Polynomials Satisfied by Square Matrices: A Converse to the Cayley-Hamilton Theorem

Anandam Banerjee

Anandam Banerjee is a student of B.Sc. IInd year at the Chennai Mathematical Institute. This work was done during a visit to the Indian Statistical Institute, Bangalore during May-July 2002.

Some Linear Algebra

Given a matrix $A \in M_n(\mathbf{R})$, the polynomial $\chi_A(x) = det(A - xI)$ is called the characteristic polynomial of A. We can also define it for matrices over $\mathbf{C}$ or more generally for any arbitrary field K, or even for any commutative ring[1] Now, if $A = (a_{ij}) \in M_n(K)$, we have

$$A - xI = \begin{pmatrix} a_{11} - x & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} - x & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} - x \end{pmatrix}.$$

Thus $\chi_A(x) = det(A - xI) = a_0 + a_1 x + \cdots + a_n x^n$, a polynomial of degree n with coefficients from K. Note that a_i's can be treated as polynomials in n^2 variables over K.

We will denote a polynomial f over K in n^2 variables, say $x_{11}, x_{12}, \cdots, x_{nn}$ by $f(X)$, where $X = (x_{ij}) \in M_n(K)$. That is, we may write $f(X) \in K[x_{ij}]$. Also, for any polynomial $f(X) \in K[x_{ij}]$ and for $\lambda \in K$, we can write,

$$f(A - \lambda.I) = f_0(A) + f_1(A)\lambda + \cdots + f_d(A)\lambda^d$$

where f_i's are polynomials in n^2 variables, $A \in M_n(K)$, and d is some non-negative integer. Note that $f_0(A) = f(A)$. (Put $\lambda = 0$).
Thus, we can write

$$\chi_A(x) = c_0(A) + c_1(A)x + \cdots + c_n(A)x^n.$$

[1] Recall that a ring is a set, which is an Abelian group under addition, and closed under multiplication. Multiplication is associative and distributive with addition. A commutative ring is one in which multiplication is commutative.

Recall that $\lambda \in K$ is called an eigenvalue of $A \in M_n(K)$, if $A.v = \lambda.v$ for some $0 \neq v \in K^n$. Note that any eigenvalue of the matrix A is a root of $\chi_A(x)$.

We now state the well-known theorem in linear algebra concerning characteristic polynomials of matrices known as :

Cayley-Hamilton Theorem:
Let A be a $n \times n$ matrix with entries in a field K and let $\chi_A(x) = det(A - xI)$ be its characteristic polynomial. Then $\chi_A(A) = 0$ as an $n \times n$ matrix.

In fact, the theorem is valid for matrices over any commutative ring which has a multiplicative unity 1. However, we will concentrate on fields only. We will prove a slightly generalised version of the above theorem. We also draw attention to the fact that, in a sense - made precise at the end of this article - every polynomial identity satisfied by the set of all $n \times n$ matrices, is a consequence of the Cayley-Hamilton theorem.

Theorem :
Let $A, B \in M_n(K)$ be such that $AB = BA$. Then, $\chi_A(B) = (B - A)C$ for some $C \in M_n(K)$. In particular, $\chi_A(A) = 0$.
Proof: We know that, for any matrix A, $\det(A).I = A.Adj(A)$, where $Adj(A)$ is the adjoint ofthe matrix A. Since $\mathrm{Adj}(A - xI)$ can be written as

$$Adj(A - xI) = g_0(A) + g_1(A)x + \cdots + g_{n-1}(A)x^{n-1},$$

where $g_i(A)$ are matrix-valued functions of A and, since $\chi_A(x) = det(A - xI)$, we have

$$\chi_A(x)I = (A - xI)Adj(A - xI)$$
$$= (A - xI)(g_0(A) + g_1(A)x + \cdots + g_{n-1}(A)x^{n-1})$$
$$= c_0(A) + c_1(A)x + \cdots + c_n(A)x^n.$$

Hence,

$$\chi_A(B) = c_0(A)I + c_1(A)B + \cdots + c_n(A)B^n$$
$$= g_0(A)A + (g_1(A)A - g_0(A))B + \cdots + (g_{n-1}(A)A - g_{n-2}(A))B^{n-1} - g_{n-1}(A)B^n$$
$$= (A - B)(g_0(A) + g_1(A)B + \cdots + g_{n-1}(A)B^{n-1}).$$

Thus, $\chi_A(A) = 0$.

Hence, if $f(X) = g(X).det(X) \in K[x_{ij}]$, we have

$$f(A - xI) = g(A - xI)(c_0(A) + c_1(A)x + \cdots + c_n(A)x^n).$$

Therefore,

$$f_0(A).I+f_1(A).A+\cdots+f_d(A).A^d = p(A)(c_0(A)I+c_1(A)A+\cdots+c_n(A)A^n) = 0$$

where $p(A)$ is some polynomial in A.

A natural question that arises now is whether the converse is true. That is, if $f(X) \in K[x_{ij}]$ satisfies

$$f_0(A).I + f_1(A).A + \cdots + f_d(A).A^d = 0 \cdots (1)$$

for every matrix A, then is $f(X)$ a multiple of $det(X)$? Let us try to check this for some finite fields first.

Example: Consider the matrix $X = (x_{ij}) \in M_2(\mathbf{F}_p)$ and let

$$f(X) = x_{12}^p - x_{12}.$$

Here, $\mathbf{F}_p$ is the field with p elements, where p is a prime.
Then $f(A - \lambda I) = 0 \forall A \in M_2(\mathbf{F}_p)$. But $det(X) = x_{11}x_{22} - x_{12}x_{21}$ does not divide $f(X)$, since $f(X)$ does not involve $x_{11}x_{22}, x_{21}$. Hence, the converse is not true for $\mathbf{F}_p$.

Let us give a slightly more non-trivial example for matrices over $\mathbf{F}_2$.

Example : Let $f(X) = (x_{12} + x_{21})x_{11}x_{22}$. Let $A \in M_2(\mathbf{F}_2)$. Then

$$f(A - \lambda I) = (a_{12} + a_{21})(a_{11} - \lambda)(a_{22} - \lambda)$$

$$= (a_{12} + a_{21})a_{11}a_{22} - (a_{12} + a_{21})(a_{11} + a_{22})\lambda + (a_{12} + a_{21})\lambda^2.$$

We claim that

$$(a_{12} + a_{21})a_{11}a_{22}I - (a_{12} + a_{21})(a_{11} + a_{22})A + (a_{12} + a_{21})A^2 = 0 \cdots (2)$$

for each A. To see this, suppose $a_{12} + a_{21} \neq 0$ in $\mathbf{F}_2$ (for otherwise our claim is true). Now there may be three cases :

- $a_{11} = a_{22} = 0$; here, we must have $A^2 = 0$.

- $a_{11} = a_{22} = 1$; it is easily checked that $A^2 = I$ in this case. Hence, $I + A^2 = I + I = 0$.
- $a_{11} + a_{22} = 1$; here again, one can check that $A^2 = A$.

Thus, in all cases, (2) is satisfied.

But $det(X) = x_{11}x_{22} - x_{12}x_{21}$ does not divide $f(X) = (x_{12} + x_{21})x_{11}x_{22}$ since $f(X)$ does not involve the term $x_{12}x_{21}$, while $det(X)$ does.

We shall now consider the field of complex numbers or, more generally, the following kind of fields.

Definition : A field K is said to be algebraically closed, if any non-constant polynomial $f(x) \in K[x]$ has a root in K.
Note that if K is algebraically closed, all roots of $f(x)$ are in K. This follows from the remainder theorem, on using induction.

In fact, we will prove that the converse statement to the Cayley-Hamilton theorem, as asserted above, is indeed true for any algebraically closed field. For proving this, we will use some commutative algebra; in particular, we shall make use of a fundamental theorem of Hilbert.

Some Commutative Algebra

Recall that an ideal I of a ring R is dened to be an additive subgroup of the ring, such that $rI \subset I \forall r \in R$. For example, nZ is an ideal of Z for any $n \in Z$.In the ring of polynomials, the polynomials with constant term 0 is an ideal. The whole ring is an ideal in any ring. In aring R containing a multiplicative unity 1, an ideal is proper (i.e. not the whole) if, and only if, 1 is not in it.

Definition: Let J be a proper ideal of $K[x_1, \cdots, x_n]$. The *variety* V(J) is defined to be the set of n-tuples $a = (a_1, \cdots, a_n)) \in K^n$, where every polynomial contained in J vanishes. That is,

$$V(J) = \{a \in K^n : f(a) = 0 \forall f \in J\}.$$

Definition: The *radical* of an ideal J in a ring R is defined to be the set

$$rad(J) = \{f \in R : \exists n \ \ with \ \ f^n \in J\}.$$

Note that rad(J) is an ideal of R. This follows, because if $x^n, y^m \in J$, then $(x+y)^{m+n} \in J$, and $(ax)^n \in J$.

If $f \in rad(J) \subset K[x_1, \cdots, x_n]$, then for some k, we have $f^k(a) = 0 \forall a \in V(J)$. Hence, $f(a) = 0 \forall a \in V(J)$. The following fundamental theorem of Hilbert, called the Nullstellensatz[2] asserts that the converse is also true for if K is algebraically closed.

Hilbert's Nullstellensatz:
Given an algebraically closed field K, a non-zero proper ideal $J \subset K[x_1, \cdots, x_n]$, and $f \in K[x_1, \cdots, x_n]$,

$$f(a) = 0 \forall a \in V(J) \Leftrightarrow f \in rad(J).$$

A weaker version of the nullstellensatz is the statement that for any ideal $J \neq K[x_1, \cdots, x_n]$, the variety $V(J)$ is non-empty. For $n = 1$, this is evidently the property of being algebraically closed that was defined. A detailed account of Hilbert's nullstellensatz is given in [2]. One may also refer to [1].

Definition: An ideal $J \subset R$ is called a prime ideal of a ring R, if $ab \in J \Rightarrow a \in J$ or $b \in J$.
For example, pZ is a prime ideal of Z for any prime number p. The only other prime ideal in Z is $\{0\}$. Moreover, in Z, any prime number p is characterized by either of the two properties :
(a) $p|ab \Rightarrow p|a$ or $p|b$.
(b) $p = uv \Rightarrow p = \pm u$ or $p = \pm v$.

In a general integral domain (this is a ring in which the product of two non-zero elements is never zero), one has to make a distinction between these properties. For example, as shown below, the two properties are not equivalent in the ring $A = \{a + b\sqrt{3}i : a, b \in Z\}$.

Definition: Let R be an integral domain.
An element $p \in R$ is called a prime element, if it is not a unit and $p|ab \Rightarrow p|a$ or $p|b$.
An element $d \in R$ is called irreducible, if it is not a unit and any expression $d = pq$ implies that either p or q is a unit in R. Here, a unit is an element

[2] It is a German word, meaning 'Theorem on position of Zeroes.'

$u \in R$ which has a multiplicative inverse in R, i.e. $\exists v \in R$, such that $uv = 1$ in R. The only units in Z are ±1.

In any integral domain, it is very easy to see that prime elements are irreducible. As remarked above, the converse is not true, in general. For instance, in the ring $A = \{a + b\sqrt{3}i : a, b \in Z\}$, the element $1 + \sqrt{3}i$ is easily shown to be irreducible. However, it is not prime since it divides $2.2 = 4 = (1 + \sqrt{3}i)(1 - \sqrt{3}i)$ but does not divide 2, which can also be verified easily.

Definition: An integral domain A is called a *unique factorisation domain* (abbreviated UFD), if every element $a \in A$ can be expressed as a product of irreducibles, up to units, that is, $a = up_1p_2 \cdots p_k$, where u is unit and p_i's are irreducibles in A and the expression is unique in the following sense:
If $a = up_1 \cdots p_k = vq_1 \cdots q_l$, then $k = l$, and $p_i = w_i q_j$, where w_i is a unit. For example, Z is a UFD,since any integer can be written uniquely as a product of primes (or irreducibles) upto sign.

The importance of UFD's stems from the following fact. Consider $\zeta = e^{2i\pi/p}$, where p is an odd prime number. Look at the commutative ring R consisting of all complex numbers of the form $\sum_{r=0}^{s} a_r \zeta^r$. If this ring were a UFD, then Fermat's last theorem would follow for this prime p quite easily. The fact that this ring is not a UFD for many pis the basic reason behind Fermat's last theorem being a deep problem.

Let us look at the polynomial ring $K[x]$, where K is any field. As K is a field, one can easily see that any element $f(x) \in K[x]$ can be written as $f(x) = uf_1(x)f_2(x) \cdots f_k(x)$; where $u \in K$ and f_i's are irreducibles in $K[x]$. To see this, note that any polynomial of degree 1 is irreducible. We assume that all polynomials of degree less than n can be written as a product of irreducibles. Now, if a polynomial of degree n is not itself irreducible, then it can be written as a product of two polynomials of lesser degree. Hence, by induction on degree, any polynomial can be written as a product of irreducible polynomials in $K[x]$. Also, note that any ideal of K[x] is generated by a single element. This can be seen by observing that the element of smallest degree in any ideal must divide all other elements in that ideal. Now, if f_i is an irreducible polynomial in K[x], note that the ideal (f_i) cannot be contained in any proper ideal of K[x]. This follows, because

$(f_i) \subseteq (\alpha) \Rightarrow f_i = \alpha g \Rightarrow g$ is constant $\Rightarrow (\alpha) = (f_i)$.
Now, suppose for some irreducible polynomial $f \in K[x]$, we have $f|ab$, $a, b \in K[x]$. That is, $ab \in (f)$. If $a \notin (f)$, we have $(f, a) = K[x]$. Hence, we can write $1 = fg_1 + ag_2$. Thus, $b = fbg_1 + abg_2 \in (f)$. Therefore, $f|b$. Hence, f is a prime in $K[x]$. Now, given some polynomial $f \in K[x]$, suppose it has two expansions into irreducibles, say

$$f = up_1p_2 \cdots p_r = q_1q_2 \cdots q_s,$$

where p_i's and q_j's are irreducibles in $K[x]$ and $u \in K$. We saw above that all irreducible polynomials in K[x] are prime elements. Hence, each p_i divides q_j for some j. Since q_j's are irreducible, it follows that $q_j = ap_i$,where a is a unit. Thus, we must have that the expansion of f into irreducibles is unique. Hence, K[x] is a UFD.

A famous theorem of Gauss implies that $K[x_1, \cdots, x_n]$ is also a UFD.

Gauss's Theorem: R[x] is a UFD,ifand only if R is a UFD. For a proof of Gauss's theorem and a detailed proof of the fact that K[x] isa UFD, look at [3].

Corollary: Let K be a field. Then $K[x_1, \cdots, x_n]$ is a UFD.
Proof: We have already seen that, for any field K, $K[x]$ is a UFD. The rest follows by induction and the fact that if R is a UFD, then so is $R[x]$. Thus, assuming that $K[x_1, \cdots, x_n]$ is a UFD,we get that $K[x_1, \cdots, x_n] = K[x_1, \cdots, x_{n-1}][x_n]$ is a UFD.

Converse to Cayley-Hamilton Theorem

We now proceed to prove the converse of Cayley-Hamilton theorem for an algebraically closed field. The result is known even for infinite integral domains and the reader who wants to investigate further may consult [4].

Main Theorem :
Let K be an algebraically closed field, $f \in K[x_{11}, x_{12}, \cdots, x_{nn}]$. Let $A \in M_n(K)$ and let f_i's be defined as

$$f(A - \lambda I) = f_0(A) + f_1(A)\lambda + \cdots + f_d(A)\lambda^d.$$

Now, if, for all $A \in M_n(K)$, we have the relation

$$f_0(A)I + f_1(A)A + \cdots + f_d(A)A^d = 0 \in M_n(K),$$

then $f(X) = g(X)det(X) \forall X \in M_n(K)$ for some $g \in K[x_{11}, x_{12}, \cdots, x_{nn}]$.
Proof :
Let $I = (det(X))$ be the ideal of $K[x_{11}, x_{12}, \cdots, x_{nn}]$ generated by $det(X)$. Then,

$$V(I) = \{X \in M_n(K) : det(X) = 0\}.$$

Hence, any matrix $A \in V(I)$ is singular. That is, $\exists 0 \neq v \in K^n$, such that $A.v = 0$. Thus, we have

$$f_0(A)I.v = 0 \Rightarrow f_0(A) = 0.$$

But we saw earlier that $f(A) = f_0(A)$. Hence, $f(A) = 0 \forall A \in V(I)$. Thus, by Hilbert's nullstellensatz, $f \in rad(I)$.
We shall show that f itself is in I.

Claim : $I = (det(X))$ is a prime ideal of $K[x_{11}, x_{12}, \cdots, x_{nn}]$.

Note that, it follows from the denition of a prime ideal, that for any prime ideal P of R, we have $rad(P) = P$ (since $f^n \in P \Rightarrow f \in P$).

Proof of Claim: Since, by Gauss's theorem, $K[x_{11}, x_{12}, \cdots, x_{nn}]$. is a UFD, it is enough to show that $det(X)$ is an irreducible element. Suppose, on the contrary, that $det(X) = \alpha(X)\beta(X)$, for some $\alpha, \beta \in K[x_{11}, x_{12}, \cdots, x_{nn}] \setminus K$. As α is not constant, it involves x_{ij} for some i, j. Since $det(X)$ is row-linear, $det(X)$ does not involve terms of the form $x_{ij}x_{kj}$ for any k. Hence, the variables $x_{1j}, x_{2j}, \cdots, x_{nj}$ cannot occur in β. Thus, α must involve all of these. Again, since $det(X)$ is column-linear, we get similarly that α involves all the x_{ij}'s. That is, $\beta \in K$ a contradiction. Hence $det(X)$ is irreducible in $K[x_{11}, x_{12}, \cdots, x_{nn}]$.

Every Polynomial Identity is a Consequence of C-H

Apart from its evident role as the polynomial carrying information about the eigenvalues of a given matrix, the Cayley-Hamilton theorem has also another more universal role. We shall explain this, to put it in the right perspective.

Any two diagonal matrices with complex entries evidently commute. This can be viewed as saying that when one looks at the polynomial $f(x, y) = xy - yx$ in noncommuting variables x, y, wehave $f(A; B) = 0$ for any two diagonal matrices $A, B \in M_n(C)$.

Similarly, if one considers the polynomial $g(xy) = (xy - yx)^n$ in noncommuting variables x, y, then $g(U, V) = 0$ for any two upper triangular matrices $U, V \in M_n(C)$. One can think of these statements as saying that the sets T_n of diagonal matrices and B_n of upper triangular matrices satisfy some polynomial identities. The set $M_n(C)$ of $n \times n$ complex matrices and the sets T_n, B_n are examples of algebras over C. In fact, they are examples of algebras satisfying a polynomial identity or PI-algebras.

Indeed, $M_n(C)$ satisfies the standard polynomial of degree $2n$ viz.,

$$F(x_1, x_2, \cdots, x_n) = \sum_{\sigma \in S_{2n}} sgn(\sigma) x_{\sigma 1} \cdots x_{\sigma n}.$$

Further, $M_n(C)$ does not satisfy any polynomial identity of lower (than $2n$) degree. This is the assertion of a famous theorem of Amitsur and Levitskii [5]. This is rather tricky to prove but can be done by starting with the Cayley-Hamilton theorem and using the multilinearization technique as indicated below ([6], p.173 for a proof).

Given a permutation $\sigma \in S_r$, if we write its cycle decomposition (including all 1-cycles also) as

$$(a_1, \cdots, a_{k1})(b_1, \cdots, b_{k2}) \cdots,$$

then one can look at the function

$$F_\sigma : M_n(C)^r \to C$$

defined by

$$F_\sigma(A_1, \cdots, A_r) = tr(A_{a_1} \cdots A_{a_{k1}}) tr(A_{b_1} \cdots A_{b_{k2}}) \cdots$$

It is a fact that if $r \geq n + 1$, then the function $F_r := \sum_{\sigma \in S_r} sgn(\sigma) F_\sigma : M_n(C)^r \to C$ is identically zero. This can be seen as follows. For simplicity, let us illustrate it first for n=2. The Cayley-Hamilton theorem gives us $A^2 - tr(A)A + det(A) = 0$. We can rewrite the determinant as $det(A) = \frac{tr(A)^2 - tr(A^2)}{2}$ since

$$det(A) = \lambda_1 \lambda_2 = \frac{(\lambda_1 + \lambda_2)^2 - (\lambda_1^2 + \lambda_2^2)}{2},$$

where λ_1, λ_2 are the eigenvalues of A. On bilinearizing this form, we have the bilinear form of Cayley-Hamilton theorem for 2 × 2 matrices viz.,

$$A_1A_2 + A_2A_1 - tr(A_1)A_2 - tr(A_2)A_1 + tr(A_1)tr(A_2)I - tr(A_1A_2)I = 0.$$

One can multiply by any A_3 on the right and take traces to get (in our earlier notation) that $F_3 : M_2(C)^3 \to C$ is identically zero. One can similarly, get $F_r = 0$ on $M_2(C)^r$ for all $r \geq 3$ and then on, show that $F_r = 0$ on $M_n(C)^r$ for all $r \geq n + 1$.

An important theorem due, independently, to Procesi and Razmyslov [7] asserts that all polynomial identities are consequences of the identities $F_r = 0, r \geq n + 1$. In other words, *all polynomial identities on $n \times n$ complex matrices are consequences of the Cayley-Hamilton theorem.*

Suggested Reading :

[1] M Reid, Undergraduate Commutative Algebra, London Mathematical Society Student Texts, 1995.
[2] V Pati, Hilbert's Nullstellensatz and the Beginning of Algebraic Geometry, Resonance, Vol. 4, No. 8, August, p. 70, 1999.
[3] C Musili, Introduction to Rings and Modules, Narosa Publishers, 1997.
[4] C Chicone, N T Kalton and I J Papick, American Math.Monthly, Vol.92, 1985.
[5] S Amitsur and J Levitzki, Minimal identities for algebras, Proc. Amer. Math. Society, Vol.1, 449-463, 1950.
[6] L H Rowen, Ring theory II, Academic Press, 1988.
[7] E Formanek, Polynomial identities and the Cayley-Hamilton theorem, Math. Intelligencer, Vol.11, 1989.