

ƯỚC CHUNG LỚN NHẤT CỦA CÁC MA TRẬN VUÔNG

Nguyễn Thị Khánh Hòa – Nguyễn Thị Kiều Trinh

Trường Đại học Thủ Dầu Một

TÓM TẮT

Dựa trên những kiến thức đã có về ước chung lớn nhất (UCLN) của các số nguyên, kết hợp sử dụng một số kết quả về ma trận trên miền chính, bài viết làm rõ định nghĩa UCLN của các ma trận vuông, chứng minh sự tồn tại UCLN của các ma trận vuông trên miền chính, trình bày chi tiết phương pháp tìm UCLN của hai ma trận vuông với các phần tử là các số nguyên và chứng minh một số tính chất của ước và UCLN các ma trận vuông.

Từ khóa: ước chung, lớn nhất, ma trận, miền chính

1 GIỚI THIỆU

Trên vành số nguyên $\mathbb{Z}$, d là UCLN của các số nguyên $a_1, a_2, \dots, a_n$ khi và chỉ khi d là ước chung lớn nhất của $\{a_1, a_2, \dots, a_n\}$ cũng chính là d là ước chung lớn nhất của $\{a_1, a_2, \dots, a_n\}$. Vì $\mathbb{Z}$ là miền chính nên luôn tồn tại UCLN của các số nguyên và dựa vào phép chia có dư trong $\mathbb{Z}$, chúng ta có phương pháp tìm UCLN chính là thuật toán Ôclit.

Khái niệm “ước chung lớn nhất” của các ma trận đã được Eugene Cahen định nghĩa tương tự như UCLN của các số nguyên[4]. Tuy nhiên, giữa vành số nguyên $\mathbb{Z}$ và vành các ma trận $M_{m \times n}(R)$ với R là vành tùy ý, là có sự khác biệt. Chẳng hạn, phép nhân các số nguyên có tính giao hoán nhưng phép nhân các ma trận thì không, trong vành số nguyên có phép chia có dư nhưng trong vành ma trận thì chưa có, vành số nguyên $\mathbb{Z}$ là miền chính nhưng với R là vành tùy ý thì vành $M_n(R)$ không chắc là miền chính. Do đó, khi R là vành tùy ý thì sự tồn tại của UCLN của các ma trận không được đảm bảo và phương pháp tìm UCLN của hai ma trận cũng không thể làm tương tự như thuật toán Ôclit được. Eugene Cahen cũng chưa đề cập đến vấn đề rằng UCLN của các ma trận vuông có luôn tồn tại hay không[4]. Phương pháp tìm UCLN của các

ma trận cũng không được thể hiện một cách tường minh. Để góp phần làm sáng tỏ vấn đề này, chúng tôi sẽ đưa ra một điều kiện vành R là một miền chính (bổ đề 2) và từ đó có thể khẳng định UCLN của các ma trận vuông trên miền chính luôn tồn tại (định lý 1). Chúng tôi cũng sẽ trình bày chi tiết phương pháp tìm UCLN của hai ma trận vuông với các phần tử là các số nguyên (định lý 2, định lý 3) và chứng minh một số tính chất của ước và UCLN các ma trận vuông.

2. KIẾN THỨC CƠ BẢN

2.1 Bổ đề 1 (định lý 6.1, trang 218, [8]): Cho R là miền chính và M là môđun con của R - môđun R^n . Khi đó M là môđun tự do với hạng không vượt quá n .

2.2 Bổ đề 2 (bài tập 17 chương 15, trang 203, [9]): Cho R là miền chính. I là d -đơn trái của $M_n(R)$. Khi đó I là d -đơn trái chính của $M_n(R)$.

3. MỘT SỐ KẾT QUẢ

Trong phần này, ta luôn giả sử R là miền chính.

3.1. Các định nghĩa

Eugene Cahen định nghĩa ước cho các ma trận với cấp tùy ý[4]. Trong phạm vi của bài viết này, chúng tôi chỉ đề cập đến ước và UCLN của các ma trận vuông.

3.1.1. Ước của ma trận vuông

Định nghĩa:

Cho $M_n(R)$ là vành. Giả sử $A \in M_n(R)$, $D \in M_n(R)$, $D \neq O$.

Ta nói D là *ước bên phải (trái) của ma trận* A , nếu tồn tại $P \in M_n(R)$ sao cho

$$A = PD \text{ (tương ứng } A = DP).$$

Ví dụ:

Trên $M_2(\mathbb{Z})$, cho hai ma trận

$$A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, D = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, D \neq O.$$

D là ước bên phải của A vì tồn tại

$$P = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \in M_2(\mathbb{Z}) \text{ để } A = PD.$$

Tính chất:

i) A là *ước bên phải, trái của ma trận đơn vị* I_n khi và chỉ khi A là ma trận khả nghịch.

Chứng minh:

($\Leftarrow$) Giả sử A là ma trận khả nghịch.

Suy ra tồn tại B là ma trận nghịch đảo của A sao cho $I_n = AB$.

Do đó A vừa là ước bên phải, vừa là ước bên trái của I_n .

($\Rightarrow$) Giả sử A là ước bên phải, trái của I_n . Suy ra tồn tại ma trận B sao cho $I_n = BA$.

Khi đó: $\det B \cdot \det A = \det I_n = 1$. Suy ra A khả nghịch.

Chứng minh tương tự cho A là ước bên trái của I_n .

ii) (Mục 368, chương 19, [4]) A là *ước (bên phải và bên trái) của* A .

Chứng minh: Hiển nhiên, bởi vì tồn tại ma trận đơn vị I_n để $A = I_n A = A I_n$.

iii) Nếu A là *ước bên phải của* B và B là *ước bên phải của* C thì A là *ước bên phải*

của C .

Chứng minh: Vì A là ước bên phải của B và B là ước bên phải của C nên tồn tại $P, Q \in M_n(R)$ để $B = PA$ và $C = QB$. Suy ra $C = (QP)A$. Do đó, A là ước bên phải của C .

iv) Với $A_1, A_2, \dots, A_n \in M_n(R)$, nếu D là *ước bên phải của* $A_1, A_2, \dots, A_n$ thì D là *ước bên phải của* $(P_1 A_1 + P_2 A_2 + \dots + P_n A_n)$ với $P_i \in M_n(R)$, $\forall i = \overline{1, n}$.

Chứng minh: Vì D là ước bên phải của A_i , $i = \overline{1, n}$ nên tồn tại các ma trận $Q_i \in M_n(R)$, $i = \overline{1, n}$ sao cho $A_i = Q_i D$. Khi đó:

$$\begin{aligned} & P_1 A_1 + P_2 A_2 + \dots + P_n A_n \\ &= P_1 (Q_1 D) + P_2 (Q_2 D) + \dots + P_n (Q_n D) \\ &= (P_1 Q_1 + P_2 Q_2 + \dots + P_n Q_n) D. \end{aligned}$$

3.1.2 Ước chung của các ma trận vuông

Định nghĩa:

Trên $M_n(R)$, ma trận D được gọi là *ước chung bên phải (trái) của các ma trận* $A_1, A_2, \dots, A_n$ nếu D là ước bên phải (trái) đồng thời của mỗi ma trận đó.

Ví dụ:

Trên $M_2(\mathbb{Z})$, $D = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$ là ước chung bên phải của $A = \begin{bmatrix} 3 & 3 \\ 3 & 3 \end{bmatrix}$ và $B = \begin{bmatrix} 2 & 2 \\ 1 & 1 \end{bmatrix}$.

Vì tồn tại các ma trận $M = \begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix}$, $N = \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}$ để $A = MD$ và $B = ND$.

3.1.3 UCLN của các ma trận vuông

Định nghĩa:

Trên $M_n(R)$, cho D là một ước chung bên phải (trái) của các ma trận $A_1, A_2, \dots, A_n$.

Nếu mọi ước chung bên phải (trái) của $A_1, A_2, \dots, A_n$ đều là ước bên phải (trái) của D thì D được gọi là *ước chung lớn nhất bên phải (trái) của các ma trận đó*.

bên phải của các ma trận và ta viết tắt ước chung lớn nhất của $A_1, A_2, \dots, A_n$ là $UCLN(A_1, A_2, \dots, A_n)$.

Sau đây, ta chỉ xét ước chung lớn nhất

Ví dụ:

Trên $M_2(\mathbb{Z})$, cho $A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}, B = \begin{bmatrix} 4 & 3 \\ 2 & 1 \end{bmatrix}$. Khi đó, $D = \begin{bmatrix} 1 & 2 \\ 0 & -1 \end{bmatrix}$ là $UCLN(A, B)$.

Thật vậy, ta có: $\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 3 & 2 \end{bmatrix} \cdot \begin{bmatrix} 1 & 2 \\ 0 & -1 \end{bmatrix}$ và $\begin{bmatrix} 4 & 3 \\ 2 & 1 \end{bmatrix} = \begin{bmatrix} 4 & 5 \\ 2 & 3 \end{bmatrix} \cdot \begin{bmatrix} 1 & 2 \\ 0 & -1 \end{bmatrix}$

nên D là ước chung bên phải của A và B .

Hơn nữa, ta có: $\begin{bmatrix} 1 & 2 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 2 & -2 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 4 & 3 \\ 2 & 1 \end{bmatrix}$.

hay $D = XA + YB$ với $X = \begin{bmatrix} 1 & 0 \\ 2 & -2 \end{bmatrix}$ và $Y = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$.

Do đó, nếu D_1 là ước chung bên phải của A và B , tức là $A = A_1 D_1$; $B = B_1 D_1$ thì $D = (XA_1)D_1 + (YB_1)D_1 = (XA_1 + YB_1)D_1$, tức là D_1 là ước bên phải của D .

Nhận xét:

1) Nếu D và D' là $UCLN(A_1, A_2, \dots, A_n)$ thì D và D' sai khác nhau một ma trận khả nghịch, nghĩa là tồn tại $U, V \in M_n(R)$ khả nghịch sao cho $D = UD'$ và $D' = VD$.

Chứng minh:

Vì D, D' là $UCLN(A_1, A_2, \dots, A_n)$ nên D là ước bên phải của D' , D' là ước bên phải của D . Do đó tồn tại $U, V \in M_n(R)$ để $D = UD'$ và $D' = VD$.

Khi đó $D = UD' = UVD$. Suy ra $\det D = \det U \cdot \det V \cdot \det D$.

Vì R là miền nguyên nên $\det U \cdot \det V = 1$. Suy ra U, V khả nghịch.

2) Theo nhận xét 1, ta có thể kết luận $UCLN(A_1, A_2, \dots, A_n)$ là không duy nhất.

3.2 Sự tồn tại và phương pháp tìm UCLN của các ma trận vuông

3.2.1 Sự tồn tại UCLN của các ma trận vuông

Định lý 1: Giả sử R là miền chính. Khi đó, luôn tồn tại UCLN bên phải (trái) của các ma trận vuông thuộc $S = M_n(R)$.

Chứng minh: Giả sử $A_1, A_2, \dots, A_n$ là các ma trận tùy ý thuộc $M_n(R)$, ta sẽ chứng minh luôn tồn tại $UCLN(A_1, A_2, \dots, A_n)$.

– Xét $M = SA_1 + SA_2 + \dots + SA_n = \{D_1 A_1 + D_2 A_2 + \dots + D_n A_n \mid D_1, D_2, \dots, D_n \in S\}$.

– Ta thấy M là ideal trái của S .

– Theo bổ đề 2 (mục 2.2), vì R là miền chính nên mọi ideal trái của S đều là ideal trái chính. Suy ra tồn tại $D \in S$ sao cho: $M = SD = \{K.D \mid K \in S\}$.

– Ta chứng minh D là $UCLN(A_1, A_2, \dots, A_n)$.

Hệ quả: Trên $M_n(R)$, nếu D là $UCLN(A_1, A_2, \dots, A_n)$ thì tồn tại các ma trận

$U_1, U_2, \dots, U_n \in M_n(R)$ sao cho $D = U_1 A_1 + U_2 A_2 + \dots + U_n A_n$.

Định lý 2:

Cho R là vành chính và A, B là các ma trận vuông cấp n trong vành $M_n(R)$.

Đặt $C = \begin{bmatrix} A \\ B \end{bmatrix}$ là ma trận cấp $2n \times n$. Nếu tồn tại ma trận khả nghịch V sao cho

$VC = H$ là ma trận bậc thang thì các khẳng định sau đây là đúng:

i) Gọi D là n dòng đầu của H thì D là UCLN(A, B).

ii) Đặt n cột đầu của V^{-1} là $\begin{bmatrix} P \\ Q \end{bmatrix}$ thì $A = PD$; $B = QD$.

iii) Đặt n dòng đầu của V là $\begin{bmatrix} X & Y \end{bmatrix}$ thì $XA + YB = D$.

Chứng minh:

Giả sử $V = \begin{bmatrix} X & Y \\ * & * \end{bmatrix}_{2n \times 2n}$; $V^{-1} = \begin{bmatrix} P & * \\ Q & * \end{bmatrix}_{2n \times 2n}$; $H = \begin{bmatrix} D \\ O \end{bmatrix}_{2n \times n}$ trong đó X, Y, P, Q, D là các

ma trận vuông cấp n .

– Theo giả thiết $VC = H$ mà V khả nghịch nên $C = V^{-1}H$.

Do đó $C = \begin{bmatrix} A \\ B \end{bmatrix} = V^{-1}H = \begin{bmatrix} P & * \\ Q & * \end{bmatrix} \begin{bmatrix} D \\ O \end{bmatrix}$. Điều này cho ta $A = PD$ và $B = QD$.

Có nghĩa D là ước chung bên phải của A và B .

– Cũng từ $VC = H$ ta suy ra $\begin{bmatrix} X & Y \\ * & * \end{bmatrix} \begin{bmatrix} A \\ B \end{bmatrix} = \begin{bmatrix} D \\ O \end{bmatrix} \Rightarrow XA + YB = D$.

– Giả sử D' là ước chung bên phải của A, B nghĩa là tồn tại $P', Q' \in M_n(R)$ sao cho $A = P'D'$; $B = Q'D'$. Khi đó $D = XA + YB = XP'D' + YQ'D' = (XP' + YQ')D'$.

Suy ra D' là ước bên phải của D . Vậy D là UCLN(A, B).

Kết quả sau được chứng minh trong trường hợp $R = \mathbb{Z}$.

Định lý 3: Bằng cách sử dụng hai phép biến đổi sơ cấp trên dòng (đổi chỗ 2 dòng; Cộng vào 1 dòng một bội của dòng khác) ta luôn đưa được một ma trận C bất kỳ về dạng bậc thang H và tồn tại một ma trận khả nghịch V sao cho $VC = H$.

Chứng minh:

– Chứng minh: mọi ma trận C bất kỳ đều đưa được về dạng bậc thang H .

– Chứng minh: tồn tại một ma trận khả nghịch V sao cho $VC = H$.

Giả sử H là ma trận bậc thang nhận được sau k phép biến đổi sơ cấp.

Khi đó $E_k \dots E_1 C = H$. Đặt $V = E_k \dots E_1$. Ta sẽ chứng minh V khả nghịch.

Nếu E_i ($1 \leq i \leq k$) là ma trận sơ cấp có được do đổi dòng thì $\det E_i = -\det I_m = -1$.

Nếu E_i ($1 \leq i \leq k$) là ma trận sơ cấp có được do cộng vào một dòng một bội của dòng khác thì $\det E_i = \det I_m = 1$. Do đó $\det V = \pm 1$. Có nghĩa là V là ma trận khả nghịch.

3.2.2 Phương pháp tìm UCLN của các ma trận vuông

Từ chứng minh của định lý 2 và định lý 3 mục 3.2.1, ta có được thuật toán sau:

Thuật toán tìm UCLN của hai ma trận vuông A, B trên vành $M_n(\mathbb{Z})$

Với $A, B \in M_n(\mathbb{Z})$. Đặt $C = \begin{bmatrix} A \\ B \end{bmatrix}_{2n \times n}$.

Đưa ma trận C về dạng bậc thang H bằng hai phép biến đổi sơ cấp trên dòng (phép đổi chỗ hai dòng, phép cộng vào dòng này một bội của dòng khác).

Bước 1: Giả sử j là cột đầu tiên khác 0 của C , sử dụng phép đổi chỗ các dòng để $c_{kj} \neq 0$ là phần tử đầu tiên của cột j và là phần tử có giá trị tuyệt đối nhỏ nhất trên cột j .

Bước 2: Khử các phần tử c_{ij} ($i > k$) bằng cách cộng vào dòng i một bội $-q_i$ của dòng j . Trong đó: $c_{ij} = q_i \cdot c_{jj} + r_i$; $0 \leq r_i < c_{jj}$, $q_i, r_i \in \mathbb{Z}$.

Bước 3: Lập lại các bước 1 và bước 2 cho các cột kế tiếp của C .

Bước 4: Ma trận D tạo bởi n dòng đầu của H là $UCLN(A, B)$.

Ví dụ: Tìm UCLN của hai ma trận vuông A và B , biết $A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$ và $B = \begin{bmatrix} 4 & 3 \\ 2 & 1 \end{bmatrix}$.

Đặt $C = \begin{bmatrix} 1 & 2 \\ 3 & 4 \\ 4 & 3 \\ 2 & 1 \end{bmatrix}$. Ta tiến hành đưa ma trận C về dạng bậc thang.

Bước 1: Ta có $c_{11} = 1 \neq 0$ là phần tử có giá trị tuyệt đối nhỏ nhất trên cột 1 của C .

Bước 2: Khử các phần tử (của cột 1) nằm bên dưới phần tử c_{11} của C .

– Để khử $c_{21} = 3$, ta cộng vào dòng 2 một bội $-q_1 = -3$ dòng 1. Ta được:

$$C_1 = \begin{bmatrix} 1 & 2 \\ 0 & -2 \\ 4 & 3 \\ 2 & 1 \end{bmatrix}. \text{ Khử phần tử } c_{31} = 4 \text{ và } c_{41} = 2 \text{ thu được ma trận: } C_2 = \begin{bmatrix} 1 & 2 \\ 0 & -2 \\ 0 & -5 \\ 0 & -3 \end{bmatrix}.$$

Bước 3: Lập lại bước 1 và bước 2 cho cột 2 của ma trận C_2 .

Ta có $c_{22} = -2 \neq 0$ là phần tử có giá trị tuyệt đối nhỏ nhất trên cột 2 của ma trận C_2 .

– Để khử $c_{32} = -5$, ta cộng vào dòng 3 một bội $-q_4 = -3$ dòng 2. Ta được:

$$C_3 = \begin{bmatrix} 1 & 2 \\ 0 & -2 \\ 0 & 1 \\ 0 & -3 \end{bmatrix}.$$

Vì $c_{32} = 1 \neq 0$ là phần tử có giá trị tuyệt đối nhỏ nhất trên cột 2 của ma trận C_3 , nên ta thực hiện phép đổi chỗ $d_2 \leftrightarrow d_3$ của C_3 .

– Ta tiếp tục khử phần tử $c_{32} = -2$ và $c_{42} = -3$ tương tự như trên.

Bước 4: Sau bước 3, ma trận C được đưa về dạng bậc thang là $C_4 = \begin{bmatrix} 1 & 2 \\ 0 & 1 \\ 0 & 0 \\ 0 & 0 \end{bmatrix}$.

Vậy $UCLN(A, B)$ là $D = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$ (D là ma trận tạo bởi 2 dòng đầu của C_4).

Phương pháp tìm UCLN của nhiều ma trận:

Cho $A_1, A_2, \dots, A_n \in M_n(\mathbb{Z})$.

Gọi D_2 là $UCLN(A_1, A_2)$, D_3 là $UCLN(D_2, A_3)$, ..., D_n là $UCLN(D_{n-1}, A_n)$.

Khi đó D_n là $UCLN(A_1, A_2, \dots, A_n)$.

Thật vậy, ta thấy rằng mọi ước chung của $A_1, A_2, \dots, A_n$ đều là ước chung của $D_2, A_3, \dots, A_n$ và ngược lại. Vì vậy ta có $UCLN(A_1, A_2, \dots, A_n) = UCLN(D_2, A_3, \dots, A_n)$.

Lặp lại lí luận này nhiều lần, ta sẽ được $UCLN(A_1, A_2, \dots, A_n) = UCLN(D_2, A_3, \dots, A_n) = UCLN(D_3, A_4, \dots, A_n) = \dots = UCLN(D_{n-1}, A_n)$

nghĩa là D_n là $UCLN(A_1, A_2, \dots, A_n)$.

3.3 Một số tính chất của UCLN của các ma trận vuông

1) (Mục 379, chương 19, [4]) $\forall K \in M_n(R)$, nếu D là $UCLN(A_1, A_2, \dots, A_n)$ thì DK là $UCLN(A_1K, A_2K, \dots, A_nK)$.

Chứng minh

– Giả sử D là $UCLN(A_1, A_2, \dots, A_n)$.

Suy ra tồn tại $U_1, U_2, \dots, U_n \in M_n(R)$ để $D = U_1A_1 + U_2A_2 + \dots + U_nA_n$.

Suy ra $DK = U_1(A_1K) + U_2(A_2K) + \dots + U_n(A_nK)$.

Suy ra DK là ước chung bên phải của $A_1K, A_2K, \dots, A_nK$.

– Giả sử E là ước chung bên phải tùy ý của $A_1K, A_2K, \dots, A_nK$.

Ta có: $A_iK = X_iE$ ($X_i \in M_n(R)$, $\forall i = \overline{1, n}$).

Khi đó:

$$\begin{aligned} DK &= U_1(X_1E) + U_2(X_2E) + \dots + U_n(X_nE) = (U_1X_1)E + (U_2X_2)E + \dots + (U_nX_n)E \\ &= (U_1X_1 + U_2X_2 + \dots + U_nX_n)E \end{aligned}$$

Suy ra E là ước bên phải của DK . Vậy DK là $UCLN(A_1K, A_2K, \dots, A_nK)$

2) Cho K là ước chung bên phải của $A_1, A_2, \dots, A_n$ (tức là tồn tại K_i để $A_i = K_iK$ với $i = \overline{1, n}$). Nếu D là $UCLN(K_1, K_2, \dots, K_n)$ thì DK là $UCLN(A_1, A_2, \dots, A_n)$.

Chứng minh: Tính chất 2 được suy ra trực tiếp từ tính chất 1.

3) $\forall K \in M_n(R)$, nếu E là $UCLN(A_1K, A_2K, \dots, A_nK)$ thì $E = D.K$ với $D \in M_n(R)$.

Chứng minh: Vì E là $UCLN(A_1K, A_2K, \dots, A_nK)$ nên tồn tại các ma trận

$X_1, X_2, \dots, X_n \in M_n(R)$ sao cho

$$E = X_1(A_1K) + X_2(A_2K) + \dots + X_n(A_nK) = (X_1A_1 + X_2A_2 + \dots + X_nA_n).K$$

Đặt $D = X_1A_1 + X_2A_2 + \dots + X_nA_n \in M_n(R)$. Khi đó $E = D.K$.

4) Cho D là ước chung của $A_1, A_2, \dots, A_n$ (tức là tồn tại E_i để $A_i = E_iD$ với $i = \overline{1, n}$).

Khi đó, D là $UCLN(A_1, A_2, \dots, A_n)$ khi và chỉ khi I là $UCLN(E_1, E_2, \dots, E_n)$.

Chứng minh: Giả sử D là $UCLN(A_1, A_2, \dots, A_n)$ và U là $UCLN(E_1, E_2, \dots, E_n)$.

Khi đó, theo tính chất 1, ta suy ra UD cũng là $UCLN(A_1, A_2, \dots, A_n)$.

Do đó, UD là ước của D , tức là tồn tại ma trận V sao cho $D = V(UD)$.

Suy ra $D = (VU)D$. Suy ra $\det(VU) = 1 \neq 0$ hay ma trận U khả nghịch.

Do đó, theo nhận xét 2 (mục 3.1.3), ta có $U^{-1}U = I$ cũng là $UCLN(E_1, E_2, \dots, E_n)$.

Điều ngược lại được suy ra trực tiếp từ tính chất 1.

5) Nếu I là $UCLN(A, B)$ và B là ước của AC thì B là ước của C .

Chứng minh: Vì I là $UCLN(A, B)$ nên tồn tại $X, Y \in M_n(R)$ để $I = XA + YB$.

Suy ra $IC = (XA + YB)C$. Suy ra $C = XAC + YBC$.

Vì B là ước của AC và B là ước của BC nên B là ước của $(XAC + YBC)$.

Do đó B là ước của C .

6) Nếu I là $UCLN(A, B)$ và D là $UCLN(C, B)$ thì D là $UCLN(AC, B)$ và ngược lại.

Chứng minh

– Giả sử D là ước chung của AC và B . Suy ra D là ước chung của AC và BC .

Mà theo tính chất 1, vì I là $UCLN(A, B)$ nên C là $UCLN(AC, BC)$.

Do đó D là ước của C . Vậy D là ước chung của B và C .

– Ngược lại, giả sử D là ước chung của C và B . Suy ra D là ước chung của AC và B .

– Như vậy, tập hợp các ước chung của AC và B trùng với tập hợp các ước chung của C và B nên nếu D là $UCLN(C, B)$ thì D là $UCLN(AC, B)$.

7) Nếu I là $UCLN(A, B)$ và I là $UCLN(A, C)$ thì I cũng là $UCLN(A, BC)$.

Chứng minh: Giả sử D là $UCLN(A, BC)$, theo tính chất 6, D cũng là $UCLN(A, C)$.

Mà I là $UCLN(A, C)$ nên D là ước của I , tức là D khả nghịch.

Do đó $D^{-1}D = I$ cũng là $UCLN(A, BC)$.

GREATEST COMMON DIVISOR OF SQUARE MATRICES

Nguyễn Thị Khánh Hòa – Nguyễn Thị Kiều Trinh

ABSTRACT

Based on existing knowledge about the greatest common divisor of integers in combination with matrix results on the primary domain, the article clarifies definition of greatest common divisor of square matrices, proving the existence of the greatest common divisor of the square matrices on the main domain, detailing how to find the greatest

common divisor of two square matrices with elements as integers, and proving some properties of the divisor and the greatest common divisor of square matrices.

TÀI LIỆU THAM KHẢO

- [1] Bùi Xuân Hải (Chủ biên), *Đại số tuyến tính*, Trường Đại học Khoa học Tự nhiên TP.HCM, 2000.
- [2] Donald Knuth -Addison wesleef Longman, *Ine - Seminumericalalgorithms (The art of computer programming)*, Third edition, 1997.
- [3] Dương Quốc Việt, *Cơ sở lý thuyết module*, NXB Đại học Sư phạm, 2008.
- [4] Éugene Cahen, *Théorie des nombres*, Librairie Sciencetifique A. Hermann & Fils, 1914.
- [5] Hoàng Xuân Sính, *Đại số đại cương*, NXB Giáo dục, 1999
- [6] Nguyễn Hữu Việt Hưng, *Đại số đại cương*, NXB Giáo dục, 1998.
- [7] Nguyễn Tiến Tài (Chủ biên), *Số học*, NXB Giáo dục, 1999.
- [8] Thomas W. Hungerford, *Algebra*, Springer Science & Business Media, 1974.
- [9] William Brown, *Matrices over commutative rings*, Marcel Dekker, 1993.