# A Galois-Theoretic Proof of the Fundamental Theorem of Algebra

Laura Zielinski
The University of Chicago
Abstract Algebra, Winter 2023

This paper aims to provide a Galois-theoretic proof of the fundamental theorem of algebra which requires only a knowledge of basic group theory, ring theory, and Galois theory. Importantly, the theorem states that any polynomial of degree $d$ with complex coefficients has exactly $d$ complex roots, and can thus be written as the product of $d$ linear factors.

**Remark.** *We take fields to be commutative rings where $1 \neq 0$ and all nonzero elements have a multiplicative inverse.*

**Remark.** *Let $F$ be a field. We say a polynomial with coefficients in $F$ is a* polynomial over $F$*, i.e. an element of $F[x]$.*

## Algebraic Closures

The statement of the fundamental theorem of algebra requires the notion of an algebraic closure, which intuitively is the smallest extension of a field $F$ over which every polynomial in $F[x]$ splits completely.

**Definition** (Algebraic extension)**.** *Let $F$ be a field and let $K$ be an extension of $F$. An element $\alpha \in K$ is* algebraic *over $F$ if there is a polynomial over $F$ that has $\alpha$ as a root. Furthermore, $K$ is an* algebraic extension *of $F$ (alternatively, $K/F$ is algebraic) if every $\alpha \in K$ is algebraic over $F$.*

**Definition** (Algebraically closed)**.** *A field $K$ is* algebraically closed *if every non-constant polynomial over $K$ has a root in $K$.*

**Corollary.** *If a field $K$ is algebraically closed, then every non-constant polynomial over $K$ splits completely over $K$.*

*Proof.* Let $f(x)$ be a non-constant polynomial over $K$. Recall that $f(x)$ splits completely over $K$ if and only if we can write $f(x)$ as a product of linear factors in $K[x]$. We induct on the degree of $f(x)$.

Suppose $f(x)$ has degree 1, then $f(x) = ax + b$ for $a, b \in K$ where $a \neq 0$. Hence, we can write $f(x) = a \cdot (x + b/a)$, so $f(x)$ splits completely over $K$.

Next, suppose $f(x)$ has degree $d > 1$, and assume every polynomial of degree $d - 1$ splits completely over $K$. Since $K$ is algebraically closed, $f(x)$ has a root $\alpha$ in $K$. Then we can write $f(x) = (x - \alpha) \cdot g(x)$ where $g(x)$ is a degree $d-1$ polynomial over $K$. By the inductive hypothesis, $g(x)$ splits completely over $K$ so $f(x)$ splits completely over $K$ as well. □

**Definition** (Algebraic closure)**.** *An* algebraic closure *of a field $F$ is an algebraic extension which is algebraically closed.*

For any field $F$, we will show an algebraic closure exists which moreover is unique up to isomorphism. In other words, any field $F$ has an algebraic extension over which all polynomials over $F$ split completely. For example, we will prove later that the algebraic closure of $\mathbb{R}$ is $\mathbb{C}$.

**Lemma.** *Let $F$ be a field. Then there exists an algebraically closed extension of $F$.*

*Proof.* Let $\{f_\sigma(x) \mid \sigma \in S\} \subseteq F[x]$ denote all nonconstant monic polynomials over $F$, where $S$ is an indexing set. For each $\sigma \in S$, let $x_\sigma$ be an indeterminate. Consider $R = F[x_\sigma \mid \sigma \in S]$, the ring of polynomials over $F$ with indeterminates in $\{x_\sigma \mid \sigma \in S\}$. Let $I \subseteq R$ be the ideal generated by $\{f_\sigma(x_\sigma) \mid \sigma \in S\}$, i.e. the collection of all finite linear combinations of elements from $\{f_\sigma(x_\sigma) \mid \sigma \in S\}$.

We will show that $I$ is a proper ideal. Suppose for the sake of contradiction that $I = R$. Hence, $1 \in I$ and so there exist polynomials $g_1, \ldots, g_k \in R$ and $\sigma_1, \ldots, \sigma_k \in S$ for some $k$ such that

$$1 = g_1 f_{\sigma_1}(x_{\sigma_1}) + \cdots + g_k f_{\sigma_k}(x_{\sigma_k}) \in I.$$

For each $i \in \{1, \ldots, k\}$, let $\alpha_i$ be a root of $f_{\sigma_i}(x_{\sigma_i})$, which we defined to be nonconstant. Then

$$1 = g_1 f_{\sigma_1}(\alpha_1) + \cdots + g_k f_{\sigma_k}(\alpha_k) = 0$$

in $R(\alpha_1, \ldots, \alpha_k)$, which is a contradiction. Thus, $I$ must be a proper ideal.

By Zorn's lemma, there is some maximal ideal $\mathfrak{m}$ of $R$ containing $I$. Furthermore, $R/\mathfrak{m}$ is a field, which we denote $K_1$. We can define a map $F \to R \to K_1$ by composing inclusion with the natural quotient map, which is a homomorphism between fields and thus injective. Hence, we consider $K_1$ to be a field extension of $F$.

For any element $y \in F$, let $\overline{y}$ denote its image in $K_1$. Hence, for each $\sigma \in S$, we have that $f_\sigma(x_\sigma) \in I \subseteq \mathfrak{m}$ so $\overline{f_\sigma(x_\sigma)} = 0$. It follows that $\overline{x_\sigma} \in K_1$ is a root of $f_\sigma(x)$, so every nonconstant polynomial over $F$ has a root in $K_1$. We can repeat this construction with $K_1$ instead of $F$ to define an extension $K_2$ of $K_1$, and so on. Hence, for each $i \in \mathbb{Z}_{\geq 0}$, every nonconstant polynomial over $K_i$ has a root in $K_{i+1}$ (defining $K_0 = F$).

Let $K = \bigcup_{i \geq 0} K_i$, a field extension of $F$. Let $f(x)$ be a nonconstant polynomial over $K$; then there exists $j \in \mathbb{Z}_{\geq 0}$ such that $f(x) \in K_j[x]$. Furthermore, $f(x)$ has a root in $K_{j+1} \subseteq K$, so $K$ is algebraically closed. $\square$

**Proposition.** *Let $F$ be a field. Then there exists an algebraic closure of $F$.*

*Proof.* By the previous lemma, there exists an algebraically closed extension $K$ of $F$. Let $\overline{F}$ denote the set of elements of $K$ which are algebraic over $F$. By definition, $\overline{F}$ is an algebraic extension of $F$, as all elements of $F$ are trivially algebraic over $F$ and so $F \subseteq \overline{F}$.

Let $f(x)$ be a nonconstant polynomial over $\overline{F} \subseteq K$. Since $K$ is algebraically closed, $f(x)$ has a root $\alpha$ in $K$. Hence, as $\alpha$ is algebraic over $\overline{F}$, we have that $\overline{F}(\alpha)$ is an algebraic extension of $\overline{F}$. As $\overline{F}$ is an algebraic extension of $F$, thus $\overline{F}(\alpha)$ is an algebraic extension of $F$ by transitivity. In particular, $\alpha$ is algebraic over $F$, so $\alpha \in \overline{F}$. It follows that $\overline{F}$ is algebraically closed, and therefore an algebraic closure of $F$. $\square$

**Proposition.** *Let $F$ be a field. Then its algebraic closure is unique up to isomorphism.*

We omit the proof of this proposition, which uses Zorn's lemma and is similar to the proof of the uniqueness of splitting fields. Hence, "the" algebraic closure of a field $F$, denoted $\overline{F}$, can be thought of as the largest algebraic extension of $F$ as well as the smallest algebraically closed extension of $F$.

To see the first statement, given any algebraic extension $K$ of $F$, we have that $\overline{K}$ is an algebraic closure of $F$ and thus isomorphic to $\overline{F}$. Since $\overline{K}$ is an extension of $K$, it follows that $\overline{F}$ is an extension of $K$. To see the second statement, given any algebraically closed extension $K$ of $F$, as in the proof above, $\overline{F}$ is the set of elements which are algebraic over $F$, and so $K$ is an extension of $\overline{F}$.

## Normal Closures

We also require the notion of a normal closure for algebraic extensions, though it is a less useful one than that of an algebraic extension.

**Definition** (Normal extension)**.** *Let $F$ be a field and let $K$ be an algebraic extension of $F$. Then $K$ is a* normal extension *of $F$ (alternatively, $K/F$ is normal) if every irreducible polynomial over $F$ with one root in $K$ splits completely over $K$, i.e. has all its roots in $K$.*

**Definition** (Normal closure)**.** *Let $F$ be a field and let $K$ be an algebraic extension of $F$. An algebraic extension $N$ of $K$ is a* normal closure *of $K/F$ if $N$ is a normal extension of $F$ which is minimal. That is, the only subfield of $N$ which is both algebraic over $K$ and normal over $F$ is itself.*

**Proposition.** *Let $K/F$ be a finite algebraic extension. Then there exists a unique (up to isomorphism) normal closure of $K/F$ which is also a finite extension of $K$.*

*Proof.* As $K/F$ is finitely generated, we can write $K = F(\alpha_1, \ldots, \alpha_k)$ for some $\{\alpha_1, \ldots, \alpha_k\} \subseteq K$. Moreover, as $K/F$ is algebraic, for each $i \in \{1, \ldots, k\}$ we can take $P_{\alpha_i}(x)$ to be the minimal polynomial of $\alpha_i$ over $F$. Let $f(x) = P_{\alpha_1}(x) \cdots P_{\alpha_k}(x)$ and take $N$ to be the splitting field of $f(x)$, a finite extension of $F$. Hence, $N/F$ is a normal extension as well. Furthermore, as $N$ contains all the roots of each $P_{\alpha_i}$, we have $\{\alpha_1, \ldots, \alpha_k\} \subseteq N$ and so $N$ is a finite extension of $K$ and thus algebraic.

Let $N'$ be another algebraic extension of $K$ which is normal over $F$. Then, for each $i \in \{1, \ldots, k\}$, $N'$ contains $\alpha_i$ so must contain all roots of $P_{\alpha_i}(x)$. It follows that $N'$ contains all roots of $f(x)$ and so must be an extension of its splitting field, $N$. Hence, $N$ must be a normal closure of $K/F$; by the same argument, it must be unique up to isomorphism. $\square$

In fact, a normal closure exists for non-finite algebraic extensions as well; for our purposes, however, we need only the finite case.

### The Fundamental Theorem of Algebra

We now display a Galois-theoretic proof of the fundamental theorem of algebra and discuss its consequences. Our proofs uses the first Sylow theorem, which we now state, as well as three more results.

**Theorem** (First Sylow theorem)**.** *For every prime factor $p$ with multiplicity $n$ of the order of a finite group $G$, there exists a subgroup of $G$ of order $p^n$.*

**Lemma.** *A real polynomial of odd degree has a real root.*

*Proof.* Let $g(x)$ be a real polynomial of degree $d$ where $d$ is odd. Take $f(x)$ to be $g(x)$ divided by its leading coefficient so that $f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_0$ is monic. Let $m = \max\{|a_i| \mid i \in \{0, \ldots, d-1\}\}$ and let $y = m \cdot d + 1$. Hence,

$$\begin{aligned} f(y) &\geq y^d - |a_{d-1}y^{d-1} + \cdots + a_0| \\ &\geq y^d - (|a_{d-1}||y^{d-1}| + \cdots + |a_0|) \\ &\geq y^d - m \cdot d \cdot y^{d-1} = y^{d-1}(y - m \cdot d) > 0. \end{aligned}$$

Similarly, $f(-y) < 0$. Hence, by the intermediate value theorem, as real polynomials are continuous, there is some $\alpha \in (-y, y)$ such that $f(\alpha) = 0$. Then $\alpha$ is a real root of $f(x)$, and thus a real root of $g(x)$. $\square$

**Corollary.** *There are no nonlinear irreducible real polynomials of odd degree.*

*Proof.* Let $f(x)$ be a nonlinear real polynomial of odd degree. By the previous lemma, $f(x)$ has a root $\alpha \in \mathbb{R}$. But then $f(x) = (x - \alpha) \cdot g(x)$ where $g(x)$ is a real nonconstant polynomial, so $f(x)$ is reducible. $\square$

**Lemma.** *$\mathbb{C}$ has no extension of degree 2.*

*Proof.* Let $K$ be an extension of $\mathbb{C}$ and suppose for the sake of contradiction $[K : \mathbb{C}] = 2$. Then $K \neq \mathbb{C}$ so we can find some $\alpha \in K \setminus \mathbb{C}$. Thus, $[\mathbb{C}(\alpha) : \mathbb{C}] > 1$ and divides $[K : \mathbb{C}]$, so $[\mathbb{C}(\alpha) : \mathbb{C}] = 2$. Moreover, the minimal polynomial $f(x)$ of $\alpha$ over $\mathbb{C}$ is a quadratic monic irreducible polynomial.

Let $f(x) = x^2 + bx + c$. By the quadratic formula, $(-b \pm \sqrt{b^2 - 4c})/2$ are the roots of $f(x)$. As every complex number has a complex square root, $f(x)$ can be written as the product of two linear polynomials over $\mathbb{C}$. Thus, $f(x)$ is not irreducible, a contradiction. $\square$

**Theorem** (Fundamental theorem of algebra)**.** *The field $\mathbb{C}$ is algebraically closed.*

*Proof.* We aim to show that any nonconstant polynomial $f(x)$ over $\mathbb{C}$ has a root in $\mathbb{C}$. If $\alpha$ is a root of $f(x)$, then $\mathbb{C}(\alpha)$ is an extension of $\mathbb{C}$ such that $[\mathbb{C}(\alpha) : \mathbb{C}] \leq \deg(f(x))$, and so $\mathbb{C}(\alpha)$ is a finite extension containing a root of $f(x)$. Hence, it suffices to show that $\mathbb{C}$ has no proper finite extensions, as then we know $\mathbb{C}(\alpha) = \mathbb{C}$ and so $\mathbb{C}$ contains a root of $f(x)$.

Let $K_1$ be a finite extension of $\mathbb{C}$. Considering $\mathbb{C}$ an extension of $\mathbb{R}$, we have that $[\mathbb{C} : \mathbb{R}] = 2$ as $\{1, i\}$ is a basis of $\mathbb{C}$ over $\mathbb{R}$. Thus, $K_1$ is a finite extension of $\mathbb{R}$ as well and hence an algebraic extension. Let $K$ be the normal closure of $K_1/\mathbb{R}$, which means $K$ is a normal extension of $\mathbb{R}$. Moreover, as $K_1/\mathbb{R}$ is finite, we have $K/\mathbb{R}$ is finite as well and thus algebraic. We also know $K/\mathbb{R}$ is separable since $\mathbb{R}$ has characteristic 0. Therefore, $K$ is a finite Galois extension of $\mathbb{R}$, and thus a finite Galois extension of $\mathbb{C}$. Let $G = \mathrm{Gal}(K/\mathbb{R})$ where $|G| = [K : \mathbb{R}]$.

We have that $[\mathbb{C} : \mathbb{R}] = 2$ divides the order of $G$. Denote the maximal multiplicity of 2 in $|G|$ by $n$; hence, by the first Sylow theorem, there is some subgroup $H$ of $G$ of order $2^n$ such that $[G : H]$ is odd. By the fundamental theorem of Galois theory, there is an intermediate extension $E$ of $K/\mathbb{R}$ such that $[E : \mathbb{R}] = [G : H]$.

We have $E/\mathbb{R}$ is algebraic as it is finite. Take $\alpha \in E$ and let $P_\alpha(x)$ be its minimal polynomial over $\mathbb{R}$. As $[\mathbb{R}(\alpha) : \mathbb{R}] = \deg(P_\alpha(x))$ and $[R(\alpha) : \mathbb{R}]$ divides $[E : \mathbb{R}]$ which is odd, we must have $P_\alpha(x)$ has odd degree. By our corollary, $P_\alpha(x)$ must be linear so $\alpha \in \mathbb{R}$. Thus, $E = \mathbb{R}$ and so $[E : \mathbb{R}] = [G : H] = 1$. In particular, $G$ has order $2^n$. As $\mathrm{Gal}(K/\mathbb{C})$, denoted $M$, is also a subgroup of $G$, its order is $2^m$ for some $m \in \{0, \ldots, n\}$.

Suppose for the sake of contradiction $m > 0$. Again, by the first Sylow theorem, there is some subgroup $J$ of $M$ of order $2^{m-1}$ such that $[M : J] = 2$. By the fundamental theorem of Galois theory, there is an intermediate extension $E'$ of $K/\mathbb{C}$ such that $[E' : \mathbb{C}] = 2$, which contradicts our lemma. Hence, $m = 0$, which means $|M| = |\mathrm{Gal}(K/\mathbb{C})| = [K : \mathbb{C}] = 2^0 = 1$. Therefore, $K = \mathbb{C}$, and since $K_1$ was an intermediate extension of $K/\mathbb{C}$, it follows that $K_1 = \mathbb{C}$. We conclude that $\mathbb{C}$ has no proper finite extensions and is thus algebraically closed. $\square$