Azerbaijan Journal of Mathematics
V. 9, No 1, 2019, January
ISSN 2218-6816

On the Fundamental Theorem of Algebra and Its Equivalence to the Frobenius Theorem on Division Algebras

I.Sh. Jabbarov*, G.K. Hasanova

Abstract. In this article we give a new proof of the Fundamental Theorem of Algebra. Our proof is algebraic. We simplify the known proof of the Fundamental Theorem considering special case of polynomials of odd degree with real coefficients. This case allows us to apply the method of mathematical induction to get the proof in general case without using infiniteness of the field.

Key Words and Phrases: Fundamental Theorem of Algebra, algebraic extension, complex number, polynomial, real coefficients, real root, minimal polynomial.

2010 Mathematics Subject Classifications: 13M10, 12F05

1. Introduction

Formulation of the Fundamental Theorem of Algebra (FTA) was given by A. Girard (in 1617) as a conjecture: an algebraic equation of degree n has n complex roots. But first complete and strict proof was given by J. Argand in 1814. In 1816 C. Gauss had published a new complete proof. These were great development of algebraic and analytic methods. Later, FTA has been proved by many other mathematicians. Today, the number of known proofs of FTA is very large ([1-2]). Some of these proofs are based on the properties of analytic functions. Several proofs using projective spaces can be found in [2].

In [3], FTA was proved for ordered fields. In that proof essential role was played by the assumption that the main field is infinite. In this paper we give a new proof for which this assumption isn't made.

One of the interesting questions on this direction is a construction of algebraic proof without using topological or geometric ideas. So far none of the methods

[*] Corresponding author.

for proving FTA is purely algebraic (see [4-6]). Our proof is also algebraic in which we use, as many other proofs, the fact that the algebraic equation of odd degree with real coefficients has at least one real root. This is due to the fact that the field of real numbers is a complete field of strict linear order. This is a unique argument related to the topology of real axes. Using special construction allows us to avoid assumption on infiniteness of the field. By this reason this method can be used in the case of finite fields. Another basic argument consisted in the existence of a square root of negative real numbers in the field of complex numbers.

In [7], G. Frobenius had proved the theorem on division associative algebras. He proved that there exists only 3 associative division algebras over the field of real numbers. Proof of this deep result is based on FTA (see [6]). There is close connection between these two results, which was not observed in the literature. In this paper we show that the Frobenius theorem on division algebras is equivalent to the Fundamental Theorem of Algebra.

2. Auxiliary lemmas

Our considerations for the questions about extensions of the field of real numbers are based on some important notions of the theory of polynomials over the field of real numbers.

Definition 1. *Let $f(x) \in K[x]$ be a polynomial. We call this polynomial irreducible if it can't be represented as a product of two polynomials of positive degree such as*

$$f(x) = g(x)h(x);\ g(x), h(x) \in K[x].$$

Definition 2. *Let α be an algebraic element over the field K. Unitary polynomial $f(x) \in K[x]$ is called a minimal polynomial if $f(x)$ is a polynomial of least degree such that $f(\alpha) = 0$.*

The basic properties of irreducible and minimal polynomials are given below.

Lemma 1. *Let $f_1(x), f_2(x) \in K[x]$ be two unitary irreducible polynomials. Then, $f_1(x) = f_2(x)$, or $(f_1(x), f_2(x)) = 1$.*

Lemma 2. *Let α be an algebraic element over the field K with minimal polynomial $f(x) \in K[x]$. If $g(x) \in K[x]$ is a polynomial with the root α, then $g(x) \vdots f(x)$.*

Lemma 3. *Let $f_1(x), f_2(x) \in K[x]$ be two different irreducible polynomials. If $f(x) \vdots f_1(x)$ and $f(x) \vdots f_2(x)$, then*

$$f(x) \vdots f_1(x) f_2(x).$$

We shall use some general results known from the theory of algebraic extensions. Suppose we are given some algebraic extension L/K. We shall call the extension L a *splitting field* for the polynomial $f(x) \in K[x]$ if all roots of this polynomial belong to L. It is known that every polynomial has a splitting field (see [2, p.193]). Note that every splitting field of the polynomial of degree 2 $x^2+a_1x+a_2 \in \mathbf{R}[x]$, with negative discriminant, contains as a subfield (coincides with) the field of complex numbers.

Lemma 4. *Let α be an algebraic element over the field K, and $f(x) \in K[x]$ be its minimal polynomial. Then:*

1) the polynomial $f(x)$ is irreducible;

2) if $g(x)$ is an irreducible unitary polynomial and has a root α, then $g(x)$ is a minimal polynomial for α;

3) the minimal polynomial is unique.

Lemma 5. *If a polynomial $f(x) \in \mathbb{R}[x]$ has an odd degree, then this polynomial has a real root.*

This result is based on the property of continuous functions. If the polynomial has an odd degree, then for sufficiently great positive a at the points $-a$ and a this polynomial takes values with different signs. As a consequence of continuity, $f(x)$ vanishes at some real $c, -a < c < a$.

For our considerations it is necessary to state one result from the theory of symmetric polynomials.

Lemma 6. *Let $g(y_1, y_2, ..., y_n) \in K[y_1, y_2, ..., y_n]$ be a symmetric polynomial over the field K, and $\alpha_1, \alpha_2, ..., \alpha_n$ be the roots of the polynomial $f(x) \in K[X]$. Then $g(\alpha_1, \alpha_2, ..., \alpha_n) \in K$.*

The proofs of Lemmas 4-6 can be found in [5-6].

Lemma 7. *If $\alpha \neq 0$ is a complex number, then $\sqrt{\alpha}$ has two complex values.*

Lemma 8. *Let the condition $f(x) = f(-x)$ be satisfied for the polynomial $f(x) \in K[x]$. Then one can find a polynomial $g(x) \in K[x]$ such that $f(x) = g(x^2)$.*

Proof. Let

$$f(x) = a_0 + a_1x + \cdots + a_nx^n.$$

Then

$$f(-x) = a_0 - a_1x + \cdots + (-1)^n a_nx^n,$$

and by the condition of the lemma

$$f(x) = (f(x) + f(-x))/2 = a_0 + a_2x^2 + \cdots + a_{2k}x^{2k} + \cdots .$$

So, at the right-hand side of this equality we see some polynomial of x^2. ◄

3. Fundamental Theorem of Algebra

Theorem 1. *(FTA) Every polynomial of positive degree with complex coefficients has complex roots only.*

Proof. We shall prove this theorem by induction with respect to the degree of the polynomial. It is clear that the theorem is valid for the polynomials of first degree. Suppose that the statement of the theorem holds for all polynomials of degree $\leq n-1$. Prove now FTA for the polynomials of degree n.

Let $f(x) \in \mathbb{C}[x]$ be some polynomial with complex coefficients, and

$$\deg f(x) = n = 2^k r,$$

where $k \geq 0, r \in \mathbb{N}, r \not\vdots 2$. We shall apply the method of induction with respect to k for reducing the case $\deg f(x) = n$ to the cases of less degree.

1) Consider the case $k = 0$. If the polynomial has an odd degree, then we put

$$g(x) = f(x)\bar{f}(x),$$

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n,$$

with the coefficients $a_0, a_1, ..., a_n$ being complex numbers, and

$$\bar{f}(x) = \bar{a}_0 + \bar{a}_1 x + \cdots + \bar{a}_n x^n.$$

Then,

$$g(x) = f(x)\bar{f}(x) = c_0 + c_1 x + \cdots + c_{2n} x^{2n},$$

and

$$c_m = a_0\bar{a}_m + a_1\bar{a}_{m-1} + \cdots + a_m\bar{a}_0, 0 \leq m \leq 2n,$$

moreover, we put $a_m = 0$ when $m > n$. It is clear that $c_m = \bar{c}_m$. So, the polynomial $g(x)$ is a polynomial with real coefficients of degree $2n$, and n is an odd number.

Let's denote by P the splitting field of considered polynomials. Suppose that in this field $g(x)$ has zeroes $\alpha_1, ..., \alpha_{2n}$. Consider the sums $\alpha_{ij} = \alpha_i + \alpha_j, i > j,$ where $i, j = 1, ..., 2n$. The number of these sums is equal to the odd number

$$1 + \cdots + 2n - 1 = 2n(2n-1)/2 = n(2n-1).$$

Construct a new polynomial

$$h(x) = \prod_{i>j} (x - \alpha_{ij})$$

of degree $d = n(2n-1)$. If we permute the roots $\alpha_1, ..., \alpha_{2n}$, then we get the polynomial $h(x)$ again, because after permutation the factors of $h(x)$ can change their orders only. So, the coefficients of this polynomial are symmetric polynomials of roots. By Lemma 6, the coefficients of the polynomial $h(x)$ belong to the main field, i.e. they are real numbers. Therefore, $h(x)$ has a real root $2c \in \mathbb{R}$. Then, for some roots α and β of $g(x)$ we have $\alpha + \beta = 2c \in \mathbb{R}$. Then we have $\alpha - c = -(\beta - c)$. By Taylor's formula

$$g(x) = g(c) + g'(c)(x-c) + \cdots + \frac{1}{(2n)!} g^{(2n)}(c)(x-c)^{2n} = \phi(y),$$

where we have denoted $y = x - c$. If we write $\theta_1 = \alpha - c, \theta_2 = \beta - c$, then we have $\theta_1 = -\theta_2$. Denote by $\psi(y) \in \mathbf{R}[y]$ the minimal polynomial for the root θ_1. One of the numbers $\theta_1 + c, \theta_2 + c$, say $\theta_1 + c$, is a root of the polynomial $f(x)$ (or the polynomial $\bar{f}(x)$) with complex coefficients. Then θ_1 will be a root of the polynomial

$$f(x+c) = f(c) + f'(c)x + \cdots + \frac{1}{n!} f^{(n)}(c)x^n = \tau(x).$$

Then $\tau(x)$ is divisible by $\psi(x) \in \mathbb{R}[x]$. If $\deg \psi(x) < \deg f(x)$, then by an inductive assumption all of the roots of polynomial $\tau(x)$ must be complex numbers. Then the same statement is valid for the roots of the polynomial$f(x)$.

Prove that the case $\deg \psi(x) = \deg f(x)$ is impossible. In fact, if $\deg \psi(x) = \deg f(x)$, then the polynomials $\tau(x)$ and $\psi(x)$ are associated. Since the polynomial $\psi(-y)$ is irreducible, then $\psi(-y)$ will be a minimal polynomial for θ_2 by virtue of Lemma 4. According to Lemma 1, we have either $\psi(y) = \psi(-y)$ or $(\psi(y), \psi(-y)) = 1$. Consider now polynomial $\gamma(y) = \psi(y) = \psi(-y)$ in the first case, and $\gamma(y) = \psi(y)\psi(-y)$ in the second case. Then, the polynomial $\gamma(y)$ is an even function, i.e. $\gamma(y) = \lambda(y^2)$, by Lemma 8. In the first case this is impossible, since the polynomial $\tau(x)$ has odd degree. Then, we have $(\psi(y), \psi(-y)) = 1$ and $\psi(-x)$ must be associated with $\bar{f}(x)$. So, $g(x)$ is associated with the polynomial $\gamma(x) = \lambda(x^2)$. Now we note that the polynomial $\lambda(y)$ has odd degree and real coefficients. Then this polynomial has a real root δ which must be root of the irreducible polynomial $f(x)$ (or $\bar{f}(x)$), which is impossible. So, the case $\deg \psi(x) = \deg f(x)$ is impossible, and the statement of the theorem is true for the case $k = 0$.

2) Assume that every polynomial $f(x) \in \mathbb{C}[x]$ with $\deg f(x) = n = 2^k r$ and $k \geq 1$ has complex zeros only for all odd numbers $r \in \mathbb{N}, r \not\vdots 2$. Prove that the same statement is valid for polynomials $f(x) \in \mathbb{C}[x]$ with $\deg f(x) = n = 2^{k+1} r$, where $r \in \mathbb{N}, r \not\vdots 2$. Take some splitting field P where this polynomial has roots

$\alpha_1, ..., \alpha_n$. Construct the sums

$$\alpha_{ij} = \alpha_i + \alpha_j, i > j,$$

where $i, j = 1, ..., n$. The number of these sums is equal to

$$1 + \cdots + n - 1 = n(n-1)/2 = 2^k(2^{k+1} - 1).$$

Consider a new polynomial

$$h(x) = \prod_{i>j} (x - \alpha_{ij})$$

of degree $d = 2^k(2^{k+1} - 1)$. As we see, the number $2^{k+1} - 1 = m$ is odd. It is clear that if we permute the roots $\alpha_1, ..., \alpha_n$, then we get the polynomial $h(x)$ again. So, the coefficients of this polynomial are symmetric polynomials of roots. By Lemma 6, the coefficients of the polynomial $h(x)$ belong to the main field, i.e. they are complex numbers. Then, by inductive assumption, the constructed polynomial has a complex root, say $2c$, i. e. for some roots α and β of $f(x)$ we have $\alpha + \beta = 2c \in \mathbb{C}$. Then $\alpha - c = -(\beta - c)$. By Taylor's formula

$$f(x) = f(c) + f'(c)(x-c) + \cdots + \frac{1}{n!} f^{(n)}(c)(x-c)^n = \phi(y), \qquad (1)$$

in which we have assumed $y = x - c$. If we write $\theta_1 = \alpha - c, \theta_2 = \beta - c$, then we have $\theta_1 = -\theta_2$. The polynomial $\phi(y)$ has complex coefficients, and roots θ_1, θ_2, as seen from the expansion above. Denote by $\psi(y) \in \mathbb{C}[y]$ a minimal polynomial for the root θ_1. We can apply the reasoning above. Since the polynomial $\psi(-y)$ is irreducible, then $\psi(-y)$ will be a minimal polynomial for θ_2 in accordance with Lemma 4. Then $\psi(y) = \psi(-y)$ or $(\psi(y), \psi(-y)) = 1$. Consider now the polynomial $\gamma(y) = \psi(y) = \psi(-y)$ in the first case, and $\gamma(y) = \psi(y)\psi(-y)$ in the second case. In both cases the polynomial $\gamma(y)$ is an even function, i.e. $\psi(y) = \lambda(y^2)$.

In the first case we have $\phi(y) \vdots \psi(y)$. Then, $\phi(y) = \psi(y)\sigma(y)$, with the polynomials $\psi(y), \sigma(y)$ of positive degree. So, both of these polynomials have a degree $\leq n-1$ and have complex roots only, in accordance with an inductive assumption. Therefore, in this case the theorem is valid. If the polynomials $\psi(y)$ and $\phi(y)$ are associated, then $\phi(y) = c\lambda(y^2)$, and the polynomial $\lambda(y)$ has degree $n/2$. So, this polynomial has complex roots only. Then, $\phi(y)$, accordance with Lemma 7, also has complex roots only.

Consider the second case $\gamma(y) = \psi(y)\psi(-y)$. From Lemma 3 it follows that the polynomial $\phi(y)$ is divisible by $\gamma(y)$. In this case the polynomials $\psi(y), \psi(-y)$

as well as the polynomial $\phi(y)$ have complex roots only by virtue of inductive assumption.

The FTA is now proved. ◀

4. Equivalence of FTA to the Frobenius Theorem

Consider some field P, and let V denote a linear associative algebra over this field. If for any elements $a, b \in V$ the equations $ax = b$ and $xa = b$ have solutions when $a \neq 0$, then this algebra is called *algebra with division.* The dimension of the linear space V is called a *rank* of the algebra. The field of complex numbers is a division algebra of rank 2.

Now we recall the Frobenius theorem.

Theorem (Frobenius). *There are only three associative division algebras over the field of real numbers: the fields of real and complex numbers, and the quaternion algebra.*

The proof of this theorem is based on some results on associative division algebras which have analogs in the theory of fields extensions.

Lemma 9. *Let V be a division algebra of rank n over the field of real numbers R. Then:*

1) every element $\alpha \in V$ is a root of a polynomial of first or second degree with real coefficients;

2) if $\alpha \in V \backslash R$, then one can find real numbers a and b such that $(a\alpha + b)^2 = -1$ with $a \neq 0$;

3) if $n = 2$, then $V \cong C$.

Proof of this lemma is a consequence of FTA (see [8]).

Lemma 10. *There is no associative division algebra of rank 3 over the field of real numbers.*

This lemma can be proved by the methods of the theory of finite extensions (see [8]). If we suppose an existence of such an algebra, then this algebra must contain linearly independent elements $1, \alpha, \beta$. Then division algebra containing the elements $1, \alpha$ will be an extension isomorphic to the field of complex numbers. Now we can consider the division algebra given above as an analog of extension of the field of complex numbers. In accordance with Lemma 9, we then could have an extension of rank 2, because the element β doesn't belong to the constructed algebra of dimension 2. In the theory of algebraic extensions there is a statement:

Let E and F be two finite extensions of the field K. If the field F is of degree m over the field E, and E is an extension of degree n over the field K, then the *field F is of degree mn over the field K. Moreover, if the set $\{x_1, ..., x_m\}$ is a base of F over E, and $\{y_1, ..., y_n\}$ is a base of E over the field K, then the set $\{x_i y_j\}_{1\leq i,j\leq j}$ will be a base for F over the field K.*

These observations allow to conjecture that the rank of the division algebra containing linearly independent elements $1, \alpha, \beta$ must have at least rank 4. This fact was established in a similar way (see [8]).

As a consequence of the proved results we have

Lemma 11. *Let V be an associative division algebra of the rank $n \geq 3$. Then for every pair of elements α, β satisfying conditions $\alpha^2 = -1, \beta^2 = -1$ we have $\alpha\beta = -\beta\alpha$.*

Frobenius theorem is a consequence of the above lemmas ([6,8]).

Our goal is to prove equivalence of this theorem to FTA.

Theorem 2. *FTA is equivalent to the Frobenius Theorem.*

Proof. It is well known that Frobenius Theorem is possible to deduce from FTA. To complete the proof of Theorem 2, we must prove an implication Frobenius Theorem ⇒ FTA. Assume Frobenius Theorem is true, i.e. there are only three associative division algebras over the field of real numbers. It is well known that for every polynomial $f(x) \in \mathbb{C}[x]$ there exists a polynomial $g(x) \in \mathbb{R}[x]$ such that every root of given polynomial or its conjugate is a root of $g(x)$. On other hand, there exist an extension L of the field of real numbers containing all roots of the polynomial $g(x)$. It is clear that the field L is a commutative division algebra of finite rank over the field of real numbers. By the Frobenius Theorem, this algebra can be isomorphic, in accordance with commutativity, to the algebras $\mathbb{R}$ or $\mathbb{C}$ only, because the quaternion algebra is not commutative. So, all roots of given polynomial belong to the field L being isomorphic to $\mathbb{C}$. ◄

References

[1] H. Derksen, *The fundamental theorem of algebra and linear algebra*, American Mathematical Monthly, **110(7)**, 2003, 620-623.

[2] V.M. Tikhomirov, V.V. Uspenskii, *Ten proofs of the Fundamental Theorem of Algebra*, Math. Prosv., **1**, 1997, 50–70.

[3] N. Bourbaki, *Algebra, Polynomials and Fields. Ordered groups*, Moscow, Nauka, 1965.

[4] S. Leng, *Algebra*, Moscow, Mir, 1968.

[5] A.I. Kostrikin, *Introduction to the Algebra*, Moscow, Nauka, 1977.

[6] A.G. Kurosh, *Lectures on general algebra*, Moscow, Nauka, 1971.

[7] G. Frobenius, *Ueber lineare Substitutionen and bilineare Formen*, J. Reine Angew. Math., **84**, 1878, 1–63.

[8] V.I. Nechayev, *Number Systems*, Moscow, Prosveshenie, 1975.

Ilgar Sh. Jabbarov
Ganja State University, Haydar Aliyev ave. 159, Ganja AZ2000, Azerbaijan
E-mail: ilgar_j@rambler.ru

Gunay K. Hasanova
Ganja State University, Haydar Aliyev ave. 159, Ganja AZ2000, Azerbaijan
E-mail: gunay.hasanova@mail.ru

Received 12 July 2018
Accepted 19 September 2018