

Харківський національний університет імені В.Н. Каразіна
Факультет математики і інформатики
Кафедра прикладної математики

Кваліфікаційна робота

освітньо-кваліфікаційний рівень: **магістр**

на тему **«Неявні лінійні різницеві рівняння над
деякими скінченними комутативними
кільцями»**

Виконав: студент групи M162 VI курсу
(другий магістерський рівень),
спеціальності 111
“Математика”
освітньо-професійної програми
“Математика”
Генералов М.В.

Керівник: доктор фіз.-мат. наук,
доцент кафедри
прикладної математики
Півень О.Л.

Рецензент: доктор фіз.-мат. наук,
доцент, провідний науковий
співробітник відділу матема-
тичної фізики ФТІНТ ім. Б.І.
Веркіна НАН України
Нессонов М.І.

Анотації

Генералов М.В. Неявні лінійні різницеві рівняння над деякими скінченними комутативними кільцями.

Наведено класифікацію кілець порядку p^2 . Досліджено неявне лінійне різницеве рівняння над деякими скінченним комутативними кільцями. Для цього рівняння отримано теореми існування та єдиності розв'язку і одержано загальний розв'язок. Також записано приклади, що ілюструють роботу доведених теорем.

Heneralov M.V. Implicit linear difference equations over some finite commutative rings.

The classification of p^2 -order rings is given. Investigated the implicit linear difference equations over some finite commutative rings. We obtained the theorems of existence and uniqueness of the solution for this equation and got the formulas of the general solution. We give the examples, which show the work of the proved theorems.

Зміст

Анотації	2
Вступ	5
1. Загальна інформація про кільця	7
1.1. Означення.	7
1.2. Властивості та приклади скінченних кілець.	9
1.3. Опис кілець порядку p^2 , де p просте.	10
1.3.1. Представлення кільця за допомогою адитивних генераторів	10
1.3.2. Кільце з єдиним адитивним генератором	11
1.3.3. Пряма сума полів	12
1.3.4. Поле Галуа	13
1.3.5. Спеціальне кільце	14
2. Розв'язність неявних лінійних різницьових рівнянь над деякими скінченними комутативними кільцями	16
2.1. Постановка задачі.	16
2.2. Розв'язність лінійного різницьового рівняння над полем . . .	16
2.3. Розв'язність лінійного різницьового рівняння над прямою сумою скінченних полів	18
2.4. Розв'язність неявного лінійного різницьового рівняння над спеціальним кільцем порядку 4	21
Висновки	25

Список використаних джерел

26

Вступ

Теорія лінійних різницевих рівнянь є важливим розділом математики, котрий має широкий спектр застосувань (див., наприклад, [1–4]). У 80–90-х роки ХХ століття в роботах [4–6] було розвинено теорію неявних лінійних різницевих рівнянь у векторних просторах. На відміну від класичної теорії, у новій теорії необоротні оператори грають важливу роль. У зв’язку з цим цікавою виявилась проблема дослідження неявного лінійного різницевого рівняння з коефіцієнтами із довільного комутативного кільця. До сьогодні неявні різницеві рівняння над областями цілісності досліджено у [7], і більш детально над кільцем цілих чисел у [8–10]. У [11] такі рівняння досліджувались у різних класах топологічних векторних просторів. У даній кваліфікаційній роботі такі рівняння досліджуються над деякими скінченними комутативними кільцями.

У розділі 1 розглядаються необхідні в цій роботі означення загальної теорії кілець (підрозділ 1.1) та деякі властивості і приклади скінченних кілець (підрозділ 1.2), після чого в підрозділі 1.3 наводиться класифікація всіх комутативних кілець порядку p^2 з одиницею, що є результатом статті [12, с. 250]. Виявляється, що існує 4 таких кільця: кільце з єдиним адитивним генератором R_1 , пряма сума полів R_2 , поле Галуа R_3 і кільце спеціального вигляду R_4 (див. п. 1.3.5). Наведено альтернативні зображення цих кілець у вигляді факторкілець, а для спеціального кільця і матричне зображення.

Для натурального числа m позначимо через \mathbb{Z}_m кільце лишків за модулем m . Для простого числа p і елементу $s \in \mathbb{Z}_p$ визначимо $R'(s) = \mathbb{Z}_p[t]/(t^2 - s)$.

В підрозділі 1.3 доведено ряд наступних ізоморфностей:

$$R'(s) \simeq \begin{cases} \text{спеціальному кільцю } R_4, & p = 2 \text{ або } s = 0, \\ R_2 \text{ (прямій сумі полів)}, & p > 2 \text{ і } s \text{ це квадратичний лишок}, \\ \text{полю з } p^2 \text{ елементів } R_3, & p > 2 \text{ і } s \text{ це квадратичний нелишок}. \end{cases}$$

Нехай A, B, F_n ($n \in \mathbb{Z}_+ = \{0, 1, 2, \dots\}$) є заданими елементами скінченного комутативного кільця R з одиницею. У розділі 2 досліджується неявне лінійне різницеве рівняння

$$BX_{n+1} = AX_n + F_n, \quad n \in \mathbb{Z}_+ \quad (0.1)$$

над кільцем R . Рівняння (0.1) називається *неявним*, якщо B не є оборотним елементом кільця R [7]. Сформульовано і доведено критерії розв'язності рівняння (0.1) над прямою сумою полів (теорема 2.2) та над спеціальним кільцем порядку 4, тобто кільцем R_4 для випадку $p = 2$ (теорема 2.4). Разом із критеріями отримано формулу загального розв'язку відповідних рівнянь у випадку існування розв'язку. Розглянуто приклади, що ілюструють роботу доведених теорем (див. приклади 2.3 і 2.5).

Рівняння (0.1) над кільцем лишків \mathbb{Z}_m для довільного натурального $m \geq 2$ досліджувалось в [13]. Результати цієї роботи оприлюднено також на міжнародних наукових конференціях [14–16].

Розділ 1

Загальна інформація про кільця

1.1. Означення.

Надамо означення кільця і суміжних понять (комутативне кільце, оборотний елемент кільця, одиниця кільця, і поле) [17–19].

Означення 1.1. Нехай R це множина. Ця множина називається *кільцем*, якщо задані бінарні операції ‘+’ (названу *додаванням*) і ‘ \cdot ’ (*множенням*), $+, \cdot : R \rightarrow R$ тоді і тільки тоді, коли справедливі наступні аксіоми:

1. $(R, +)$ — є абелева група. Тобто:
 - (i) Існує нейтральний елемент (нуль) $0 = 0_R$: $0_R + x = x + 0_R = x$, $\forall x \in R$.
 - (ii) Операція додавання є асоціативною і комутативною, тобто $(a + b) + c = a + (b + c)$ і $a + b = b + a$, $\forall a, b, c \in R$.
 - (iii) $\forall x \in R \exists y = (-x) \in R$ (протилежний) такий, що $x + y = y + x = 0$.
2. (R, \cdot) це напівгрупа, тобто $(a \cdot b)c = a(b \cdot c)$ для всіх $a, b, c \in R$.
3. Дистрибутивність: $(a + b)c = ac + bc$, $a(b + c) = ab + ac$, $\forall a, b, c \in R$.

Позначення операції множення часто упускають, тобто ab і $a \cdot b$, де $a, b \in R$, значать одне.

Означення 1.2. Кільце R *комутативне*, якщо $ab = ba$, $\forall a, b \in R$.

Означення 1.3. Елемент $x \in R$ називають оборотним (*invertible*), якщо існує обернений до нього $y = x^{-1} \in R$ такий, що $xy = yx = 1$.

Означення 1.4. Кільце R є *одиницею*, якщо існує $1 = 1_R \in R$ (одиниця): $1_R \cdot x = x, \forall x \in R$.

Означення 1.5. Кільце R є *полем* тоді і тільки тоді, коли R містить одиницю, $R \neq 0$ і будь-який ненульовий елемент кільця R є оборотним.

Далі розглядаємо тільки комутативні кільця з одиницею, $1_R \neq 0$.

Означення 1.6. Елемент $x \in R$ називають *дільником нуля*, якщо в кільці R існує елемент $y \neq 0$ такий, що $xy = 0$.

Означення 1.7. Кільце R називають *скінченним* якщо R скінченне як множина. Число елементів такого кільця називатимемо *порядком* кільця R .

Теорії скінченних кілець присвячено монографії [17,20], а теорії скінченних полів — монографію [21].

Означення 1.8. Нехай R є кільце. *Ідеал* I кільця R є підкільце кільця R таке, що $IR \subseteq I$.

Якщо $I = aR$ для деякого $a \in R$, то I називають *головним ідеалом* кільця R і позначають $I = (a)$.

Означення 1.9. Елемент x кільця R називають *нільпотентним*, якщо $x^n = 0$ для деякого натурального n . Індекс нільпотентності елемента x — це найменше натуральне число n , що задовольняє цій умові.

Означення 1.10. Нехай R — кільце. Характеристика кільця R — це $\text{char } R = \min \{n \in \mathbb{N} : n \cdot 1_R = 0\}$, де $nx = \underbrace{x + \dots + x}_{n \text{ доданків}}$. Якщо такого $n \in \mathbb{N}$ не існує, то $\text{char } R = 0$.

Означення 1.11. Нехай R — кільце, і I це його ідеал. Тоді множина R/I елементів $x + I$, де $x \in R$, називається факторкільцем, якщо на ній уведені операції $(+, \cdot)$ наступним чином:

- $(a + I) + (b + I) = (a + b) + I$,
- $(a + I)(b + I) = ab + I$.

Означення 1.12. Ізоморфізм кілець R і Q — це така бієкція $\varphi: R \rightarrow Q$, що зберігає операції кільця, тобто виконані для всіх елементів r_1, r_2 кільця R виконані рівності

- $\varphi(r_1 + r_2) = \varphi(r_1) + \varphi(r_2)$,
- $\varphi(r_1 r_2) = \varphi(r_1) \varphi(r_2)$.

Якщо ізоморфізм кілець R і Q існує, то кажуть, що кільця R і Q ізоморфні; позначатимемо це $R \simeq Q$.

Означення 1.13. Якщо R_1, \dots, R_n — кільця, то кажемо, що R є прямою сумою цих кілець і позначаємо $R = \bigoplus_{i=1}^n R_i$, якщо $R = R_1 \times \dots \times R_n$ і операції $(+, \cdot)$ уведені по координатно. Множина R із так визначеними операціями є кільцем.

1.2. Властивості та приклади скінченних кілець.

Далі розглядаємо скінченні комутативні кільця з одиницею.

Твердження 1.1. Характеристика скінченного кільця є додатною [20, с. 1].

Теорема 1.14. Нехай кільце R скінченне. Тоді будь-який необоротний елемент кільця R це дільник нуля 0 [22, с. 20].

Наведемо різноманітні приклади скінченних кілець.

Приклад 1.15. Кільце класів лишків $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$. Його елементи це *класи*, зазвичай позначаються як $[n]_m$ або $[n]$ (якщо m зрозуміло): вони дорівнюють $n + m\mathbb{Z}$ (відповідно).

Приклад 1.16. Кільця $R_k^{(m)} = \mathbb{Z}_{p^k}[t]/(t^m)$, де p фіксоване просте.

Приклад 1.17. Поля \mathbb{F}_q , де q ступінь простого [17, с. 82, с. 92]. Справедливе наступне представлення: $\mathbb{F}_{p^n} = \mathbb{Z}_p[t]/(f)$, де f незвідний многочлен ступені n зі старшим коефіцієнтом 1.

Приклад 1.18. Факторкільце $\mathbb{Z}[t]/(10, t^2)$.

Наступна теорема описує комутативні кільця з одиницею простого порядку.

Теорема 1.19 ([12, с. 249]). *Будь-яке скінченне кільце з простого числа елементів є полем.*

Наступна теорема дає повну класифікацію скінченних комутативних кілець порядку m , що дорівнює добутку попарно різних простих чисел.

Теорема 1.20 ([12, с. 250]). *Нехай R — комутативне кільце з одиницею порядку m , де m дорівнює добутку $p_1 \dots p_k$ попарно різних простих чисел. Тоді $R \simeq \mathbb{Z}_{p_1} \oplus \dots \oplus \mathbb{Z}_{p_k}$.*

1.3. Опис кілець порядку p^2 , де p просте.

1.3.1. Представлення кільця за допомогою адитивних генераторів

Елементи кільця \mathbb{Z}_p для спрощення викладок позначатимемо так само, як їх представників.

Уведемо до розгляду представлення кільця.

Нехай R є довільне кільце (можливо, некомутативне або без одиниці). Адитивним порядком елемента $x \in R$ називається найменше натуральне n , при якому $nx = 0$.

Нехай g_1, \dots, g_k — адитивні генератори кільця R (тобто $\alpha_1 g_1 + \dots + \alpha_k g_k \neq 0$, якщо серед цілих чисел $\alpha_1, \dots, \alpha_k$ є принаймні одне ненульове, і $\{\alpha_1 g_1 + \dots + \alpha_k g_k : \alpha_1, \dots, \alpha_k \in \mathbb{Z}\} = R$), цілі числа m_1, \dots, m_k — їх адитивні порядки відповідно, множення задається рівностями $g_i g_j = \sum_{t=1}^k c_{ij}^t g_t$, де c_{ij}^t цілі, $i, j = \overline{1, k}$ [12, с. 248], [23]. Позначаємо це наступним чином:

$$R \simeq \left\langle g_1, \dots, g_k; m_i g_i = 0 \text{ при } i = 1, \dots, k, g_i g_j = \sum_{t=1}^k c_{ij}^t g_t \right\rangle.$$

Наприклад $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \simeq \langle a, b; 2a = 2b = 0, a^2 = a, b^2 = b, ab = ba = 0 \rangle$.

У [12, с. 250] наведено класифікацію всіх кілець порядку p^2 (включно некомутативні або без одиниці) за допомогою такого представлення і показано, що всього таких кілець 11 з точністю до ізоморфізму.

Перелічимо ті з них, які є комутативними та мають одиницю. Уведемо позначення $R'(s) = \mathbb{Z}_p[t]/(t^2 - s)$. Кільце $R'(s)$ має рівно p^2 елементів.

1.3.2. Кільце з єдиним адитивним генератором

$$R_1 = \langle a; p^2 a = 0, a^2 = a \rangle$$

Це кільце ізоморфне \mathbb{Z}_{p^2} [12, с. 250]. Кільце R_1 не ізоморфне ні одному кільцю $R'(s)$ при жодному p .

1.3.3. Пряма сума полів

$$R_2 = \langle a, b; pa = pb = 0, a^2 = a, b^2 = b, ab = ba = 0 \rangle \simeq \mathbb{Z}_p + \mathbb{Z}_p \quad (1.1)$$

Означення 1.21. Елемент $s \in \mathbb{Z}_p$ називатимемо квадратичним лишком за модулем p [24, с. 68], якщо $s = j^2$ (мовою чисел, $s \equiv j^2 \pmod{p}$) при деякому ненульовому j . Число a називають квадратичним нелишком за модулем p , якщо $s \not\equiv j^2 \pmod{p}$ при жодному $j \in \mathbb{Z}_p$.

Теорема 1.22. Нехай s є квадратичним лишком за модулем $p > 2$. Тоді $R'(s) \simeq R_2$.

Доведення. Для довільного елементу $x = \alpha + t\beta \in R'(s)$ маємо

$$x^2 = \alpha^2 + s\beta^2 + t\,2\alpha\beta.$$

Нехай $x^2 = x$ і $x \neq 0$. Тоді в \mathbb{Z}_p виконані рівності:

$$\begin{cases} \alpha^2 + s\beta^2 = \alpha, \\ 2\alpha\beta = \beta. \end{cases} \quad (1.2)$$

Якщо $\beta = 0$, то з системи (1.2) випливає, що $\alpha^2 = \alpha$. Враховуючи, що $\alpha \neq 0$, маємо $x = 1$.

Нехай $\beta \neq 0$. Тоді з другого рівняння системи (1.2) одержується рівність $\alpha = 2^{-1} = \frac{p+1}{2}$ (число p непарне).

Домножуючи перше рівняння системи (1.2) на 4, отримуємо еквівалентне рівняння

$$4s\beta^2 = 4(\alpha - \alpha^2). \quad (1.3)$$

Виконаємо алгебраїчні перетворення:

$$4(\alpha - \alpha^2) = 4\left(\frac{p+1}{2} - \frac{p^2 + 2p + 1}{4}\right) = 2 - 1 = 1.$$

Користуючись цією рівністю, маємо, що розв'язком рівняння (1.3) є $\beta = \pm \frac{1}{2r}$, де $s = r^2$.

Відповідно, $x_{1,2} = \frac{p+1}{2} \pm \frac{1}{2b}t$ є розв'язками рівняння $x^2 = x$ у $R'(s)$.

Виконаємо обчислення: $x_1 x_2 = \alpha^2 - s\beta^2 = 4^{-1}(p^2 + 2p + 1 - 1) = 0$. Покажемо, що x_1 і x_2 є адитивними генераторами кільця R_4 . Для довільного елемента $\gamma + t\delta$ кільця \mathbb{Z}_p знайдемо такі $\lambda, \mu \in \mathbb{Z}_p$, що $\lambda \cdot (\alpha + t\beta) + \mu \cdot (\alpha - t\beta) = \gamma + t\delta$. Прирівнюючи коефіцієнти при однакових степенях t , отримаємо систему лінійних рівнянь над \mathbb{Z}_p відносно λ, μ , яку запишемо у матричному вигляді:

$$M \begin{pmatrix} \lambda \\ \mu \end{pmatrix} = \begin{pmatrix} \gamma \\ \delta \end{pmatrix}, \text{ де } M = \begin{pmatrix} \alpha & \beta \\ \alpha & -\beta \end{pmatrix}. \quad (1.4)$$

Визначник матриці M дорівнює $-2\alpha\beta \neq 0$, тому, за теоремою I.7 а [25], матриця M є оборотною. Із рівності (1.4) випливає, що

$$\begin{pmatrix} \lambda \\ \mu \end{pmatrix} = (-2\alpha\beta)^{-1} \begin{pmatrix} -\beta & -\beta \\ -\alpha & \alpha \end{pmatrix} \begin{pmatrix} \gamma \\ \delta \end{pmatrix}.$$

Отже, x_1 і x_2 справді є адитивними генераторами кільця $R'(s)$. Зазначимо, що порядки адитивних генераторів елементів x_1, x_2 дорівнюють p . Тому кільце $R'(s)$ має представлення R_2 , тобто $R'(s) \simeq R_2$. \square

1.3.4. Поле Галуа

$$R_3 = \begin{cases} \langle a, b; pa = pb = 0, a^2 = a, b^2 = ja, ab = b, ba = b \rangle, \\ \quad j \text{ квадратичний нелишок у } \mathbb{Z}_p, \quad p \neq 2, \\ \langle a, b; 2a = 2b = 0, a^2 = a, b^2 = a + b, ab = b, ba = b \rangle, \quad p = 2 \end{cases}$$

Це кільце — поле. Зазвичай його називають *поле Галуа порядку p^2* , або *поле з p^2 елементів*, і позначають \mathbb{F}_{p^2} . Загальновідомо: для кожного простого p існує єдине, з точністю до ізоморфізму, поле порядку p^2 [21].

Поле R_3 ізоморфне такому факторкільцю: $\mathbb{Z}_p[t]/(f)$, де поліном $f = t^2 + at + b$ незвідний над кільцем $\mathbb{Z}_p[t]$ [22, задача 4.17].

При $p > 2$ у якості f можна обрати $t^2 - r$, де r це квадратичний нелишок за модулем p — тоді $R_3 \simeq R'(r)$. Зокрема, якщо $p \equiv 3 \pmod{4}$, то обрання $-1 \equiv p - 1$ як квадратичного нелишку дає представлення $F_{p^2} \simeq R'(-1) = \mathbb{Z}_p[t]/(t^2 + 1)$ [22, задача 4.35].

1.3.5. Спеціальне кільце

$$R_4 = \langle a, b; pa = pb = 0, a^2 = 0, b^2 = b, ab = a, ba = a \rangle$$

Оскільки $ba = b$ і $bb = b$, то $bx = x$ для всіх $x \in R_4$, отже $b = 1_{R_4}$.

Для спрощення позначень далі писатимемо, що елементи кільця $R'(0)$ мають вигляд $\alpha t + \beta$ ($\alpha, \beta \in \mathbb{Z}_p$), враховуючи, що $t^2 = 0$. Покажемо, що $R'(0) = \mathbb{Z}_p[t]/(t^2) \simeq R_4$. Для цього розглянемо лінійну функцію φ , що ставить у відповідність генераторам a, b представлення R_4 наступні елементи: $\varphi(a) = [t]$, $\varphi(b) = 1$. Тоді φ є ізоморфізмом, бо $a^2 = 0$, b — одиниця.

Вірною є ізоморфізмість $R_4 \simeq R'(s)$, коли $p = 2$ [22, задача 4.16].

$$\text{Тепер покажемо, що } R_4 \simeq S_1 = \left\{ \begin{pmatrix} \alpha & \beta \\ 0 & \alpha \end{pmatrix} \mid \alpha, \beta \in \mathbb{Z}_p \right\}.$$

$$\text{Одиниця } 1_{S_1} \text{ в } S_1 \text{ має вигляд } \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Визначимо адитивну функцію $\varphi: R_4 \rightarrow S_1$ умовами $\varphi(b) = 1_{S_1}$ і $\varphi(a) = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = s_1$. Вочевидь, 1_{S_1} і s_1 є адитивними генераторами кільця S_1 ,

$\varphi(b)^2 = \varphi(b)$, $\varphi(a)^2 = 0$ і $\varphi(a)\varphi(b) = \varphi(a)$. Отже, φ є ізоморфізмом кілець R_4 і S_1 , а R_4 є зображенням кільця S_1 , тобто $R_4 \simeq S_1$.

Далі спеціальним кільцем називатимемо кільце $R'(0)$ і саме його позначатимемо R_4 .

Визначимо оборотні та нільпотентні елементи цього кільця.

Якщо елемент кільця $R'(0)$ має вигляд $e = a + bt$, де a, b це елементи кільця \mathbb{Z}_p , то елемент e оборотний, коли $a \neq 0$, і $e^p = 0$, якщо $a = 0$. Зокрема, будь-який необоротний елемент кільця $R'(0)$ є нільпотентним.

Розділ 2

Розв'язність неявних лінійних різницевих рівнянь над деякими скінченними комутативними кільцями

2.1. Постановка задачі.

Через \mathbb{Z}_+ позначатимемо множину $\{0, 1, 2, \dots\}$.

Нехай A, B, F_n ($n \in \mathbb{Z}_+$) — задані елементи комутативного кільця R з одиницею. Розглянемо лінійне різницеве рівняння першого порядку

$$BX_{n+1} = AX_n + F_n, \quad n \in \mathbb{Z}_+, \quad (2.1)$$

над кільцем R . Рівняння (2.1) називається *неявним*, якщо B є необоротним елементом кільця R [7].

2.2. Розв'язність лінійного різницевого рівняння над полем

Наступна допоміжна лема встановлює достатні умови розв'язності рівняння (2.1) над полем.

Лема 2.1. *Нехай R — це поле. Справедливі наступні твердження.*

1. (i) *Якщо $B \neq 0$, то загальний розв'язок рівняння (2.1) визначено*

наступним чином:

$$X_n = B^{-n} A^n X_0 + \sum_{s=0}^{n-1} B^{-s-1} A^s F_{n-s-1}, \quad n \in \mathbb{N} = \{1, 2, \dots\}, \quad (2.2)$$

де $X_0 \in R$ довільне.

(ii) Якщо $B = 0$ і $A \neq 0$, то єдиний розв'язок рівняння (2.1) визначено формулою

$$X_n = -A^{-1} F_n, \quad n \in \mathbb{Z}_+. \quad (2.3)$$

2. Якщо $B = A = 0$ і $F_n = 0$ при всіх $n \in \mathbb{Z}_+$, то будь-яка послідовність $\{X_n\}_{n=0}^\infty$ є розв'язком рівняння (2.1).
3. Якщо $B = A = 0$ і $F_n \neq 0$ при деякому $n \in \mathbb{Z}_+$, то рівняння (2.1) не має розв'язків.

Доведення. Доведемо твердження 1 (i): якщо $B \neq 0$, то рівняння (2.1) є явним. Рівняння (2.1) є еквівалентним рівнянню

$$X_{n+1} = B^{-1} A X_n + B^{-1} F_n, \quad n \in \mathbb{Z}_+.$$

Загальний розв'язок цього рівняння, за [3, с. 4], визначається формулою (2.2).

Доведемо твердження 1 (ii): якщо $B = 0$ і $A \neq 0$, рівняння (2.1) має вигляд $A X_n + F_n = 0$, $n \in \mathbb{Z}_+$. Оскільки A є оборотним елементом кільця R , то єдиний розв'язок рівняння (2.1) визначено формулою (2.3).

Твердження 2 і 3 є очевидними. □

2.3. Розв'язність лінійного різницевого рівняння над прямою сумою скінченних полів

Позначимо $I = \{1, 2, \dots, r\}$, де число r натуральне. Розглянемо кільце $R = \bigoplus_{i \in I} K_i$, де K_i — це поле для кожного $i \in I$.

Уведемо $A = (A_1, A_2, \dots, A_r)$, $B = (B_1, B_2, \dots, B_r)$, $F_n = (F_{1,n}, F_{2,n}, \dots, F_{r,n})$ — елементи кільця R . Позначимо $I_B = \{i \in I : B_i = 0\}$, $I_A = \{i \in I : A_i = 0\}$, $I_F = \{i \in I : F_{i,n} = 0 \text{ при всіх } n \in \mathbb{N}\}$.

Очевидно: $I = (I \setminus I_B) \sqcup (I_B \setminus I_A) \sqcup (I_A \cap I_B)$, об'єднання множин тут диз'юнктне.

Наступна теорема є критерієм розв'язності рівняння (2.1) над кільцем R .

Теорема 2.2. Нехай кільце R скінченне й $R = \bigoplus_{i \in I} K_i$, де K_i це поле для кожного $i \in I$. Справедливі наступні твердження.

1. Рівняння (2.1) має скінченне число розв'язків тоді і тільки тоді, коли $I_A \cap I_B = \emptyset$. При цьому рівняння (2.1) має

$$m = \begin{cases} \prod_{i \in I \setminus I_B} \text{card}(K_i), & I_B \neq I, \\ 1, & I_B = I \end{cases}$$

розв'язків і загальний розв'язок цього рівняння має вигляд

$$X_n = (X_{1,n}, \dots, X_{r,n}), \quad n \in \mathbb{Z}_+,$$

$$X_{i,n} = \begin{cases} B_i^{-n} A_i^n X_{i,0} + \sum_{s=0}^{n-1} B_i^{-s-1} A_i^s F_{i,n-s-1}, & i \in I \setminus I_B, \\ -A_i^{-1} F_{i,n}, & i \in I_B, \end{cases} \quad (2.4)$$

де $X_{i,0}$ — довільний елемент поля K_i при кожному $i \in I \setminus I_B$.

Зокрема, рівняння має єдиний розв'язок тоді і тільки тоді, коли $B = 0$ і $I_A = \emptyset$.

2. Рівняння (2.1) має нескінченне число розв'язків тоді і тільки тоді, коли $\emptyset \neq I_A \cap I_B \subset I_F$. При цьому загальний розв'язок цього рівняння має вигляд

$$X_n = (X_{1,n}, \dots, X_{r,n}), \quad n \in \mathbb{Z}_+,$$

$$X_{i,n} = \begin{cases} B_i^{-n} A_i^n X_{i,0} + \sum_{s=0}^{n-1} B_i^{-s-1} A_i^s F_{i,n-s-1}, & i \in I \setminus I_B, \\ -A_i^{-1} F_{i,n}, & i \in I_B \setminus I_A, \\ \text{довільний елемент поля } K_i, & i \in I_A \cap I_B, \end{cases}$$

де $X_{i,0}$ — довільний елемент поля K_i при кожному $i \in I \setminus I_B$.

3. Рівняння (2.1) не має розв'язків тоді і тільки тоді, коли $(I_A \cap I_B) \setminus I_F \neq \emptyset$.

Доведення. Рівняння (2.1) еквівалентне системі рівнянь

$$\begin{cases} B_1 X_{1,n+1} = A_1 X_{1,n} + F_{1,n}, & n \in \mathbb{Z}_+, \\ B_2 X_{2,n+1} = A_2 X_{2,n} + F_{2,n}, & n \in \mathbb{Z}_+, \\ \vdots \\ B_r X_{r,n+1} = A_r X_{r,n} + F_{r,n}, & n \in \mathbb{Z}_+, \end{cases}$$

де $i \in I$. Для кожного $i \in I$ рівняння

$$B_i X_{i,n+1} = A_i X_{i,n} + F_{i,n}, \quad n \in \mathbb{Z}_+, \quad (2.5)$$

розглядається над полем K_i .

Достатні твердження цієї теореми є загалом вичерпними і їх твердження не перетинаються, тому достатньо довести їх.

Доводимо достатність в першому твердженні теореми. Нехай $I_A \cap I_B = \emptyset$. Тоді для будь-якого $i \in I$ або $B_i \neq 0$, або $B_i = 0$ і $A_i \neq 0$. Тоді за першим твердженням леми 2.1 загальний розв'язок рівняння (2.5) визначено рівністю (2.2) у випадку $B_i \neq 0$ або рівністю (2.3) у випадку $B_i = 0$ і $A_i \neq 0$. В обох випадках рівняння (2.1) має скінченну кількість розв'язків. Звідси випливає формула (2.4).

Доводимо достатність в другому твердженні теореми. Якщо $i \notin I_A \cap I_B$, то, як і раніше, за першим твердженням леми 2.1, загальний розв'язок рівняння (2.5) визначено рівністю (2.2) у випадку $B_i \neq 0$ або рівністю (2.3) у випадку $B_i = 0$ і $A_i \neq 0$. Нехай тепер $i \in I_A \cap I_B$. Тоді $F_{i,n} = 0, \forall n \in \mathbb{Z}_+$, то, за твердженням 2 леми 2.1, будь-яка послідовність $\{X_{i,n}\}_{n=0}^{\infty}$ є розв'язком відповідного рівняння (2.5). Тоді за умови $\emptyset \neq I_A \cap I_B \subset I_F$ рівняння (2.1) має нескінченно багато розв'язків.

Доводимо достатність в третьому твердженні теореми. Нехай існує $i \in I_A \cap I_B$ таке, що $i \notin I_F$. Тоді за твердженням 3 леми 2.1 відповідне рівняння (2.5) не має розв'язків. Тому не має розв'язків і рівняння (2.1). Теорему доведено. □

Розглянемо приклад застосування цієї теореми до розв'язання неявного рівняння (2.1) над скінченною прямою сумою скінченних полів.

Приклад 2.3. Розглянемо рівняння

$$(B_1, 0, 0)X_{n+1} = (1, A_2, 0)X_n + F_n, \quad n \in \mathbb{Z}_+ \quad (2.6)$$

над кільцем $R = K_1 \oplus K_2 \oplus K_3$, де K_1, K_2, K_3 є скінченними полями і $B_1 \neq 0$ є елементом поля K_1 , $A_2 \neq 0$ є елементом поля K_2 , $F_n = (F_{1,n}, F_{2,n}, F_{3,n})$ ($n \in \mathbb{Z}_+$). Визначимо: $B = (B_1, 0, 0)$, $A = (1, A_2, 0)$, $I_B = \{2, 3\}$, $I_A = \{3\}$. Якщо $F_{3,n} \neq 0$ при деякому n , то, за третім твердженням теореми 2.2,

рівняння (2.6) не має розв'язків.

Нехай $F_{3,n} = 0$ при всіх $n \in \mathbb{Z}_+$. Тоді, за твердженням 2 теореми 2.2, існує нескінченно багато розв'язків рівняння (2.6). Загальний розв'язок $X_n = (X_{1,n}, X_{2,n}, X_{3,n})$ ($n \in \mathbb{Z}_+$) рівняння (2.6) визначається наступною формулою:

$$\begin{cases} X_{1,n} = B_1^{-n} X_{1,0} + \sum_{s=0}^{n-1} B_1^{-s-1} F_{1,n-s-1}, \\ X_{2,n} = -A_2^{-1} F_{2,n}, \\ X_{3,n} = \text{довільний елемент поля } K_3, \end{cases}$$

де $X_{1,0}$ — довільний елемент поля K_1 .

2.4. Розв'язність неявного лінійного різницевого рівняння над спеціальним кільцем порядку 4

У кільці $R = \mathbb{Z}_2[t]/(t^2)$ (кільце R_4 із п. 1.3.5 для $p = 2$) розглянемо елементи $A = A_0 + t A_1$, $B = B_0 + t B_1$, $F_n = F_{0,n} + t F_{1,n}$ ($n \in \mathbb{Z}_+$), де $A_0, B_0, F_{0,n}, A_1, B_1, F_{1,n}$ ($n \in \mathbb{Z}_+$) — елементи кільця \mathbb{Z}_2 . Наступна теорема є критерієм розв'язності неявного лінійного різницевого рівняння (2.1) над кільцем R .

Теорема 2.4. *Нехай $B \neq 0$. Справедливі наступні твердження.*

1. Рівняння (2.1) має скінченно багато розв'язків тоді і тільки тоді, коли або $A_0 \neq 0$, або $B_0 \neq 0$. При цьому рівняння (2.1) має

$$N = \begin{cases} 4, & B_0 \neq 0, \\ 1, & B_0 = 0 \end{cases}$$

розв'язків і загальний розв'язок цього рівняння має вигляд

$$X_n = \begin{cases} B^{-n} A^n X_0 + \sum_{s=0}^{n-1} B^{-s-1} A^s F_{n-s-1}, & B_0 \neq 0, \\ -A^{-1} F_n - B A^{-2} F_{n+1}, & B_0 = 0, \end{cases}$$

де X_0 — довільний елемент кільця R , якщо $B_0 \neq 0$.

Зокрема, рівняння (2.1) має єдиний розв'язок тоді і тільки тоді, коли $B_0 = 0$ і $A_0 \neq 0$.

2. Рівняння (2.1) має нескінченно багато розв'язків тоді і тільки тоді, коли $A_0 = B_0 = 0$, $F_{0,n} = 0$ при всіх $n \in \mathbb{Z}_+$. Загальний розв'язок цього рівняння визначено рівністю $X_n = X_{0,n} + t X_{1,n}$ ($n \in \mathbb{Z}_+$), послідовність елементів $X_{1,n}$ довільна у \mathbb{Z}_2 , і $\{X_{0,n}\}_{n=0}^{\infty}$ визначено умовою

$$X_{0,n} = B_1^{-n} A_1^n X_{0,0} + \sum_{s=0}^{n-1} B_1^{-s-1} A_1^s F_{0,n-s-1}, \quad n \in \mathbb{N}, \quad (2.7)$$

де $X_{0,0}$ — довільний елемент множини \mathbb{Z}_2 .

3. Рівняння (2.1) не має розв'язків тоді і тільки тоді, коли $A_0 = B_0 = 0$ і $F_{0,n} \neq 0$ при деякому $n \in \mathbb{Z}_+$.

Доведення. Якщо $B_0 \neq 0$, то рівняння (2.1) має єдиний розв'язок, визначений формулою (2.2), оскільки елемент B оборотний (див. 1.3.5). Якщо $B_0 = 0$ і $A_0 \neq 0$, то (2.1) можна переписати у вигляді

$$X_n = B A^{-1} X_{n+1} - A^{-1} F_n, \quad n \in \mathbb{Z}_+.$$

Скориставшись рівністю двічі і рівністю $B^2 = 0$, отримаємо:

$$X_n = -A^{-1} F_n - B A^{-2} F_{n+1}, \quad n \in \mathbb{Z}_+. \quad (2.8)$$

Підставляючи (2.8) у рівняння (2.1) і враховуючи, що $B^2 = 0$, переко-

наємось, що послідовність (2.8) є розв'язком рівняння (2.1):

$$\begin{aligned} BX_{n+1} &= -B(A^{-1}F_{n+1} + BA^{-2}F_{n+2}) = -BA^{-1}F_{n+1} - B^2A^{-2}F_{n+2} = \\ &= A(-A^{-1}F_n - BA^{-2}F_{n+1}) + F_n = AX_n + F_n. \end{aligned}$$

Довели достатність твердження 1.

Нехай $B_0 = A_0 = 0$. Доведемо достатності останніх двох тверджень. Для цього зауважимо, що рівняння (2.1) еквівалентне системі рівнянь

$$\begin{cases} B_0X_{0,n+1} = A_0X_{0,n} + F_{0,n}, & n \in \mathbb{Z}_+, \\ B_0X_{1,n+1} + B_1X_{0,n+1} = A_0X_{1,n} + F_{1,n} + A_1X_{0,n}, & n \in \mathbb{Z}_+ \end{cases}$$

над \mathbb{Z}_2 . Цю систему можна переписати наступним чином:

$$\begin{cases} F_{0,n} = 0 \text{ при всіх } n, \\ B_1X_{0,n+1} = A_1X_{0,n} + F_{1,n}, & n \in \mathbb{Z}_+. \end{cases} \quad (2.9)$$

Тому для розв'язності рівняння (2.1) повинна бути виконана умова $F_{0,n} = 0$ при всіх n . Якщо цю умову не виконано, то рівняння (2.1) не має розв'язків, тобто доведено достатність твердження 3 теореми.

Нехай далі $F_{0,n} = 0$ при всіх n . Оскільки $B \neq 0$ і $B_0 = 0$, то $B_1 \neq 0$. Отже, елемент B_1^{-1} існує. За твердженням 1 (i) леми 2.1, розв'язок другого рівняння системи (2.9) визначається рівністю (2.7), де $X_{0,0}$ — довільний елемент поля \mathbb{Z}_2 . Якщо $\{X_{1,n}\}_{n=0}^{\infty}$ — довільна послідовність елементів поля \mathbb{Z}_2 , то $(\{X_{0,n}\}_{n=0}^{\infty}, \{X_{1,n}\}_{n=0}^{\infty})$ є загальним розв'язком системи (2.9).

Отже, загальний розв'язок рівняння (2.1) має вигляд $X_n = X_{0,n} + tX_{1,n}$ ($n \in \mathbb{Z}_+$), де $\{X_{0,n}\}_{n=0}^{\infty}$ визначається формулою (2.7), а $\{X_{1,n}\}_{n=0}^{\infty}$ довільна послідовність елементів поля \mathbb{Z}_2 .

Ми довели достатність кожного з тверджень теореми. Оскільки достатні

умови всіх трьох тверджень теореми вичерпують всі можливості і попарно не перетинаються, то доведення критерію завершено. \square

Наведемо приклад застосування теореми 2.4.

Приклад 2.5. Нехай $a_0 \in \mathbb{Z}_2$. Розглянемо рівняння

$$tX_{n+1} = (a_0 + t)X_n + F_n, \quad n \in \mathbb{Z}_+, \quad (2.10)$$

над кільцем R . Визначимо елементи: $A = a_0 + t$, $B = t$. Якщо $a_0 \neq 0$, тобто $A = 1 + t$, то елемент A оборотний, і $A^{-1} = 1 + t$. За твердженням 1 теореми 2.4, існує єдиний розв'язок рівняння (2.10). Він визначається наступним чином:

$$X_n = -A^{-1}F_n - A^{-2}BF_{n+1} = (1 + t)F_n + tF_{n+1}.$$

Нехай $a_0 = 0$ і $F_{0,n} = 0$ при всіх $n \in \mathbb{Z}_+$, то за другим твердженням теореми, існує нескінченно багато розв'язків рівняння (2.1). При цьому загальний розв'язок має вигляд $X_n = X_{0,n} + X_{1,n}t$, де $\{X_{1,n}\}_{n=0}^{\infty}$ це довільна послідовність елементів поля \mathbb{Z}_2 , $X_{0,0} \in \mathbb{Z}_2$ довільне, а $X_{0,n}$ визначається формулою

$$X_{0,n} = B_1^{-n}A_1^nX_{0,0} + \sum_{s=0}^{n-1} B_1^{-s-1}A_1^sF_{0,n-s-1} = X_{0,0} + \sum_{s=0}^{n-1} F_{0,n-s-1}, \quad n \in \mathbb{N}.$$

Якщо, $a_0 = 0$ і $f_{0,n} \neq 0$ для деякого $n \in \mathbb{Z}_+$, то, за третім твердженням теореми 2.4, рівняння (2.1) не має розв'язків.

Висновки

Наведено огляд результатів роботи [12] щодо класифікації кілець порядку p^2 , де p — просте число.

Записано різні представлення цих кілець у вигляді факторкілець, а для спеціального кільця $R''(0)$ також матричне представлення.

Сформульовано і доведено критерії розв'язності рівняння (2.1) над прямою сумою полів та над спеціальним кільцем $R'(0)$. Разом із критеріями наведено формулу загального розв'язку відповідних рівнянь у випадку існування розв'язку. Розглянуто приклади, що ілюструють роботу доведених теорем.

Список використаних джерел

- [1] A. Halanay, D. Wexler, Teoria Calitativa A Sistemelor Cu Impulsuri, Academiei Republicii Socialiste Romania, Bucuresti, 1968.
- [2] W.G. Kelley, A.C. Peterson, Difference Equation: An Introduction with Applications. 2nd ed., Academic Press, 2001.
- [3] S. Elaydi, Introduction to difference equations, Springer-Verlag, New York, 2005.
- [4] S.L. Campbell, Singular system of differential equations I San Fransisco, London, Mellbourne: Pitman Publishing, Research Notes in Mathematics, Vol. 40, 1980.
- [5] M. Benabdallah, A.G. Rutkas, A.A. Solovov, Application of Asymptotic Expansions to the Investigation of an Infinite System of Equations $AX_{n+1} + BX_n = f_n$ in a Banach Space, J. Soviet Math., 48 (1990), Iss. 2, P. 124–130.
- [6] M.F. Bondarenko, A.G. Rutkas, On a class of implicit difference equations, Dopovidi NANU of Uktaine (1998), No. 7, P. 11–15.
- [7] S. Gefter, A. Goncharuk, A. Piven, Implicit Linear First Order Difference Equations Over Commutative Rings. In: Elaydi, S., Kulenovic, M.R.S., Kalabusic, S. (eds) Advances in Discrete Dynamical Systems, Difference Equations and Applications. ICDEA 2021. Springer Proceedings in Mathematics & Statistics, vol 416, Springer, 2023, P. 199–216.

- [8] V.A. Gerasimov, S.L. Gefter, A.B. Goncharuk, Application of the p-adic Topology on \mathbb{Z} to the Problem of Finding Solutions in Integers of an Implicit Linear Difference Equation, J. Math. Sci., 235 (2018), No. 3. P. 256–261.
- [9] V.V. Martseniuk, S.L. Gefter and A.L. Piven, Uniqueness criterion and Cramers rule for implicit higher order linear difference equations over \mathbb{Z} , Progress on Difference Equations and Discrete Dynamical Systems (eds. S. Baigent, M. Bohner, S. Elaydi), Vol. 341, Springer, 2020, P. 311–325.
- [10] S.L. Gefter, A.L. Piven', Implicit Linear Nonhomogeneous Difference Equation over \mathbb{Z} with a Random Right-Hand Side, J. Math. Physics, Analysis, Geometry, 18 (2022), No.1, P. 105–117.
- [11] S.L. Gefter, A.L. Piven, Implicit Linear Nonhomogeneous Difference Equation in Banach and Locally Convex Spaces, J. Math. Physics, Analysis, Geometry, 15 (2019), No. 3, P. 336–353.
- [12] B. Fine. Classification of Finite Rings of Order p^2 . Mathematics Magazine, 66 (1993), No. 4. P. 248–252.
- [13] M. V. Heneralov and A. L. Piven', Implicit Linear Difference Equation over Residue Class Rings, 2023. // <http://arxiv.org/abs/2301.13704>.
- [14] M. V. Heneralov, A. L. Piven', Implicit difference equations over some residue class rings // International Conference of Young Mathematicians, June 3–5, 2021, Kyiv, Ukraine, abstracts, 2021. P. 24.
- [15] M.V. Heneralov, A.L. Piven', Implicit linear difference equations over finite commutative rings// International conference in complex and functional analysis dedicated to the memory of Bohdan Vynnytskyi, Drohobjch, 2021, P. 20–21.

- [16] M. Heneralov, A. Piven', Implicit difference equations over residue class rings // ICDEA 2022, 27th International Conference on Difference Equations and Applications, 18–22 July 2022, Paris-Saclay, France, P. 92.
- [17] G. Bini, F. Flamini. Finite commutative rings and their applications / Gilberto Bini, Flaminio Flamini, Springer Science+Business Media, LLC. 2002.
- [18] D. S. Dummit, R. M. Foote. Abstract Algebra. Third edition. John, Wiley & Sons, Inc., 2004.
- [19] M. F. Atiyah, I. G. Macdonald. Introduction to Commutative Algebra — Addison Wesley publishing Company, Reading, Massachusetts, 1969.
- [20] B. R. Macdonald. Finite Commutative Rings with Identity, New York, M. Dekker, Inc., 1974.
- [21] R. Lidl, H. Niedderraiter. Finite fields. Cambridge University Press. 1996.
- [22] Н.С. Головащук, Є.А. Кочубінська, С.А. Овсієнко. Збірник задач з теорії кілець (базовий курс). Навчальний посібник для студентів механіко – математичного факультету. — Київ: Видавничо-поліграфічний центр “Київський університет”, 2013.
- [23] P. Karimi Beiranvand, R. Beyranvand, and M. Gholami. Classification of Finite Rings of Order p^6 by Generators and Relations. Hindawi Publishing Corporation Journal of Mathematics Volume 2013, Article ID 467905, 8 pages // <http://dx.doi.org/10.1155/2013/467905>.
- [24] K. Ireland, M. Rosen, A Classical Introduction to Modern Number Theory, Springer-Verlag, New York, 1990.
- [25] B. R. McDonald. Bernard McDonald Linear Algebra Over Commutative Rings, M. Dekker. Inc., 1984.