8 Algebras

3/3: **8.1.** Let M_1, M_2 be $A[X]$-modules for an arbitrary ring A, and let $T_i \in \mathrm{End}_A(M_i)$ for $i = 1, 2$ be defined by $T_i(m) = Xm$ for all $m \in M_i$ $(i = 1, 2)$. Let $S : M_1 \to M_2$ be a function.

(i) Prove that S is an $A[X]$-module homomorphism iff...

(a) S is an A-module homomorphism;

(b) $T_2 S = S T_1$.

Proof. Suppose first that S is an $A[X]$-module homomorphism. S is an A-module homomorphism by restriction to A; we already have the group homomorphism condition on the abelian group and the commutativity with scalars as a subset of $A[X]$. Let $m \in M_1$ be arbitrary. Then

$$T_2S(m) = T(Sm) = XS(m) = S(Xm) = ST_1(m)$$

Now suppose that conditions (a)-(b) hold. To prove that S is an $A[X]$-module homomorphism, it will suffice to show that S is a group homomorphism and commutes with scalar multiplication. Just check axioms?? □

(ii) Prove that S is an $A[X]$-module isomorphism iff...

(a) S is an A-module isomorphism;

(b) $T_2 = ST_1S^{-1}$.

Proof. Suppose first that S is an $A[X]$-module isomorphism. S is an A-module isomorphism by restriction to A as above. Let $m \in M_2$ be arbitrary. Then

$$ST_1S^{-1}m = S(T_1(S^{-1}m)) = S(XS^{-1}(m)) = S(S^{-1}(Xm)) = Xm = T_2m$$

Now suppose that conditions (a)-(b) hold. To prove that S is an $A[X]$-module isomorphism, it will suffice to show that S is a group homomorphism and commutes with scalar multiplication. Just check axioms?? □

8.2. Consider (M, T) with $M = A^n$ and $T(a_1, \ldots, a_n) = (0, a_1, \ldots, a_{n-1})$. Prove that the corresponding $A[X]$-module is isomorphic to $A[X]/(X^n)$.

Proof. Lecture 3.1: $A[X]/(X^n) \cong \{p \in A[X] : \deg(p) < n\} \cong (A^n, +)$ as groups. The group isomorphism is defined like f below. (M, T) is the $A[X]$-module with action

$$\left(\sum_{n=0}^{\ell} b_n X^n\right)(a_1, \ldots, a_n) = \sum_{n=0}^{\ell} b_n T^n(a_1, \ldots, a_n)$$

It follows from the definition that $T^i = 0$ for $i \geq n$. Define the isomorphism $f : M \to A[X]/(X^n)$ by $(a_0, \ldots, a_{n-1}) \mapsto a_0 + a_1X + \cdots + a_{n-1}X^{n-1}$. Turn $A[X]/(X^n)$ into an $A[X]$-module under the action of left multiplication by elements of $A[X]$. Does f commute with scalar multiplication? Let $b \in A[X]$ be arbitrary. Then

$$f(ba) = f(\sum_{i=0}^{\ell} b_i T^i(a_0, \ldots, a_{n-1})) = f(\sum_{p=0}^{0} a_p b_{0-p}, \sum_{p=0}^{1} a_p b_{1-p}, \ldots, \sum_{p=0}^{n-1} a_p b_{n-1-p})$$

□

8.3. Let V be a finite dimensional vector space and $T : V \to V$ be a linear transformation. Consider the pair (V, T). Why is V a finitely generated torsion $F[X]$-module?

8.4. $T : V \to V$ is diagonalizable if there is a basis $e_1, \ldots, e_n$ of V consisting of eigenvectors of T, i.e., $Te_i = a_ie_i$ for some $a_i \in F$.

(i) What is the minimal polynomial of T?

Proof. $\ker(\rho)$ is the set of all polynomials in $F[X]$, the corresponding linear transformations of which annihilate V. Consider the $F[X]$-module (V,T). We know that $V=\bigoplus_{i=1}^{n} F[X]/(X-a_i)$. Thus, a basis of the $F[X]$-module V is the e_i's. We want to construct a linear transformation that is a polynomial in T of minimal degree such that $p(T)v=0$ for an arbitrary $v\in V$. Let $f_1e_1+\cdots+f_ne_n$ be arbitrary. The smallest polynomial that sends e_i to 0 is $(X-e_i)$. The smallest polynomial that sends e_i and e_j to zero is $(X-e_i)(X-e_j)$. Suppose one of smaller degree did. Then it's a monomial $X-a$ that's monic up to units. But unless $X-a\in(X-a_i),(X-a_j)$, we have no bueno. Thus, $(X-a_i)\mid X-a$ and $(X-a_j)\mid X-a$, so we have a contradiction. Inducting, we get that the minimal polynomial is $\prod_{i=1}^{n}(X-a_i)$. ☐

(ii) What condition on $a_1,\dots,a_n$ is necessary and sufficient for the existence of a cyclic vector for T?

Proof. Some mutual divisibility relation? Distinct would be sufficient, right? The minimal polynomial is of degree n?

Suppose a cyclic vector $v=f_1e_1+\cdots+f_ne_n$ exists. Then $Tv=f_1a_1e_1+\cdots+f_na_ne_n$.

A necessary and sufficient condition is that

$$\boxed{\text{The } a_1,\dots,a_n \text{ are all distinct.}}$$

Suppose first that the above condition holds. Let $v=e_1+\cdots+e_n$. Then $Tv=a_1e_1+\cdots+a_ne_n$. Suppose that $Tv=bv$ for some $b\in F$. Then $a_1=\cdots=a_n=b$, a contradiction.

Suppose that $b_1v+b_2Tv=0$. Then $b_1+b_2a_i=0$ for all i, so $a_i=-b_1/b_2$. I.e., the polynomial has at most one solution. Inducting, such polynomials have at most so many solutions. Done.

Now suppose inductively that $T^kv=b_1v+b_2Tv+\cdots+b_{k-1}T^{k-1}v$ for some $k<n$. Then

$$a_1^kf_1e_1+\cdots+a_n^kf_ne_n=b_1$$

Now suppose that $v=f_1e_1+\cdots+f_ne_n$ is a cyclic vector for T. Then $Tv\neq bv$ for any $b\in F$. In particular, $a_1f_1e_1+\cdots+a_nf_ne_n\neq bf_1e_1+\cdots+bf_ne_n$, so at least two of the a_i's are distinct. $b_0v+b_1Tv\neq 0$ for any not-both-zero b_0,b_1. Then $(b_0+b_1a_1)f_1e_1+\cdots+(b_0+b_1a_n)f_ne_n\neq 0$. Choose b_0,b_1 such that $b_0+b_1a_1=0$. Then there is some i such that $b_0+b_1a_i\neq 0$; this a_i must be distinct. Scaling up, choose $b_0,\dots,b_{n-1}$ such that $a_1,\dots,a_{n-1}$ go to zero, i.e., such that $b_0+\cdots+b_{n-1}X^{n-1}=(X-a_1)\cdots(X-a_{n-1})$. Then a_n is distinct. We can build up our sequence WLOG so that each new a_i is a_2, for instance, then a_3, then so on. ☐

8.5. Let V be an n-dimensional vector space. Let $T\in\mathrm{End}_F(V)$. Let $A=\{S\in\mathrm{End}_F(V):ST=TS\}$. *Hint*: We may regard V as an $F[X]$-module. Identify A with $\mathrm{End}_{F[X]}(V)$. And then use the rational canonical from.

(i) Show that the dimension of A (as an F-vector space) is greater than or equal to n.

Proof. The scalar matrices are certainly a subspace.

How about the subspace of diagonal matrices? ☐

(ii) Show that the equality is attained iff T has a cyclic vector.

8.6. Let $f\in R[X]$ be a monic polynomial of degree n. Let M be a free R-module with basis $e_1,\dots,e_n$.

(i) Show that there is a unique R-module homomorphism $T:M\to M$ such that $T(e_i)=e_{i+1}$ for all $i=1,\dots,n-1$ and $f(T)e_1=0$.

(ii) Show that $f(T)v=0$ for all $v\in M$.

(iii) Let $b\in R$. Define $S:M\to M$ by $S(v)=bv-Tv$ for all $v\in M$. Compute $\Lambda^k(S)e_1\cdots e_k$. for all $k=1,\dots,n$ inductively and deduce that $\det(S)=f(b)$.

8.7. Let V be a vector space over a field F. Let $v_1, \ldots, v_r \in V$.

(i) Prove that if $v_1, \ldots, v_r$ are linearly dependent, then $v_1 \cdots v_r \in \Lambda^r(V)$ equals zero.

(ii) Prove that if $v_1, \ldots, v_r$ are linearly independent, then $v_1 \cdots v_r \in \Lambda^r(V)$ is nonzero.

(iii) Prove that if W is a linear subspace of V and $w_1, \ldots, w_r$ is a basis of W, then the one-dimensional subspace $Fw_1 \cdots w_r$ of $\Lambda^r(V)$ depends only on W, i.e., it does not depend on the choice of the basis $w_1, \ldots, w_r$. It is conventional to refer to this one dimensional subspace as $\det(W) \subset \Lambda^r(V)$.

(iv) If W_1, W_2 are both r-dimensional subspaces of V, ad if the one-dimensional subspaces $\det(W_1)$ and $\det(W_2)$ of $\Lambda^r(V)$ are equal to each other, show that $W_1 = W_2$.

8.8. Let V be a vector space of dimension 4, and let $\omega \in \Lambda^2(V)$ be nonzero. Prove that $\omega^2 = 0$ iff $F\omega = \det(W)$ for a two-dimensional subspace $W \subset V$.

8.9. Prove that the characteristic polynomial is monic of degree n. Prove that the coefficient of λ^{n-1} in the characteristic polynomial of L is the negative of the trace of L, which is defined to be the sum of the diagonal terms of the matrix that represents L when a basis $e_1, \ldots, e_n$ is specified.

8.10. Deduce the Cayley-Hamilton theorem for fields from Problem 8.6 and the fact that every torsion $F[X]$-module is the direct sum of cyclic modules.

8.11. (i) Show that the Cayley-Hamilton theorem for fields implies the theorem for integral domains as well.

(ii) Show that the Cayley-Hamilton theorem for the polynomial ring $\mathbb{Z}[X_1, \ldots, X_{n^2}]$ implies the theorem for all $L : R^n \to R^n$ where R is a commutative ring.