FORMALIZED MATHEMATICS
Vol. **16**, No. **2**, Pages 195–202, **2008**
DOI: 10.2478/v10037-008-0025-z

Invertibility of Matrices of Field Elements

Yatsuka Nakamura
Shinshu University
Nagano, Japan

Kunio Oniumi
Shinshu University
Nagano, Japan

Wenpai Chang
Nan Kai Institute of Technology
Nantou County, Taiwan

Summary. In this paper the theory of invertibility of matrices of field elements (see e.g. [5], [6]) is developed. The main purpose of this article is to prove that the left invertibility and the right invertibility are equivalent for a matrix of field elements. To prove this, we introduced a special transformation of matrix to some canonical forms. Other concepts as zero vector and base vectors of field elements are also introduced as a preparation.

MML identifier: `MATRIX14`, version: `7.9.01 4.101.1015`

The papers [14], [3], [7], [17], [4], [13], [15], [10], [1], [12], [18], [16], [9], [8], [2], and [11] provide the terminology and notation for this paper.

1. Preliminaries

We use the following convention: x, y denote sets, n, m, i, j denote elements of $\mathbb{N}$, and K denotes a field.

Let K be a non empty zero structure and let us consider n. The functor 0_K^n yields a finite sequence of elements of K and is defined by:

(Def. 1) $0_K^n = n \mapsto 0_K$.

Let K be a non empty zero structure and let us consider n. Then 0_K^n is an element of (the carrier of K)^n.

In the sequel L denotes a non empty additive loop structure.

The following three propositions are true:

ISSN 1426–2630(p), 1898-9934(e)

(1) Every finite sequence x of elements of L is an element of (the carrier of $L)^{\operatorname{len} x}$.

(2) For all finite sequences x_1, x_2 of elements of L such that $\operatorname{len} x_1 = \operatorname{len} x_2$ holds $\operatorname{len}(x_1 + x_2) = \operatorname{len} x_1$.

(3) For all finite sequences x_1, x_2 of elements of L such that $\operatorname{len} x_1 = \operatorname{len} x_2$ holds $\operatorname{len}(x_1 - x_2) = \operatorname{len} x_1$.

In the sequel G is a non empty multiplicative loop structure.

Next we state four propositions:

(4) Let x_1, x_2 be finite sequences of elements of G and given i. If $i \in \operatorname{dom}(x_1 \bullet x_2)$, then $(x_1 \bullet x_2)(i) = (x_1)_i \cdot (x_2)_i$ and $(x_1 \bullet x_2)_i = (x_1)_i \cdot (x_2)_i$.

(5) Let x_1, x_2 be finite sequences of elements of L and i be a natural number. If $\operatorname{len} x_1 = \operatorname{len} x_2$ and $1 \leq i \leq \operatorname{len} x_1$, then $(x_1 + x_2)(i) = (x_1)_i + (x_2)_i$ and $(x_1 - x_2)(i) = (x_1)_i - (x_2)_i$.

(6) For every element a of K and for every finite sequence x of elements of K holds $-a \cdot x = (-a) \cdot x$ and $-a \cdot x = a \cdot -x$.

(7) For all finite sequences x_1, x_2, y_1, y_2 of elements of G such that $\operatorname{len} x_1 = \operatorname{len} x_2$ and $\operatorname{len} y_1 = \operatorname{len} y_2$ holds $x_1 \frown y_1 \bullet x_2 \frown y_2 = (x_1 \bullet x_2) \frown (y_1 \bullet y_2)$.

Let us consider K and let e_1, e_2 be finite sequences of elements of K. We introduce $|(e_1, e_2)|$ as a synonym of $e_1 \cdot e_2$.

Next we state several propositions:

(8) Let x, y be finite sequences of elements of K and a be an element of K. If $\operatorname{len} x = \operatorname{len} y$, then $a \cdot x \bullet y = a \cdot (x \bullet y)$ and $x \bullet a \cdot y = a \cdot (x \bullet y)$.

(9) For all finite sequences x, y of elements of K and for every element a of K such that $\operatorname{len} x = \operatorname{len} y$ holds $|(a \cdot x, y)| = a \cdot |(x, y)|$.

(10) For all finite sequences x, y of elements of K and for every element a of K such that $\operatorname{len} x = \operatorname{len} y$ holds $|(x, a \cdot y)| = a \cdot |(x, y)|$.

(11) Let x, y_1, y_2 be finite sequences of elements of K and a be an element of K. If $\operatorname{len} x = \operatorname{len} y_1$ and $\operatorname{len} x = \operatorname{len} y_2$, then $|(x, y_1 + y_2)| = |(x, y_1)| + |(x, y_2)|$.

(12) For all finite sequences x_1, x_2, y_1, y_2 of elements of K such that $\operatorname{len} x_1 = \operatorname{len} x_2$ and $\operatorname{len} y_1 = \operatorname{len} y_2$ holds $|(x_1 \frown y_1, x_2 \frown y_2)| = |(x_1, x_2)| + |(y_1, y_2)|$.

(13) For every element p_1 of (the carrier of $K)^n$ holds $p_1 \bullet n \mapsto 0_K = n \mapsto 0_K$.

Let us consider n, let us consider K, and let A be a square matrix over K of dimension n. We introduce $\operatorname{Inv} A$ as a synonym of $A^{\smile}$.

2. Zero Vector and Base Vectors of Field Elements

Next we state several propositions:

(14) $I_K^{0 \times 0} = 0_K^{0 \times 0}$ and $I_K^{0 \times 0} = \emptyset$.

(15) For every square matrix A over K of dimension 0 holds $A = \emptyset$ and $A = I_K^{0\times 0}$ and $A = 0_K^{0\times 0}$.

(16) Every square matrix over K of dimension 0 is invertible.

(17) For all square matrices A, B, C over K of dimension n holds $(A\cdot B)\cdot C = A\cdot(B\cdot C)$.

(18) Let A, B be square matrices over K of dimension n. Then A is invertible and $B = A^{\smile}$ if and only if $B\cdot A = I_K^{n\times n}$ and $A\cdot B = I_K^{n\times n}$.

(19) Let A be a square matrix over K of dimension n. Then A is invertible if and only if there exists a square matrix B over K of dimension n such that $B\cdot A = I_K^{n\times n}$ and $A\cdot B = I_K^{n\times n}$.

(20) For every finite sequence x of elements of K holds $|(x, 0_K^{\mathrm{len}\,x})| = 0_K$.

(21) For every finite sequence x of elements of K holds $|(0_K^{\mathrm{len}\,x}, x)| = 0_K$.

(22) For every element a of K holds $|(\langle 0_K\rangle, \langle a\rangle)| = 0_K$.

Let K be a non empty set, let n be a natural number, and let a be an element of K. Then $n \mapsto a$ is a finite sequence of elements of K.

Let us consider K and let n, i be natural numbers. The i-versor in K^n yields a finite sequence of elements of K and is defined by:

(Def. 2) The i-versor in $K^n = \mathrm{Replace}(n \mapsto 0_K, i, 1_K)$.

Next we state several propositions:

(23) For all natural numbers n, i holds len (the i-versor in K^n) $= n$.

(24) For all natural numbers i, n such that $1 \leq i \leq n$ holds (the i-versor in K^n)$(i) = 1_K$.

(25) Let i, j, n be natural numbers. Suppose $1 \leq i \leq n$ and $1 \leq j \leq n$ and $i \neq j$. Then (the i-versor in K^n)$(j) = 0_K$.

(26) For all natural numbers i, n such that $1 \leq i \leq n$ holds $I_K^{n\times n}(i) =$ the i-versor in K^n.

(27) For all i, j such that $1 \leq i \leq n$ and $1 \leq j \leq n$ holds ${I_K^{n\times n}}_{i,j} =$ (the i-versor in K^n)(j).

(28) Let A be a square matrix over K of dimension n. Then $A = 0_K^{n\times n}$ if and only if for all elements i, j of $\mathbb{N}$ such that $1 \leq i \leq n$ and $1 \leq j \leq n$ holds $A_{i,j} = 0_K$.

(29) Let A be a square matrix over K of dimension n. Then $A = I_K^{n\times n}$ if and only if for all elements i, j of $\mathbb{N}$ such that $1 \leq i \leq n$ and $1 \leq j \leq n$ holds $A_{i,j} = (i = j \rightarrow 1_K, 0_K)$.

3. Conditions of Invertibility

One can prove the following propositions:

(30) For all square matrices A, B over K of dimension n holds $(A \cdot B)^{\mathrm{T}} = B^{\mathrm{T}} \cdot A^{\mathrm{T}}$.

(31) For every square matrix A over K of dimension n such that A is invertible holds A^{T} is invertible and $(A^{\mathrm{T}})^{\smile} = (A^{\smile})^{\mathrm{T}}$.

(32) Let x be a finite sequence of elements of K and a be an element of K. Given i such that $1 \leq i \leq \mathrm{len}\, x$ and $x(i) = a$ and for every j such that $j \neq i$ and $1 \leq j \leq \mathrm{len}\, x$ holds $x(j) = 0_K$. Then $\sum x = a$.

(33) Let f_1, f_2 be finite sequences of elements of K. Then $\mathrm{dom}(f_1 \bullet f_2) = \mathrm{dom}\, f_1 \cap \mathrm{dom}\, f_2$ and for every i such that $i \in \mathrm{dom}(f_1 \bullet f_2)$ holds $(f_1 \bullet f_2)(i) = (f_1)_i \cdot (f_2)_i$.

(34) Let x, y be finite sequences of elements of K and given i. Suppose $\mathrm{len}\, x = m$ and $y = x \bullet$ the i-versor in K^m and $1 \leq i \leq m$. Then $y(i) = x(i)$ and for every j such that $j \neq i$ and $1 \leq j \leq m$ holds $y(j) = 0_K$.

(35) Let x be a finite sequence of elements of K. Suppose $\mathrm{len}\, x = m$ and $1 \leq i \leq m$. Then $|(x, \text{the } i\text{-versor in } K^m)| = x(i)$ and $|(x, \text{the } i\text{-versor in } K^m)| = x_i$.

(36) For all m, i such that $1 \leq i \leq m$ holds $|(\text{the } i\text{-versor in } K^m, \text{the } i\text{-versor in } K^m)| = 1_K$.

(37) Let a be an element of K and P, Q be square matrices over K of dimension n. Suppose that $n > 0$ and $a \neq 0_K$ and $P_{1,1} = a^{-1}$ and for every i such that $1 < i \leq n$ holds $P(i) =$ the i-versor in K^n and $Q_{1,1} = a$ and for every j such that $1 < j \leq n$ holds $Q_{1,j} = -a \cdot P_{1,j}$ and for every i such that $1 < i \leq n$ holds $Q(i) =$ the i-versor in K^n. Then P is invertible and $Q = P^{\smile}$.

(38) Let a be an element of K and P be a square matrix over K of dimension n. Suppose $n > 0$ and $a \neq 0_K$ and $P_{1,1} = a^{-1}$ and for every i such that $1 < i \leq n$ holds $P(i) =$ the i-versor in K^n. Then P is invertible.

(39) Let A be a square matrix over K of dimension n. Suppose $n > 0$ and $A_{1,1} \neq 0_K$. Then there exists a square matrix P over K of dimension n such that
  (i) P is invertible,
  (ii) $(A \cdot P)_{1,1} = 1_K$,
  (iii) for every j such that $1 < j \leq n$ holds $(A \cdot P)_{1,j} = 0_K$, and
  (iv) for every i such that $1 < i \leq n$ and $A_{i,1} = 0_K$ holds $(A \cdot P)_{i,1} = 0_K$.

(40) Let A be a square matrix over K of dimension n. Suppose $n > 0$ and $A_{1,1} \neq 0_K$. Then there exists a square matrix P over K of dimension n such that

(i) P is invertible,
(ii) $(P \cdot A)_{1,1} = 1_K$,
(iii) for every i such that $1 < i \leq n$ holds $(P \cdot A)_{i,1} = 0_K$, and
(iv) for every j such that $1 < j \leq n$ and $A_{1,j} = 0_K$ holds $(P \cdot A)_{1,j} = 0_K$.

(41) Let A be a square matrix over K of dimension n. Suppose $n > 0$ and $A_{1,1} \neq 0_K$. Then there exist square matrices P, Q over K of dimension n such that
(i) P is invertible,
(ii) Q is invertible,
(iii) $(P \cdot A \cdot Q)_{1,1} = 1_K$,
(iv) for every i such that $1 < i \leq n$ holds $(P \cdot A \cdot Q)_{i,1} = 0_K$, and
(v) for every j such that $1 < j \leq n$ holds $(P \cdot A \cdot Q)_{1,j} = 0_K$.

4. A Transformation of Matrix to Some Canonical Form

We now state the proposition

(42) Let D be a non empty set, m, n, i, j be elements of $\mathbb{N}$, and A be a matrix over D of dimension $m \times n$. Then $\mathrm{Swap}(A, i, j)$ is a matrix over D of dimension $m \times n$.

Let us consider K, let n be an element of $\mathbb{N}$, and let i_0 be a natural number. The functor $\mathrm{SwapDiagonal}(K, n, i_0)$ yields a square matrix over K of dimension n and is defined as follows:

(Def. 3) $\mathrm{SwapDiagonal}(K, n, i_0) = \mathrm{Swap}(I_K^{n \times n}, 1, i_0)$.

Next we state a number of propositions:

(43) Let n be an element of $\mathbb{N}$, i_0 be a natural number, and A be a square matrix over K of dimension n. Suppose $1 \leq i_0 \leq n$ and $A = \mathrm{SwapDiagonal}(K, n, i_0)$. Let i, j be natural numbers. Suppose $1 \leq i \leq n$ and $1 \leq j \leq n$. Suppose $i_0 \neq 1$. Then
(i) if $i = 1$ and $j = i_0$, then $A_{i,j} = 1_K$,
(ii) if $i = i_0$ and $j = 1$, then $A_{i,j} = 1_K$,
(iii) if $i = 1$ and $j = 1$, then $A_{i,j} = 0_K$,
(iv) if $i = i_0$ and $j = i_0$, then $A_{i,j} = 0_K$, and
(v) if $i \neq 1$ and $i \neq i_0$ or $j \neq 1$ and $j \neq i_0$, then if $i = j$, then $A_{i,j} = 1_K$ and if $i \neq j$, then $A_{i,j} = 0_K$.

(44) Let n be an element of $\mathbb{N}$, A be a square matrix over K of dimension n, and i be a natural number. If $1 \leq i \leq n$, then $(\mathrm{SwapDiagonal}(K, n, 1))_{i,i} = 1_K$.

(45) Let n be an element of $\mathbb{N}$, A be a square matrix over K of dimension n, and i, j be natural numbers. If $1 \leq i \leq n$ and $1 \leq j \leq n$, then if $i \neq j$, then $(\mathrm{SwapDiagonal}(K, n, 1))_{i,j} = 0_K$.

(46) Let given K, n, i_0 be elements of $\mathbb{N}$, and A be a square matrix over K of dimension n. Suppose that

(i) $1 \leq i_0$,

(ii) $i_0 \leq n$,

(iii) $i_0 = 1$, and

(iv) for all natural numbers i, j such that $1 \leq i \leq n$ and $1 \leq j \leq n$ holds if $i = j$, then $A_{i,j} = 1_K$ and if $i \neq j$, then $A_{i,j} = 0_K$.

Then $A = \mathrm{SwapDiagonal}(K, n, i_0)$.

(47) Let given K, n, i_0 be elements of $\mathbb{N}$, and A be a square matrix over K of dimension n. Suppose that

(i) $1 \leq i_0$,

(ii) $i_0 \leq n$,

(iii) $i_0 \neq 1$, and

(iv) for all natural numbers i, j such that $1 \leq i \leq n$ and $1 \leq j \leq n$ holds if $i = 1$ and $j = i_0$, then $A_{i,j} = 1_K$ and if $i = i_0$ and $j = 1$, then $A_{i,j} = 1_K$ and if $i = 1$ and $j = 1$, then $A_{i,j} = 0_K$ and if $i = i_0$ and $j = i_0$, then $A_{i,j} = 0_K$ and if $i \neq 1$ and $i \neq i_0$ or $j \neq 1$ and $j \neq i_0$, then if $i = j$, then $A_{i,j} = 1_K$ and if $i \neq j$, then $A_{i,j} = 0_K$.

Then $A = \mathrm{SwapDiagonal}(K, n, i_0)$.

(48) Let A be a square matrix over K of dimension n and i_0 be an element of $\mathbb{N}$. Suppose $1 \leq i_0 \leq n$. Then

(i) for every j such that $1 \leq j \leq n$ holds $(\mathrm{SwapDiagonal}(K, n, i_0) \cdot A)_{i_0,j} = A_{1,j}$ and $(\mathrm{SwapDiagonal}(K, n, i_0) \cdot A)_{1,j} = A_{i_0,j}$, and

(ii) for all i, j such that $i \neq 1$ and $i \neq i_0$ and $1 \leq i \leq n$ and $1 \leq j \leq n$ holds $(\mathrm{SwapDiagonal}(K, n, i_0) \cdot A)_{i,j} = A_{i,j}$.

(49) For every element i_0 of $\mathbb{N}$ such that $1 \leq i_0 \leq n$ holds $\mathrm{SwapDiagonal}(K, n, i_0)$ is invertible and $(\mathrm{SwapDiagonal}(K, n, i_0))^{\smile} = \mathrm{SwapDiagonal}(K, n, i_0)$.

(50) For every element i_0 of $\mathbb{N}$ such that $1 \leq i_0 \leq n$ holds $(\mathrm{SwapDiagonal}(K, n, i_0))^{\mathrm{T}} = \mathrm{SwapDiagonal}(K, n, i_0)$.

(51) Let A be a square matrix over K of dimension n and j_0 be an element of $\mathbb{N}$. Suppose $1 \leq j_0 \leq n$. Then

(i) for every i such that $1 \leq i \leq n$ holds $(A \cdot \mathrm{SwapDiagonal}(K, n, j_0))_{i,j_0} = A_{i,1}$ and $(A \cdot \mathrm{SwapDiagonal}(K, n, j_0))_{i,1} = A_{i,j_0}$, and

(ii) for all i, j such that $j \neq 1$ and $j \neq j_0$ and $1 \leq i \leq n$ and $1 \leq j \leq n$ holds $(A \cdot \mathrm{SwapDiagonal}(K, n, j_0))_{i,j} = A_{i,j}$.

(52) Let A be a square matrix over K of dimension n. Then $A = 0_K^{n \times n}$ if and only if for all i, j such that $1 \leq i \leq n$ and $1 \leq j \leq n$ holds $A_{i,j} = 0_K$.

5. Left/Right Invertibility and Invertibility

The following four propositions are true:

(53) Let A be a square matrix over K of dimension n. Suppose $A \neq 0_K^{n\times n}$. Then there exist square matrices B, C over K of dimension n such that

(i) B is invertible,

(ii) C is invertible,

(iii) $(B \cdot A \cdot C)_{1,1} = 1_K$,

(iv) for every i such that $1 < i \leq n$ holds $(B \cdot A \cdot C)_{i,1} = 0_K$, and

(v) for every j such that $1 < j \leq n$ holds $(B \cdot A \cdot C)_{1,j} = 0_K$.

(54) Let A, B be square matrices over K of dimension n. Suppose $B \cdot A = I_K^{n\times n}$. Then there exists a square matrix B_2 over K of dimension n such that $A \cdot B_2 = I_K^{n\times n}$.

(55) Let A be a square matrix over K of dimension n. Then the following statements are equivalent

(i) there exists a square matrix B_1 over K of dimension n such that $B_1 \cdot A = I_K^{n\times n}$,

(ii) there exists a square matrix B_2 over K of dimension n such that $A \cdot B_2 = I_K^{n\times n}$.

(56) For all square matrices A, B over K of dimension n such that $A \cdot B = I_K^{n\times n}$ holds A is invertible and B is invertible.

References

[1] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.
[2] Czesław Byliński. Finite sequences and tuples of elements of a non-empty sets. *Formalized Mathematics*, 1(**3**):529–536, 1990.
[3] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.
[4] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.
[5] Shigeru Furuya. *Matrix and Determinant.* Baifuukan (in Japanese), 1957.
[6] Felix R. Gantmacher. *The Theory of Matrices.* AMS Chelsea Publishing, 1959.
[7] Katarzyna Jankowska. Matrices. Abelian group of matrices. *Formalized Mathematics*, 2(**4**):475–480, 1991.
[8] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Formalized Mathematics*, 1(**2**):335–342, 1990.
[9] Takaya Nishiyama and Yasuho Mizuhara. Binary arithmetics. *Formalized Mathematics*, 4(**1**):83–86, 1993.
[10] Andrzej Trybulec. Binary operations applied to functions. *Formalized Mathematics*, 1(**2**):329–334, 1990.
[11] Wojciech A. Trybulec. Binary operations on finite sequences. *Formalized Mathematics*, 1(**5**):979–981, 1990.
[12] Wojciech A. Trybulec. Groups. *Formalized Mathematics*, 1(**5**):821–827, 1990.
[13] Wojciech A. Trybulec. Vectors in real linear space. *Formalized Mathematics*, 1(**2**):291–296, 1990.
[14] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[15] Hiroshi Yamazaki, Yoshinori Fujisawa, and Yatsuka Nakamura. On replace function and swap function for finite sequences. *Formalized Mathematics*, 9(**3**):471–474, 2001.

[16] Xiaopeng Yue, Xiquan Liang, and Zhongpin Sun. Some properties of some special matrices. *Formalized Mathematics*, 13(**4**):541–547, 2005.
[17] Katarzyna Zawadzka. The sum and product of finite sequences of elements of a field. *Formalized Mathematics*, 3(**2**):205–211, 1992.
[18] Katarzyna Zawadzka. The product and the determinant of matrices with entries in a field. *Formalized Mathematics*, 4(**1**):1–8, 1993.

Received April 2, 2008