Determinant trick, Cayley-Hamilton Theorem and Nakayama's Lemma

Qiangru Kuang

Let A be a commutative ring and M be an A-module generated by $\{m_1, \dots, m_n\}$. Note that M is naturally an $\mathrm{End}(M)$-module and for all $f \in \mathrm{End}(M)$, write $[f] \in \mathcal{M}_n(A)$ for its representation with respect to the generators above, i.e. $f(m_i) = \sum_j [f]_{ij} m_j$. In particular, there is a ring homomorphism $\mu : A \to \mathrm{End}(M), a \mapsto a \cdot -$ sending an element to its multiplication action. Let $A' = \mu(A)$.

There is a technical remark to make: later we will use determinant of matrices over $\mathrm{End}(M)$, which is non-commutative. However, throughout the discussion we are concerned with only one endomorphism φ (besides multiplication, of course) so we can restrict the scalars to $A'[\varphi]$, a subring contained in the centre of $\mathrm{End}(M)$.

Given a module endomorphism $\varphi : M \to M$, its characteristic polynomial is defined to be

$$\chi_{[\varphi]}(x) = \det(x \cdot I - [\varphi]) \in A[x]$$

where I is the $n \times n$ identity matrix and the product $x \cdot I$ is multiplication of a matrix by a scalar. We have

Theorem 0.1 (Cayley-Hamilton)**.**

$$\chi_{[\varphi]}(\varphi) = 0.$$

This is a slight generalisation of the result one might be familiar with from linear algebra. Note that this is a relation of endomorphisms with coefficients in A.

Proof. Let $[\varphi]_{ij} = a_{ij}$ and view M as an $A'[\varphi]$-module. Since

$$\varphi m_i = \sum_j a_{ij} m_j,$$

we have

$$\sum_j \underbrace{(\varphi \delta_{ij} - a_{ij})}_{\Delta_{ij}} m_j = 0 \qquad (*)$$

with

$$\Delta = \varphi \cdot I - N \in \mathcal{M}_n(A'[\varphi]).$$

Again, the multiplication is by scalar φ, viewed as an element of the ring $\mathrm{End}(M)$.

Claim that if $\det \Delta = 0 \in \mathrm{End}(M)$ then we are done: consider the ring homomorphism

$$\begin{aligned} A[x] &\to \mathrm{End}(M) \\ x &\mapsto \varphi \end{aligned}$$

which maps $\chi_{[\varphi]}(t) \mapsto \chi_{[\varphi]}(\varphi) = \det \Delta$ since det is a polynomial function. So done.

To show this, recall that

$$(\operatorname{adj} \Delta) \cdot \Delta = \det \Delta \cdot I \in \mathcal{M}_n(A'[\varphi])$$

where multiplication on the left is between matrices. Let $(\operatorname{adj} \Delta)_{ij} = b_{ij}$. Then multiply $(*)$ by b_{ki} and apply the identity,

$$\sum_{i,j} (b_{ki} \Delta_{ij}) m_j = \sum_j (\det \Delta \delta_{kj}) m_j = (\det \Delta) m_k = 0.$$

so $\det \Delta = 0$ as required. □

We extract the key idea in the proof, which some authors call the *determinant trick*, which has many applications in commutative algebra:

Theorem 0.2. *Let M be an A-module generated by n elements and $\varphi : M \to M$ a homomorphism. Suppose I is an ideal of A such that $\varphi(M) \subseteq IM$, then there is a relation*

$$\varphi^n + a_1 \varphi^{n-1} + \dots + a_{n-1} \varphi + a_n = 0$$

where $a_i \in I^i$ for all i.

Proof. Let $\{m_1, \dots, m_n\}$ be a set of generators of M. Since $\varphi(m_i) \in IM$, we can write

$$\varphi m_i = \sum_j a_{ij} m_j$$

with $a_{ij} \in I$. Multiply

$$\sum_j \underbrace{(\varphi \delta_{ij} - a_{ij})}_{\Delta_{ij}} m_j = 0$$

by $\operatorname{adj} \Delta$, we deduce that $(\det \Delta) m_j = 0$ so $\det \Delta = 0 \in \operatorname{End}(M)$. Expand. □

Corollary 0.3 (Nakayama's Lemma)**.** *If M is a finitely generated A-module and $I \trianglelefteq R$ is such that $M = IM$ then there exists $x \in A$ such that $x - 1 \in I$ and $xM = 0$.*

Proof. Apply the trick to id_M. Since $\mathrm{id}_M^i = \mathrm{id}_M$ and $a_n = a_n \,\mathrm{id}_M$, we get

$$\left(1 + \sum_{i=1}^n a_i\right) \mathrm{id}_M = 0.$$

□

We use the result to prove a rather interesting fact about module homomorphism:

Proposition 0.4. *Let M be a finitely generated A-module. Then every surjective module homomorphism on M is also injective.*

Proof. Let $\varphi : M \to M$ be surjective. Let M be an $A'[\varphi]$ module and $I = (\varphi) \trianglelefteq A'[\varphi]$. Then $M = IM$ by surjectivity of φ. Thus by Nakayama's Lemma, there exists $x = 1 + \varphi\psi$, $\psi \in A'[\varphi]$ such that $(1 + \varphi\psi)M = 0$, i.e. for all $m \in M$, $(1 + \varphi\psi)m = 0$. It follows that $\varphi^{-1} = -\psi$. $\square$