Lecture 3s

Invertible Matrices

(pages 165-166)

Back in section 3.1, we defined matrix multiplication. At the time, I noted that we would not be able to define division of matrices. Well, while that is true in general, there are some matrices that we can "divide" by. To see this, let's think about what it means to divide by a number. There are many ways to look at division, but for matrices we want to look at the idea of a multiplicative inverse.

Definition: Let A be an $n \times n$ matrix. If there exists an $n \times n$ matrix B such that $AB = I = BA$, then A is said to be **invertible**, and B is called the **inverse** of A (and A is the inverse of B). The inverse of A is denoted A^{-1}.

If this definition seems a bit abstract, think of it in terms of real numbers first.

Example: $\frac{1}{3}$ is the inverse of 3, since $(3)\left(\frac{1}{3}\right) = 1 = \left(\frac{1}{3}\right)(3)$.

The way that inverses relate to division is that when you say "$a \div b$", you are saying the same thing as "$a \times b^{-1}$". But there are two restrictions to note in our definition of a matrix inverse. The first, is that it only applies to square matrices, so this already rules out a general definition of matrix division. But even in the restricted case of $n \times n$ matrices, our definition states "if there exists...". This is, of course, because some $n \times n$ matrices do not have an inverse.

Example: $B = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -3 & 0 & 1 \end{bmatrix}$ is the inverse of $A = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 3 & 0 & 1 \end{bmatrix}$, because

$$AB = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 3 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -3 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \text{ and}$$

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

Example: The matrix $\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$ does not have an inverse. To see this, suppose by way of contradiction that $\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$ does have an inverse $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$. Then

$$\begin{aligned}
&\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \\
\Rightarrow \quad &\begin{bmatrix} a+c & b+d \\ a+c & b+d \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \\
\Rightarrow \quad & a+c=1, a+c=0, b+d=0, b+d=1
\end{aligned}$$

But $a+c=1$ and $a+c=0$ is a contradiction (as is $b+d=0$ and $b+d=1$), so we see that $\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$ is not an invertible matrix.

We will soon explore how to determine if a matrix has an inverse, and how to find the inverse if it does. But we will finish this lecture by looking at some of the theoretical properties of an inverse.

The first is to note that we have been referring to "the" inverse of A. The fact that a matrix has only one inverse is proved in the following theorem:

<u>Theorem 3.5.1</u>: Let A be a square matrix and suppose that $BA = AB = I$ and $CA = AC = I$. Then $B = C$.

<u>Proof of Theorem 3.5.1</u>: We have $B = BI = B(AC) = (BA)C = IC = C$.

This, by the way, is a classic example of showing that something is "unique." Want to show that there is only one of something? Assume there are two, and show that they are equal!

Our definition of the inverse says that we need $AB = I$ *and* $BA = I$. Because matrix multiplication is not commutative, it is important to list both of these conditions. Except, as it turns out, it wasn't that important after all...

<u>Theorem 3.5.2</u>: Suppose that A and B are $n \times n$ matrices such that $AB = I$. Then $BA = I$, so that $B = A^{-1}$. Moreover, B and A have rank n.

<u>Proof of Theorem 3.5.2</u>: To show that $BA = I$, we will use the fact that if $(BA)\vec{y} = I\vec{y}$ for all $\vec{y} \in \mathbb{R}^n$, then $BA = I$. But, as $I\vec{y} = \vec{y}$, we will in fact aim to show that $(BA)\vec{y} = \vec{y}$ for all $\vec{y} \in \mathbb{R}^n$. The first step in this process will be to start at the ending–that is, to show that B has rank n.

We will prove this by contradiction, so let us assume that B does NOT have rank n. Then the homogeneous system $B\vec{x} = \vec{0}$ has a non-trivial solution. This means that there is some non-zero vector $\vec{y}$ such that $B\vec{y} = \vec{0}$. But this means that $\vec{y} = I\vec{y} = (AB)\vec{y} = A(B\vec{y}) = A\vec{0} = \vec{0}$, which is a contradiction, and so we have shown that B has rank n.

Since B has rank n, we know that the system of equations $B\vec{x} = \vec{y}$ is consistent for all $\vec{y} \in \mathbb{R}^n$. This means that for any $\vec{y} \in \mathbb{R}^n$, there is some $\vec{z} \in \mathbb{R}^n$ such that $B\vec{z} = \vec{y}$. And so, for every $\vec{y} \in \mathbb{R}^n$, we have

$$(BA)\vec{y} = (BA)(B\vec{z}) = B((AB)\vec{z}) = B(I\vec{z}) = B\vec{z} = \vec{y}$$

And so we have shown that $(BA)\vec{y} = \vec{y}$ for all $\vec{y} \in \mathbb{R}^n$, and thus that $BA = I$. And now that we have $BA = I$, we can prove that A has rank n using the same argument that we used to show that B has rank n.

Note: We also get that if $BA = I$, then $AB = I$ and thus that $B = A^{-1}$, by simply reversing the roles of A and B in Theorem 3.5.2, and using the fact that if $A = B^{-1}$, then $B = A^{-1}$.

And now for our "useful properties" theorem...

Theorem 3.5.3: Suppose that A and B are invertible matrices and that t is a non-zero real number.

(a) $(tA)^{-1} = \frac{1}{t}A^{-1}$
(b) $(AB)^{-1} = B^{-1}A^{-1}$
(c) $(A^T)^{-1} = (A^{-1})^T$.

Proof of Theorem 3.5.3: These proof will make use of Theorem 3.5.2, which has the effect of saying that to show that $C = A^{-1}$, we need only show that $AC = I$. These proofs also make use of a variety of previous "useful property" theorems.

(a): $(tA)(\frac{1}{t}A^{-1}) = (\frac{1}{t})(tAA^{-1}) = \frac{t}{t}I = I$
(b): $(AB)(B^{-1}A^{-1}) = A(BB^{-1})A^{-1} = AIA^{-1} = AA^{-1} = I$
(c): $(A)^T(A^{-1})^T = (A^{-1}A)^T = I^T = I$ (uses fact that $(AB)^T = B^TA^T$)

There's just one last thing before we move on to finding inverses, and that involves considering the notion of an inverse for a matrix that is not square. So, suppose that A is an $n \times m$ matrix. Then there could be an $m \times n$ matrix such that $AB = I$ and $BA = I$, but you wouldn't have $AB = BA$, since AB is an $n \times n$ matrix and BA is an $m \times m$ matrix. And so, we break the idea of an inverse into a **left inverse** (an $m \times n$ matrix B such that $BA = I$) and a **right inverse** (an $m \times n$ matrix C such that $AC = I$). Theorem 3.5.2 explains why it isn't necessary to bother with such a distinction for square matrices, but if $m \neq n$ all sorts of crazy things can happen. You can have a left inverse but not right inverse. You can have a right inverse but no left inverse. You can even have multiple left inverses or right inverses.

Example: $\begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \end{bmatrix}$ is a right inverse for $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$, since

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

We also see that $\begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{bmatrix}$ is a right inverse for $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$, since

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

But $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$ does not have a left inverse, since for any 3×2 matrix $\begin{bmatrix} a & b \\ c & d \\ e & f \end{bmatrix}$, we have

$$\begin{bmatrix} a & b \\ c & d \\ e & f \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} a & b & 0 \\ c & d & 0 \\ e & f & 0 \end{bmatrix}$$

and $\begin{bmatrix} a & b & 0 \\ c & d & 0 \\ e & f & 0 \end{bmatrix}$ cannot be the identity matrix, since its last column is all zeros.

It turns out that only square matrices can have both a left and a right inverse, and so from this point on we will only concern ourselves with the inverses of square matrices.