First, HW4 Problem 6:

Given $f(x) = \sum a_k x^k \in \mathbb{C}[x]$,
define the conjugate polynomial
$f^*(x) = \sum a_k^* x^k$.

Claim that $f(x) f^*(x) \in \mathbb{R}[x]$.

Note that

$$f(x) f^*(x) = \sum_{k \geq 0} \left(\sum_{i=1}^{k} a_i a_{k-i}^* \right) x^k$$

But each coefficient is real because

$$\left(\sum_{i=1}^{k} a_i a_{k-i}^* \right)^* = \sum_{i=1}^{k} a_i^* a_{k-i}^{**}$$

$$= \sum_{i=1}^{k} a_i^* a_{k-i} = \sum_{j=1}^{k} a_j a_{k-j}^* \quad \checkmark$$

$$\boxed{j = k - i}$$

Conclusion:

$$f(x) \in \mathbb{C}[x] \implies f(x) f^*(x) \in \mathbb{R}[x].$$

Why did I ask you to think about this? Because it's the trickiest step in the following theorem.

Theorem (Equivalent Statements of FTA).
The following 6 statements are equivalent:

i) Every prime in $\mathbb{C}[x]$ has degree 1.

ii) Every nonconstant $f(x) \in \mathbb{C}[x]$ splits.

iii) Every non-const. $f(x) \in \mathbb{C}[x]$ has a root $\in \mathbb{C}$.

iv) Every n.-c. $f(x) \in \mathbb{R}[x]$ has a root in $\mathbb{C}$

v) Every prime in $\mathbb{R}[x]$ has deg 1 or 2.

vi) Every n.c. $f(x) \in \mathbb{R}[x]$ factors into real polynomials of degree 1 & 2.

Proof sketch:

i) $\Rightarrow$ ii) Consider prime factorization.

ii) $\Rightarrow$ iii) Easy (?)

iii) $\Rightarrow$ iv) Vacuous.

iv) $\Rightarrow$ v) We will show that every $f(x) \in \mathbb{R}[x]$ of degree ≥ 3 is not prime.

So let $\deg(F) \geq 3$. By iv) $\exists \alpha \in \mathbb{C}$ such that $f(\alpha) = 0$. If in fact $\alpha \in \mathbb{R}$ then $f(x) = (x-\alpha)\, g(x)$, $g(x) \in \mathbb{R}[x]$, $\deg(g) \geq 2$, hence $f(x)$ not prime in $\mathbb{R}[x]$. Otherwise, $\alpha^* \neq \alpha$ is another root of f.

Factor: $f(x) = (x-\alpha)(x-\alpha^*)\, h(x)$ where $h(x) \in \mathbb{C}[x]$, $\deg(h) \geq 1$. But

$$f(x) = \underset{\mathbb{R}[x]}{\left(x^2 - (\underset{\mathbb{R}}{\alpha+\alpha^*})x + \underset{\mathbb{R}}{\alpha\alpha^*}\right)} h(x).$$

(?) Uniqueness of quotients $\Rightarrow h(x) \in \mathbb{R}[x]$

$\Rightarrow f(x)$ is not prime in $\mathbb{R}[x]$. ✓

v) $\Rightarrow$ vi) Consider prime factorization.

Finally, vi) $\Rightarrow$ v).

Let $p(x) \in \mathbb{C}[x]$ be prime in $\mathbb{C}[x]$.

Assume for contradiction $\deg(p) \geq 2$.

Consider $f(x) = p(x)\, p^*(x) \in \mathbb{R}[x]$.

By vi) $f(x)$ has deg 1 & 2 factors in the ring $\mathbb{R}[x]$.

By factoring the degree 2 polynomials in $\mathbb{C}[x]$ (using quadratic formula), we see that $f(x)$ splits over $\mathbb{C}$:

$$f(x) = q_1(x)\, q_2(x) \cdots q_k(x) \in \mathbb{C}[x]$$

where $\deg(q_j) = 1$ for all j.

Observe that $p(x) \mid f(x) = p(x)\, p^*(x)$, hence $p(x) \mid q_1(x) \cdots q_k(x)$. Since $p(x)$ is prime, Euclid's Lemma implies $p(x) \mid q_j(x)$ for some j.

But then

$$2 \leq \deg(p) \leq \deg(q_j) = 1.$$

Contradiction.

QED.

Bad News: We still have not proved FTA.

Good News: In order to prove FTA, it suffices to prove any one of the 6 equivalent statements.

We will discuss Laplace's Proof (1795), which proves (iv).

Actually, Laplace's Proof is incomplete. There really should be 2 steps to the proof:

(1) Given $f(x) \in \mathbb{R}[x]$ of degree n, prove that $\exists$ field $\mathbb{F} \supseteq \mathbb{C}$ and elements $\alpha_1, \alpha_2, \cdots, \alpha_n \in \mathbb{F}$ (not nec. distinct) such that

$$f(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n) \in \mathbb{F}[x].$$

I.e., show that every real polynomial has all of its roots in some "imaginary" number system.

This statement was too abstract/philosophical for the 1700s, so every attempted proof of FTA just assumed that (1) is true. It was finally proved in 1880s by Leopold Kronecker using ABSTRACT methods.

(2) Assuming the roots of $f(x) \in \mathbb{R}[x]$ exist in some field $\mathbb{F} \supseteq \mathbb{C}$, show that at least one of them is actually in $\mathbb{C}$.
[Then by induction all the roots are in $\mathbb{C}$.]

This is what Laplace proved.

I will show you the proof now and we will understand it later (promise).

Laplace's Proof: Let $f(x) \in \mathbb{R}[x]$ have roots $\alpha_1, \cdots, \alpha_n \in \mathbb{F} \supseteq \mathbb{C}$. For all $\lambda \in \mathbb{R}$ and $1 \leq i < j \leq n$, define the number

$$\beta_{ij\lambda} := \alpha_i + \alpha_j + \lambda \alpha_i \alpha_j \in \mathbb{F}.$$

Given any $\lambda \in \mathbb{R}$ consider the auxiliary polynomial

$$g_\lambda(x) = \prod_{1 \leq i < j \leq n} (x - \beta_{ij\lambda})$$

Two Important facts (I.O.U.):

- $g_\lambda(x)$ has real coefficients !
- If $\deg(f) = 2^e$(some odd number), $e \geq 1$, then $\deg(g_\lambda) = 2^{e-1}$(some odd number). ///

By induction on e, $g_\lambda(x) \in \mathbb{R}[x]$ has some complex root $\beta_{ij\lambda} \in \mathbb{C}$ for some specific i, j. Since $\mathbb{R}$ is infinite, $\exists$ some indices i, j and some $\lambda, \mu \in \mathbb{R}$, $\lambda \neq \mu$, such that

$\beta_{ij\lambda}$ & $\beta_{ij\mu}$ are both in $\mathbb{C}$.

Then since

$$\alpha_i + \alpha_j + \lambda \alpha_i \alpha_j = \beta_{ij\lambda} \in \mathbb{C}$$
$$\alpha_i + \alpha_j + \mu \alpha_i \alpha_j = \beta_{ij\mu} \in \mathbb{C}$$

it follows from the quadratic formula(?) that $\alpha_i, \alpha_j \in \mathbb{C}$.

Hence $f(x)$ has at least one root in $\mathbb{C}$.

QED

Whew !