MATH 437: Homework V.
Due in class on Wednesday, March 3

1. **[Spectrum of a matrix.]**
Let $\mathbb{A} \in Mat_n(k)$ where k is an algebraically closed field. Let $p_{\mathbb{A}}^{char}(\lambda) = det(\lambda\mathbb{I} - \mathbb{A})$ be the characteristic polynomial of $\mathbb{A}$. This is a monic polynomial of degree n and since k is algebraically closed, it factors as $p_{\mathbb{A}}^{char}(\lambda) = \prod_{i=1}^{s}(\lambda - \lambda_i)^{m_i}$ where $\lambda_i \neq \lambda_j$ when $i \neq j$ and the m_i are positive integers. The λ_i are called the **eigenvalues** of $\mathbb{A}$ and the set $\{\lambda_i | 1 \leq i \leq s\}$ of eigenvalues is called the **spectrum** of $\mathbb{A}$, denoted $Spectrum(\mathbb{A})$. Recall that similar matrices have the same characteristic polynomial and hence they have the same spectrum.
(a) Let $f \in k[x]$ be a polynomial and consider the matrix $f(\mathbb{A})$. Show that if $Spectrum(\mathbb{A}) = \{\lambda_i | 1 \leq i \leq s\}$ then $Spectrum(f(\mathbb{A})) = \{f(\lambda_i) | 1 \leq i \leq s\}$. In fact show that if $p_{\mathbb{A}}^{char}(\lambda) = \prod_{i=1}^{s}(\lambda - \lambda_i)^{m_i}$ then
$p_{f(\mathbb{A})}^{char}(\lambda) = \prod_{i=1}^{s}(\lambda - f(\lambda_i))^{m_i}$.
(Hint: Prove it for lower (upper) triangular matrices and then use that over k, every matrix is similar to a Jordan form.)
(b) Show that if $f \in k[x]$ and $\mathbb{A} \in Mat_n(k)$ then $f(\mathbb{A})$ is invertible if and only if no eigenvalue of $\mathbb{A}$ is a root of f.
(c) Given $\mathbb{B} \in Mat_n(k)$ which is diagonalizable (whose Jordan form is a diagonal matrix) and a polynomial $f \in k[x]$ with $deg(f) \geq 1$ show that there exists $\mathbb{A} \in Mat_n(k)$ such that $f(\mathbb{A}) = \mathbb{B}$. (Hint: As k is algebraically closed, every positive degree polynomial in $k[x]$ will have a root in k.)

2.**[Traces and exponentials]**
For $\mathbb{A} \in Mat_n(k)$ we define the trace of $\mathbb{A}$, denoted $Tr(\mathbb{A}) \in k$ as the sum of the main diagonal entries of $\mathbb{A}$.
(a) Using the definition of matrix multiplication show that $Tr(\mathbb{AB}) = Tr(\mathbb{BA})$ for all matrices $\mathbb{A}, \mathbb{B} \in Mat_n(k)$. Use this to show that similar matrices have the same trace.
(b) If k is algebraically closed, and $p_{\mathbb{A}}^{char}(\lambda) = \prod_{i=1}^{n}(\lambda - \lambda_i)$ then show that $Tr(\mathbb{A}) = \sum_{i=1}^{n} \lambda_i$. (Hint: It might be easier to use Jordan form and (a) than an explicit determinant computation.)
(c) Let $\mathbb{C}$ be the field of complex numbers and $p_n(x) = \sum_{k=0}^{n} \frac{x^k}{k!} \in \mathbb{C}[x]$ be the nth taylor polynomial of e^x. One can show that for any $\mathbb{A} \in Mat_m(\mathbb{C})$, the matrices $p_n(\mathbb{A})$ converge entrywise to a matrix in $Mat_m(\mathbb{C})$ as $n \to \infty$. This matrix is denoted $e^{\mathbb{A}}$. Informally we say $e^{\mathbb{A}} = \sum_{k=0}^{\infty} \frac{\mathbb{A}^k}{k!}$.

Show that if $\mathbb{B} = \mathbb{S}\mathbb{A}\mathbb{S}^{-1}$ then $e^{\mathbb{B}} = \mathbb{S}e^{\mathbb{A}}\mathbb{S}^{-1}$ and use this to prove

$$det(e^{\mathbb{A}}) = e^{Tr(\mathbb{A})}$$

for a general matrix $\mathbb{A} \in Mat_m(\mathbb{C})$.
(d) If $\mathbb{A}$ and $\mathbb{B}$ commute in $Mat_m(\mathbb{C})$, show that $e^{\mathbb{A}+\mathbb{B}} = e^{\mathbb{A}}e^{\mathbb{B}}$. (This is not true when $\mathbb{A}$ and $\mathbb{B}$ don't commute!!) Use this to show that $e^{\mathbb{A}}$ has inverse $e^{-\mathbb{A}}$ and in particular lies in $GL_m(\mathbb{C})$. Thus exponentiation defines a function from the vector space $Mat_m(\mathbb{C})$ to the group $GL_m(\mathbb{C})$. Because of this association, sometimes $Mat_m(\mathbb{C})$ is denoted as $\mathfrak{gl}_m(\mathbb{C})$.
(e) Given $\mathbb{A} \in Mat_m(\mathbb{C})$ we define $\mathbb{A}^*$ as the transpose conjugate of $\mathbb{A}$. (complex conjugate the entries of $\mathbb{A}$ and then transpose the matrix.) $\mathbb{A}$ is said to be **Hermitian** if $\mathbb{A}^* = \mathbb{A}$, it is said to be **skew Hermitian** if $\mathbb{A}^* = -\mathbb{A}$ and it is said to be **unitary** if $\mathbb{A}^*\mathbb{A} = \mathbb{I} = \mathbb{A}\mathbb{A}^*$. The unitary matrices are easily checked to form a group under matrix multiplication which is denoted U_m.
Let $\mathfrak{sl}_m(\mathbb{C})$ denote the matrices of trace zero. Show that $\mathfrak{sl}_m(\mathbb{C})$ is a $\mathbb{C}$-vector space and that exponentiation defines a function from $\mathfrak{sl}_m(\mathbb{C})$ to $SL_m(\mathbb{C})$, the special linear group (matrices of determinant one).
Let $\mathfrak{u}_m(\mathbb{C})$ denote the skew-Hermitian matrices. Show that $\mathfrak{u}_m(\mathbb{C})$ is a $\mathbb{R}$-vector space and that exponentiation defines a function from $\mathfrak{u}_m(\mathbb{C})$ to U_m.
(Note: The above examples are special cases of a general exponential map between a "Lie algebra" and its corresponding "Lie group".)

3. **Square roots of $-\mathbb{I}$.**
(a) Find all matrices $\mathbb{A}$ (if any) in $Mat_n(\mathbb{R})$ (up to similarity) which solve the equation $\mathbb{A}^2 = -\mathbb{I}$. State how many solutions there are up to similarity and give explicit representatives. (Your answer might depend on n.)
(b) Find all matrices $\mathbb{A}$ (if any) in $Mat_n(\mathbb{C})$ (up to similarity) which solve the equation $\mathbb{A}^2 = -\mathbb{I}$. State how many solutions there are up to similarity and give explicit representatives. (Your answer might depend on n.)

4. **Elements of order 3 in $GL_n(\mathbb{F}_p)$**
If k is any field and q is a prime number, the set of roots of $x^q - 1$ is easily seen to be a subgroup of $(k^\times, \cdot)$, the multiplicative group of the field. Since there are at most q roots and since every finite subgroup of a multiplicative group of a field is cyclic (proven in class last semester or see Thm 1.9 Lang, Pg 177), it follows that $R = \{x \in k | x^q = 1\}$ is a cyclic subgroup of $(k^\times, \cdot)$ of order dividing q. Thus either $R = \{1\}$ or $R = \{1, \alpha, \alpha^2, \ldots, \alpha^{q-1}\}$ in which

case α is called a **primitive qth root of unity in** k and has order q in $(k^\times, \cdot)$.
(a) Let p and q be primes. Show that the field $\mathbb{F}_p$ has a primitive qth root of unity if and only if $p \equiv 1 \bmod q$.
(Hint: For one direction, it is useful to note that $\mathbb{F}_p^\times$ is cyclic (a corollary to the theorem mentioned above) and so one may write $\mathbb{F}_p^\times = \{1, s, s^2, \ldots, s^{p-2}\}$ where s has order $p-1$ and is called a primitive generator of $\mathbb{F}_p^x$.)
(b) Find a complete factorization of $x^3 - 1$ into irreducibles in $\mathbb{F}_p[x]$. The type of factorization will depend on p and you should clearly state the cases.
(c) Use (b) to find representatives of the conjugacy (similarity) classes of elements of order 3 in $GL_5(\mathbb{F}_p)$. You should find the number of such conjugacy classes and write down representatives for each one in rational canonical form. (It will probably be easier to use elementary divisors over invariant factors, but when using elementary divisors note that uniqueness is only up to permuting the blocks. Also if you need to use a primitive 3rd root of unity, just call it α as finding an explicit representative in $\mathbb{F}_p$ for given p is difficult!) If you have time, try to do the same thing for $GL_n(\mathbb{F}_p)$ for general n.