Finite Math - Fall 2016

Lecture Notes - 10/26/2016

Section 4.5 - Inverse of a Square Matrix

The Identity Matrix.

Example 1. *Find the products*

(a) $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$ *and* $\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

(b) $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 2 & 4 & 6 \\ 3 & 6 & 9 \end{bmatrix}$ *and* $\begin{bmatrix} 2 & 4 & 6 \\ 3 & 6 & 9 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$

Solution.

(a)

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} = \begin{bmatrix} 1+0 & 2+0 \\ 0+3 & 0+4 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1+0 & 0+2 \\ 3+0 & 0+4 \end{bmatrix}$$

(b)

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 2 & 4 & 6 \\ 3 & 6 & 9 \end{bmatrix} = \begin{bmatrix} 2+0 & 4+0 & 6+0 \\ 0+3 & 0+6 & 0+9 \end{bmatrix} = \begin{bmatrix} 2 & 4 & 6 \\ 3 & 6 & 9 \end{bmatrix}$$

$$\begin{bmatrix} 2 & 4 & 6 \\ 3 & 6 & 9 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 2+0+0 & 0+4+0 & 0+0+6 \\ 3+0+0 & 0+6+0 & 0+0+9 \end{bmatrix} = \begin{bmatrix} 2 & 4 & 6 \\ 3 & 6 & 9 \end{bmatrix}$$

Definition 1 (Identity Matrix)**.** *The* $n \times n$ identity matrix *is a matrix, denoted by* I *or* I_n*, which is an* $n \times n$ *matrix with* 1*'s on the primcipal diagonal and* 0*'s everywhere else. For an* $m \times n$ *matrix* M*, we have*

$$I_m M = M = M I_n.$$

From the above example, we have the two forms of the identity matrix

$$I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad I_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Inverse of a Square Matrix. It is only possible to find a multiplicative inverse of a matrix if it is a square matrix. So, we now restrict ourselves to square matrices.

Definition 2 (Inverse Matrix)**.** *If M is a square matrix of size n, and if there is a matrix, denoted M^{-1}, such that*

$$MM^{-1} = M^{-1}M = I_n$$

we call M^{-1} the inverse *of M. If M does not have an inverse, then M is called a* singular matrix*.*

Example 2. *Find the inverse of the matrix*

$$M = \begin{bmatrix} 2 & 3 \\ 1 & 2 \end{bmatrix}.$$

Solution. *Since we're looking for a matrix which satisfies $MX = I_n$, we can use the trick from the previous section and just row reduce $[M|A]$ to the form $[I_n|X]$, then check that $XM = I_n$ as well.*

$$\left[\begin{array}{cc|cc} 2 & 3 & 1 & 0 \\ 1 & 2 & 0 & 1 \end{array}\right] \underset{\sim}{R_1 \leftrightarrow R_2} \left[\begin{array}{cc|cc} 1 & 2 & 0 & 1 \\ 2 & 3 & 1 & 0 \end{array}\right] \underset{\sim}{R_2 - 2R_1 \to R_2} \left[\begin{array}{cc|cc} 1 & 2 & 0 & 1 \\ 0 & -1 & 1 & -2 \end{array}\right] \underset{\sim}{-R_2 \to R_2}$$

$$\left[\begin{array}{cc|cc} 1 & 2 & 0 & 1 \\ 0 & 1 & -1 & 2 \end{array}\right] \underset{\sim}{R_1 - 2R_2 \to R_1} \left[\begin{array}{cc|cc} 1 & 0 & 2 & -3 \\ 0 & 1 & -1 & 2 \end{array}\right]$$

So we should have that $M^{-1} = \begin{bmatrix} 2 & -3 \\ -1 & 2 \end{bmatrix}$. We need to check that $M^{-1}M = I_2$.

$$\begin{bmatrix} 2 & -3 \\ -1 & 2 \end{bmatrix} \begin{bmatrix} 2 & 3 \\ 1 & 2 \end{bmatrix} = \begin{bmatrix} 4-3 & 6-6 \\ -2+2 & -3+4 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I_2.$$

Thus we have that

$$M^{-1} = \begin{bmatrix} 2 & -3 \\ -1 & 2 \end{bmatrix}.$$

Example 3. *Find the inverse of the matrix*

$$N = \begin{bmatrix} 1 & 2 \\ 2 & 4 \end{bmatrix}.$$

Solution.

$$\left[\begin{array}{cc|cc} 1 & 2 & 1 & 0 \\ 2 & 4 & 0 & 1 \end{array}\right] \underset{\sim}{R_2 - 2R_1 \to R_2} \left[\begin{array}{cc|cc} 1 & 2 & 1 & 0 \\ 0 & 0 & -2 & 1 \end{array}\right]$$

Since there is only zeros in the bottom line of the left side, the matrix N does not have an inverse.

Example 4. *Find the inverse of the matrix*

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

Solution.

$$\left[\begin{array}{ccc|ccc} 2 & 2 & 0 & 1 & 0 & 0 \\ 1 & 2 & -3 & 0 & 1 & 0 \\ -2 & -3 & -1 & 0 & 0 & 1 \end{array}\right] \underset{\sim}{R_1 \leftrightarrow R_2} \left[\begin{array}{ccc|ccc} 1 & 2 & -3 & 0 & 1 & 0 \\ 2 & 2 & 0 & 1 & 0 & 0 \\ -2 & -3 & -1 & 0 & 0 & 1 \end{array}\right] \underset{\sim}{R_3+R_2 \leftrightarrow R_3} \left[\begin{array}{ccc|ccc} 1 & 2 & -3 & 0 & 1 & 0 \\ 2 & 2 & 0 & 1 & 0 & 0 \\ 0 & -1 & -1 & 1 & 0 & 1 \end{array}\right]$$

$$\underset{\sim}{R_2-3R_3 \leftrightarrow R_2} \left[\begin{array}{ccc|ccc} 1 & 2 & -3 & 0 & 1 & 0 \\ 0 & 1 & 9 & -2 & -2 & -3 \\ 0 & -1 & -1 & 1 & 0 & 1 \end{array}\right] \underset{\sim}{R_3+R_2 \leftrightarrow R_3} \left[\begin{array}{ccc|ccc} 1 & 2 & -3 & 0 & 1 & 0 \\ 0 & 1 & 9 & -2 & -2 & -3 \\ 0 & 0 & 8 & -1 & -2 & -2 \end{array}\right]$$

$$\underset{\sim}{R_1-2R_2 \leftrightarrow R_1} \left[\begin{array}{ccc|ccc} 1 & 0 & -21 & 4 & 5 & 6 \\ 0 & 1 & 9 & -2 & -2 & -3 \\ 0 & 0 & 8 & -1 & -2 & -2 \end{array}\right] \underset{\sim}{\tfrac{1}{8}R_3 \leftrightarrow R_3} \left[\begin{array}{ccc|ccc} 1 & 0 & -21 & 4 & 5 & 6 \\ 0 & 1 & 9 & -2 & -2 & -3 \\ 0 & 0 & 1 & -\frac{1}{8} & -\frac{1}{4} & -\frac{1}{4} \end{array}\right]$$

$$\underset{\sim}{R_1+21R_3 \leftrightarrow R_3} \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & \frac{11}{8} & -\frac{1}{4} & \frac{3}{4} \\ 0 & 1 & 9 & -2 & -2 & -3 \\ 0 & 0 & 1 & -\frac{1}{8} & -\frac{1}{4} & -\frac{1}{4} \end{array}\right] \underset{\sim}{R_1+21R_3 \leftrightarrow R_3} \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & \frac{11}{8} & -\frac{1}{4} & \frac{3}{4} \\ 0 & 1 & 1 & -\frac{7}{8} & \frac{1}{4} & -\frac{3}{4} \\ 0 & 0 & 1 & -\frac{1}{8} & -\frac{1}{4} & -\frac{1}{4} \end{array}\right]$$

Theorem 1. *To find the inverse of an $n \times n$ matrix M, one begins with the augmented matrix $[M|\, I_n]$ and uses row operations to transform it into $\left[I_n|\, M^{-1}\right]$. However, if one or more rows of all 0's appear on the left side of the augmented matrix, M is not invertible, i.e., M^{-1} does not exist.*

Example 5. *Find the inverse of the following matrices (if possible):*

(a)

$$M = \begin{bmatrix} 2 & -6 \\ 1 & -2 \end{bmatrix}$$

(b)

$$P = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 1 & 1 \\ 2 & 3 & 2 \end{bmatrix}$$

(c)

$$N = \begin{bmatrix} 3 & 1 \\ 6 & 2 \end{bmatrix}$$

Remark 1. *There is a trick to invert a* 2×2 *matrix. If* $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, *then*

$$M^{-1} = \frac{1}{ad - bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.$$

Cryptography.

Suppose we represent letters by numbers as follows

Blank	0	I	9	R	18
A	1	J	10	S	19
B	2	K	11	T	20
C	3	L	12	U	21
D	4	M	13	V	22
E	5	N	14	W	23
F	6	O	15	X	24
G	7	P	16	Y	25
H	8	Q	17	Z	26

Then, for example, the message "SECRET CODE" would correspond to the sequence

19 5 3 18 5 20 0 3 15 4 5

The goal of Cryptography is to encode messages in a different sequence which can only be translated back to the message using a decoder.

Definition 3 (Encoding matrix/Decoding matrix)**.** *Any matrix with positive integer elements whose inverse exists can be used as an* encoding matrix*. The inverse of an encoding matrix is a* decoding matrix*.*

To encode a message, we must first decide on a encoding matrix A. If A is a $n \times n$ matrix, then we create another matrix $n \times p$ matrix B by entering the message going down columns and taking as many columns as necessary to fit the whole message. Note that the number of rows of B MUST MATCH the size of A. If there are extra entries in B after fitting the whole message, just fill them with 0's.

Example 6. *Encode the message "SECRET CODE" using the encoding matrix*

$$A = \begin{bmatrix} 2 & 3 \\ 1 & 1 \end{bmatrix}.$$

Solution. *We first make the matrix* B

$$B = \begin{bmatrix} 19 & 3 & 5 & 0 & 15 & 5 \\ 5 & 18 & 20 & 3 & 4 & 0 \end{bmatrix}$$

Then to encode the message we find the product

$$\begin{aligned} AB &= \begin{bmatrix} 2 & 3 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 19 & 3 & 5 & 0 & 15 & 5 \\ 5 & 18 & 20 & 3 & 4 & 0 \end{bmatrix} \\ &= \begin{bmatrix} 38+15 & 6+54 & 10+60 & 0+9 & 30+12 & 10+0 \\ 19+5 & 3+18 & 5+20 & 0+3 & 15+4 & 5+0 \end{bmatrix} \\ &= \begin{bmatrix} 53 & 60 & 70 & 9 & 42 & 10 \\ 24 & 21 & 25 & 3 & 19 & 5 \end{bmatrix} \end{aligned}$$

So the coded message is

$$53 \ 24 \ 60 \ 21 \ 70 \ 25 \ 9 \ 3 \ 42 \ 19 \ 10 \ 5$$

Example 7. *A message was encoded with A from the previous example. Decode the sequence*

$$29 \ 12 \ 69 \ 28 \ 70 \ 25 \ 111 \ 43$$

Solution. *First we have to invert the encoding matrix to get the decoding matrix*

$$A^{-1} = \frac{1}{-1} \begin{bmatrix} 1 & -3 \\ -1 & 2 \end{bmatrix}$$

Make a matrix out of the coded message in the same way as above

$$C = \begin{bmatrix} 29 & 69 & 70 & 111 \\ 12 & 28 & 25 & 43 \end{bmatrix}$$

and find the product

$$\begin{aligned} A^{-1}C &= \begin{bmatrix} -1 & 3 \\ 1 & -2 \end{bmatrix} \begin{bmatrix} 29 & 69 & 70 & 111 \\ 12 & 28 & 25 & 43 \end{bmatrix} \\ &= \begin{bmatrix} -29+36 & -69+84 & -70+75 & -111+129 \\ 29-24 & 69-56 & 70-50 & 111-86 \end{bmatrix} \\ &= \begin{bmatrix} 7 & 15 & 5 & 18 \\ 5 & 13 & 20 & 25 \end{bmatrix} \end{aligned}$$

Example 8. *Use the encoding matrix*

$$E = \begin{bmatrix} 1 & 1 & 1 \\ 2 & 1 & 2 \\ 2 & 3 & 1 \end{bmatrix}.$$

(a) *Encode the message "MATH IS FUN" using E.*

(b) *Decode the sequence*

$$39 \ 60 \ 91 \ 65 \ 110 \ 125 \ 6 \ 7 \ 16 \ 44 \ 63 \ 113 \ 37 \ 53 \ 87$$