УДК 512.6

Раєвська І. Ю., Раєвська М. Ю.

DOI: https://doi.org/10.18523/2617-7080i2018p38-48

СКІНЧЕННІ ЛОКАЛЬНІ МАЙЖЕ-КІЛЬЦЯ

У статті здійснено огляд сучасного стану дослідження скінченних локальних майже-кілець, а саме їх похідних структур — адитивної та мультиплікативної груп. Наведено класифікацію локальних майже-кілець, порядок яких не перевищує 32.

Ключові слова: локальне майже-кільце, майже-кільце з одиницею, адитивна група, мультиплікативна група.

Попередні результати

Майже-кільця — це множини з двома бінарними операціями, додаванням та множенням, що задовольняють усі аксіоми асоціативного кільця, за винятком комутативності додавання та одного (у нашому випадку, правого) дистрибутивного закону. Отже, майже-кільця можна розглядати як узагальнення асоціативних кілець.

Означення 1. 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 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. За аксіомою 3) означення 1 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 $0 \cdot x = 0$, та *майже-кільцем з одиницею* i, якщо напівгрупа $(R, \cdot)$ є моноїдом з одиничним елементом i. Група всіх оборотних елементів моноїда $(R, \cdot)$ називається *мультиплікативною групою* в R та позначається через R^*.

Як звичайно, для елементів r та s з майже-кільця R запис rs означає $r \cdot s$. Крім того, якщо n — додатне ціле число, то rn означає

$$\underbrace{r + \ldots + r}_{n}.$$

Означення 2. Майже-кільце R з одиницею називається *локальним*, якщо множина $L = R \setminus R^*$ всіх необоротних елементів із $(R, \cdot)$ утворює адитивну підгрупу в R^+, та *майже-полем*, коли $L = 0$.

Майже-кільця з одиницею

Однією з характерних рис сучасного етапу розвитку алгебри є підвищення активності досліджень в областях, що узагальнюють теорії класичних алгебраїчних систем. До таких областей належить і теорія майже-кілець.

Історично першим кроком назустріч майже-кільцям була аксіоматика, зроблена в дослідженні Діксоном [1]. Він показав, що існують «поля з одним дистрибутивним законом», та навів приклади, які показують, що такі системи (Цассенхауз назвав їх майже-полями) можуть насправді бути недистрибутивними. Пізніше Цассенхауз [2] довів, що приклади Діксона охоплюють усі, крім сімох скінченних майже-полів, які не є тілами. Після 1960-х років Карзель розширив методи Діксона та Цассенхауза в побудові майже-полів.

Уперше майже-поля застосували в геометрії Веблен і Ваддербарн [3]. У подальшому майже-поля вивчали, головним чином, завдяки їх застосуванням у геометрії (див. [4]). Теорії майже-полів присвячено монографію Виглінга [5], в якій систематизовано більшість результатів про майже-поля.

Основи аксіоматики теорії майже-кілець було закладено в працях Оре [6], Фуртванглера та Таусскі-Тод [7], Таусскі-Тод [8].

До початку 1940-х років відбувалося дослідження основних загальних властивостей майже-кілець, опис деяких класів скінченних майже-кілець, застосування в теорії груп підстановок (Цассенхауз, Віландт, Таусскі-Тод, Фіттінг, Веблен, Ваддербарн). Подальший розвиток цієї теорії стимулювали праці Блекетта [9], Х. Нойман [10; 11], Бетча [12], Бейдлемана [13; 14] та ін.

З початку 1940-х до кінця 1970-х років теорія майже-кілець застосовується в задачах класифікації нелінійних математичних структур. Закладено основи структурної теорії майже-кілець. У цей період виявлено простоту майже-кілець деяких класів і, зокрема, повних майже-кілець перетворень груп (симетричних майже-кілець на групах) та поліноміальних майже-кілець над полями нульової характеристики. Отримано аналоги теорем Джекобсона, Ваддербарна — Артіна, деяких інших теорем структурної теорії кілець. Покладено початок теорії радикалів майже-кілець.

На сучасному етапі поглиблюється класифікація майже-кілець, численнішими стають майже-кільцеві конструкції, поширюються застосування. Активно розвивається теорія радикалів. Вивчаються матричні, групові та напівгрупові майже-кільця, інші алгебраїчні системи, пов'язані з майже-кільцями, з'явилися деякі узагальнення. Методи теорії майже-кілець почали відігравати суттєву роль у класифікації кратнотранзитивних груп підстановок. Почалося структурне вивчення складових майже-кілець.

Загальній теорії майже-кілець присвячено монографії Пільца [15], Мелдрума [16], Клея [17], а також К. Ферреро та Г. Ферреро [18].

До проблематики теорії майже-кілець звертались Курош, Плоткін та їхні учні. Деяким питанням теорії майже-кілець та її зв'язкам з теорією мультиоператорних груп тощо присвячено праці Поліна, Кузьміна, Марина, Каарлі та ін.

В Україні однією з перших праць, у якій розглянуто майже-кільця, є робота Калужніна та Сущанського [19]. Пізніше з'явилися праці, пов'язані з вивченням групових відображень та майже-кілець перетворень (Кириченко, Усенко, Кіртадзе, Міхайлова, Рябухо).

Певні труднощі в цій області, з одного боку, зумовлено обмеженістю класичних факторизаційних методів та відсутністю адекватних майже-кільцевих конструкцій — з іншого.

Добре відомо і легко перевіряється, що якщо в майже-кільці з одиницею виконуються обидва дистрибутивних закони, то операція додавання в них обов'язково комутативна. Тому відсутність одного з дистрибутивних законів в означенні майже-кільця є значно більш важливою умовою, ніж відсутність аксіоми комутативності додавання, і саме з цим пов'язані головні труднощі, які виникають під час вивчення майже-кілець.

Типовим прикладом майже-кільця є множина $M(G)$ всіх відображень довільної групи G в себе, якщо операцію додавання відображень визначити як поелементну операцію їх образів у 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.

Згідно з добре відомим результатом із теорії кілець, кожне кільце може бути вкладене в кільце $E(G)$ всіх ендоморфізмів деякої абелевої групи G. Аналогічно, кожне майже-кільце може бути вкладене в майже-кільце відображень групи $M(G)$ для деякої групи G.

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 визначених вище операцій:

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

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

Оскільки будь-яка скінченна абелева група A є прямою сумою примарних циклічних підгруп, кожну з яких можна розглядати як адитивну групу деякого кільця лишків $\mathbb{Z}/p^iZ$, то 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 є правильним. Питання про те, які групи можуть бути адитивними групами майже-кілець з одиницею, досліджується з кінця 1960-х років.

Один із перших результатів у цьому напрямку отримали Клей та Малоне [20], які показали, що з точністю до ізоморфізму існує єдине майже-кільце з одиницею, адитивна група якого циклічна і яке фактично є комутативним кільцем. Там само було встановлено, що адитивна група скінченного майже-кільця з одиницею є простою тоді і тільки тоді, коли це майже-кільце є полем простого порядку. Також було 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.

Клей та Дой [21] довели, що знакозмінна група A_4 також не може бути адитивною групою майже-кільця з одиницею.

Результати статті Клейя та Малоне розвинув Лай [22], який довів, що скінченні неабелеві групи з точно однією власною нормальною підгрупою та скінченні досконалі групи не можуть бути адитивними групами майже-кілець з одиницею.

Наведені вище результати узагальнив Кріммел [23]. Він, зокрема, довів, що кожна скінченна група непростого порядку, ґратка нормальних підгруп якої лінійно впорядкована, не може бути адитивною групою майже-кільця з одиницею.

Клей [24] показав, що не існує майже-кільця з одиницею, адитивна група якого ізоморфна групі кватерніонів Q_8, та встановив, що існує сім неізоморфних майже-кілець з одиницею на групі діедра D_4 порядку 8. Клей та Мексон [25] довели, що узагальнені групи кватерніонів Q_{2^n} при $n > 3$ також не можуть бути адитивними групами майже-кілець з одиницею. Групи діедра D_n порядку $2n$ як адитивні групи майже-кілець з одиницею дослідив Джонсон [26]. Він встановив, що для непарного n група D_n не може бути адитивною групою майже-кільця з одиницею, та довів, що з точністю до ізоморфізму існує єдине таке майже-кільце на групі D_n при $n = 2p$, де p — просте число.

Використовуючи систему комп'ютерної алгебри GAP [27], Бойкетт та Нибауер [28] класифікували всі майже-кільця з одиницею на групах порядку, що не перевищує 31. Це дозволило їм визначити всі неабелеві групи вказаних порядків, які не можуть бути адитивними групами майже-кілець з одиницею. Зокрема, вони показали, що квазідіедральна група порядку 16 є такою.

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 вивчали Міллер та Морено [29]. Будова таких груп добре відома і повністю описується такою теоремою (див. [30, Chapter XII]).

Теорема 1. *Скінченні групи Міллера — Морено вичерпуються групами таких 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.*

Далі 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 1, кожна метациклічна p-група Міллера — Морено ізоморфна або групі кватерніонів Q_8, або групі $G(p^m, p^n)$.

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 1, кожна неметациклічна p-група Міллера — Морено ізоморфна групі $G(p^m, p^n, p)$.

У наступній теоремі (див. [31]) описано всі можливі типи груп Міллера — Морено, які можуть бути адитивними групами майже-кілець з одиницею.

Теорема 2. *Група Міллера — Морено G є адитивною групою майже-кільця R з одиницею і тоді та тільки тоді, коли є p-групою для деякого простого p та виконується одне з таких тверджень:*

1) *група G ізоморфна одній з груп $G(p^m, p^n)$ з $p^{m+n} > 8$ та $m > n$, циклічна підгрупа порядку p^m, породжена i, є нормальною в G;*
2) *$p = 2$, група G ізоморфна одній з груп $G(2^m, 2^n)$ з $m \leq n$ та циклічна підгрупа порядку 2^n, породжена i, не є нормальною в G;*
3) *група G ізоморфна одній з груп $G(p^m, p^n, p)$ та циклічна підгрупа, породжена i, не є нормальною в G;*
4) *група G ізоморфна групі $G(4, 2)$.*

Як наслідок, маємо таке твердження.

Наслідок 3. *Не існує майже-кілець з одиницею, адитивна група яких ізоморфна групі $G(p^m, p^n)$ з $p > 2$ та $2 \leq m \leq n$.*

Групою Шмідта, або *мінімальною ненільпотентною групою*, називається скінченна ненільпотентна група, будь-яка власна підгрупа якої нільпотентна. Вивчення таких груп започаткував О. Ю. Шмідт [32]. У наступній теоремі дано структурний опис цих груп (див. [33, Satz 5.5.2]).

Теорема 4. *Скінченна група G тоді і лише тоді є групою Шмідта, коли вона розкладається в напівпрямий добуток $G = S \rtimes T$ своїх нормальної силовської p-підгрупи S порядку p^s з $s \geq 1$ та циклічної силовської q-підгрупи $T = \langle b\rangle$ порядку q^t з $t \geq 1$, що задовольняють такі умови:*

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

Очевидно, що непримарні групи Міллера — Морено є групами Шмідта.

Маємо таке твердження (див. [34]).

Теорема 5. *Не існує майже-кілець з одиницею, адитивна група яких ізоморфна групі Шмідта.*

Локальні майже-кільця, їхні адитивні та мультиплікативні групи

Локальні майже-кільця. 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 ініціював у 1968 році Мексон [35]. У цій самій статті встановлено, що адитивна група скінченного нуль-симетричного локального майже-кільця є p-групою. Більш загальний результат, з якого випливає, що періодична і, зокрема, скінченна адитивна група кожного локального майже-кільця є p-групою скінченної експоненти, отримали Амберг, Хуберт та Сисак [36].

Мексон [37] 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. Разом із фундаментальною працею Цассенхауза про майже-поля й роботою Клея та Малоне [20] ця стаття дає повний опис усіх нуль-симетричних локальних майже-кілець порядку p^2.

Далі Мексон [38] довів, що кожна нециклічна скінченна абелева p-група порядку, більшого за 4, є адитивною групою деякого нуль-симетричного локального майже-кільця, що не є кільцем. Цей же автор [39] показав, що група діедра D_4 не може бути адитивною групою локального майже-кільця, 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 $p = 2$.

Як показав Файгелсток [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-кільця. У вказаній статті зазначено, що залишається відкритим питання про те, які неабелеві групи порядку p^n можуть бути адитивними групами локальних майже-кілець.

Основні результати, що стосуються локальних майже-кілець, підсумовано в огляді Сисака [41].

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

Наступна лема (див. [36]) характеризує основні властивості довільних скінченних локальних майже-кілець.

Лема 6. *Нехай R — скінченне локальне майже-кільце 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 такі 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^*.*

Як доведено в [20], кожне майже-кільце з одиницею, адитивна група якого циклічна, є насправді комутативним кільцем, а отже, ізоморфним кільцю лишків $\mathbb{Z}/n\mathbb{Z}$ для деякого цілого числа n. У зв'язку з цим природно виникає питання про будову локальних майже-кілець з циклічними підгрупами необоротних елементів. Очевидно, що кожне майже-поле має цю властивість.

У наступній теоремі (див. [42]) описано скінченні локальні майже-кільця, підгрупи необоротних елементів яких є циклічними.

Теорема 7. *Нехай R — локальне майже-кільце порядку p^n з $n > 1$, підгрупа L необоротних елементів якого циклічна та нетривіальна. Тоді його адитивна група R^+ або сама циклічна, або є елементарною абелевою групою порядку p^2. У 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 напівпрямому добутку двох циклічних підгруп порядків p та $p-1$.*

Локальні майже-кільця на метациклічних групах Міллера — Морено. Питання існування локальних майже-кілець на метациклічних групах Міллера — Морено було досліджено в статті [43].

Нехай R — локальне майже-кільце, адитивна група R^+ якого ізоморфна групі $G(p^m, p^n)$. Тоді $R^+ = \langle a \rangle + \langle b \rangle$ з елементами a, b, що задовольняють співвідношення $ap^m = bp^n = 0$ та $a + b = b + a(1 + p^{m-1})$. Крім того, $\langle a \rangle$ є нормальною підгрупою в R^+ та кожний елемент $x \in R$ єдиним чином записується у вигляді $x = ax_1 + bx_2$ з коефіцієнтами $0 \leq x_1 < p^m$ та $0 \leq x_2 < p^n$.

Оскільки, як зазначено вище, локальних майже-кілець з адитивною групою кватерніонів не існує, то розглядались локальні майже-кільця, адитивна група яких ізоморфна групі $G(p^m, p^n)$. Наступна теорема характеризує основні властивості таких майже-кілець за умови, що вони існують.

Теорема 8. *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 такі твердження:*

1) *$ap^m = bp^n = 0$ та $a + b = b + a(1 + p^{m-1})$;*
2) *якщо a — одиничний елемент в R, то $m > n$, $L = \langle a \cdot p \rangle + \langle b \rangle$ та*
$$R^* = \{ax_1 + bx_2 \mid x_1 \not\equiv 0 \pmod p\};$$
3) *якщо b — одиничний елемент в R, то $p = 2$, $m \leq n$, $L = \langle a \rangle + \langle b \cdot 2 \rangle$ та*
$$R^* = \{ax_1 + bx_2 \mid x_2 \equiv 1 \pmod 2\}.$$

Спираючись на цей результат, знайдено необхідні та достатні умови, за яких група $G(p^m, p^n)$

є адитивною групою деякого локального майже-кільця, і в такий спосіб отримано повну класифікацію таких адитивних груп.

Теорема 9. *Для довільного простого числа p та таких натуральних чисел m, n, що $m > n > 1$ або $p = 2$ та $1 < m \leq n$, існує локальне майже-кільце R, адитивна група R^+ якого ізоморфна групі $G(p^m, p^n)$.*

Локальні майже-кільця на неметациклічних групах Міллера — Морено. У працях [44] та [45] вивчались локальні майже-кільця на неметациклічних групах Міллера — Морено.

Нехай адитивна група локального майже-кільця R ізоморфна групі $G(p^m, p^n, p)$ для підходящих простого p та натуральних чисел m, n, тоді $R^+ = \langle a\rangle + \langle b\rangle + \langle c\rangle$ з елементами a, b та c, що задовольняють співвідношення $ap^m = bp^n = 0$, $-b + a + b = a + c$ та $-b + c + b = c$, причому a є одиничним елементом в R та кожний елемент $x \in R$ однозначно записується у вигляді $x = ax_1 + bx_2 + cx_3$ з коефіцієнтами $0 \leq x_1 < p^m$, $0 \leq x_2 < p^n$ та $0 \leq x_3 < p$. Зокрема, для кожного $x \in R$ виконується рівність $xa = ax = x$ та існують однозначно визначені відображення $\alpha : R \to \mathbb{Z}_{p^m}$, $\beta : R \to \mathbb{Z}_{p^n}$ та $\gamma : R \to \mathbb{Z}_p$, для яких

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

Теорема 10. *Виконуються такі твердження:*
1) *$L = \langle a \cdot p\rangle + \langle b\rangle + \langle c\rangle$ та, зокрема, L — підгрупа індексу p в R^+;*
2) *елемент $x = ax_1 + bx_2 + cx_3$ є оборотним тоді і тільки тоді, коли $x_1 \not\equiv 0 \pmod p$.*

Що стосується неметациклічних p-груп Міллера — Морено, тобто груп $G(p^m, p^n, p)$, то доведено, що кожна така група порядку $p^n > 8$ є адитивною групою деякого локального майже-кільця, причому мультиплікативна група кожного такого майже-кільця має порядок $p^{n-1}(p-1)$. Більш того, оскільки в групі $G(p^m, p^n, p)$, записаній адитивно, кожний елемент $x = ax_1 + bx_2 + cx_3$ єдиним чином задається коефіцієнтами $0 < x_1 < p^m$, $0 < x_2 < p^n$ та $0 < x_3 < p$, то операцію множення можна записати в явному вигляді.

Теорема 11. *У групі $G = G(p^m, p^n, p)$ операція «$*$», задана як*

$$x * y = a(x_1y_1 + p^k x_2y_2) + b(x_2y_1 + x_1y_2) + \\ + c(-x_1x_2\binom{y_1}{2} + x_3y_1 + x_1^2y_3),$$

є асоціативною та ліво-дистрибутивною по відношенню до операції «$+$» групи G та визначає деяке нуль-симетричне локальне майже-кільце $(G, +, *)$.

Локальні майже-кільця на розщеплювальних метациклічних групах. Нагадаємо, що група G називається метациклічною, якщо існує така нормальна підгрупа $\langle a\rangle$, що фактор-група $G/\langle a\rangle$ є циклічною. Для простого p метациклічна p-група G є розщеплювальною, якщо і тільки якщо вона розкладається в напівпрямий добуток $G = \langle a\rangle \rtimes \langle b\rangle$ циклічної нормальної підгрупи $\langle a\rangle$ та циклічної підгрупи $\langle b\rangle$.

Нехай R — локальне майже-кільце, адитивна група R^+ якого є неабелевою розщеплювальною метациклічною p-групою. Тоді група R^+ породжується елементами a та b порядків p^m та p^n, відповідно, один з яких збігається з одиничним елементом з R та $a + b = b + a(1 + p^{m-r})$, якщо R^+ є ізоморфною групі $G(p^m, p^n, r)$, та $a + b = b + a(-1 + 2^{m-r})$, якщо R^+ є ізоморфною групі $G(2^m, 2^n, -r)$.

У наступних теоремах (див. [46]) отримано класифікацію розщеплюваних метациклічних груп, які є адитивними групами локальних майже-кілець.

Теорема 12. *Нехай R — локальне майже-кільце, адитивна група R^+ якого ізоморфна групі $G(p^m, p^n, r)$. Тоді $R^+ = \langle a\rangle + \langle b\rangle$, один з елементів a або b збігається з одиницею в R та виконуються такі твердження:*
1) *$ap^m = bp^n = 0$ та $a + b = b + a(1 + p^{m-r})$ з $1 \leq r < \min\{m, n+1\}$ та $r < m - 1$ для $p = 2$;*
2) *якщо a є одиницею в R, то $m \geq n + r \geq 2r$, $L = \langle ap\rangle + \langle b\rangle$ та*
$$R^* = \{ax_1 + bx_2 \mid x_1 \not\equiv 0 \pmod p\};$$
3) *якщо b є одиницею в R, то $p = 2 < m \leq n$, $r = 1$, $L = \langle a\rangle + \langle b2\rangle$ та*
$$R^* = \{ax_1 + bx_2 \mid x_2 \equiv 1 \pmod 2\}.$$

Теорема 13. *Нехай R — локальне майже-кільце, адитивна група R^+ якого ізоморфна групі $G(2^m, 2^n, -r)$. Тоді $R^+ = \langle a\rangle + \langle b\rangle$, елемент b є одиницею в R та виконуються такі твердження:*
1) *$r + 1 < m \leq n$ та $0 \leq r \leq 1$;*
2) *$a2^m = b2^n = 0$ та $a + b = b + a(-1 + 2^{m-r})$;*
3) *$L = \langle a\rangle + \langle b2\rangle$ та*
$$R^* = \{ax_1 + bx_2 \mid x_2 \equiv 1 \pmod 2\}.$$

Мультиплікативні групи локальних майже–кілець. Як відомо, теорія груп оборотних елементів виникла як одна з областей застосування груп і бере свій початок із вивчення мультиплікативних груп полів. Починаючи з XIX століття у цьому напрямку було одержано значну кількість результатів, багато з яких є класичними: теорема Діріхле про групи оборотних елементів у полях алгебраїчних чисел, опис Гензеля групи одиниць поля p-адичних чисел, будова мультиплікативних груп полів Ґалуа. На сьогодні охарактеризовано мультиплікативну структуру всіх найбільш важливих класів полів.

Наступним природним кроком був перехід до вивчення груп одиниць «некомутативних полів» (тобто тіл). Одна з перших задач на цьому шляху була пов'язана з класичною теоремою Ваддербарна, яка говорить, що кожне скінченне тіло є полем. А саме: з цієї теореми випливає, що кожна скінченна підгрупа мультиплікативної групи тіла ненульової характеристики циклічна. Проте у випадку тіла характеристики нуль це твердження неправильне, і тому виникає питання про класифікацію скінченних груп, які можуть бути підгрупами мультиплікативної групи тіла характеристики нуль. Цю проблему повністю розв'язав Аміцур (1955 р.).

Значна увага також була зосереджена на вивченні будови кілець, мультиплікативна група яких задовольняє деякі узагальнення абелевості (зокрема умови нільпотентності та розв'язності).

Доволі детальна інформація про будову мультиплікативних груп тіл дала змогу дослідникам вивчати більш широкі класи асоціативних кілець із заданими групами оборотних елементів. Наприклад, Джілмер [47] описав усі скінченні локальні кільця з циклічною групою одиниць.

Низку праць було спрямовано на встановлення взаємозв'язків між локальним майже-кільцем та його мультиплікативною групою.

Мультиплікативні групи скінченних майже-полів вивчав Цассенхауз. Лай [48] надав повну характеризацію скінченних спадкових груп майже-полів.

Властивості локальних майже-кілець із комутативною групою одиниць вивчав Городник [49]. Зокрема, він описав локальні майже-кільця з циклічними групами одиниць. А саме: якщо мультиплікативна група локального майже-кільця є циклічною, то адитивна група є або групою типу $(2,2,2)$, або $(2,4)$.

У статті [36] досліджено локальні майже-кільця з мультиплікативною групою діедра та доведено, що кожне локальне майже-кільце з мультиплікативною групою діедра є скінченним з адитивною групою, яка є або 3-групою порядку не вище 9, або 2-групою порядку не вище 32. Опис таких майже-кілець було продовжено в дисертації Хуберта [50], зокрема, було встановлено, що якщо мультиплікативна група локального майже-кільця є групою діедра, то порядок цього майже-кільця не перевищує 16.

Сисак та Ді Терміні в [51] показали, що якщо R є локальним майже-кільцем (не обов'язково нуль-симетричним), мультиплікативна група якого є узагальненою групою кватерніонів, то мультиплікативна група є або групою кватерніонів порядку 8, або узагальненою групою кватерніонів порядку 16 з абелевими адитивними групами таких типів: $(3,3)$, $(2,2,2,2)$, $(2,2,4)$, $(2,2,2,2,2)$ та $(2,2,2,4)$, а підгрупа необоротних елементів є тривіальною в першому випадку та елементарною абелевою індексу 2 в інших.

Наступним природним кроком є дослідження майже-полів та локальних майже-кілець, мультиплікативна група яких є групою Міллера — Морено, тобто мінімальною неабелевою. Майже-поля із зазначеною властивістю описали автори в статті [52].

У наступній теоремі (див. [53]) описано локальні майже-кільця порядку 2^n з мультиплікативною групою Міллера — Морено.

Теорема 14. *Нехай R — локальне майже-кільце порядку 2^n, мультиплікативна група якого є групою Міллера–Морено, та L підгрупа всіх необоротних елементів з R. Тоді $n \geq 4$ та виконуються такі твердження:*

I) *якщо R — майже-поле, то R^* — група Міллера — Морено порядку* 63;

II) *якщо $|R : L| > 2$, то R^+ — група порядку 2^{2p} та експоненти не вище 4, де p — просте число, для якого число $2^p - 1$ є простим числом Мерсенна, R^* — група Міллера — Морено порядку $2^p(2^p - 1)$ та L — елементарна абелева 2-група, в якій $xy = 0$ для всіх $x, y \in L$;*

III) *якщо $|R : L| = 2$, то при $n \geq 7$ підгрупа L абелева, а R^* — неметациклічна група Міллера — Морено порядку 2^{n-1} та експоненти не вище 2^{n-4}.*

Оскільки майже-поля з мультиплікативною групою Шмідта повністю описано в статті одного з авторів [54], то далі було досліджено локальні майже-кільця, підгрупи необоротних елементів яких є нетривіальними. Підсумовуючи, отримаємо таку теорему (див. [55]).

Теорема 15. *Нехай R — локальне майже-кільце порядку p^n, мультиплікативна група R^* якого є групою Шмідта, та не є майже-полем. Тоді виконуються такі твердження:*

I) *якщо R — майже-поле, то R^* — або неабелева метациклічна група одного з порядків* 24, 63, 80, *або група* $SL(2,3)$;

II) *якщо $p > 2$, то $|R| = p^2$ для деякого простого числа Ферма p, адитивна група R^+ є елементарною абелевою та існує такий необоротний елемент a із R, що $R^+ = \langle i \rangle + \langle a \rangle$, де i — одиниця в R, $a^2 = 0$ та $(ik)a = -ak$ для довільного первісного кореня k за модулем p. Зокрема, для кожного простого числа Ферма p існує єдине локальне майже-кільце порядку p^2, мультиплікативна група якого є групою Міллера — Морено*;

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

Система комп'ютерної алгебри GAP та локальні майже-кільця

Розробку системи комп'ютерної алгебри GAP (Groups, Algorithms and Programming) було розпочато у 1986 році в місті Аахен, Німеччина. Спочатку систему GAP розробляли під Unix, а потім адаптували для роботи в інших операційних системах. Зауважимо, що ряд пакетів, які розширюють функціональність системи, працює тільки в середовищі Unix/Linux. Поточна версія системи — GAP 4.8.10.

Система GAP є вільно розповсюджуваною, відкритою та розширюваною. Разом із системою розповсюджується багато нових версій пакетів для неї.

Система складається з чотирьох основних компонент:

- ядра системи, що забезпечує підтримку мови GAP, роботу з системою в програмному та інтерактивному режимах;
- бібліотеки функцій, в яких реалізовано різноманітні алгебраїчні алгоритми;
- бібліотеки даних, яка містить, наприклад, бібліотеку всіх груп порядку не більшого за 2000 (за винятком 49487365422 груп порядку 1024), що в сукупності є ефективним засобом висування та тестування наукових гіпотез;
- документації, що доступна в різних форматах, а також через Інтернет.

Групи в системі GAP можуть бути задані в різній формі, наприклад, як групи підстановок, матричні групи та ін. Окремі групи задані безпосередньо як бібліотечні функції (наприклад, симетрична та знакозмінна групи, група діедра, циклічна група та ін.). Кожна група з бібліотеки задана в ній типом ізоморфізму у вигляді пари $[n, m]$, де n — порядок групи та m — її номер у списку всіх неізоморфних груп порядку n. Групу, яка має тип $[n, m]$, можна викликати з бібліотеки за допомогою функції *SmallGroup*. Наприклад, група кватерніонів Q_8 задається як

```
G:=SmallGroup(8,4);
```

Пакет SONATA [56] (абревіатура від «Systems of nearrings and their applications») — це пакет для побудови та аналізу скінченних майже-кілець. У цьому пакеті міститься бібліотека всіх 68659 майже-кілець порядку меншого за 16, та всіх майже-кілець з одиницею порядку меншого за 32, а також різноманітні функції для аналізу структури та елементів скінченних майже-кілець. Кожне майже-кільце N з бібліотеки пакета SONATA задається парою (G, n), в якій G — група підстановок, ізоморфна адитивній групі N^+, та n — номер майже-кільця N у списку всіх неізоморфних майже-кілець з адитивною групою, ізоморфною G. Кількість m

Таблиця 1

ІдГрупи (R^+)	Структурний опис	ІдГрупи (L)	Структурний опис
$[4,1]$	C_4	$[2,1]$	C_2
$[4,2]$	$C_2\times C_2$	$[2,1]$	C_2
$[8,1]$	C_8	$[4,1]$	C_4
$[8,2]$	$C_4\times C_2$	$[4,2]$	$C_2\times C_2$
$[8,5]$	$C_2\times C_2\times C_2$	$[4,2]$	$C_2\times C_2$
$[9,1]$	C_9	$[3,1]$	C_3
$[9,2]$	$C_3\times C_3$	$[3,1]$	C_3
$[16,1]$	C_{16}	$[8,1]$	$C_4\times C_2$
$[16,2]$	$C_4\times C_4$	$[8,2]$	$C_4\times C_2$
$[16,3]$	$(C_4\times C_2)\rtimes C_2$	$[8,5]$	$C_2\times C_2\times C_2$
$[16,4]$	$C_4\rtimes C_4$	$[8,2]$	$C_4\times C_2$
$[16,5]$	$C_8\times C_2$	$[8,2]$	$C_4\times C_2$
$[16,6]$	$C_8\times C_2$	$[8,2]$	$C_4\times C_2$
$[16,10]$	$C_4\times C_2\times C_2$	$[8,5]$	$C_2\times C_2\times C_2$
$[16,12]$	$C_2\times Q_8$	$[4,2]$	$C_2\times C_2$
$[16,14]$	$C_2\times C_2\times C_2\times C_2$	$[8,5]$	$C_2\times C_2\times C_2$
$[16,14]$	$C_2\times C_2\times C_2\times C_2$	$[4,2]$	$C_2\times C_2$
$[25,1]$	C_{25}	$[5,1]$	C_5
$[25,2]$	$C_5\times C_5$	$[5,1]$	C_5
$[27,1]$	C_{27}	$[9,1]$	C_9
$[27,2]$	$C_9\times C_3$	$[9,2]$	$C_3\times C_3$
$[27,3]$	$(C_3\times C_3)\rtimes C_3$	$[9,2]$	$C_3\times C_3$
$[27,4]$	$C_9\rtimes C_3$	$[9,2]$	$C_3\times C_3$
$[27,5]$	$C_3\times C_3\times C_3$	$[9,2]$	$C_3\times C_3$

майже-кілець на заданій групі визначається однією з команд

```
m:=Size(AllLibraryNearRings(G));
```

або

```
m:=Size(
  AllLibraryNearRingsWithOne(G));
```

Майже-кільце N можна викликати з бібліотеки, відповідно, командами

```
N:=LibraryNearRing(G,n);
```

або

```
N:=LibraryNearRingWithOne(G,n);
```

У першому випадку G — група порядку не вище 15, і тоді N не обов'язково матиме мультиплікативну одиницю, а в другому — порядок G не перевищує 31 та N є майже-кільцем з одиницею.

Локальні майже-кільця з пакета SONATA. Щоб визначити, чи буде вибране майже-кільце R локальним, за допомогою команди

```
u:=Size(NearRingUnits(R));
```

знаходимо порядок u мультиплікативної групи R^* цього майже-кільця. Далі за допомогою команди

Таблиця 2

ІдГрупи(G), $n(G)$	ІдГрупи(R^*)	Структурний опис	$n(R^*)$
$[4,1]$ 1	$[2,1]$	C_2	1
$[4,2]$ 2	$[2,1]$	C_2	2
$[8,1]$ 1	$[4,2]$	$C_2\times C_2$	1
$[8,2]$ 5	$[4,1]$	C_4	2
	$[4,2]$	$C_2\times C_2$	3
$[8,5]$ 6	$[4,1]$	C_4	2
	$[4,2]$	$C_2\times C_2$	4
$[9,1]$ 1	$[6,2]$	C_6	1
$[9,2]$ 3	$[6,1]$	S_3	2
	$[6,2]$	C_6	1
$[16,1]$ 1	$[8,2]$	$C_4\times C_2$	1
$[16,2]$ 29	$[8,2]$	$C_4\times C_2$	10
	$[8,3]$	D_8	9
	$[8,5]$	$C_2\times C_2\times C_2$	6
	$[12,3]$	A_4	2
	$[12,5]$	$C_6\times C_2$	2

ІдГрупи(G), $n(G)$	ІдГрупи(R^*)	Структурний опис	$n(R^*)$
$[16,3]$ 37	$[8,2]$	$C_4\times C_2$	14
	$[8,3]$	D_8	17
	$[8,5]$	$C_2\times C_2\times C_2$	6
$[16,4]$ 24	$[8,2]$	$C_4\times C_2$	7
	$[8,3]$	D_8	10
	$[8,5]$	$C_2\times C_2\times C_2$	7
$[16,5]$ 33	$[8,2]$	$C_4\times C_2$	8
	$[8,3]$	D_8	16
	$[8,5]$	$C_2\times C_2\times C_2$	9
$[16,6]$ 33	$[8,2]$	$C_4\times C_2$	8
	$[8,3]$	D_8	17
	$[8,5]$	$C_2\times C_2\times C_2$	8
$[16,10]$ 251	$[8,2]$	$C_4\times C_2$	96
	$[8,3]$	D_8	90
	$[8,4]$	Q_8	24
	$[8,5]$	$C_2\times C_2\times C_2$	41
$[16,12]$ 2	$[12,3]$	A_4	2
$[16,14]$ 229	$[8,2]$	$C_4\times C_2$	84
	$[8,3]$	D_8	77
	$[8,4]$	Q_8	24

ІдГрупи(G), $n(G)$	ІдГрупи(R^*)	Структурний опис	$n(R^*)$
	$[8,5]$	$C_2\times C_2\times C_2$	37
	$[12,3]$	A_4	5
	$[12,5]$	$C_6\times C_2$	2
$[25,1]$ 1	$[20,2]$	C_{20}	1
$[25,2]$ 5	$[20,1]$	$C_5\rtimes C_4$	1
	$[20,2]$	C_{20}	1
	$[20,3]$	$C_5\rtimes C_4$	3
$[27,1]$ 1	$[18,2]$	C_{18}	1
$[27,2]$ 13	$[18,3]$	$C_3\times S_3$	4
	$[18,5]$	$C_6\times C_3$	9
$[27,3]$ 4	$[18,3]$	$C_3\times S_3$	4
$[27,4]$ 4	$[18,3]$	$C_3\times S_3$	4
$[27,5]$ 12	$[18,3]$	$C_3\times S_3$	3
	$[18,4]$	$(C_3\times C_3)\rtimes C_2$	4
	$[18,5]$	$C_6\times C_3$	5

```
Id:=NearRingIdeals(R);
```

визначаємо список усіх ідеалів майже-кільця R, а командою

```
Ord:=List(Id,Size);
```

— відповідний список їх порядків. Найбільший із 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, *ІдГрупи*(R^+) тип групи G у бібліотеці *AllSmallGroups* системи GAP.

Наступні два твердження легко отримати з результатів статті [42].

Твердження 16. *Нехай R — локальне майже-кільце порядку не вище 31, яке не є майже-полем. Тоді група R^+ та її підгрупа L є такими (див. табл. 1).*

Наступне твердження містить кількість неізоморфних локальних майже-кілець порядку не вище 31, які не є майже-полями, із заданими адитивними та мультиплікативними групами.

Твердження 17. *Нехай $n(G)$ — кількість усіх неізоморфних локальних майже-кілець R порядку не вище 31, які не є майже-полями, адитивна група R^+ яких ізоморфна групі G. Якщо $n(R^*)$ — кількість цих майже-кілець, для яких ІдГрупи(R^*) є фіксованим, то виконується таке (див. табл. 2).*

Таблиця 3

ІдГрупи (R^+)	Структурний опис	ІдГрупи (L)	Структурний опис
$[32,1]$	C_{32}	$[16,1]$	C_{16}
$[32,2]$	$(C_4\times C_2)\rtimes C_4$	$[16,10]$	$C_4\times C_2\times C_2$
$[32,3]$	$C_8\times C_4$	$[16,2]$	$C_4\times C_4$
$[32,4]$	$C_8\rtimes C_4$	$[16,2]$	$C_4\times C_4$
$[32,5]$	$(C_8\times C_2)\rtimes C_2$	$[16,10]$	$C_4\times C_2\times C_2$
$[32,6]$	$((C_4\times C_2)\rtimes C_2)\rtimes C_2$	$[16,11]$	$C_2\times D_8$
$[32,7]$	$(C_8\rtimes C_2)\rtimes C_2$	$[16,11]$	$C_2\times D_8$
$[32,8]$	$C_2.((C_4\times C_2)\rtimes C_2)$	$[16,12]$	$C_2\times Q_8$
$[32,12]$	$C_4\rtimes C_8$	$[16,2]$	$C_4\times C_4$
$[32,16]$	$C_{16}\times C_2$	$[16,5]$	$C_8\times C_2$
$[32,17]$	$C_{16}\rtimes C_2$	$[16,5]$	$C_8\times C_2$
$[32,21]$	$C_4\times C_4\times C_2$	$[16,10]$	$C_4\times C_2\times C_2$
$[32,22]$	$C_2\times((C_4\times C_2)\rtimes C_2)$	$[16,14]$	$C_2\times C_2\times C_2\times C_2$
$[32,23]$	$C_2\times(C_4\rtimes C_4)$	$[16,10]$	$C_4\times C_2\times C_2$
$[32,24]$	$(C_4\times C_4)\rtimes C_2$	$[16,10]$	$C_4\times C_2\times C_2$
$[32,36]$	$C_8\times C_2\times C_2$	$[16,10]$	$C_4\times C_2\times C_2$
$[32,37]$	$C_2\times(C_8\rtimes C_2)$	$[16,10]$	$C_4\times C_2\times C_2$
$[32,45]$	$C_4\times C_2\times C_2\times C_2$	$[16,14]$	$C_2\times C_2\times C_2\times C_2$
$[32,51]$	$C_2\times C_2\times C_2\times C_2\times C_2$	$[16,14]$	$C_2\times C_2\times C_2\times C_2$

Таблиця 4

ІдГрупи(G), $n(G)$	ІдГрупи (R^*)	Структурний опис	$n(R^*)$	ІдГрупи(G), $n(G)$	ІдГрупи (R^*)	Структурний опис	$n(R^*)$
$[32,1]$	$[16,5]$	$C_8 \times C_2$	1		$[16,10]$	$C_4 \times C_2 \times C_2$	14457
1					$[16,11]$	$C_2 \times D_8$	66579
$[32,2]$	$[16,3]$	$(C_4 \times C_2) \rtimes C_2$	369		$[16,12]$	$C_2 \times Q_8$	4368
1397	$[16,10]$	$C_4 \times C_2 \times C_2$	198		$[16,13]$	$(C_4 \times C_2) \rtimes C_2$	49368
	$[16,11]$	$C_2 \times D_8$	764		$[16,14]$	$C_2 \times C_2 \times C_2 \times C_2$	4472
	$[16,14]$	$C_2 \times C_2 \times C_2 \times C_2$	66	$[32,23]$	$[16,3]$	$(C_4 \times C_2) \rtimes C_2$	458
$[32,3]$	$[16,3]$	$(C_4 \times C_2) \rtimes C_2$	208	157905	$[16,4]$	$C_4 \rtimes C_4$	4
880	$[16,10]$	$C_4 \times C_2 \times C_2$	128		$[16,10]$	$C_4 \times C_2 \times C_2$	13414
	$[16,11]$	$C_2 \times D_8$	489		$[16,11]$	$C_2 \times D_8$	85208
	$[16,14]$	$C_2 \times C_2 \times C_2 \times C_2$	55		$[16,12]$	$C_2 \times Q_8$	4416
$[32,4]$	$[16,3]$	$(C_4 \times C_2) \rtimes C_2$	238		$[16,13]$	$(C_4 \times C_2) \rtimes C_2$	49920
798	$[16,10]$	$C_4 \times C_2 \times C_2$	100		$[16,14]$	$C_2 \times C_2 \times C_2 \times C_2$	4485
	$[16,11]$	$C_2 \times D_8$	424	$[32,24]$	$[16,10]$	$C_4 \times C_2 \times C_2$	24576
	$[16,14]$	$C_2 \times C_2 \times C_2 \times C_2$	36	262544	$[16,11]$	$C_2 \times D_8$	123080
$[32,5]$	$[16,3]$	$(C_4 \times C_2) \rtimes C_2$	548		$[16,12]$	$C_2 \times Q_8$	8192
1945	$[16,10]$	$C_4 \times C_2 \times C_2$	232		$[16,13]$	$(C_4 \times C_2) \rtimes C_2$	98504
	$[16,11]$	$C_2 \times D_8$	1077		$[16,14]$	$C_2 \times C_2 \times C_2 \times C_2$	8192
	$[16,14]$	$C_2 \times C_2 \times C_2 \times C_2$	88	$[32,36]$	$[16,3]$	$(C_4 \times C_2) \rtimes C_2$	448
$[32,6]$	$[16,3]$	$(C_4 \times C_2) \rtimes C_2$	64	177175	$[16,10]$	$C_4 \times C_2 \times C_2$	16770
433	$[16,11]$	$C_2 \times D_8$	225		$[16,11]$	$C_2 \times D_8$	83244
	$[16,13]$	$(C_4 \times C_2) \rtimes C_2$	144		$[16,12]$	$C_2 \times Q_8$	5472
$[32,7]$	$[16,3]$	$(C_4 \times C_2) \rtimes C_2$	32		$[16,13]$	$(C_4 \times C_2) \rtimes C_2$	65536
225	$[16,11]$	$C_2 \times D_8$	121		$[16,14]$	$C_2 \times C_2 \times C_2 \times C_2$	5705
	$[16,13]$	$(C_4 \times C_2) \rtimes C_2$	72	$[32,37]$	$[16,3]$	$(C_4 \times C_2) \rtimes C_2$	496
$[32,8]$	$[16,3]$	$(C_4 \times C_2) \rtimes C_2$	32	527419	$[16,10]$	$C_4 \times C_2 \times C_2$	49514
208	$[16,11]$	$C_2 \times D_8$	104		$[16,11]$	$C_2 \times D_8$	247431
	$[16,13]$	$(C_4 \times C_2) \rtimes C_2$	72		$[16,12]$	$C_2 \times Q_8$	16384
$[32,12]$	$[16,3]$	$(C_4 \times C_2) \rtimes C_2$	624		$[16,13]$	$(C_4 \times C_2) \rtimes C_2$	197008
2406	$[16,10]$	$C_4 \times C_2 \times C_2$	312		$[16,14]$	$C_2 \times C_2 \times C_2 \times C_2$	16586
	$[16,11]$	$C_2 \times D_8$	1350	$[32,45]$	$[16,2]$	$C_4 \times C_4$	16435
	$[16,14]$	$C_2 \times C_2 \times C_2 \times C_2$	120	>6684533	$[16,3]$	$(C_4 \times C_2) \rtimes C_2$	40447
$[32,16]$	$[16,10]$	$C_4 \times C_2 \times C_2$	33		$[16,4]$	$C_4 \rtimes C_4$	47904
129	$[16,11]$	$C_2 \times D_8$	16		$[16,5]$	$C_8 \times C_2$	24
	$[16,12]$	$C_2 \times Q_8$	16		$[16,6]$	$C_8 \rtimes C_2$	32
	$[16,13]$	$(C_4 \times C_2) \rtimes C_2$	64		$[16,8]$	QD_{16}	14
$[32,17]$	$[16,10]$	$C_4 \times C_2 \times C_2$	32		$[16,9]$	Q_{16}	14
129	$[16,11]$	$C_2 \times D_8$	16		$[16,10]$	$C_4 \times C_2 \times C_2$	741652
	$[16,12]$	$C_2 \times Q_8$	16		$[16,11]$	$C_2 \times D_8$	2190035
	$[16,13]$	$(C_4 \times C_2) \rtimes C_2$	65		$[16,12]$	$C_2 \times Q_8$	710359
$[32,21]$	$[16,2]$	$C_4 \times C_4$	256		$[16,13]$	$(C_4 \times C_2) \rtimes C_2$	2847717
135558	$[16,3]$	$(C_4 \times C_2) \rtimes C_2$	634		$[16,14]$	$C_2 \times C_2 \times C_2 \times C_2$	>89900
	$[16,4]$	$C_4 \rtimes C_4$	136	$[32,51]$	$[16,2]$	$C_4 \times C_4$	5983
	$[16,5]$	$C_8 \times C_2$	4	>7007053	$[16,3]$	$(C_4 \times C_2) \rtimes C_2$	23205
	$[16,6]$	$C_8 \rtimes C_2$	2		$[16,4]$	$C_4 \rtimes C_4$	17100
	$[16,10]$	$C_4 \times C_2 \times C_2$	13630		$[16,5]$	$C_8 \times C_2$	24
	$[16,11]$	$C_2 \times D_8$	62910		$[16,6]$	$C_8 \rtimes C_2$	32
	$[16,12]$	$C_2 \times Q_8$	4368		$[16,8]$	QD_{16}	14
	$[16,13]$	$(C_4 \times C_2) \rtimes C_2$	49152		$[16,9]$	Q_{16}	14
	$[16,14]$	$C_2 \times C_2 \times C_2 \times C_2$	4466		$[16,10]$	$C_4 \times C_2 \times C_2$	789167
$[32,22]$	$[16,2]$	$C_4 \times C_4$	1024		$[16,11]$	$C_2 \times D_8$	2566765
149374	$[16,3]$	$(C_4 \times C_2) \rtimes C_2$	5936		$[16,12]$	$C_2 \times Q_8$	703803
	$[16,4]$	$C_4 \rtimes C_4$	3120		$[16,13]$	$(C_4 \times C_2) \rtimes C_2$	2808419
	$[16,5]$	$C_8 \times C_2$	20		$[16,14]$	$C_2 \times C_2 \times C_2 \times C_2$	>92527
	$[16,6]$	$C_8 \rtimes C_2$	30				

***Локальні майже-кільця порядку* 32.** Наступні теореми, отримані разом з Я. П. Сисаком, — результат обчислень, виконаних на суперкомп'ютері Інституту кібернетики та кластері Інституту математики НАН України з використанням системи комп'ютерної алгебри GAP.

Зауважимо, що з 51 неізоморфної групи порядку 32 тільки 19 є адитивними групами локальних майже-кілець.

Теорема 18. *Нехай R — локальне майже-кільце порядку* 32. *Тоді група R^+ та її підгрупа L є такими (див. табл. 3).*

Наступна теорема містить кількість неізоморфних локальних майже-кілець порядку 32 із заданими адитивними та мультиплікативними групами.

Теорема 19. *Нехай $n(G)$ — кількість усіх неізоморфних локальних майже-кілець R порядку 32, адитивна група R^+ яких ізоморфна групі G. Якщо $n(R^*)$ — кількість цих майже-кілець, для яких ІдГрупи(R^*) є фіксованим, то виконується таке (див. табл. 4).*

Список літератури

1. Dixon L. Definitions of a group and a field by independent postulates / L. Dixon // Trans. Amer. Math. Soc. — 1905. — Vol. 6. — P. 198–204.
2. Zassenhaus H. Über endliche Fastkörper / H. Zassenhaus // Abh. Math. Sem., Univ. Hamburg. — 1935/36. — Bd. 11. — S. 187–220.
3. Veblen O. Non-desarguesian and non-pascalian geometrie / O. Veblen, J. H. Wedderburn // Trans. Amer. Math. Soc. — 1907. — Vol. 8. — P. 379–388.
4. Холл М. Теория групп / М. Холл. — Москва : Издательство иностранной литературы, 1962. — 468 с.
5. Wähling H. Theorie der Fastkörper / H. Wähling. — Essen : Thales Verlag, 1987. — 393 S.
6. Ore Q. Linear equations in non-commutative fields / Q. Ore // Ann. of Math. — 1931. — Vol. 32. — P. 463–477.
7. Furtwangler P. Über Schiefringe / P. Furtwangler, O. Taussky-Todd // Sitzber. Akad. Wiss. Wien, Math. Nat. Klasse, Abt. IA. — 1936. — Bd. 145. — S. 525.
8. Taussky-Todd O. Rings with non-commutative addition / O. Taussky-Todd // Bull. Calcutta Math. Soc. — 1936. — Vol. 28. — P. 245–246.
9. Blackett D. W. Simple and semi-simple near-rings / D. W. Blackett // Proc. American Math. Soc. — 1953. — Vol. 4. — P. 772–785.
10. Neumann H. Near-rings connected with free groups / H. Neumann // Proc. International Conference. — Amsterdam, 1954. — P. 46–47.
11. Neumann H. On varieties of groups and their assotiated near-rings / H. Neumann // Math. Z. — 1956. — Vol. 65. — P. 36–69.
12. Betsch G. Ein Radikal für Fastringe / G. Betsch // Math. Z. — 1962. — Bd. 78. — S. 86–90.
13. Beidleman J. C. On the theory of radicals of distributively generated near-rings. I. The primitive-radical / J. C. Beidleman // Math. Annalen. — 1967. — Vol. 173. — P. 89–101.
14. Beidleman J. C. On the theory of radicals of distributively generated near-rings. II. The nil-radical / J. C. Beidleman // Math. Annalen. — 1967. — Vol. 173. — P. 200–218.
15. Pilz G. Near-rings. The theory and its applications / G. Pilz. — Amsterdam : North Holland, 1977. — 393 p.
16. Meldrum J. D. P. Near-rings and their links with groups / J. D. P. Meldrum. — London : Pitman Publishing Limited, 1985. — 273 p.
17. Clay J. R. Nearrings. Geneses and Applications / J. R. Clay. — New York : Oxford University Press, 1992. — 469 p.
18. Ferrero C. C. Nearrings. Some developments linked to semigroups and groups / C. C. Ferrero, G. Ferrero. — Dordrecht : Kluwer Academic Publishers, 2002. — 609 p.
19. Калужнин Л. А. Вербальные функции на группах / Л. А. Калужнин, В. И. Сущанский // Теоретические и прикладные вопросы дифференциальных уравнений и алгебра : сб. науч. тр. — Киев : Наук. думка, 1978. — С. 105–110.
20. Clay J. R. The near-rings with identities on certain finite groups / J. R. Clay, Jr. Malone // Math. Scand. — 1966. — Vol. 19. — P. 146–150.
21. Clay J. R. Near-rings with identity on alternating groups / J. R. Clay, D. Doi // Math. Scand. — 1968. — Vol. 23. — P. 54–56.
22. Ligh S. Near rings with identities on certain groups / S. Ligh // Monatsh. Math. — 1971. — Vol. 75. — P. 38–43.
23. Krimmel J. E. A condition on near-rings with identity / J. E. Krimmel // Monatsh. Math. — 1973. — Vol. 77. — P. 52–54.
24. Clay J R. Research in near-ring theory using a digital computer / J. R. Clay // BIT. — 1970. — Vol. 10. — P. 249–265.
25. Clay J. R. The near-rings with identities on generalized quaternion groups / J. R. Clay, C. J. Maxson // Ist. Lombardo Accad. Sci. Lett. Rend. A. — 1970. — Vol. 104. — P. 525–530.
26. Johnson M. J. Near-rings with identities on dihedral groups / M. J. Johnson // Proceedings of the Edinburgh Mathematical Society. — 1973. — Vol. 18. — P. 219–228.
27. GAP — Groups, Algorithms, and Programming, Version 4.8.10 [Electronic resource]. — 2018. — Mode of access: https://www.gap-system.org. — Title from the screen.
28. Boykett T. A class of groups which cannot be the additive groups of near-rings with identity / T. Boykett, C. Nöbauer // Contributions to general algebra 10: Proceedings of the Klagenfurt Conference. — Klagenfurt : Heyn, 1998. — P. 89–99.
29. Miller G. A. Non-abelian groups in which every subgroup is abelian / G. A. Miller, H. Moreno // Trans. Amer. Math. Soc. — 1903. — Vol. 4. — P. 398–404.
30. 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 / L. Redei // Comment. Math. Helv. — 1947. — Bd. 20. — S. 225–264.
31. Raievska I. Yu. Finite nearrings with identity on Miller — Moreno groups / I. Yu. Raievska, M. Yu. Raievska // Mat. Stud. — 2014. — Vol. 42, no. 1. — P. 15–20.
32. Шмидт О. Ю. Группы, все подгруппы которых специальные / О. Ю. Шмидт // Мат. сб. — 1924. — Т. 31. — С. 366–372.
33. Huppert. B. Endliche gruppen I / B. Huppert. — Berlin, Heidelberg, New York : Springer-Verlag, 1967. — 793 S.
34. Раєвська І. Ю. Адитивні групи скінченних майже-кілець з одиницею / І. Ю. Раєвська, М. Ю. Раєвська // Міжнародна конференція молодих математиків, присвячена 100-річчю з дня народження академіка НАН України Ю. О. Митропольського (1917–2008). Тези доповідей. — Київ : Інститут математики НАН України, 2017. — 7–10 червня. — С. 20.
35. Maxson C. J. On local near-rings / C. J. Maxson // Math. Z. — 1968. — Vol. 106. — P. 197–205.
36. Amberg B. Local near-rings with dihedral multiplicative group / B. Amberg, P. Hubert, Ya. Sysak // J. Algebra. — 2004. — Vol. 273. — P. 700–717.
37. Maxson C. J. Local near-rings of cardinality p^2 / C. J. Maxson // Canad. Math. Bull. — 1968. — Vol. 11, no. 4. — P. 555–561.
38. Maxson C. J. On the construction of finite local near-rings (I): on non-cyclic abelian p-groups / C. J. Maxson // Quart. J. Math. Oxford (2). — 1970. — Vol. 21. — P. 449–457.

39. Maxson C. J. On the construction of finite local near-rings (II): on non-abelian p-groups / C. J. Maxson // Quart. J. Math. Oxford (2). — 1971. — Vol. 22. — P. 65–72.
40. Feigelstock S. Additive groups of local near-rings / S. Feigelstock // Comm. Algebra. — 2006. — Vol. 34. — P. 743–747.
41. Sysak Ya. P. Products of groups and local nearrings / Ya. P. Sysak // Note di Mat. — 2008. — Vol. 28, no. 2. — P. 179–213.
42. Раєвська І. Ю. Локальні майже-кільця з обмеженнями на мультиплікативні групи та підгрупи необоротних елементів / І. Ю. Раєвська, М. Ю. Раєвська // Науковий часопис НПУ імені М. П. Драгоманова. Серія 1. Фізико-математичні науки. — 2013. — № 14. — С. 134–145.
43. Raievska I. Yu. Finite local nearrings on metacyclic Miller — Moreno p-groups / I. Yu. Raievska, Ya. P. Sysak // Algebra Discrete Math. — 2012. — Vol. 13, no. 1. — P. 111–127.
44. Раєвська І. Ю. Локальні майже-кільця на неметациклічній p-групі Міллера — Морено / І. Ю. Раєвська // Вісн. Київ. ун-ту. Математика. Механіка. — 2011. — Т. 25. — С. 43–45.
45. Раєвська І. Ю. Локальні майже-кільця на неметациклічних групах Міллера — Морено / І. Ю. Раєвська, М. Ю. Раєвська, Я. П. Сисак // Вісн. Київ. ун-ту. Серія: фіз.-мат. науки. — 2012. — Т. 3. — С. 39–46.
46. Raievska I. Yu. Finite local nearrings with split metacyclic additive group / I. Yu. Raievska, M. Yu. Raievska, Ya. P. Sysak // Algebra Discrete Math. — 2016. — Vol. 22, no. 1. — P. 129–152.
47. Gilmer R. W. Finite rings, having a cyclic group of units / R. W. Gilmer // Amer. J. Math. — 1963. — Vol. 85, no. 3. — P. 447–452.
48. Ligh S. Finite hereditary near-field groups / S. Ligh // Monatsh. Math. — 1978. — Vol. 86. — P. 7–11.
49. Gorodnik A. Local near-rings with commutative groups of units / A. Gorodnik // Houston J. Math. — 1999. — Vol. 25. — P. 223–234.
50. Hubert P. Nearrings and a construction of triply factorized groups : dis. ... Doktor der Naturwissenschaften am Fachbereich Physik, Mathematik und Informatik / P. Hubert. — Mainz, 2005. — 146 p.
51. Sysak Ya. P. Local nearrings with generalized quaternion multiplicative group / Ya. P. Sysak, S. Di Termini // Ricerche Mat. — 2007. — Vol. 56. — P. 61–72.
52. Раєвська І. Ю. Майже-поля з неабелево спадковими мультиплікативними групами / І. Ю. Раєвська, М. Ю. Раєвська // Мат. студії. — 2010. — Т. 34, № 1. — С. 38–43.
53. Раєвська М. Ю. Про локальні майже-кільця з мультиплікативною групою Міллера — Морено / М. Ю. Раєвська, Я. П. Сисак // Укр. мат. журн. — 2012. — Т. 64, № 6. — С. 811–818.
54. Раєвська М. Ю. Локальні майже-кільця з мультиплікативною групою Міллера — Морено / М. Ю. Раєвська // Вісн. Київ. ун-ту. Математика. Механіка. — 2011. — Т. 25. — С. 45–48.
55. Raievska I. Yu. Finite local nearrings with multiplicative Schmidt group / I. Yu. Raievska, M. Yu. Raievska, Ya. P. Sysak // XI International School-Conference on Group Theory, dedicated to the 70th anniversary of A. Yu. Olshanskii. Abstracts. — Krasnoyarsk : Siberian Federal University, 2016. — July 27 – August 2. — P. 78–79.
56. Aichinger E., Binder F., Ecker J., Mayr P., Nöbauer C. — SONATA — system of near-rings and their applications, GAP package, Version 2.8 [Electronic resource]. — 2015. — Mode of access: http://www.algebra.uni-linz.ac.at/Sonata/. — Title from the screen.

I. Raievska, M. Raievska

FINITE LOCAL NEARRINGS

Nearrings arise naturally in the study of systems of nonlinear mappings, and they have been studied for many decades. Basic definitions and many results concerning nearrings can be, for instance, found in [G. Pilz. Near-rings. The theory and its applications. North Holland, Amsterdam, 1977].

Nearrings are generalized rings in the sense that the addition need not be commutative and only one distributive law is assumed. Clearly, every associative ring is a nearring, and each group is an additive group of a nearring, but not necessarily of a nearring with identity. The question what group can be an additive group of a nearring with identity is far from solution.

A nearring with identity is called local if the set of all its non-invertible elements is a subgroup of its additive group. A study of local nearrings was initiated by Maxson (1968) who defined a number of their basic properties and proved, in particular, that the additive group of a finite zero-symmetric local nearring is a p-group. The determination of the non-abelian finite p-groups which are the additive groups of local nearrings is an open problem (Feigelstock, 2006).

The list of all local nearrings of order at most 31 can be extracted from the package SONATA (https://www.gap-system.org/Packages/sonata.html) of the computer system algebra GAP (https://www.gap-system.org/).

We observe also that there exist 14 non-isomorphic groups of order $16 = 2^4$ from which 9 are the additive groups of local nearrings. Groups of order $32 = 2^5$ with this property are described. In particular, among 51 non-isomorphic groups of this order only 19 are these additive groups.

In this paper finite local nearrings are studied. Moreover, local nearrings of order at most 32 are classified.

Keywords: local nearring, nearring with identity, additive group, multiplicative group.

Матеріал надійшов 14.05.2018