NOTES

Edited by **William Adkins**

The Fundamental Theorem of Algebra and Linear Algebra

Harm Derksen

1. INTRODUCTION. The first widely accepted proof of the fundamental theorem of algebra was published by Gauss in 1799 in his Ph.D. thesis, although by today's standards this proof has gaps. In 1814 Argand gave a proof (with only small gaps) that was based on a flawed 1746 proof of d'Alembert. Many other proofs followed, including three more by Gauss. For more about the history of the fundamental theorem of algebra, see [**5**] or [**6**].

Proofs of the fundamental theorem of algebra can be divided roughly into three categories (see [**3**] for a collection of proofs). First there are the *topological proofs* (see [**1**] or [**8**]). These proofs are based on topological considerations such as the winding number of a curve in $\mathbb{R}^2$ around 0. Gauss's original proof might fit under this heading as well. Then there are *analytical proofs* (see [**9**]), which are related to Liouville's theorem: a nonconstant entire function on $\mathbb{C}$ is unbounded. Finally, there are the *algebraic proofs* (see [**4**] or [**10**]). These proofs use only the fact that every polynomial of odd degree with real coefficients has a real root and that every complex number has a square root. The deeper reasons why these arguments work can be understood in terms of Galois theory.

Since the fundamental theorem of algebra is needed in linear algebra courses, it would be desirable to have a proof of it in terms of linear algebra. In this paper we prove that every square matrix with complex coefficients has an eigenvector. This statement is equivalent to the fundamental theorem of algebra. In fact, we will prove the slightly stronger result that any number of commuting square matrices with complex entries have a common eigenvector. The proof lies entirely within the framework of linear algebra, and unlike most other algebraic proofs of the fundamental theorem of algebra, it does not require Galois theory or splitting fields. Another (but longer) proof using linear algebra can be found in [**7**].

2. PRELIMINARIES. For the proof we use only the following elementary properties of real and complex numbers.

Lemma 1. *Every polynomial of odd degree with real coefficients has a zero.*

Proof. It is enough to prove that a monic polynomial

$$P(x) = x^n + a_1x^{n-1} + \cdots + a_n$$

with $a_1, \ldots, a_n$ in $\mathbb{R}$ and n odd has a zero. If $a = |a_1| + \cdots + |a_n| + 1$, then it is easy to see that $P(a) > 0$ and $P(-a) < 0$. By the intermediate value theorem there exists λ in the interval $[-a, a]$ such that $P(\lambda) = 0$. ∎

Lemma 2. *Every complex number has a square root.*

Proof. Consider $\alpha + \beta i$ with α and β real. If $\gamma = \sqrt{\alpha^2 + \beta^2}$, then

$$\left(\sqrt{\frac{\gamma+\alpha}{2}} + \sqrt{\frac{\gamma-\alpha}{2}}\,i\right)^2 = \alpha + \beta i. \qquad \blacksquare$$

3. THE PROOF. For a field K and for positive integers d and r, consider the following statement:

$\mathcal{P}(K, d, r)$: *Any r commuting endomorphisms $A_1, A_2, \ldots, A_r$ of a K-vector space V of dimension n such that d does not divide n have a common eigenvector.*

Lemma 3. *If $\mathcal{P}(K, d, 1)$ holds, then $\mathcal{P}(K, d, r)$ holds for all $r \geq 1$.*

Proof. We prove the lemma by induction on r.

Assume that $\mathcal{P}(K, d, r-1)$ holds. Suppose that $A_1, A_2, \ldots, A_r$ are commuting endomorphisms of a K-vector space V of dimension n such that d does not divide n. By induction on n we prove that $A_1, A_2, \ldots, A_r$ have a common eigenvector. The case $n = 1$ is trivial.

Because $\mathcal{P}(K, d, 1)$ holds, A_r has an eigenvalue λ in K. Let W be the kernel and Z the image of $A_r - \lambda I$. Note that W and Z are stable under $A_1, A_2, \ldots, A_{r-1}$.

Suppose that $W \neq V$. Because $\dim W + \dim Z = \dim V$, either d does not divide $\dim W$ or d does not divide $\dim Z$. Since $\dim W < n$ and $\dim Z < n$, we may assume by induction on n that $A_1, \ldots, A_r$ already have a common eigenvector in W or in Z.

In the remaining case, $W = V$. Because $\mathcal{P}(K, d, r-1)$ holds, we may assume that $A_1, \ldots, A_{r-1}$ have a common eigenvector in V, say v. Since $A_r v = \lambda v$, v is a common eigenvector of $A_1, \ldots, A_r$. $\blacksquare$

Lemma 4. *$\mathcal{P}(\mathbb{R}, 2, r)$ holds for all r, i.e., if $A_1, \ldots, A_r$ are commuting endomorphisms on an odd dimensional $\mathbb{R}$-vector space, then they have a common eigenvector.*

Proof. By Lemma 3 it is enough to show that $\mathcal{P}(\mathbb{R}, 2, 1)$ is true. If A is an endomorphism of an odd dimensional $\mathbb{R}$-vector space, then $\det(xI - A)$ is a polynomial of odd degree, which has a zero λ by Lemma 1. Then λ is a real eigenvalue of A. $\blacksquare$

Lemma 5. *$\mathcal{P}(\mathbb{C}, 2, 1)$ holds, i.e., every endomorphism of a $\mathbb{C}$-vector space of odd dimension has an eigenvector.*

Proof. Suppose that $A : \mathbb{C}^n \to \mathbb{C}^n$ is a $\mathbb{C}$-linear map with n odd. Let V be the $\mathbb{R}$-vector space $\mathrm{Herm}_n(\mathbb{C})$, the set of $n \times n$ Hermitian matrices. We can define commuting endomorphisms L_1 and L_2 of V by

$$L_1(B) = \frac{AB + BA^\star}{2}$$

and

$$L_2(B) = \frac{AB - BA^\star}{2i}.$$

Here $A^\star = \overline{A}^t$ is the transpose of the complex conjugate of the matrix A.

Observe that $\dim_{\mathbb{R}} V = n^2$ is odd. Now $\mathcal{P}(\mathbb{R}, 2, 2)$ (see Lemma 4) implies that L_1 and L_2 have a common eigenvector B, say $L_1(B) = \lambda B$ and $L_2(B) = \mu B$ with λ and μ real. But then

$$(L_1 + iL_2)(B) = AB = (\lambda + \mu i)B,$$

and any nonzero column vector of B gives an eigenvector for the matrix A. ∎

Lemma 6. *$\mathcal{P}(\mathbb{C}, 2^k, r)$ holds for all k and r.*

Proof. We prove the lemma by induction on k. The case $k = 1$ follows from Lemmas 5 and 3. Assume that $\mathcal{P}(\mathbb{C}, 2^l, r)$ holds for $l < k$. We will establish $\mathcal{P}(\mathbb{C}, 2^k, r)$. In view of Lemma 3, it suffices to prove $\mathcal{P}(\mathbb{C}, 2^k, 1)$. Suppose that $A : \mathbb{C}^n \to \mathbb{C}^n$ is linear, where n is divisible by 2^{k-1} but not by 2^k. Let V be the $\mathbb{C}$-vector space $\mathrm{Skew}_n(\mathbb{C})$, the set of $n \times n$ skew-symmetric matrices with complex entries. Define two commuting endomorphisms L_1 and L_2 of V by

$$L_1(B) = AB - BA^t$$

and

$$L_2(B) = ABA^t.$$

Note that $\dim V = n(n-1)/2$, which ensures that 2^{k-1} does not divide $\dim V$. By $\mathcal{P}(\mathbb{C}, 2^{k-1}, 2)$, L_1 and L_2 have a common eigenvector B, say $L_1(B) = \lambda B$ and $L_2(B) = \mu B$, where λ and μ are now complex numbers. It follows that

$$\mu B = ABA^t = A(AB - \lambda B),$$

so

$$(A^2 - \lambda A - \mu I)B = 0.$$

Let v be a nonzero column of B. Then

$$(A^2 - \lambda A - \mu I)v = 0.$$

By Lemma 3 there is a δ in $\mathbb{C}$ such that $\delta^2 = \lambda^2 + 4\mu$. We can write $(x^2 - \lambda x - \mu) = (x - \alpha)(x - \beta)$, where $\alpha = (\lambda + \delta)/2$ and $\beta = (\lambda - \delta)/2$. We then have

$$(A - \alpha I)w = 0,$$

where $w = (A - \beta I)v$. If $w = 0$, then v is an eigenvector of A with eigenvalue β; if $w \neq 0$, then w is an eigenvector of A with eigenvalue α. ∎

Theorem 7. *If $A_1, A_2, \ldots, A_r$ are commuting endomorphisms of a finite dimensional nonzero $\mathbb{C}$-vector space V, then they have a common eigenvector.*

Proof. Let n be the dimension of V. There exists a positive integer k such that 2^k does not divide n. Since $\mathcal{P}(\mathbb{C}, 2^k, r)$ holds by Lemma 6, the theorem follows. ∎

Corollary 8 (Fundamental Theorem of Algebra). *If $P(x)$ is a nonconstant polynomial with complex coefficients, then there exists a λ in $\mathbb{C}$ such that $P(\lambda) = 0$.*

Proof. It suffices to prove this for monic polynomials. Suppose that

$$P(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_n.$$

Then $P(x) = \det(xI - A)$, where A is the companion matrix of P:

$$A = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_n \\ 1 & 0 & & 0 & -a_{n-1} \\ 0 & 1 & & 0 & -a_{n-2} \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & 1 & -a_1 \end{pmatrix}.$$

Theorem 7 implies that A has a complex eigenvalue λ in $\mathbb{C}$, from which it follows that $P(\lambda) = 0$. ■

Remark. As for all algebraic proofs of the fundamental theorem of algebra, the statement can be generalized to more general fields. An *ordered field* R is a field with the following properties: (i) for every α in $R \setminus \{0\}$, either α or $-\alpha$ is a square and (ii) the sum of any two squares in R is also a square. On such an ordered field there is a total ordering defined by $\alpha \leq \beta$ if and only if $\beta - \alpha$ is a square. If α in R is a square in R, then we define $\sqrt{\alpha}$ to be the unique β in R such that $\beta^2 = \alpha$ and β is itself a square in R. The element -1 is not a square in an ordered field. We can construct a field C by adjoining an element i with $i^2 = -1$ to R in a fashion similar to the way $\mathbb{C}$ is constructed from $\mathbb{R}$. It can be shown (just as for $\mathbb{C}$) that any element of C has a square root. If we assume R is an ordered field such that every polynomial of odd degree has a zero, then the foregoing proof goes through with $\mathbb{R}$ replaced by R and $\mathbb{C}$ replaced by C. In particular, C is algebraically closed.

ACKNOWLEDGMENT. The author was partially supported by NSF Award DMS-0102193.

REFERENCES

1. B. H. Arnold, A topological proof of the fundamental theorem of algebra, this MONTHLY **56** (1949) 465–466.
2. J. L. Brenner and R. C. Lyndon, Proof of the fundamental theorem of algebra, this MONTHLY **88** (1981) 253–256.
3. B. Fine and G. Rosenberger, *The Fundamental Theorem of Algebra*, Springer-Verlag, New York, 1997.
4. L. Horowitz, A proof of the "fundamental theorem of algebra" by means of Galois theory and 2-Sylow groups, *Nieuw Arch. Wisk.* (3) **14** (1966) 95–96.
5. H.-D. Ebbinghaus, H. Hermes, F. Hirzebruch, M. Koecher, K. Mainzer, A. Prestel, and R. Remmert, *Zahlen*, K. Lamotke, ed., Springer-Verlag, Berlin, 1983.
6. C. Gilain, Sur l'histoire du théorème fondamental de l'algèbre: théorie des équations et calcul intégral, *Arch. Hist. Exact Sci.* **42** (1991) 91–136.
7. H.-J. Kowalsky, Zum Fundamentalsatz der Algebra, *Abh. Braunschweig. Wiss. Ges.* **35** (1983) 111–120.
8. S. Stein, The fundamental theorem of algebra, this MONTHLY **61** (1954) 109.
9. F. Terkelsen, The fundamental theorem of algebra, this MONTHLY **83** (1976) 647.
10. H. Zassenhaus, On the fundamental theorem of algebra, this MONTHLY **74** (1967) 485–497.

Department of Mathematics, University of Michigan, East Hall, 525 East University, Ann Arbor, MI 48109-1109
hderksen@umich.edu