A TOPOLOGICAL PROOF OF THE CAYLEY-HAMILTON THEOREM

Jeffrey A. Rosoff

Gustavus Adolphus College

The Cayley-Hamilton theorem in linear algebra is generally proven by solely algebraic means, e.g. the use of cyclic subspaces, companion matrices, etc. [1,2]. In this article we give a short and basically topological proof of this very algebraic theorem. First the theorem:

Cayley-Hamilton. Let V be a finite-dimensional vector space over a field, and let $T: V \to V$ be a linear transformation with characteristic polynomial $p_T(x)$. Then $p_T(T)$ is the zero transformation.

The correspondence between linear transformations and matrices allows us to prove the equivalent matrix form of the theorem.

Cayley-Hamilton (matrix form). Let A be an $n \times n$ matrix over a field with characteristic polynomial $p_A(x) = \det(xI - A)$, where I is the $n \times n$ identity matrix. Then $p_A(A)$ is the zero matrix.

For simplicity, we will prove the result over the field $\mathbb{C}$ of complex numbers and, as promised, use topological techniques. However, essentially the same proof works over any field (see the remark at the end of the proof).

Notation. Let

$$P_n = \{ \text{ monic polynomials of degree } n \text{ over } \mathbb{C}\},$$

let

$$M_n = \{n \times n \text{ matrices over } \mathbb{C}\},$$

and let

$$D_n = \{A \in M_n \mid A \text{ is diagonalizable } \}.$$

Note that we may identify P_n with $\mathbb{C}^n$ and M_n with $\mathbb{C}^{n^2}$, making each into a topological (in fact metric) space.

Lemma 1. Let $F\colon \mathbb{C}^n \to \mathbb{C}$ be a non-constant polynomial mapping. Then if U is open in $\mathbb{C}^n$, $F(U)$ is open in $\mathbb{C}$.

Proof. (Induction on n).

1) Say $F\colon \mathbb{C} \to \mathbb{C}$ is a non-constant polynomial mapping, and suppose that we have an open set U in $\mathbb{C}$. If $F(U)$ is not open then there is a point p in U and a sequence $\{q_i\}$ in $\mathbb{C}$ converging to $F(p)$ such that $F^{-1}(q_i) \cap U$ is empty. Hence, there is a number $h > 0$ such that whenever $t \in F^{-1}(q_i)$ for any i, then $|t - p| > h$.

For each q_i as above, we have the factorization

$$F(x) - q_i = a(x - r_{1,i})(x - r_{2,i}) \cdots (x - r_{k,i}),$$

where a is the leading coefficient of F and $\{r_{j,i}\}_{j=1}^{k} = F^{-1}(q_i)$; $k =$ degree of F.

Thus,

$$|F(p) - q_i| = |a||p - r_{1,i}| \cdots |p - r_{k,i}| > |a|h^k;$$

letting i get large yields a contradiction, so $F(U)$ is open.

2) Now suppose that $F\colon \mathbb{C}^n \to \mathbb{C}$ is a non-constant polynomial mapping, with U open in $\mathbb{C}^n$, and $n \geq 2$. Since $F(x_1, x_2, \ldots, x_n)$ is non-constant, we may assume that it is non-constant in one of the n coordinates, say x_{n-1}. Let

$$H_t = \{(x_1, \ldots, x_n) \in \mathbb{C}^n \mid x_n = t\}.$$

Then H_t is naturally identified with $\mathbb{C}^{n-1}$, and $U \cap H_t$ is open in H_t, i.e. open in $\mathbb{C}^{n-1}$.

Now,

$$F(U) = \bigcup_t F(U \cap H_t),$$

and $F|U \cap H_t$ can be regarded as a non-constant polynomial in the $n - 1$ variables $x_1, \ldots, x_{n-1}$; by the inductive hypothesis $F(U \cap H_t)$ is open in $\mathbb{C}$, so $F(U)$ is open.

Corollary. Let $F\colon \mathbb{C}^n \to \mathbb{C}$ be as in Lemma 1. Then if S is a dense subset of $\mathbb{C}$, $F^{-1}(S)$ is dense in $\mathbb{C}^n$; in particular $F^{-1}(\mathbb{C} - \{0\})$ is dense in $\mathbb{C}^n$.

Proof. If $F^{-1}(S)$ is not dense in $\mathbb{C}^n$, there would be a non-empty open set U in the complement of $F^{-1}(S)$. By Lemma 1, $F(U)$ would be open in the complement of S, which contradicts the density of S.

We recall a couple of well-known facts about polynomials, the details of which may be found in [3]. Let $x_1, x_2, \ldots, x_n$ be variables. The kth elementary symmetric function of the $\{x_i\}$ is defined by

$$\mu_k(x_1, \ldots, x_n) = \sum (x_{i_1} \cdots x_{i_k}),$$

where the sum is taken over all subsets $\{i_1, \ldots, i_k\}$ of $\{1, 2, \ldots, n\}$. Then

1) If G is a symmetric polynomial in the $\{x_i\}$, i.e. if

$$G(x_1, \ldots, x_n) = G(x_{\beta(1)}, \ldots, x_{\beta(n)})$$

for all permutations β on n letters, then G can be written as a polynomial in the elementary symmetric functions $\mu_k(x_1, \ldots, x_n)$.

2) If $f \in P_n$ is given by

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0,$$

then the coefficients of f are given by elementary symmetric functions of its roots $\{r_i\}$, i.e.

$$a_{n-k} = (-1)^k \mu_k(r_1, \ldots, r_n),$$

for $k = 1, 2, \ldots, n$.

Lemma 2. D_n is dense in M_n.

Proof. Let $\triangle \colon P_n \to \mathbb{C}$ be given by

$$\triangle(f) = \prod_{i<j} (r_i - r_j)^2$$

where the $\{r_i\}$ are the roots of f; note that $\triangle(f)$ vanishes if and only if f has a multiple root. Clearly $\triangle(f)$ is invariant under any permutation of the roots $\{r_i\}$, so in light of our observations 1) and 2) above, $\triangle(f)$ is a polynomial in the coefficients of f. Hence, $\triangle$ can be regarded as a polynomial mapping from $\mathbb{C}^n$ to $\mathbb{C}$.

Let $\partial \colon M_n \to P_n$ be given by

$$\partial(A) = \det(xI - A).$$

Then ∂ can be regarded as a polynomial mapping from $\mathbb{C}^{n^2}$ to $\mathbb{C}^n$, and the composition $\triangle \cdot \partial \colon M_n \to \mathbb{C}$ can be viewed as a (non-constant) polynomial mapping from $\mathbb{C}^{n^2}$ to $\mathbb{C}$. By

the Corollary to Lemma 1, $(\triangle \cdot \partial)^{-1}(\mathbb{C} - \{0\})$ is dense in M_n (i.e. in $\mathbb{C}^{n^2}$); since a sufficient criterion for diagonalizability of an $n \times n$ matrix is the existence of n distinct eigenvalues, $(\triangle \cdot \partial)^{-1}(\mathbb{C} - \{0\}) \subset D_n$, proving the lemma.

Lemma 3. The Cayley-Hamilton theorem holds for diagonalizable matrices.

Proof. Suppose that A is diagonalizable, so $A = QDQ^{-1}$ for some invertible matrix Q and some diagonal matrix

$$D = \begin{pmatrix} r_1 & 0 & \dots & 0 \\ 0 & r_2 & \dots & 0 \\ . & . & \dots & . \\ 0 & . & \dots & r_n \end{pmatrix}.$$

If

$$p_A(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

then we have

$$\begin{aligned} p_A(A) &= (QDQ^{-1})^n + a_{n-1}(QDQ^{-1})^{n-1} + \cdots + a_1(QDQ^{-1}) + a_0 I \\ &= Q(p_A(D))Q^{-1}. \end{aligned}$$

But

$$p_A(D) = \begin{pmatrix} p_A(r_1) & \dots & 0 \\ . & & . \\ . & & . \\ 0 & \dots & p_A(r_n) \end{pmatrix},$$

which is the zero matrix since the r_i are merely the eigenvalues of A.

Proof of the Cayley-Hamilton Theorem. The mapping $\Omega\colon M_n \times P_n \to M_n$ given by $\Omega(A, f(x)) = f(A)$ is continuous (it is really a polynomial map from $\mathbb{C}^{n^2} \times \mathbb{C}^n$ to $\mathbb{C}^{n^2}$), and the mapping $\Phi\colon M_n \to M_n \times P_n$ given by $\Phi(A) = (A, p_A(x))$ is similarly continuous. Hence, the composition

$$\Omega \cdot \Phi\colon M_n \to M_n,$$

which is given by $\Omega \cdot \Phi(A) = p_A(A)$, is continuous. By Lemmas 2 and 3, this mapping is identically zero on a dense subset of M_n, so by continuity vanishes everywhere.

Remark. For an analogous proof of the Cayley-Hamilton theorem over an arbitrary field F, first replace F by its algebraic closure $\overline{F}$. Then, as in the above proof, identify P_n and M_n with $\overline{F}^n$ and $\overline{F}^{n^2}$ respectively, and give each of these spaces the Zariski topology (in which the closed sets are the zero-loci of finite sets of polynomials [4]). As in our proof, Lemma 2 is obtained by noting that D_n contains those matrices A for which the characteristic polynomial $p_A(x)$ has distinct roots; this set is open and dense in the Zariski topology. The remainder of the proof is identical to that given above.

References

More standard (i.e. purely algebraic) proofs of the Cayley-Hamilton theorem can be found in most linear algebra tests, e.g.

1. I. Friedberg and S. Friedberg, *Linear Algebra*, 2nd edition, Prentice Hall, 1989.
2. Walker, *Introduction to Abstract Algebra*, Random House, 1987.
3. Van der Waerden, *Algebra*, Vol. 1, Ungar Publishing Co., 1970.

For a good description of the Zariski topology, one can consult

4. R. Hartshorne, *Algebraic Geometry*, GTM, Springer-Verlag, 1977.

A complex-analytic proof of the Cayley-Hamilton theorem (valid only over $\mathbb{C}$) based on the Cauchy Integral Theorem can be found in

5. C. A. McCarthy, "The Cayley-Hamilton Theorem," *American Mathematical Monthly*, 82 (April 1975).