Section V.3.Appendix. The Fundamental Theorem of Algebra

Note. The Fundamental Theorem of Algebra states that the field of complex numbers, $\mathbb{C}$, is algebraically closed. If you like, it states that any polynomial of degree n with complex coefficients has n complex roots (counting multiplicity). You would be right to expect that we are now in a position to use the material we have developed to prove the Fundamental Theorem of Algebra. Surprisingly, the algebraic equipment we have developed is *not* sufficient for us to give a complete proof!

Note. Every known proof of the Fundamental Theorem of Algebra depends on some result(s) from analysis. We shall give a proof which is algebraic, except for the following two results from analysis:

(A) Every positive real number has a real positive square root.

(B) Every polynomial in $\mathbb{R}[x]$ of odd degree has a root in $\mathbb{R}$ (that is, every irreducible polynomial in $\mathbb{R}[x]$ of degree greater than one has even degree).

Both results actually follow from the Axiom of Completeness of the real numbers.

Note. You will recall that the real numbers are a complete ordered field. You are very familiar with what a field is at this stage! An ordering of a field F is a subset P of F (called the positive subset) such that (i) P is closed under addition, (ii) P is closed under multiplication, and (iii) for any $a \in F$ then exactly one of the following holds: $a \in P$, $-a \in P$, or $a = 0$ (property (iii) is *The Law of Trichotomy*). An ordering on $\mathbb{R}$ is given by set $P = \{x \in \mathbb{R} \mid x > 0\}$. We use P to define "$<$" on $\mathbb{R}$ by defining $a < b$ to mean $b - a \in P$. Interestingly, one can prove that there is no ordering on the field $\mathbb{C}$. The Axiom of Completeness states that every set of real numbers with an upper bound has a least upper bound. To illustrate this, consider the subset $S_{\mathbb{Q}} = \{x \in \mathbb{Q} \mid x^2 < 2\}$ of field $\mathbb{Q}$. Set $S_{\mathbb{Q}}$ has an upper bound in $\mathbb{Q}$, say 2, but it has no least upper bound in $\mathbb{Q}$. So field $\mathbb{Q}$ is not complete (though it is an ordered field). However, set $S_{\mathbb{R}} = \{x \in \mathbb{R} \mid x^2 < 2\}$ has an upper bound in $\mathbb{R}$, say 2 again, and therefore by the Axiom of Completeness must have a least upper bound in $\mathbb{R}$. The least upper bound is $\sqrt{2}$ (in fact, this is the definition of $\sqrt{2}$ as a real number). Result (A) follows similarly and the real positive square root of positive $p \in \mathbb{R}$ is the least upper bound of $\{x \in \mathbb{R} \mid x^2 < p\}$. Result (B) follows from the Intermediate Value Theorem which states (for our purposes) that a continuous function which is positive at real value a and negative at real value b, must be 0 for some real value between a and b (the Intermediate Value Theorem also follows from the Axiom of Completeness).

Note. The real numbers are defined as *a* complete ordered field. However, it can be shown that there is only one complete ordered field (up to isomorphism).

Note. Notes are posted online dealing with many of these ideas. Here are some references:

1. The real numbers as an ordered field:

`http://faculty.etsu.edu/gardnerr/4217/notes/1-2.pdf`

(notes from Analysis 1 [MATH 4217/5217]).

2. The Axiom of Completeness:

`http://faculty.etsu.edu/gardnerr/4217/notes/1-3.pdf`

(notes from Analysis 1 [MATH 4217/5217]).

3. The Intermediate Value Theorem:

`http://faculty.etsu.edu/gardnerr/4217/notes/4-1.pdf`

(notes from Analysis 1 [MATH 4217/5217]; see Corollary 4-9).

4. The complex number cannot be ordered:

`http://faculty.etsu.edu/gardnerr/5510/Ordering-C.pdf`

(notes from Complex Analysis 1 [MATH 5510]).

5. There is only one complete ordered field (that is, the real numbers are unique, up to isomorphism): See *Which Numbers are Real?* by Micael Henle, Washington, DC: Mathematical Association of America, Inc. (2012) (see Theorem 2.3.3 on page 48). Also see Chapter 29 "Uniqueness of the Real Numbers" of Michael Spivak's *Calculus*, 2nd Edition, Wilmington, DE: Publish or Perish, Inc. (1980).

Note. In the early study of equations, in particular by Niccoló Tartaglia, Gerolamo Cardano, and Ludovico Ferrari (circa 1540), it was noticed that a cubic equation always has three roots and a quartic equation always has four roots *if* we allow the use of complex numbers. In fact, the study of polynomial equations were inspiration for the acceptance of both negative and complex numbers as *numbers*. For more details, see my historical motivation for the undergraduate modern algebra class: `http://faculty.etsu.edu/gardnerr/4127/notes/Why-am-I-here.pdf`. The first to claim that an n degree polynomial equation must have n roots was Albert Girard in his 1629 *L'invention en algèbre*. However, a clear understanding of the reality of this claim was delayed by the lack of knowledge about complex numbers. Jean Le Rond D'Alembert made the first serious attempt at proving the Fundamental Theorem of Algebra in 1746. However, a lack of knowledge about compactness and completeness resulted in weaknesses in D'Alembert's "proof." Leonhard Euler proved that every real polynomial of degree n, where $n \leq 6$, has exactly n complex roots. Unsuccessful attempts to prove the Fundamental Theorem of Algebra include: Euler in 1749, Joseph-Louis Lagrange in 1772, and Pierre-Simon Laplace in 1795. Carl Friederich Gauss is usually credited with the first correct proof of the Fundamental Theorem. In his doctoral thesis in 1799 he gave a proof which today would be called "topological," but also by today's standards might be accepted as completely rigorous! Gauss published a second proof in 1816 which is "complete and correct." Gauss gave a third proof (again topological) in 1816. Of some importance is a proof published by Jean Robert Argand in 1814; Argand introduced a geometric interpretation of complex numbers as the complex plane which we use today. In 1849 Gauss gave the first proof that a polynomial equation of degree n

with complex coefficients has n complex roots. This brief historical description is based on (accessed 2/26/2015):

`http://www-history.mcs.st-and.ac.uk/HistTopics/Fund_theorem_of_algebra.html`

A more detailed historical survey is given by Daniel Velleman of Amherst College in "The Fundamental Theorem of Algebra: A Visual Approach" available online at (accessed 2/26/2015):

`http://www.cs.amherst.edu/~djv/FTAp.pdf`

My supplement on the history of the Fundamental Theorem is at (accessed 3/4/2015):

`http://faculty.etsu.edu/gardnerr/5410/notes/FTA-history.pdf`

Also see the PowerPoint presentation of the history which includes an intuitive argument for the validity of the F.T.A. (accessed 4/10/2015):

`http://faculty.etsu.edu/gardnerr/5410/notes/FTA-history.pptx`

Note. We need two more preliminary lemmas before proving the Fundamental Theorem. We include proofs in these notes.

Lemma V.3.17. If F is a finite dimensional separable extension of an infinite field K, then $F = K(u)$ for some $u \in F$.

Proof. Since F is a separable extension of K, then it is an algebraic extension and so by Theorem V.3.16(iii) there is a Galois extension F_1 of K that contains

F (here, $K \subset F \subset F_1$). Since we hypothesize $[F : K]$ is finite then by Theorem V.3.16(iv) we have that $[F_1 : K]$ is finite. By the Fundamental Theorem of Galois Theory (Theorem V.2.5(i)) $\mathrm{Aut}_K(F_1)$ is finite (since $|\mathrm{Aut}_K(F_1)| = [F_1 : K]$) and, since there is a one-to-one correspondence between the set of intermediate fields of the extension and the set of all subgroups of $\mathrm{Aut}_K(F_1)$ (by the Fundamental Theorem) with $|\mathrm{Aut}_K(F_i)| = [F_i : K]$ for each intermediate field F_i, then there are only finitely many intermediate fields between K and F_1. Therefore, there can be only a finite number of intermediate fields in the extension of K by F.

Since $[F : K]$ is finite, we can choose $u \in F$ such that $[K(u) : K]$ is maximal. ASSUME $K(u) \neq F$. Then there exists $v \in F \setminus K(u)$. Consider all (simple extension) intermediate fields of the form $K(u + av)$ with $a \in K$. Since K is an infinite field then there are infinitely many elements of F of the form $u + av$ where $u \in F$, $v \in F \setminus K(u)$, and $a \in K$. However, there are only finitely many intermediate fields between K and F. So for some $a, b \in K$ with $a \neq b$ we must have $K(u + av) = K(u + bv)$ (or else we have infinitely many simple extensions of K intermediate to K and F). So for this a and b, $u + bv \in K(u + av)$ and $(a - b)v = (u + av) - (u + bv) \in K(u + av)$. Since $a, b \in K$ and $a \neq b$, then $(a - b), (a - b)^{-1} \in K$ and so $v = (a - b)^{-1}(a - b)v \in K(u + av)$. Whence $av \in K(u+av)$ and $u = (u+av)-av \in K(u+av)$. So $u \in K(u+av)$ and $v \notin K(u)$ (by the choice of v), so $K \subset K(u) \subsetneq K(u+av)$ Whence $[K(u+av) : K] > [K(u) : K]$. But this CONTRADICTS the choice of u such that $[K(u) : K]$ is maximal (for all simple extensions of K). So the assumption that $K(u) \neq F$ is false and hence $F = K(u)$. ∎

Lemma V.3.18. There are no extension fields of dimension 2 over the field of complex numbers.

Proof. ASSUME F is an extension field of $\mathbb{C}$ of dimension 2 (that is, $[F:\mathbb{C}]=2$). Then a basis for F over $\mathbb{C}$ is of the form $\{1,u\}$ where $u\in F\backslash\mathbb{C}$ by Theorem V.1.6(iv) and $F=K(u)$. In fact, for *any* $u\in F\setminus\mathbb{C}$ we have $F=K(u)$ (if $u_1,u_2\in F\setminus\mathbb{C}$ then $a(1)+b(u_1)=u_2$ for some $a,b\in K$ and so $b^{-1}(-a)(1)+b^{-1}(u_2)=u_1$ and $\{1,u_2\}$ is a basis for $K(u_1)$). By Theorem V.1.6(ii) u must be a root of an irreducible monic polynomial $f\in\mathbb{C}[x]$ of degree 2. We next show that no such f can exist.

For each $a+bi\in\mathbb{C}=\mathbb{R}(i)$, we know that a^2+b^2 has a real positive square root be Assumption (A), denoted $\sqrt{a^2+b^2}$. Also by Assumption (A) the positive real numbers $(a+\sqrt{a^2+b^2})/2$ and $(-a+\sqrt{a^2+b^2})/2$ have real positive square roots, say c and d respectively. Now

(1) $(c+di)^2=c^2-d^2+2cdi=(a+\sqrt{a^2+b^2})/2-(-a+\sqrt{a^2+b^2})/2$

$$+2\sqrt{(a+\sqrt{a^2+b^2})/2\times(-a+\sqrt{a^2+b^2})/2}\,i=a+\sqrt{-a^2+(a^2+b^2)}\,i$$

$$=a+|b|i=a+bi \text{ if } b\geq 0.$$

(2) $(c-di)^2=c^2-d^2-2cdi=(a+\sqrt{a^2+b^2})/2-(-a+\sqrt{a^2+b^2})/2$

$$-2\sqrt{(a+\sqrt{a^2+b^2})/2\times(-a+\sqrt{a^2+b^2})/2}\,i=a-\sqrt{-a^2+(a^2+b^2)}\,i$$

$$=a-|b|i=a+bi \text{ if } b\leq 0.$$

Hence every element $a+bi$ has a square root in $\mathbb{C}$ (of course, $(-c-di)$ and $(-c+di)$ are also square roots when $b\geq 0$ and $b\leq 0$, respectively). Consequently, if $f(x)=x^2+sx+t\in\mathbb{C}[x]$, then f has roots $(-s\pm\sqrt{s^2-4t})/2$ in $\mathbb{C}$ (by the

quadratic equation—THANKS CLASSICAL ALGEBRA!), and so f splits over $\mathbb{C}$. So there are no irreducible monic polynomials of degree 2 in $\mathbb{C}[x]$ and as explained above this CONTRADICTS the assumption of the existence of $u \in F = \mathbb{C}(u)$ where $u \in F \setminus \mathbb{C}$. So there is no dimension 2 extension of $\mathbb{C}$. ∎

Theorem V.3.19. The Fundamental Theorem of Algebra.
The field of complex numbers is algebraically closed.

Proof. We need to show that every nonconstant polynomial $f \in \mathbb{C}[x]$ splits over $\mathbb{C}$. By Kronecker's Theorem (Theorem V.1.10) we know that for any u algebraic over $\mathbb{C}$, there exists extension field $\mathbb{C}(u)$ where $[\mathbb{C}(u) : \mathbb{C}] = \deg(u, \mathbb{C})$. So if we prove that $\mathbb{C}$ has no finite dimensional extension except itself, then the result will follow. Since $[\mathbb{C} : \mathbb{R}] = 2$ then every finite dimensional extension field E_1 of $\mathbb{C}$ is a finite dimensional extension of $\mathbb{R}$ because, by Theorem V.1.2, $[E_1 : \mathbb{R}] = [E_1 : \mathbb{C}][\mathbb{C} : \mathbb{R}]$. Now every algebraic extension field of a field of characteristic 0 is separable (see the Remark on page 261 and "Lemma" before Theorem V.3.11 in the notes for Section V.3) and $\text{char}(\mathbb{R}) = 0$, so E_1 is a separable extension of $\mathbb{R}$. By Theorem V.3.16(iii), there exists extension field F of $\mathbb{R}$ such that F contains E_1 and F is Galois over $\mathbb{R}$ (here, $\mathbb{R} \subset E_1 \subset F$). By Theorem V.3.16(iv) F is a finite dimensional extension of $\mathbb{R}$. That is, $[F : \mathbb{R}]$ is finite. We need only show that $F = \mathbb{C}$ to conclude $E_1 = \mathbb{C}$.

The Fundamental Theorem of Galois Theory (Theorem V.2.5(i)) shows that $|\text{Aut}_{\mathbb{R}}(F)| = [F : \mathbb{R}]$ is finite. So $\text{Aut}_{\mathbb{R}}(F)$ is a finite group of even order (since $[\mathbb{C} : \mathbb{R}] = 2$ divides $[F : \mathbb{R}]$). By the First Sylow Theorem (Theorem II.5.7) $\text{Aut}_{\mathbb{R}}(F)$ has a Sylow 2-subgroup H of order 2^n where 2^{n+1} does not divide $|\text{Aut}_{\mathbb{R}}(F)|$ (that is, the

Sylow 2-subgroup H has odd index $[\mathrm{Aut}_{\mathbb{R}}(F) : H]$). By the Fundamental Theorem (Theorem V.2.5(i)) for E the fixed field of H we have that E has odd dimension over $\mathbb{R}$ since $[E : \mathbb{R}] = [\mathrm{Aut}_{\mathbb{R}}(F) : H]$. Similar to above, since $\mathrm{char}(\mathbb{R}) = 0$ then E is separable over $\mathbb{R}$ and so by Lemma V.3.17 $E = \mathbb{R}(u)$ (notice that the fact that $\mathbb{R}$ is infinite is used here). Of course E is algebraic over $\mathbb{R}$. Thus the irreducible polynomial of u has odd degree $[E : \mathbb{R}] = [\mathbb{R}(u) : \mathbb{R}]$ by Theorem V.1.6(iii). By Assumption (B), every irreducible polynomial in $\mathbb{R}[x]$ of degree greater than one has even degree, so the degree of the irreducible polynomial in $\mathbb{R}[x]$ must be 1. Therefore $u \in \mathbb{R}$ and $[\mathrm{Aut}_{\mathbb{R}}(F) : H] = [E : \mathbb{R}] = [\mathbb{R} : \mathbb{R}] = 1$. Whence $\mathrm{Aut}_{\mathbb{R}}(F) = H$ and $|\mathrm{Aut}_{\mathbb{R}}(F)| = |H| = 2^n$. Consequently the subgroup $\mathrm{Aut}_{\mathbb{C}}(F)$ of $\mathrm{Aut}_{\mathbb{R}}(F)$ has order 2^m for some m where $0 \leq m \leq n$.

ASSUME $m > 0$. Then by the First Sylow Theorem (Theorem II.5.7), $\mathrm{Aut}_{\mathbb{C}}(F)$ has a subgroup J of index 2 (that is, $[\mathrm{Aut}_{\mathbb{C}}(F) : J] = 2$, or $|J| = |\mathrm{Aut}_{\mathbb{C}}(F)|/2$). Let E_0 be the fixed field of J. By the Fundamental Theorem of Galois Theory (Theorem V.2.5(i)) E_0 is an extension of $\mathbb{C}$ with dimension $[E_0 : \mathbb{C}] = [\mathrm{Aut}_{\mathbb{C}}(F) : J] = 2$. But this CONTRADICTS Lemma V.3.18. This contradiction to the assumption that $m > 0$ implies that $m = 0$. So $|\mathrm{Aut}_{\mathbb{C}}(F)| = 2^0 = 1$ and by the Fundamental Theorem of Galois Theory (Theorem V.2.5(i)) we have that $[F : \mathbb{C}] = [\mathrm{Aut}_{\mathbb{C}}(F) : \mathrm{Aut}_F(F)] = [\mathrm{Aut}_{\mathbb{C}}(F) : \{e\}] = |\mathrm{Aut}_{\mathbb{C}}(F)| = 1$ ($[\mathrm{Aut}_{\mathbb{C}}(F) : \{e\}]$ is the number of cosets of $\{e\}$ in $\mathrm{Aut}_{\mathbb{C}}(F)$ and so equals $|\mathrm{Aut}_{\mathbb{C}}(F)|$). Whence $F = \mathbb{C}$ and (since $\mathbb{C} \subset E_1 \subset F$) $E_1 = \mathbb{C}$. That is, every finite dimensional algebraic extension $\mathbb{C}$ equals $\mathbb{C}$ and $\mathbb{C}$ is algebraically closed. ∎

Corollary V.3.20. Every proper algebraic extension field of the field of real numbers is isomorphic to the field of complex numbers.

Proof. If F is an algebraic extension of $\mathbb{R}$ and $u \in F \setminus \mathbb{R}$ has irreducible polynomial $f \in \mathbb{R}[x]$ of degree greater than one, then by the Fundamental Theorem of Algebra (Theorem V.3.19) f splits over $\mathbb{C}$. If $v \in \mathbb{C}$ is a root of f then by Corollary V.1.9 the identity map on $\mathbb{R}$ extends to an isomorphism $\mathbb{R}(u) \cong \mathbb{R}(v) = \mathbb{C}$. Since $[\mathbb{R}(v) : \mathbb{R}] = [\mathbb{R}(u) : \mathbb{R}] > 1$ and $[\mathbb{C} : \mathbb{R}] = 2$, we must have $[\mathbb{C} : \mathbb{R}] = [\mathbb{C} : \mathbb{R}(v)][\mathbb{R}(v) : \mathbb{R}] = 2$ by Theorem V.1.2, and so it must be that $[\mathbb{R}(v) : \mathbb{R}] = 2$ and $[\mathbb{C} : \mathbb{R}(v)] = 1$. So $\mathbb{R}(v) = \mathbb{C}$. Therefore F is an algebraic extension of $\mathbb{R}(u)$ (which, in turn, is an algebraic extension of $\mathbb{R}$). But $\mathbb{R}(u) \cong \mathbb{R}(v) = \mathbb{C}$ and $\mathbb{C}$ is algebraically closed by the Fundamental Theorem of Algebra (Theorem V.3.19) and by Theorem V.3.3 (or the definition of "algebraically closed" on page 258) an algebraically closed field has no algebraic extensions (except itself). Thus it must be that $F = \mathbb{R}(u) \cong \mathbb{C}$. ∎

Note. In your graduate career, you have several opportunities to see a proof of the Fundamental Theorem of Algebra. Here are some of them:

1. In Complex Analysis [MATH 5510/5520] where Liouville's Theorem is used to give a very brief proof. See

`http://faculty.etsu.edu/gardnerr/5510/notes/IV-3.pdf`

(Theorems IV.3.4 and IV.3.5). You are likely to see the same proof in our Complex Variables class [MATH 4337/5337]. In fact, this is the proof which Fraleigh presents in his *A First Course In Abstract Algebra*, 7th Edition:

`http://faculty.etsu.edu/gardnerr/4127/notes/VI-31.pdf`

(see Theorem 31.18).

2. In Complex Analysis [MATH 5510/5520] *again* where Rouche's Theorem (based on the argument principle) is used:

`http://faculty.etsu.edu/gardnerr/5510/notes/V-3.pdf`

(see Theorem V.3.8 and page 4).

3. In Introduction to Topology [MATH 4357/5357] where path homotopies and fundamental groups of a surface are used:

`http://faculty.etsu.edu/gardnerr/5210/notes/Munkres-56.pdf`.

Note. There are no *purely* algebraic proofs of the Fundamental Theorem of Algebra [*A History of Abstract Algebra*, Israel Kleiner, Birkhäuser (2007), page 12]. There are proofs which are mostly algebraic, but which borrow result(s) from analysis (such as the proof presented by Hungerford). However, if we are going to use a result from analysis, the easiest approach is to use Liouville's Theorem from complex analysis. This leads us to a philosophical question concerning the legitimacy of the title "Fundamental Theorem of *Algebra*" for this result! If seems more appropriate to refer to it as "Liouville's Corollary"! Polynomials with complex coefficients are best considered as special analytic functions (an analytic function is one with a power series representation) and are best treated in the realm of complex analysis. Your humble instructor therefore argues that the Fundamental Theorem of Algebra is actually a result of some moderate interest in the theory of analytic complex functions. After all, *algebra* in the modern sense does not deal so much with polynomials (though this is a component of modern algebra), but instead deals with the theory of groups, rings, and fields!

Revised: 5/1/2018