УДК 512.643+519.612

Про квадратні корені матриць над областю головних ідеалів

Прокіп В. М., к.ф.-м.н., старший науковий співробітник

Інститут прикладних проблем механіки і математики НАН України
(вул. Наукова, 3Б, м. Львів, 79060, Україна)

Нехай R — область головних ідеалів з одиницею $e \neq 0$. Позначимо: I_n — одинична $(n \times n)$-матриця; $0_{n,m}$ — нульова $(n \times m)$-матриця; $\mathrm{R}_{n,m}$ і $\mathrm{R}_{n,m}[\lambda]$ — множини $(n \times m)$-матриць над R і кільцем многочленів $\mathrm{R}[\lambda]$ відповідно. Для матриці $B \in \mathrm{R}_{n,n}$ через $b(\lambda) = \det(I_n\lambda - B)$ позначимо її характеристичний многочлен.

Кажуть, що матриця $B \in \mathrm{R}_{n,n}$ є квадратним коренем із матриці $A \in \mathrm{R}_{n,n}$, якщо $B^2 = A$. Аналітично задача про знаходження коренів 2-го степеня із матриці над полем комплексних чисел добре вивчена. Зокрема, в [1] детально описана структура коренів із матриці A в термінах кліток Жордано. Проте задача про описання квадратних коренів матриць при переході до довільного поля або комутативного кільця з одиницею значно ускладнюється (див., напр. [5]).

Очевидно, що знаходження квадратних коренів із матриці $A \in \mathrm{R}_{n,n}$ рівносильне пошуку розв'язків матричного рівняння $X^2 = A$. На підставі узагальненої теореми Безу ([1], [4]) матриця $B \in \mathrm{R}_{n,n}$ є квадратним коренем із матриці A тоді і тільки тоді, коли для матриці $A(\lambda) = I_n\lambda^2 - A \in \mathrm{R}_{n,n}[\lambda]$ існує зображення у вигляді добутку $A(\lambda) = (I_n\lambda - B)(I_n\lambda + B)$. Таким чином, знаходження квадратних коренів із матриці A рівносильне пошуку лінійних унітальних дільників $I_n\lambda - B$ із многочленної матриці $A(\lambda)$.

Нехай матриця $B \in \mathrm{R}_{n,n}$ із характеристичним многочленом $\det(I_n\lambda - B) = b(\lambda) = \lambda^n + b_1\lambda^{n-1} + \cdots + b_n$ є розв'язком матричного рівняння $X^2 = A$. Із рівності $A(\lambda) = (I_n\lambda - B)(I_n\lambda + B)$ отримуємо $\det A(\lambda) = b(\lambda)\widetilde{b}(\lambda)$. В цьому зв'язку пошук квадратних коренів із матриці $A \in \mathrm{R}_{n,n}$ розділимо на частини. Спочатку вкажемо розклади $\det A(\lambda)$ у вигляді $\det A(\lambda) = b(\lambda)\widetilde{b}(\lambda)$, де $b(\lambda) \in \mathrm{R}[\lambda]$ — унітальний многочлен степеня n. Потім будемо шукати лівий дільник $I_n\lambda - B \in \mathrm{R}_{n,n}[\lambda]$ із характеристичним многочленом $b(\lambda)$ для матриці $A(\lambda)$.

З огляду на вищесказане матриці $A(\lambda) = I_n\lambda^2 - A$ та многочлену $b(\lambda) = \lambda^n + b_1\lambda^{n-1} + \cdots + b_n$ поставимо у відповідність матриці (див., напр. [2])

$$M = \begin{bmatrix} I_n & 0_{n,n} & -A & 0_{n,n} & \dots & \dots & 0_{n,n} \\ 0_{n,n} & I_n & 0_{n,n} & -A & 0_{n,n} & \dots & 0_{n,n} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0_{n,n} & \dots & \dots & 0_{n,n} & I_n & 0_{n,n} & -A \\ I_n & I_nb_1 & I_nb_2 & \dots & \dots & I_nb_{n-1} & I_nb_n \end{bmatrix} \in \mathrm{R}_{n^2,n(n+1)},$$

$$N = \begin{bmatrix} I_nb_1 & I_nb_2 + A & I_nb_3 & \dots & \dots & I_nb_{n-1} & I_nb_n \end{bmatrix} \in \mathrm{R}_{n,n(n+1)}.$$

Нижче через $d_A(\lambda)$ позначатимемо н.с.д. мінорів $(n-1)$-го порядку матриці $A(\lambda) \in \mathrm{R}_{n,n}[\lambda]$. Основним результатом цього повідомлення є наступна теорема.

Теорема 1. *Нехай визначник матриці* $A(\lambda) = I_n\lambda^2 - A \in \mathrm{R}_{n,n}[\lambda]$ *допускає зображення у вигляді добутку* $\det A(\lambda) = b(\lambda)\widetilde{b}(\lambda)$, *де* $b(\lambda) = \lambda^n + b_1\lambda^{n-1} + \cdots + b_n \in \mathrm{R}[\lambda]$. *Якщо* $\big(b(\lambda), \widetilde{b}(\lambda), d_A(\lambda)\big) = e$, *то для матриці* A *існує квадратний корінь* $B \in \mathrm{R}_{n,n}$ *із характеристичним многочленом* $\det(I_n\lambda - B) = b(\lambda)$ *тоді і тільки тоді, коли матриці* $\begin{bmatrix} M \\ 0_{n,(n+1)n} \end{bmatrix}$ *і* $\begin{bmatrix} M \\ N \end{bmatrix}$ *лівоеквівалентні, тобто коли ліві форми Ерміта цих матриць збігаються. Якщо матриця* B *існує, то вона однозначно визначена характеристичним многочленом* $b(\lambda)$.

Зауважимо, якщо за умов Теореми 1 матриця B існує, то на підставі результатів із робіт [2] і [3] отримуємо метод її знаходження. Крім цього, із Теореми 1 отримуємо наступні наслідки.

Наслідок 1. *Нехай визначник матриці* $A(\lambda) = I_n\lambda^2 - A \in \mathrm{R}_{n,n}[\lambda]$ *допускає зображення у вигляді добутку* $\det A(\lambda) = b(\lambda)\widetilde{b}(\lambda)$, *де* $b(\lambda) = \lambda^n + b_1\lambda^{n-1} + \cdots + b_n \in \mathrm{R}[\lambda]$. *Якщо* $\big(b(\lambda), \widetilde{b}(\lambda)\big) = e$, *то для матриці* A *існує квадратний корінь* $B \in \mathrm{R}_{n,n}$ *із характеристичним многочленом* $b(\lambda)$ *тоді і тільки тоді, коли матриці* $\begin{bmatrix} M \\ 0_{n,(n+1)n} \end{bmatrix}$ *і* $\begin{bmatrix} M \\ N \end{bmatrix}$ *лівоеквівалентні, тобто коли ліві форми Ерміта цих матриць збігаються. Якщо матриця* B *існує, то вона єдина із заданим характеристичним многочленом* $b(\lambda)$.

Наслідок 2. *Нехай визначник матриці* $A(\lambda) = I_n\lambda^2 - A \in \mathrm{R}_{n,n}[\lambda]$ *допускає зображення у вигляді добутку* $\det A(\lambda) = b(\lambda)\widetilde{b}(\lambda)$, *де* $b(\lambda) = \lambda^n + b_1\lambda^{n-1} + \cdots + b_n \in \mathrm{R}[\lambda]$. *Якщо* $d_A(\lambda) = e$, *то для* A *існує квадратний корінь* $B \in \mathrm{R}_{n,n}$ *із характеристичним многочленом* $b(\lambda)$ *тоді і тільки тоді, коли матриці* $\begin{bmatrix} M \\ 0_{n,(n+1)n} \end{bmatrix}$ *і* $\begin{bmatrix} M \\ N \end{bmatrix}$ *лівоеквівалентні, тобто коли ліві форми Ерміта цих матриць збігаються. Якщо матриця* B *існує, то вона єдина із заданим характеристичним многочленом* $b(\lambda)$.

[1] *Гантмахер Ф. Р.* Теория матриц. – 5-е изд. – М.: Физматлит, 2004. 560 с.

[2] *Прокіп В. М.* Про факторизацію многочленних матриць над областю головних ідеалів // Український математичний журнал. – 1996. – Т. 48, № 10. – С. 1435–1439.

[3] *Прокіп В. М.* Про розв'язність системи лінійних рівнянь над областю головних ідеалів // Український математичний журнал. – 2014. – Т. 66, № 4. – С. 566–570.

[4] *Hautus M. L. J.* Substitution of matrices over rings // Linear algebra and its applications. – 1995. – V. 226. – P. 353–370.

[5] *Melnyk O. M., Kolyada R. V.* On square roots of integer matrices. Book of Abstracts of 11th International Algebraic Conference in Ukraine. 2017, Kyiv, Ukraine. P. 83.