

Ірина Раєвська, Марина Раєвська¹ (Варшавський університет, Польща;
Інститут математики НАН України, Київ)

ГРУПИ ПОРЯДКУ p^4 ЯК АДИТИВНІ ГРУПИ ЛОКАЛЬНИХ МАЙЖЕ-КІЛЕЦЬ

Near-rings can be considered as a generalization of associative rings. In general, a near-ring is a ring $(R, +, \cdot)$ in which the operation “+” is not necessarily Abelian and at least one distributive law holds. A near-ring with identity is called local if the set of all invertible elements forms a subgroup of the additive group. In particular, every group is an additive group of some near-ring but not of a near-ring with identity. Finding non-Abelian finite p -groups that are additive groups of local near-rings is an open problem.

We considered groups of nilpotency class 2 and 3 of order p^4 as additive groups of local near-rings in [https://arxiv.org/abs/2303.17567 and https://arxiv.org/abs/2309.14342]. It was shown that, for $p > 3$, there exist local near-rings on one of four nonisomorphic groups of nilpotency class 3 of order p^4 . In the present paper, we continue our investigation of the groups of nilpotency class 3 of order p^4 . In particular, it is shown that another group of this class is an additive group of a local near-ring and, hence, of a near-ring with identity. Examples of local near-rings on this group have been constructed in the GAP computer algebra system.

Майже-кілець можна розглядати як узагальнення асоціативних кілець. У загальних рисах, майже-кілець — це кілець $(R, +, \cdot)$, де операція додавання необов'язково абелева та принаймні один дистрибутивний закон має місце. Майже-кілець з одиницею називається локальним, якщо множина всіх необоротних елементів утворює підгрупу в адитивній групі. Зокрема, кожна група є адитивною групою деякого майже-кілеця, але не майже-кілець з одиницею. Визначення неабелевих скінченних p -груп, які є адитивними групами локальних майже-кілець, є відкритою проблемою.

Групи класу нільпотентності 2 та 3 порядку p^4 як адитивні групи локальних майже-кілець розглядалися в [https://arxiv.org/abs/2303.17567 та https://arxiv.org/abs/2309.14342]. Було показано, що для $p > 3$ існують локальні майже-кілець на одній з чотирьох неізоморфних груп класу нільпотентності 3 порядку p^4 . У цій статті продовжено дослідження груп класу нільпотентності 3 порядку p^4 . Зокрема, показано, що ще одна з цих груп є адитивною групою локального майже-кілеця, а отже майже-кілець з одиницею. В системі комп'ютерної алгебри GAP побудовано приклади локальних майже-кілець на цій групі.

1. Вступ. Кожна скінченна абелева група є адитивною групою асоціативного (і навіть комутативного) кілець 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 був отриманий Клейом та Малоне [4], які показали, що з точністю до ізоморфізму існує єдине майже-кілець з одиницею, адитивна група якого циклічна, і яке фактично є комутативним кільцем. Там же було встановлено, що адитивна група скінченного майже-кілець з одиницею є простою тоді й лише тоді, коли це майже-кілець 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.

В роботі [7] доведено, що кожна нециклічна скінченна абелева p -група порядку більшого за 4 є адитивною групою деякого нуль-симетричного локального майже-кілець, що не є кільцем, а в статті [8] показано, що група діедра D_4 не може бути адитивною групою локального майже-

¹ Відповідальна за листування, e-mail: raemarina@imath.kiev.ua.

кільця, та побудовано приклади локальних майже-кілець на неабелевих групах порядку p^n і експоненти p^{n-1} для $n \geq 3$ при $p \neq 2$ і для $n \geq 4$ при $p = 2$.

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

Як було показано у [5], для кожного простого числа p і кожного цілого n з $n > p$ існує група G порядку p^n , яка не може бути адитивною групою локального майже-кілця.

У статті [11] отримано нижні оцінки кількості локальних майже-кілець на групах порядку p^3 . На кожній неметациклічній неабелевій або метациклічній абелевій групі порядку p^3 існують принаймні $p + 1$ неізоморфне локальне майже-кілце. В [9] розглянуто групи класу нільпотентності 2 порядку p^4 , які є адитивними групами локальних майже-кілець. Показано, що для непарних p із шести таких груп чотири є адитивними групами локальних майже-кілець. У статті [10] показано, що для $p > 3$ існують локальні майже-кілця на одній з чотирьох неізоморфних груп класу нільпотентності 3 порядку p^4 . У цій статті продовжено дослідження груп класу нільпотентності 3 порядку p^4 . Зокрема, показано, що ще одна з цих груп є адитивною групою локального майже-кілця, а отже майже-кілця з одиницею. В системі комп'ютерної алгебри GAP [6] побудовано приклади локальних майже-кілець на цій групі.

2. Попередні результати. Непорожня множина R з двома бінарними операціями $+$ і $\cdot$ є (лівим) майже-кілцем, якщо:

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

Означення 1. Майже-кілце R , в якому напівгрупа $(R, \cdot)$ є моноїдом з одиничним елементом i , називається майже-кілцем з одиницею i . Група всіх оборотних елементів цього моноїда позначається через R^* і називається мультиплікативною групою майже-кілця R , а її доповнення $L = R \setminus R^*$ — множиною необоротних елементів із R . Майже-кілце R з одиницею називається локальним, якщо множина L всіх необоротних елементів із $(R, \cdot)$ утворює адитивну підгрупу в R^+ , і майже-полем, якщо $L = 0$.

Майже-кілця з'являються природним чином: беремо множину $M(G)$ всіх відображень групи $(G, +)$ в себе, визначаємо додавання $+$ поелементно та множення $\cdot$ як композицію. Тоді $(M(G), +, \cdot)$ є майже-кілцем. Зауважимо, що якщо G є абелевою групою, то завжди виконується лише один дистрибутивний закон.

Наступна лема визначає експоненту адитивної групи скінченного майже-кілця з одиницею [14] (лема 5).

Лема 1. Експонента адитивної групи скінченного майже-кілця R з одиницею дорівнює адитивному порядку його одиниці, який збігається з адитивним порядком кожного елемента його мультиплікативної групи R^* .

Наступна лема характеризує основні властивості скінчених локальних майже-кілець (див. [2], лема 3.2).

Лема 2. Нехай R — локальне майже-кілце з одиницею i , а L — підгрупа всіх необоротних елементів R . Тоді справджуються такі твердження:

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

У наступному твердженні встановлено порядки підгрупи необоротних елементів L [10] (наслідок 1).

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

Наступна теорема містить класифікацію груп класу нільпотентності 3 порядку p^4 з $p > 3$ (див., наприклад, [1, 3]).

Теорема 1. Існують чотири неізоморфні групи класу нільпотентності 3 порядку p^4 з $p > 3$:

$H_1 = \langle a, b : a^p = b^p = c^p = [a, c]^p = [b, c] = e, [a, [a, c]] = [b, [a, c]] = e \rangle = (C_p \times C_p \times C_p) \rtimes C_p$, де $c = [a, b]$,

$H_2 = \langle a, b : a^{p^2} = b^p = [a, b]^p = [b, [a, b]] = e, [a, [a, b]] = a^p \rangle = (C_{p^2} \rtimes C_p) \rtimes C_p$,

$H_3 = \langle a, b : a^{p^2} = b^p = [a, b]^p = [a, [a, b]] = e, [b, [a, b]] = a^p \rangle = (C_{p^2} \rtimes C_p) \rtimes C_p$,

$H_4 = \langle a, b : a^{p^2} = b^p = [a, b]^p = [a, [a, b]] = e, [b, [a, b]] = a^{2p} \rangle = (C_{p^2} \times C_p) \rtimes C_p$.

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

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

2.1. Про групу H_2 . Нехай H_2 — адитивно записана група з теореми 1. Тоді $H_2 = \langle a \rangle + \langle b \rangle + \langle c \rangle$ для деяких елементів a, b і 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. Для довільних цілих k і m в групі H_2 виконуються рівності $-am - ck + am + ck = aktp$ і $ck + am = am(1 - kp) + ck$.

Доведення. Оскільки $-a - c + a + c = ap$, то отримуємо $-c + a + c = a(1 + p)$. Тоді

$$-ck + am + ck = am(1 + kp).$$

Отже, $-ak - cm + ak + cm = aktp$ і $ck + am = am(1 - kp) + ck$.

Лема 5. Для довільних цілих n і m в групі H_2 виконуються рівності $-bn + am + bn = a\left(m - \binom{m}{2}np\right) + cmn$ і $bn + am = a\left(m + \binom{m}{2}np\right) + bn - cmn$.

Доведення проведемо індукцією по m . Нехай $m = 1$. Оскільки $-a - b + a + b = c$, то $-b + a + b = a + c$. Із співвідношень групи за лемою 4 маємо $-bn + a + bn = a\left(1 - n\binom{1}{2}p\right) + cn$, тому $bn + a = a\left(1 + \binom{1}{2}np\right) + bn - cn$, тобто для $m = 1$ рівність виконується.

Нехай для m виконується рівність, тобто $-bn + am + bn = a\left(m - \binom{m}{2}np\right) + cmn$.

Доведемо рівність для $m + 1$:

$$\begin{aligned} -bn + a(m+1) + bn &= -bn + am + a + bn = -bn + am + bn + a + cn \\ &= -bn + bn + a\left(m - \binom{m}{2}np\right) + cmn + a + cn \end{aligned}$$

$$= a \left(m - \binom{m}{2} np \right) + a(1 - mnp) + cmn + cn$$

$$= a \left((m+1) - \binom{m+1}{2} np \right) + cm(n+1).$$

Отже, $-bn + am + bn = a \left(m - \binom{m}{2} np \right) + cmn$ і $bn + am = a \left(m + \binom{m}{2} np \right) + bn - cmn$.

Лема 6. Для будь-яких невід'ємних цілих k, l, m і натурального r в H_2 має місце рівність

$$(ak + bl + cm)r = a \left(kr + \left(\binom{k}{2} \binom{r}{2} l - km \binom{r}{2} + k^2 l \binom{r}{r-3} \right) p \right) + blr + c \left(mr - kl \binom{r}{2} \right).$$

Доведення проведемо індукцією по r . Нехай $r = 1$. Тоді маємо

$$\begin{aligned} (ak + bl + cm)1 &= a \left(k + \left(\binom{k}{2} \binom{1}{2} l - km \binom{1}{2} + k^2 l \binom{1}{-2} \right) p \right) + bl + c \left(m - \binom{1}{2} kl \right) \\ &= ak + bl + cm. \end{aligned}$$

Отже, для $r = 1$ рівність виконується.

Нехай для r виконується рівність, тобто

$$(ak + bl + cm)r = a \left(kr + \left(\binom{k}{2} \binom{r}{2} l - km \binom{r}{2} + k^2 l \binom{r}{r-3} \right) p \right) + blr + c \left(mr - kl \binom{r}{2} \right).$$

З огляду на леми 4 і 5 доведемо рівність для $r + 1$:

$$\begin{aligned} (ak + bl + cm)(r+1) &= (ak + bl + cm)r + ak + bl + cm \\ &= a \left(kr + \left(\binom{k}{2} \binom{r}{2} l - km \binom{r}{2} + k^2 l \binom{r}{r-3} \right) p \right) \\ &\quad + blr + c \left(mr - kl \binom{r}{2} \right) + ak + bl + cm \\ &= a \left(kr + \left(\binom{k}{2} \binom{r}{2} l - lm \binom{r}{2} + k^2 l \binom{r}{r-3} \right) p \right) \\ &\quad + brl + ak - ak \left(mr - kl \binom{r}{2} \right) p + c \left(mr - kl \binom{r}{2} \right) + bl + cm \\ &= a \left(kr + \left(\binom{k}{2} \binom{r}{2} l - km \binom{r}{2} + k^2 l \binom{r}{r-3} \right) p \right) \\ &\quad + a \left(k - kmrp + k^2 l \binom{r}{2} p + \binom{k}{2} lrp \right) + blr \\ &\quad - clr \left(k - kmrp + k^2 l \binom{r}{2} p \right) + c \left(mr - kl \binom{r}{2} \right) + bl + cm \\ &= a \left(kr + \binom{k}{2} \binom{r}{2} lp - km \binom{r}{2} p \right) \end{aligned}$$

$$\begin{aligned}
& + k^2 l \binom{r}{r-3} p + k - kmr p + k^2 l \binom{r}{2} p + \binom{k}{2} l r p \\
& + bl(r+1) + c \left(m(r+1) - kl \binom{r}{2} - klr \right) \\
& = a \left(k(r+1) + \left(\binom{k}{2} \binom{r+1}{2} l - km \binom{r+1}{2} + k^2 l \binom{r+1}{r-2} \right) p \right) \\
& + bl(r+1) + c \left(m(r+1) - kl \binom{r+1}{2} \right).
\end{aligned}$$

Отже, рівність справедлива для будь-якого r .

Враховуючи властивість симетричності біноміальних коефіцієнтів, тобто $\binom{r}{r-3} = \binom{r}{3}$, і лему 6, отримуємо таке твердження.

Наслідок 1. Для будь-яких невід'ємних цілих k, l, m і натурального r в H_2 має місце рівність

$$(ak + bl + cm)r = a \left(kr + \left(\binom{k}{2} \binom{r}{2} l - km \frac{r}{2} + k^2 l \binom{r}{3} \right) p \right) + blr + c \left(mr - kl \binom{r}{2} \right).$$

2.2. Майже-кільця з одиницею, адитивні групи яких ізоморфні H_2 . Наступна лема описує множення в майже-кільці R , адитивна група якого R^+ ізоморфна групі H_2 . Тоді $R^+ = \langle a \rangle + \langle b \rangle + \langle c \rangle$ для деяких елементів a, b, c з R , що 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 7. Нехай R — майже-кільце з одиницею, адитивна група якого R^+ ізоморфна H_2 . Якщо a збігається з одиничним елементом R , $x = ax_1 + bx_2 + cx_3$, $y = ay_1 + by_2 + cy_3 \in R$ і $xb = a\alpha(x) + b\beta(x) + c\gamma(x)$, то

$$\begin{aligned}
xy &= a \left(x_1 y_1 + \alpha(x) y_2 + \left(\binom{x_1}{2} \binom{y_1}{2} x_2 - x_1 x_3 \binom{y_1}{2} + x_1^2 x_2 \binom{y_1}{3} \right) \right. \\
&+ \left. \binom{\alpha(x) y_2}{2} x_2 y_1 - \alpha(x) x_3 y_1 y_2 - x_1 x_2 \alpha(x) y_2 \binom{y_1}{2} \right. \\
&+ \left. \binom{\alpha(x)}{2} \beta(x) \binom{y_2}{2} - \alpha(x) \gamma(x) \binom{y_2}{2} + \alpha(x)^2 \beta(x) \binom{y_2}{3} \right. \\
&- \left. \binom{x_1}{2} \beta(x) y_3 + \binom{\alpha(x)}{2} x_2 y_3 - x_3 \alpha(x) y_3 \right) p + b(x_2 y_1 + \beta(x) y_2) \\
&+ c \left(x_3 y_1 - x_2 \alpha(x) y_1 y_2 - x_1 x_2 \binom{y_1}{2} + \gamma(x) y_2 \right. \\
&- \left. \alpha(x) \beta(x) \binom{y_2}{2} + x_1 \beta(x) y_3 - x_2 \alpha(x) y_3 \right). \tag{2.1}
\end{aligned}$$

Навіть більше, для відображень $\alpha: R \rightarrow \mathbb{Z}_{p^2}$, $\beta: R \rightarrow \mathbb{Z}_p$, $\gamma: R \rightarrow \mathbb{Z}_p$ справджуються такі твердження:

(0) $\alpha(0) \equiv 0 \pmod{p^2}$, $\beta(0) \equiv 0 \pmod{p}$, $\gamma(0) \equiv 0 \pmod{p}$ тоді й лише тоді, коли майже-кільце R є нуль-симетричним;

$$(1) \alpha(a) \equiv 0 \pmod{p^2}, \beta(a) \equiv 1 \pmod{p}, \gamma(a) \equiv 0 \pmod{p};$$

$$(2) \text{ якщо } x_1 \not\equiv 0 \pmod{p}, \text{ то } x_1\beta(x) - x_2\alpha(x) \equiv 1 \pmod{p};$$

$$(3) xc = a\left(-\binom{x_1}{2}\beta(x) + \binom{\alpha(x)}{2}x_2 - x_3\alpha(x)\right)p + c(x_1\beta(x) - x_2\alpha(x));$$

$$(4) \alpha(xy) \equiv x_1\alpha(y) + \alpha(x)\beta(y) + \left(\binom{x_1}{2}\binom{\alpha(y)}{2}x_2 - x_1x_3\binom{\alpha(y)}{2}\right) \\ + x_1^2x_2\binom{\alpha(y)}{3} + \binom{\alpha(x)\beta(y)}{2}x_2\alpha(y) - \alpha(x)x_3\alpha(y)\beta(y) \\ + x_1x_2\alpha(x)\beta(y)\binom{\alpha(y)}{2} + \binom{\alpha(x)}{2}\beta(x)\binom{\beta(y)}{2} - \alpha(x)\gamma(x)\binom{\beta(y)}{2} \\ + \alpha(x)^2\beta(x)\binom{\beta(y)}{3} + \binom{x_1}{2}\beta(x)\gamma(y) \\ + \binom{\alpha(x)}{2}x_2\gamma(y) - x_3\alpha(x)\gamma(y)\Big)p \pmod{p^2};$$

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

$$(6) \gamma(xy) \equiv x_3\alpha(y) - x_2\alpha(x)\alpha(y)\beta(y) - x_1x_2\binom{\alpha(y)}{2} + \gamma(x)\beta(y) \\ - \alpha(x)\beta(x)\binom{\beta(y)}{2} + x_1\beta(x)\gamma(y) - x_2\alpha(x)\gamma(y) \pmod{p}.$$

Доведення. Оскільки $0 \cdot a = a \cdot 0 = 0$, звідси випливає, що R є нуль-симетричним майже-кільцем тоді й лише тоді, коли $0 = 0 \cdot b = a\alpha(0) + b\beta(0) + c\gamma(0)$ або, еквівалентно, $\alpha(0) \equiv 0 \pmod{p^2}$, $\beta(0) \equiv 0 \pmod{p}$, $\gamma(0) \equiv 0 \pmod{p}$. Навіть більше, 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, справджуються твердження (0) і (1) леми.

Далі, використовуючи леми 4 і 5, отримуємо

$$xc = x(-a - b + a + b) = -xa - xb + xa + xb \\ = -cx_3 - bx_2 - ax_1 - c\gamma(x) - b\beta(x) - a\alpha(x) \\ + ax_1 + bx_2 + cx_3 + a\alpha(x) + b\beta(x) + c\gamma(x) \\ = -cx_3 - bx_2 - c\gamma(x) - ax_1 + ax_1\gamma(x)p - b\beta(x) - a\alpha(x) \\ + ax_1 + bx_2 + a\alpha(x) - ax_3\alpha(x)p + cx_3 + b\beta(x) + c\gamma(x) \\ = -cx_3 - bx_2 - c\gamma(x) - a\binom{x_1}{2}\beta(x)p - b\beta(x) + cx_1\beta(x) \\ - ax_1 + ax_1\gamma(x)p - a\alpha(x) + ax_1 + a\alpha(x) + a\binom{\alpha(x)}{2}x_2p$$

$$\begin{aligned}
& + bx_2 - cx_2\alpha(x) - ax_3\alpha(x)p + cx_3 + b\beta(x) + c\gamma(x) \\
& = a\left(-\binom{x_1}{2}\beta(x) + \binom{\alpha(x)}{2}x_2 - x_3\alpha(x)\right)p + c(x_1\beta(x) - x_2\alpha(x)).
\end{aligned}$$

Отримали рівність (3) леми.

Далі, використовуючи ліву дистрибутивність, на підставі лем 4–6 і наслідку 1 одержуємо

$$\begin{aligned}
xy &= x(ay_1) + x(by_2) + x(cy_3) \\
&= (ax_1 + bx_2 + cx_3)y_1 + (a\alpha(x) + b\beta(x) + c\gamma(x))y_2 \\
&\quad + \left(a\left(-\binom{x_1}{2}\beta(x) + \binom{\alpha(x)}{2}x_2 - x_3\alpha(x)\right)p + c(x_1\beta(x) - x_2\alpha(x))\right)y_3 \\
&= a\left(x_1y_1 + \binom{x_1}{2}\binom{y_1}{2}x_2p - x_1x_3\binom{y_1}{2}p + x_1^2x_2\binom{y_1}{3}p\right) + bx_2y_1 \\
&\quad + c\left(x_3y_1 - x_1x_2\binom{y_1}{2}\right) + a\left(\alpha(x)y_2 + \binom{\alpha(x)}{2}\beta(x)\binom{y_2}{2}p - \alpha(x)\gamma(x)\binom{y_2}{2}p\right. \\
&\quad \left.+ \alpha(x)^2\beta(x)\binom{y_2}{3}p\right) + b\beta(x)y_2 + c\left(\gamma(x)y_2 - \alpha(x)\beta(x)\binom{y_2}{2}p\right) \\
&\quad + a\left(-\binom{x_1}{2}\beta(x) + \binom{\alpha(x)}{2}x_2 - x_3\alpha(x)\right)y_3p + c(x_1\beta(x) - x_2\alpha(x))y_3 \\
&= a\left(x_1y_1 + \binom{x_1}{2}\binom{y_1}{2}x_2p - x_1x_3\binom{y_1}{2}p + x_1^2x_2\binom{y_1}{3}p\right) + bx_2y_1 \\
&\quad + a\alpha(x)y_2 - a\alpha(x)y_2\left(x_3y_1 - x_1x_2\binom{y_1}{2}\right)p + c\left(x_3y_1 - x_1x_2\binom{y_1}{2}\right) \\
&\quad + a\left(\left(\binom{\alpha(x)}{2}\beta(x)\binom{y_2}{2} - \alpha(x)\gamma(x)\binom{y_2}{2} + \alpha(x)^2\beta(x)\binom{y_2}{3}\right)p + b\beta(x)y_2\right. \\
&\quad \left.+ c\left(\gamma(x)y_2 - \alpha(x)\beta(x)\binom{y_2}{2}\right)\right) + a\left(-\binom{x_1}{2}\beta(x) + \binom{\alpha(x)}{2}x_2 - x_3\alpha(x)\right)y_3p \\
&\quad + c(x_1\beta(x) - x_2\alpha(x))y_3 \\
&= a\left(x_1y_1 + \binom{x_1}{2}\binom{y_1}{2}x_2p - x_1x_3\binom{y_1}{2}p + x_1^2x_2\binom{y_1}{3}p + \alpha(x)y_2 + \binom{\alpha(x)y_2}{2}x_2y_1p\right) \\
&\quad + bx_2y_1 - cx_2\alpha(x)y_1y_2 - a\left(\alpha(x)x_3y_1y_2p\right. \\
&\quad \left.+ x_1x_2\alpha(x)y_2\binom{y_1}{2}p\right) + c\left(x_3y_1 - x_1x_2\binom{y_1}{2}\right) \\
&\quad + a\left(\left(\binom{\alpha(x)}{2}\beta(x)\binom{y_2}{2}p - \alpha(x)\gamma(x)\binom{y_2}{2}p + \alpha(x)^2\beta(x)\binom{y_2}{3}p\right)\right)
\end{aligned}$$

$$\begin{aligned}
& + b\beta(x)y_2 + c\left(\gamma(x)y_2 - \alpha(x)\beta(x)\binom{y_2}{2}\right) \\
& + a\left(-\binom{x_1}{2}\beta(x) + \binom{\alpha(x)}{2}x_2 - x_3\alpha(x)\right)y_3p + c(x_1\beta(x) - x_2\alpha(x))y_3 \\
& = a\left(x_1y_1 + \alpha(x)y_2 + \left(\binom{x_1}{2}\binom{y_1}{2}x_2 - x_1x_3\binom{y_1}{2} + x_1^2x_2\binom{y_1}{3}\right.\right. \\
& \quad \left. + \binom{\alpha(x)y_2}{2}x_2y_1 - \alpha(x)x_3y_1y_2 - x_1x_2\alpha(x)y_2\binom{y_1}{2} + \binom{\alpha(x)}{2}\beta(x)\binom{y_2}{2}\right. \\
& \quad \left. - \alpha(x)\gamma(x)\binom{y_2}{2} + \alpha(x)^2\beta(x)\binom{y_2}{3} - \binom{x_1}{2}\beta(x)y_3 + \binom{\alpha(x)}{2}x_2y_3 - x_3\alpha(x)y_3\right)p \\
& \quad + b(x_2y_1 + \beta(x)y_2) + c\left((x_3y_1 - x_2\alpha(x)y_1y_2\right. \\
& \quad \left. - x_1x_2\binom{y_1}{2} + \gamma(x)y_2 - \alpha(x)\beta(x)\binom{y_2}{2} + x_1\beta(x)y_3 - x_2\alpha(x)y_3\right).
\end{aligned}$$

Далі, нехай $y = a(1 - p) + c$, тоді

$$\begin{aligned}
xy &= a\left(x_1(1 - p) + \left(-\binom{x_1}{2}\beta(x) + \binom{\alpha(x)}{2}x_2 - x_3\alpha(x)\right)p\right) \\
&\quad + bx_2 + c(x_3 + x_1\beta(x) - x_2\alpha(x))
\end{aligned}$$

за формулою (2.1). З іншого боку, $y = c + a$, тому

$$\begin{aligned}
xy &= xc + x = a\left(x_1(1 - (x_1\beta(x) - x_2\alpha(x))p)\right) \\
&\quad + \left(-\binom{x_1}{2}\beta(x) + \binom{\alpha(x)}{2}x_2 - x_3\alpha(x)\right)p + bx_2 + c(x_3 + x_1\beta(x) - x_2\alpha(x))
\end{aligned}$$

за лемою 4.

Порівнюючи обидва результати для xy , отримуємо

$$x_1(1 - p) \equiv x_1(1 - (x_1\beta(x) - x_2\alpha(x))p) \pmod{p^2}.$$

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

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

а з іншого —

$$x(yb) = a\left(x_1\alpha(y) + \alpha(x)\beta(y) + \left(\binom{x_1}{2}\binom{\alpha(y)}{2}x_2 - x_1x_3\binom{\alpha(y)}{2} + x_1^2x_2\binom{\alpha(y)}{3}\right)\right.$$

$$\begin{aligned}
& + \binom{\alpha(x)\alpha(y)}{2} x_2 \alpha(y) - \alpha(x) x_3 \alpha(y) \beta(y) + x_1 x_2 \alpha(x) \beta(y) \binom{\alpha(y)}{2} \\
& + \binom{\alpha(x)}{2} \beta(x) \binom{\beta(y)}{2} - \alpha(x) \gamma(x) \binom{\beta(y)}{2} + \alpha(x)^2 \beta(x) \binom{\beta(y)}{3} - \binom{x_1}{2} \beta(x) \gamma(y) \\
& + \left(\binom{\alpha(x)}{2} x_2 \gamma(y) - x_3 \alpha(x) \gamma(y) \right) p + b(x_2 \alpha(y) + \beta(x) \beta(y)) \\
& + c \left(x_3 \alpha(y) - x_2 \alpha(x) \alpha(y) \beta(y) - x_1 x_2 \binom{\alpha(y)}{2} + \gamma(x) \beta(y) \right. \\
& \left. - \alpha(x) \beta(x) \binom{\beta(y)}{2} + x_1 \beta(x) \gamma(y) - x_2 \alpha(x) \gamma(y) \right).
\end{aligned}$$

Порівнюючи коефіцієнти біля a , b і c в двох останніх виразах для xy , одержуємо конгруентності (4)–(6) леми.

2.3. 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 з R , що 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 $0 \leq x_3 < p$.

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 за модулем p^2 , p і p , тому визначені відображення $\alpha: R \rightarrow \mathbb{Z}_{p^2}$, $\beta: R \rightarrow \mathbb{Z}_p$ і $\gamma: R \rightarrow \mathbb{Z}_p$.

За наслідком 3 L є нормальною підгрупою порядку p^3 або p^2 в R .

У цьому підпункті будемо вважати, що R — локальне майже-кільце з $|R : L| = p$.

Теорема 2. Нехай R — локальне майже-кільце, адитивна група якого R^+ ізоморфна H_2 і $|R : L| = p$. Тоді $R^+ = \langle a \rangle + \langle b \rangle + \langle c \rangle$ для деяких елементів a, b, c з R , що 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 справджуються такі твердження:

- 1) $L = \langle ap \rangle + \langle b \rangle + \langle c \rangle$ і $R^* = \{ax_1 + bx_2 + cx_3 \mid x_1 \not\equiv 0 \pmod{p}\}$;
- 2) $\alpha(x) \equiv 0 \pmod{p}$;
- 3) $xc = a \left(-\binom{x_1}{2} \beta(x) \right) p + c(x_1 \beta(x))$.

Доведення. Якщо $|L| = p^3$, то $L = \langle ap \rangle + \langle b \rangle + \langle c \rangle$ і L є (R, R) -підгрупою R^+ . Із твердження (1) леми 2 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 $\alpha(x) \equiv 0 \pmod{p}$, тому справджується твердження (2) теореми. Оскільки $R^* = R \setminus L$, то $R^* = \{ax_1 + bx_2 + cx_3 \mid x_1 \not\equiv 0 \pmod{p}\}$ і $x = ax_1 + bx_2 + cx_3$ є оберненим тоді й лише тоді, коли $x_1 \not\equiv 0 \pmod{p}$, як стверджується в умові (1). Далі, підставляючи $\alpha(x) \equiv 0 \pmod{p}$ у твердження (3) леми 7, отримуємо

$$xc = a \left(-\binom{x_1}{2} \beta(x) \right) p + c(x_1 \beta(x)).$$

Як наслідок леми 7 і теореми 2 одержуємо таке твердження.

Наслідок 2. Нехай R — локальне майже-кільце, адитивна група якого R^+ ізоморфна H_2 і $|R : L| = p$. Якщо a збігається з одиничним елементом R , $x = ax_1 + bx_2 + cx_3$, $y = ay_1 + by_2 + cy_3 \in R$, то

$$xy = a \left(x_1y_1 + \alpha(x)y_2 + \left(\binom{x_1}{2} \binom{y_1}{2} x_2 - x_1x_3 \binom{y_1}{2} + x_1^2x_2 \binom{y_1}{3} - \binom{x_1}{2} \beta(x)y_3 \right) p \right) + b(x_2y_1 + \beta(x)y_2) + c \left(x_3y_1 - x_1x_2 \binom{y_1}{2} + \gamma(x)y_2 + x_1\beta(x)y_3 \right). \quad (2.2)$$

Навіть більше, для відображень $\alpha: R \rightarrow \mathbb{Z}_{p^2}$, $\beta: R \rightarrow \mathbb{Z}_p$ і $\gamma: R \rightarrow \mathbb{Z}_p$ справджуються такі твердження:

(0) $\alpha(0) \equiv 0 \pmod{p^2}$, $\beta(0) \equiv 0 \pmod{p}$ і $\gamma(0) \equiv 0 \pmod{p}$ тоді й лише 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) $\gamma(xy) \equiv \gamma(x)\beta(y) + x_1\beta(x)\gamma(y) \pmod{p}$.

2.4. 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 3. 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 на G , щоб $R = (G, +, \cdot)$ було локальним майже-кільцем.

Визначаємо множення $x \cdot y$ за формулою (2.2), де $\alpha(x) \equiv 0 \pmod{p^2}$, $\beta(x) \equiv x_1^{p-2} \pmod{p}$ і $\gamma(x) \equiv 0 \pmod{p}$. Позначаємо $x_1 \pmod{p}$ через $\bar{x}_1$. Тоді маємо

$$x \cdot y = a \left(x_1y_1 + \left(\binom{x_1}{2} \binom{y_1}{2} x_2 - x_1x_3 \binom{y_1}{2} + x_1^2x_2 \binom{y_1}{3} - \binom{x_1}{2} \bar{x}_1^{p-2}y_3 \right) p \right) + b(x_2y_1 + \bar{x}_1^{p-2}y_2) + c \left(x_3y_1 - x_1x_2 \binom{y_1}{2} + \bar{x}_1^{p-2}x_1y_3 \right). \quad (2.3)$$

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 на підставі малої теореми Ферма маємо $\bar{x}_1^{p-2}x_1 \equiv \bar{x}_1^{p-1} \equiv 1 \pmod{p}$. Тоді $px_1 \equiv p\bar{x}_1 \pmod{p^2}$ і $x_1 \equiv \bar{x}_1 \pmod{p}$. 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 2.

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 система $R = (G, +, \cdot)$ є майже-кільцем з одиничним елементом a щодо операцій $+$ і $\cdot$. Очевидно, для цього 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 $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.

Справді, за формулою (2.3) маємо

$$\begin{aligned} x \cdot z = a \left(x_1 z_1 + \left(\binom{x_1}{2} \binom{z_1}{2} x_2 - x_1 x_3 \binom{z_1}{2} + x_1^2 x_2 \binom{z_1}{3} - \binom{x_1}{2} \bar{x}_1^{p-2} z_3 \right) p \right) \\ + b(x_2 z_1 + \bar{x}_1^{p-2} z_2) + c \left(x_3 z_1 - x_1 x_2 \binom{z_1}{2} + \bar{x}_1^{p-2} x_1 z_3 \right). \end{aligned}$$

Оскільки

$$\begin{aligned} y + z &= ay_1 + by_2 + cy_3 + az_1 + bz_2 + cz_3 \\ &= ay_1 + by_2 + az_1(1 - y_3p)cy_3 + bz_2 + cz_3 \\ &= a \left(y_1 + z_1 + \left(\binom{z_1}{2} y_2 - z_1 y_3 \right) p \right) + b(y_2 + z_2) + c(y_3 + z_3 - y_2 z_1), \end{aligned}$$

то

$$\begin{aligned} x \cdot (y + z) &= a \left(x_1 \left(y_1 + z_1 + \left(\binom{z_1}{2} y_2 - z_1 y_3 \right) p \right) \right. \\ &\quad + \left(\binom{x_1}{2} \binom{y_1 + z_1}{2} x_2 - x_1 x_3 \binom{y_1 + z_1}{2} + x_1^2 x_2 \binom{y_1 + z_1}{3} \right. \\ &\quad \left. \left. - \binom{x_1}{2} \bar{x}_1^{p-2} (y_3 + z_3 - y_2 z_1) \right) p \right) + b(x_2(y_1 + z_1) + \bar{x}_1^{p-2}(y_2 + z_2)) \\ &\quad + c \left(x_3(y_1 + z_1) - x_1 x_2 \binom{y_1 + z_1}{2} + \bar{x}_1^{p-1}(y_3 + z_3 - y_2 z_1) \right) \\ &= a \left(x_1(y_1 + z_1) + \left(x_1 \binom{z_1}{2} y_2 - x_1 y_3 z_1 + \binom{x_1}{2} x_2 \binom{y_1 + z_1}{2} \right. \right. \\ &\quad \left. \left. - x_1 x_3 \binom{y_1 + z_1}{2} + x_1^2 x_2 \binom{y_1 + z_1}{3} - \binom{x_1}{2} \bar{x}_1^{p-2} (y_3 + z_3) \right. \right. \\ &\quad \left. \left. + \binom{x_1}{2} \bar{x}_1^{p-2} y_2 z_1 \right) p \right) + b(x_2(y_1 + z_1) + \bar{x}_1^{p-2}(y_2 + z_2)) \\ &\quad + c \left(x_3(y_1 + z_1) - x_1 x_2 \binom{y_1 + z_1}{2} + (y_3 + z_3) - y_2 z_1 \right). \end{aligned}$$

З іншого боку,

$$\begin{aligned} x \cdot y + x \cdot z &= a \left(x_1 y_1 + \left(\binom{x_1}{2} \binom{y_1}{2} x_2 - x_1 x_3 \binom{y_1}{2} + x_1^2 x_2 \binom{y_1}{3} - \binom{x_1}{2} \bar{x}_1^{p-2} y_3 \right) p \right) \\ &\quad + b(x_2 y_1 + \bar{x}_1^{p-2} y_2) + c \left(x_3 y_1 - x_1 x_2 \binom{y_1}{2} + \bar{x}_1^{p-1} y_3 \right) \\ &\quad + a \left(x_1 z_1 + \left(\binom{x_1}{2} \binom{z_1}{2} x_2 - x_1 x_3 \binom{z_1}{2} + x_1^2 x_2 \binom{z_1}{3} - \binom{x_1}{2} \bar{x}_1^{p-2} z_3 \right) p \right) \end{aligned}$$

$$\begin{aligned}
& + b(x_2 z_1 + \bar{x}_1^{p-2} z_2) + c\left(x_3 z_1 - x_1 x_2 \binom{z_1}{2} + \bar{x}_1^{p-1} z_3\right) \\
& = a\left(x_1 y_1 + \left(\binom{x_1}{2} \binom{y_1}{2} x_2 - x_1 x_3 \binom{y_1}{2} + x_1^2 x_2 \binom{y_1}{3} - \binom{x_1}{2} \bar{x}_1^{p-2} y_3\right) p\right) \\
& \quad + b(x_2 y_1 + \bar{x}_1^{p-2} y_2) + a\left(x_1 z_1 + \left(\binom{x_1}{2} \binom{z_1}{2} x_2 \right. \right. \\
& \quad \left. \left. - x_1 x_3 \binom{z_1}{2} + x_1^2 x_2 \binom{z_1}{3} - \binom{x_1}{2} \bar{x}_1^{p-2} z_3\right) p\right) \\
& \quad \times \left(1 - \left(x_3 y_1 - x_1 x_2 \binom{y_1}{2} + \bar{x}_1^{p-1} y_3\right) p\right) + c\left(x_3 y_1 - x_1 x_2 \binom{y_1}{2} + \bar{x}_1^{p-1} y_3\right) \\
& \quad + b(x_2 z_1 + \bar{x}_1^{p-2} z_2) + c\left(x_3 z_1 - x_1 x_2 \binom{z_1}{2} + \bar{x}_1^{p-1} z_3\right).
\end{aligned}$$

За лемами 4–6 маємо

$$\begin{aligned}
& = a\left(x_1 y_1 + \left(\binom{x_1}{2} \binom{y_1}{2} x_2 - x_1 x_3 \binom{y_1}{2} + x_1^2 x_2 \binom{y_1}{3} - \binom{x_1}{2} \bar{x}_1^{p-2} y_3\right) p\right) \\
& \quad + b(x_2 y_1 + \bar{x}_1^{p-2} y_2) + a\left(x_1 z_1 + \left(\binom{x_1}{2} \binom{z_1}{2} x_2 \right. \right. \\
& \quad \left. \left. - x_1 x_3 \binom{z_1}{2} + x_1^2 x_2 \binom{z_1}{3} - \binom{x_1}{2} \bar{x}_1^{p-2} z_3 - x_1 x_3 y_1 z_1 \right. \right. \\
& \quad \left. \left. + x_1^2 x_2 \binom{y_1}{2} z_1 - \bar{x}_1^p y_3 z_1\right) p\right) + c\left(x_3 y_1 - x_1 x_2 \binom{y_1}{2} + \bar{x}_1^{p-1} y_3\right) \\
& \quad + b(x_2 z_1 + \bar{x}_1^{p-2} z_2) + c\left(x_3 z_1 - x_1 x_2 \binom{z_1}{2} + \bar{x}_1^{p-1} z_3\right).
\end{aligned}$$

Далі,

$$\begin{aligned}
& = a\left(x_1 y_1 + \left(\binom{x_1}{2} \binom{y_1}{2} x_2 - x_1 x_3 \binom{y_1}{2} + x_1^2 x_2 \binom{y_1}{3} - \binom{x_1}{2} \bar{x}_1^{p-2} y_3\right) p\right) \\
& \quad + a\left(x_1 z_1 + \left(\binom{x_1}{2} \binom{z_1}{2} x_2 - x_1 x_3 \binom{z_1}{2} + x_1^2 x_2 \binom{z_1}{3} \right. \right. \\
& \quad \left. \left. - \binom{x_1}{2} \bar{x}_1^{p-2} z_3 - x_1 x_3 y_1 z_1 + x_1^2 x_2 \binom{y_1}{2} z_1 - \bar{x}_1^p y_3 z_1\right) p\right) \\
& \quad + \binom{x_1 z_1}{2} (x_2 y_1 + x_1^{p-2} y_2) p + b(x_2 y_1 + \bar{x}_1^{p-2} y_2) \\
& \quad - c x_1 z_1 (x_2 y_1 + \bar{x}_1^{p-2} y_2) + c\left(x_3 y_1 - x_1 x_2 \binom{y_1}{2} + \bar{x}_1^{p-1} y_3\right) \\
& \quad + b(x_2 z_1 + \bar{x}_1^{p-2} z_2) + c\left(x_3 z_1 - x_1 x_2 \binom{z_1}{2} + \bar{x}_1^{p-1} z_3\right).
\end{aligned}$$

В результаті отримуємо

$$\begin{aligned}
 & a \left(x_1(y_1 + z_1) + \left(\binom{x_1}{2} x_2 \left(\binom{y_1}{2} + \binom{z_1}{2} \right) - x_1 x_3 \left(\binom{y_1}{2} + \binom{z_1}{2} \right) \right. \right. \\
 & \quad \left. \left. + x_1^2 x_2 \left(\binom{y_1}{3} + \binom{z_1}{3} \right) - \binom{x_1}{2} \bar{x}_1^{p-2} (y_3 + z_3) \right. \right. \\
 & \quad \left. \left. - x_1 x_3 y_1 z_1 + x_1^2 x_2 \left(\binom{y_1}{2} z_1 - \bar{x}_1 y_3 z_1 + \binom{x_1 z_1}{2} x_2 y_1 + \binom{x_1 z_1}{2} \bar{x}_1^{p-2} y_2 \right) p \right) \right. \\
 & \quad \left. + b(x_2(y_1 + z_1) + \bar{x}_1^{p-2}(y_2 + z_2)) + c \left(x_3(y_1 + z_1) \right. \right. \\
 & \quad \left. \left. - x_1 x_2 \left(\binom{y_1}{2} + \binom{z_1}{2} + y_1 z_1 \right) + (y_3 + z_2) - y_2 z_1 \right). \right.
 \end{aligned}$$

Наведемо конгруентності та тотожності, які використаємо при доведенні лівої дистрибутивності.

По-перше,

$$\begin{aligned}
 \binom{x_1 z_1}{2} \bar{x}_1^{p-2} y_2 &= \frac{1}{2} (x_1^2 z_1^2 - x_1 z_1) \bar{x}_1^{p-2} y_2 \\
 &= \frac{1}{2} (\bar{x}_1^p y_2 z_1^2 - \bar{x}_1^{p-1} y_2 z_1) \equiv \frac{1}{2} (\bar{x}_1 z_1^2 y_2 - y_2 z_1) \pmod{p^2}
 \end{aligned}$$

i

$$x_1 \binom{z_1}{2} y_2 + \binom{x_1}{2} \bar{x}_1^{p-2} y_2 z_1 \equiv \frac{1}{2} (\bar{x}_1 z_1^2 y_2 - y_2 z_1) \pmod{p^2}.$$

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 $x \cdot y + x \cdot z$, отримуємо

$$\begin{aligned}
 & \binom{x_1}{2} x_2 y_1 z_1 + x_1^2 x_2 \binom{y_1 + z_1}{2} \\
 & \equiv x_1^2 x_2 \left(\binom{y_1}{3} + \binom{z_1}{3} \right) + x_1^2 x_2 \binom{y_1}{2} z_1 - \binom{x_1 z_1}{2} x_2 y_1 \pmod{p^2}.
 \end{aligned}$$

Далі,

$$\frac{1}{2} (x_1^2 x_2 y_1 z_1 - x_1 x_2 y_1 z_1) + \frac{1}{6} x_1^2 x_2 (y_1^3 + 3y_1^2 z_1$$

$$\begin{aligned}
& + 3y_1z_1^2 + z_1^3 - 3y_1^2 - 6y_1z_1 - 3z_1^2 + 2y_1 + 2z_1) \\
& \equiv \frac{1}{6}x_1^2x_2(y_1^3 - 3y_1^2 + 2y_1 + z_1^3 - 3z_1^2 + 2z_1) \\
& + \frac{1}{2}(x_1^2x_2y_1^2z_1 - x_1^2x_2y_1z_1 + x_1^2x_2y_1z_1^2 - x_1x_2y_1z_1) \pmod{p^2}.
\end{aligned}$$

Спростуючи, маємо

$$-x_1^2x_2y_1z_1 + \frac{1}{2}x_1^2x_2y_1z_1 \equiv -\frac{1}{2}x_1^2x_2y_1z_1 \pmod{p^2}.$$

Звідси, прирівнюючи коефіцієнти при твірних b і c , одержуємо $x \cdot (y + z) = x \cdot y + x \cdot z$.

Далі перевіримо асоціативність множення. З одного боку,

$$\begin{aligned}
(x \cdot y) \cdot z &= a \left(x_1y_1z_1 + \left(\binom{x_1}{2} \binom{y_1}{2} x_2 - x_1x_3 \binom{y_1}{2} + x_1^2x_2 \binom{y_1}{3} - \binom{x_1}{2} \bar{x}_1^{p-2}y_3 \right) z_1 \right. \\
&+ \left. \binom{x_1y_1}{2} \binom{z_1}{2} (x_2y_1 + \bar{x}_1^{p-2}y_2) - x_1y_1 \left(x_3y_1 - x_1x_2 \binom{y_1}{2} + \bar{x}_1^{p-1}y_3 \right) \binom{z_1}{2} \right. \\
&+ \left. x_1^2y_1^2(x_2y_1 + \bar{x}_1^{p-2}y_2) \binom{z_1}{3} - \binom{x_1y_1}{2} \bar{x}_1^{p-2} \bar{y}_1^{p-2} z_3 \right) p \\
&+ b((x_2y_1 + \bar{x}_1^{p-2}y_2)z_1 + \bar{x}_1^{p-2} \bar{y}_1^{p-2} z_2) \\
&+ c \left(\left(x_3y_1 - x_1x_2 \binom{y_1}{2} + \bar{x}_1^{p-1}y_3 \right) z_1 \right. \\
&- \left. x_1y_1(x_2y_1 + \bar{x}_1^{p-2}y_2) \binom{z_1}{2} + \bar{x}_1^{p-1} \bar{y}_1^{p-1} z_3 \right) \\
&= a \left(x_1y_1z_1 + \left(\binom{x_1}{2} \binom{y_1}{2} x_2z_1 - x_1x_3 \binom{y_1}{2} z_1 + x_1^2x_2 \binom{y_1}{3} z_1 \right. \right. \\
&- \left. \left. \binom{x_1}{2} \bar{x}_1^{p-2}y_3z_1 + \binom{x_1y_1}{2} \binom{z_1}{2} x_2y_1 + \binom{x_1y_1}{2} \binom{z_1}{2} \bar{x}_1^{p-2}y_2 \right. \right. \\
&- \left. \left. x_1x_3y_1^2 \binom{z_1}{2} + x_1^2x_2y_1 \binom{y_1}{2} \binom{z_1}{2} - x_1y_1y_3 \binom{z_1}{2} \right. \right. \\
&+ \left. \left. x_1^2y_1^3 \binom{z_1}{3} + \bar{x}_1^p y_1^2 y_2 \binom{z_1}{3} - \binom{x_1y_1}{2} \bar{x}_1^{p-2} \bar{y}_1^{p-2} z_3 \right) p \right. \\
&+ b(x_2y_1z_1 + \bar{x}_1^{p-2}y_2z_1 + \bar{x}_1^{p-2} \bar{y}_1^{p-2} z_2) \\
&+ c \left(x_3y_1z_1 - x_1x_2 \binom{y_1}{2} z_1 + \bar{x}_1^{p-1}y_3z_1 - x_1x_2y_1^2 \right. \\
&- \left. \bar{x}_1^{p-1}y_1y_2 \binom{z_1}{2} + \bar{x}_1^{p-1} \bar{y}_1^{p-1} z_3 \right),
\end{aligned}$$

а з іншого —

$$\begin{aligned}
 x \cdot (y \cdot z) &= a \left(x_1 \left(y_1 z_1 + \binom{y_1}{2} \binom{z_1}{2} y_2 - y_1 y_3 \binom{z_1}{2} + y_1^2 y_2 \binom{z_1}{3} - \binom{y_1}{2} \bar{y}_1^{p-2} z_3 \right) p \right) \\
 &\quad + \left(\binom{x_1}{2} \binom{y_1 z_1}{2} x_2 - x_1 x_2 \binom{y_1 z_1}{2} + x_1^2 x_2 \binom{y_1 z_1}{3} \right) \\
 &\quad - \binom{x_1}{2} \bar{x}_1^{p-2} \left(y_3 z_1 - y_1 y_2 \binom{z_1}{2} + \bar{y}_1^{p-1} z_3 \right) p \\
 &\quad + b(x_2 y_1 z_1 + \bar{x}_1^{p-2} (y_2 z_1 + \bar{y}_1^{p-2} z_2)) \\
 &\quad + c \left(x_3 y_1 z_1 - x_1 x_2 \binom{y_1 z_1}{2} + \bar{x}_1^{p-1} \left(y_3 z_1 - y_1 y_2 \binom{z_1}{2} + \bar{y}_1^{p-1} z_3 \right) \right) \\
 &= a \left(x_1 y_1 z_1 + \left(x_1 \binom{y_1}{2} \binom{z_1}{2} y_2 - x_1 y_1 y_3 \binom{z_1}{2} \right) \right. \\
 &\quad + x_1 y_1^2 y_2 \binom{z_1}{3} - x_1 \binom{y_1}{2} \bar{y}_1^{p-2} z_3 + \binom{x_1}{2} \binom{y_1 z_1}{2} x_2 \\
 &\quad - x_1 x_2 \binom{y_1 z_1}{2} + x_1^2 x_2 \binom{y_1 z_1}{3} - \binom{x_1}{2} \bar{x}_1^{p-2} y_3 z_1 \\
 &\quad + \left. \left(\binom{x_1}{2} \bar{x}_1^{p-2} y_1 y_2 \binom{z_1}{2} - \binom{x_1}{2} \bar{x}_1^{p-2} \bar{y}_1^{p-2} z_3 \right) p \right) \\
 &\quad + b(x_2 y_1 z_1 + \bar{x}_1^{p-2} y_2 z_1 + \bar{x}_1^{p-2} \bar{y}_1^{p-2} z_2) \\
 &\quad + c \left(x_3 y_1 z_1 - x_1 x_2 \binom{y_1 z_1}{2} + y_3 z_1 - y_1 y_2 \binom{z_1}{2} + z_3 \right).
 \end{aligned}$$

Отже, $x \cdot (y \cdot z) = (x \cdot y) \cdot z$. Тому $R = (G, +, \cdot)$ є майже-кільцем з одиничним елементом a .

Для завершення доведення залишилося 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 й лише 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

$$x_1 y_1 + \left(\binom{x_1}{2} \binom{y_1}{2} x_2 - x_1 x_3 \binom{y_1}{2} + x_1^2 x_2 \binom{y_1}{3} - \binom{x_1}{2} \bar{x}_1^{p-2} y_3 \right) p \equiv 1 \pmod{p^2}$$

за визначенням добутку $x \cdot y$. Звідси $x_1 y_1 \equiv 1 \pmod{p^2}$, а отже, $x_1 \equiv 1 \pmod{p}$.

І навпаки, якщо виконується остання конгруенція, то $\beta(x) \equiv 1 \pmod{p}$ за твердженням (3) наслідку 2. Тому існують такі натуральні числа y_1, y_2 та y_3 , що $x_1 y_1 \equiv 1 \pmod{p^2}$, $x_2 y_1 + \bar{x}_1^{p-2} y_2 \equiv 0 \pmod{p}$ та $x_3 z_1 - x_1 x_2 \binom{z_1}{2} + \bar{x}_1^{p-2} x_1 z_3 \equiv 0 \pmod{p}$. Покладемо $y = ay_1 + by_2 + cy_3$ і

$$z_1 = 1 + \left(\binom{x_1}{2} \binom{y_1}{2} x_2 - x_1 x_3 \binom{y_1}{2} + x_1^2 x_2 \binom{y_1}{3} - \binom{x_1}{2} \bar{x}_1^{p-2} y_3 \right) p.$$

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-кілець R є локальним, що завершує доведення.

Наведемо приклад локального майже-кілця порядку $5^4 = 625$, адитивна група якого R^+ ізоморфна H_2 .

Приклад 1. Нехай $G \cong (C_{25} \rtimes C_5) \rtimes C_5$. Якщо $x = ax_1 + bx_2 + cx_3$, $y = ay_1 + by_2 + cy_3 \in G$ і $(G, +, \cdot)$ є локальним майже-кілцем, то згідно з прикладом з теореми 3 функції α , β і γ можуть бути такими: $\alpha(x) \equiv 0 \pmod{25}$, $\beta(x) \equiv x_1^3 \pmod{5}$ і $\gamma(x) \equiv 0 \pmod{5}$. Підставляючи ці функції у формулу (2.2), маємо

$$\begin{aligned} x \cdot y = a \left(x_1 y_1 + \binom{x_1}{2} \binom{y_1}{2} x_2 - x_1 x_3 \binom{y_1}{2} + x_1^2 x_2 \binom{y_1}{y_1 - 3} - \binom{x_1}{2} \bar{x}_1^3 y_3 \right) 5 \\ + b(x_2 y_1 + \bar{x}_1^3 y_2) + c \left(x_3 y_1 - x_1 x_2 \binom{y_1}{2} + x_1 \bar{x}_1^3 y_3 \right). \end{aligned}$$

Наведемо комп'ютерну програму, яка будує майже-кілець з прикладу 1 (див. також GitHub):

https://github.com/raemarina/Examples/blob/main/LNR_625-8.txt

```
LoadPackage("LocalNR");
G := SmallGroup(625, 8);
gen := MinimalGeneratingSet(G);
List(gen, Order);
a := gen[1];
b := gen[2];
c := a^4 - 1 * b^4 - 1 * a * b;
alpha := function(x, y, z)
return 0; fi; end;
gamma := function(x)
return 0; end;
beta := function(x)
return x^3 mod 5; end;
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 := ExplicitMultiplicationNearRingNC(G, mulGR);
M := MultiplicationTable(n);
mu_NR := NearRingMultiplicationByOperationTable(G, M, AsSortedList(G));
N := ExplicitMultiplicationNearRing(G, mu_NR).
```

З пакету LocalNR [12] та [13] маємо таку 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

2.5. Групи H_3 і H_4 . Проаналізувавши групи H_3 та H_4 порядку 625 за допомогою GAP, ми з'ясували, що не існує локальних майже-кілець на цих групах. Це дозволяє зробити таке припущення.

Гіпотеза. *Не існує локального майже-кілець, адитивна група якого ізоморфна H_3 чи H_4 .*

Конфлікт інтересів. Авторки заявляють, що вони не мають потенційного конфлікту інтересів щодо дослідження у цій статті.

Фінансування. Це дослідження підтримано фондом ПЕ-SRF.

Авторські внески. Усі авторки внесли рівний внесок у роботу.

Література

1. B. N. Al-Hasanat, A. Almazaydeh, *On classification of groups of order p^4 , where p is an odd prime*, Int. J. Math. and Comput. Sci., **17**, № 4, 1569–1593 (2022).
2. B. Amberg, P. Hubert, Ya. Sysak, *Local near-rings with dihedral multiplicative group*, J. Algebra, **273**, 700–717 (2004).
3. W. Burnside, *Theory of groups of finite order*, University Press, Cambridge (1897).
4. J. R. Clay, J. J. (Jr.) Malone, *The near-rings with identities on certain finite groups*, Math. Scand., **19**, 146–150 (1966).
5. S. Feigelstock, *Additive groups of local near-rings*, Comm. Algebra, **34**, 743–747 (2006).
6. *The GAP Group*, GAP — Groups, Algorithms, and Programming, Version 4.12.0 (2022); <https://www.gap-system.org>.
7. C. J. Maxson, *On the construction of finite local near-rings (I): on non-cyclic Abelian p -groups*, Quart. J. Math. Oxford (2), **21**, 449–457 (1970).
8. C. J. Maxson, *On the construction of finite local near-rings (II): on non-Abelian p -groups*, Quart. J. Math. Oxford (2), **22**, 65–72 (1971).
9. I. Raievska, M. Raievska, *Groups of the nilpotency class 2 of order p^4 as additive groups of local nearrings* (2023); <https://arxiv.org/abs/2303.17567>.
10. I. Raievska, M. Raievska, *Groups of the nilpotency class 3 of order p^4 as additive groups of local nearrings* (2023); <https://arxiv.org/abs/2309.14342>.
11. I. Raievska, M. Raievska, *Lower bounds for the number of local nearrings on groups of order p^3* (2023); <https://arxiv.org/abs/2205.08359>.
12. I. Raievska, M. Raievska, Y. Sysak, *Local NR*, Package of Local Nearrings, Version 1.0., **3** (GAP package) (2021); <https://gap-packages.github.io/LocalNR>.
13. I. Raievska, M. Raievska, Ya. Sysak, *Database Endom625: (v0.2)* [Data set], Zenodo (2023); <https://zenodo.org/record/7613145#.ZChqJXZBy39>.
14. I. Raievska, Ya. P. Sysak, *Finite local nearrings on metacyclic Miller–Moreno p -groups*, Algebra and Discrete Math., **13**, № 1, 111–127 (2012).
15. І. Ю. Раєвська, М. Ю. Раєвська, *Локальні майже-кілець з обмеженнями на мультиплікативні групи та підгрупи необоротних елементів*, Науковий часопис НПУ імені М. П. Драгоманова, Сер. 1, № 14, 134–145 (2013).

Одержано 27.12.23