

(b) Prove that if $m_1(t)$ and $m_2(t)$ are relatively prime, then

$$m(t) = m_1(t) \cdot m_2(t).$$

(c) Give an example of a case in which $m(t) \neq m_1(t) \cdot m_2(t)$.

(Indiana)

Solution.

As usual, V can be viewed as a $K[t]$ -module via the linear transformation S . Since W is an S -invariant subspace of V , W is a $K[t]$ -submodule of V . Then it is clear that $(m(t)) = \text{Ann}_{K[t]}V$, $(m_1(t)) = \text{Ann}_{K[t]}W$ and $(m_2(t)) = \text{Ann}_{K[t]}V/W$.

(a) Since

$$\begin{aligned} m_1(t) \cdot m_2(t) \cdot V &\subseteq m_1(t) \cdot W = 0, \\ m_1(t) \cdot m_2(t) &\in \text{Ann}_{K[t]}V = (m(t)). \end{aligned}$$

Hence $m(t)$ divides $m_1(t) \cdot m_2(t)$.

(b) Since

$$m(t) \in \text{Ann}_{K[t]}V \subseteq \text{Ann}_{K[t]}W = (m_1(t)),$$

$m_1(t)$ divides $m(t)$. Similarly, $m_2(t)$ divides $m(t)$. Since $m_1(t)$ and $m_2(t)$ are relatively prime, $m_1(t) \cdot m_2(t)$ divides $m(t)$. Then we have $m(t) = m_1(t) \cdot m_2(t)$, since $m(t)$, $m_1(t)$ and $m_2(t)$ are all monic polynomials.

(c) Let W be a 2-dimensional vector space over the field Q of rational numbers and $S : W \rightarrow W$ be a linear transformation with minimal polynomial $t^2 + 1$. Let $V = W \oplus W$ and $S : V \rightarrow V$ be the natural extension of S to V . Then it is clear that $m(t) = m_1(t) = m_2(t) = t^2 + 1$. So $m(t) \neq m_1(t) \cdot m_2(t)$ in this example.

1103

Let V be a finite dimensional vector space over \mathbb{R} and $T : V \rightarrow V$ be a linear transformation such that (a) the minimal polynomial of T is irreducible and (b) there exists a vector $v \in V$ such that $\{T^i v \mid i \geq 0\}$ spans V . Show that V doesn't have proper T -invariant subspace.

(Indiana)

Solution.

V can be viewed as a module over the polynomial ring $\mathbb{R}[\lambda]$ via $f(\lambda) \cdot x = f(T) \cdot (x)$, for any $f(\lambda) \in \mathbb{R}[\lambda]$ and $x \in V$. Then we have $V = \mathbb{R}[\lambda] \cdot v$, a cyclic module, since $\{T^i v \mid i \geq 0\}$ spans V by (b). Let $m(\lambda)$ be the minimal

polynomial of the linear transformation $T : V \rightarrow V$. Then $m(\lambda) \in \text{Ann}_{\mathbb{R}[\lambda]}(v)$. Since $m(\lambda)$ is irreducible, we have

$$\mathbb{R}[\lambda]/(m(\lambda)) \simeq \mathbb{R}[\lambda] \cdot v = V$$

(we may assume that $V \neq 0$). So V is an irreducible $\mathbb{R}[\lambda]$ -module. Thus, V does not have proper T -invariant subspace.

1104

Let A be an $n \times n$ matrix with entries in \mathcal{C} . Show that A has n distinct eigenvalues in \mathcal{C} if and only if A commutes with no nonzero nilpotent matrix. (Indiana)

Solution.

Necessity. Suppose that A has n distinct eigenvalues $\lambda_1, \lambda_2, \dots, \lambda_n$ in \mathcal{C} . Then there exists an invertible $n \times n$ matrix P such that

$$PAP^{-1} = \text{diag}\{\lambda_1, \dots, \lambda_n\}.$$

If A commutes with some nilpotent matrix B , we have to show $B = 0$. Since $\lambda_1, \lambda_2, \dots, \lambda_n$ are distinct and

$$PAP^{-1} = \text{diag}\{\lambda_1, \dots, \lambda_n\}$$

commutes with $P^{-1}BP$, $P^{-1}BP$ is a diagonal matrix. But the nilpotency of B implies that $P^{-1}BP$ is nilpotent. Hence we have $P^{-1}BP = 0$. So $B = 0$.

Sufficiency. Suppose that the characteristic polynomial of A has multiple roots. We have to show that A commutes with some nonzero nilpotent matrix. Let $\text{diag}(J_1, J_2, \dots, J_t)$ be the Jordan canonical form of A and

$$PAP^{-1} = \text{diag}(J_1, J_2, \dots, J_t),$$

where P is an $n \times n$ invertible matrix and J_i is a Jordan block of order e_i . Without loss of generality, we may assume that $e_1 > 1$ (If all the $e_i = 1$, then it is easy to see that A commutes with some nonzero nilpotent matrix).

Let B_1 be the Jordan block of order e_1 , with 0 on the diagonal. Then $J_1 B_1 = B_1 J_1$ and $B_1 (\neq 0)$ is nilpotent. Let

$$B' = \text{diag}(B_1, B_2, \dots, B_t)$$

where $B_i (i \geq 2) = 0 \in M_{e_i}(\mathcal{C})$. Then

$$B' \cdot PAP^{-1} = PAP^{-1} \cdot B'.$$

Taking $B = P^{-1}B'P$, we have $B \neq 0$, which is nilpotent, and $AB = BA$.