Characteristic Polynomials and Irreducibility

Problem 1: Let T be a linear operator on a finite dimensional vector space over field F of characteristic p. Suppose the characteristic polynomial of T is $t^2(t-1)^3(t^p-1)$. What are the eigenvalues of T?

Proof. By binomial expansion,

$$(t+1)^p = \sum_{i=0}^{p} \binom{p}{i} t^i$$

But since p is prime,

$$\binom{p}{i} = \frac{p(p-1)!}{(p-i)!i!}$$

Since both terms of the denominator will be less than p, it won't divide prime p, which means $\binom{p}{i}$ is divisible by p when $i \notin \{0, p\}$. Since the characteristic is p, then multiples of p are 0. And thus,

$$(t+1)^p = \binom{p}{0} t^0 + \binom{p}{p} t^p = (t^p + 1)$$

Since the characteristic polynomial of p splits the eigenvalues of T are $\lambda \in \{0, 1, -1\}_F$. Since we do not know if T is diagonalizable, the dimension of each eigenspace is at least 1, and at most the multiplicity of the eigenvalue.

Thus, $\dim E_0 \in [1,2] \cap \mathbb{N}$, $\dim E_1 \in [1,3] \cap \mathbb{N}$, $\dim E_{-1} \in [1,p] \cap \mathbb{N}$. $\square$

Problem 2: For $A \in M_{n\times n}$ define $e^A = \displaystyle\sum_{k=0}^{\infty} \frac{1}{k!}A^k$.

Prove the following:

1. If $AB = BA$, then $e^{A+B} = e^A e^B$.
2. If A is nilpotent, then the characteristic polynomial of e^A is $(-1)^n(t-1)^n$.

Proof.

1. First, we expand $e^A e^B$. Note $AB = BA$ tells us A and B have commutative multiplication.

$$\begin{aligned} e^A e^B &= \left(\sum_{a=0}^{\infty} \frac{1}{a!}A^a\right)\left(\sum_{b=0}^{\infty} \frac{1}{b!}B^b\right) \\ &= \left(\sum_{a=0}^{\infty} \left(\sum_{b=0}^{\infty} \frac{1}{b!}B^b\right) \frac{1}{a!}A^a\right) \\ &= \sum_{a=0}^{\infty}\sum_{b=0}^{\infty} \frac{1}{a!b!}A^aB^b \end{aligned}$$

Now, we expand e^{A+B}

$$\begin{aligned} e^{A+B} &= \sum_{j=0}^{\infty} \frac{1}{j!}(A+B)^j \\ &= \sum_{j=0}^{\infty} \frac{1}{j!}\left(\binom{j}{0}A^j + \binom{j}{1}A^{j-1}B + \ldots + \binom{j}{j}B^j\right) \\ &= \sum_{j=0}^{\infty} \frac{1}{j!}\left(\sum_{k=0}^{j} \binom{j}{k}A^{j-k}B^k\right) \\ &= \sum_{j=0}^{\infty} \left(\sum_{k=0}^{\infty} \binom{j}{k}\frac{1}{j!}A^{j-k}B^k\right) && \text{(since } \tbinom{j}{k} = 0 \text{ for } k > j\text{)} \\ &= \sum_{l=-k}^{\infty} \left(\sum_{k=0}^{\infty} \binom{l+k}{k}\frac{1}{(l+k)!}A^lB^k\right) && \text{(substitute } l = j-k\text{)} \\ &= \sum_{l=0}^{\infty} \left(\sum_{k=0}^{\infty} \frac{(l+k)!}{(l+k-k)!k!}\frac{1}{(l+k)!}A^lB^k\right) && \text{(since } \tbinom{l+k}{k} = 0 \text{ for } k > l+k\text{)} \\ &= \sum_{l=0}^{\infty}\sum_{k=0}^{\infty} \frac{1}{l!k!}A^lB^k && \text{which is equal to our first expansion above.} \end{aligned}$$

Therefore $e^{A+B} = e^A e^B$.

2. Since A is nilpotent, it's only eigenvalue is 0. It thus has a characteristic polynomial of $(-t)^n$. It splits for all F and thus, there exists a basis for A such that A is upper triangular. Thus let $PAP^{-1} = B$ where P is that change of basis matrix. Note that the diagonal of B is 0. First, I will show that e^A and e^B are similar:

$$e^A = e^{P^{-1}BP} = \sum_{k=0}^{\infty} \frac{1}{k!}(P^{-1}BP)^k = P^{-1}\left(\sum_{k=0}^{\infty} \frac{1}{k!}B^k\right) P = P^{-1}e^B P$$

We know that the characteristic polynomial of similar matrices are the same. So,

$$p_{e^A}(t) = \det(e^A - tI) = \det(e^B - tI)$$

But

$$e^B - tI = \sum_{k=0}^{\infty} \left(\frac{1}{k!}B^k\right) - tI = I - tI + \sum_{k=1}^{\infty} \left(\frac{1}{k!}B^k\right)$$

All the above terms are upper-triangular. Thus the resulting matrix is upper triangular. Thus, we can get the determinant by multiplying all the terms in the diagonal. But, since the summand has a 0 diagonal, the diagonal entries are all just $(1 - t)$. Thus, $\det(e^A - tI) = (1 - t)^n = (-1)^n(t - 1)^n$ as wanted. $\square$

Problem 3: Consider a finite-dimensional vector space over field F. Suppose $f(t)$ is the minimal polynomial of linear transformation T. Show that if $g(t) \in F[t]$ be any polynomial such that $g(T) = 0$, then $f(t)|g(t)$.

Proof. Let $g(t)$ and $f(t)$ be defined as per the question. By division algorithm, we have $g(t) = f(t)q(t) + r(t)$ for some $q(t), r(t) \in F[t]$. If we substitute $t = T$:

$$0 = g(T) = f(T)q(T) + r(T) = 0q(T) + r(T) \Rightarrow r(T) = 0$$

But, $f(t)$ is the minimal polynomial and $\deg f(t) > \deg r(t)$. By minimality of $\deg f(t)$, $r(t) = 0$. Thus, $g(t) = f(t)q(t) \Rightarrow f(t)|g(t)$ as wanted. $\square$

Problem 4:

First, show that for any $f(t) \in F[t]$, the kernel of $f(T)$ is T-invariant.

Then, suppose that $f(t)$ is an irreducible factor of the characteristic polynomial $p_T(t)$ of T. Show that either $\ker f(T) = 0$ or $\dim \ker(f(T)) \geq \deg(f(t))$.

Proof.

1. First, lets prove the following lemma: $Tf(T) = f(T)T$.

   Since $f(t)$ is a polynomial, $f(T) = \sum_{i=0}^{\infty} a_i T^i$ for some $a_i \in F$. Also, T commutes with itself since $TT = TT$ so:

   $$Tf(T) = T\left(\sum_{i=0}^{\infty} a_i T^i\right) = \sum_{i=0}^{\infty} a_i T^{i+1} = \left(\sum_{i=0}^{\infty} a_i T^i\right) T = f(T)T$$

   .

   Now, we want to prove $T(\ker f(T)) \subseteq \ker f(T)$. To do that, let $v \in \ker f(T)$ and show $T(v) \in \ker f(T)$. Indeed,

   $$f(T)v = \vec{0} \Rightarrow T(f(T)(v)) = \vec{0} \Rightarrow f(T)(Tv) = \vec{0} \Rightarrow T(v) \in \ker f(T)$$

2. Let $f(t)$ be an irreducible factor of the characteristic polynomial $p_T(t)$ of T.

   If $\ker(f(T)) = 0$, we are done.

   So suppose otherwise and lets prove $\dim \ker(f(T)) \geq \deg(f(t))$.

   Let $\ker(f(T)) = W$. From 4(a), we know that W is T-invariant. If we restrict T to $T_W : W \to W$, where $T_W(w) = T(w)$, then for any $v \in W$,

   $$f(T_W)v = \left(\sum_{i=0}^{\infty} a_i T_W^i\right) v = \left(\sum_{i=0}^{\infty} a_i T^i\right) v = f(T)v = \vec{0}$$

   and so we have $f(T_W) = 0$.

   Now let $g(t)$ be the characteristic polynomial of T_W. Since $\dim W \neq 0$, $\deg g(t) > 0$. And by Problem 3, $g(t)|f(t)$. But $f(t)$ is irreducible.

   Thus, $\deg(f(t)) = \deg(g(t)) \leq \dim W = \dim \ker(f(T))$ as wanted. $\square$

Problem 5:

Let V be an n-dimensional vector space over a field F. Suppose $T : V \to V$ is a linear map such that the characteristic polynomial $p_T(t)$ is irreducible.

Show that the only T-invariant subspaces of V are V and 0, and for some non-zero $v \in V$, $\{v, T(v), ..., T^{n-1}(v)\}$ is a basis of V

Proof.

1. First, let $n \notin \{0, 1\}$ since there will be nothing to prove as the only subspaces of V will be V and 0.

   Now, lets suppose that there is a non-trivial T-invariant subspace W. Let $g(t)$ be the characteristic polynomial of T restricted to W. Now $0 < g(t) < \dim V$ since W is non-trivial. Since W satisfies the characteristic polynomial (as shown in Problem 4.2) and W satisfies $g(t)$ by the Cayley-Hamilton Theorem, $g(t)|f(t)$ as per Problem 3. BUT $f(t)$ is irreducible, and thus we reach a contradiction.

2. If $V = 0$, we are done since $T^0(v) = \vec{0}$ spans V. Thus, suppose $\dim V > 0$.

   Let $\beta = \{v, T(v), ..., T^{n-1}(v)\}$. Since $\dim V = n$ and $|\beta| = n$, we just need to show that β is linearly independent to show that β is a basis for V.

   Let $v \neq 0$ and j be the largest possible integer such that $\gamma = \{v, T(v), ..., T^{j-1}(v)\}$ is linearly independent. Such a j exists since $\dim V = n$ and thus $j \leq n$.

   Let $\text{span}\{\gamma\} = W$. $T^j(v) \in W$ by the minimality of j. That is, if $T^j(v)$ is not in W, then $T^j(v) \in \gamma$, which is not true.

   Let $w \in W$. It can be written as a linear combination of vectors in γ. But we can see that

   $$w = \sum_{i=0}^{j-1} a_i T^i(v) \Rightarrow T(w) = \sum_{i=0}^{j-1} a_i T^{i+1}(v)$$

   which means that $T(w) \in \text{span}\{\gamma\} = W$. And thus, W is T-invariant. But the only T-invariant subspaces of T is V (it cannot be 0 since γ is non-empty). Thus, $W = V$.

   Thus, $|\gamma| = n = |\beta| \Rightarrow \gamma = \beta$ and hence β is linearly independent as wanted. $\square$

Problem 6: Show that the degree of the minimal polynomial of A over F is equal to the smallest integer k such that there exists a nonzero vector $(c_0, ..., c_k) \in F^{k+1}$ such that $c_0 I + c_1 A + c_2 A^2 + ... + c_k A^k = 0$.

Proof. Let $f(t)$ be the minimal polynomial of A and $g(t) = c_o + c_1 t + ... + c_k t^k$. Note that $\deg(g(t)) = k$ since if $c_k = 0$, then that would contradict the minimality of k.

As per definition, $g(A) = 0$. Thus, $\deg(f(t)) \leq \deg(g(t))$.

Now, suppose for sake of contradiction that $\deg(f(t)) = m < k = \deg(g(t))$.

Well, $f(t) = \sum_{i=0}^{m} a_i t^i$ and $f(A) = 0$. Thus, $(a_0, ..., a_m) \in F^{m+1}$ exists and

$$a_0 I + ... + a_m A^m = 0$$

But $m < k$, which contradicts the minimality of k. Thus, $\deg(f(t)) \geq \deg(g(t))$.

Therefore, $\deg(f(t)) = \deg(g(t))$. $\square$

Problem 7: Let K be a field that contains F (as a subfield). Show that the minimal polynomial of A over F is the same as its minimal polynomial over K.

Proof. Let's denote $m_F(t)$ and $m_K(t)$ as the minimal polynomials of A over F and K respectively. Well, $m_F(t) \in K[t]$ and $m_F(A) = 0$ and so, $m_K(t)|m_F(t)$. That tells us $\deg(m_K(t)) \leq \deg(m_F(t))$.

Now, let $\deg(m_K(t)) = r$. Well, then the set $S = \{I, A, ...A^r\} \in \mathcal{P}(M_{n\times n}(F))$ is linearly dependent over K since a linear combination of them can be equal to 0.

Since the process of Gaussian elimination will be the same over F as it is in K, then S must also be linearly dependent on F. So, there's a degree r polynomial, $g(t)$ in F such that $g(A) = 0$. So, $\deg(m_F(t)) \leq r = \deg(m_K(t))$.

Combining both inequalities, we have, $\deg(m_F(t)) = \deg(m_K(t)) = r$.

Going back to the fact $m_K(t)|m_F(t)$, we can write $m_F(t) = h(t)m_K(t)$ for some $h(t) \in F[t]$. Since the degree of the two minimal polynomials are the same, $\deg(h(t)) = 0$. And since both minimal polynomials are monic by definition, it follows that $h(t) = 1$.

Therefore $m_F(t) = m_K(t)$. $\square$

Problem 8:

Let T be a linear operator on a finite-dimensional vector space V over F. Let $f, g \in F[t]$ be relatively prime. Show that the restriction of $f(T)$ to $\ker(g(T))$ is injective.

Then, deduce that if ϕ and ψ are distinct monic irreducible polynomials in $F[t]$, and A is the companion matrix of ψ^m, then $\phi(A)$ is invertible.

Proof. We want to show that $f(T)$ restricted to $\ker g(T)$ is injective. Which means, if $v \in \ker g(T)$, then $f(T)v = 0 \Rightarrow v = 0$. In other words, $\ker f(T) \cap \ker g(T) = \{0\}$.

So, let $v \in \ker f(T) \cap \ker g(T)$. Since f and g are relatively prime, there exists polynomials a, b such that $a(T)f(T) + b(T)g(T) = I$. So,

$$\begin{aligned} (a(T)f(T) + b(T)g(T))v &= v \\ a(T)f(T)v + b(T)g(T)v &= v \\ 0 + 0 &= v && \text{(since } v \in \ker(T) \text{ and } v \in \ker g(T)\text{)} \\ \Rightarrow v &= 0 && \text{as wanted.} \end{aligned}$$

Now, let A be a linear operator on vector space V. It can be shown that ϕ and ψ^m are relatively prime if ϕ and ψ are themselves relatively prime. Now, the characteristic polynomial of A is ψ^m. Thus, $\psi(A)^m = 0 \Rightarrow \ker \psi(A)^m = V$.

By the first part, $\ker \phi(A) \cap \ker \psi(A)^m = \{0\}$ and thus $\ker \phi(A) = \{0\}$. And so, $\phi(A)$ is of full rank, and is therefore invertible. $\square$