Exponential of a sum of matrices

I'm going to do this a little differently than I did in class. It brings out the role of commutativity more clearly.

Theorem 0.1. *Let $A, B \in M_{n\times n}(\mathbf{C})$ be commuting (real or) complex matrices. Then $e^{A+B} = e^A e^B$.*

Proof. I begin by observing that $Be^A = \sum_{j=0}^{\infty} \frac{BA^j}{j!} = \sum_{j=0}^{\infty} \frac{A^j B}{j!} = e^A B$.

Let $\mathbf{v} \in \mathbf{C}^n$ be any vector and define $\mathbf{y}(t) = e^{(A+B)t}\mathbf{v}$, $\mathbf{z}(t) = e^{At}e^{B}t\mathbf{v}$. Then $\mathbf{y}(0) = \mathbf{z}(0) = \mathbf{v}$ and $\mathbf{y}'(t) = (A+B)e^{(A+B)t}\mathbf{v} = (A+B)\mathbf{y}(t)$. From the product rule and my initial observation, I further find

$$\mathbf{z}'(t) = Ae^{At}e^{Bt}\mathbf{v} + e^{At}Be^{Bt}\mathbf{v} = Ae^{At}e^{Bt}\mathbf{v} + Be^{At}e^{Bt}\mathbf{v} = (A+B)\mathbf{z}(t).$$

Hence $\mathbf{y}$ and $\mathbf{z}$ solve exactly the same initial value problem. By uniqueness of solutions, I conclude $\mathbf{y}(t) = \mathbf{z}(t)$ for all $t \in \mathbf{R}$. Taking $t = 1$ concludes the proof. □

Now here's a point I didn't make in class. The above theorem allows to give elementary instances of subspaces of $n \times n$ matrices that exponentiate to (multiplicative) subgroups.

Corollary 0.2. *Suppose that $H \subset M_{n\times n}(\mathbf{C})$ is a subspace consisting entirely of matrices that commute with each other. Then*

$$e^H := \{e^A : A \in H\}$$

is an abelian subgroup of the (multiplicative) group $GL(n, \mathbf{C})$ of invertible $n \times n$ matrices. That is,

- *any $M \in e^H$ is invertible with $M^{-1} \in e^H$;*
- *given $M_1, M_2 \in e^H$, we also have $M_1 M_2 = M_2 M_1 \in e^H$.*

Proof. Given $A \in H$, I note that $-A \in H$ always commutes with A. Hence $e^A e^{-A} = e^{A-A} = e^0 = I$. Hence e^A is invertible with inverse in $e^{-A} \in e^H$.

Given $A_1, A_2 \in H$, I have $A_1 + A_2 \in H$. Since A_1 and A_2 commute by hypothesis, I also have $e^{A_1}e^{A_2} = e^{A_1+A_2} \in e^H$. □

Given any fixed $n \times n$ matrix A, the subspace H spanned by $I, A, A^2, \dots$ the non-negative powers of A satisfies the hypothesis of this theorem. Indeed, elements of H all have the form $p(A)$ for some polynomila $p(x)$, and I observed last term that for any two polynomials p and q, we have $p(A)q(A) = (pq)(A) = (qp)(A) = q(A)p(A)$. So any two elements of H commute. The Cayley-Hamilton theorem says $p(A) = 0$ when p is the characteristic polynomial of p, which implies that $\dim H$ cannot exceed $n = \deg p$ even though the full vector space of $n \times n$ matrices has dimension n^2. As it turns out, *no* subspace of $M_{n\times n}$ that consists of mutually commuting matrices can have dimension larger that n.

A further interesting problem is to determine which subspaces of $M_{n\times n}$ exponentiate to "reasonable" (and possibly non-abelian) subgroups. It turns out that the most important condition here is that for all $A, B \in H$ one has $AB - BA \in H$—i.e. H is closed with respect to commutators. This is the beginning of the story of the correspondence between Lie groups and Lie algebras.