The Cayley-Hamilton Theorem

We prove:

THEOREM (Cayley-Hamilton Theorem). Let R be a commutative ring, and $A \in M_{n\times n}(R)$. Then A satisfies its characteristic polynomial.

1. Preliminary definitions

DEFINITION 1.1. $M_{n\times n}(R)$ is the ring of n-by-n matrices with entries in R.

DEFINITION 1.2. Let $I \in M_{n\times n}(R)$ be the identity matrix. Then

$$xI - A \in M_{n\times n}(R[x]).$$

The determinant

$$\det(xI - A) =: p_A(x) \in R[x]$$

is the *characteristic polynomial* of A.

DEFINITION 1.3. Fix a polynomial

$$f(x) = a_n x^n + \ldots + a_1 x + a_0 \in R[x].$$

We say that a matrix A satisfies f if

$$f(A) = a_n A^n + \ldots + a_1 A + a_0 = 0 \in M_{n\times n}(R).$$

REMARK 1.4. Recall that given a matrix M and a scalar $a \in R$, the product aM is the matrix obtained by scaling every entry of M by a. Also, in the above equation, a_0 is the diagonal matrix whose diagonal entries are all equal the scalar a_0.

2. The main homomorphism, ϵ_A

The main tool we use is a map called ϵ_A. It takes a matrix with polynomial entries and produces a matrix with R entries.

First, let $\mathbb{M}$ be a matrix whose entries are elements of $R[x]$. By decomposing $\mathbb{M}$ by degree of x, we can write $\mathbb{M}$ as a sum

$$\mathbb{M} = \mathbb{M}^{(0)} + \mathbb{M}^{(1)}x + \ldots \mathbb{M}^{(d)}x^d \tag{1}$$

where each $\mathbb{M}^{(a)}$ is an $n \times n$-matrix with entries in R. Moreover, given another matrix $\mathbb{N} = \sum_{b \geq 0} \mathbb{N}^{(b)}x^b$, one can verify

$$\mathbb{M}\mathbb{N} = \sum_{i \geq 0} \sum_{a+b=i} \mathbb{M}^{(a)}\mathbb{N}^{(b)}x^i.$$

Here, $\mathbb{M}^{(a)}\mathbb{N}^{(b)}$ is the usual matrix multiplication of the matrix $\mathbb{M}^{(a)}$ with the matrix $\mathbb{N}^{(b)}$.

Fixing an element $A \in M_{n\times n}(R)$, we have the following group homomorphism:

$$\epsilon_A : M_{n\times n}(R[t]) \to M_{n\times n}(R), \qquad \sum_{i\geq 0} \mathbb{M}^{(i)}x^i \mapsto \sum_{i \geq 0} \mathbb{M}^{(i)}A^i.$$

You can check that ϵ_A respects addition. However, note that ϵ_A is *not* a ring homomorphism; indeed,

$$\mathbb{M}^{(a)}\mathbb{N}^{(b)}A^{a+b} \neq \mathbb{M}^{(a)}A^a\mathbb{N}^{(b)}A^b$$

unless $\mathbb{N}^{(b)}$ commutes with A^a for all a and b.

Remark 2.1. Note that $\mathbb{M}^{(a)}$ is simply the ath matrix in some sequence, while A^a is the ath power of the matrix A. Also, $\mathbb{M}^{(a)}A^a$ is the product of the matrices $\mathbb{M}^{(a)}$ and A^a.

3. The three main facts

To prove the theorem, we use three lemmas:

Lemma 3.1. Let $\mathbb{N} = \sum_{b\geq 0} \mathbb{N}^{(b)}x^b$. If for each b, $\mathbb{N}^{(b)}$ is a matrix which commutes with A, then

$$\epsilon_A(\mathbb{M}\mathbb{N}) = \epsilon_A(\mathbb{M})\epsilon_A(\mathbb{N}).$$

Lemma 3.2. Let $\mathbb{D}$ be a diagonal matrix all of whose entries is equal to $f(x) \in R[x]$. Then

$$\epsilon_A(\mathbb{D}) = f(A).$$

For the last lemma, recall that $Cof(A)_{j,i}$ is the matrix obtained by deleting the jth row and ith column of A.

LEMMA 3.3. Let S be any commutative ring. Fix $A \in M_{n\times n}(S)$, and define a matrix $C \in M_{n\times n}(S)$ by:

$$C_{ij} := (-1)^{i+j} \det(Cof(A)_{j,i}).$$

Then

$$CA = \det(A) I_{n\times n}.$$

That is, the product CA is a diagonal matrix, and all of the diagonal entries are equal to $\det(A) \in S$.

4. Proof of Theorem

PROOF OF CAYLEY-HAMILTON ASSUMING THE LEMMAS. Let $\mathbb{A}$ be the matrix $xI - A$. Let $\mathbb{C}$ be the matrix where

$$\mathbb{C}_{ij} := (-1)^{i+j} \det(Cof(\mathbb{A})_{j,i}).$$

Using Lemma 3.3 and setting $S = R[t]$, we know

$$\mathbb{C}\mathbb{A} = \mathbb{D} \in M_{n\times n}(R[t])$$

where $\mathbb{D}$ is diagonal and the diagonal entries are given by the characteristic polynomial of A:

$$\det(\mathbb{A}) = \det(xI - A) = p_A(x).$$

By Lemma 3.2, we conclude

$$\epsilon_A(\mathbb{C}\mathbb{A}) = \epsilon_A(\mathbb{D}) = p_A(A).$$

On the other hand, note that

$$\mathbb{A}^{(0)} = -A, \qquad \mathbb{A}^{(1)} = I$$

both of which commute with A (and hence any power of A). By Lemma 3.1, we conclude

$$\epsilon_A(\mathbb{C}\mathbb{A}) = \epsilon_A(\mathbb{C})\epsilon_A(\mathbb{A}).$$

Moreover,

$$\epsilon_A(\mathbb{A}) = \epsilon_A(xI - A) = \epsilon_A(xI) - \epsilon_A(A) = A - A = 0.$$

Thus

$$0 = \epsilon_A(\mathbb{C}) \cdot 0 = \epsilon_A(\mathbb{C})\epsilon_A(\mathbb{A}) = \epsilon_A(\mathbb{C}\mathbb{A}) = p_A(A).$$

□

5. Proof of Lemmas

The third lemma was proven in a previous class, so we just prove the first two.

Proof of Lemma 3.1. We use the hypothesis in the second line below:

$$\begin{aligned}\epsilon_A(\mathbb{M}\mathbb{N}) &= \sum_{a,b} \mathbb{M}^{(a)}\mathbb{N}^{(b)}A^{a+b} \\ &= \sum_{a,b} \mathbb{M}^{(a)}A^a\mathbb{N}^{(b)}A^b \\ &= \left(\sum_a \mathbb{M}^{(a)}A^a\right)\left(\sum_b \mathbb{N}^{(b)}A^b\right) \\ &= \epsilon_A(\mathbb{M})\epsilon_A(\mathbb{N}).\end{aligned}$$

□

Proof of Lemma 3.2. Since $\mathbb{D}$ is diagonal, each $\mathbb{D}^{(i)}$ is diagonal in the decomposition

$$\mathbb{D} = \sum_{a\geq 0} \mathbb{D}^{(a)}x^a.$$

Let $f(x) = \sum_{a\geq 0} r_a x^a$ be the polynomial of the hypothesis, so that $\mathbb{D}^{(a)} = r_a I$. Then

$$\begin{aligned}\epsilon_A(\mathbb{D}) = \epsilon_A(\sum_{a\geq 0}\mathbb{D}^{(a)}x^a) &= \sum_{a\geq 0}\epsilon_A(\mathbb{D}^{(a)}x^a) \\ &= \sum_{a\geq 0} r_a I A^a \\ &= \sum_{a\geq 0} r_a A^a \\ &= f(A).\end{aligned}$$

□

6. Some big picture remarks

Remark 6.1. The decomposition (1) of $\mathbb{M}$ realizes a ring isomorphism

$$M_{n\times n}(R[x]) \cong M_{n\times n}(R)[x].$$

On the righthand side is the polynomial ring with coefficients in a *non-commutative* ring $M_{n\times n}(R)$.

Remark 6.2. The map ϵ_A may seem mysterious—it is "almost" a ring homomorphism, in that multiplication is respected only by certain elements $\mathbb{N}$, and only when these certain elements act from the right.

In fact, what Lemma 3.1 says is that ϵ_A is actually a map of *right modules* over a particular ring Q_A.

Let Q_A be the ring of matrices $\mathbb{N} \in M_{n\times n}(R[x])$ such that, writing $\mathbb{N} = \sum_{b\geq 0} \mathbb{N}^{(b)} x^b$, each $\mathbb{N}^{(b)}$ commutes with A. One can check that this is a subring of $M_{n\times n}(R[x])$.

We have an obvious action

$$M_{n\times n}(R[x]) \times Q_A \to M_{n\times n}(R[x]), \qquad (\mathbb{M}, \mathbb{N}) \mapsto \mathbb{M}\mathbb{N}$$

making $M_{n\times n}(R[x])$ into a right module over Q_A.

Moreover, we have another right module action

$$M_{n\times n}(R) \times Q_A \to M_{n\times n}(R), \qquad (B, \mathbb{N}) \mapsto \sum_{b\geq 0} B\mathbb{N}^{(b)} A^b.$$

And Lemma 3.1 says ϵ_A is a map of right Q_A-modules.

7. Some clarifying examples

Example 7.1. Consider the matrix

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Then

$$p_A(A) = x^2 - trace(A)x + \det(A).$$

Example 7.2. Consider the matrix

$$\mathbb{M} = \begin{pmatrix} ax^2 + bx + c & d & e \\ f & g & hx^2 \\ i & j & kx \end{pmatrix}.$$

Then

$$\mathbb{M}^{(0)} = \begin{pmatrix} c & d & e \\ f & g & 0 \\ i & j & 0 \end{pmatrix}$$

$$\mathbb{M}^{(1)} = \begin{pmatrix} b & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & k \end{pmatrix}$$
$$\mathbb{M}^{(2)} = \begin{pmatrix} a & 0 & 0 \\ 0 & 0 & h \\ 0 & 0 & 0 \end{pmatrix}.$$

8. Some applications

EXAMPLE 8.1. Suppose A is a 2-by-2 matrix with $trace(A) = 0$. Then the characteristic polynomial is $p_A(x) = x^2 + \det(A)$. By the Cayley-Hamilton theorem, we conclude

$$A^2 = -\det(A)I.$$

Hence to compute A^{1000}, we observe

$$A^{1000} = (A^2)^{500} = (-\det A)^{500} I.$$

So, rather than tediously computing the matrix multiplication of A with itself 1000 times, we need only compute the 500th power of a scalar (called the determinant of A).

By the way, a quick way to compute the Nth power of something is to break down N in base 2:

$$N = e_a 2^a + e_{a-1} 2^{a-1} + \ldots + e_1 2 + e_0$$

where each e_i is 0 or 1. Then you only need to compute $a-1$ squares

$$A^2, (A^2)^2, \ldots, (A^{2^{a-1}})^2$$

then multiply the a matrices appropriately to compute A^N.

EXAMPLE 8.2. Let's say you want to know whether there is an element of order k in $GL_n(R)$. Well, an element of order k must satisfy the polynomial

$$x^k - 1.$$

In any ring, this polynomial factors as

$$x^k - 1 = (x-1)(x^{k-1} + \ldots + x^2 + x + 1).$$

So if A is an element of order k, then we know that A satisfies both its characteristic polynomial $p_A(x)$ and the polynomial $x^k - 1$. Thus, a question about A is reduced to questions about the polynomials $p_A(x)$ and $x^k - 1$. For example, if R is a field, then for A to satisfy both these polynomials, these polynomials must have a common factor—some polynomial $h(x)$ which mutually divides them both. One can often rule out the existence of such an $h(x)$ based on knowledge of R, hence one can often rule out the existence of elements of order k in $GL_n(R)$.