22M: 121 Final Exam

This is 2 hour exam. Begin each question on a new sheet of paper. All notations are standard and the ones used in class. Please write clearly and provide all details of your work. Good luck.

1 Linear Algebra

Answer any three in this section. Each question is worth 10 points.

1. Let $V$ be a 8-dimensional vector space over a field $F$ and let $T \in \text{End}_F(V)$. Let $k_j$ be the dimension of $\text{Ker}(T - 5)^j$ over $F$. It is known that $k_1 = 4$, $k_2 = 7$, and $k_3 = 8$. Write the rational canonical and the jordan canonical form for $T$.

Since $\text{Ker}(T - 5)^3 = V$, we see that $m_T(x)/(x-5)^3$. This implies that $m_T(x) = (x-5)^3$ since $\text{Ker}(T - 5)^j, j=1,2$, are proper subspaces of $V$. We also conclude that there are 4 jordan blocks corresponding to the eigenvalue 5. Since the invariant factors are divisors of $(x-5)^3$, we have the following two possibilities:

$$V_T \cong F[x]/(x-5) \oplus F[x]/(x-5) \oplus F[x]/(x-5)^3 \oplus F[x]/(x-5)^3 \quad (1)$$

$$V_T \cong F[x]/(x-5) \oplus F[x]/(x-5)^2 \oplus F[x]/(x-5)^2 \oplus F[x]/(x-5)^3 \quad (2)$$

But (1) implies that $\dim \text{Ker}(T - 5)^2 = 6$ which contradicts the hypothesis. Thus the Jordan canonical form is

$$J = J_{5,1} \oplus J_{5,2} \oplus J_{5,2} \oplus J_{5,3}$$

and the rational canonical form is

$$R = C(x-5) \oplus C(x^2 - 10x + 25) \oplus C(x^2 - 10x + 25) \oplus C(x^3 - 15x^2 + 75x - 125)$$

2. Let $V$ be a $n$-dimensional vector space over a field $F$. Suppose $T : V \rightarrow V$ is a cyclic linear transformation, i.e., there exists $v \in V$ such that $\{v, T(v), \ldots, T^{n-1}(v)\}$ is a basis for $V$ over $F$. Let $S : V \rightarrow V$ be a linear transformation that commutes with $T$, i.e., $ST = TS$. Prove that $S$ is a polynomial in $T$, namely, $S = p(T)$ for some polynomial $p(x) \in F[x]$. 

1
The fact that $V$ has a basis as stated above implies that $V_T = F[x]v$ (i.e., it is cyclic $F[x]$-module). Since $ST = TS$, we see that

$$S : V_T \rightarrow V_T$$

is a $F[x]$-linear, i.e., a morphism of $F[x]$-modules. Write $S(v) = a_0 + a_1T(v) + \cdots + a_{n-1}T^{n-1}(v)$ for some $a_i \in F$, $0 \leq i \leq n - 1$. Let

$$p(x) = a_0 + a_1x + a_2x^2 \cdots + a_{n-1}x^{n-1} \in F[x].$$

Then for any $w \in V$, we have $w = f(x) \cdot v$, for some $f(x) \in F[x]$. Hence

$$S(w) = S(f(x) \cdot v) = f(x) \cdot S(v) = f(x)(p(x) \cdot v) = p(x)(f(x) \cdot v) = p(x) \cdot w.$$

Whence $S = p(T)$.

3. Let $A$ be a $n \times n$ with entries in $F$, and let $f(x) \in F[x]$. Assume that the characteristic polynomial of $A$ is of the form $C_A(x) = \prod_i (x - \alpha_i) \in F[x]$. Show that the characteristic polynomial $C_{f(A)}(x)$ of $f(A)$ is given by

$$C_{f(A)}(x) = \prod_i (x - f(\alpha_i)).$$

It is easy to check that $f$ preserves similarity classes, namely, if $A = PBP^{-1}$, then $f(A) = Pf(B)P^{-1}$. Since the characteristic polynomial only depends on the similarity class, we may assume that $A$ is in upper triangular form with diagonal entries $\alpha_1, \alpha_2, \ldots, \alpha_n$. For such a matrix $A$, $f(A)$ is also upper triangular with diagonal entries $f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_n)$, and the conclusion follows.

4. Suppose $A$ is a $n \times n$ invertible matrix over $\mathbb{C}$ and $k \geq 1$ an integer. Show that if $A^k$ is diagonalizable, then so is $A$.

We may replace $A$ by any matrix similar to $A$. So we may assume $A$ is in the Jordan form. We may further assume that $A$ has only one Jordan block, say, $J_{\lambda,n}$. Since $J_{\lambda,n} = \lambda I + N$, where $N$ is upper triangular with all super diagonal entries being 1, in particular, $N$ is nilpotent. Then

$$A^k = (\lambda I + D)^k = \lambda^k I + k\lambda^{k-1}N + \binom{\lambda}{2} N^2 + \cdots + N^k$$

Since $N$ is nilpotent, it follows that $\{I, N, \ldots, N^{k-1}\}$ are linearly independent in $M_{n \times n}(\mathbb{C})$ (prove this!) Therefore $A^k$ is not diagonalizable unless $n = 1$, or in other words, unless $A$ is diagonalizable.
2 Field Theory

Answer the following questions. Each is worth 10 points.

1. Let $L \supset F$ be a field extension. Prove that the extension $L \supset F$ is finite if and only if it is finitely generated and algebraic.

Suppose $L/F$ is algebraic and finitely generated. Then $L = F(\alpha_1, \alpha_2, \ldots, \alpha_k)$ with each $\alpha_i$ algebraic over $F$. Let $n_i$ be the degree of $\alpha_i$ and let $F_i = F(\alpha_1, \alpha_2, \ldots, \alpha_i)$. Then the minimal polynomial of $\alpha_i$ over $F_{i-1}$ divides the minimal polynomial of $\alpha_i$ over $F$. Since $F \subset F_1 \subset F_2 \subset \cdots \subset F_k = L$, we have $[L : F] \leq n_1 n_2 \cdots n_k$.

Conversely, if $[L : F] = n < \infty$, say $\{x_1, x_2, \ldots, x_n\}$ is a $F$-basis of $L$, then clearly $L = F(x_1, x_2, \ldots, x_n)$. Further, for any $\alpha \in L$, the set $\{1, \alpha, \ldots, \alpha^n\}$ is linearly dependent over $F$, i.e., there exists scalars $a_i, 0 \leq i \leq n$, not all zero, such that $a_0 + a_1 \alpha + \cdots + a_n \alpha^n = 0$. Hence $\alpha$ is algebraic over $F$.

2. Let $f(x) \in \mathbb{Q}(x)$ be irreducible with splitting field $K$ over $\mathbb{Q}$. Suppose that the Galois group of $K/\mathbb{Q}$ is abelian. Prove that $K = \mathbb{Q}(\alpha)$ for any root $\alpha$ of $f(x)$.

We know that the splitting field of $f$ is generated by the roots of $f$. Let $\alpha$ be a root of $f$, then $K$ is Galois over $\mathbb{Q}(\alpha)$, and let $H$ be the corresponding Galois group. Then, for $\sigma \in H$, and $\tau \in G(K/\mathbb{Q})$, $\sigma(\tau(\alpha)) = \tau(\sigma(\alpha)) = \tau(\alpha)$, i.e., $\sigma$ fixes $\tau(\alpha)$. Since $K$ is generated by the roots of $f$, it follows that $\sigma$ is the identity map, i.e., $H = \{1\}$. Thus $K = \mathbb{Q}(\alpha)$.

3. Suppose $K$ is a field of characteristic $p$ which is not a perfect field, i.e., $K^p \neq K$. Prove that there exist irreducible inseparable polynomials over $K$. Conclude that there exist inseparable finite extensions of $K$.

Let $a \in K$ such that $a^p \notin K$. Let $p(x) = x^p - a \in K[x]$. Suppose $\beta$ is a root of $K$ in some algebraic closure of $K$. Then $\beta^p = a$, this implies that $p(x) = x^p - \beta^p = (x - \beta)^p$ over $K(\beta)$. Thus $\beta$ is the only root of $p(x)$ with multiplicity $p$. In particular $p(x)$ is inseparable. It remains to see that $p(x)$ is irreducible over $K$. Suppose $g(x) \in K[x]$ is an irreducible factor of $p(x)$ with degree $r < p$. Then, $g(x) = (x - \beta)^r = x^r - r\beta x^{r-1} + \cdots$; since $g(x)$ has coefficients in $K$, this implies that $r \beta \in K$. But, $r \neq 0$ since $r < p$, therefore $\beta \in K$ which is a contradiction. Whence $g(x) = (x - \beta)^p = p(x)$ is irreducible. Let $L = K(\beta)$. Then, for any embedding $\sigma$ of $L$ over $K$, $\sigma(\beta)$ is also a root of $p(x)$, i.e., $\sigma(\beta) = \beta$. Thus any such embedding $\sigma$ is the identity morphism. Thus $[L : K]_s = 1$, or in other words, $L/K$ is purely inseparable.

4. Let $L/F$ be a Galois extension of degree $2p$, where $p$ is an odd prime.

a. Show that there is a unique quadratic subfield $E$, i.e., $F \subset E \subset L$ and $[E : F] = 2$. Let $G$ be the Galois group of $L$ over $F$. Any $p$-Sylow subgroup of $G$ is of index 2, and hence normal in $G$. Thus there exists a unique $p$-Sylow subgroup $H$
of $G$. Let $E$ be the subfield corresponding to $H$ which is the required quadratic subfield.

b. Does there exist a unique subfield $K$ of index 2, i.e., $F \subset K \subset L$ and $[L : K] = 2$? Prove or give a counterexample.

No. Take $L$ to be the splitting field of $x^3 - 2$ over $\mathbb{Q}$. Then $[L : \mathbb{Q}] = 6$. Let $\omega \neq 1$ be a cube root of unity. Then $\mathbb{Q}(\sqrt[3]{2})$ and $\mathbb{Q}(\sqrt[3]{2} \omega)$ are two distinct subfields of $L$ of degree 3 over $\mathbb{Q}$.

5. Determine the Galois group of $x^3 + 3$ over $\mathbb{Q}$. By Eisensteins criterion, the given polynomial is irreducible over $\mathbb{Q}$. Let $\alpha = -\sqrt[3]{3}$, and $\beta = \sqrt{-3}$. Then the splitting field of $x^3 + 3$ is the compositum of $\mathbb{Q}(\alpha)$ (of degree 3 over $\mathbb{Q}$) and $\mathbb{Q}(\beta)$ (a quadratic extension of $\mathbb{Q}$) which is of degree 6. Hence the Galois group of $x^3 + 3$ is $S_3$.

**Answer one of the following two questions. They are worth 15 points each.**

5. Let $f(x) \in \mathbb{Q}(x)$ be an irreducible quartic with Galois group $G$. If $f(x)$ has exactly two real roots, then either $G \simeq S_4$ or $G \simeq D_8$.

The given information reveals that the resolvent cubic $h(x)$ has one real root and two complex roots. Suppose $h(x)$ is irreducible, then its Galois group is isomorphic to $S_3$ (this was a HW problem). In particular the discriminant of $f(x)$ is not a square, and hence its Galois group is not contained in $A_4$ with its order divisible by 6. This implies that the Galois group $G$ of $f(x)$ is isomorphic to $S_4$. Now, if $h(x)$ is reducible, then it splits into a linear and a quadratic. Then $G$ stabilizes one root of $h(x)$ but not the other two. Hence $G$ is isomorphic to a subgroup of $D_8$. This implies that either $G$ is cyclic of order 4, or is isomorphic to $D_8$. But, according to #2, $G$ cannot be abelian. Thus $G \simeq D_8$.

6. Let $K/F$ be any finite extension and let $\alpha \in K$. Let $L$ be a Galois extension of $F$ containing $K$ and let $H \leq G(L/F)$ be the subgroup corresponding to $K$. Define the norm of $\alpha$ from $K$ to $F$ to be

$$N_{K/F}(\alpha) = \prod_{\sigma} \sigma(\alpha),$$

where the product is taken over all the embeddings of $K$ into an algebraic closure of $F$. (This is a product of Galois conjugates of $\alpha$. In particular, if $K/F$ is Galois this is $\prod_{\sigma \in G(K/F)} \sigma(\alpha)$.)

a. Prove that $N_{K/F}(\alpha) \in F$.

Let $\{\sigma_1 = 1, \sigma_2, \ldots, \sigma_n\}$ be the coset representatives of $G/H$, where $G = G(L/F)$. Then their restrictions to $K$ are the distinct embeddings of $K$ into an algebraic closure $\bar{L}$ of $L$. Moreover, for any $\alpha \in K$, $\tau \in G$ permutes the set $\{\sigma_1(\alpha), \sigma_2(\alpha), \ldots, \sigma_n(\alpha)\}$. Hence $\tau$ fixes $N_{K/F}(\alpha)$, and consequently $N_{K/F}(\alpha) \in F$. 

4
b. Prove that $N_{K/F}(\alpha \beta) = N_{K/F}(\alpha)N_{K/F}(\beta)$, so that the norm is a multiplicative map from $K$ to $F$.

This is clear since $\sigma(\alpha \beta) = \sigma(\alpha)\sigma(\beta)$ for any embedding $\sigma$ of $K$ into $\bar{L}$.

c. Let $m_\alpha(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_1x + a_0 \in F[x]$ be the minimal polynomial for $\alpha \in K$ over $F$. Let $n = [K : F]$. Prove that $d$ divides $n$, that there are $d$ distinct Galois conjugates of $\alpha$ which are all repeated $n/d$ times in the product above and conclude that $N_{K/F}(\alpha) = (-1)^{n}a_0^{n/d}$.

Since $F \subset K \subset L$ and $L$ is separable over $F$, we conclude that $K$ is also separable over $F$. Consider the tower $F \subset F(\alpha) \subset K$, from this we see that $d = [F(\alpha) : F]$ divides $n = [K : F]$. Let $\{\tau_1, \tau_2, \ldots, \tau_d\}$ be the distinct $F$-embeddings of $F(\alpha)$ into $\bar{L}$. By separability, each $\tau_i$ extends to $n/d$ distinct embeddings of $K$ into $\bar{L}$, and these give all the embeddings of $K$ into $\bar{L}$. Hence each $\tau_i(\alpha)$ appears $n/d$ times in the product in question. Further, since $\prod_i \tau_i(\alpha) = (-1)^d a_0$, the last conclusion follows.