MAT 260 LINEAR ALGEBRA
LECTURE 18

WING HONG TONY WONG

1.4 — Algebraic properties of matrix operations

Assuming that the sizes of the matrices are such that the indicated operations can be performed, we have the following properties in matrix arithmetic.
1. $A+B=B+A$ (commutative law for addition)
2. $A+(B+C)=(A+B)+C$ (associative law for addition)
3. $A(BC)=(AB)C$ (associative law for multiplication)
4. $k(AB)=(kA)B$ (associative law for scalar multiplication)
5. $k(\ell A)=(k\ell)A$ (associative law for scalar multiplication)
6. $A(B+C)=AB+AC$ (left distributive law for multiplication)
7. $(A+B)C=AC+BC$ (right distributive law for multiplication)
8. $k(A+B)=kA+kB$ (distributive law for scalar multiplication and matrix addition)
9. $(k+\ell)A=kA+\ell A$ (distributive law for scalar multiplication and scalar addition)

The zero matrix, i.e. a matrix with all the entries 0, is often denoted by O. It is the additive identity for matrix addition. By that, we mean
$$A+O=A \quad \text{and} \quad O+A=A$$
for all A such that A and O are of the same size. Note that $0A=O$ (0 is a scalar) since scalar multiplication is entry-wise. In fact, if $kA=O$, then either $k=0$ or $A=O$.

Warning: If $AB=O$, it does not mean that $A=O$ or $B=O$. (Recall the example from last lecture.) As a result, the cancellation law does not work, i.e. $AB=AC$ and $A\neq O$ may not imply that $B=C$, since $A(B-C)=O$ and $A\neq O$ does not imply that $B-C=O$.

The square matrices
$$(1),\ \begin{pmatrix}1&0\\0&1\end{pmatrix},\ \begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix},\ \begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix},\ \ldots$$
are multiplicative identities for matrix multiplication, denoted by I_n and are called the **identity matrix** of order n. This means that for all matrix A of dimensions $r\times c$,
$$AI_c=I_rA=A.$$

Theorem 1. *If A is a square matrix of order n, then the reduced row echelon form of A is either I_n or has a zero row.*

Given a square matrix A of order n, B is the **multiplicative inverse** of A if

Date: Monday, February 29, 2016.

$$AB = BA = I_n.$$

This is an analogue of how we deal with real numbers. 1 is the multiplicative identity among real numbers, and a multiplicative inverse of a nonzero number k is $\frac{1}{k}$ since $k \cdot \frac{1}{k} = \frac{1}{k} \cdot k = 1$.

Theorem 2. *If B is a multiplicative inverse of A, then it is unique.*

Proof. Assume that we have another matrix C such that $AC = CA = I_n$, then

$$B = BI_n = B(AC) = (BA)C = I_nC = C.$$

□

By uniqueness, we can safely write that $B = A^{-1}$ if B is a multiplicative inverse of A.

Let A be a square matrix of order n. If A has a multiplicative inverse, then A is called **invertible** or **nonsingular**; otherwise, A is called **singular**. Note that if A is invertible, then A^{-1} is also invertible, and the inverse of A^{-1} is A. Hence, A and A^{-1} are inverses of each other.

If A is a square matrix with a zero row, then it is always singular. This is because AB also has a zero row in the same position for all matrices B of the same size. Similarly, if A is a square matrix with a zero column, then it is singular.

Recall that when we have a system of linear equations, it can be written as the matrix equation

$$A \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}.$$

If A is an invertible square matrix, then

$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = A^{-1} \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}.$$

In general, we would always like to detect which square matrix is invertible or not.

Theorem 3. *The matrix*

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

is invertible if and only if $ad - bc \neq 0$. Furthermore, if A is invertible, then

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

Theorem 4. *If both A and B are invertible matrices of order n, then the matrix AB is also invertible, and $(AB)^{-1} = B^{-1}A^{-1}$.*

Question. How about $(ABC)^{-1}$?

Warning: $A + B$ may not be invertible even if A and B are invertible matrices of order n.

If A is a square matrix of order n, then we define $A^0 = I_n$, and $A^s = A \cdot A \cdot \cdots \cdot A$ (s copies). Moreover, if A is invertible, by Theorem **??**, we have $(A^2)^{-1} = (A^{-1})^2$. Hence, we can define $A^{-s} = A^{-1} \cdot A^{-1} \cdot \cdots \cdot A^{-1}$ (s copies). We also have the index law $A^sA^t = A^{s+t}$ and $(A^s)^t = A^{st}$. Finally, $(kA)^{-1} = k^{-1}A^{-1}$ if $k \neq 0$.

With all these exponents of A defined, we can have a **matrix polynomial** in A. For example, if $p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_sx^s$ is an s degree polynomial in x, then $p(A) = a_0I_n + a_1A + a_2A^2 + \cdots + a_sA^s$. Since we are only dealing with exponents of A, we have $p_1(A)p_2(A) = p_2(A)p_1(A)$, where $p_1(x)$ and $p_2(x)$ are polynomials in x.

However, be very careful when we deal with polynomials involving two or more matrices. For instance, $(A + B)^2 \neq A^2 + 2AB + B^2$ in general. Rather, it is $A^2 + AB + BA + B^2$.

Theorem 5. *If A is an invertible matrix, then $(A^{-1})^\top = (A^\top)^{-1}$.*