1.8

The Inverse of a Matrix

In this module we introduce the concept of the matrix inverse. We will see how an inverse can be used to solve certain systems of linear equations, and we will see an application of matrix inverse in cryptography, the study of codes.

We motivate the idea of the inverse of a matrix by looking at the multiplicative inverse of a real number. If number b is the inverse of a, then

$$ab = 1 \text{ and } \ ba = 1$$

For example, $\frac{1}{4}$ is the inverse of 4 and we have

$$4\left(\frac{1}{4}\right) = \left(\frac{1}{4}\right)4 = 1$$

These are the ideas that we extend to matrices.

Definition: Let A be an $n \times n$ matrix. If a matrix B can be found such that $AB = BA = I_n$, then A is said to be **invertible** and B is called the **inverse** of A. If such a matrix B does not exist, then A has no inverse.

Example: Prove that the matrix $A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$ has inverse $B = \begin{bmatrix} -2 & 1 \\ \frac{3}{2} & -\frac{1}{2} \end{bmatrix}$.

Solution: We have that

$$AB = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \begin{bmatrix} -2 & 1 \\ \frac{3}{2} & -\frac{1}{2} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I_2$$

and

$$BA = \begin{bmatrix} -2 & 1 \\ \frac{3}{2} & -\frac{1}{2} \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I_2$$

Thus $AB = BA = I_2$, proving that the matrix A has inverse B.

We know that a real number can have at most one inverse. We now see that this is also the case for a matrix.

Theorem: The inverse of an invertible matrix is unique.

Proof: Let B and C be inverses of A. Thus $AB = BA = I_n$ and $AC = CA = I_n$. Multiply both sides of the equation $AB = I_n$ by C and use the algebraic properties of matrices.

$$C(AB) = CI_n$$

$$(CA)B = C$$

$$I_nB = C$$

$$B = C$$

Thus an invertible matrix has only one inverse.

Notation: Let A be an invertible matrix. We denote its inverse A^{-1}.

Thus $AA^{-1} = A^{-1}A = I_n$

Let $A^{-n} = (A^{-1})^n = \underbrace{A^{-1}A^{-1} \dots A^{-1}}_{n \text{ times}}$

We now derive a method, based on the Gauss-Jordan algorithm, for finding the inverse of a matrix.

Let A be an invertible matrix. Let the columns of A^{-1} be $X_1, X_2, \dots, X_n$, and the columns of I_n be $C_1, C_2, \dots, C_n$. Write A^{-1} and I_n in terms of their columns as follows

$$A^{-1} = [X_1 \quad X_2 \dots X_n] \text{ and } I_n = [C_1 \quad C_2 \dots C_n]$$

We shall find A^{-1} by finding $X_1 \quad X_2 \dots X_n$. Since $AA^{-1} = I_n$, then

$$A[X_1 \quad X_2 \dots X_n] = [C_1 \quad C_2 \dots C_n]$$

Matrix multiplication, carried out in terms of columns, gives

$$[AX_1 \quad AX_2 \dots AX_n] = [C_1 \quad C_2 \dots C_n]$$

leading to

$$AX_1 = C_1, AX_2 = C_2, \dots, AX_n = C_n$$

Thus $X_1 \quad X_2 \dots X_n$ are solutions to the equations $AX = C_1, AX = C_2, \dots, AX = C_n$, all having the same matrix of coefficients A. Solve these systems by using Gauss-Jordan elimination on the large augmented matrix $[A{:}\, C_1 \quad C_2 \dots C_n]$.

$$[A{:}\, C_1 \quad C_2 \dots C_n] \approx \cdots \approx [I_n{:}\, X_1 \quad X_2 \dots X_n]$$

Thus

$$[A{:}\, I_n] \approx \cdots \approx [I_n{:}\, A^{-1}]$$

Therefore, if we compute the reduced echelon form of $[A{:}\, I_n]$ and get a matrix of the form $[I_n{:}\, B]$, then $B = A^{-1}$.

On the other hand, if we compute the reduced echelon form of $[A\colon I_n]$ and find that it is not of the form $[I_n\colon B]$, then A is not invertible.

We now summarize the results of this discussion.

Gauss-Jordan Elimination for Finding the Inverse of a Matrix

Let A be an $n \times n$ matrix.

1. Adjoin the identity $n \times n$ matrix I_n to A to form the matrix $[A\colon I_n]$.
2. Compute the reduced echelon form of $[A\colon I_n]$.
   If the reduced echelon form is of the type $[I_n\colon B]$, then B is the inverse of A.
   If the reduced echelon form is not of the type $[I_n\colon B]$, in that the first $n \times n$ submatrix is not I_n, then A has no inverse.

The Gauss-Jordan method of computing the inverse of a matrix tells us that A is invertible if and only if the reduced echelon form of $[A\colon I_n]$ is $[I_n\colon B]$. As $[A\colon I_n]$ is transformed to $[I_n\colon B]$, A is transformed to I_n. This observation leads to the following result.

Theorem: An $n \times n$ matrix A is invertible if and only if its reduced echelon form is I_n.

If the matrix of coefficients of a system of linear equations is invertible then the inverse can be used to discuss the solutions. The following is a key result in such discussions.

Theorem: Let $AX = B$ be a system of n linear equations in n variables. If A^{-1} exists, the solution is unique and is given by $X = A^{-1}B$.

Proof: We first prove that $X = A^{-1}B$ is solution.

Substitute $X = A^{-1}B$ into the matrix equation. Using the properties of matrices we get

$$AX = A(A^{-1}B) = (AA^{-1})B = I_n B = B$$

$X = A^{-1}B$ satisfies the equation; thus it is a solution.

We now prove the uniqueness of the solution. Let X_1 be solution. Thus $AX_1 = B$. Multiplying both sides of this equation by A^{-1} gives

$$A^{-1}AX_1 = A^{-1}B$$

$$I_n X_1 = A^{-1}B$$

$$X_1 = A^{-1}B$$

Thus there is a unique solution $A^{-1}B$.

We now summarize some of the algebraic properties of matrix inverse.

Properties of Matrix Inverse

Let A and B be invertible matrices and c a nonzero scalar. Then

1. $(A^{-1})^{-1} = A$
2. $(cA)^{-1} = \frac{1}{c}A^{-1}$
3. $(AB)^{-1} = B^{-1}A^{-1}$

4. $(A^n)^{-1} = (A^{-1})^n$
5. $(A^t)^{-1} = (A^{-1})^t$

We verify results 1 and 3 to illustrate the techniques involved, leaving the remaining results for the reader to verify.

$\boldsymbol{(A^{-1})^{-1} = A}$**:** This result follows directly from the definition of inverse of a matrix. Since A^{-1} is the inverse of A, we have

$$AA^{-1} = A^{-1}A = I_n$$

This statement also tells us that A is the inverse of A^{-1}. Thus $(A^{-1})^{-1} = A$.

$\boldsymbol{(AB)^{-1} = B^{-1}A^{-1}}$**:** We want to show that the matrix $B^{-1}A^{-1}$ is the inverse of the matrix AB. We get, using the properties of matrices,

$$\begin{aligned}(AB)(B^{-1}A^{-1}) &= A(BB^{-1})A^{-1} \\ &= AI_nA^{-1} \\ &= AA^{-1} \\ &= I_n\end{aligned}$$

Similarly, it can be shown that $(B^{-1}A^{-1})(AB) = I_n$. Thus $B^{-1}A^{-1}$ is the inverse of the matrix AB.

Example: If $= \begin{bmatrix} 4 & 1 \\ 3 & 1 \end{bmatrix}$, then it can be shown that $A^{-1} = \begin{bmatrix} 1 & -1 \\ -3 & 4 \end{bmatrix}$. Use this information to compute $(A^t)^{-1}$.

Solution: Result 5 above tells us that if we know the inverse of a matrix we also know the inverse of its transpose. We get

$$(A^t)^{-1} = (A^{-1})^t = \begin{bmatrix} 1 & -1 \\ -3 & 4 \end{bmatrix}^t = \begin{bmatrix} 1 & -3 \\ -1 & 4 \end{bmatrix}.$$

Cryptography

Cryptography is the process of coding and decoding messages. The word comes from the Greek *kryptos*, meaning "hidden". The technique can be traced back to the ancient Greeks. Today governments use sophisticated methods of coding and decoding messages. One type of code that is extremely difficult to break makes use of a large matrix to encode a message. The receiver of the message decodes it using the inverse of the matrix. This first matrix is called the **encoding matrix** and its inverse is called the **decoding matrix**. We illustrate the method for a 3 X 3 matrix.

Let the message be

PREPARE TO ATTACK

and the encoding matrix be

$$\begin{bmatrix} -3 & -3 & -4 \\ 0 & 1 & 1 \\ 4 & 3 & 4 \end{bmatrix}$$

We assign a number to each letter of the alphabet. For convenience, let us associate each letter with its position in the alphabet: A is 1, B is 2, and so on. Let a space between words be denoted by the number 27. Thus the message becomes

P	R	E	P	A	R	E	*	T	O	*	A	T	T	A	C	K
16	18	5	16	1	18	5	27	20	15	27	1	20	20	1	3	11

Since we are going to use a 3 X 3 matrix to encode the message, we break the enumerated message up into a sequence of 3 X 1 column matrices as follows.

$$\begin{bmatrix}16\\8\\5\end{bmatrix} \qquad \begin{bmatrix}16\\1\\18\end{bmatrix} \qquad \begin{bmatrix}5\\27\\20\end{bmatrix} \qquad \begin{bmatrix}15\\27\\1\end{bmatrix} \qquad \begin{bmatrix}20\\20\\1\end{bmatrix} \qquad \begin{bmatrix}3\\11\\27\end{bmatrix}$$

Observe that it was necessary to add a space at the end of the message in order to complete the last matrix. We now put the message into code by multiplying each of the above column matrices by the encoding matrix. This step can be conveniently done by writing the column matrices as columns of a matrix and pre-multiplying that matrix by the encoding matrix. We get

$$\begin{bmatrix}-3 & -3 & -4\\0 & 1 & 1\\4 & 3 & 4\end{bmatrix}\begin{bmatrix}16 & 16 & 5 & 15 & 20 & 3\\18 & 1 & 27 & 27 & 20 & 11\\5 & 18 & 20 & 1 & 1 & 27\end{bmatrix}$$

$$= \begin{bmatrix}-122 & -123 & -176 & -130 & -124 & -150\\23 & 19 & 47 & 28 & 21 & 38\\138 & 139 & 181 & 145 & 144 & 153\end{bmatrix}$$

The columns of this matrix give the encoded message. The message is transmitted in the following linear form.

$$-122, 23, 138, -123, 19, 139, -176, 47, 181,$$

$$-130, 28, 145, -124, 21, 144, -150, 38, 153$$

To decode the message, the receiver writes this string as a sequence of 3 X 1 column matrices and repeats the technique using the inverse of the encoding matrix. The inverse of this encoding matrix, the decoding matrix, is

$$\begin{bmatrix} 1 & 0 & 1 \\ 4 & 4 & 3 \\ -4 & -3 & -3 \end{bmatrix}$$

To decode the message, we multiply

$$\begin{bmatrix} 1 & 0 & 1 \\ 4 & 4 & 3 \\ -4 & -3 & -3 \end{bmatrix}\begin{bmatrix} -122 & -123 & -176 & -130 & -124 & -150 \\ 23 & 19 & 47 & 28 & 21 & 38 \\ 138 & 139 & 181 & 145 & 144 & 153 \end{bmatrix}$$

$$= \begin{bmatrix} 16 & 16 & 5 & 15 & 20 & 3 \\ 18 & 1 & 27 & 27 & 20 & 11 \\ 5 & 18 & 20 & 1 & 1 & 27 \end{bmatrix}$$

The columns of the final matrix, written in linear form, give the original message:

16 18 5 16 1 18 5 27 20 15 27 1 20 20 1 3 11

P R E P A R E * T O * A T T A C K

Problem 1: Determine the inverse of the matrix

$$A = \begin{bmatrix} 1 & -1 & -2 \\ 2 & -3 & -5 \\ -1 & 3 & 5 \end{bmatrix}$$

Solution: Applying the method of Gauss-Jordon elimination, we get

$$[A: I_3] = \begin{bmatrix} 1 & -1 & -2 & 1 & 0 & 0 \\ 2 & -3 & -5 & 0 & 1 & 0 \\ -1 & 3 & 5 & 0 & 0 & 1 \end{bmatrix}$$

$$\underset{\substack{R_2 + (-2)R_1 \\ R_3 + R_1}}{\approx} \begin{bmatrix} 1 & -1 & -2 & 1 & 0 & 0 \\ 0 & -1 & -1 & -2 & 1 & 0 \\ 0 & 2 & 3 & 1 & 0 & 1 \end{bmatrix}$$

$$\underset{(-1)R_2}{\approx} \begin{bmatrix} 1 & -1 & -2 & 1 & 0 & 0 \\ 0 & 1 & 1 & 2 & -1 & 0 \\ 0 & 2 & 3 & 1 & 0 & 1 \end{bmatrix}$$

$$\underset{\substack{R_1 + R_2 \\ R_3 + (-2)R_2}}{\approx} \begin{bmatrix} 1 & 0 & -1 & 3 & -1 & 0 \\ 0 & 1 & 1 & 2 & -1 & 0 \\ 0 & 0 & 1 & -3 & 2 & 1 \end{bmatrix}$$

$$\underset{\substack{R_1 + R_3 \\ R_2 + (-1)R_3}}{\approx} \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 5 & -3 & -1 \\ 0 & 0 & 1 & -3 & 2 & 1 \end{bmatrix}$$

Thus

$$A^{-1} = \begin{bmatrix} 0 & 1 & 1 \\ 5 & -3 & -1 \\ -3 & 2 & 1 \end{bmatrix}$$

Problem 2: Determine the inverse of the following matrix, if it exists.

$$A = \begin{bmatrix} 1 & 1 & 5 \\ 1 & 2 & 7 \\ 2 & -1 & 4 \end{bmatrix}$$

Solution: Applying the method of Gauss-Jordon elimination, we get

$$[A: I_3] = \begin{bmatrix} 1 & 1 & 5 & 1 & 0 & 0 \\ 1 & 2 & 7 & 0 & 1 & 0 \\ 2 & -1 & 4 & 0 & 0 & 1 \end{bmatrix}$$

$$\begin{array}{c} \approx \\ R_2 + (-1)R_1 \\ R_3 + (-2)R_1 \end{array} \begin{bmatrix} 1 & 1 & 5 & 1 & 0 & 0 \\ 0 & 1 & 2 & -1 & 1 & 0 \\ 0 & -3 & -6 & -2 & 0 & 1 \end{bmatrix}$$

$$\begin{array}{c} \approx \\ R_1 + (-1)R_2 \\ R_3 + 3R_2 \end{array} \begin{bmatrix} 1 & 0 & 3 & 2 & -1 & 0 \\ 0 & 1 & 2 & -1 & 1 & 0 \\ 0 & 0 & 0 & -5 & 3 & 1 \end{bmatrix}$$

There is no need to proceed further. The reduced echelon form cannot have a one in the (3,3) location. The reduced echelon form cannot be of the form $[I_n : B]$. Thus A^{-1} does not exist.

Problem 3: Solve the system of equations

$$x_1 - x_2 - 2x_3 = 1$$

$$2x_1 - 3x_2 - 5x_3 = 3$$

$$-x_1 + 3x_2 + 5x_3 = -2$$

Solution: This system can be written in the following matrix form:

$$\begin{bmatrix} 1 & -1 & -2 \\ 2 & -3 & -5 \\ -1 & 3 & 5 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 1 \\ 3 \\ -2 \end{bmatrix}$$

If the matrix of coefficients is invertible, the unique solution is

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 1 & -1 & -2 \\ 2 & -3 & -5 \\ -1 & 3 & 5 \end{bmatrix}^{-1} \begin{bmatrix} 1 \\ 3 \\ -2 \end{bmatrix}$$

This inverse has already been found in Problem 1. Using that result we get

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 1 \\ 5 & -3 & -1 \\ -3 & 2 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 3 \\ -2 \end{bmatrix} = \begin{bmatrix} 1 \\ -2 \\ 1 \end{bmatrix}$$

The unique solution is $x_1 = 1, x_2 = -2, x_3 = 1$.

Exercise

1. Determine the inverse of each of the following 3 X 3 matrices, if it exists, using the method of Gauss Jordan elimination.

   a. $\begin{bmatrix} 1 & 2 & 3 \\ 0 & 1 & 2 \\ 4 & 5 & 3 \end{bmatrix}$

   b. $\begin{bmatrix} 1 & 2 & -3 \\ 1 & -2 & 1 \\ 5 & -2 & -3 \end{bmatrix}$

2. Determine the inverse of each of the following 4 X 4 matrices, if it exists, using the method of Gauss Jordan elimination.

   a. $\begin{bmatrix} -3 & -1 & 1 & -2 \\ -1 & 3 & 2 & 1 \\ 1 & 2 & 3 & -1 \\ -2 & 1 & -1 & -3 \end{bmatrix}$

   b. $\begin{bmatrix} -1 & 0 & -1 & -1 \\ -3 & -1 & 0 & -1 \\ 5 & 0 & 4 & 3 \\ 3 & 0 & 3 & 2 \end{bmatrix}$

3. Solve the following systems of three equations in three variables by determining the inverse of the matrix of coefficients and then using matrix multiplication.

   a. $$\begin{aligned} x_1 + 2x_2 - x_3 &= 2 \\ x_1 + x_2 + 2x_3 &= 0 \\ x_1 - x_2 - x_3 &= 1 \end{aligned}$$

b.
$$\begin{aligned} x_1 + 2x_2 + 3x_3 &= 1 \\ 2x_1 + 5x_2 + 3x_3 &= 3 \\ x_1 + 8x_3 &= 15 \end{aligned}$$

c.
$$\begin{aligned} -x_1 + x_2 &= 5 \\ -x_1 + x_3 &= -2 \\ 6x_1 - 2x_2 - 3x_3 &= 1 \end{aligned}$$

4. Prove that $(ABC)^{-1} = C^{-1}B^{-1}A^{-1}$.
5. Prove that if A has no inverse then A^t also has no inverse.
6. Prove that a diagonal matrix is invertible if and only if all its diagonal elements are nonzero. Can you find a quick way for determining the inverse of an invertible diagonal matrix?
7. Encode the message RETREAT using the matrix $\begin{bmatrix} 4 & -3 \\ 3 & -2 \end{bmatrix}$.
8. Decode the message $49, 38, -5, -3, -61, -39$, which was encoded using the matrix $\begin{bmatrix} 4 & -3 \\ 3 & -2 \end{bmatrix}$.

Answers

1.

a. $\begin{bmatrix} \frac{7}{3} & -3 & -\frac{1}{3} \\ -\frac{8}{3} & 3 & \frac{2}{3} \\ \frac{4}{3} & -1 & -\frac{1}{3} \end{bmatrix}$

b. The inverse does not exist

2.

a. $\begin{bmatrix} -\frac{1}{5} & -\frac{1}{5} & \frac{1}{5} & 0 \\ -\frac{1}{5} & \frac{1}{5} & 0 & \frac{1}{5} \\ \frac{1}{5} & 0 & \frac{1}{5} & -\frac{1}{5} \\ 0 & \frac{1}{5} & -\frac{1}{5} & -\frac{1}{5} \end{bmatrix}$

b. $\begin{bmatrix} 1 & 0 & 1 & -1 \\ 0 & -1 & -3 & 4 \\ 1 & 0 & -1 & 2 \\ -3 & 0 & 0 & -1 \end{bmatrix}$

3.

a. $\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} \frac{1}{9} & \frac{3}{9} & \frac{5}{9} \\ \frac{3}{9} & 0 & -\frac{3}{9} \\ -\frac{2}{9} & \frac{3}{9} & -\frac{1}{9} \end{bmatrix} \begin{bmatrix} 2 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} \frac{7}{9} \\ \frac{3}{9} \\ -\frac{5}{9} \end{bmatrix}$

b. $\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} -40 & 16 & 9 \\ 13 & -5 & -3 \\ 5 & -2 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ 3 \\ 15 \end{bmatrix} = \begin{bmatrix} 143 \\ -47 \\ -16 \end{bmatrix}$

c. $\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 2 & 3 & 1 \\ 3 & 3 & 1 \\ 2 & 4 & 1 \end{bmatrix} \begin{bmatrix} 5 \\ -2 \\ 1 \end{bmatrix} = \begin{bmatrix} 5 \\ 10 \\ 3 \end{bmatrix}$

7. $57, 44, 26, 24, 17, 13, -1, 6$

8. PEACE