УДК 512.552.13

О.М. Романів, А.В. Саган
Львівський національний університет імені Івана Франка, Львів, Україна

ЕВКЛІДОВІСТЬ ПОВНИХ МАТРИЦЬ

В цій роботі показано, що над комутативними кільцями елементарних дільників довільна множина повних матриць порядку *n* є 2-евклідовою множиною. Над областю головних ідеалів довільна множина повних матриць порядку 2 є евклідовою множиною, а порядку *n* – 2-евклідовою множиною.
Ключові слова: повна матриця, кільце елементарних дільників, евклідове кільце, *ω*-евклідове кільце, область головних ідеалів.

Всі розглянуті нижче кільця є асоціативними з відмінною від нуля одиницею. Під областю цілісності розумітимемо комутативне кільце без дільників нуля. Область цілісності, в якій кожен ідеал є головним, називатимемо областю головних ідеалів [2].

Якщо R – кільце, то через $U(R)$ позначимо групу одиниць цього кільця. Кільце матриць порядку *n* над кільцем R позначимо через $M_n(R)$, а через $GL_n(R)$ – групу всіх оборотних матриць порядку *n* з елементами із R.

Нехай *k* – фіксоване натуральне число, $a,b\in R$, причому $b\neq 0$. Якщо існують такі елементи $q_i, r_i \in R$, *i=1,2,...,k*, що

$$a=bq_1+r_1,\ b=r_1q_2+r_2,\ \ldots,\ r_{k-2}=r_{k-1}q_k+r_k, \tag{1}$$

то послідовність рівностей (1) називається правим *k*-членним ланцюгом подільності для заданої пари елементів a, b. Аналогічно можна означити поняття лівого *k*-членного ланцюга подільності. Очевидно, що в комутативному випадку ці поняття співпадають і говорять про *k*-членний ланцюг подільності вигляду (1).

Зауваження 1. *Будь-який правий (лівий) 1-членний ланцюг подільності можна продовжити до правого (лівого) 2-членного ланцюга. Дійсно, якщо* $r_{k-2}=r_{k-1}q_k+r_k$, *то* $\begin{cases} r_{k-2}=r_{k-1}(q_k-1)+r_{k-1}, \\ r_{k-1}=r_{k-1}\cdot 1+r_k. \end{cases}$

Нормою над кільцем R називають таке відображення $\varphi: R\to \mathbb{Z}_{\geq 0}$, для якого, по-перше, $\varphi(0)=0$ тоді і лише тоді, коли $a=0$ і, по-друге, $\varphi(ab)\geq\varphi(a)$ для всіх $a,b\in R$ таких, що $ab\neq 0$.

Кільце R називається правим *ω*-евклідовим кільцем стосовно норми φ, якщо для довільної пари елементів $a,b\in R, b\neq 0$ існує такий правий *k*-членний (для деякого натурального *k*) ланцюг подільності вигляду (1), що $\varphi(r_k)<\varphi(b)$. Кільце R називається правим евклідовим кільцем стосовно норми φ, якщо для довільних елементів $a,b\in R,\ b\neq 0$, існує такий елемент $q\in R$, що $\varphi(b)>\varphi(a-bq)$. Аналогічно визначаються поняття лівого *ω*-евклідового та лівого евклідового кілець. Кільце, яке є лівим і правим *ω*-евклідовим (лівим і правим евклідовим), називається *ω*-евклідовим (відповідно, евклідовим).

Матриця $A\in M_n(R)$ є повною, якщо $M_n(R)AM_n(R)=M_n(R)$. Множину всіх повних матриць кільця $M_n(R)$ позначатимемо через $F(M_n(R))$.

Відомо, що матриця $A\in M_n(R)$ володіє діагональною редукцією над кільцем R, якщо існують такі оборотні матриці $P,Q\in GL_n(R)$, що

$$PAQ=diag(\varepsilon_1,\ldots,\varepsilon_r,0,\ldots,0),$$

де $R\varepsilon_{i+1}R\subseteq R\varepsilon_i\cap\varepsilon_i R$ для усіх *i=1,2,..,r-1*. Якщо над кільцем R довільна матриця володіє діагональною редукцією, то це кільце R називається кільцем елементарних дільників [3]. Зауважимо, якщо R − кільце елементарних дільників і $A\in M_n(R)$ − повна матриця, яка володіє діагональною редукцією, то $PAQ=diag(1,\varepsilon_2,\ldots,\varepsilon_r,0,\ldots,0)$ для деяких оборотних матриць $P,Q\in M_n(R)$ і елементів $\varepsilon_i\in R$, *i=2,..,r*.

Теорема 2. *Нехай* R − *комутативне кільце елементарних дільників і* $n\in\mathbb{Z}_{>1}$. *Тоді для довільних* $A,B\in F(M_n(R))$, $B\neq O_n$, *існує правий (лівий) 2(n-1)-членний ланцюг подільності.*

Доведення. Проведемо доведення за індукцією за n. Випадок $n=2$ є теоремою 4 [6]. Тому нехай $n>2$. Розглянемо матриці $A,B\in F(M_n(R))$, $B\neq O_n$. Існують такі матриці $P,U,Q\in GL_n(R)$ і $A',B'\in F(M_{n-1}(R))$, що

$$PAU=\begin{pmatrix} a_1 & O_{1,n-1} \\ a_2 & \\ \vdots & A' \\ a_n & \end{pmatrix} \text{ і } PBQ=\begin{pmatrix} 1 & O_{1,n-1} \\ O_{n-1,1} & B' \end{pmatrix}. \tag{2}$$

За індукцією, для матриць із $F(M_{n-1}(R))$ існує правий $2(n-2)$-членний ланцюг подільності і, в силу зауваження 1, цей ланцюг ми можемо продовжити до правого $2(n-1)$-членного ланцюга подільності. Позначимо через Q'_k дільники і через R'_k остачі для $1\le k\le 2n-2$. Позначимо $Q_1=\begin{pmatrix} a_1-1 & O_{1,n-1} \\ O_{n-1,1} & Q'_1 \end{pmatrix}$, $Q_i=\begin{pmatrix} 0 & O_{1,n-1} \\ O_{n-1,1} & Q'_i \end{pmatrix}$ для $1<i<2n-2,$ і $Q_{2n-2}=\begin{pmatrix} 1 & O_{1,n-1} \\ O_{n-1,1} & Q'_{2n-2} \end{pmatrix}$. Тоді ми отримаємо правий $2(n-1)$-членний ланцюг подільності з тами остачами

$$\text{для } 1\le i\le n-1,\ R_{2i-1}=\begin{pmatrix} 1 & O_{1,n-1} \\ a_2 & \\ \vdots & R'_{2i-1} \\ a_n & \end{pmatrix},$$

$$\text{для } 1\le i\le n-1,\ R_{2i}=\begin{pmatrix} 1 & O_{1,n-1} \\ O_{n-1,1} & R'_{2i} \end{pmatrix}.$$

Лівобічний випадок доводиться аналогічно.

Теорему доведено.

Нехай R – область головних ідеалів і x – довільний ненульовий елемент R. Оскільки R є областю з однозначним розкладом на множники, то $x=u\prod_{i=1}^{n} p_i^{e_i}$, де $n\in\mathbb{Z}_{\ge 0}$, u – оборотний елемент R, $1\le i\le n$, $p_i\in R$ і $e_i\in\mathbb{Z}_{>0}$. Тоді позначимо $l(x)=\sum_{i=1}^{n} e_i$. Усі решта позначення, які будуть використані при доведенні теорем 3 та 4, наведено у [5].

Твердження 3. *Нехай R – область головних ідеалів. Тоді $F(M_2(R))$ є правою (лівою) евклідовою множиною.*

Доведення. Виконаємо доведення для правобічного випадку. Під нормою розуміємо функцію:

$$f_2:\begin{cases} F(M_2(R)) \;\to\; \mathbb{Z}_{\ge 0} \\ O_2 \;\to\; 0 \\ M\sim diag(b_1,b_2),\ b_1\,|\,b_2\neq 0 \;\to\; \ell(b_1)+1 \end{cases}.$$

Візьмемо $n=2$, і нехай $A,B\in F(M_2(R))$, $B\neq O_2$. Тоді існують такі матриці $P,U,Q\in GL_2(R)$ і елементи $a,b,c,b_1,b_2\in R$, що

$$PAU=\begin{pmatrix} a & 0 \\ b & c \end{pmatrix} \text{ і } PBQ=\begin{pmatrix} b_1 & 0 \\ 0 & b_2 \end{pmatrix}, \tag{3}$$

де $b_1\in U(R)$.

Розглянемо таку матрицю $T=U\begin{pmatrix} 0 & -1 \\ 0 & 0 \end{pmatrix}Q^{-1}$, що

$$A-BT=P^{-1}\begin{pmatrix} a & b_1 \\ b & c \end{pmatrix}Q^{-1}.$$

Отже, за теоремою 3.9 [1], перший інваріантний елемент матриці $A-BT$ є повним дільником b_1. Отже, правильним є співвідношення $f_2(A-BT)<f_2(B)$, звідки й випливає, що $F(M_2(R))$ є правою евклідовою множиною.
Теорему доведено.

Теорема 4. *Нехай* R – область головних ідеалів і $n\in\mathbb{Z}_{>1}$. *Тоді* $F(M_n(R))$ *є правою (лівою) 2-евклідовою множиною.*

Доведення. Під нормою розуміємо функцію:

$$f_n:\begin{cases} F(M_n(R)) \;\to\; \mathbb{Z}_{\geq 0} \\ O_n \;\to\; 0 \\ M\sim diag(b_1,b_2,\dots,b_r,0,\dots,0), \; b_1\,|\,b_2\,|\dots|\,b_r, b_r\neq 0 \;\to\; \ell\Big(\prod_{i=1}^{\min(r,n-1)} b_i\Big)+1 \end{cases}.$$

Проведемо доведення індукцією за n. Оскільки будь-яка евклідова множина є ω-евклідовою множиною, то для випадку $n=2$ твердження теореми випливає з твердження.

Візьмемо $n>2$, і нехай $A,B\in F(M_n(R))$, $B\neq O_n$. Тоді існують такі матриці $P,U,Q\in GL_n(R)$, що $PBQ=diag(b_1,b_2,\dots,b_r,0,\dots,0)$, де $b_1\in U(R)$, $b_1\,|\,b_2\,|\dots|\,b_r\neq 0$ і PAU є верхньою трикутною матрицею.

1. Розглянемо перший випадок: $r=1$. Запишемо $(a_{i,j})_{1\leq i,j\leq n}=PAU$ і $E=(e_{i,j})_{1\leq i\leq n-1, 1\leq j\leq n}\in M_{n-1,n}(R)$, де для всіх $1\leq i\leq n-1, 1\leq j\leq n, e_{i,j}=a_{i+1,j}$. Звідси легко бачити, що

$$PAU=\begin{pmatrix} a_{11} & O_{1,n-1} \\ & E \end{pmatrix}.$$

Ядро E – нетривіальне. Маємо $\nu=(\nu_i)_{1\leq i\leq n}\in M_{n,1}(R/\{0\})$, де $\nu\in\ker E$ і

$$\sum_{i=1}^{n} R\nu_i=R. \tag{4}$$

Оскільки $b_1\in U(R)$, тоді $a_{11}\nu_i\in R$ і з (4) ми маємо $\lambda=(\lambda_i)_{1\leq i\leq n}\in M_{1,n}(R)$, що $\sum_{i=1}^{n}\lambda_i\nu_i=-a_{11}\nu_1+1$. Отримаємо 2-членний ланцюг подільності:

$$\begin{cases} A-BQ\begin{pmatrix} -\lambda \\ O_{n-1,n} \end{pmatrix}U^{-1}=P^{-1}\begin{pmatrix} a_{11}+\lambda_1 & \lambda_2 & \cdots & \lambda_n \\ & E & & \end{pmatrix} \\ B-P^{-1}\begin{pmatrix} a_{11}+\lambda_1 & \lambda_2 & \cdots & \lambda_n \\ & E & & \end{pmatrix}U^{-1}U\begin{pmatrix} \nu & O_{n,n-1} \end{pmatrix}Q^{-1}=O_n. \end{cases}$$

2. Розглянемо другий випадок. Нехай $r>1$ і $b_r\in U(R)$, тобто згідно припущення $b_1=b_2=\dots=b_r=1$. Розглянемо такі матриці $M\in M_{r,n}(R)$ і $M^{(0)}\in M_{n-r,n}(R)$, що

$$PAU=\begin{pmatrix} M \\ M^{(0)} \end{pmatrix}.$$

Візьмемо $\nu^{(i)}\in M_{n,1}(R)$ і $\lambda^{(i)}\in M_{1,n}(R)$ для $1\leq i\leq r$. Ядро $M^{(0)}$ є нетривіальним, тоді існує $\nu^{(1)}=(\nu_i^{(1)})_{1\leq i\leq n}\in M_{n,1}(R)$, що $M^{(0)}\nu^{(1)}=(0)_{n,1}$. Виберемо $\nu^{(1)}$ координати якого є взаємно прості, тобто задовольняють $\sum_{i=1}^{n}R\nu_i^{(1)}=R$. Це дозволяє нам взяти такі $\lambda^{(1)}\in M_{1,n}(R)$, що $\lambda^{(1)}\nu^{(1)}=(1)$.

Маючи побудову $\nu^{(i)}$ і $\lambda^{(i)}$ для $1 \le i \le i_0 < r$, тепер будуємо $\nu^{(i_0+1)}$ і $\lambda^{(i_0+1)}$. Визначимо $M^{(i_0)} \in M_n(R)$, де

$$M^{(i_0)} = \begin{pmatrix} \lambda^{(1)} \\ \vdots \\ \lambda^{(i_0)} \\ (0)_{r-i_0,n} \\ M^{(0)} \end{pmatrix}.$$

Ядро $M^{(i_0)}$ є нетривіальним, тоді існують $\nu^{(i_0+1)} \in M_{n,1}(R)$, що $M^{(i_0+1)}\nu^{(i_0+1)} = O_{n,1}$. Ми можемо вибрати $\nu^{(i_0+1)}$ так, що його координати будуть взаємно простими, що дозволяє взяти нам $\lambda^{(i_0+1)} \in M_{1,n}(R)$, що задовольняє $\lambda^{(i_0+1)}\nu^{(i_0+1)} = (1)$. Тоді ми отримаємо правий 2-членний ланцюг подільності.

$$\begin{cases} A - BQ\begin{pmatrix} M - \begin{pmatrix} \lambda^{(1)} \\ \vdots \\ \lambda^{(r)} \end{pmatrix} \\ O_{n-r,n} \end{pmatrix} U^{-1} = P^{-1}\begin{pmatrix} \lambda^{(1)} \\ \vdots \\ \lambda^{(r)} \\ M^{(0)} \end{pmatrix} U^{-1} \\ B - P^{-1}\begin{pmatrix} \lambda^{(1)} \\ \vdots \\ \lambda^{(r)} \\ M^{(0)} \end{pmatrix} U^{-1}U\begin{pmatrix} \nu^{(1)} & \cdots & \nu^{(r)} & (0)_{n,n-r} \end{pmatrix} Q^{-1} = O_n. \end{cases}$$

3. Розглянемо третій випадок. Нехай $r > 1$ і $b_r \notin U(R)$. Розглянемо такі матриці $A', B' \in F(M_{n-1}(R))$, що

$$PAU = \begin{pmatrix} a_1 & (0)_{1,n-1} \\ a_2 & \\ \vdots & A' \\ a_n & \end{pmatrix} \text{ і } PBQ = \begin{pmatrix} b & O_{1,n-1} \\ O_{n-1,1} & B' \end{pmatrix}.$$

Зрозуміло, що матриця $B' = diag(b_2, \ldots, b_r, 0, \ldots, 0)$. Тоді за припущенням, ми можемо записати 2-членний правий ланцюг подільності для матриці A', B' стосовно норми f_{n-1}, а тому існують такі матриці $Q'_1, Q'_2, R'_1, R'_2 \in M_{n-1}(R)$, що

$$\begin{cases} A' - B'Q'_1 = R'_1, \\ B' - R'_1 Q'_2 = R'_2, \end{cases} \quad f_{n-1}(R'_2) < f_{n-1}(B'). \tag{5}$$

3(а). Якщо $r = n$ і $b_{n-1} \in U(R)$, тоді $f_{n-1}(B') = 1$, тому $f_{n-1}(R'_2) = O$ і тоді $R'_2 = O_{n-1}$. Для всіх $1 \le i < n-1$, b_i ділить b_{n-1}, тому $b_i \in U(R)$ і ми маємо, що $b_1 = \cdots = b_{n-1} = 1$. Використовуючи (5), ми маємо

$$\begin{cases} A - BQ\begin{pmatrix} a_1 - 1 & O_{1,n-1} \\ a_2 & \\ \vdots & Q'_1 \\ a_n & \end{pmatrix} U^{-1} = P^{-1}\begin{pmatrix} 1 & O_{1,n-1} \\ O_{n-1,1} & R'_1 \end{pmatrix} U^{-1} \\ B - P^{-1}\begin{pmatrix} 1 & O_{1,n-1} \\ O_{n-1,1} & R'_1 \end{pmatrix} U^{-1}U\begin{pmatrix} 1 & O_{1,n-1} \\ O_{n-1,1} & Q'_2 \end{pmatrix} Q^{-1} = O_n. \end{cases}$$

Тепер розглянемо випадки, коли $r < n$ або $b_{n-1} \notin U(R)$. В обох випадках $b_r \notin U(R)$, $b_{\min(r,n-1)} \notin U(R)$.

3(б). Припустимо, що $R'_2 = O_{n-1}$. Продовжуючи (5) до порядку n ми отримаємо:

$$\begin{cases} A - BQ\begin{pmatrix} 0 & O_{1,n-1} \\ O_{n-1,1} & Q'_1 \end{pmatrix}U^{-1} = P^{-1}\begin{pmatrix} a_1 & O_{1,n-1} \\ a_2 & \\ \vdots & R'_1 \\ a_n & \end{pmatrix}U^{-1}, \\ B - P^{-1}\begin{pmatrix} a_1 & O_{1,n-1} \\ a_2 & \\ \vdots & R'_1 \\ a_n & \end{pmatrix}U^{-1}U\begin{pmatrix} 0 & O_{1,n-1} \\ O_{n-1,n} & Q'_2 \end{pmatrix}Q^{-1} = R_2, \end{cases} \tag{6}$$

де $R_2 = P^{-1}\begin{pmatrix} b_1 & O_{1,n-1} \\ O_{n-1,1} & R'_2 \end{pmatrix}Q^{-1}$. Тоді

$$f_n(B) = \ell\left(\prod_{i=1}^{\min(r,n-1)} b_i\right) \geq \ell(b_1 b_{\min(r,n-1)}) + 1 > \ell(b_1) + 1 \text{ і } f_n(R_2) = \ell(\text{b}_1) + 1,$$

де

$$f_n(R_2) < f_n(B),$$

що доводить, що (6) є 2-членним правим евклідовим алгоритмом для (A, B).

3(в). Припустимо, що $R'_2 \neq O_{n-1}$. Поставимо $r' = rk(R'_2) + 1$, запишемо

$$R'_2 \sim diag(b'_2, \ldots, b'_{r'}, 0, \ldots, 0),$$

де $b'_2 \mid b'_3 \mid \cdots \mid b'_{r'} \neq 0$. За побудовою, ці інваріантні елементи задовольняють

$$\ell\left(\prod_{i=2}^{\min(r',n-1)} b'_i\right) = f_{n-1}(R'_2) - 1 < f_{n-1}(B') - 1 = \ell\left(\prod_{i=2}^{\min(r,n-1)} b_i\right). \tag{7}$$

Крім того, ми все ще можемо розширити (5) до розміру n, як в (6). Тоді R_2 має ранг r' і $R_2 \sim diag(b_1'', b_2'', \ldots, b_{r'}'', 0, \ldots, 0)$, де $b_1'' \mid b_2'' \mid \cdots \mid b_{r'}'' \neq 0$. Тоді за теоремою 3.9 [1], $\left(\prod_{i=1}^{\min(r',n-1)} b_i''\right)$ ділить $\left(b_1 \prod_{i=2}^{\min(r',n-1)} b_i'\right)$, де з (7) випливає

$$f_n(R_2) = \ell\left(\prod_{i=1}^{\min(r',n-1)} b_i''\right) + 1 < \ell\left(\prod_{i=1}^{\min(r,n-1)} b_i\right) + 1 = f_n(\text{B}).$$

Це означає, що (6) є 2-членним правим евклідовим алгоритмом для пари (A, B). Лівобічний випадок доводиться аналогічно. Теорему доведено.

СПИСОК ЛІТЕРАТУРИ

1. Jacobson N. Basic Algebra 1 / N. Jacobson. – W. H. Freeman and Company, 1985.
2. Jacobson N. Ring theory. / N. Jacobson. – M.: Izdatelsvo inostrannoy literatury, 1947.
3. Kaplansky I. Elementary divisors and modules / I. Kaplansky // Trans. Amer. Math. Soc. – 1949. – V. 166. – P. 464-491.
4. Samuel P. About Euclidean rings / P. Samuel // Journal of Algebra. – 1971. – V. 19. – P. 282-301.
5. P. Lezowski. On some Euclidean properties of matrix algebras [Electronic resourse] / Pierre Lezowski // Electronic data. – [Talence, 2015]. – Mode of access: https://hal.inria.fr/hal-01135202v2/document (viewed on July 10, 2016).
6. Забавський Б.В. Стабільний ранг множини повних матриць над кільцем елементарних дільників / Б.В. Забавський, Б.М. Кузніцька // Укр. мат. журнал. – 2014. – Т. 66, № 5. – с. 697-700.

ЕВКЛИДОВОСТЬ ПОЛНЫХ МАТРИЦ

А.М. Романов, А.В. Саган

РЕЗЮМЕ

В этой работе показано, что над коммутативных кольцами элементарных делителей произвольное множество полных матриц порядка n является 2-евклидовым множеством. Над областью главных идеалов произвольное множество полных матриц порядка 2 является евклидовым множеством, а порядка n является 2-евклидовым множеством.

Ключевые слова: полная матрица, кольцо элементарных делителей, евклидовое кольцо, ω-евклидовое кольцо, область главных идеалов.

EUCLIDEAN FULL MATRICES

A.M. Romanov, A.V. Sagan

SUMMARY

This paper shows that over commutative rings elementary divisors of an arbitrary set of full matrix order n is 2-Euclidean set. Over arbitrary principal ideal domain full set of matrices of order 2 set is Euclidean, and the order n is 2-Euclidean set.

Keywords: full matrix, elementary divisor ring, Euclidean ring, ω-euclidean ring, principal ideal domains.