**Math 461 F** **Spring 2011**
**Fundamental Theorem of Algebra** **Drew Armstrong**

---

When we proved the impossibility of the classical construction problems, we were interested in the existence of certain roots of polynomials. The flavor of what we did is contained in the following example: Suppose that a **cubic** polynomial $f(x)$ with **rational** coefficients has $1+\sqrt{2}$ as a root. Applying conjugation in the field extension $\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{2}]$ we conclude that $1-\sqrt{2}$ is also a root, and then we can use Descartes' Factor Theorem to conclude that

$$\begin{aligned} f(x) &= \Big(x-(1+\sqrt{2})\Big)\Big(x-(1-\sqrt{2})\Big)\,g(x) \\ &= (x^2-2x-3)g(x), \end{aligned}$$

for some polynomial $g(x)$ of degree 1 with coefficients in $\mathbb{Q}[\sqrt{2}]$. However, if we use long division to divide $f(x)$ by the polynomial $x^2-2x-3$ we find that $g(x)$ in fact has **rational** coefficients. That is, $g(x)=ax+b$ for some $a,b \in \mathbb{Q}$, in which case $-a/b$ is a root of $g(x)$, and hence $f(x)$. We conclude that $f(x)$ has a rational root.

This argument depends vitally on the fact that $f(x)$ is cubic; for higher degrees the proof falls apart. In general it is quite hard to tell whether a given polynomial has a root in a given field. (The exception is the field $\mathbb{Q}$ in which we can use the Rational Root Test.)

Over time people began to suspect that "every" polynomial has a root in the complex numbers $\mathbb{C}$. The precise statement of this is one of the most famous theorems in mathematics.

**The Fundamental Theorem of Algebra.** *Every polynomial in* $\mathbb{C}[x]$ *has a root in* $\mathbb{C}$.

The FTA is relatively difficult to prove and we will not see a really complete proof in this class. However, we will explore the FTA from several angles. Here is an immediate corollary.

**Corollary To FTA.** *Every polynomial in* $\mathbb{C}[x]$ splits *over* $\mathbb{C}$. *That is, we have*

$$f(x) = k(x-r_1)(x-r_2)\cdots(x-r_n)$$

*for some* $k, r_1, r_2, \ldots, r_n \in \mathbb{C}$.

*Proof.* We will use induction on the degree of $f(x)$. Suppose the Corollary has been proved for all complex polynomials of degree $< n$, and consider $f(x) \in \mathbb{C}[x]$ of degree $n$. By the FTA we know that $f(x)$ has a complex root, say $r \in \mathbb{C}$. Then by the Factor Theorem we can write $f(x) = (x-r)g(x)$ for some complex polynomial of degree $n-1$. By induction, $g(x)$ splits over $\mathbb{C}$. Hence $f(x)$ splits over $\mathbb{C}$. □

Strange as it may seem, when the FTA was first discovered and stated, it made no mention of complex numbers. From an 18th century perspective, why would they want to think about polynomials with *complex* coefficients? Complex numbers were just a necessary evil, used to solve *real* equations. In the time of Euler, they would have stated the theorem as follows.

**The *Real* Fundamental Theorem of Algebra.** *Every polynomial in* $\mathbb{R}[x]$ *factors into real polynomials of degrees* 1 *and* 2.

It becomes less elegant when you say it this way, but it has the advantage(?) of avoiding mention of "imaginary" numbers. Before proceeding, we should mention that (although they look different) the real and complex forms of FTA are logically equivalent.

**Theorem.** $\mathbb{C}FTA \Leftrightarrow \mathbb{R}FTA$.

*Proof.* First let us assume the $\mathbb{C}$FTA. In this case we wish to prove that $\mathbb{R}$FTA holds, so consider an arbitrary real polynomial $f(x) \in \mathbb{R}[x]$. Since $\mathbb{R} \subseteq \mathbb{C}$, the polynomial $f(x)$ also has complex coefficients (real numbers are by definition complex). Hence the $\mathbb{C}$FTA implies that $f(x)$ splits *over* $\mathbb{C}$. We also know that the non-real complex roots of $f(x)$ come in conjugate pairs. Hence we can write

$$f(x) = k\prod_{i=1}^{k}(x - r_i)\prod_{j=1}^{\ell}(x - z_j)(x - \overline{z_j}).$$

where $k, r_1, \ldots, r_k$ are real and $z_1, \ldots, z_\ell$ are complex and non-real. But then we have

$$f(x) = k\prod_{i=1}^{k}(x - r_i)\prod_{j=1}^{\ell}(x^2 - (z_j + \overline{z_j})x + z_j\overline{z_j}).$$

Since $z_j + \overline{z_j}$ and $z_j\overline{z_j}$ are real, we have factored $f(x)$ into degree 1 and 2 real polynomials, as desired.

Conversely, suppose that $\mathbb{R}$FTA holds. In this case we wish to prove $\mathbb{C}$FTA, so consider an arbitrary complex polynomial $p(x) \in \mathbb{C}[x]$. Let $\overline{p}(x)$ denote the conjugate polynomial (in which coefficients have been conjugated). You proved on HW5 that the polynomial $f(x) = p(x)\overline{p}(x)$ has real coefficients, hence it can be factored into degree 1 and 2 real polynomials. Then using the Quadratic Formula, each of these degree 2 real polynomials can be factored into two degree 1 complex polynomials. In other words, $f(x)$ splits over $\mathbb{C}$ and we can write

$$f(x) = k(x - r_1)(x - r_2)\cdots(x - r_{2n})$$

for some $k, r_1, r_2, \ldots, r_{2n} \in \mathbb{C}$ (because the degree of $f(x)$ is even). We wish to show that $p(x)$ splits over $\mathbb{C}$. Since $f(r_1) = p(r_1)\overline{p}(r_1) = 0$ we conclude that at least one of $p(r_1)$ and $\overline{p}(r_1)$ is zero. Without loss of generality, let's say that $p(r_1) = 0$. Now use the Factor Theorem to write $p(x) = (x - r_1)p'(x)$ for some $p'(x)$. Divide $(x - r_1)$ from both sides of the equation $f(x) = p(x)\overline{p}(x)$ to get

$$k(x - r_2)(x - r_3)\cdots(x - r_n) = p'(x)\overline{p}(x).$$

Now repeat the argument for $r_2, r_3, \ldots, r_n$. In the end we will succeed in splitting both $p(x)$ and $\overline{p}(x)$ over $\mathbb{C}$, which is even more than we needed to show. □

So, although we have proved *neither* form of the FTA, we now know that the two forms are logically equivalent. The very first proof of the FTA arose from a correspondence between Nicolaus Bernoulli and Leonhard Euler between the years 1742 and 1745. The proof had a few gaps, but the gaps were not really serious. Joseph-Louis Lagrange (born Giuseppe Lodovico Lagrangia) filled in most of the details by 1772. Even so, when Gauss published the "first" proof of FTA in 1799, he cricized the Bernoulli-Euler-Lagrange proof for assuming the existence of a splitting field for any real polynomial. Gauss had a point, but the existence of splitting fields was set on a firm basis by Kronecker in the late 1800's, whose proof is abstract but really not difficult. Ironically, Gauss' accepted "first" proof of FTA had a gap that proved much more difficult to fill, and was not completed until 1920.

I have posted Euler's account of his own proof on the course website.