УДК 512.643

В. М. Прокіп*

КАНОНІЧНА ФОРМА ІНВОЛЮТИВНИХ МАТРИЦЬ НАД ОБЛАСТЮ ГОЛОВНИХ ІДЕАЛІВ ВІДНОСНО ПЕРЕТВОРЕНЬ ПОДІБНОСТІ

Описано структуру інволютивних матриць над областю головних ідеалів відносно перетворення подібності та побудовано канонічну форму відносно цього перетворення. Як наслідок встановлено критерій подібності інволютивних матриць над областю головних ідеалів. Отримані результати застосовано до опису структури розв'язків матричного рівняння $X^2 = I_n$ *над областю головних ідеалів.*

Ключові слова: *область головних ідеалів, інволютивна матриця, матричне рівняння.*

Вступ. Нехай R – комутативне кільце з одиницею $e \neq 0$. Позначимо: $U(R)$ – мультиплікативна група області R; $M_{m,n}(R)$ – множина $m \times n$-матриць над R; I_n – одинична матриця порядку n; $0_{m,n}$ – нульова $m \times n$-матриця і O – нульова матриця, розмір якої визначається з контексту.

Матриці $A, B \in M_{n,n}(R)$ називають *подібними*, якщо існує матриця $T \in GL(n,R)$ така, що $A = TBT^{-1}$. Матрицю T називають *матрицею перетворення подібності* або трансформуючою матрицею. Структура матриць над полем відносно перетворень подібності описана повністю [2]. Проте задача про опис структури матриць відносно перетворень подібності при переході до довільного комутативного кільця з одиницею, (яке не є полем), значно ускладнюється. У більшості випадків ця задача містить в собі класичну нерозв'язну задачу про канонічну форму пари матриць над полем відносно перетворення подібності. Такі задачі називають дикими [3]. На теперішній час не існує критерію, який давав би змогу вказати умови, за яких дві матриці над кільцем є подібними.

Нагадаємо, що матрицю $A \in M_{n,n}(R)$ називають інволютивною, якщо вона співпадає зі своєю оберненою, тобто $A^2 = I_n$. Очевидно, якщо інволютивна матриця $A \neq \pm I_n$, то її власними значеннями є елементи $\pm e$, а $m(\lambda) = \lambda^2 - e$ – її мінімальний многочлен. Дослідження структури інволютивних матриць над скінченними полями та комутативними кільцями відносно перетворень подібності проводились багатьма математиками (див. [1, 9–25] і цитовану там літературу). Можна стверджувати, що цей інтерес викликаний не тільки тим, що інволютивні матриці відіграють вагому роль в лінійній алгебрі [8, 10, 11, 15, 20, 25], але і в теорії груп [12, 14, 23] та алгебраїчній криптографії [18, 22].

У роботах [17, 20] вивчалась структура інволютивних матриць над полем Ґалуа F_q з $q = p^m$ елементами, де p – просте число і $m \in \mathbb{N}$. Зокрема, в [17] встановлено, що розв'язки рівняння $X^2 = I_n \pmod p$ подібні діагональній матриці $\operatorname{diag}(I_t, -I_{n-t})$, а в [20] вказано їх кількість. У роботі [24] доведено, що інволютивна $n \times n$-матриця над полем Ґалуа R/p^n, $n \neq 2$, подібна єдиній матриці $\operatorname{diag}(I_t, -I_{n-t})$, і встановлено кількість інволютивних

* v.prokip@gmail.com

матриць. Пізніше, в роботі [16] обґрунтовано, що метод дослідження, запропонований у [24], не можна застосувати у випадку, коли $p = 2$.

У роботі [21] встановлено, якщо R – скінченне локальне кільце характеристики p^a ($p \neq 2$ – просте число), то інволютивна $n \times n$-матриця над R подібна діагональній матриці $\operatorname{diag}(I_t, -I_{n-t})$. У роботі [13] наведено огляд результатів, які стосуються подібності інволютивних матриць над локальними кільцями. Основним результатом роботи [13] є встановлення канонічної форми інволютивної матриці відносно перетворень подібності над локальним кільцем характеристики 2^n. Одночасно зауважено (див. [13, с. 187]), що доведення основного результату не дає конструктивного методу побудови канонічної форми та трансформуючої матриці T. Конструктивне доведення основного результату роботи [13] дає теорема 2 у статті [1]. Крім цього, в [1] наведено алгоритм зведення інволютивної матриці над скінченним комутативним локальним кільцем характеристики 2^n до канонічної форми.

Пропонована робота є продовженням досліджень, які проводились у [4–7], де вивчалась структура матриць над областю головних ідеалів відносно перетворень подібності. Метою роботи є опис структури інволютивних матриць над областю головних ідеалів відносно перетворень подібності та побудови їхніх канонічних форм відносно таких перетворень. Як наслідок, встановлено критерій подібності інволютивних матриць над областю головних ідеалів. Отримані результати застосовано до опису структури розв'язків (із заданим характеристичним многочленом) матричного рівняння $X^2 = I_n$ над областю головних ідеалів. Зауважимо, що розроблені методи та наведені результати можуть бути використані для дослідження структури матриць над областями елементарних дільників відносно перетворення подібності.

1. Основний результат. Надалі R – область головних ідеалів характеристики $\operatorname{char} R \neq 2$. В цьому розділі встановимо канонічну форму інволютивної матриці над областю головних ідеалів R ($\operatorname{char} R \neq 2$) відносно перетворення подібності. Зауважимо, якщо $R = F$ – поле, то для інволютивної матриці $A \in M_{n,n}(F)$ існує зображення у вигляді $A = 2P - I_n$, де $P \in M_{n,n}(F)$ – ідемпотентна матриця, яка для A визначена однозначно. Проте цей факт не завжди справджується для інволютивних матриць над комутативними кільцями. Наступна лема описує структуру характеристичного многочлена інволютивної матриці над R.

Лема 1. *Нехай* $A \in M_{n,n}(R)$ – *інволютивна матриця. Тоді*

(***i***) $\operatorname{rank}(I_n + A) = k$;

(***ii***) *слід матриці* $\operatorname{tr}(I_n + A) = 2k$;

(***iii***) $\det(I_n\lambda - A) = (\lambda - e)^k(\lambda + e)^{n-k}$.

Д о в е д е н н я. Твердження леми є очевидними, якщо $A = \pm I_n$.

Нехай $A \neq \pm I_n$. Нехай, далі, F – поле часток області R ($R \subset F$). На підставі того, що $\operatorname{char} R \neq 2$, для матриці $A \in M_{n,n}(F)$ існує зображення $A = 2P - I_n$, де $P \in M_{n,n}(F)$ – ідемпотентна матриця. Покладемо $\operatorname{rank} P = k$. Тепер із рівності $A = 2P - I_n$ отримуємо, що $\operatorname{rank}(A + I_n) = \operatorname{rank} P = k$.

Оскільки матриця P є ідемпотентною, то

$$UPU^{-1} = \begin{Vmatrix} I_k & 0_{k,n-k} \\ 0_{n-k,k} & 0_{n-k,n-k} \end{Vmatrix}, \qquad U \in GL(n,F).$$

Отже,

$$U(I_n\lambda - A)U^{-1} = I_n\lambda - 2U\,PU^{-1} + I_n = I_n\lambda - \begin{Vmatrix} I_k & O \\ O & -I_{n-k} \end{Vmatrix}.$$

Звідси отримуємо, що $\det(I_n\lambda - A) = (\lambda - \alpha)^k(\lambda - \beta)^{n-k}$.

Лему доведено. ♦

З огляду на лему 1, надалі будемо вважати, що для інволютивної матриці її характеристичний многочлен є відомим.

Теорема 1. *Нехай $A \in M_{n,n}(R)$ – інволютивна матриця з характеристичним многочленом $a(\lambda) = (\lambda - e)^k(\lambda + e)^{n-k}$, де $1 \le k < n$. Тоді для матриці A існує матриця $T \in GL(n,R)$ така, що*

$$TAT^{-1} = A_r = \begin{Vmatrix} I_k & 0_{k,n-k} \\ J_r & -I_{n-k} \end{Vmatrix},$$

де

$$J_r = \begin{Vmatrix} I_r & 0_{r,k-r} \\ 0_{n-k-r,r} & 0_{n-k=r,k-r} \end{Vmatrix} \in M_{n-k,k}(R).$$

Число r дорівнює кількості інваріантних множників, які збігаються з одиницею e матриці $A + I_n$. При цьому матриця A_r для A визначена однозначно.

Д о в е д е н н я. Над областю головних ідеалів R характеристики $\operatorname{char} R \ne 2$ існує лише два суміжних класи A_0 і A_1 за модулем $2e$. Представниками цих суміжних класів є елементи 0 і e відповідно. Отже, згідно з теоремою 4.1 із [6], для інволютивної матриці A існує матриця $T \in GL(n,R)$ така, що

$$TAT^{-1} = A_r = \begin{Vmatrix} I_k & 0_{k,n-k} \\ J_r & -I_{n-k} \end{Vmatrix},$$

де

$$J_r = \begin{Vmatrix} I_r & 0_{r,k-r} \\ 0_{n-k-r,r} & 0_{n-k=r,k-r} \end{Vmatrix} \in M_{n-k,k}(R), \qquad r \le \min\{k, n-k\}.$$

Доведемо, що A_r для іволютивної матриці A визначена однозначно. Припустимо, що для матриці A існує матриця $W \in GL(n,R)$ така, що

$$WAW^{-1} = A_\ell = \begin{Vmatrix} I_k & 0_{k,n-k} \\ J_\ell & -I_{n-k} \end{Vmatrix},$$

де

$$J_\ell = \begin{Vmatrix} I_\ell & 0_{\ell,k-\ell} \\ 0_{n-k-\ell,\ell} & 0_{n-k-\ell,k-\ell} \end{Vmatrix}, \qquad \ell \ne r, \qquad \ell \le \min\{k, n-k\}.$$

Оскільки матриці A_r і A_ℓ подібні, то зрозуміло, що матриці

$$A_r + I_n = \begin{Vmatrix} 2I_k & 0_{k,n-k} \\ J_r & 0_{n-k,n-k} \end{Vmatrix} \qquad \text{і} \qquad A_\ell + I_n = \begin{Vmatrix} 2I_k & 0_{k,n-k} \\ J_\ell & 0_{n-k,n-k} \end{Vmatrix}$$

теж подібні. Отже, ці матриці еквівалентні. Легко переконатись у тому, що

$$S_r = \operatorname{diag}(I_r, 2I_{k-r}, 0, \ldots, 0) \qquad \text{і} \qquad S_\ell = \operatorname{diag}(I_\ell, 2I_{k-\ell}, 0, \ldots, 0)$$

є формами Сміта матриць $A_r + I_n$ і $A_\ell + I_n$, відповідно. Оскільки $\ell \neq r$, то очевидно, що форми Сміта S_r і S_ℓ не є еквівалентними. Таким чином, припущення про те, що $\ell \neq r$, не є правильним.

Тим самим доведено єдиність матриці A_r, яка є канонічною формою для інволютивної матриці A відносно перетворення подібності. Число r дорівнює кількості інваріантних множників матриці $A + I_n$, які збігаються з одиницею e області R. Теорему доведено. ♦

Із теореми 1 отримуємо умови подібності інволютивних матриць над областю головних ідеалів R характеристики $\operatorname{char} R \neq 2$.

Наслідок 1. *Інволютивні матриці $A, B \in M_{n,n}(R)$ подібні тоді й тільки тоді, коли форми Сміта матриць $A + I_n$ і $B + I_n$ збігаються.*

Д о в е д е н н я. Якщо інволютивні матриці $A, B \in M_{n,n}(R)$ подібні, то згідно з теоремою 1 форми Сміта матриць $A + I_n$ і $B + I_n$ збігаються.

Навпаки, нехай форми Сміта матриць $A + I_n$ і $B + I_n$ збігаються. Отже, $\operatorname{rank}(A + I_n) = \operatorname{rank}(B + I_n)$. На підставі леми 1 характеристичні многочлени матриць A і B збігаються. Згідно з теоремою 1, канонічні форми матриць A і B відносно перетворень подібності збігаються. Отже, матриці A і B подібні. ♦

Нехай A – $n \times n$-матриця над полем F. Відомо, що матриця A і транспонована матриця $A^\top$ над F подібні. Проте цей факт не завжди справджується для матриць над комутативним кільцем.

На підставі наслідку 1 отримуємо

Наслідок 2. *Якщо $A \in M_{n,n}(R)$ – інволютивна матриця, то матриці A і $A^\top$ подібні.*

Якщо для інволютивної матриці A виконується $A - I_n = 0_{n,n} \pmod{2e}$, то, згідно з роботою [4], така інволютивна матриця A над R є матрицею простої структури, тобто вона подібна до діагональної матриці з елементами $\pm e$ на головній діагоналі. Крім цього, для матриці A існує єдина пара ідемпотентних матриць $P, Q \in M_{n,n}(R)$ таких, що $PQ = QP = O$ і $A = P - Q$ (див. також [5]). На підставі цього отримуємо

Наслідок 3. *Якщо $2e \in U(R)$, то інволютивна матриця A є матрицею простої структури.*

Наслідок 4. *Якщо $2e \in U(R)$, то інволютивні матриці $A, B \in M_{n,n}(R)$ подібні тоді й тільки тоді, коли $\operatorname{rank}(A + I_n) = \operatorname{rank}(B + I_n)$.*

Зауважимо, якщо F – поле характеристики $\operatorname{char} F \neq 2$, то, згідно з наслідком 3, отримуємо, що всі інволютивні матриці із $M_{n,n}(F[\lambda])$ є матрицями простої структури.

Нехай $A \in M_{n,n}(R)$ – матриця з мінімальним многочленом $m(\lambda) = (\lambda - \alpha)(\lambda - \beta)$, де $\alpha, \beta \in R$, $\alpha \neq \beta$. Будемо говорити, що A «*близька*» до інволютивної матриці, якщо $\alpha - \beta = \pm 2e$. Не втрачаючи загальності, в цьому випадку можемо вважати, що $\alpha - \beta = 2e$. Отже, в такому випадку є очевид-

ним, що $\alpha+\beta=2\gamma$ і $I_n\gamma+A$ – інволютивна матриця.

На підставі леми 1 і теореми 1 отримуємо

Наслідок 5. *Нехай* $A\in M_{n,n}(R)$ – *матриця з мінімальним многочленом* $m(\lambda)=(\lambda-\alpha)(\lambda-\beta)$, *де* $\alpha,\beta\in R$, $\alpha\neq\beta$. *Якщо* $\alpha-\beta=\pm 2e$, *то* A *подібна до матриці*

$$TAT^{-1}=A_r=\begin{Vmatrix} I_k\alpha & 0_{k,n-k} \\ J_r & I_{n-k}\beta \end{Vmatrix}, \qquad T\in GL(n,R),$$

де

$$J_r=\begin{Vmatrix} I_r & 0_{r,k-r} \\ 0_{n-k-r,r} & 0_{n-k=r,k-r} \end{Vmatrix}\in M_{n-k,k}(R), \qquad k=\operatorname{rank}(A+I_n\beta).$$

Число r *дорівнює кількості інваріантних множників, які збігаються з одиницею матриці* $A+I_n\alpha$. *При цьому матриця* A_r *для* A *визначається однозначно.*

2. Застосування. Розглянемо сумісне матричне рівняння

$$X^2=I_n, \qquad n\geq 2. \tag{1}$$

Очевидно, що матриці $\pm I_n$ є розв'язками рівняння (1), які будемо називати тривіальними. Проте для рівняння (1), крім тривіальних розв'язків, існують інші розв'язки, які є інволютивними матрицями.

Нехай матриця $X_0\in M_{n,n}(R)$ є розв'язком рівняння (1). Тоді для довільної матриці $U\in GL(n,R)$ матриця $X_u=UX_0U^{-1}$ є розв'язком рівняння (1). Оскільки перетворення подібності є відношенням еквівалентності, то множина розв'язків рівняння (1) розбивається на суміжні класи відносно перетворення подібності.

Отже, опис усіх розв'язків рівняння (1) містить задачу про канонічну форму інволютивної матриці над областю головних ідеалів R відносно перетворення подібності. Використовуючи теорему 1, опишемо структуру розв'язків рівняння (1) із наперед заданим характеристичним многочленом. Відмітимо, що структура розв'язків рівняння (1) над скінченними полями та кільцями досліджувалась в роботах [17, 19, 24].

Теорема 2. *Нехай* $a(\lambda)=(\lambda-e)^k(\lambda+e)^{n-k}$, *де* $1\leq k<n$. *Рівняння* (1) *над областю головних ідеалів* R *має* $1+\min\{k,n-k\}$ *суміжних класів розв'язків відносно подібності із характеристичним многочленом* $a(\lambda)$. *Представниками цих суміжних класів є матриці*

$$X_r=\begin{Vmatrix} I_k & 0_{k,n-k} \\ J_r & -I_{n-k} \end{Vmatrix},$$

де

$$J_r=\begin{Vmatrix} I_r & 0_{r,k-r} \\ 0_{n-k-r,r} & 0_{n-k=r,k-r} \end{Vmatrix}\in M_{n-k,k}(R),$$

$$r=0,1,\ldots,\min\{k,n-k\}.$$

Д о в е д е н н я. Нехай M_a – множина інволютивних матриць із $M_{n,n}(R)$ з характеристичним многочленом $a(\lambda)=(\lambda-e)^k(\lambda+e)^{n-k}$, де $1\leq k<n$. Очевидно, що кожна матриця із M_a є розв'язком рівняння (4). Нехай матриця $X_0\in M_a$. На підставі теореми 1 матриця $X_0\in M_a$ подібна до матриці

$$X_r = \begin{Vmatrix} I_k & 0_{k,n-k} \\ J_r & -I_{n-k} \end{Vmatrix}, \qquad 0 \le r \le \min\{k, n-k\},$$

яка для матриці X_0 визначається однозначно. Покладемо $m = \min\{k, n-k\}$. З огляду на теорему 1, множина M_a містить матриці

$$X_0 = \begin{Vmatrix} I_k & 0_{k,n-k} \\ 0_{n-k,k} & -I_{n-k} \end{Vmatrix}, \quad X_1 = \begin{Vmatrix} I_k & 0_{k,n-k} \\ J_1 & -I_{n-k} \end{Vmatrix}, \quad \ldots, \quad X_m = \begin{Vmatrix} I_k & 0_{k,n-k} \\ J_m & -I_{n-k} \end{Vmatrix},$$

які попарно не є подібними. Отже, множина M_a містить $m+1$ суміжних класів відносно подібності нетривіальних розв'язків із характеристичним многочленом $a(\lambda)$. Теорему доведено. ♦

Проілюструємо застосування теореми 2.

► ***Приклад***. Розглянемо рівняння $X^2 = I_5$.

Опишемо структуру його розв'язків із характеристичним многочленом $a(\lambda) = (\lambda - e)^2(\lambda + e)^3$. Оскільки $m = \min\{2, 3\} = 2$, то множина M_a містить три суміжних класи відносно подібності нетривіальних розв'язків із характеристичним многочленом $a(\lambda)$. Запишемо матриці, які є представниками цих суміжних класів відносно подібності нетривіальних розв'язків рівняння $X^2 = I_5$ із характеристичним многочленом $a(\lambda) = (\lambda - e)^2(\lambda + e)^3$:

$$X_0 = \begin{Vmatrix} I_2 & 0_{2,3} \\ 0_{3,2} & -I_3 \end{Vmatrix}, \qquad X_1 = \begin{Vmatrix} I_2 & 0_{2,3} \\ J_1 & -I_3 \end{Vmatrix}, \qquad X_2 = \begin{Vmatrix} I_2 & 0_{2,3} \\ J_2 & -I_3 \end{Vmatrix},$$

де

$$J_1 = \begin{Vmatrix} e & 0 \\ 0 & 0 \\ 0 & 0 \end{Vmatrix}, \qquad J_2 = \begin{Vmatrix} e & 0 \\ 0 & e \\ 0 & 0 \end{Vmatrix}$$ ◄

Встановлена вище канонічна форма для інволютивних матриць над областю головних ідеалів R відносно перетворення подібності може бути використана для опису структури розв'язків рівняння Янґа – Бакстера $AXA = XAX$ над R. Зауважимо, що структура розв'язків рівняння Янґа – Бакстера над полем описана лише у випадках, коли на матрицю A накладено певні обмеження (ідемпотентна, інволютивна, простої структури). Якщо ж у рівнянні Янґа – Бакстера над R матриця A є інволютивною, то результати роботи [8] справджуються для областей головних ідеалів R.

1. *Газарян Т. Г.* Подобие инволютивных матриц над локальным кольцом характеристики 2^k // Дискретная математика. – 1995. – **7**, № 4. – С. 145–156.
   Те саме: *Gazaryan T. G.* Similarity of involutive matrices over a local ring of characteristic 2^k // Discrete Math. Appl. – 1995. – **5**, No. 6. – P. 587–601. – https://doi.org/10.1515/dma.1995.5.6.587.
2. *Гантмахер Ф. Р.* Теория матриц. – Москва: Наука, 1988. – 552 с.
   Те саме: *Gantmacher F. R.* The theory of matrices. – New York: Chelsea Publ. Co., 1959. – Vol. 1: x+377 p.; Vol. 2: x+277 p.
   http://science.sciencemag.org/content/131/3408/1216.2
3. *Дрозд Ю. А.* Ручные и дикие матричные задачи // Представления и квадратичные формы. – Киев: Ин-т математики АН УССР, 1979. – С. 39–74.
4. *Прокіп В. М.* Діагоналізація матриць над областю головних з мінімальним многочленом $m(\lambda) = (\lambda - \alpha)(\lambda - \beta),\ \alpha \neq \beta$ // Укр. мат. вісн. – 2010. – **7**, № 2. – С. 212–219.
   Те саме: *Prokip V. M.* Diagonalization of matrices over the domain of principal ideals with minimal polynomial $m(\lambda) = (\lambda - \alpha)(\lambda - \beta),\ \alpha \neq \beta$ // J. Math. Sci. – 2011. – **174**, No. 4. – P. 481–485. – https://doi.org/10.1007/s10958-011-0313-y.

5. *Прокіп В. М.* Діагоналізовність матриць над областю головних ідеалів // Укр. мат. журн. – 2012. – **64**, № 2. – С. 283–288.
Те саме: *Prokip V. M.* Diagonalizability of matrices over the principal ideal domain // Ukr. Math. J. – 2012. – **64**, No. 2. – P. 316–323. https://doi.org/10.1007/s11253-012-0649-6.
6. *Прокіп В. М.* Про структуру матриць над областю головних ідеалів відносно перетворення подібності // Праці міжнар. геометр. центру (*Proc. Int. Geometry Center*). – 2019. – **12**, № 1. – С. 56–69.
– https://doi.org/10.15673/tmgc.v12i1.1368.
7. *Прокіп В. М.* Структура матриць рангу один над областю головних ідеалів відносно перетворення подібності // Мат. методи та фіз.-мех. поля. – 2016. – **59**, № 3. – С. 68–76.
Те саме: *Prokip V. M.* Structure of rank-one matrices over the domain of principal ideals relative to similarity transformations // J. Math. Sci. – 2019. – **236**, No. 1. – P. 71–82.
– https://doi.org/10.1007/s10958-018-4098-0.
8. *Adam M. S. I., Ding J., Huang Q., Zhu L.* Solving a class of quadratic matrix equations // Appl. Math. Letters. – 2018. – **82**. – P. 58–63.
– https://doi.org/10.1016/j.aml.2018.02.017.
9. *Ballantine C. S.* Some involutory similarities // Linear Multilinear Algebra. – 1975. – **3**, No. 1-2. – P. 19–23. – https://doi.org/10.1080/03081087508817087.
10. *Brawley J. V.* (*Jr.*) Similar involutory matrices ($\mathrm{mod}\, p^m$) // Am. Math. Monthly. – 1966. – **73**, No. 5. – P. 499–501. – https://www.jstor.org/stable/2315470.
11. *Brawley J. V.* (*Jr.*) Similar involutory matrices modulo R // Duke Math. J. – 1967. – **34**, No. 4. – P. 649–665. – https://projecteuclid.org/euclid.dmj/1077377300.
12. *Brawley J. V.* Certain sets of involutory matrices and their groups // Duke Math. J. – 1969. – **36**, No. 3. – P. 473–478.
– https://projecteuclid.org/euclid.dmj/1077378464.
13. *Brawley J. V., Gamble R. O.* Involutory matrices over finite commutative rings // Linear Algebra Appl. – 1978. – **21**, No. 2. – P. 175–188.
https://doi.org/10.1016/0024-3795(78)90041-1.
14. *Cline R. E., McConnel R. M.* Extensions of the Levine-Nahikian method for constructing involutory matrices // Linear Algebra Appl. – 1984. – **57**. – P. 247–270.
– https://doi.org/10.1016/0024-3795(84)90191-5.
15. *Fulton J. D.* Symmetric involutory matrices over finite fields and modular rings of integers // Duke Math. J. – 1969. – **36**, No. 2. – P. 401–407.
https://projecteuclid.org/euclid.dmj/1077378310.
16. *Hodges J. H.* Idempotent matrices ($\mathrm{mod}\, p^a$) // Am. Math. Monthly. – 1966. – **73**, No. 3. – P. 276–278. – https://www.jstor.org/stable/2315343.
17. *Hodges J. H.* The matrix equation $X^2 = I$ over a finite field // Am. Math. Monthly. – 1958. – **65**, No. 7. – P. 518–520. – https://www.jstor.org/stable/2308579.
18. *Hoffstein J., Pipher J. C., Silverman J. H.* An introduction to mathematical cryptography. – New York: Springer, 2008. – xvi+524 p.
19. *Korfhage R. R.* Solutions of $X^2 = I$ for matrices over finite rings with unity // Am. Math. Monthly. – 1968. – **75**, No. 6. – P. 634–636.
– https://www.jstor.org/stable/2313783.
20. *Levine J., Nahikian H. M.* On the construction of involutory matrices // Am. Math. Monthly. – 1962. – **69**, No. 4. – P. 267–272.
– https://www.jstor.org/stable/2312939.
21. *Mcdonald B. R.* Involutory matrices over finite local rings // Can. J. Math. – 1972. – **24**, No. 3. – P. 369–378.
22. *Overbey J., Traves W., Wojdylo J.* On the keyspace of the Hill cipher // Cryptologia. – 2005. – **29**, No. 1. – P. 59–72.
23. *Reiner I.* The matrix congruence $X^2 = I\ (\mathrm{mod}\, p^a)$ // Am. Math. Monthly. – 1960. – **67**, No. 8. – P. 773–775. – https://www.jstor.org/stable/2308658.
24. *Reiner I.* Integral representation of cyclic groups of prime order // Proc. Am. Math. Soc. – 1957. – **8**, No. 1. – P. 142–146.
– https://doi.org/10.1090/S0002-9939-1957-0083493-6.
25. *Słowik R.* Expressing infinite matrices as products of involutions // Linear Algebra Appl. – 2013. – **438**, No. 1. – С. 399–404.
– https://doi.org/10.1016/j.laa.2012.07.032.

КАНОНИЧЕСКАЯ ФОРМА ИНВОЛЮТИВНЫХ МАТРИЦ НАД ОБЛАСТЬЮ ГЛАВНЫХ ИДЕАЛОВ ОТНОСИТЕЛЬНО ПРЕОБРАЗОВАНИЯ ПОДОБИЯ

Описана структура инволютивных матриц над областью главных идеалов относительно преобразования подобия и построена каноническая форма относительно этого преобразования. Как следствие установлен критерий подобия инволютивных матриц над областью главных идеалов. Полученные результаты применены к описанию структуры решений матричного уравнения $X^2 = I_n$ *над областью главных идеалов.*

***Ключевые слова**: область главных идеалов, инволютивная матрица, матричное уравнение.*

THE CANONICAL FORM OF INVOLUTORY MATRICES OVER THE PRINCIPAL IDEAL DOMAIN WITH RESPECT TO SIMILARITY TRANSFORMATION

The structure of involutory matrices over a domain of principal ideals with respect to the similarity transformation is described and the canonical form of this transformation is constructed. As a corollary, the criterion of similarity of involutory matrices over a domain of principal ideals is established. The obtained results are applied for description of the structure of solutions of the matrix equation $X^2 = I_n$ *over a domain of principal ideals.*

***Key words**: principal ideal domain, involutory matrix, matrix equation.*

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

Одержано
21.10.18