УДК 517.6

І. Ю. Раєвська, М. Ю. Раєвська (Ін-т математики НАН України, Київ)

ЛОКАЛЬНІ МАЙЖЕ-КІЛЬЦЯ З МУЛЬТИПЛІКАТИВНОЮ ГРУПОЮ ШМІДТА

We propose a classification of finite local nearrings with multiplicative Shmidt group. Moreover, it is shown that there are no nearrings with identity on the Shmidt groups.

Отримано класифікацію скінченних локальних майже-кілець із мультиплікативною групою Шмідта. Більш того, доведено, що не існує майже-кілець з одиницею на групах Шмідта.

1. Вступ. Систематичне вивчення скінченних майже-полів було започатковано в [1], де доведено абелевість їхньої адитивної групи та охарактеризовано мультиплікативні групи як групи регулярних автоморфізмів абелевих груп.

У роботі [2] отримано повну характеризацію скінченних так званих спадкових груп майже-полів, кожна підгрупа яких ізоморфна мультиплікативній групі деякого майже-поля. В [3] наведено опис усіх майже-полів із мультиплікативною групою Шмідта. А саме, якщо R — майже-поле, то мультиплікативна група R^* ізоморфна або групі $SL(2,3)$, або одній із груп Міллера – Морено порядків 24, 63 і 80.

Властивості локальних майже-кілець із абелевою мультиплікативною групою вивчалися в [4]. У роботах [5, 6] досліджувалися локальні майже-кільця з мультиплікативною групою діедра, а в [7] — з узагальненою групою кватерніонів. Локальні майже-кільця порядку 2^n з мультиплікативною групою Міллера – Морено вивчалися в [8].

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 60-х років минулого століття. Один із перших результатів в цьому напрямку було отримано у статті [9], де показано, що існує єдине майже-кільце з одиницею, адитивна група якого циклічна, і яке фактично є комутативним кільцем. Також було доведено, що симетрична група S_n при $n \geq 3$ не може бути адитивною групою майже-кільця з одиницею. Пізніше в роботі [10] було доведено, що знакозмінна група A_4 також не може бути адитивною групою майже-кільця з одиницею. В [11] показано, що не існує майже-кільця з одиницею, адитивна група якого ізоморфна групі кватерніонів Q_8, і встановлено, що існує сім майже-кілець з одиницею на групі діедра D_4 порядку 8. У [12] за допомогою системи комп'ютерної алгебри GAP класифіковано всі майже-кільця з одиницею на групах порядку, що не перевищує 31, і визначено всі неабелеві групи вказаних порядків, які не можуть бути адитивними групами майже-кілець з одиницею. В [13] наведено всі можливі типи груп Міллера – Морено, які можуть бути адитивними групами майже-кілець з одиницею.

У даній статті наведено класифікацію скінченних локальних майже-кілець із мультиплікативною групою Шмідта. Більш того, доведено, що не існує майже-кілець з одиницею на групах Шмідта.

2. Попередні результати. Непорожня множина R із двома бінарними операціями $+$ та $\cdot$ є (*лівим*) *майже-кільцем*, якщо:

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

З умови 3 означення випливає, що для кожної підгрупи M групи R^+ і кожного елемента $x\in R$ множина $xM=\{xy\mid y\in M\}$ є підгрупою в R^+ і, зокрема, $x0=0$. Майже-кільце R називається *нуль-симетричним*, якщо $0x=0$ для всіх $x\in R$, і *майже-кільцем з одиницею* i, якщо напівгрупа $(R,\cdot)$ є моноїдом з одиничним елементом i. Група R^* оборотних елементів моноїда $(R,\cdot)$ називається *мультиплікативною*, а група R^+ — *адитивною* групою майже-кільця R. Підгрупа M із R^+ називається R^**-інваріантною*, якщо $rM\le M$ для кожного $r\in R^*$, і (R,R)*-підгрупою*, якщо $xMy\subseteq M$ для довільних $x,y\in R$.

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

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

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

Далі будемо позначати через L підгрупу в R^+ усіх необоротних елементів із R.

Наступна лема (див. [5], лема 3.2) характеризує основні властивості локальних майже-кілець.

Лема 2. *Нехай R — скінченне локальне майже-кільце з одиницею i. Тоді R^+ — p-група для деякого простого p, експонента якої збігається з порядком елемента i в R^+, і справджуються такі твердження*:

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

Як наслідок із тверджень 3 і 5 леми 2 випливає таке твердження.

Лема 3. *Нехай R — скінченне локальне майже-кільце з одиницею i. Тоді*

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

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

Має місце така теорема [15] (теорема 2.1) про зв'язок порядків локального майже-кільця і підгрупи необоротних елементів.

Теорема 1. *Якщо R — локальне майже-кільце, яке не є майже-полем, то $|R|\le|L|^2$.*

Скінченні локальні майже-кільця з циклічною підгрупою необоротних елементів описано в [16] (теорема 1).

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

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

Наступну лему доведено в [2] (лема 1).

Лема 4. *Нехай p — непарне просте число. Якщо m і n — додатні цілі числа, для яких $2^n - 1 = p^m$, то $m = 1$ і n — просте число.*

Групою Шмідта або *мінімальною нільпотентною групою* називається скінченна нільпотентна група, будь-яка власна підгрупа якої нільпотентна. Вивчення таких груп започаткував О. Ю. Шмідт [17]. У наступній теоремі дано структурний опис цих груп (див. [18], пропозиція 5.5.2).

Теорема 3. *Скінченна група G тоді і лише тоді є групою Шмідта, коли вона розкладається в напівпрямий добуток $G = S \leftthreetimes T$ своїх нормальної силовської p-підгрупи S порядку p^s, $s \geq 1$, і циклічної силовської q-підгрупи $T = \langle b \rangle$ порядку q^t, $t \geq 1$, 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 числа* p;

3) *якщо* S — *неабелева, то* $Z(S) = S' = \Phi(S)$.

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

Нехай G — непримарна група Міллера – Морено, тобто $G = P \leftthreetimes \langle b \rangle$ з нормальною елементарною абелевою підгрупою P порядку p^r, на якій елемент b порядку q^s індукує незвідний автоморфізм простого порядку q, де p, q — прості, q ділить $p^r - 1$ і r, s — натуральні числа.

Лема 5. *У групі G не існує елемента, порядок якого збігається з її експонентою.*

Доведення. Припустимо, що існує елемент g в групі G, порядок якого збігається з її експонентою pq^s. Тоді $G = P\langle g \rangle$, і тому перетин $P \cap \langle g \rangle$ є нормальною підгрупою порядку p в G. Оскільки P — мінімальна нормальна підгрупа в G, то $P = P \cap \langle g \rangle$ і, таким чином, $G = \langle g \rangle$. Отримана суперечність завершує доведення леми.

Нагадаємо, що *цілком характеристичною підгрупою* називається підгрупа групи G, яка інваріантна відносно всіх ендоморфізмів групи G.

Наступна лема є безпосереднім наслідком леми 1 [12].

Лема 6. *Нехай R — майже-кільце з одиницею i, адитивна група R^+ якого ізоморфна групі G. Тоді для кожного елемента $y \in G$ існує такий ендоморфізм φ групи G, що $i^\varphi = y$.*

Теорема 4. *Не існує майже-кілець з одиницею, адитивна група яких ізоморфна групі Шмідта.*

Доведення. За лемою 2 [13] не існує майже-кілець з одиницею, адитивна група яких ізоморфна непримарній групі Міллера – Морено.

Нехай тепер G ізоморфна групі Шмідта, яка не є групою Міллера – Морено. Припустимо, що група G є адитивною групою деякого майже-кільця з одиницею. Тоді за лемою 6 для кожного елемента $y \in G$ існує такий ендоморфізм φ групи G, що $i^\varphi = y$. Оскільки $\Phi(G)$

є цілком характеристичною підгрупою, то $\bar{i}^{\varphi} = \bar{y}$ для всіх $\bar{y} \in G/\Phi(G)$. Враховуючи, що $G/\Phi(G)$ — група Міллера – Морено, з огляду на леми 1 і 5 отримуємо суперечність.

Теорему доведено.

3. Основна теорема. Оскільки майже-поля з мультиплікативною групою Шмідта повністю описано в [3] (теорема 6), то розглянемо локальні майже-кільця, підгрупи необоротних елементів яких є нетривіальними.

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

Теорема 5. *Нехай R — локальне майже-кільце порядку p^n, яке не є майже-полем і мультиплікативна група R^* якого є групою Шмідта. Тоді мають місце такі твердження*:

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

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

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

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

Доведення. Оскільки підгрупа L є нетривіальною власною підгрупою R^+, то $|L| = p^m$ з $1 \leq m < n$. Покладемо $l = n - m$. Внаслідок того, що $R = R^* \cup L$, маємо $|R^*| = p^n - p^m = p^m(p^l - 1)$. За теоремою 3 порядок групи Шмідта ділиться на два простих числа, звідки $p^l - 1 = q^k$. Далі, якщо через i позначити одиницю майже-кільця R, то за лемою 3 група R^* розкладається в напівпрямий добуток $R^* = S \rtimes \langle b \rangle$ з нормальною силовською p-підгрупою $S = i + L$ і циклічною підгрупою $\langle b \rangle = K$ порядку q^k. Більш того, за теоремою 3 b^q лежить в центрі групи R^*.

Нехай $p > 2$. Враховуючи, що число $p^l - 1$ є парним, звідси отримуємо $p^l - 1 = 2^k$ для деякого $k \geq 1$. Оскільки елемент b індукує на фактор-групі S/S' незвідний автоморфізм порядку 2, то це можливо лише у випадку, коли $|S/S'| = p$. Звідси $|S| = p$.

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

Якщо a — твірний елемент L, то $R^+ = \langle i \rangle + \langle a \rangle$, де $\langle i \rangle$ — підгрупа, породжена одиницею i майже-кільця R. Нехай k — первісний корінь за модулем p і T — мультиплікативна підгрупа ненульових елементів з адитивної підгрупи $\langle i \rangle$. Тоді T — циклічна підгрупа порядку $p - 1$ із твірним елементом ik мультиплікативної групи R^*, і тому $R^* = S \rtimes T$. За теоремою 3 елемент $(ik)^2$ централізує підгрупу S, а тому $(ik)^2(i + a) = (i + a)(ik)^2$. Враховуючи, що $(ik)^2 = ik^2$, звідси виводимо

$$(ik)^2 a = ak^2. \tag{1}$$

Далі, за твердженням 1 леми 2 $xa \in L$ для всіх $x \in R$. Отже, $xa = a\rho(x)$ для кожного $x \in R$, де число $\rho(x)$ однозначно визначено за модулем p. Для довільних $x, y \in R$ з останньої рівності випливає $a\rho(xy) = (xy)a = x(ya) = x(a\rho(y)) = (xa)\rho(y) = a(\rho(x)\rho(y))$, звідки

маємо $(xy)a = a(\rho(x)\rho(y))$. Зокрема, поклавши $x = y = ik$, з рівності (1) отримаємо $ak^2 = (ik)^2a = a\rho(ik)^2$. Це означає, що $\rho(ik)^2 \equiv k^2 \pmod p$, звідки $\rho(ik) \equiv \pm k \pmod p$. Якщо $\rho(ik) \equiv k \pmod p$, то $(ik)(i + a) = ik + (ik)a = ik + ak = (i + a)(ik)$, і тому група R^* буде абелевою, що суперечить умові теореми. Отже, $\rho(ik) \equiv -k \pmod p$, тобто $(ik)a = -ak$. Помноживши цю рівність зліва на 0, одержимо $0a = (0(ik))a = -(0a)k$, звідки $(0a)(k+1) = 0$. Оскільки k — довільний первісний корінь за модулем p, то з останньої рівності отримуємо $0a = 0$.

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

Нехай тепер $p = 2$. Очевидно, що мультиплікативна група локального майже-кільця R порядку 2^n тоді і тільки тоді не є 2-групою, коли L є підгрупою в R^+ індексу $|R^+ : L| > 2$. Тоді $|R : L| = 2^l$ і $|L| = 2^m$, звідки $|R^* : S| = 2^l - 1$. Оскільки $2^l - 1 = q^k$, то згідно з лемою 4 це можливо лише, коли $k = 1$ і m — просте число. Зокрема, $|\langle b\rangle| = q = 2^l - 1$. Крім того, елемент b індукує незвідний автоморфізм порядку $q = 2^l - 1$ на фактор-групі S/S'. Оскільки $|S/S'| = 2^{m-s}$ з $s \geq 0$, то $q = 2^l - 1$ — дільник числа $2^{m-s} - 1$ (див., наприклад, [19], лема 5.6.3). Припустимо, що підгрупа S є неабелевою. Тоді за теоремою 5.6.5 [19] $2^l - 1$ ділить $2^r + 1$, де $r \leq (m - s)/2$. Очевидно, $r = tm + w$, де $t \in N$ і $0 \leq w < m$. Оскільки $2^r + 1 = 2^{tm+w} + 1 = 2^w(2^{tm} - 1) + 2^w + 1$, то $2^l - 1$ ділить $2^r + 1$ лише при $r = 1$ і $m = 2$. Звідси $|R : L| = 2^2 = 4$ і $|\langle b\rangle| = 3$, а тому $|S/S'| = 4$. Звідси, а також з теореми 5.4.5 [19] випливає, що S ізоморфна або групі діедра, або групі кватерніонів порядку 8, а отже, $n = 5$, $|R| = 32$ і $|S| = |L| = 8$. За допомогою системи комп'ютерної алгебри GAP [20] перевірено, що не існує локальних майже-кілець порядку 32 з підгрупою L порядку 8. Отже, підгрупа S є абелевою, а тому елементарною абелевою порядку 2^m. Звідси R^* — група Міллера – Морено, що доводить твердження 2 теореми.

Література

1. *Zassenhaus H.* Über endliche Fastkörper // Abh. Math. Semin. Univ. Hamburg. – 1935/36. – **11**. – S. 187 – 220.
2. *Ligh S.* Finte hereditary near-field groups // Monatsh. Math. – 1978. – **86**. – P. 7 – 11.
3. *Раєвська М. Ю.* Локальні майже-кільця з мультиплікативною групою Міллера – Морено // Вісн. Київ. ун-ту. Математика. Механіка. – 2011. – **25**. – С. 45 – 48.
4. *Gorodnik A.* Local near-rings with commutative groups of units // Houston J. Math. – 1999. – **25**. – P. 223 – 234.
5. *Amberg B., Hubert P., Sysak Ya.* Local nearrings with dihedral multiplicative group // J. Algebra. – 2004. – **273**. – P. 700 – 717.
6. *Hubert P.* Nearrings and a construction of triply factorized groups. – Mainz, 2005. – 146 p.
7. *Sysak Ya. P., Termini Di S.* Local nearrings with generalized quaternion multiplicative group // Ric. Mat. – 2007. – **56**. – P. 61 – 72.
8. *Раєвська М. Ю., Сисак Я. П.* Про локальні майже-кільця з мультиплікативною групою Міллера – Морено // Укр. мат. журн. – 2012. – **64**, № 6. – С. 811 – 818.
9. *Clay J. R., Malone Jr.* The near-rings with identities on certain finite groups // Math. Scand. – 1966. – **19**. – P. 146 – 150.
10. *Clay J. R., Doi D.* Near-rings with identity on alternating groups // Math. Scand. – 1968. – **23**. – P. 54 – 56.
11. *Clay J. R.* Research in near-ring theory using a digital computer // BIT. – 1970. – **10**. – P. 249 – 265.

12. *Boykett T. H. H., Nobauer C.* A class of groups which cannot be the additive groups of near-rings with identity // Contributions to General Algebra (Klagenfurt, 1997). – Klagenfurt: Heyn, 1998. – P. 89 – 99.
13. *Raievska I. Yu., Raievska M. Yu.* Finite nearrings with identity on Miller – Moreno groups // Mat. Stud. – 2014. – **42**, № 1. – P. 15 – 20.
14. *Raievska I. Yu., Sysak Ya. P.* Finite local nearrings on metacyclic Miller – Moreno p-groups // Algebra Discrete Math. – 2012. – **13**, № 1. – P. 111 – 127.
15. *Maxson C. J.* Local near-rings of cardinality p^2 // Canad. Math. Bull. – 1968. – **11**, № 4. – P. 555 – 561.
16. *Раєвська І. Ю., Раєвська М. Ю.* Локальні майже-кільця з обмеженнями на мультиплікативні групи та підгрупи необоротних елементів // Наук. часопис НПУ ім. М. П. Драгоманова. Сер. 1. Фіз.-мат. науки. – 2013. – **14**. – С. 134 – 145.
17. *Шмидт О. Ю.* Группы, все подгруппы которых специальные // Мат. сб. – 1924. – **31**. – С. 366 – 372.
18. *Huppert B.* Endliche Gruppen I. – Berlin etc.: Springer-Verlag, 1967.
19. *Gorenstein D.* Finite groups. – New York: Harper & Row, 1968. – 527 p.
20. *The GAP Group*, GAP — Groups, Algorithms, and Programming, Version 4.8.8. – 2017 // https://www.gap-system.org.

Одержано 10.01.18