An Algebraic Proof of the Fundamental Theorem of Algebra.

Oct. 19, 2022

Blake Madill

bmadill@uwaterloo.ca

Thm [FTA]

If $f(x)$ is a non-constant polynomial with complex coefficients (ie. $f(x) \in \mathbb{C}[x]$)

then there exists $z \in \mathbb{C}$

s.t. $f(z) = 0$.

Common Proofs:

① Complex Analysis

② Algebraic Topology

Goal: Prove the FTA using algebra!

Disclaimer: We do steal a little calculus:

If $f(x) \in \mathbb{R}[x]$ has odd degree, then $f(x)$ has a real root.

IVT.

Main Tools

① A field K is a set with two operations

$$+ : K \times K \to K$$

$$\cdot : K \times K \to K,$$

satisfying some nice/usual axioms, where every nonzero element is mult. invertible.

Ex) $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ fields

Ex) $\mathbb{Z}$ not a field.

$$\frac{1}{2} \notin \mathbb{Z}$$

② Let $F \subseteq K$ be fields (same operations).

An <u>automorphism</u> of K is an invertible function $\varphi : K \to K$ s.t.

a) $\varphi(x+y) = \varphi(x) + \varphi(y)$

b) $\varphi(xy) = \varphi(x)\varphi(y)$.

We write $\varphi \in \mathrm{Aut}(K)$.

We define

$$\mathrm{Gal}(K/F) = \{\varphi \in \mathrm{Aut}(K) : \forall x \in F,\ \varphi(x) = x\}$$

Ex) $K = \mathbb{Q}(\sqrt{2})$

$= \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$

↳ field

$\varphi(a + b\sqrt{2}) = a - b\sqrt{2}$

$\varphi \in \mathrm{Gal}(K/\mathbb{Q})$

Who Cares?!

$F \subseteq K$ fields

$\alpha \in K$, $f(x) \in F[x]$.

Suppose $f(\alpha) = 0$.

Then .....

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

$$a_n \alpha^n + \dots + a_1 \alpha + a_0 = 0$$

$$\varphi \in \mathrm{Gal}(K/F)$$

① $\varphi(0) = \varphi(0+0)$

$= \varphi(0) + \varphi(0)$

$\Rightarrow \varphi(0) = 0$

② $0 = \varphi(0)$

$= \varphi(a_n \alpha^n + \dots + a_1 \alpha + a_0)$

$= a_n \varphi(\alpha)^n + \dots + a_1 \varphi(\alpha) + a_0$

$\Longrightarrow f(\varphi(\alpha)) = 0$

Step 1: Set Up the Contradiction!

Suppose we can find a polynomial $f(x) \in \mathbb{C}[x]$ of minimal degree s.t. $f(x)$ has no roots in $\mathbb{C}$.

Note: $f(x)$ is irred.

Fact: There exists a field $\mathbb{C} \subseteq L$ s.t. $f(x)$ has a root $\alpha \in L$.

Step 2: Make a field!

Consider

$$\mathbb{C}(\alpha) = \{ g(\alpha) : g(x) \in \mathbb{C}[x] \}$$

Fact: $\mathbb{C}(\alpha)$ is a field

Ex) $\alpha = \sqrt{2+\sqrt{2}}$

$$(\alpha^2 - 2)^2 = 2$$

$$\Rightarrow \alpha^4 - 4\alpha^2 + 2 = 0$$

$$\Rightarrow \alpha^4 = 4\alpha^2 - 2$$

$$\mathbb{Q}(\alpha) = \{ a + b\alpha + c\alpha^2 + d\alpha^3 : a, b, c, d \in \mathbb{Q} \}$$

Step 3: Get Dimensional

Say $f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0.$

Then,

$$\mathbb{C}(\alpha) = \{ c_0 + c_1\alpha + \dots + c_{n-1}\alpha^{n-1} : c_i \in \mathbb{C} \}$$

By Minimality,

$$\underbrace{\dim_{\mathbb{C}} \mathbb{C}(\alpha)}_{[\mathbb{C}(\alpha):\mathbb{C}]} = n = \deg f(x)$$

Step 4 : Generalize a Little

If $F \subseteq K$ are fields then K is an F-vector space.

$$[K:F] := \dim_F K$$

Fact: $F \subseteq K \subseteq L$ fields

$$[L:F] = [L:K][K:F]$$

Now suppose $[K:F]=n<\infty$.

For $\alpha \in K$,

$\{1, \alpha, \dots, \alpha^n\}$ is ....

Linearly Dependent

We may find $g(x) \in F[x]$ s.t. $g(\alpha)=0$.

$$c_0 + c_1\alpha + \dots + c_n\alpha^n = 0$$

Suppose $[K:F] < \infty$ and let $\alpha \in K$.

Let $g(x) \in F[x]$ be of minimal degree s.t. $g(\alpha) = 0$.

Then ....

$$[F(\alpha):F] = \deg g(x).$$

Step 5: Subgroups + Fixed Fields

Let $G = Gal(K/F)$.

① We say $H \leq G$ is a <u>subgroup</u> of G if

a) $\varphi, \psi \in H \Rightarrow \varphi \circ \psi \in H$

b) $\varphi \in H \Rightarrow \varphi^{-1} \in H$.

② Let H be a subgroup of G.

Define $Fix(H) = \{a \in K : \forall \varphi \in H, \varphi(a) = a\}$

Note: $Fix(H)$ is a field.

Step 6: Normal Extensions

Let $\mathbb{Q} \subseteq F \subseteq K$ be fields.

We say $F \subseteq K$ is normal if whenever $f(x) \in F[x]$ has a root in K, then $f(x)$ completely factors over ~~F.~~ K

Ex) $K = \mathbb{Q}(\sqrt{2})$, $F = \mathbb{Q}$

$a + b\sqrt{2} \to a - b\sqrt{2}$

Ex) $K = \mathbb{Q}(\sqrt[3]{2})$, $F = \mathbb{Q}$.

$K \subseteq \mathbb{R}$

$g(x) = x^3 - 2$

$\underbrace{\sqrt[3]{2} \cdot \zeta_3}_{\in \mathbb{C} \setminus \mathbb{R}} \notin K$

Step 7: Galois Theory

$\mathbb{Q} \subseteq F \subseteq K$ Normal, $[K:F] < \infty$.

$G = Gal(K/F)$, $H \subseteq G$ subgroup

$E = Fix\, H$

Big Facts:

① $|G| = [K:F]$

② $|H| = [K:E]$

Step 8: Sylow Theory.

$G = Gal(K/F)$ Facts:

① Say $|G| = 2^i m$, m odd.

Then G has a subgroup of order 2^i.

② If $|G| = 2^i$, then G has a subgroup of order 2^{i-1}.

Step 9: Back to the Proof!

We have

$[\mathbb{C}(\alpha):\mathbb{C}] = \deg f(x) = n,$

where $f(\alpha)=0$ and $f(x) \in \mathbb{C}[x]$

has no complex roots.

Let K be the smallest field containing $\mathbb{R}$ s.t. $f(x)(x^2+1)$ factors completely over $\mathbb{R}$.

Facts:

1) K exists
2) $K/\mathbb{R}$ is normal.
3) $\mathbb{R} \subseteq \mathbb{C} \subseteq K$.

$G = \mathrm{Gal}(K/\mathbb{R})$

$|G| = [K:\mathbb{R}] = [K:\mathbb{C}][\mathbb{C}:\mathbb{R}]$

$= 2[K:\mathbb{C}]$

Say $|G| = 2^j m$, m odd, $j \geq 1$.

Let $H \leq G$ with $|H| = 2^j$.

and let $E = \mathrm{Fix}\, H$.

$\therefore |H| = [K:E] = 2^j$.

$\Rightarrow [E:\mathbb{R}] = m$ odd.

$\Uparrow$

1

Take $\beta \in E$.

Let $g(x) \in \mathbb{R}[x]$ be of minimal degree s.t. $g(\beta) = 0$. Note: $g(x)$ irreducible

Similar to before,

$[\mathbb{R}(\beta):\mathbb{R}] = \deg g(x)$ odd.

$\Rightarrow \deg g(x) = 1$

$\Rightarrow \beta \in \mathbb{R}$

$\Rightarrow m = 1$.

$$\underset{\substack{\| \\ m}}{[E:\mathbb{R}]} = [E:\mathbb{R}(\beta)][\mathbb{R}(\beta):\mathbb{R}]$$

At this point:

$[K:\mathbb{R}] = |G| = 2^j m = 2^j.$

Again,

$[K:\mathbb{R}] = 2[K:\mathbb{C}]$, $K \neq \mathbb{C}$.

$\Rightarrow j \geq 2$, $[K:\mathbb{C}] = 2^{j-1}$

Let $\tilde{G} = \mathrm{Gal}(K/\mathbb{C})$. Still Norm

Let $\tilde{H}$ be a subgroup of order 2^{j-2}.

If $F = \mathrm{Fix}\,\tilde{H}$, then

$[K:F] = |\tilde{H}| = 2^{j-2}$

$\Rightarrow [K:\mathbb{C}]$

$= [K:F][F:\mathbb{C}]$

$\Rightarrow 2^{j-1} = 2^{j-2}[F:\mathbb{C}]$

$\Rightarrow [F:\mathbb{C}] = 2$

Why is this a contradiction ?

$\beta \in F$, $\beta \notin \mathbb{C}$

$$[\mathbb{C}(\beta) : \mathbb{C}] = 2$$

$\exists$ irred, $g(x) \in \mathbb{C}[x]$

$$g(\beta) = 0$$

$$\deg g(x) = 2$$