) \rtimes C_2) \rtimes C_2) \rtimes C_2$.

7.5. Класифікація локальних майже-кілець малих порядків

Наступне твердження легко отримати з результатів статті [5].

Наступна таблиця містить кількість неізоморфних локальних майже-кілець порядку не вище 31, які не є майже-полями, з заданими адитивними та мультиплікативними групами.

Твердження 7.8. *Нехай $n(G)$ — кількість всіх неізоморфних локальних майже-кілець R порядку не вище 31, які не є майже-полями, адитивна група R^+ яких ізоморфна групі G . Якщо $n(R^*)$ є кількість цих майже-кілець, для яких $IdGroup(R^*)$ є фіксованим, то наступне має місце.*

- $IdGroup(G) = [4, 1]$, $G \cong C_4$, $n(G) = 1$, $IdGroup(R^*) = [2, 1]$, $R^* \cong C_2$ та $n(R^*) = 1$;

- $IdGroup(G) = [4, 2]$, $G \cong C_2 \times C_2$, $n(G) = 2$, $IdGroup(R^*) = [2, 1]$, $R^* \cong C_2$ *ma* $n(R^*) = 2$;
- $IdGroup(G) = [8, 1]$, $G \cong$, $n(G) = 1$, $IdGroup(R^*) = [4, 2]$, $R^* \cong C_2 \times C_2$ *ma* $n(R^*) = 1$;
- $IdGroup(G) = [8, 2]$, $G \cong C_4 \times C_2$, $n(G) = 5$:
 - $IdGroup(R^*) = [4, 1]$, $R^* \cong C_4$ *ma* $n(R^*) = 2$;
 - $IdGroup(R^*) = [4, 2]$, $R^* \cong C_2 \times C_2$ *ma* $n(R^*) = 3$;
- $IdGroup(G) = [8, 5]$, $G \cong C_2 \times C_2 \times C_2$, $n(G) = 6$:
 - $IdGroup(R^*) = [4, 1]$, $R^* \cong C_4$ *ma* $n(R^*) = 2$;
 - $IdGroup(R^*) = [4, 2]$, $R^* \cong C_2 \times C_2$ *ma* $n(R^*) = 4$;
- $IdGroup(G) = [9, 1]$, $G \cong$, $n(G) = 1$, $IdGroup(R^*) = [6, 2]$, $R^* \cong C_6$ *ma* $n(R^*) = 1$;
- $IdGroup(G) = [9, 2]$, $G \cong$, $n(G) = 3$:
 - $IdGroup(R^*) = [6, 1]$, $R^* \cong S_3$ *ma* $n(R^*) = 2$;
 - $IdGroup(R^*) = [6, 2]$, $R^* \cong C_6$ *ma* $n(R^*) = 1$;
- $IdGroup(G) = [16, 1]$, $G \cong C_{16}$, $n(G) = 1$, $IdGroup(R^*) = [8, 2]$, $R^* \cong C_4 \times C_2$ *ma* $n(R^*) = 1$;
- $IdGroup(G) = [16, 2]$, $G \cong C_4 \times C_4$, $n(G) = 29$:
 - $IdGroup(R^*) = [8, 2]$, $R^* \cong C_4 \times C_2$ *ma* $n(R^*) = 10$;
 - $IdGroup(R^*) = [8, 3]$, $R^* \cong D_8$ *ma* $n(R^*) = 9$;
 - $IdGroup(R^*) = [8, 5]$, $R^* \cong C_2 \times C_2 \times C_2$ *ma* $n(R^*) = 6$;
 - $IdGroup(R^*) = [12, 3]$, $R^* \cong A_4$ *ma* $n(R^*) = 2$;
 - $IdGroup(R^*) = [12, 5]$, $R^* \cong C_6 \times C_2$ *ma* $n(R^*) = 2$;

- $IdGroup(G) = [16, 3]$, $G \cong (C_4 \times C_2) \rtimes C_2$, $n(G) = 37$:
 - $IdGroup(R^*) = [8, 2]$, $R^* \cong C_4 \times C_2$ *ma* $n(R^*) = 14$;
 - $IdGroup(R^*) = [8, 3]$, $R^* \cong D_8$ *ma* $n(R^*) = 17$;
 - $IdGroup(R^*) = [8, 5]$, $R^* \cong C_2 \times C_2 \times C_2$ *ma* $n(R^*) = 6$;
- $IdGroup(G) = [16, 4]$, $G \cong C_4 \rtimes C_4$, $n(G) = 24$:
 - $IdGroup(R^*) = [8, 2]$, $R^* \cong C_4 \times C_2$ *ma* $n(R^*) = 7$;
 - $IdGroup(R^*) = [8, 3]$, $R^* \cong D_8$ *ma* $n(R^*) = 10$;
 - $IdGroup(R^*) = [8, 5]$, $R^* \cong C_2 \times C_2 \times C_2$ *ma* $n(R^*) = 7$;
- $IdGroup(G) = [16, 5]$, $G \cong C_8 \times C_2$, $n(G) = 33$:
 - $IdGroup(R^*) = [8, 2]$, $R^* \cong C_4 \times C_2$ *ma* $n(R^*) = 8$;
 - $IdGroup(R^*) = [8, 3]$, $R^* \cong D_8$ *ma* $n(R^*) = 16$;
 - $IdGroup(R^*) = [8, 5]$, $R^* \cong C_2 \times C_2 \times C_2$ *ma* $n(R^*) = 9$;
- $IdGroup(G) = [16, 6]$, $G \cong C_8 \rtimes C_2$, $n(G) = 33$:
 - $IdGroup(R^*) = [8, 2]$, $R^* \cong C_4 \times C_2$ *ma* $n(R^*) = 8$;
 - $IdGroup(R^*) = [8, 3]$, $R^* \cong D_8$ *ma* $n(R^*) = 17$;
 - $IdGroup(R^*) = [8, 5]$, $R^* \cong C_2 \times C_2 \times C_2$ *ma* $n(R^*) = 8$;
- $IdGroup(G) = [16, 10]$, $G \cong C_4 \times C_2 \times C_2$, $n(G) = 251$:
 - $IdGroup(R^*) = [8, 2]$, $R^* \cong C_4 \times C_2$ *ma* $n(R^*) = 96$;
 - $IdGroup(R^*) = [8, 3]$, $R^* \cong D_8$ *ma* $n(R^*) = 90$;
 - $IdGroup(R^*) = [8, 4]$, $R^* \cong Q_8$ *ma* $n(R^*) = 24$;
 - $IdGroup(R^*) = [8, 5]$, $R^* \cong C_2 \times C_2 \times C_2$ *ma* $n(R^*) = 41$;
- $IdGroup(G) = [16, 12]$, $G \cong C_2 \times Q_8$, $n(G) = 2$, $IdGroup(R^*) = [12, 3]$, $R^* \cong A_4$ *ma* $n(R^*) = 2$;

- $IdGroup(G) = [16, 14]$, $G \cong C_2 \times C_2 \times C_2 \times C_2$, $n(G) = 229$:
 - $IdGroup(R^*) = [8, 2]$, $R^* \cong C_4 \times C_2$ *ma* $n(R^*) = 96$;
 - $IdGroup(R^*) = [8, 3]$, $R^* \cong D_8$ *ma* $n(R^*) = 90$;
 - $IdGroup(R^*) = [8, 4]$, $R^* \cong Q_8$ *ma* $n(R^*) = 24$;
 - $IdGroup(R^*) = [8, 5]$, $R^* \cong C_2 \times C_2 \times C_2$ *ma* $n(R^*) = 41$;
 - $IdGroup(R^*) = [12, 3]$, $R^* \cong A_4$ *ma* $n(R^*) = 5$;
 - $IdGroup(R^*) = [12, 5]$, $R^* \cong C_6 \times C_2$ *ma* $n(R^*) = 2$;
- $IdGroup(G) = [25, 1]$, $G \cong C_{25}$, $n(G) = 1$, $IdGroup(R^*) = [20, 2]$, $R^* \cong C_{20}$ *ma* $n(R^*) = 1$;
- $IdGroup(G) = [25, 2]$, $G \cong C_5 \times C_5$, $n(G) = 5$:
 - $IdGroup(R^*) = [20, 1]$, $R^* \cong C_5 \rtimes C_4$ *ma* $n(R^*) = 1$;
 - $IdGroup(R^*) = [20, 2]$, $R^* \cong C_{20}$ *ma* $n(R^*) = 1$;
 - $IdGroup(R^*) = [20, 3]$, $R^* \cong C_5 \rtimes C_4$ *ma* $n(R^*) = 3$;
- $IdGroup(G) = [27, 1]$, $G \cong C_{27}$, $n(G) = 1$, $IdGroup(R^*) = [18, 2]$, $R^* \cong C_{18}$ *ma* $n(R^*) = 1$;
- $IdGroup(G) = [27, 2]$, $G \cong C_9 \times C_3$, $n(G) = 13$:
 - $IdGroup(R^*) = [18, 3]$, $R^* \cong C_3 \times S_3$ *ma* $n(R^*) = 4$;
 - $IdGroup(R^*) = [18, 5]$, $R^* \cong C_6 \times C_3$ *ma* $n(R^*) = 9$;
- $IdGroup(G) = [27, 3]$, $G \cong (C_3 \times C_3) \rtimes C_3$, $n(G) = 4$, $IdGroup(R^*) = [18, 3]$, $R^* \cong C_3 \times S_3$ *ma* $n(R^*) = 4$;
- $IdGroup(G) = [27, 4]$, $G \cong C_9 \rtimes C_3$, $n(G) = 4$, $IdGroup(R^*) = [18, 3]$, $R^* \cong C_3 \times S_3$ *ma* $n(R^*) = 4$;
- $IdGroup(G) = [27, 5]$, $G \cong C_3 \times C_3 \times C_3$, $n(G) = 12$:

- $IdGroup(R^*) = [18, 3]$, $R^* \cong C_3 \times S_3$ та $n(R^*) = 3$;
- $IdGroup(R^*) = [18, 4]$, $R^* \cong (C_3 \times C_3) \rtimes C_2$ та $n(R^*) = 4$;
- $IdGroup(R^*) = [18, 5]$, $R^* \cong C_6 \times C_3$ та $n(R^*) = 5$.

7.5.1. Локальні майже-кільця порядку 32

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

Зауважимо, що з 51 неізоморфної групи порядку 32 тільки 19 є адитивними групами локальних майже-кільць.

Теорема 7.9. *Нехай R — локальне майже-кільце порядку 32. Тоді група R^+ та її підгрупа L є наступними:*

- $IdGroup(G) = [32, 1]$, $G \cong C_{32}$ та $IdGroup(L) = [16, 1]$, $L \cong C_{16}$;
- $IdGroup(G) = [32, 2]$, $G \cong (C_4 \times C_2) \rtimes C_4$ та $IdGroup(L) = [16, 10]$, $L \cong C_4 \times C_2 \times C_2$;
- $IdGroup(G) = [32, 3]$, $G \cong C_8 \times C_4$ та $IdGroup(L) = [16, 2]$, $L \cong C_4 \times C_4$;
- $IdGroup(G) = [32, 4]$, $G \cong C_8 \rtimes C_4$ та $IdGroup(L) = [16, 2]$, $L \cong C_4 \times C_4$;
- $IdGroup(G) = [32, 5]$, $G \cong (C_8 \times C_2) \rtimes C_2$ та $IdGroup(L) = [16, 10]$, $L \cong C_4 \times C_2 \times C_2$;
- $IdGroup(G) = [32, 6]$, $G \cong ((C_4 \times C_2) \rtimes C_2) \rtimes C_2$ та $IdGroup(L) = [16, 11]$, $L \cong C_2 \times D_8$;

- $IdGroup(G) = [32, 7], G \cong (C_8 \rtimes C_2) \rtimes C_2$ *ma* $IdGroup(L) = [16, 11], L \cong C_2 \times D_8$;
- $IdGroup(G) = [32, 8], G \cong C_2 \cdot ((C_4 \times C_2) \rtimes C_2)$ *ma* $IdGroup(L) = [16, 12], L \cong C_2 \times Q_8$;
- $IdGroup(G) = [32, 12], G \cong C_4 \rtimes C_8$ *ma* $IdGroup(L) = [16, 2], L \cong C_4 \times C_4$;
- $IdGroup(G) = [32, 16], G \cong C_{16} \times C_2$ *ma* $IdGroup(L) = [16, 5], L \cong C_8 \times C_2$;
- $IdGroup(G) = [32, 17], G \cong C_{16} \rtimes C_2$ *ma* $IdGroup(L) = [16, 5], L \cong C_8 \times C_2$;
- $IdGroup(G) = [32, 21], G \cong C_4 \times C_4 \times C_2$ *ma* $IdGroup(L) = [16, 10], L \cong C_4 \times C_2 \times C_2$;
- $IdGroup(G) = [32, 22], G \cong C_2 \times ((C_4 \times C_2) \rtimes C_2)$ *ma* $IdGroup(L) = [16, 14], L \cong C_2 \times C_2 \times C_2 \times C_2$;
- $IdGroup(G) = [32, 23], G \cong C_2 \times (C_4 \rtimes C_4)$ *ma* $IdGroup(L) = [16, 10], L \cong C_4 \times C_2 \times C_2$;
- $IdGroup(G) = [32, 24], G \cong (C_4 \times C_4) \rtimes C_2$ *ma* $IdGroup(L) = [16, 10], L \cong C_4 \times C_2 \times C_2$;
- $IdGroup(G) = [32, 36], G \cong C_8 \times C_2 \times C_2$ *ma* $IdGroup(L) = [16, 10], L \cong C_4 \times C_2 \times C_2$;
- $IdGroup(G) = [32, 37], G \cong C_2 \times (C_8 \rtimes C_2)$ *ma* $IdGroup(L) = [16, 10], L \cong C_4 \times C_2 \times C_2$;
- $IdGroup(G) = [32, 45], G \cong C_4 \times C_2 \times C_2 \times C_2$ *ma* $IdGroup(L) = [16, 14], L \cong C_2 \times C_2 \times C_2 \times C_2$;

- $IdGroup(G) = [32, 51]$, $G \cong C_2 \times C_2 \times C_2 \times C_2 \times C_2$ та $IdGroup(L) = [16, 14]$, $L \cong C_2 \times C_2 \times C_2 \times C_2$.

Наступна таблиця містить кількість неізоморфних локальних майже-кілець порядку 32 з заданими адитивними та мультиплікативними групами.

Теорема 7.10. *Нехай $n(G)$ — кількість всіх неізоморфних локальних майже-кілець R порядку 32, адитивна група R^+ яких ізоморфна групі G . Якщо $n(R^*)$ є кількість цих майже-кілець, для яких $IdGroup(R^*)$ є фіксованим, то наступне має місце.*

- $IdGroup(G) = [32, 1]$, $G \cong C_{32}$, $n(G) = 1$, $IdGroup(R^*) = [16, 5]$, $R^* \cong C_8 \times C_2$ та $n(R^*) = 1$.
- $IdGroup(G) = [32, 2]$, $G \cong (C_4 \times C_2) \rtimes C_4$, $n(G) = 1397$:
 - $IdGroup(R^*) = [16, 3]$, $R^* \cong (C_4 \times C_2) \rtimes C_2$ та $n(R^*) = 369$;
 - $IdGroup(R^*) = [16, 10]$, $R^* \cong C_4 \times C_2 \times C_2$ та $n(R^*) = 198$;
 - $IdGroup(R^*) = [16, 11]$, $R^* \cong C_2 \times D_8$ та $n(R^*) = 764$;
 - $IdGroup(R^*) = [16, 14]$, $R^* \cong C_2 \times C_2 \times C_2 \times C_2$ та $n(R^*) = 66$.
- $IdGroup(G) = [32, 3]$, $G \cong C_8 \times C_4$, $n(G) = 880$:
 - $IdGroup(R^*) = [16, 3]$, $R^* \cong (C_4 \times C_2) \rtimes C_2$ та $n(R^*) = 208$;
 - $IdGroup(R^*) = [16, 10]$, $R^* \cong C_4 \times C_2 \times C_2$ та $n(R^*) = 128$;
 - $IdGroup(R^*) = [16, 11]$, $R^* \cong C_2 \times D_8$ та $n(R^*) = 489$;
 - $IdGroup(R^*) = [16, 14]$, $R^* \cong C_2 \times C_2 \times C_2 \times C_2$ та $n(R^*) = 55$.
- $IdGroup(G) = [32, 4]$, $G \cong C_8 \rtimes C_4$, $n(G) = 798$:
 - $IdGroup(R^*) = [16, 3]$, $R^* \cong (C_4 \times C_2) \rtimes C_2$ та $n(R^*) = 238$;

- $IdGroup(R^*) = [16, 10]$, $R^* \cong C_4 \times C_2 \times C_2$ *ma* $n(R^*) = 100$;
- $IdGroup(R^*) = [16, 11]$, $R^* \cong C_2 \times D_8$ *ma* $n(R^*) = 424$;
- $IdGroup(R^*) = [16, 14]$, $R^* \cong C_2 \times C_2 \times C_2 \times C_2$ *ma* $n(R^*) = 36$.
- $IdGroup(G) = [32, 5]$, $G \cong (C_8 \times C_2) \rtimes C_2$, $n(G) = 1945$:
 - $IdGroup(R^*) = [16, 3]$, $R^* \cong (C_4 \times C_2) \rtimes C_2$ *ma* $n(R^*) = 548$;
 - $IdGroup(R^*) = [16, 10]$, $R^* \cong C_4 \times C_2 \times C_2$ *ma* $n(R^*) = 232$;
 - $IdGroup(R^*) = [16, 11]$, $R^* \cong C_2 \times D_8$ *ma* $n(R^*) = 1077$;
 - $IdGroup(R^*) = [16, 14]$, $R^* \cong C_2 \times C_2 \times C_2 \times C_2$ *ma* $n(R^*) = 88$.
- $IdGroup(G) = [32, 6]$, $G \cong ((C_4 \times C_2) \rtimes C_2) \rtimes C_2$, $n(G) = 433$:
 - $IdGroup(R^*) = [16, 3]$, $R^* \cong (C_4 \times C_2) \rtimes C_2$ *ma* $n(R^*) = 64$;
 - $IdGroup(R^*) = [16, 11]$, $R^* \cong C_2 \times D_8$ *ma* $n(R^*) = 225$;
 - $IdGroup(R^*) = [16, 13]$, $R^* \cong (C_4 \times C_2) \rtimes C_2$ *ma* $n(R^*) = 144$.
- $IdGroup(G) = [32, 7]$, $G \cong (C_8 \rtimes C_2) \rtimes C_2$, $n(G) = 225$:
 - $IdGroup(R^*) = [16, 3]$, $R^* \cong (C_4 \times C_2) \rtimes C_2$ *ma* $n(R^*) = 32$;
 - $IdGroup(R^*) = [16, 11]$, $R^* \cong C_2 \times D_8$ *ma* $n(R^*) = 121$;
 - $IdGroup(R^*) = [16, 13]$, $R^* \cong (C_4 \times C_2) \rtimes C_2$ *ma* $n(R^*) = 72$.
- $IdGroup(G) = [32, 8]$, $G \cong C_2 \cdot ((C_4 \times C_2) \rtimes C_2)$, $n(G) = 208$:
 - $IdGroup(R^*) = [16, 3]$, $R^* \cong (C_4 \times C_2) \rtimes C_2$ *ma* $n(R^*) = 32$;
 - $IdGroup(R^*) = [16, 11]$, $R^* \cong C_2 \times D_8$ *ma* $n(R^*) = 104$;
 - $IdGroup(R^*) = [16, 13]$, $R^* \cong (C_4 \times C_2) \rtimes C_2$ *ma* $n(R^*) = 72$.
- $IdGroup(G) = [32, 12]$, $G \cong C_4 \rtimes C_8$, $n(G) = 2406$:
 - $IdGroup(R^*) = [16, 3]$, $R^* \cong (C_4 \times C_2) \rtimes C_2$ *ma* $n(R^*) = 624$;

- $IdGroup(R^*) = [16, 10]$, $R^* \cong C_4 \times C_2 \times C_2$ *ma* $n(R^*) = 312$;
- $IdGroup(R^*) = [16, 11]$, $R^* \cong C_2 \times D_8$ *ma* $n(R^*) = 1350$;
- $IdGroup(R^*) = [16, 14]$, $R^* \cong C_2 \times C_2 \times C_2 \times C_2$ *ma* $n(R^*) = 120$.
- $IdGroup(G) = [32, 16]$, $G \cong C_{16} \times C_2$, $n(G) = 129$:
 - $IdGroup(R^*) = [16, 10]$, $R^* \cong C_4 \times C_2 \times C_2$ *ma* $n(R^*) = 33$;
 - $IdGroup(R^*) = [16, 11]$, $R^* \cong C_2 \times D_8$ *ma* $n(R^*) = 16$;
 - $IdGroup(R^*) = [16, 12]$, $R^* \cong C_2 \times Q_8$ *ma* $n(R^*) = 16$;
 - $IdGroup(R^*) = [16, 13]$, $R^* \cong (C_4 \times C_2) \rtimes C_2$ *ma* $n(R^*) = 64$.
- $IdGroup(G) = [32, 17]$, $G \cong C_{16} \rtimes C_2$, $n(G) = 129$:
 - $IdGroup(R^*) = [16, 10]$, $R^* \cong C_4 \times C_2 \times C_2$ *ma* $n(R^*) = 32$;
 - $IdGroup(R^*) = [16, 11]$, $R^* \cong C_2 \times D_8$ *ma* $n(R^*) = 16$;
 - $IdGroup(R^*) = [16, 12]$, $R^* \cong C_2 \times Q_8$ *ma* $n(R^*) = 16$;
 - $IdGroup(R^*) = [16, 13]$, $R^* \cong (C_4 \times C_2) \rtimes C_2$ *ma* $n(R^*) = 65$.
- $IdGroup(G) = [32, 21]$, $G \cong C_4 \times C_4 \times C_2$, $n(G) = 135558$:
 - $IdGroup(R^*) = [16, 2]$, $R^* \cong C_4 \times C_4$ *ma* $n(R^*) = 256$;
 - $IdGroup(R^*) = [16, 3]$, $R^* \cong (C_4 \times C_2) \rtimes C_2$ *ma* $n(R^*) = 634$;
 - $IdGroup(R^*) = [16, 4]$, $R^* \cong C_4 \rtimes C_4$ *ma* $n(R^*) = 136$;
 - $IdGroup(R^*) = [16, 5]$, $R^* \cong C_8 \times C_2$ *ma* $n(R^*) = 4$;
 - $IdGroup(R^*) = [16, 6]$, $R^* \cong C_8 \rtimes C_2$ *ma* $n(R^*) = 2$;
 - $IdGroup(R^*) = [16, 10]$, $R^* \cong C_4 \times C_2 \times C_2$ *ma* $n(R^*) = 13630$;
 - $IdGroup(R^*) = [16, 11]$, $R^* \cong C_2 \times D_8$ *ma* $n(R^*) = 62910$;
 - $IdGroup(R^*) = [16, 12]$, $R^* \cong C_2 \times Q_8$ *ma* $n(R^*) = 4368$;
 - $IdGroup(R^*) = [16, 13]$, $R^* \cong (C_4 \times C_2) \rtimes C_2$ *ma* $n(R^*) = 49152$;

- $IdGroup(R^*) = [16, 14], R^* \cong C_2 \times C_2 \times C_2 \times C_2$ *ma* $n(R^*) = 4466$.
- $IdGroup(G) = [32, 22], G \cong C_2 \times ((C_4 \times C_2) \rtimes C_2), n(G) = 149374$:
 - $IdGroup(R^*) = [16, 2], R^* \cong C_4 \times C_4$ *ma* $n(R^*) = 1024$;
 - $IdGroup(R^*) = [16, 3], R^* \cong (C_4 \times C_2) \rtimes C_2$ *ma* $n(R^*) = 5936$;
 - $IdGroup(R^*) = [16, 4], R^* \cong C_4 \rtimes C_4$ *ma* $n(R^*) = 3120$;
 - $IdGroup(R^*) = [16, 5], R^* \cong C_8 \times C_2$ *ma* $n(R^*) = 20$;
 - $IdGroup(R^*) = [16, 6], R^* \cong C_8 \rtimes C_2$ *ma* $n(R^*) = 30$;
 - $IdGroup(R^*) = [16, 10], R^* \cong C_4 \times C_2 \times C_2$ *ma* $n(R^*) = 14457$;
 - $IdGroup(R^*) = [16, 11], R^* \cong C_2 \times D_8$ *ma* $n(R^*) = 66579$;
 - $IdGroup(R^*) = [16, 12], R^* \cong C_2 \times Q_8$ *ma* $n(R^*) = 4368$;
 - $IdGroup(R^*) = [16, 13], R^* \cong (C_4 \times C_2) \rtimes C_2$ *ma* $n(R^*) = 49368$;
 - $IdGroup(R^*) = [16, 14], R^* \cong C_2 \times C_2 \times C_2 \times C_2$ *ma* $n(R^*) = 4472$.
- $IdGroup(G) = [32, 23], G \cong C_2 \times (C_4 \rtimes C_4), n(G) = 157905$:
 - $IdGroup(R^*) = [16, 3], R^* \cong (C_4 \times C_2) \rtimes C_2$ *ma* $n(R^*) = 458$;
 - $IdGroup(R^*) = [16, 4], R^* \cong C_4 \rtimes C_4$ *ma* $n(R^*) = 4$;
 - $IdGroup(R^*) = [16, 10], R^* \cong C_4 \times C_2 \times C_2$ *ma* $n(R^*) = 13414$;
 - $IdGroup(R^*) = [16, 11], R^* \cong C_2 \times D_8$ *ma* $n(R^*) = 85208$;
 - $IdGroup(R^*) = [16, 12], R^* \cong C_2 \times Q_8$ *ma* $n(R^*) = 4416$;
 - $IdGroup(R^*) = [16, 13], R^* \cong (C_4 \times C_2) \rtimes C_2$ *ma* $n(R^*) = 49920$;
 - $IdGroup(R^*) = [16, 14], R^* \cong C_2 \times C_2 \times C_2 \times C_2$ *ma* $n(R^*) = 4485$.
- $IdGroup(G) = [32, 24], G \cong (C_4 \times C_4) \rtimes C_2, n(G) = 262544$:
 - $IdGroup(R^*) = [16, 10], R^* \cong C_4 \times C_2 \times C_2$ *ma* $n(R^*) = 24576$;
 - $IdGroup(R^*) = [16, 11], R^* \cong C_2 \times D_8$ *ma* $n(R^*) = 123080$;

- $IdGroup(R^*) = [16, 12]$, $R^* \cong C_2 \times Q_8$ $ma\ n(R^*) = 8192$;
- $IdGroup(R^*) = [16, 13]$, $R^* \cong (C_4 \times C_2) \rtimes C_2$ $ma\ n(R^*) = 98504$;
- $IdGroup(R^*) = [16, 14]$, $R^* \cong C_2 \times C_2 \times C_2 \times C_2$ $ma\ n(R^*) = 8192$.
- $IdGroup(G) = [32, 36]$, $G \cong C_8 \times C_2 \times C_2$, $n(G) = 177175$:
 - $IdGroup(R^*) = [16, 3]$, $R^* \cong (C_4 \times C_2) \rtimes C_2$ $ma\ n(R^*) = 448$;
 - $IdGroup(R^*) = [16, 10]$, $R^* \cong C_4 \times C_2 \times C_2$ $ma\ n(R^*) = 16770$;
 - $IdGroup(R^*) = [16, 11]$, $R^* \cong C_2 \times D_8$ $ma\ n(R^*) = 83244$;
 - $IdGroup(R^*) = [16, 12]$, $R^* \cong C_2 \times Q_8$ $ma\ n(R^*) = 5472$;
 - $IdGroup(R^*) = [16, 13]$, $R^* \cong (C_4 \times C_2) \rtimes C_2$ $ma\ n(R^*) = 65536$;
 - $IdGroup(R^*) = [16, 14]$, $R^* \cong C_2 \times C_2 \times C_2 \times C_2$ $ma\ n(R^*) = 5705$.
- $IdGroup(G) = [32, 37]$, $G \cong C_2 \times (C_8 \rtimes C_2)$, $n(G) = 527419$:
 - $IdGroup(R^*) = [16, 3]$, $R^* \cong (C_4 \times C_2) \rtimes C_2$ $ma\ n(R^*) = 496$;
 - $IdGroup(R^*) = [16, 10]$, $R^* \cong C_4 \times C_2 \times C_2$ $ma\ n(R^*) = 49514$;
 - $IdGroup(R^*) = [16, 11]$, $R^* \cong C_2 \times D_8$ $ma\ n(R^*) = 247431$;
 - $IdGroup(R^*) = [16, 12]$, $R^* \cong C_2 \times Q_8$ $ma\ n(R^*) = 16384$;
 - $IdGroup(R^*) = [16, 13]$, $R^* \cong (C_4 \times C_2) \rtimes C_2$ $ma\ n(R^*) = 197008$;
 - $IdGroup(R^*) = [16, 14]$, $R^* \cong C_2 \times C_2 \times C_2 \times C_2$ $ma\ n(R^*) = 16586$.
- $IdGroup(G) = [32, 45]$, $G \cong C_4 \times C_2 \times C_2 \times C_2$, $n(G) > 6684533$:
 - $IdGroup(R^*) = [16, 2]$, $R^* \cong C_4 \times C_4$ $ma\ n(R^*) = 16435$;
 - $IdGroup(R^*) = [16, 3]$, $R^* \cong (C_4 \times C_2) \rtimes C_2$ $ma\ n(R^*) = 40447$;
 - $IdGroup(R^*) = [16, 4]$, $R^* \cong C_4 \rtimes C_4$ $ma\ n(R^*) = 47904$;
 - $IdGroup(R^*) = [16, 5]$, $R^* \cong C_8 \times C_2$ $ma\ n(R^*) = 24$;

- $IdGroup(R^*) = [16, 6], R^* \cong C_8 \rtimes C_2$ *ma* $n(R^*) = 32$;
 - $IdGroup(R^*) = [16, 8], R^* \cong QD_{16}$ *ma* $n(R^*) = 14$;
 - $IdGroup(R^*) = [16, 9], R^* \cong Q_{16}$ *ma* $n(R^*) = 14$;
 - $IdGroup(R^*) = [16, 10], R^* \cong C_4 \times C_2 \times C_2$ *ma* $n(R^*) = 741652$;
 - $IdGroup(R^*) = [16, 11], R^* \cong C_2 \times D_8$ *ma* $n(R^*) = 2190035$;
 - $IdGroup(R^*) = [16, 12], R^* \cong C_2 \times Q_8$ *ma* $n(R^*) = 710359$;
 - $IdGroup(R^*) = [16, 13], R^* \cong (C_4 \times C_2) \rtimes C_2$ *ma* $n(R^*) = 2847717$;
 - $IdGroup(R^*) = [16, 14], R^* \cong C_2 \times C_2 \times C_2 \times C_2$ *ma* $n(R^*) > 89900$.
- $IdGroup(G) = [32, 51], G \cong C_2 \times C_2 \times C_2 \times C_2 \times C_2, n(G) > 7007053$:
- $IdGroup(R^*) = [16, 2], R^* \cong C_4 \times C_4$ *ma* $n(R^*) = 5983$;
 - $IdGroup(R^*) = [16, 3], R^* \cong (C_4 \times C_2) \rtimes C_2$ *ma* $n(R^*) = 23205$;
 - $IdGroup(R^*) = [16, 4], R^* \cong C_4 \rtimes C_4$ *ma* $n(R^*) = 17100$;
 - $IdGroup(R^*) = [16, 5], R^* \cong C_8 \times C_2$ *ma* $n(R^*) = 24$;
 - $IdGroup(R^*) = [16, 6], R^* \cong C_8 \rtimes C_2$ *ma* $n(R^*) = 32$;
 - $IdGroup(R^*) = [16, 8], R^* \cong QD_{16}$ *ma* $n(R^*) = 14$;
 - $IdGroup(R^*) = [16, 9], R^* \cong Q_{16}$ *ma* $n(R^*) = 14$;
 - $IdGroup(R^*) = [16, 10], R^* \cong C_4 \times C_2 \times C_2$ *ma* $n(R^*) = 789167$;
 - $IdGroup(R^*) = [16, 11], R^* \cong C_2 \times D_8$ *ma* $n(R^*) = 2566765$;
 - $IdGroup(R^*) = [16, 12], R^* \cong C_2 \times Q_8$ *ma* $n(R^*) = 703803$;
 - $IdGroup(R^*) = [16, 13], R^* \cong (C_4 \times C_2) \rtimes C_2$ *ma* $n(R^*) = 2808419$;
 - $IdGroup(R^*) = [16, 14], R^* \cong C_2 \times C_2 \times C_2 \times C_2$ *ma* $n(R^*) > 92527$.

7.5.2. Локальні майже-кілець порядку 128

У роботах [108] і [75] побудовано і досліджено локальні майже-кілець порядку $2^7 = 128$ на 2-породжених групах засобами комп'ютерної алгебри GAP.

Існує 2328 неізоморфних груп порядку $128 = 2^7$, з яких 162 є 2-породженими групами: 5 груп мають експоненту 64 і лише 2 з цих груп є адитивними групами локальних майже-кілець, 18 груп мають експоненту 32 і лише 6 з цих груп є адитивними групами локальних майже-кілець, 65 груп мають експоненту 16 і лише 16 з цих груп є адитивними групами локальних майже-кілець, 72 групи мають експоненту 8 (невідомо кількість груп, які є адитивними групами локальних наближених кілець), а групи 2 мають експоненту 4 і обидві ці групи є адитивними групами локальних майже-кілець.

Теорема 7.11. *Наступні 2-породжені групи G експоненти 4 і тільки вони є адитивними групами нуль-симетричних локальних майже-кілець порядку 128:*

- $IdGroup(G) = [128, 36]$, $G \cong (C_2 \times ((C_4 \times C_2) \rtimes C_2)) \rtimes C_4$ та $n(G) > 80384$;
- $IdGroup(G) = [128, 125]$, $G \cong (C_4 \times C_4 \times C_2) \rtimes C_4$ та $n(G) > 35040$.

Лема 7.12. *Наступні 2-породжені групи G експоненти 8 є адитивними групами нуль-симетричних локальних майже-кілець порядку 128:*

- $IdGroup(G) = [128, 2]$, $G \cong ((C_8 \times C_2) \rtimes C_4) \rtimes C_2$ та $n(G) > 41184$;

- $IdGroup(G) = [128, 4]$, $G \cong (C_2 \times Q_8) \rtimes C_8$ *ma* $n(G) > 103424$;
- $IdGroup(G) = [128, 5]$, $G \cong (C_8 \times C_2) \rtimes C_8$ *ma* $n(G) > 1536$;
- $IdGroup(G) = [128, 6]$, $G \cong (C_8 \times C_4) \rtimes C_4$ *ma* $n(G) > 73728$;
- $IdGroup(G) = [128, 7]$, $G \cong (C_8 \times C_2) \rtimes C_8$ *ma* $n(G) > 4160$;
- $IdGroup(G) = [128, 8]$, $G \cong (C_4 \rtimes C_8) \rtimes C_4$ *ma* $n(G) > 10240$;
- $IdGroup(G) = [128, 12]$, $G \cong ((C_8 \times C_2) \rtimes C_2) \rtimes C_4$ *ma* $n(G) > 1336$;
- $IdGroup(G) = [128, 13]$, $G \cong (C_8 \times C_2) \rtimes C_8$ *ma* $n(G) > 33928$;
- $IdGroup(G) = [128, 27]$, $G \cong (C_8 \rtimes C_4) \rtimes C_4$ *ma* $n(G) > 106240$;
- $IdGroup(G) = [128, 38]$, $G \cong ((C_8 \times C_2) \rtimes C_2) \rtimes C_4$ *ma* $n(G) > 80384$;
- $IdGroup(G) = [128, 48]$, $G \cong (((C_8 \times C_2) \rtimes C_2) \rtimes C_2) \rtimes C_2$ *ma* $n(G) > 194080$;
- $IdGroup(G) = [128, 49]$, $G \cong (C_4 \times C_2 \times C_2) \rtimes C_8$ *ma* $n(G) > 191520$;
- $IdGroup(G) = [128, 50]$, $G \cong ((C_4 \times C_2) \rtimes C_8) \rtimes C_2$ *ma* $n(G) > 16992$;
- $IdGroup(G) = [128, 51]$, $G \cong (C_2 \times Q_8) \rtimes C_8$ *ma* $n(G) > 16992$;
- $IdGroup(G) = [128, 56]$, $G \cong (C_4 \times C_4) \rtimes C_8$ *ma* $n(G) > 254208$;
- $IdGroup(G) = [128, 57]$, $G \cong (C_4 \times C_4) \rtimes C_8$ *ma* $n(G) > 127488$.

Питання 1. Чи є наступні 2-породжені групи G експоненти 8 адитивними групами нуль-симетричних локальних майже-кілець порядку 128?

- $IdGroup(G) = [128, 9]$, $G \cong (C_8 \times C_2) \rtimes C_8$;

- $IdGroup(G) = [128, 28]$, $G \cong (C_8 \times C_2) \rtimes C_8$;
- $IdGroup(G) = [128, 126]$, $G \cong (C_2 \cdot ((C_4 \times C_2) \rtimes C_2) = (C_2 \times C_2) \cdot (C_4 \times C_2)) \rtimes C_4$.

Теорема 7.13. *Тільки наступні групи G порядку 128 і експоненти 16 є адитивними групами нуль-симетричних локальних майже-кілець:*

- $IdGroup(G) = [128, 42]$, $G \cong C_{16} \times C_8$ та $n(G) > 134754$;
- $IdGroup(G) = [128, 43]$, $G \cong C_{16} \rtimes C_8$ та $n(G) > 133866$;
- $IdGroup(G) = [128, 44]$, $G \cong C_8 \rtimes C_{16}$ та $n(G) > 145648$;
- $IdGroup(G) = [128, 46]$, $G \cong ((C_{16} \times C_2) \rtimes C_2) \rtimes C_2$ та $n(G) > 24704$;
- $IdGroup(G) = [128, 47]$, $G \cong ((C_{16} \times C_2) \rtimes C_2) \rtimes C_2$ та $n(G) = 252928$;
- $IdGroup(G) = [128, 52]$, $G \cong ((C_{16} \rtimes C_2) \rtimes C_2) \rtimes C_2$ та $n(G) > 115840$;
- $IdGroup(G) = [128, 53]$, $G \cong ((C_{16} \rtimes C_2) \rtimes C_2) \rtimes C_2$ та $n(G) > 277248$;
- $IdGroup(G) = [128, 54]$, $G \cong (C_4 \times C_2) \rtimes C_{16}$ та $n(G) > 82944$;
- $IdGroup(G) = [128, 55]$, $G \cong (C_4 \times C_2) \cdot ((C_4 \times C_2) \rtimes C_2) = (C_4 \times C_2) \cdot (C_8 \times C_2)$ та $n(G) = 640$;
- $IdGroup(G) = [128, 59]$, $G \cong C_4 \cdot ((C_2 \times C_2 \times C_2) \rtimes C_4) = (C_4 \times C_2) \cdot (C_8 \times C_2)$ та $n(G) > 13056$;
- $IdGroup(G) = [128, 99]$, $G \cong C_8 \rtimes C_{16}$ та $n(G) > 29248$;

- $IdGroup(G) = [128, 102]$, $G \cong C_8 \rtimes C_{16}$ та $n(G) > 5376$;
- $IdGroup(G) = [128, 106]$, $G \cong (C_{16} \times C_2) \rtimes C_4$ та $n(G) > 2808$;
- $IdGroup(G) = [128, 107]$, $G \cong (C_{16} \times C_2) \rtimes C_4$ та $n(G) > 16460$;
- $IdGroup(G) = [128, 108]$, $G \cong (C_{16} \rtimes C_2) \rtimes C_4$ та $n(G) > 1344$;
- $IdGroup(G) = [128, 109]$, $G \cong (C_{16} \rtimes C_2) \rtimes C_4$ та $n(G) > 2344$.

Теорема 7.14. Існують 389976 нуль-симетричні локальні майже-кільця на 2-породжених адитивних групах G експоненти 32 порядку 128:

- $IdGroup(G) = [128, 128]$, $G \cong C_{32} \times C_4$ та $n(G) = 48968$;
- $IdGroup(G) = [128, 129]$, $G \cong C_{32} \rtimes C_4$ та $n(G) = 48968$;
- $IdGroup(G) = [128, 131]$, $G \cong (C_{32} \times C_2) \rtimes C_2$ та $n(G) = 144016$;
- $IdGroup(G) = [128, 132]$, $G \cong (C_{32} \rtimes C_2) \rtimes C_2$ та $n(G) = 23936$;
- $IdGroup(G) = [128, 153]$, $G \cong C_4 \rtimes C_{32}$ та $n(G) >$;
- $IdGroup(G) = [128, 154]$, $G \cong C_{16}.D_8 = C_4.(C_{16} \times C_2)$ та $n(G) = 5120$.

Теорема 7.15. Існують 1024 нуль-симетричні локальні майже-кільця на 2-породжених адитивних групах G експоненти 64 порядку 128:

- $IdGroup(G) = [128, 159]$, $G \cong C_{64} \times C_2$ та $n(G) = 512$;
- $IdGroup(G) = [128, 160]$, $G \cong C_{64} \rtimes C_2$ та $n(G) = 512$.

7.5.3. 2-Породжені групи експоненти 8 як адитивні групи нуль-симетричних локальних майже-кілець порядку 128

Існує 2328 неізоморфних груп порядку $128 = 2^7$, з яких 162 є 2-породженими групами (5 груп експоненти 64, 18 груп експоненти 32, 65 груп експоненти 16, 72 групи експоненти 8 та 2 групи експоненти 4).

Наступне твердження частково відповідає на питання 1.

Твердження 7.16. *Наступні 2-породжені групи G експоненти 8 є адитивними групами нуль-симетричних локальних майже-кілець порядку 128:*

- $IdGroup(G) = [128, 2]$, $G \cong ((C_8 \times C_2) \rtimes C_4) \rtimes C_2$ та $n(G) > 41184$.
- $IdGroup(G) = [128, 4]$, $G \cong (C_2 \times Q_8) \rtimes C_8$ та $n(G) > 103424$.
- $IdGroup(G) = [128, 5]$, $G \cong (C_8 \times C_2) \rtimes C_8$ та $n(G) > 1536$.
- $IdGroup(G) = [128, 6]$, $G \cong (C_8 \times C_4) \rtimes C_4$ та $n(G) > 73728$.
- $IdGroup(G) = [128, 7]$, $G \cong (C_8 \times C_2) \rtimes C_8$ та $n(G) > 4160$.
- $IdGroup(G) = [128, 8]$, $G \cong (C_4 \rtimes C_8) \rtimes C_4$ та $n(G) > 10240$.
- $IdGroup(G) = [128, 12]$, $G \cong ((C_8 \times C_2) \rtimes C_2) \rtimes C_4$ та $n(G) > 1336$.
- $IdGroup(G) = [128, 13]$, $(C_8 \times C_2) \rtimes C_8$ та $n(G) > 33928$.
- $IdGroup(G) = [128, 27]$, $(C_8 \rtimes C_4) \rtimes C_4$ та $n(G) > 106240$.
- $IdGroup(G) = [128, 38]$, $G \cong ((C_8 \times C_2) \rtimes C_2) \rtimes C_4$ та $n(G) > 80384$.
- $IdGroup(G) = [128, 48]$, $G \cong (((C_8 \times C_2) \rtimes C_2) \rtimes C_2) \rtimes C_2$ та $n(G) > 194080$.

- $IdGroup(G) = [128, 49]$, $G \cong (C_4 \times C_2 \times C_2) \rtimes C_8$ та $n(G) > 191520$.
- $IdGroup(G) = [128, 50]$, $G \cong ((C_4 \times C_2) \rtimes C_8) \rtimes C_2$ та $n(G) > 16992$.
- $IdGroup(G) = [128, 51]$, $G \cong (C_2 \times Q_8) \rtimes C_8$ та $n(G) > 16992$.
- $IdGroup(G) = [128, 56]$, $G \cong (C_4 \times C_4) \rtimes C_8$ та $n(G) > 254208$.
- $IdGroup(G) = [128, 57]$, $G \cong (C_4 \times C_4) \rtimes C_8$ та $n(G) > 127488$.
- $IdGroup(G) = [128, 126]$, $G \cong (C_2 \cdot ((C_4 \times C_2) \rtimes C_2) = (C_2 \times C_2) \cdot (C_4 \times C_2)) \rtimes C_4$ та $n(G) > 153488$.

Гіпотеза. Наступні 2-породжені групи G експоненти 8 і тільки вони є адитивними групами нуль-симетричних локальних майже-кілець порядку 128:

- групи з пропозиції 1;
- $IdGroup(G) = [128, 9]$, $G \cong (C_8 \times C_2) \rtimes C_8$;
- $IdGroup(G) = [128, 28]$, $G \cong (C_4 \rtimes C_8) \rtimes C_4$.

Алгоритм побудови скінченних локальних майже-кілець на адитивній групі $[128, 160]$ можна отримати з [125] за допомогою GAP, використовуючи пакет LocalNR та базу даних локальних майже-кілець на 2-породжених групах порядку 128.

Висновки до розділу 7

У даному розділі:

- описано побудову майже-кілець з одиницею;
- наведено деякі функції для локальних майже-кілець з пакету `LocalNR`, а саме:
 - `UnitsOfNearRing(R)` (вивід: список оборотних елементів майже-кілець, якщо R є майже-кілем з одиницею, інакше вивід має вигляд `Error, no units exist`),
 - `IsLocalNearRing(R)` (вивід: значення `true`, якщо R є локальним майже-кілем, інакше вивід має значення `false`.),
 - `IsLocalRing(R)` (вивід: значення `true`, якщо R є локальним кілем, інакше вивід має значення `false`),
 - `NearRingNonUnits(R)` (вивід: список необоротних елементів R .),
 - `NonUnitsAsAdditiveSubgroup(R)` (вивід: адитивна підгрупа необоротних елементів R);
- описано майже-кілець з одиницею пакету `SONATA` та ендоециклічні групи;
- проаналізовано локальні майже-кілець порядку 32;
- класифіковано деякі класи локальних майже-кілець порядку 128;
- знайдено 2-породжені ендоециклічні групи порядку 256 та експоненти 16, які не є адитивними групами локальних майже-кілець.

Основні результати даного розділу опубліковано у працях [11, 3, 1, 2, 6, 17, 18, 19, 20, 16] зі списку публікацій і, відповідно, [7, 11, 75, 100, 108, 109, 111, 112, 115, 123] зі списку використаних джерел, а також опубліковано у тезах конференцій [42, 38, 39, 31, 30, 29, 25, 22, 21] і, відповідно, [78, 81, 89–91, 99, 105, 116, 124].

Основні результати та висновки

Основні результати дисертації можна сформулювати таким чином:

- Описано майже-кілець з одиницею на групах порядку p^3 .
- Наведено необхідні умови існування майже-кілець з одиницею на абелевих групах порядку p^3 .
- Наведено необхідні умови існування майже-кілець з одиницею на неабелевих групах порядку p^3 .
- Описано локальні майже-кілець з адитивними групами порядку p^3 . Визначено формули множення для таких майже-кілець та описано функції, що їх задають.
- Наведено приклад локального майже-кілець з адитивною групою порядку p^3 .
- Дано оцінку нижньої межі кількості локальних майже-кілець на групах порядку p^3 .
- Наведено алгоритм побудови локального майже-кілець з елементарною абелевою адитивною групою порядку 5^3 , що реалізовано в системі комп'ютерної алгебри GAP.
- Проаналізовано існування та кількість неізоморфних локальних майже-кілець на групах порядку p^3 .
- Наведено деякі структурні результати стосовно груп порядку p^4 .
- Отримано необхідні умови існування майже-кілець з одиницею на групах порядку p^4 .

- Визначено формули множення для таких майже-кілець та описано функції, що їх задають.
- Описано локальні майже-кільця з адитивними групами порядку p^4 . Вказано формули множення для таких майже-кілець та описано функції, що їх задають.
- Наведено приклад локального майже-кільця порядку $5^4 = 625$.
- Дано алгоритм побудови локального майже-кільця з неабелевою адитивною адитивною групою порядку 5^4 , що реалізовано в системі комп'ютерної алгебри GAP.
- Наведено необхідні та достатні умови існування майже-кілець з одиницею на групах Міллера–Морено.
- Показано, що не існує майже-кілець з одиницею, адитивна група яких ізоморфна групі Шмідта.
- Описано прямі добутки p -груп Міллера–Морено та циклічних p -груп як адитивні групи майже-кілець з одиницею та локальних майже-кілець. Визначено формули множення для таких майже-кілець та описано функції, що їх задають.
- Описано побудова майже-кілець з одиницею.
- Наведено деякі функції для локальних майже-кілець з пакету LocalNR, а саме:
 - `UnitsOfNearRing(R)` (вивід: список оборотних елементів майже-кільця, якщо R є майже-кільцем з одиницею, інакше вивід має вигляд `Error, no units exist`),
 - `IsLocalNearRing(R)` (вивід: значення `true`, якщо R є локальним майже-кільцем, інакше вивід має значення `false`.),

- $\text{IsLocalRing}(R)$ (вивід: значення **true**, якщо R є локальним кільцем, інакше вивід має значення **false**),
 - $\text{NearRingNonUnits}(R)$ (вивід: список необоротних елементів R .),
 - $\text{NonUnitsAsAdditiveSubgroup}(R)$ (вивід: адитивна підгрупа необоротних елементів R).
- Описано майже-кільця з одиницею пакету SONATA та ендоеиклічні групи.
 - Проаналізовано локальні майже-кільця порядку 32.
 - Наведено часткову класифікацію локальних майже-кілець порядку 128.
 - Знайдено 2-породжені ендоеиклічні групи порядку 256 та експоненти 16, які не є адитивними групами локальних майже-кілець.

Список використаних джерел

1. Раєвська І. Ю. Локальні майже-кільця на неметациклічній p -групі Міллера–Морено, *Вісн. Київ. Ун-ту. Математика, Механіка*, **25** (2011), 43–45.
2. Раєвська І. Адитивні групи скінченних локальних майже-кілець, канд. дис... фіз.-мат. наук: 01.01.06; Інститут математики НАН України. — К., 2012. — 113 с.
3. Раєвська І. Про прямі добутки неметациклічних p -груп Міллера–Морено та циклічних p -груп як адитивні групи локальних майже-кілець, *Науковий вісник Ужгородського університету. Серія «Математика і інформатика»*, **46** (2025), № 1, 79–88.
4. Раєвська І. Про прямі добутки неметациклічних p -груп Міллера–Морено та циклічних p -груп як адитивні групи локальних майже-кілець, The conference of young scientists “Pidstryhach Readings — 2025”, Lviv, Ukraine, May 27–29, 2025,
http://iapmm.lviv.ua/chyt2025/abstracts/Raievska_Iryna.pdf
5. 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.
6. Раєвська І. Ю., Раєвська М. Ю. Адитивні групи скінченних майже-кілець з одиницею. Тези доповідей Міжнародної конференції молодих математиків, присвяченої 100-річчю з дня народження академі-

- ка НАН України Ю. О. Митропольського (1917–2008), 7–10 червня 2017 р., Ін-т математики НАН України, Київ, С. 20.
7. Раєвська І. Ю., Раєвська М. Ю. Скінченні локальні майже-кільця, *Могиллянський математичний журнал*, **1** (2018), 38–48.
 8. Раєвська І. Ю., Раєвська М. Ю. Локальні майже-кільця з мультиплікативною групою Шмідта, *Укр. мат. журн.*, **71** (2019), № 10, 1435–1440.
 9. 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.
 10. Раєвська І. Ю., Раєвська М. Ю., Локальні майже-кільця на елементарних абелевих групах порядку p^3 , Тези доповідей конференції молодих учених “Підстригачівські читання — 2021”, Львів, Україна, 26–28 травня, 2021,
<http://www.iapmm.lviv.ua/chyt2021/abstracts/Raievska.pdf>
 11. Раєвська І., Раєвська М. Про ендоеиклічні 2-породжені групи порядку 256 та експоненти 16. *Буковинський матем. журнал*, 2025, 13 (2), 161–169,
[https://bmj.chnu.edu.ua/media/gbdhv1v1/161-169_raievski_raievski_cor.pdf](https://bmj.chnu.edu.ua/media/gbdhv1v1/161-169_raievska_raievski_cor.pdf)
 12. 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.

13. Раєвська М. Ю. Локальні майже-кільця з мультиплікативною групою Міллера–Морено, *Вісн. Київ. Ун-ту. Математика, Механіка*, **25** (2011), 45–48.
14. Раєвська М. Ю., Сисак Я. П. Про локальні майже-кільця з мультиплікативною групою Міллера–Морено, *Укр. мат. журн.*, **64** (2012), № 6, 811–818.
15. Усенко В. М. Напівгрупи та майжекільця перетворень, автореф. дис... д-ра фіз.-мат. наук: 01.01.06; Київський ун-т ім. Тараса Шевченка. — К., 1999. — 32 с.
16. Холл М. Теорія груп, М.: Видавництво іноземної літератури, 1962 (рос.).
17. Шмідт О. Ю. Групи, всі підгрупи яких спеціальні, *Мат. зб.*, **31** (1924), 366–372 (рос.).
18. About, <https://www.gap-system.org/about/>
19. 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/>
20. 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.
21. Amberg B., Hubert P., Sysak Ya. Local near-rings with dihedral multiplicative group, *J. Algebra*, **273** (2004), 700–717.

22. Arunma M., Ezhilmaran D. A new multiparty identification scheme based on nearing root extraction problem, *Journal of Discrete Mathematical Sciences and Cryptography*, **22** (2019), 1, 59–64.
23. Beidleman J. C. On the theory of radicals of distributively generated near-rings. I. The primitive-radical, *Math. Annalen.*, **173** (1967), 89–101.
24. Beidleman J. C. On the theory of radicals of distributively generated near-rings. II. The nil-radical, *Math. Annalen.*, **173** — (1967), 200–218.
25. Betsch G. Ein Radikal für Fastringe, *Math. Z.*, **78** (1962), 86–90.
26. Bidwell J. N. S., Curran M. J. The automorphism group of a split metacyclic p -group, *Arch. Math.*, **87** (2006), 488–497.
27. Blackett D. W. Simple and semi-simple near-rings, *Proc. American Math. Soc.*, **4** (1953), 772–785.
28. Burnside W. Theory of groups of finite order, Cambridge: At the University press, 1897, 430 p.
29. Boykett T. H. H., Nobauer C. A class of groups which cannot be the additive groups of near-rings with identity, *Contributions to general algebra*, **10** (1998) (Klagenfurt, 1997), Klagenfurt: Heyn, 89–99.
30. Clay J. R. The near rings on a finite cyclic group, *The American Mathematical Monthly*, **71** (Jan., 1964), no. 1 , 47–50.
31. Clay J. R. Research in near-ring theory using a digital computer, *BIT*, **10** (1970), 249–265.
32. Clay J. R. Nearrings. Geneses and Applications, New York: Clarendon Press, Oxford University Press, 1992.

33. Clay J. R., Doi D., Near-rings with identity on alternating groups, *Math. Scand.*, **23** (1968), 54–56.
34. Clay J. R., Malone Jr. The near-rings with identities on certain finite groups, *Math. Scand.*, **19** (1966), 146–150.
35. 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.
36. Curran M. J. The automorphism group of a split metacyclic 2-group, *Arch. Math.*, **89** (2007), 10–23.
37. Dixon L. Definitions of a group and a field by independent postulates, *Trans. Amer. Math. Soc.*, **6** (1905), 198–204.
38. Ezhilmaran D., Muthukumaran V. Key exchange protocol using decomposition problem in near-ring, *Gazi University Journal of Science*, **29** (2016), no. 1, 123–127.
39. Ezhilmaran D., Muthukumaran V. Authenticated group key agreement protocol based on twist conjugacy problem in near-rings, *Wuhan University Journal of Natural Sciences*, **22** (2017), no. 6, 472–476.
40. Feigelstock S. Additive groups of local near-rings, *Comm. Algebra*, **34** (2006), 743–747.
41. Ferrero C. C., Ferrero G., Nearrings. Some developments linked to semigroups and groups, Kluwer Academic Publishers, Dordrecht, 2002, 609 p.
42. Furtwangler P., Taussky-Todd O. Über Schieftringe, *Sitzber. Akad. Wiss. Wien, Math. Nat. Klasse, Abt. IA*, **145** (1936), 525.

43. The GAP Group, Aachen, St Andrews. *GAP — Groups, Algorithms and Programming*, Version 4.13.0, 2024, <https://www.gap-system.org/>
44. GAP Packages, <https://www.gap-system.org/packages/>
45. Gorodnik A. Local near-rings with commutative groups of units, *Houston J. Math.*, **25** (1999), 223–234.
46. Heatherly H. Matrix near-rings, *J. London Math. Soc. (2)*, **7** (1973), 355–356.
47. Hubert P. Nearrings and a construction of triply factorized groups, Doctoral dissertation, Mainz, 2005, 146 p.
48. Hulpke A. Computing subgroups invariant under a set of automorphisms, *J. Symbolic Comput.*, **27** (1999), no. 4, 415–427.
49. Johnson M. J. Near-rings with identities on dihedral groups, *Proc. Edinburgh Math. Soc. (2)*, **18** (1972/73), 219–228.
50. Kaluzhnin L. A., Suhchanskyy V. I. Verbal functions on groups, *Theoretical and applied questions of differential equations and algebra*, 105–110, 264, “Naukova Dumka”, Kiev, 1978.
51. King B. W. Presentations of metacyclic groups, *Bul. Austral. Math. Soc.*, **8** (1973), 103–131.
52. Krimmel J. E. Conditions on Near-Rings with identity and the near-ring with identity on some metacyclic groups, Doctoral dissertation, Univ. of Arizona, Tucson, 1972.
53. Krimmel J. E. A condition on near-rings with identity, *Monatsh. Math.*, **77** (1973), 52–54.
54. Laxton R. R., Lockhart R. The near-rings hosted by a class of groups, *Proc. Edinb. Math. Soc.* **23** (1980), 69–86.

55. Ligh S. Near rings with identities on certain groups, *Monatsh. Math.*, **75** (1971), 38–43.
56. Lockhart R. The theory of near-rings, *Lecture Notes in Math.*, **2295**, Springer, Cham, 2021, 537 p.
57. Malone J. J. Review on the paper [61],
[http://mathscinet.imath.kiev.ua/mathscinet/
 article?mr=0236229](http://mathscinet.imath.kiev.ua/mathscinet/article?mr=0236229)
58. Mason G. On pseudo-distributive near-rings, *Proc. Edinburgh Math. Soc. (2)*, **28** (1985), no. 2, 133–141.
59. Maxson C. J. On finite near-rings with identity, *American Mathematical Monthly*, **74** (Dec., 1967), no. 10, 1228–1230.
60. Maxson C. J. On local near-rings, *Math. Z.*, **106** (1968), 197–205.
61. Maxson C. J. Local near-rings of cardinality p^2 , *Canad. Math. Bull.*, **11** (1968), no. 4, 555–561.
62. 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.
63. 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.
64. Meldrum J. D. P. Near-rings and their links with groups, PPL, 1985, 273 p.
65. Menegazzo F. Automorphisms of p -groups with cyclic commutator subgroup, *Rend. Sem. Mat. Univ. Padova*, **90** (1993), 81–101.
66. Miech R. J. On p -groups with a cyclic commutator, *J. Austral. Math. Soc.*, **20** (1975), 178–198.

67. Miller G. A., Moreno H. Non-abelian groups in which every subgroup is abelian, *Trans. Amer. Math. Soc.*, **4** (1903), 398–404.
68. Muthukumaran V., Ezhilmaran D., Muchtadi-Alamsyah I., Udhayakumar R., Manickam A. New public key cryptosystem based on combination of NREP and CSP in noncommutative near-ring, *Journal of Xi'an University of Architecture & Technology*, Volume XII (2020), Issue III, 4534–4540.
69. Neumann H. On varieties of groups and their associated near-rings, *Math. Z.*, **65** (1956), 36–69.
70. Ore Q. Linear equations in non-commutative fields, *Ann. of Math.*, **32** (1931), 463–477.
71. Peterson G. L. Centralizers and the isomorphism problem for nearrings, *Math. Pannon.*, **17** (2006), no. 1, 3–16.
72. Pilz G. Near-rings. The theory and its applications (Second edition), North-Holland, Amsterdam, 1983, 470 p.
73. Raievska I. Yu. Local nearrings on Miller-Moreno p -group, *Bulletin of Taras Shevchenko National University of Kyiv. Series: Mathematics, Mechanics*, **25** (2011), 43–45 (in Ukrainian).
74. Raievska I. On additive groups of finite local nearrings. Abstracts of AAA89: Workshop on General Algebra, Dresden, Germany, February 26–March 01, 2015,
<https://tu-dresden.de/mn/math/algebra/forschung/tagungen/aaaseries/aaa89>
75. Raievska I. Yu. Local nearrings with additive groups of order 128, *Наукoвий вісник Ужгородського університету. Серія “Математика і інформатика”*, **44** (2024), no. 1, 46–50.

76. Raievska I. On direct products of metacyclic Miller—Moreno p -groups and cyclic p -groups as additive groups of local nearrings. *Прикл. проблеми мех. і мат.*, **22** (2024), 123–130.
77. Raievska I., On direct products of metacyclic Miller—Moreno p -groups and cyclic p -groups as additive groups of local nearrings, 15th Ukraine Algebra Conference, Lviv, Ukraine, July 8–12, 2025. P. 86,
<https://xvuac.mmf.com.ua/index.php/abstracts>
78. Raievska I. Yu., Raievska M. Yu. Local nearrings of order at most 31. Abstracts of 2nd EUMLS Conference Mathematics for Life Sciences. Olenivka, Crimea, Ukraine, September 5–10, 2013, P. 27.
79. Raievska I., Raievska M. Nearrings with identity on Miller—Moreno groups. Abstracts of II Ukrainian Scientific Conference “Applying of mathematics methods in science and technics”. Lutsk, Ukraine, November 22–23, 2013, P. 104–109.
80. Raievska I. Yu., Raievska M. Yu. Finite nearrings with identity on Miller—Moreno groups, *Mat. Stud.*, **42** (2014), no. 1, 15–20.
81. Raievska I., Raievska M. Using the computer algebra system GAP for constructing and studying of algebraic structures. Abstracts of IXth Summer School “Algebra, Topology and Analysis”, Polianytsia, Ukraine, July 7–18, 2014, P. 68–69.
82. Raievska I., Raievska M. Finite nearrings with identity on Miller—Moreno groups. Abstracts of IV International Hahn conference dedicated to the 135-th anniversary of Hans Hahn, Chernivtsi, Ukraine, June 30–July 5, 2014, P. 253–255.
83. 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
84. Raievska I. Yu., Raievska M. Yu. Local nearrings of order p^3 . Abstracts of 11th International Algebraic Conference in Ukraine dedicated to the 75th anniversary of V. V. Kirichenko, July 3—7, 2017, Institute of Mathematics of NAS of Ukraine, Kyiv, Ukraine, P. 113.
 85. Raievska I. Yu., Raievska M. Yu. Finite dihedral groups as the additive groups of nearrings with identity. Тези доповідей Міжнародної конференції молодих математиків, 6–8 червня 2019 р., Ін-т математики НАН України, Київ, Україна, С. 17.
 86. 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>
 87. Raievska I., Raievska M., On local nearrings of order p^3 , Abstracts of 11th International Skorobohatko Mathematical Conference, Lviv, Ukraine, October 26—30, 2020, P. 97,
http://www.iapmm.lviv.ua/conf_skorob2020/documents/2020tezy.pdf
 88. Raievska I. Yu., Raievska M. Yu. Local nearrings on finite non-abelian 2-generated p -groups, *Carpathian Math. Publ.*, **12** (2020), no. 1, 199–207.
 89. Raievska I., Raievska M., Finite one-sided distributive structures and GAP, International Algebraic Conference “At the End of the Year 2022”

- (online), Kyiv, Ukraine, December 27–28, 2022,
<https://www.imath.kiev.ua/~algebra/algebra2022/abstracts>
90. 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>
 91. 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
 92. Raievska I., Raievska M., Groups of order p^4 as additive groups of local nearrings, Ukraine Algebra Conference “At the End of the Year 2023”, Kyiv, Ukraine, December 26–27, 2023 (online),
<https://sites.google.com/view/aey2023/home?authuser=0>
 93. Raievska I., Raievska M., Groups of nilpotency class 3 of order p^4 as additive groups of local nearrings, XIX International Scientific Mykhailo Kravchuk Conference, dedicated to the 125th anniversary of Igor Sikorsky Kyiv Polytechnic Institute, Igor Sikorsky Kyiv Polytechnic Institute, October 11–12, 2023 (online),
<https://matan.kpi.ua/en/kravchuk-conf-2023/>
 94. Raievska I., Raievska M., Groups of the nilpotency class 2 of order p^4 as additive groups of local nearrings, The 103rd Workshop on General Algebra, Tartu, Estonia, June 9–11, 2023,

[https://kodu.ut.ee/~vlaan/AAA103abstracts/
abstract_Raievska.pdf](https://kodu.ut.ee/~vlaan/AAA103abstracts/abstract_Raievska.pdf)

95. Raievska I., Raievska M. Lower bounds for the number of local nearrings on groups of order p^3 , *Math. Commun.*, **29** (2024), 177–191.
96. 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
97. 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.
98. 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.
99. 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](https://www.gapdays.de/gapdays2024-spring/abstracts/raievska)
100. Raievska I., Raievska M. Local nearrings, their structure, and the GAP system. *Ukrainian Math. J.*, 2025, **76** (11), 1831–1848, translation of *Ukrain. Mat. Zh.*, 2024, **76** (11), 1629–1644.
101. 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)

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 I. Yu., Raievska M. Yu., Sysak Ya. P. Finite local nearrings with split metacyclic additive group, *Algebra Discrete Math.*, **22** (2016), no. 1, 129–152.
104. Raievska I. Yu., Raievska M. Yu., Sysak Ya. P. On local nearrings of order 32, International Conference dedicated to 100th anniversary of S. M. Chernikov, August 20–26, 2012, Kyiv, Ukraine. Book of abstracts. — Kyiv: Institute of Mathematics of NAS of Ukraine, 2012. — P. 124.
105. Raievska I. Yu., Raievska M. Yu., Sysak Ya. P. Small groups as the additive groups of local nearrings. Abstracts of the International Algebraic Conference dedicated to 100-th anniversary of L. A. Kaluzhnin, Taras Shevchenko Nat. Univ., Kyiv, Ukraine, July 7–12, 2014, P. 70.
106. Raievska I. Yu., Raievska M. Yu., Sysak Ya. P. Local nearrings of order 64, International mathematical conference “Groups and Actions: Geometry and Dynamics, dedicated to the memory of professor Vitaly Sushchansky”, December 19–22, 2016, Kyiv, Ukraine. Book of abstracts. — Kyiv, 2016. — P. 43.
107. Raievska I. Yu., Raievska M. Yu., Sysak Ya. P. Local nearrings of order 243. *Proceedings of the 4th Conference of Mathematical Society of Moldova CMSM4'2017*, June 28–July 2, 2017, Chisinau, Republic of Moldova, 149–152 (2017).
108. Raievska I., Raievska M., Sysak Ya. DatabaseEndom128: (v0.2) [Data set] (2022). Zenodo,
<https://doi.org/10.5281/zenodo.7225377>

109. Raievska I., Raievska M., Sysak Ya. DatabaseEndom625: (v0.2) [Data set] (2023). Zenodo,
<https://doi.org/10.5281/zenodo.7613145>
110. Raievska I. Yu., Raievska M. Yu., Sysak Ya. P. Semidistributive nearrings with identity, *Algebra Discrete Math.*, **36** (2023), no. 2, 217–224.
111. Raievska I., Raievska M., Sysak Ya. LocalNR, Package of local nearrings, Version 1.0.4 (2024) (GAP package),
<https://gap-packages.github.io/LocalNR/>
112. Raievska I., Raievska M., Sysak Ya. DatabaseEndom32: (v1.0.2) [Data set] (2024). Zenodo,
<https://doi.org/10.5281/zenodo.10820301>
113. Raievska I., Raievska M., Sysak Ya. DatabaseEndom64: (v1.0.1) [Data set] (2024). Zenodo,
<https://doi.org/10.5281/zenodo.10820320>
114. Raievska I., Raievska M., Sysak Ya. DatabaseEndom243: (v1.0.1) [Data set] (2024). Zenodo,
<https://doi.org/10.5281/zenodo.10820318>
115. Raievska I., Raievska M., Sysak Ya. LocalNR package and some of its applications, *Algebra Discrete Math.*, **40** (2025), no. 2, 215–225.
116. Raievska I., Raievska M., Sysak Ya., Local nearrings with additive groups of order 128 and exponent 8. II, Міжнародна конференція, присвячена 75-й річниці від дня народження Володимира Маслюченка, Чернівецький національний університет імені Юрія Федьковича, 25–27 вересня 2025 року, Чернівці, Україна, С. 159,
<https://drive.google.com/file/d/1Clufy2S3NPcxiNvsyQLnBD035EKDZQsV/view>

117. Raievska M. On semidistributive local nearrings, *Науковий вісник Ужгородського університету. Серія “Математика і інформатика”*, **43** (2023), 2, 67–71.
118. 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.
119. 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.
120. The Small Groups Library,
<https://docs.gap-system.org/pkg/smallgrp/doc/chap1.html>
121. SONATA: a GAP 4 package - Chapters,
<https://docs.gap-system.org/pkg/sonata/doc/html/ref/chapters.htm>
122. Sysak Ya. P. Products of groups and local nearrings, *Note di Mat.*, **28** (2008), no. 2, 179–213.
123. Sysak Ya., Raievska I., Raievska M. Construction of local nearrings using GAP, *Algebra Discrete Math.*, **40** (2025), no. 1, 133–144.
124. Sysak Ya., Raievska I., Raievska M., Construction of local nearrings using GAP, Ukraine Mathematics Conference “At the End of the Year 2025”, December 18–19, 2025, Taras Shevchenko National University of Kyiv, Kyiv, Ukraine, P. 54,
<https://drive.google.com/file/d/1LGUD-of4DUq2LiKYbN233claruwbGIj4/view>

125. Sysak Ya., Raievska I., Raievska M., (2025) 128_160,
https://github.com/raemarina/128_160/tree/main
126. Sysak Ya. P., Termini S. Di Local nearrings with generalized quaternion multiplicative group, *Ricerche Mat.*, **56** (2007), 61–72.
127. Taussky-Todd O. Rings with non-commutative addition, *Bull. Calcutta Math. Soc.*, **28** (1936), 245–246.
128. Wähling H. Theorie der Fastkörper, Essen: Thales Verlag, 1987, 393 p.
129. Wendt G. On the multiplicative semigroup of near-rings, *Math. Pannon.*, **15** (2004), no. 2, 209–220.
130. 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 15 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 [5, 1, 2, 6, 9, 10, 14, 12]. Результати дисертації додатково відображено у 22 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 ендоеиклічні 2-порощжені групи порядку 256 та експоненти 16. *Буковинський матем. журнал*, 2025, **13** (2), 161–169, https://bmj.chnu.edu.ua/media/gbdhv1v1/161-169-raievska-raievska_cor.pdf (Категорія Б)

4. Раєвська І. Про прямі добутки неметациклічних p -груп Міллера–Морено та циклічних p -груп як адитивні групи локальних майже-кілець. *Науковий вісник Ужгородського університету. Серія «Математика і інформатика»*, 2025, **46** (1), 79–88,
[https://doi.org/10.24144/2616-7700.2025.46\(1\).79-88](https://doi.org/10.24144/2616-7700.2025.46(1).79-88) (Категорія Б)
5. Raievska I., Raievska M. Groups of the nilpotency class 3 of order p^4 as additive groups of local nearrings. *Carpathian Math. Publ.*, 2025, **17** (1), 292–301,
<https://doi.org/10.15330/cmp.17.1.292-301> (SJR — **Q1**)
6. 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. **76** (11), 1629–1644 (SJR — **Q3**)
7. 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)
8. Raievska I. On direct products of metacyclic Miller–Moreno p -groups and cyclic p -groups as additive groups of local nearrings. *Прикл. проблеми мех. і мат.*, 2024, **22**, 123–130. (Категорія Б)
9. Raievska I., Raievska M. Groups of order p^4 as additive groups of local nearrings. *Ukrainian Math. J.*, 2024, **76** (6), 1005–1024, <https://doi.org/10.1007/s11253-024-02369-w>; translation

- of *Ukrain. Mat. Zh.*, 2024, **76** (6), 890–906. **76** (6), 890–906 (SJR — **Q3**)
10. 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,
<http://dx.doi.org/10.12958/adm2269> (SJR — **Q3**)
 11. Raievska I. Yu. Local nearrings with additive groups of order 128, *Науковий вісник Ужгородського університету. Серія “Математика і інформатика”*, 2024, **44** (1), 46–50,
[https://doi.org/10.24144/2616-7700.2024.45\(2\).110-114](https://doi.org/10.24144/2616-7700.2024.45(2).110-114) (Категорія Б)
 12. Raievska I., Raievska M. Lower bounds for the number of local nearrings on groups of order p^3 . *Math. Commun.*, 2024, **29** (2), 177–191,
<https://www.mathos.unios.hr/mc/index.php/mc/issue/view/35> (SJR — **Q4**)
 13. Раєвська І. Ю., Раєвська М. Ю. Локальні майже-кільця на елементарних абелевих групах порядку p^3 . Науковий вісник Ужгородського університету. Серія “Математика і інформатика”, 2021, **38** (1), 85–93,
[https://doi.org/10.24144/2616-7700.2021.38\(1\).85-93](https://doi.org/10.24144/2616-7700.2021.38(1).85-93) (Категорія Б)
 14. Raievska I. Yu., Raievska M. Yu. Local near-rings with a multiplicative Schmidt group. *Ukr. Math. J.*, 2020, **71** (10), 1643–1649, <https://doi.org/10.1007/s11253-020-01737-6>; перекладено з *Ukr. Mat. Zh.*, 2019, **71** (10), 1435–1440. (in Ukrainian);
<http://umj.imath.kiev.ua/index.php/umj/article/view/1526/509> (SJR — **Q3**)

15. 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)
16. Раєвська І. Ю., Раєвська М. Ю. Скінченні локальні майже-кільця. *Могиллянський математичний журнал*, 2018, **1**, 38–48,
<http://mmj.ukma.edu.ua/article/view/152611/151700>
17. Raievska I., Raievska M., Sysak Ya. DatabaseEndom32: (v1.0.2) [Data set] (2024). Zenodo,
<https://doi.org/10.5281/zenodo.10820301>
18. Raievska I., Raievska M., Sysak Ya. DatabaseEndom128: (v0.2) [Data set] (2022). Zenodo,
<https://doi.org/10.5281/zenodo.7225377>
19. Raievska I., Raievska M., Sysak Ya. DatabaseEndom625: (v0.2) [Data set] (2023). Zenodo,
<https://doi.org/10.5281/zenodo.7613145>
20. 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. Sysak Ya., Raievska I., Raievska M., Construction of local nearrings using GAP, Ukraine Mathematics Conference “At the End of the Year 2025”, December 18–19, 2025, Taras Shevchenko National University of Kyiv, Kyiv, Ukraine, P. 54,
<https://drive.google.com/file/d/1LGUD-of4DUq2LiKYbN233claruwbGIj4/view>

Форма участі — online, доповідь.

2. Raievska I., Raievska M., Sysak Ya., Local nearrings with additive groups of order 128 and exponent 8. II, Міжнародна конференція, присвячена 75-й річниці від дня народження Володимира Маслюченка, Чернівецький національний університет імені Юрія Федьковича, 25–27 вересня 2025 року, Чернівці, Україна, С. 159,
<https://drive.google.com/file/d/1Clufy2S3NPcxiNvsyQLnBD035EKDZQsV/view>

Форма участі — очно, доповідь.

3. Raievska I., On direct products of metacyclic Miller–Moreno p -groups and cyclic p -groups as additive groups of local nearrings, 15th Ukraine Algebra Conference, Lviv, Ukraine, July 8–12, 2025. P. 86,
<https://xvuac.mmf.com.ua/index.php/abstracts>

Форма участі — online, доповідь.

4. Раєвська І. Про прямі добутки неметациклічних p -груп Міллера–Морено та циклічних p -груп як адитивні групи локальних майже-кілець, 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.

5. 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.

6. Raievska I., Raievska M., Groups of order p^4 as additive groups of local nearrings, Ukraine Algebra Conference “At the End of the Year 2023”, Kyiv, Ukraine, December 26–27, 2023 (online),
<https://sites.google.com/view/ae2023/home?authuser=0>
 Форма участі — online, доповідь.
7. Raievska I., Raievska M., Groups of nilpotency class 3 of order p^4 as additive groups of local nearrings, XIX International Scientific Mykhailo Kravchuk Conference, dedicated to the 125th anniversary of Igor Sikorsky Kyiv Polytechnic Institute, Igor Sikorsky Kyiv Polytechnic Institute, October 11–12, 2023 (online),
<https://matan.kpi.ua/en/kravchuk-conf-2023/>
 Форма участі — online, доповідь.
8. Raievska I., Raievska M., Groups of the nilpotency class 2 of order p^4 as additive groups of local nearrings, The 103rd Workshop on General Algebra, Tartu, Estonia, June 9–11, 2023,
https://kodu.ut.ee/~vlaan/AAA103abstracts/abstract_Raievska.pdf
 Форма участі — очно, доповідь.
9. Raievska I., Raievska M., Finite one-sided distributive structures and GAP, International Algebraic Conference “At the End of the Year 2022” (online), Kyiv, Ukraine, December 27–28, 2022,
<https://www.imath.kiev.ua/~algebra/algebra2022/abstracts>
 Форма участі — online, доповідь.
10. 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.

11. 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.

12. Раєвська І. Ю., Раєвська М. Ю., Локальні майже-кільця на елементарних абелевих групах порядку p^3 , Тези доповідей конференції молодих учених “Підстригачівські читання — 2021”, Львів, Україна, 26–28 травня, 2020,
<http://www.iapmm.lviv.ua/chyt2021/abstracts/Raievska.pdf>

Форма участі — online, доповідь.

13. Raievska I., Raievska M., On local nearrings of order p^3 , Abstracts of 11th International Skorobohatko Mathematical Conference, Lviv, Ukraine, October 26–30, 2021, P. 97,
http://www.iapmm.lviv.ua/conf_skorob2020/documents/2020tezy.pdf

Форма участі — online, доповідь.

14. Raievska I. Yu., Raievska M. Yu. Local nearrings of order p^3 . Abstracts of 11th International Algebraic Conference in Ukraine dedicated to the 75th anniversary of V. V. Kirichenko, July 3–7, 2017, Institute of Mathematics of NAS of Ukraine, Kyiv, Ukraine, P. 113.

Форма участі — очно, доповідь.

15. Раєвська І. Ю., Раєвська М. Ю. Адитивні групи скінченних майже-кілець з одиницею. Тези доповідей Міжнародної конференції молодих математиків, присвяченої 100-річчю з дня народження академіка НАН України Ю. О. Митропольського (1917–2008), 7–10 червня 2017 р., Ін-т математики НАН України, Київ, С. 20.

Форма участі — очно, доповідь.

16. 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.

17. Raievska I. On additive groups of finite local nearrings. Abstracts of AAA89: Workshop on General Algebra, Dresden, Germany, February 26–March 01, 2015,
<https://tu-dresden.de/mn/math/algebra/forschung/tagungen/aaaseries/aaa89>

Форма участі — очно, доповідь.

18. Raievska I., Raievska M. Using the computer algebra system GAP for constructing and studying of algebraic structures. Abstracts of IXth Summer School “Algebra, Topology and Analysis”, Polianytsia, Ukraine, July 7–18, 2014, P. 68–69.

Форма участі — очно, доповідь.

19. Raievska I. Yu., Raievska M. Yu., Sysak Ya. P. Small groups as the additive groups of local nearrings. Abstracts of the International Algebraic

Conference dedicated to 100-th anniversary of L. A. Kaluzhnin, Taras Shevchenko Nat. Univ., Kyiv, Ukraine, July 7–12, 2014, P. 70.

Форма участі — заочно.

20. Raievska I., Raievska M. Finite nearrings with identity on Miller-Moreno groups. Abstracts of IV International Hahn conference dedicated to the 135-th anniversary of Hans Hahn, Chernivtsi, Ukraine, June 30–July 5, 2014, P. 253–255.

Форма участі — очно, доповідь.

21. Raievska I., Raievska M. Nearrings with identity on Miller-Moreno groups. Abstracts of II Ukrainian Scientific Conference “Applying of mathematics methods in science and technics”. Lutsk, Ukraine, November 22–23, 2013, P. 104–109.

Форма участі — заочно.

22. Raievska I. Yu., Raievska M. Yu. Local nearrings of order at most 31. Abstracts of 2nd EUMLS Conference Mathematics for Life Sciences. Olenivka, Crimea, Ukraine, September 5–10, 2013, P. 27.

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;

- Міжнародній конференції, присвяченій 75-й річниці від дня народження Володимира Маслюченка, 25–27 вересня 2025 року, Чернівецький національний університет імені Юрія Федьковича, Чернівці, Україна;
- 15th Ukraine Algebra Conference, July 8–12, 2025, Lviv, Ukraine;
- The conference of young scientists “Pidstryhach Readings — 2025”, May 27–29, 2025, Lviv, Ukraine;
- GAP Days Spring 2024, March 11–15, 2024, University of Kaiserslautern-Landau, Kaiserslautern, Germany;
- Ukraine Algebra Conference “At the End of the Year 2023” (online), December 26–27, 2023, Kyiv, Ukraine;
- XIX Міжнародній науковій конференції імені академіка Михайла Кравчука, присвячена 125-річчю КПІ ім. Ігоря Сікорського (онлайн), 11–12 жовтня 2023 року, Київ, Україна;
- AAA103, The 103rd Workshop on General Algebra, June 9–11, 2023, University of Tartu, Tartu, Estonia;
- Online Twinning Conference (online), March 27–30, 2023, Digital Theme UK-Ukraine Twinning Initiative, Great Britain;
- International Algebraic Conference “At the End of the Year 2022” (online), December 27–28, 2022, Kyiv, Ukraine;
- International conference-workshop “GAP Days Summer 2022”, October 17–21, 2022, RWTH Aachen University, Aachen, Germany;
- International Conference “On the Trail of Women in Mathematics “Contemporary Women in Mathematics”, September 15–17, 2022, Gdansk, Poland;

- Конференції молодих учених “Підстригачівські читання – 2021” (онлайн), 26 – 28 травня 2021 року, Львів, Україна;
- 11th International Skorobohatko Mathematical Conference, October 26 – 30, 2020, Lviv, Ukraine;
- Конференції молодих учених “Підстригачівські читання – 2020”, 26 – 28 травня 2020 року, Львів, Україна;
- 11th International Skorobohatko Mathematical Conference, October 26 – 30, 2020, Lviv, Ukraine;
- GAP-Singular-Meeting as part of the OpenDreamKit project, August 15 – 23, 2019, PfalzAkademie, Lambrecht, Germany;
- Міжнародній конференції молодих математиків, 6 – 8 червня 2019 року, Київ, Україна;
- Міжнародній науковій конференції “Сучасні проблеми механіки та математики”, яка присвячена 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 року, Львів, Україна;
- 11th International Algebraic Conference in Ukraine dedicated to the 75th anniversary of V. V. Kirichenko, July 03 – 07, 2017, Kyiv, Ukraine;
- XI Літній школі “Алгебра, Топологія, Аналіз”, 1–14 серпня 2016 року, Одеса, Україна;
- Міжнародній конференції молодих математиків присвячена 100-річчю з дня народження академіка НАН України Юрія Олексійовича Митропольського (1917–2008), 7–10 червня 2017 року, Київ, Україна;

- Summer School on Algebra, Statistics and Combinatorics, June 27 – July 2, 2016, Espoo, Finland;
- AAA89: Workshop on General Algebra, February 26 – March 01, 2015, Dresden, Germany;
- The International Algebraic Conference dedicated to 100-th anniversary of L. A. Kaluzhnin, 07–12 July, 2014, Kyiv, Ukraine;
- IX-а Літня школа “Алгебра, топологія і аналіз”, 7–18 липня 2014 року, Поляниця, Україна;
- IV Міжнародній Ганській конференції, 30 червня – 1 липня 2014 року, Чернівці, Україна;
- Humboldt Kolleg “Education and Science and their Role in Social and Industrial Progress of Society”, June 12–15, 2014, Kyiv, Ukraine;
- II Всеукраїнській науковій конференції “Застосування математичних методів в науці і техніці”, 22–23 листопада 2013 року, Луцьк, Україна;
- 2nd EUMLS Conference Mathematics for Life Sciences, September 05–10, 2013, Olenivka, Crimea, Ukraine;
- засіданнях Вчених рад Інституту математики НАН України (20 червня 2023 р. – online, 24 червня 2025 р. – online);
- семінарі лабораторії топології Інституту математики НАН України (керівник: чл.-кор. С.І. Максименко, Київ, Україна) (19 квітня 2023 р. – online);
- семінарах “Алгебра” Варшавського університету (керівник: проф. Ян Окнінський, Варшава, Польща) (21 квітня 2022 р., 9 березня 2023 р., 18 січня 2024 р.);

- 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.);
- Алгебраїчних семінарах Інституту математики НАН України (керівник: чл.-кор. Ю. А. Дрозд, чл.-кор. С. І. Максименко, Київ, Україна) (6 жовтня 2015 р., 18 грудня 2018 р., 26 червня 2024 р. – online, 12.11.2025 р. – online);
- Scientific Seminar “Geometry, Topology, Applications” (керівник: проф. Т. О. Банах, Львів, Україна) (9 березня 2026 р.);
- 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) (22 вересня 2016 р.).