

FUNDAMENTAL THEOREM OF ALGEBRA

ALGIRDAS GRYBAS

CONTENTS

1. Historical overview	1
2. Theoretical background	1
3. Proof of the Fundamental Theorem of Algebra	5
4. Corollaries and Ending Notes	7
References	8

1. HISTORICAL OVERVIEW

Roots of the Fundamental Theorem of Algebra (FTA) can be found in early 1600s, as Petrus Roth in *Arithmetica Philosophica* (1608) asserted that a polynomial equation of degree n (with real coefficients) *may* have n solutions, and Albert Girard in *L'invention nouvelle en l'Algre* (1629) claimed that a polynomial equation of degree n always has n solutions as long as the equation is complete, i.e. no coefficient is equal to 0 (for more historical background please refer to [4, 3]).

Many great mathematicians (Euler, Bernoulli, Leibniz, Lagrange, Laplace and others) were involved in approaching the problems raised by P. Roth and A. Girard, but it was D'Alembert who first made a serious attempt to prove the FTA in 1742, followed immediately by Euler's proof that every real polynomial of degree $n \leq 6$ had exactly n complex roots (see [3]). However, Gauss is usually credited with the first proof of the FTA in his doctoral thesis published in 1799, although his proof also does not meet current standards required for a rigorous proof. In total, Gauss published four proofs of the FTA, but none of them were *constructive* (a constructive proof demonstrates the existence of a mathematical object with certain properties by creating or providing a method for creating such an object). It was only in 1940 that Hellmuth Kneser obtained a constructive proof of the FTA.

2. THEORETICAL BACKGROUND

In order to prove the Fundamental Theorem of Algebra, we will make use of the concepts of field extensions and symmetric polynomials.

Definition 1. If $F \subset F'$ are fields, then F' is an **extension field** of F . F' is then a vector space over F and the **degree of extension** is the dimension of F' as a vector space over F , denoted as $|F' : F|$.

Lemma 1. If $F \subset F' \subset F''$ are fields with F'' a finite extension of F , then $|F' : F|$ and $|F'' : F'|$ are also finite, and $|F'' : F| = |F'' : F'| |F' : F|$.

Proof. The dimension of a subspace must be less than the dimension of the whole vector space, so it is clear that $|F' : F|$ and $|F'' : F'|$ are finite. If $|F' : F| = n$ with $\alpha_1, \dots, \alpha_n$ a basis for F' over F , and $|F'' : F'| = m$ with β_1, \dots, β_m a basis for F'' over F' , then

$$\sum_{i=1}^m f_i'' \beta_i = \sum_{i=1}^m \left(\sum_{j=1}^n (f_j' \alpha_j) \beta_i \right) = \sum_{i,j} (f_{ij}' \alpha_j \beta_i)$$

and so mn products $\{\alpha_j \beta_i\}$ form a basis for F'' over F . \square

Definition 2. Suppose F' is an extension field of F and $\alpha \in F'$. Then α is **algebraic over F** if there exists a polynomial $0 \neq p(x) \in F[x]$ with $p(\alpha) = 0$, i.e. α is a root of a polynomial with coefficients in F . If every element of F' is algebraic over F , then F' is an **algebraic extension** of F .

Lemma 2. Every element of F is algebraic over F .

Proof. Simply if $f \in F$ then $p(x) = 1x - f \in F[x]$, where 1 is the identity element in F . Then obviously $p(f) = 0$. \square

Theorem 1. If F' is a finite extension of F , then F' is an algebraic extension.

Lemma 3. If $\alpha \in F'$ is algebraic over F , then there exists a unique monic ($a_n = 1$) irreducible (i.e. cannot be factorized into polynomials of lower degree) polynomial $p(x) \in F[x]$ such that $p(\alpha) = 0$. It is denoted by $\text{irr}(\alpha, F)$.

Proof. Existence: Suppose $p(\alpha) = 0$ with $0 \neq p(x) \in F[x]$. Then $p(x)$ factors into irreducible polynomials ($(x - \alpha)$ and the remainder from the long division). Since there are no zero divisors in a field, one of these factors, say, $p_1(x)$ must also have α as a root. If the leading coefficient of $p_1(x)$ has a leading coefficient a_n , then $p'(x) = a_n^{-1} p_1(x)$ is a monic irreducible polynomial in $F[x]$ that also has α as a root. Thus, there exist monic irreducible polynomials that have α as a root. Let $p(x)$ be one such polynomial of minimal degree.

Uniqueness: Now suppose $g(x)$ is another monic irreducible polynomial with $g(\alpha) = 0$. Since $p(x)$ has minimal degree, $\deg p(x) \leq \deg g(x)$. From the division of polynomials,

$$g(x) = q(x)p(x) + r(x)$$

¹In such a case, F' is called an **intermediate field** and F is the **ground field**.

where $r(x) \equiv 0$ or $\deg r(x) < \deg p(x)$. Substituting x with α implies that $r(\alpha) = 0$ since $g(\alpha) = p(\alpha) = 0$. But then if $r(x)$ is not identically 0, α is a root of $r(x)$, which contradicts the minimality of the degree of $p(x)$. Therefore, $r(x) = 0$ and $g(x) = q(x)p(x)$. The polynomial $q(x)$ must be constant (unit factor) since $g(x)$ is irreducible, but then $q(x) = 1$ since both $p(x)$, $g(x)$ are monic. Thus, $g(x) = p(x)$ and so $p(x)$ is unique. \square

Proof. Proof of this theorem is given in [1], p. 77. \square

We now show how to actually extend a field, by **adjoining a root** to it.

Definition 3. Suppose $\alpha \in F'$ is algebraic over F and $p(x) = \text{irr}(\alpha, F) = a_0 + a_1x + \dots + a_{n-1}x^{n-1} + x^n$. Let

$$F(\alpha) = \{a_0 + a_1\alpha + \dots + a_{n-1}\alpha^{n-1} \mid a_i \in F\}$$

Then $F(\alpha)$ is an **extension of F by adjoining a root α of $p(x)$ to it**. On $F(\alpha)$ define componentwise addition and subtraction and define multiplication by algebraic multiplication, replacing powers of α greater than n by using

$$\alpha^n = -a_0 - a_1\alpha - \dots - a_{n-1}\alpha^{n-1}$$

Theorem 2. $F(\alpha)$ forms a finite algebraic extension of F with $[F(\alpha) : F] = \deg \text{irr}(\alpha, F)$. $F(\alpha)$ is the smallest subfield of F' that contains the root α . A field extension of the form $F(\alpha)$ for some α is called a **simple extension** of F .

Definition 4. Let F', F'' be extension fields of F . An **F-isomorphism** is an isomorphism $\sigma : F' \rightarrow F''$ such that $\sigma(f) = f$ for all $f \in F$. In other words, **F-isomorphism fixes each element of the ground field**. If F', F'' are F-isomorphic, we denote the relationship by $F' \cong_F F''$.

Theorem 3 (Kronecker's Theorem). Let F be a field and $p(x) \in F[x]$ an irreducible polynomial over F . Then there exists a finite extension F' of F where $p(x)$ has a root. Furthermore, if α is a root in some extension F'' with $\text{irr}(\alpha, F) = p(x)$, then F' is F-isomorphic to $F(\alpha)$.

Proof. To construct the field F' , repeat the construction of $F(\alpha)$ and show that it is a field. \square

We now advance further and prove that there is a field that contains all roots of $p(x)$. For this we need the definition of a splitting field.

Definition 5. If $0 \neq p(x) \in F[x]$ and F' is an extension field of F , then $p(x)$ **splits** in F' if $p(x)$ factors into linear factors in $F'[x]$, i.e.

all roots of $p(x)$ are in F' . F' is then called a **splitting field** for $p(x)$ over F if it is the smallest extension field of F in which $p(x)$ splits.

Theorem 4. *If $0 \neq p(x) \in F[x]$, then there exists a splitting field for $f(x)$ over F .*

Proof. The splitting field is constructed by repeated adjoining of roots. WLOG, suppose that $p(x)$ is irreducible of degree n over F . From Theorem 3 there exists a field F' containing α with $p(\alpha) = 0$. Then $p(x) = (x - \alpha)g(x) \in F'[x]$ with $\deg g(x) = n - 1$. We can repeat the same procedure for $g(x)$, and since n is finite, after finitely many steps we will have reduced $p(x)$ into irreducible nontrivial factors. Then, by extending the field F by adjoining one root at a time of the irreducible factors, we will obtain the splitting field for $p(x)$. \square

Definition 6. *A field F is **algebraically closed** if every non-constant polynomial in $F[x]$ has a root in F .*

We can now state three statements, equivalent to the Fundamental Theorem of Algebra.

Theorem 5.² *Let F be a field. Then the following are equivalent:*

- (1) F is algebraically closed.
- (2) Every non-constant polynomial $p(x) \in F[x]$ splits in $F[x]$.
- (3) F has no proper algebraic extensions, i.e. there is no algebraic field extension E with $F \subset E$ and $F \neq E$.

The last notion before proving the Fundamental Theorem of Algebra is that of permutations and symmetric polynomials.

Definition 7. *If T is a set, a **permutation** on T is a bijective map $\sigma : T \rightarrow T$. We denote S_T the set of all such permutations on T .*

Definition 8. *Let y_1, \dots, y_n be (independent) unknowns over a field F . A polynomial $f(y_1, \dots, y_n) \in F[y_1, \dots, y_n]$ is a **symmetric polynomial** in y_1, \dots, y_n if $f(y_1, \dots, y_n)$ is unchanged by any permutation σ of $\{y_1, \dots, y_n\}$, i.e. $f(y_1, \dots, y_n) = f(\sigma(y_1), \dots, \sigma(y_n))$*

Definition 9. *Let x, y_1, \dots, y_n be unknowns over a field F . Construct a polynomial*

$$p(x, y_1, \dots, y_n) = (x - y_1) \cdots (x - y_n)$$

*The **i th elementary symmetric polynomial** s_i in y_1, \dots, y_n for $i = 1, \dots, n$ is $(-1)^i a_i$, where a_i is the coefficient of x^{n-i} in $p(x, y_1, \dots, y_n)$.*

The following theorem is called the Fundamental Theorem of Symmetric Polynomials, the proof of which is beyond the scope of this paper, from which two very important lemmas derive.

²Proof of this theorem is given in [1], p. 85

Theorem 6 (Fundamental Theorem of Symmetric Polynomials). *If P is a symmetric polynomial in the unknowns y_1, \dots, y_n over F , then there exists a unique $g \in F[y_1, \dots, y_n]$ such that $f(y_1, \dots, y_n) = g(s_1, \dots, s_n)$. That is, any symmetric polynomial in y_1, \dots, y_n is a polynomial expression in the elementary symmetric polynomials in y_1, \dots, y_n .*

Lemma 4. *Let $p(x) \in F[x]$ and suppose $p(x)$ has roots $\alpha_1, \dots, \alpha_n$ in the splitting field F' . Then the elementary symmetric polynomials in $\alpha_1, \dots, \alpha_n$ are in F .*

Proof. Suppose $p(x) = a_0 + a_1x + \dots + a_nx^n \in F[x]$. $p(x)$ splits in $F'[x]$ with roots $\alpha_1, \dots, \alpha_n$, so

$$p(x) = a_n(x - \alpha_1) \cdots (x - \alpha_n)$$

The coefficients are then $a_n(-1)^i s_i(\alpha_1, \dots, \alpha_n)$. However, $p(x) \in F[x]$, so each coefficient is in F . Since $a_n \in F$, $s_i(\alpha_1, \dots, \alpha_n) \in F$. \square

Lemma 5. *Let $p(x) \in F[x]$ and suppose $p(x)$ has roots $\alpha_1, \dots, \alpha_n$ in the splitting field F' . Suppose further that $g(x) = g(x, \alpha_1, \dots, \alpha_n) \in F'[x]$ and symmetric, then $g(x) \in F[x]$.*

Proof. If $g(x) = g(x, \alpha_1, \dots, \alpha_n)$ is symmetric in $\alpha_1, \dots, \alpha_n$, then from Theorem 6 it is a symmetric polynomial in the elementary symmetric polynomials in $\alpha_1, \dots, \alpha_n$. From Lemma 4 these are in the ground field F , so the coefficients of $g(x)$ are in F . Therefore, $g(x) \in F[x]$. \square

3. PROOF OF THE FUNDAMENTAL THEOREM OF ALGEBRA

We now prove the Fundamental Theorem of Algebra.

Theorem 7 (Fundamental Theorem of Algebra). *Any non-constant complex polynomial has a complex root. Equivalently, the complex field \mathbb{C} is algebraically closed.*

The proof follows from four lemmas.

Lemma 6. *Any odd-degree real polynomial has a real root.*

Proof. Recall the Intermediate Value Theorem: *Let $f : [a, b] \rightarrow \mathbb{R}$ be continuous with $f(a) \neq f(b)$. Then for each d , $f(a) < d < f(b)$ there exists $c \in (a, b)$ such that $f(c) = d$.* Suppose $p(x) \in \mathbb{R}[x]$ is a polynomial with $\deg p(x) = n = 2k + 1$ and suppose that the leading coefficient $a_n > 0$ (the proof for $a_n < 0$ is analogous). Then $p(x) = a_nx^n + o(x^{n-1})$ and n is odd. Then

$$(1) \quad \lim_{x \rightarrow \infty} p(x) = \lim_{x \rightarrow \infty} a_nx^n = \infty \text{ since } a_n > 0.$$

$$(2) \quad \lim_{x \rightarrow -\infty} p(x) = \lim_{x \rightarrow -\infty} a_nx^n = -\infty \text{ since } a_n > 0 \text{ and } n \text{ is odd.}$$

From 1, there exists x_1 with $p(x_1) > 0$. On the other hand, from 2 it follows the existence of x_2 such that $p(x_2) < 0$. A real polynomial is a continuous real-valued function on all $x \in \mathbb{R}$, and since $p(x_1)p(x_2) < 0$, it follows from the Intermediate Value Theorem that there exists an x_3 between x_1 and x_2 such that $p(x_3) = 0$. \square

The next lemma establishes the existence of a complex root for degree-two polynomials.

Lemma 7. *Any degree-two complex polynomial has a complex root.*

Proof. This is just a quadratic formula. If $az^2 + bz + c = p(z) \in \mathbb{R}[z]$, then the roots formally are

$$z_1 = \frac{-b + \sqrt{b^2 - 4ac}}{2a}, \quad z_2 = \frac{-b - \sqrt{b^2 - 4ac}}{2a}$$

From DeMoivre's theorem, every complex number has a square root, so z_1, z_2 exist in \mathbb{C} (may be the same). \square

We now move on and prove that every complex polynomial must have a complex root.

Lemma 8. *If every non-constant real polynomial has a complex root, then every non-constant complex polynomial has a complex root.*

Proof. Let $p(x) \in \mathbb{C}[x]$ and suppose that every non-constant real polynomial has at least one complex root. Let $h(x) = p(x)\bar{p}(x)$. Then

$$\bar{h}(x) = \overline{p(x)\bar{p}(x)} = \bar{p}(x)\overline{\bar{p}(x)} = \bar{p}(x)p(x) = p(x)\bar{p}(x) = h(x)$$

Hence $h(x) \in \mathbb{R}[x]$. By assumption there exists $z_0 \in \mathbb{C}$ with $h(z_0) = 0$. Then $p(z_0)\bar{p}(z_0) = 0$, and since \mathbb{C} has no zero divisors, either $p(z_0) = 0$ or $\bar{p}(z_0) = 0$. Then either z_0 is a root of $p(x)$ or $\bar{p}(z_0) = \bar{p}(\bar{z}_0) = p(\bar{z}_0) = 0$ and so \bar{z}_0 is a root of $p(x)$. \square

We now come to the final lemma that uses all the concepts covered so far and finally proves the Fundamental Theorem of Algebra.

Lemma 9. *Any non-constant real polynomial has a complex root.*

Proof. Let $a_0 + a_1x + \cdots + a_nx^n = p(x) \in \mathbb{R}[x]$ with $n \geq 1$, $a_n \neq 0$. Suppose $n = 2^mq$, where q is odd. We do the induction on m .

Case 1: $m = 0$. $p(x)$ has an odd degree and so the theorem follows from Lemma 6.

Case 2: $m > 0$. Assume that the theorem is true for all degrees $d = 2^kq'$, $k < m$ and q' is odd (inductive hypothesis), and consider $p(x)$ of degree $n = 2^mq$.

Suppose F' is the splitting field for $f(x)$ over \mathbb{R} in which the roots are $\alpha_1, \dots, \alpha_n$. Existence of such field follows from Theorem 2. We show that at least one of these roots must be in \mathbb{C} (in fact, all are in \mathbb{C} but to prove the lemma we need only show at least one).

Let $h \in \mathbb{Z}$ and construct the polynomial

$$H(x) = \prod_{i < j} (x - (\alpha_i + \alpha_j + h\alpha_i\alpha_j))$$

Since $\alpha_1, \dots, \alpha_n \in F'$, it follows from Definition 5 that $H(x) \in F'[x]$. The number of pairs of roots $\{\alpha_i, \alpha_j\}$ is

$$\binom{n}{2} = \frac{n!}{(n-2)!2!} = \frac{n(n-1)}{2} = \frac{(2^m q)(2^m q - 1)}{2} = 2^{m-1} q(2^m q - 1) = 2^{m-1} q'$$

where q' is odd. Thus, the degree of $H(x)$ is $2^{m-1} q'$.

$H(x)$ is symmetric polynomial, since it does not depend on the order we choose α_i, α_j , and so, by Lemma 5, $H(x) \in \mathbb{R}[x]$. By inductive hypothesis, $H(x)$ must have a complex root, what implies from our construction of $H(x)$ the existence of a pair $\{\alpha_i, \alpha_j\}$ with

$$\alpha_i + \alpha_j + h\alpha_i\alpha_j \in \mathbb{C}$$

Since h was arbitrary, this holds for any $h' \in \mathbb{Z}$. Let h' vary over integers. Since there are only finitely many such pairs $\{\alpha_i, \alpha_j\}$, it follows that there must be at least two different integers h', h'' such that

$$z_1 = \alpha_i + \alpha_j + h'\alpha_i\alpha_j \in \mathbb{C} \text{ and } z_2 = \alpha_i + \alpha_j + h''\alpha_i\alpha_j \in \mathbb{C}$$

Then $z_1 - z_2 = (h' - h'')\alpha_i\alpha_j \in \mathbb{C}$ and since $h', h'' \in \mathbb{Z} \subset \mathbb{C}$, $\alpha_i\alpha_j \in \mathbb{C}$. But then $h'\alpha_i\alpha_j \in \mathbb{C} \Rightarrow \alpha_i + \alpha_j \in \mathbb{C}$. Then

$$p(x) = (x - \alpha_i)(x - \alpha_j) = x^2 - (\alpha_i + \alpha_j)x + \alpha_i\alpha_j \in \mathbb{C}[x]$$

But then $\deg p(x) = 2$ and so from Lemma 7 its roots are complex. Therefore, $\alpha_i, \alpha_j \in \mathbb{C}$ and so $f(x)$ has a complex root. \square

Now Lemma 9 implies that Lemma 8 implies the Fundamental Theorem of Algebra.

4. COROLLARIES AND ENDING NOTES

The Fundamental Theorem of Algebra has numerous applications and corollaries, the most famous of which are the following.

Theorem 8 (Factorization of Complex Polynomials). *A complex polynomial completely factorizes into linear factors.*

Proof. Let $p(x) \in \mathbb{C}[x]$ and use the induction on the degree. The theorem is clearly true if $\deg p(x) = 1$, since then $p(x)$ is itself linear. So suppose $\deg p(x) = n$. From the Fundamental Theorem of Algebra, there exists a root α , and therefore $(x - \alpha)$ divides $p(x)$. Hence $p(x) = (x - \alpha)g(x)$ with $\deg g(x) < n$. From the inductive hypothesis, $g(x)$ factors into linear factors, so therefore $p(x)$ does also. \square

Theorem 9. *Suppose $p(x) \in \mathbb{C}[x]$ with $\deg p(x) = n$. Suppose the roots of $p(x)$ are $\alpha_1, \dots, \alpha_n$ (may be repeated), then*

$$p(x) = a_n(x - \alpha_1) \cdots (x - \alpha_n), a_n \in \mathbb{C}$$

Theorem 10 (Factorization of Real Polynomials). *A real polynomial factorizes into degree 1 and degree 2 factors. Equivalently, the only irreducible real polynomials are linear polynomials and quadratic polynomials without real roots.*

Proof. Suppose $p(x) \in \mathbb{R}[x]$, then $p(x) \in \mathbb{C}[x]$. Suppose z_1, \dots, z_n are its complex roots, so that

$$p(x) = a_n(x - z_1) \cdots (x - z_n)$$

where $a_n \in \mathbb{R}$. If z_i are real, then $(x - z_i)$ is a real linear factor. If $z_i \notin \mathbb{R}$, then its complex conjugate \bar{z}_i is also a root. But then $(x - z_i)(x - \bar{z}_i)$ is a real factor of degree 2. \square

Theorem 11. *An irreducible real polynomial must be of degree 1 or 2.*

REFERENCES

- [1] Fine B., Rosenberger G. *The Fundamental Theorem of Algebra*. Springer, 1997
- [2] Tikhomirov V. M., Uspenskii V. V. *Ten Proofs of the Fundamental Theorem of Algebra* (in Russian)
- [3] University of St. Andrews (Scotland), School of Mathematics and Statistics website
http://www-groups.dcs.st-and.ac.uk/~history/HistTopics/Fund_theorem_of_algebra.html
- [4] Wikipedia website
http://en.wikipedia.org/wiki/Fundamental_Theorem_of_Algebra