Lecture 32 Group Theory and Linear algebra 19.10.2011

(11) Week 1 §2: Show that the field of complex numbers is algebraically closed.

To show: If $f = a_0 + a_1 t + \cdots + a_\ell t^\ell \in \mathbb{C}[t]$

then there exists $\beta_1, \beta_2, \ldots, \beta_\ell \in \mathbb{C}$ such that

$$a_0 + a_1 t + \cdots + a_\ell t^\ell = (t-\beta_1)\cdots(t-\beta_\ell).$$

Proof by induction on ℓ:

Lemma If $f = a_0 + a_1 t + \cdots + a_\ell t^\ell \in \mathbb{C}[t]$

then there exist $\beta \in \mathbb{C}$ and $f_1 = b_0 + b_1 t + \cdots + b_{\ell-1} t^{\ell-1}$ such that

$$f = (t-\beta) f_1$$

Another version of the Lemma is

Lemma If $f = a_0 + a_1 t + \cdots + a_\ell t^\ell \in \mathbb{C}[t]$

then there exists $\beta \in \mathbb{C}$ such that

$$f(\beta) = 0.$$

Examples $\mathbb{R}$ is not algebraically closed:

t^2+1 does not factor in $\mathbb{R}[t]$,

even though $t^2+1 = (t+i)(t-i)$ factors in $\mathbb{C}[t]$.

Theorem If $f = a_0 + a_1 t + \cdots + a_k t^k \in \mathbb{R}[t]$ then there exist $p_1, \ldots, p_r$ with $\deg(p_i)$ equal to 1 or 2 such that

$$f = p_1 p_2 \cdots p_r.$$

This follows from the fundamental theorem of algebra and the fact that

If $f \in \mathbb{R}[t]$ and $\beta \in \mathbb{C}$ such that $f(\beta) = 0$ then $f(\bar{\beta}) = 0$.

So

$$f = (t-\gamma_1)\cdots(t-\gamma_r)(t-\beta_1)(t-\bar{\beta}_1)\cdots(t-\beta_s)(t-\bar{\beta}_s)$$

$$= (t-\gamma_1)\cdots(t-\gamma_r)(t^2-(\beta_1+\bar{\beta}_1)+\beta_1\bar{\beta}_1)\cdots(t-(\beta_s+\bar{\beta}_s)+\beta_s\bar{\beta}_s)$$

with $\gamma_1, \ldots, \gamma_r \in \mathbb{R}$ and $\beta_1, \ldots, \beta_s \in \mathbb{C}$ with $\beta_1, \ldots, \beta_s \notin \mathbb{R}$. Note that $\beta_j + \bar{\beta}_j \in \mathbb{R}$ and $\beta_j \bar{\beta}_j \in \mathbb{R}$.

This theorem is called the fundamental theorem of algebra.
It was first proved by d'Alembert, after which Gauss studied the theorem extensively providing 14 proofs

Further references: Wikipedia - Fundamental Theorem of Algebra
Math Over Flow - Fundamental Theorem of Algebra
Article of Harm Derksen

Theorem $\mathbb{C}$ is algebraically closed

Proof (d'Alembert-Gauss [Bou, Top. Ch VIII §1, no.1, Theorem 1].
Bourbaki define $\mathbb{C}$ as $\mathbb{R}[X]/(X^2+1)$.
To show: (a) If $a \in \mathbb{R}_{\geq 0}$ then there exists $\sqrt{a} \in \mathbb{R}$.

(b) If $p(t) \in \mathbb{R}[t]$ and $\deg p$ is odd then there exists $\alpha \in \mathbb{R}$ such that $p(\alpha) = 0$.

(b) Assume $p(t) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0$ with n odd and $a_n \neq 0$.

If $x \in \mathbb{R}^*$ and $x \neq 0$ then

$p(x) = a_n x^n q(x)$, where $q(x) = 1 + \frac{a_{n-1}}{a_n x} + \cdots + \frac{a_0}{a_n x^n}$.

$\lim_{x \to \infty} q(x) = 1$ and $\lim_{x \to -\infty} q(x) = 1$.

So there exists $a \in \mathbb{R}_{>0}$ such that

$\operatorname{sign}(a_n) = \operatorname{sign}(f(a))$ and $\operatorname{sign}(-a_n) = \operatorname{sign}(f(-a))$

Thus, by Bolzano's theorem, [Bou, Top IV §6, no.1 Theorem 2]
there exists $\alpha \in [-a, a]_{\mathbb{R}}$ such that $f(\alpha) = 0$. //

Proof 2 [Bou, Top. Ch VIII §2. Exercise 2]
Let $f(t) \in \mathbb{C}[t]$ such that $f(t) \neq 0$.
To show: there exists $r \in \mathbb{R}_{>0}$ such that
if $z \in \mathbb{C}$ and $|z| \geq r$ then $|f(z)| > |f(0)|$
Use [Exercise 1] and Weierstrass' theorem [Bou, Top. Ch IV §6 no.1, Theorem 1] to show $\mathbb{C}$ is algebraically closed.

[Bou Top. Ch. VIII §2. Exercise 1]

Let $a \in \mathbb{C}$, $a \neq 0$ and $n \in \mathbb{Z}_{>0}$.

To show: If $r \in \mathbb{R}_{>0}$ such that $r^n \leq |a|$
then there exists $z \in \mathbb{C}$ such that $|z| = r$ and
$|a + z^n| = |a| - r^n$.

(b) If $f(t) \in \mathbb{C}[t]$ and $\deg(f) > 0$
and $z_0 \in \mathbb{C}$, with $f(z_0) \neq 0$
then there exists $z \in B_\varepsilon(z_0)$ such that
$|f(z_0)| > |f(z)|$.

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 to current standards this proof has gaps. Argand gave a proof (with only small gaps) in 1814 which was based on a flawed proof of d'Alembert of 1746. Many more proofs followed, including three more proofs by Gauß. For a more about the history of the Fundamental Theorem of Algebra, see [5, 6].

Proofs roughly can be divided up in three categories (see [3] for a collection of proofs). First there are the *topological proofs* (see [1, 8]). These proofs are based on topological considerations such as the winding number of a curve in $\mathbb{R}^2$ around 0. Gauß' original proof might fit in this category as well. Then there are *analytical proofs* (see [9]) which are related to Liouville's result that an entire non-constant function on $\mathbb{C}$ is unbounded. Finally there are the *algebraic proofs* (see [4, 10]). These proofs only use the facts that every odd polynomial with real coefficients has a real root, and that every complex number has a square root. The deeper reasons why these proves work can be understood in terms of Galois Theory.

For a linear algebra course, the Fundamental Theorem of Algebra is needed, so it is therefore desireable to have a proof of it in terms of linear algebra. In this paper we will prove that every square matrix with complex coefficients has an eigenvector. This 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 will have a common eigenvector. The proof is entirely within the framework of linear algebra, and unlike most other algebraic proves 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 will only use the following elementary properties of the real and the 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

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

with $a_1, \ldots, a_n \in \mathbb{R}$ and n odd has a zero. Put $a = |a_1| + \cdots + |a_n| + 1$ 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. Suppose that $\alpha + \beta i \in \mathbb{C}$ with $\alpha, \beta \in \mathbb{R}$. Put $\gamma = \sqrt{\alpha^2 + \beta^2}$, then

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

□

3. The proof of the Fundamental Theorem of Algebra

For a field K, consider the following statement:

$\mathcal{P}(K, d, r)$: *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. Then $A_1, A_2, \ldots, A_r$ 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 $\lambda \in K$. Let W be the kernel, and Z be the image of $A_r - \lambda I$. Note also that W and Z are stable under $A_1, A_2, \ldots, A_{r-1}$.

Suppose that $W \neq V$. Because $\dim W + \dim Z = \dim V$, 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.

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

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 $\mathcal{P}(\mathbb{R}, 2, 1)$. If A is an endomorphism of an odd dimensional $\mathbb{R}$-vector space then $\det(xI - A)$ is an odd polynomial which has a zero λ by Lemma 1. Now λ is a real eigenvalue of A. □

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. Put $V = \mathrm{Herm}_n(\mathbb{C})$, the set of $n \times n$ Hermitian matrices. One can check that we can define commuting endomorphisms L_1, L_2 of V by

$$L_1(B) = \frac{AB + B\overline{A}^t}{2}$$

and

$$L_2(B) = \frac{AB - B\overline{A}^t}{2i}.$$

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

Note 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 $\lambda, \mu \in \mathbb{R}$. But then we have

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

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

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

and

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

Note that $\dim V = n(n-1)/2$ and 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 $L_2(B) = \mu B$ with $\lambda, \mu \in \mathbb{C}$. But then we have

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

so

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

Let v be a nonzero column of B. Then we get

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

By Lemma 3 there is a $\delta \in \mathbb{C}$ 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 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 non-constant polynomial with complex coefficients, then there exists an $\lambda \in \mathbb{C}$ 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

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

Theorem 7 implies that A has a complex eigenvalue $\lambda \in \mathbb{C}$. Then we get $P(\lambda) = 0$. □

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: For every $\alpha \in R \setminus \{0\}$, either α or $-\alpha$ is a square. Also, the sum of any two squares must be 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 $\alpha \in R$ is a square, then we define $\sqrt{\alpha}$ as the unique $\beta \in R$ such that $\beta^2 = \alpha$ and β is a square itself. 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 similar fashion as $\mathbb{C}$ 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 above prove goes through with $\mathbb{R}$ replaced by R and $\mathbb{C}$ replaced by C. In particular C is algebraically closed.

References

[1] B. H. Arnold, *A topological proof of the fundamental theorem of algebra*, Amer. Math. Monthly **56** (1949), 465–466.

[2] J. L. Brenner and R. C. Lyndon, *Proof of the fundamental theorem of algebra*, Amer. Math. Monthly **88** (1981), no. 4, 253–256.

[3] B. Fine and G. Rosenberger, *The fundamental theorem of algebra*, Undergraduate Texts in Mathematics, 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, R. Remmert, *Zahlen*, Edited by K. Lamotke, Grundwissen Mathematik 1, Springer Verlag, Berlin 1983, Chapter 4.
[6] C. Gilain, *Sur l'histoire du théorème fondamental de l'algèbre: théorie des équations et calcul intégral*, Arch. Hist. Exact Sci. **42** (1991), no. 2, 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*, Amer. Math. Monthly **61** (1954), 109.
[9] F. Terkelsen, *The fundamental theorem of algebra*, Amer. Math. Monthly **83** (1976), no. 8, 647.
[10] H. Zassenhaus, *On the fundamental theorem of algebra*, Amer. Math. Monthly **74** (1967), 485–497.