We will prove the Fundamental Theorem of Algebra (FTA) using Galois theory, in particular, the Fundamental Theorem of Galois Theory (FTGT) or Galois correspondence. In addition we use two facts from real analysis which are as follows.
Fact 1: Every positive real number has a square root in real numbers.
Fact 2: Every polynomial of odd degree with real coefficients has a real root.
Now we recall FTGT.

Theorem 1 (FTGT)**.** *Let E/F be a finite Galois extension with Galois group* $\mathrm{Gal}(E/F)$*. Then there is a bijection*

$$\begin{aligned} \{\textit{subgroups of } \mathrm{Gal}(E/F)\} &\leftrightarrow \{\textit{intermediate fields } M \textit{ for } E/F\} \\ H &\mapsto E^H \\ \mathrm{Gal}(E/M) &\leftarrow\!\shortmid\ M. \end{aligned}$$

Moreover, for a subgroup H of $\mathrm{Gal}(E/F)$*,*
(1) the index $[\mathrm{Gal}(E/F) : H]$ is equal to the degree of extension E^H/F, and
(2) the order of H is equal to the degree of extension E/E^H.

Theorem 2 (FTA)**.** *Every non-constant polynomial in $\mathbb{C}[X]$ has a root in $\mathbb{C}$. (In other words, the field of complex numbers $\mathbb{C}$ is algebraically closed.)*

Proof. **Step 1:** The extension $\mathbb{C}/\mathbb{R}$ is splitting field of the polynomial $X^2+1 \in \mathbb{R}[X]$. The degree of this extension is 2. We write $\mathbb{C} = \mathbb{R}[i]$.
Step 2: Every element of $\mathbb{C}$ has a square root in $\mathbb{C}$. (This is easy! You need to use **Fact 1**.)
Step 3: It is enough to show that every $f(X) \in \mathbb{R}[X]$ has a root in $\mathbb{C}$. (This has been discussed in Module 1 or Module 2.) Consider the polynomial $f(X)(X^2+1) \in \mathbb{R}[X]$. Let E be the splitting field of $f(X)(X^2+1)$. Clearly $E/\mathbb{R}$ is a finite extension and $\mathbb{R} \subset \mathbb{C} \subset E$. Since the characteristic of $\mathbb{R}$ is zero the extension $E/\mathbb{R}$ is separable and hence Galois. Now we have to prove $E = \mathbb{C}$.
Step 4: Let $H \subset \mathrm{Gal}(E/\mathbb{R})$ be a 2-Sylow subgroup. Then the index $[\mathrm{Gal}(E/\mathbb{R}) : H]$ is odd. Then the degree of extension $E^H/\mathbb{R}$ is also odd (which is clear from the following diagram: FTGT).

$$\begin{array}{rcl} E & & \mathrm{Gal}(E/\mathbb{R}) \\ | & & |(odd) \\ E^H & \leftarrow\!\shortmid & H \\ (odd)| & & | \\ \mathbb{R} & & \{1\}. \end{array}$$

Now we consider the odd degree extension $E^H/\mathbb{R}$. Let $a \in E^H$. Let $g(X) \in \mathbb{R}[X]$ be the minimal polynomial of a.

$$(\text{degree of } E^H/\mathbb{R} \text{ is odd}) \Rightarrow (\text{degree of } g(X) \text{ is odd}).$$

If the degree of $g(X)$ is odd then from **Fact 2** it has a root in $\mathbb{R}$. Since $g(X)$ is irreducible its degree will have to be one. Then $a \in \mathbb{R}$. We get $E^H = \mathbb{R}$ and $\mathrm{Gal}(E/\mathbb{R}) = H$ is a 2-group (that is the order of the group is a power of 2).
Step 5: Note that $\mathbb{R} \subset \mathbb{C} \subset E$. Therefore $\mathrm{Gal}(E/\mathbb{C}) \subset \mathrm{Gal}(E/\mathbb{R})$ is also a 2-group. If the group

$\mathrm{Gal}(E/\mathbb{C}) \neq \{1\}$ then it will have a subgroup, say N, with index 2 (from Group Theory). Then the extension $E^N/\mathbb{C}$ is of degree 2 (which is clear from the following diagram: FTGT).

$$\begin{array}{rcl} E & & \mathrm{Gal}(E/\mathbb{C}) \\ | & & |(index = 2) \\ E^N & \hookleftarrow & N \\ (degree = 2)| & & | \\ \mathbb{C} & & \{1\}. \end{array}$$

The two degree extension $E^N/\mathbb{C}$ is generated by the square root of an element of $\mathbb{C}$. But from **Step2** we know that such a square root is in $\mathbb{C}$. Thus $E^N = \mathbb{C}$ which is a contradiction. Therefore $\mathrm{Gal}(E/\mathbb{C}) = \{1\}$ and hence $E = \mathbb{C}$. □

Definition 3 (Character)**.** Let G be a group and F a field. A group homomorphism

$$\chi : G \to F^\times$$

is called a character of G (with values in F), i.e. $\chi(g_1g_2) = \chi(g_1)\chi(g_2)$ for all $g_1, g_2 \in G$.

Space of functions: Recall that for a field F and any set (and hence for a group G) the set of all functions $G \to F$ is a vector space over F. We write this space as $\mathrm{Func}(G, F)$.

Theorem 4 (Dedekind)**.** *Let F be a field and G a group. Then every finite set of characters $\{\chi_1, \cdots, \chi_m\}$ is linearly independent in* $\mathrm{Func}(G, F)$*. In other words,*

$$\textstyle\sum_{i=1}^m a_i\chi_i = 0 \text{ (as a function } G \to F) \Rightarrow a_i = 0 \text{ for all } i.$$

Proof. We will use induction on m to prove this theorem.
For $m = 1$ it is trivial.
Now let $m \geq 2$, we assume the statement for $m-1$ and prove it for m. Let $\{\chi_1, \chi_2, \cdots, \chi_m\}$ be a set of characters with m elements and $\sum_{i=1}^m a_i\chi_i = 0$ for some $a_i \in F$. We will prove that $a_i = 0$ for all i. Then for all $x \in G$ we have

$$\sum_{i=1}^m a_i\chi_i(x) = 0. \tag{0.1}$$

Since $\chi_1 \neq \chi_2$ there exists an element $g \in G$ such that $\chi_1(g) \neq \chi_2(g)$. In particular, we also have

$$\sum_{i=1}^m a_i\chi_i(gx) = 0. \tag{0.2}$$

We multiply by $\chi_1(g)$ in Equation 0.1 and substract Equation 0.2:

$$\begin{array}{l} a_1\chi_1(g)\chi_1(x) + a_2\chi_1(g)\chi_2(x) + \cdots + a_m\chi_1(g)\chi_m(x) = 0 \\ a_1\chi_1(g)\chi_1(x) + a_2\chi_2(g)\chi_2(x) + \cdots + a_m\chi_m(g)\chi_m(x) = 0 \end{array}$$

we get the following

$$a_2(\chi_2(g) - \chi_1(g))\chi_2(x) + \cdots + a_m(\chi_1(g) - \chi_m(g))\chi_m(x) = 0.$$

Now we apply induction for the set $\{\chi_2, \cdots, \chi_m\}$ which has $m-1$ elements. We get $a_2(\chi_1(g) - \chi_2(g)) = 0$. Since $\chi_1(g) \neq \chi_2(g)$ we get $a_2 = 0$. Now we have

$$\textstyle\sum_{i\neq 2} a_i\chi_i = 0$$

which involves only $m-1$ characters. We again apply the induction to this set of characters $\{\chi_1, \chi_2, \cdots, \chi_m\} \setminus \{\chi_2\}$ which has $m-1$ elements. We get $a_i = 0$ for all $i = 1, 2, \cdots, m$. □

Definition 5 (Cyclic extension)**.** A finite Galois extension E/F is said to be *cyclic* if the Galois group $\mathrm{Gal}(E/F)$ is a cyclic group.

Example 6. (1) The extensions $\mathbb{C}/\mathbb{R}$, $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ have Galois group $\mathbb{Z}/2\mathbb{Z}$ and hence are cyclic.
(2) The extension $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$ is not cyclic, since the Galois group is Klein's four group which is not cyclic.
(3) The extension $\mathbb{F}_{p^n}/\mathbb{F}_p$ is cyclic since the $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong \mathbb{Z}/n\mathbb{Z}$ is cyclic and generated by the element, say $\sigma : x \mapsto x^p$ (this is called the Frobenius element).

Definition 7 (Norm map)**.** For a finite Galois extension E/F we define the norm map $N : E \to F$ by

$$N(x) := \prod_{\sigma \in \mathrm{Gal}(E/F)} \sigma(x).$$

Example 8. (1) For the extension $\mathbb{C}/\mathbb{R}$, $N(a+ib) = (a+ib)(a-ib) = a^2+b^2$.
(2) For the extension $\mathbb{Q}(\sqrt{3})/\mathbb{Q}$, $N(a+b\sqrt{3}) = (a+\sqrt{3}b)(a-b\sqrt{3}) = a^2-3b^2$.

Theorem 9 (Hilbert's Theorem 90)**.** *Let E/F be a finite cyclic Galois extension with $\mathrm{Gal}(E/F) =< \sigma >$. Then*

$$a \in E^\times, N(a) = 1 \Leftrightarrow \textit{there exists } b \in E^\times \textit{ with } a = \tfrac{b}{\sigma(b)}.$$

Proof. Let the order of the group $\mathrm{Gal}(E/F)$ is n and $\mathrm{Gal}(E/F) = \{id, \sigma, \sigma^2, \cdots, \sigma^{n-1}\}$.
First we prove $\Leftarrow$ part as it is easier. If $a = \frac{b}{\sigma(b)}$ then

$$\begin{aligned} N(a) &= id\left(\frac{b}{\sigma(b)}\right)\sigma\left(\frac{b}{\sigma(b)}\right)\cdots\sigma^{n-1}\left(\frac{b}{\sigma(b)}\right) \\ &= \frac{b}{\sigma(b)}\frac{\sigma(b)}{\sigma^2(b)}\cdots\frac{\sigma^{n-1}(b)}{\sigma^n(b)} \\ &= 1 \end{aligned}$$

since $\sigma^n = id$.
Now we prove $\Rightarrow$ part, for which we use Dedekind's theorem on independence of characters. Note that the $\{id, \sigma, \sigma^2, \cdots, \sigma^{n-1}\}$ is an linearly independent set of $\mathrm{Func}(E, E)$. The linear combination

$$id + a\sigma + a\sigma(a)\sigma^2 + \cdots + [a\sigma(a)\cdots\sigma^{n-2}(a)]\sigma^{n-1}$$

is not identically zero. Let $x \in E$ be an element where it does not vanish and y be its value, i.e.

$$y = x + a\sigma(x) + a\sigma(a)\sigma^2(x) + \cdots + [a\sigma(a)\cdots\sigma^{n-2}(a)]\sigma^{n-1}(x) \neq 0.$$

Then

$$a\sigma(y) = a\sigma(x) + a\sigma(a)\sigma^2(a) + a\sigma(a)\sigma^2(a)\sigma^3(x) + \cdots + [a\sigma(a)\sigma^2(a)\cdots\sigma^{n-1}(a)]\sigma^n(x) = (y-x) + N(a)x$$

Since $N(a) = 1$, we get $a\sigma(y) = y$. Write $y = b$ and then

$$a = \frac{b}{\sigma(b)}.$$

□