

The Fundamental Theorem of Algebra is the assertion that the field \mathbf{C} of complex numbers is algebraically closed. Ie, every polynomial in \mathbf{C} splits. I have read that this was first rigorously proved by Gauss. However, I have also read that some of the proofs Gauss gave were incorrect. At any rate, there are now several correct proofs of this fact. My personal favorite is the one on page 184 of Rudin's book *Principles of Mathematical Analysis*. That proof uses only point-set topology. There are several other famous proofs: a complex analytic proof and a proof using very basic notions of algebraic topology (which is really an adaptation of the complex analytic proof).

Then there is the following proof using Galois theory. The main criticism people seem to have of this proof is that it is an algebraic proof of an essentially analytic fact. The point is that the topological properties (in particular, completeness) of \mathbf{C} or \mathbf{R} are an essential part of why the theorem is true. I agree with this criticism. However, I still think this proof is interesting. The proof I give is essentially the same as the one in Milne's text. However, I have abstracted the properties of \mathbf{R} we need by copying a definition from wikipedia. (This mitigates the above criticism somewhat because we get a theorem that is more general than the fundamental theorem of algebra.)

Definition 1. A field F is called *formally real* if -1 is not the sum of squares in F . A formally real field F is called a *real closed field* if every polynomial of odd degree has a root in F and, for every $a \in F$, there is a $b \in F$ such that either $a = b^2$ or $a = -b^2$.

Note that if F is formally real, then the characteristic of F must be 0. For, if F has characteristic p , then $-1 = (p-1) \cdot 1$.

The only analytic fact we will use is the following.

Theorem 2. *The real numbers are a real closed field.*

Proof. The number -1 is not the sum of squares in \mathbf{R} because the positive reals are closed under addition. The intermediate value theorem implies that every odd degree polynomial has a root in \mathbf{R} . (Note that the intermediate value theorem is a very deep analytic fact about \mathbf{R} . So we have actually used a lot of analysis already.)

I am going to use a lemma which is an important fact in its own right.

Lemma 3. *Let M/F be a finite separable field extension. Then there exists a finite extension L/M such that L/F is Galois.*

Proof. We have $M = F[\alpha_1, \dots, \alpha_r]$ for some $\alpha_i \in M$. Let f_i denote the minimal polynomial of α_i over F and set $f = \prod f_i$. Since M/F is separable, the f_i are separable. Thus f is also separable. Now set L equal to the splitting field of f over F .

Lemma 4. *Let F be a real closed field, and let P denote the set of $a \in F$ such that a is a non-zero square. Then P is closed under addition and multiplication. Moreover, F is the disjoint union of P , $-P$ and $\{0\}$. (The elements of P are sometimes called the positive elements of F .)*

Proof. It is obvious that P is closed under multiplication. Suppose that $x^2, y^2 \in P$. Then $x^2 + y^2 \neq 0$ because $x^2 = -y^2 \Rightarrow (x/y)^2 = -1$. By the definition of a real closed field, we have either $x^2 + y^2 = z^2$ or $x^2 + y^2 = -z^2$. In the second case, $z \neq 0$. Therefore $(x/z)^2 + (y/z)^2 = -1$. This contradicts the assumption that F is formally real. Therefore, only the first case can occur.

Now, suppose $a \in F$. If $a \neq 0$, we either have $a = z^2$ or $a = -z^2 \Rightarrow -a = z^2$. Thus F is the union of P , $-P$ and $\{0\}$. To show that this union is disjoint, we only need to show that $P \cap (-P) = \emptyset$. To see this, suppose $z^2 = -w^2 \neq 0$. Then $(z/w)^2 = -1$. Q.E.D.

Suppose F is a formally real field. Set $C = C(F)$ equal to $F[x]/(x^2 + 1)$. Then C is a field because, since -1 is not a square in F , the polynomial $x^2 + 1$ is irreducible in F . It is conventional to write i for the image of x in C so that $C = F[i]$.

Lemma 5. *Suppose F is a real closed field. Let $C = C(F)$ be as above. Then every element of C is a square.*

Proof. Suppose $a + ib \in F$, and suppose first that $a^2 + b^2 = 1$. Then, it follows easily from the fact that $b^2 = (1 - a)(1 + a)$ that $1 - a$ and $1 + a$ are both in P . Set $a + ib = (c + id)^2$ where

$$c = \sqrt{\frac{1+a}{2}}, d = \sqrt{\frac{1-a}{2}}$$

and the square roots are the taken to be both in P for $b \in P$ and with $c \in P$ and $d \in (-P)$ otherwise. (To guess the formula above, I used the formula $\cos \theta = 2 \cos^2(\theta/2) - 1 = 1 - 2 \sin^2(\theta/2)$.)

Now suppose $x + iy$ is a non-zero element of F . We have $x^2 + y^2 \in P$. Thus $x + iy = (x^2 + y^2)^{1/2}(a + bi)$ with $a^2 + b^2 = 1$. It follows easily that $x + iy$ is a square.

Corollary 6. *Let F be a real closed field and $C = C(F)$. Then C has no quadratic field extensions.*

Proof. Since C has characteristic 0, any quadratic field extension is obtained by adjoining a square root of an element of C which is not a square in C (by the quadratic equation).

Theorem 7. *Let F be a real closed field and $C = C(F)$. Then C is an algebraically closed field. (Ie, every polynomial in C splits.)*

Proof. To show that C is algebraically closed it suffices to show that every monic polynomial f in C splits in C . Suppose that f is a monic polynomial that does not split in C . Write M/C for the splitting field of f over C . By Lemma 3, we can find L/M such that L/F is Galois. Therefore, to proof Theorem 4, it suffices to show that there is no extension L/C of degree greater than 1 which is Galois over F .

To get a contradiction, suppose then that L/C is an extension of degree greater than 1 which is Galois over F . Set $G = \text{Gal}(L/F)$. I claim that G has order a power of 2. To see this, suppose the 2-Sylow subgroup P of G is a proper subgroup of G . Set $K = L^P$. Then K/F is an odd degree extension with $[K : F] > 1$. Thus we can find $\alpha \in K$ such that $[F(\alpha) : F] > 1$. But, since $[F(\alpha) : F]$ divides $[K : F]$, $[F(\alpha) : F]$ is odd. Therefore the minimal polynomial of α over F is odd. But this is a contradiction because there are no non-linear irreducible polynomials of odd degree over F .

Therefore G has order a power of 2. Write $H := \text{Gal}(L/C)$. Then H is an index 2 normal subgroup of G . Since H is a 2-group, H is solvable. Therefore, H contains a subgroup H_1 of index 2. Thus L^{H_1}/C is a quadratic extension. This is a contradiction to Corollary 6.