Nonostante possa sembrare bizzarro, non può esistere una dimostrazione puramente algebrica del celebre teorema fondamentale dell'Algebra (che asserisce che il campo complesso $\mathbb{C}$ è algebricamente chiuso). La motivazione essenziale di ciò consiste nel fatto che la definizione stessa di $\mathbb{C}$ è basata su quella di $\mathbb{R}$, ed il campo reale, come ben noto, è costruito con idee di Analisi, quali le sequenze di Cauchy o i tagli di Dedekind. Nonostante ciò la Teoria di Galois e quella dei Gruppi finiti ci forniscono una prova del teorema fondamentale dell'Algebra che faccia uso solamente di un minuscolo quantitativo di Analisi. Precisamente, assumeremo per noti i seguenti due fatti.

Lemma 1 *1. Ogni polinomio a coefficienti reali di grado dispari, ammette una radice reale.*

2. Per ogni $\alpha \in \mathbb{C}$ esiste un $\beta \in \mathbb{C}$ tale che $\beta^2 = \alpha$.

La parte puramente algebrica della dimostrazione è contenuta nel seguente.

Theorem 1 *Siano $R \subset C$ due campi di caratteristica zero e tali che $|R : C| = 2$. Assumiamo che valgano le seguenti ipotesi:*

1. *Ogni polinomio $f(X) \in R[X]$ a coefficienti in R di grado dispari, ha una radice in R.*

2. *Per ogni $\alpha \in C$ esiste un $\beta \in C$ tale che $\beta^2 = \alpha$.*

Allora il campo C è algebricamente chiuso.

Proof. Occorre e basta mostrare che non esistono estensioni algebriche proprie $L \supset C$.
Sia per assurdo $L \supset C$ un'estensione algebrica e sia $\alpha \in L \setminus C$.
Allora $|C[\alpha] : C| < \infty$ e anche $|C[\alpha] : R| < \infty$. Sia $E \supseteq C[\alpha]$ un campo di spezzamento per qualche polinomio su R (ad esempio per il polinomio *prodotto dei polinomi minimi* $\min_R(\alpha)$ e $\min_R(\delta)$, ove δ è un qualunque elemento di $C \setminus R$, ovvero tale per cui $C = R[\delta]$ – si ricordi che $|C : R| = 2$ –). Poiché la caratteristica di R è zero, l'estensione $E \supset R$ risulta separabile e quindi è di Galois. Sia G il gruppo di Galois di tale estensione. Proviamo che G è un $2-$gruppo finito, ovvero che $|G|$ è una potenza di 2. A tal fine sia $S \in Syl_2(G)$, un $2-$sottogruppo di Sylow di G, e sia $K := \mathrm{Inv}_E(S)$, il campo degli elementi di E fissati da S. Allora per la connessione di Galois abbiamo che

$$|K : R| = |G : S| = \text{ un numero dispari.}$$

Preso β un qualunque elemento di K e posto $f = \min_R(\beta)$, il suo polinomio minimo su R, allora

$$\deg(f) = |R[\beta] : R| \text{ divide } |K : R|$$

e pertanto $f(X)$ ha grado dispari. Per l'ipotesi *1.* segue che esiste una radice per f in R, ma essendo f un polinomio irriducibile su R, si deduce che $\deg(f) = 1$,

ovvero $F(X) = X - \beta$ e quindi $\beta \in R$. Data la genericità con cui si è scelto β in K, abbiamo che $K = R$, pertanto G coincide con il suo 2−Sylow S e quindi ha per ordine una potenza di 2.
Sia ora H il gruppo di Galois $Gal(E|C)$. Abbiamo che $H \leq G$, quindi H ha ordine potenza propria di 2 ($|H| = |E : C| > 1$, poiché $\alpha \in E \setminus C$). Per i noti risultati sui gruppi finiti, esiste un sottogruppo (massimale) M di H tale che $|H : M| = 2$. Sia $F := \mathrm{Inv}_E(M)$, allora $|F : C| = |H : M| = 2$. Preso $\gamma \in F \setminus C$ e sia $q := \min_C(\gamma)$, il suo polinomio minimo su C. Allora $\deg(q) = 2$. Per l'ipotesi *2.*, C è chiuso per l'operazione di estrazione di radice quadrata, quindi è possibile applicare la formula risolutiva per le equazioni di II grado e garantire con ciò l'esistenza di una radice di $q(X)$ in C. Questo è assurdo poiché $q(X)$ è per definizione un polinomio irriducible in $C[X]$ di grado 2. □

Corollary 1 $\mathbb{C}$ *è algerbicamente chiuso.*

Proof. Si applica il Teorema precedente con $R = \mathbb{R}$, $C = \mathbb{C}$ e si usa il Lemma 1 per verificare le ipotesi. □