УДК 512.64

В. П. Щедрик✉

АРИФМЕТИЧНІ ВЛАСТИВОСТІ КОРЕНІВ ЛІНІЙНИХ РІВНЯНЬ

Досліджуються розв'язки рівняння вигляду $a \cdot x = b$ в гомоморфному образі адекватного кільця. Відомо, що найбільший спільний дільник усіх коренів такого рівняння знову є його коренем. Доведено, що серед коренів цього рівняння також є й такі, що діляться на решту його коренів, при цьому вони є асоційованими між собою.

Ключові слова: *корені лінійного рівняння, стабільний ранг кільця, адекватне кільце.*

1. Вступ. Кільце R, у якому $1 \neq 0$, називається кільцем Безу, якщо кожний його скінченно породжений ідеал є головним. Групу одиниць цього кільця позначатимемо через $U(R)$.

Кільце R називається адекватним [6], якщо R – комутативна область Безу, в якій для всіх елементів $a, b \in R$, $a \neq 0$, існують такі елементи $c, d \in R$, що $a = cd$, причому $(c, b) = 1$ і кожний необоротний дільник d' елемента d має необоротний спільний дільник із b. Прикладом адекватних кілець є комутативні області головних ідеалів, кільця цілих аналітичних функцій, кільце неперервних дійсних функцій над цілком регулярним гаусдорфовим простором, кільця нормування.

Кільце R називається кільцем стабільного рангу 1.5, якщо для кожної трійки елементів $a, b, c \in R$, де $c \neq 0$, таких що $aR + bR + cR = R$ існує таке $r \in R$, що $(a + br)R + cR = R$. Адекватні кільця є прикладом комутативних областей стабільного рангу 1.5 (див. [13, с. 21, властивість 1.18]). Прикладом некомутативних кілець стабільного рангу 1.5 є матричні кільця другого порядку над комутативними областями Безу стабільного рангу 1.5 [1].

Лінійні рівняння вигляду $a \cdot x = b$ над різними кільцями є одними із найбільш вивчених типів рівнянь, дослідження яких продовжується і тепер. Із кожним роком розширюється спектр кілець, для яких пропонуються аналітичні та наближені методи й алгоритми пошуку коренів таких рівнянь. Поряд з питанням пошуку розв'язків у деяких задачах виникає потреба в знаходженні коренів, які задовольняють наперед задані умови. Потрібно зауважити, що потреба у дослідженні коренів рівнянь виникає у кільцях з дільниками нуля, оскільки в областях (кільцях без дільників нуля) такі рівняння мають єдиний корінь або ж є нерозв'язними.

У матричних кільцях досліджувались розв'язки з умовою симетрії у [5, 10, 14], ермітові позитивно визначені розв'язки – у [8, 11], з мінімальним рангом – у [12], діагональні та трикутні – у [9]. У роботі [2] корені матричного рівняння $AX = B$ досліджувалися над комутативною областю елементарних дільників [7] з точки зору вивчення арифметичних властивостей. Доведено [2], що лівий (правий) найбільший спільний дільник і ліве (праве) найменше спільне кратне всіх коренів розв'язного матричного рівняння $AX = B$ знову є коренем цього рівняння.

Властивості коренів лінійних рівнянь у гомоморфних образах областей Безу стабільного рангу 1.5 досліджувалися у [3, 4]. Зокрема, у [3] отримано такий результат.

Для кожного $m \in R \setminus \{0, U(R)\}$ означимо фактор кільце R/mR та гомоморфізм $\overline{\bullet} : R \to R_m$. Для кожного $a \in R$ позначаємо $\overline{a} := \overline{\bullet}(a) \in R_m$.

Теорема 1. *Нехай R – комутативна область Безу стабільного рангу*

✉ shchedrykv@ukr.net

1.5, *і нехай* $R_m := R/mR$ *та* $\overline{a}, \overline{b} \in R_m$. *Тоді*:

(***i°***) *кожне розв'язне в* R_m *рівняння* $\overline{a} \cdot \overline{x} = \overline{b}$ *має принаймні один корінь, який ділиться на решту його коренів*;

(***ii°***) *корені розв'язного в* R_m *лінійного рівняння* $\overline{a} \cdot \overline{x} = \overline{b}$, *які діляться на решту його коренів, є асоційованими між собою.*

Зауважимо, що твердження (***i°***) цієї теореми можна переформулювати таким чином: найбільший спільний дільник (н.с.д.) усіх коренів розв'язного лінійного рівняння $\overline{a} \cdot \overline{x} = \overline{b}$ знову є коренем цього рівняння. При цьому н.с.д. будь-яких двох його коренів не завжди є його коренем. Так, множиною всіх коренів рівняння $\overline{4}\overline{x} = \overline{8}$ у кільці $\mathbb{Z}_{72}$ є множина $\{\overline{2}, \overline{20}, \overline{38}, \overline{56}\}$. Н.с.д. цих коренів є $\overline{2}$, що є коренем цього рівняння, а н.с.д. $\overline{20}$ і $\overline{56}$ є $\overline{4}$, що не є його коренем.

У пропонованій роботі продовжуються дослідження, що були започатковані у [3].

2. Допоміжні твердження. Надалі R – комутативна область Безу стабільного рангу 1.5 та $m \in R \setminus \{0, U(R)\}$. Найбільший спільний дільник елементів $a, b \in R$ позначатимемо через (a, b). Елементи $a, b \in R$ називаються асоційованими, якщо $a = be$, де $e \in U(R)$. Позначення $a \mid b$ означає, що $b = ac$ для деякого $c \in R$.

У подальших дослідженнях будемо використовувати наступні результати роботи [3].

Твердження 1. *Група одиниць* $U(R_m)$ *кільця* R_m *складається з образів тих елементів* $f \in R$, *для яких* $(f, m) = 1$.

Твердження 2. *Кожний елемент* $\overline{a} \in R_m$ *має вигляд* $\overline{a} = \overline{\mu}_a \cdot \overline{e}_a$, *де* $\mu_a := (a, m)$, $\overline{e}_a \in U(R_m)$.

Зауваження 1. Зображення елемента $\overline{a} \in R_m$ у вигляді $\overline{a} = \overline{\mu}_a \cdot \overline{e}_a$ є неоднозначним. Так, у кільці $\mathbb{Z}_{36}$ елемент $\overline{33}$ зображається таким чином: $\overline{33} = \overline{15} \cdot \overline{7} = \overline{15} \cdot \overline{31}$, де $\overline{7}, \overline{31} \in U(\mathbb{Z}_{36})$.

Твердження 3. *Елементи* $\overline{a}$ *і* $\overline{b}$ *асоційовані в* R_m *тоді й тільки тоді, коли* $(a, m) = (b, m)$.

Твердження 4. *Нехай елементи* $\overline{a}$, $\overline{b}$ *є дільниками один одного в* R_m. *Тоді* $\overline{a}$, $\overline{b}$ *асоційовані в* R_m.

Твердження 5. *Якщо* $\overline{b} \in R_m$, *то* $\operatorname{Ann}(\overline{b}) = \overline{\alpha}_b R_m$, *де* $\alpha_b := \dfrac{m}{(b, m)} \in R$.

3. Основний результат.

Теорема 2. *Нехай* R – *адекватне кільце,* $R_m := R / mR$ *і* $\overline{a}, \overline{b} \in R_m$. *Тоді*:

(***i°***) *кожне розв'язне в* R_m *рівняння* $\overline{a} \cdot \overline{x} = \overline{b}$ *має принаймні один корінь, який ділиться на решту його коренів;*

(***ii°***) *корені розв'язного в* R_m *лінійного рівняння* $\overline{a} \cdot \overline{x} = \overline{b}$, *які діляться на решту його коренів є асоційованими між собою.*

Д о в е д е н н я. Нехай рівняння

$$\overline{a} \cdot \overline{x} = \overline{b}, \tag{1}$$

де $\overline{b} \neq \overline{0}$, є розв'язним в R_m. Розглянемо множину ануляторів елемента $\overline{a}$:

$$\mathrm{Ann}(\overline{a}) = \{\overline{q} \in R_m \mid \overline{a} \cdot \overline{q} = \overline{0}\}.$$

Множиною всіх коренів рівняння (1) є $\overline{c} + \mathrm{Ann}(\overline{a})$, де $\overline{c}$ – довільний розв'язок цього рівняння. Дійсно, нехай $\overline{c}_1$ – розв'язок рівняння (1). Тоді $\overline{a} \cdot \overline{c} = \overline{b}$ і $\overline{a} \cdot \overline{c}_1 = \overline{b}$. Отже,

$$\overline{a} \cdot \overline{c}_1 = \overline{a} \cdot \overline{c} \;\Rightarrow\; \overline{a}(\overline{c}_1 - \overline{c}) = \overline{0} \;\Rightarrow\; \overline{c}_1 - \overline{c} = \overline{\sigma} \in \mathrm{Ann}(\overline{a}) \;\Rightarrow\; \overline{c}_1 = \overline{c} + \overline{\sigma}.$$

Таким чином, кожний розв'язок $\overline{c}_1$ рівняння $\overline{a} \cdot \overline{x} = \overline{b}$ є елементом множини $\overline{c} + \mathrm{Ann}(\overline{a})$.

З іншого боку, якщо $\overline{\delta} \in \mathrm{Ann}(\overline{a})$, то

$$\overline{a}(\overline{c} + \overline{\delta}) = \overline{a} \cdot \overline{c} + \overline{a} \cdot \overline{\delta} = \overline{b} + \overline{0} = \overline{b}.$$

Отже, множина $\overline{c} + \mathrm{Ann}(\overline{a})$ є множиною всіх коренів рівняння $\overline{a} \cdot \overline{x} = \overline{b}$.

Згідно з твердженням 2, $\overline{a} = \overline{\mu}_a \cdot \overline{e}_a$, $\overline{b} = \overline{\mu}_b \cdot \overline{e}_b$, де $\mu_a := (a, m)$, $\mu_b := (b, m)$, a, b – прообрази $\overline{\mu}_a$, $\overline{\mu}_b$, $\overline{a}$, $\overline{b}$ в R, $\overline{e}_a, \overline{e}_b \in U(R_m)$. Коренем рівняння (1) буде

$$\overline{c} = \overline{\left(\frac{\mu_b}{\mu_a}\right)} \cdot (\overline{e}_a)^{-1} \cdot \overline{e}_b \tag{2}$$

(див. доведення теореми 1 в [1]). Отже, множиною всіх коренів рівняння (1) є $\overline{c} + \mathrm{Ann}(\overline{a})$. Використавши твердження 5, маємо

$$\overline{c} + \mathrm{Ann}(\overline{a}) = \overline{c} + \overline{\alpha}_a R_m, \qquad \text{де} \qquad \alpha_b := \frac{m}{(b, m)} \in R.$$

Отже,

$$\overline{c} + \mathrm{Ann}(\overline{a}) = \overline{\left(\frac{\mu_b}{\mu_a}\right)} \cdot (\overline{e}_a)^{-1} \cdot \overline{e}_b + \overline{\left(\frac{m}{\mu_a}\right)} R_m =$$

$$= \left(\overline{\left(\frac{\mu_b}{\mu_a}\right)} \cdot (\overline{e}_a)^{-1} \cdot \overline{e}_b\right) \cdot \left(\overline{1} + \overline{\left(\frac{m}{\mu_b}\right)} R_m\right).$$

Таким чином,

$$\overline{c} + \mathrm{Ann}(\overline{a}) = \overline{c} \cdot \left(\overline{1} + \overline{\left(\frac{m}{\mu_b}\right)} R_m\right). \tag{3}$$

Оскільки R – адекватне кільце, то елемент $\mu_a = (a, m)$ можна записати у вигляді $\mu_a = s \cdot t$, де $\left(t, \frac{m}{\mu_b}\right) = 1$, а кожний дільник елемента s має спільний дільник з $\frac{m}{\mu_b}$. Розглянемо рівняння

$$\frac{m}{\mu_b} \cdot x \equiv -1 (\mathrm{mod}\, t).$$

Оскільки $\left(t, \frac{m}{\mu_b}\right) = 1$, то це рівняння розв'язне і має деякий корінь x_0. Отже, $1 + \frac{m}{\mu_b} \cdot x_0 = tk$ при деякому $k \in R$. Таким чином, $\overline{c}_1 := \overline{c} \cdot \overline{t} \cdot \overline{k}$ є коренем рівняння (1) (див. рівність (3)).

Покажемо, що $\overline{c}_1$ ділиться на решту коренів рівняння (1). Нехай $\overline{d}$ – довільний корінь цього рівняння. На підставі рівності (3) елемент $\overline{d}$ має вигляд $\overline{d} = \overline{c} \cdot \left(\overline{1} + \overline{\left(\frac{m}{\mu_b}\right)}\,\overline{\ell} \right)$, де $\overline{\ell} \in R_m$. Отже, прообраз елемента $\overline{d}$ в R має вигляд $d = c \cdot q$, де $q := 1 + \frac{m}{\mu_b}\ell$. Маємо

$$(d, m) = (cq, m) = (c, m)\left(\frac{c}{(c, m)}q, \frac{m}{(c, m)}\right) = (c, m)\left(q, \frac{m}{(c, m)}\right).$$

Із рівності (2) випливає, що $(c, m) = \frac{\mu_b}{\mu_a}$. Зважаючи на те, що $\left(q, \frac{m}{\mu_b}\right) = 1$, отримуємо

$$(d, m) = \frac{\mu_b}{\mu_a}\left(q, \frac{m}{\mu_b}\mu_a\right) = \frac{\mu_b}{\mu_a}(q, \mu_a) = \frac{\mu_b}{\mu_a}q_1,$$

де $q_1 := (q, \mu_a)$. Таким чином, $q_1 \mid \mu_a = s \cdot t$. Припустимо, що $(q_1, s) = \sigma \neq 1$. Оскільки $\sigma \mid s$, то згідно з тими обмеженнями, які накладено на елемент s, маємо $\left(\sigma, \frac{m}{\mu_b}\right) \neq 1$. Оскільки $\sigma \mid q_1$, то і $\left(q_1, \frac{m}{\mu_b}\right) \neq 1$. З іншого боку, $q_1 \mid q$, де $\left(q, \frac{m}{\mu_b}\right) \neq 1$ – протиріччя. Отже, $(q_1, s) = 1$. Це означає, що $q_1 \mid t$. Отже, $(d, m) = (c, m)q_1 \mid (c, m)t$, тобто $\overline{(d, m)} \mid \overline{(c, m)} \cdot \overline{t}$. Оскільки $\overline{d} = \overline{(d, m)}\,\overline{e}_d$, де $\overline{e}_d \in R_m$, то $\overline{d} \mid \overline{c}_1$. Таким чином, $\overline{c}_1$ ділиться на всі корені рівняння (1).

Припустимо, що $\overline{s}_1$ і $\overline{s}_2$ – корені рівняння (1), які діляться на решту його коренів. Тоді $\overline{s}_1$ і $\overline{s}_2$ ділять одне одного. З огляду на твердження 4, $\overline{s}_1$ і $\overline{s}_2$ є асоційованими в кільці R_m. ♦

Розглянемо рівняння $\overline{a} \cdot \overline{x} = \overline{0}$. Множиною його коренів є $\mathrm{Ann}(\overline{a})$. Очевидно, що $\overline{0} \in \mathrm{Ann}(\overline{a})$ і ділиться на решту коренів цього рівняння.

► ***Приклад 1***. Знайдемо корінь рівняння $\overline{12} \cdot \overline{x} = \overline{36}$ у кільці $R_m = \mathbb{Z}_{72}$, який ділиться на решту його коренів.

Використаємо позначення теореми 2:

$$m = 72,\ a = 12,\ b = 36,\quad \mu_a = (12, 72) = 12,\quad \mu_b = (36, 72) = 36,\ c = 3.$$

Зважаючи на те, що

$$\mathrm{Ann}(\overline{12}) = 6 \cdot \mathbb{Z}_{72} = \left\{\overline{0}, \overline{6}, \overline{12}, \overline{18}, \overline{24}, \overline{30}, \overline{36}, \overline{42}, \overline{48}, \overline{54}, \overline{60}, \overline{66}\right\},$$

отримуємо, що множиною розв'язків цього рівняння є

$$\overline{3} + \mathrm{Ann}(\overline{12}) = \left\{\overline{3}, \overline{9}, \overline{15}, \overline{21}, \overline{27}, \overline{33}, \overline{39}, \overline{45}, \overline{51}, \overline{57}, \overline{63}, \overline{69}\right\}.$$

Запишемо елемент $\mu_a = 12$ у вигляді добутку $12 = s \cdot t$, де $\left(t, \frac{m}{\mu_b}\right) = (t, 2) = 1$, а кожний дільник s має спільний дільник з $\frac{m}{\mu_b} = 2$. Очевидно, що $t = 3$ і $s = 4$. Розглянемо рівняння

$$\frac{m}{\mu_b} \cdot x \equiv -1 (\mathrm{mod}\, t),$$

тобто рівняння

$$2 \cdot x \equiv -1 (\mathrm{mod}\, 3).$$

Його коренем є $x_0 = 1$. Маємо $2 \cdot (1) + 1 = 3 = tk$. Таким чином, на підставі теореми 2, $\overline{c}_1 = \overline{c} \cdot \overline{t} \cdot \overline{k} = \overline{3} \cdot \overline{3} = \overline{9}$, є коренем, який ділиться на решту коренів рівняння $\overline{12} \cdot \overline{x} = \overline{36}$.

Потрібно зауважити, що серед коренів рівняння $\overline{12} \cdot \overline{x} = \overline{36}$ є елемент $\overline{27}$, який, на перший погляд, не ділить $\overline{c}_1 = \overline{9}$. Проте це не так. Щоб переконатися у цьому, застосуємо методи, які використовувалися при доведенні лем 2 і 3 у [3]. Для цього в кільці $\mathbb{Z}$ розглянемо рівняння

$$27 \cdot x \equiv 9 (\mathrm{mod}\, 72).$$

Оскільки $(27, 72) = 9$, то це рівняння має розв'язок. Кільце $\mathbb{Z}$ є адекватним, а отже, має стабільний ранг 1.5. Тоді з теореми 1.9 із [13] випливає, що серед його коренів є такі, які є взаємно простими з 3. Зокрема, таким є корінь $x_0 = 11$. Отже, $\overline{9} = \overline{27} \cdot \overline{11}$, де, згідно з твердженням 1, $\overline{11} \in U(\mathbb{Z}_{72})$. Таким чином, $\overline{27}$ асоційоване до $\overline{9}$ і є одним із тих коренів, що діляться на решту коренів рівняння $\overline{12} \cdot \overline{x} = \overline{36}$ у кільці $\mathbb{Z}_{72}$. ◄

1. *Щедрик В. П.* Кільця Безу стабільного рангу 1.5 // Укр. мат. журн. – 2015. – **67**, № 6. – С. 849–860.
   Те саме: *Shchedryk V. P.* Bezout ring of stable range 1.5 // Ukr. Math. J. – 2015. – **67**, No. 6. – P. 960–974. – https://doi.org/10.1007/s11253-015-1126-9.
2. *Щедрик В. П.* Лівий найбільший спільний дільник і ліве найменше спільне кратне всіх розв'язків матричного рівняння $BX = A$ над комутативною областю елементарних дільників // Укр. мат. журн. – 2021. – **73**, № 2. – С. 261–267. – https://doi.org/10.37863/umzh.v73i2.6321.
   Те саме: *Shchedryk V. P.* The left greatest common divisor and the left least common multiple for all solutions of the matrix equation $BX = A$ over a commutative domain of elementary divisors // Ukr. Math. J. – 2021. – **73**, No. 2. – P. 303–310. – https://doi.org/10.1007/s11253-021-01923-0.
3. *Bovdi V. A., Shchedryk V. P.* Generating solutions of a linear equation and structure of elements of the Zelisko group // Linear Algebra Appl. – 2021. – **625**. – P. 55–67. – https://doi.org/10.1016/j.laa.2021.04.019.
4. *Bovdi V. A., Shchedryk V. P.* Generating solutions of a linear equation and structure of elements of the Zelisko group II // http://arxiv.org/abs/2201.02817v1. – https://doi.org/10.2989/16073606.2022.2112629.
5. *Don F. J. H.* On the symmetric solutions of a linear matrix equation // Linear Algebra Appl. – 1987. – **93**. – P. 1–7.
6. *Helmer O.* The elementary divisor theorem for certain rings without chain conditions // Bull. Amer. Math. Soc. – 1943. – **49,** No. 4. – P. 225–236. – https://doi.org/10.1090/S0002-9904-1943-07886-X.
7. *Kaplansky I.* Elementary divisors and modules // Trans. Amer. Math. Soc. – 1949. – **66,** No. 2. – P. 464–491. – https://doi.org/10.1090/S0002-9947-1949-0031470-3.
8. *Khatri C. G., Mitra S. K.* Hermitian and nonnegative definite solutions of linear matrix equations // SIAM J. Appl. Math. – 1976. – **31**, No. 4. – P. 579–585. – https://doi.org/10.1137/0131050.
9. *Magnus J. R.* L-structured matrices and linear matrix equations // Linear Algebra Appl. – 1983. – **14**, No. 1. – P. 67–88. – https://doi.org/10.1080/03081088308817543.
10. *Magnus J. R., Neudecker H.* The elimination matrix: Some lemmas and applications // SIAM J. Algebraic Discrete Methods. – 1980. – **1**, No. 4. – P. 422–449. – https://doi.org/10.1137/0601049.
11. *Ran A. C. M., Reurings M. C. B.* A fixed point theorem in partially ordered sets and some applications to matrix equations // Proc. Amer. Math. Soc. – 2004. – **132**, No. 5. – P. 1435–1443. – https://doi.org/10.1090/S0002-9939-03-07220-4.

12. *Recht B., Fazel M., Parrilo P. A.* Guaranteed minimum-rank solutions of linear matrix equations via nuclear norm minimization // SIAM Review. – 2010. – **52**, No. 3. – https://doi.org/10.1137/070697835.
13. *Shchedryk V.* Arithmetic of matrices over rings – Київ: Академперіодика, 2021. – 278 с. – https://doi.org/10.15407/akademperiodika.430.278. – http://www.iapmm.lviv.ua/14/index.htm.
14. *Vetter W. J.* Vector structures and solutions of linear matrix equations // Linear Algebra Appl. – 1975. – **10**, No. 2. – P. 181–188. – https://doi.org/10.1016/0024-3795(75)90010-5.

ARITHMETIC PROPERTIES OF THE SOLUTIONS OF LINEAR EQUATIONS

The solutions of the equation of the form $a \cdot x = b$ *in homomorphic image of an adequate ring are studied. It is known that the greatest common divisor of all solutions of such equation is its solution again. It is proved that among the solutions of this equation there are also those that are divisible by the rest of its solutions. Moreover, such solutions are associated.*

Key words: *solutions of a linear equation, stable range of ring, adequate ring.*

Ін-т прикл. проблем механіки і математики
ім. Я. С. Підстригача НАН України, Львів

Одержано
12.03.22