Section VI.31. Algebraic Extensions

Note. In the past we have only discussed the extension of a field either abstractly or by a single element at a time (eg., $\mathbb{Q}(\sqrt{2})$). We generalize this idea in this section. We also introduce the idea of algebraic closure, give a brief proof based on complex analysis which shows that $\mathbb{C}$ is algebraically closed, and then show that every field has an algebraically closed extension field.

Definition 31.1. An extension field E of field F is an *algebraic extension* of F if every element in E is algebraic over F.

Example. $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$ are algebraic extensions of $\mathbb{Q}$. $\mathbb{R}$ is not an algebraic extension of $\mathbb{Q}$.

Definition 31.2. If an extension field E of field F is of finite dimension n as a vector space over F, then E is a *finite extension of degree n over F*. We denote this as $n = [E : F]$.

Example. $\mathbb{Q}(\sqrt{2})$ is a degree 2 extension of $\mathbb{Q}$ since every element of $\mathbb{Q}(\sqrt{2})$ is of the form $a + \sqrt{2}b$ where $a, b \in \mathbb{Q}$. $\mathbb{Q}(\sqrt[3]{2})$ is a degree 3 extension of $\mathbb{Q}$ since every element of $\mathbb{Q}(\sqrt[3]{2})$ is of the form $a + b(\sqrt[3]{2}) + c(\sqrt[3]{2})^2$ for $a, b, c \in \mathbb{Q}$. $\mathbb{C} = \mathbb{R}(i)$ is a degree 2 extension field of $\mathbb{R}$ since every element of $\mathbb{C}$ is of the form $a + bi$ for $a, b \in \mathbb{R}$.

Lemma. Let E be a finite degree extension of F. Then $[E : F] = 1$ if and only if $E = F$.

Proof. Trivially, $\{1\}$ is a basis of F (every element of F is of the form $a(1) = a$ where $a \in F$). So if $E = F$ then $[E : F] = [F : F] = 1$. Next, if $[E : F] = 1$, we know by Theorem 30.19 that the basis of F, $\{1\}$, can be extended to a basis of E and since $[E : F] = 1$, then the basis for E is also $\{1\}$. So every element of E is of the form $a(1) = a$ for $a \in F$. That is, $E = F$. ∎

Theorem 31.3. A finite (degree) extension field E of field F is an algebraic extension of F.

Note. The following result "plays a role in field theory analogous to the role of the theorem of Lagrange in group theory." (Page 283)

Theorem 31.4. If E is a finite extension field of a field F, and K is a finite extension field of E, then K is a finite extension of F and $[K : F] = [K : E][E : F]$.

Note. The following follows easily from Theorem 31.4 by Mathematical Induction.

Corollary 31.6. If F_i is a field for $i = 1, 2, \ldots, r$ and F_{i+1} is a finite extension of F_i, then F_r is a finite extension of F_1 and

$$[F_r : F_1] = [F_r : F_{r-1}][F_{r-1} : F_{r-2}] \cdots [F_2 : F_1].$$

Corollary 31.7. If E is an extension field of F, $\alpha \in E$ is algebraic over F, and $\beta \in F(\alpha)$, then $\deg(\beta, F)$ divides $\deg(\alpha, F)$.

Example 31.8. We can use Corollary 31.7 to quickly show certain elements are *not* in an extension field. For example, since $\deg(\sqrt{2}, \mathbb{Q}) = 2$ and $\deg(\sqrt[3]{2}, \mathbb{Q}) = 3$, then there is no element of $\mathbb{Q}(\sqrt{2})$ that is a zero of $x^3 - 2$ since 3 does not divide 2. Conversely, there is no element of $\mathbb{Q}(\sqrt[3]{2})$ that is a zero of $x^2 - 2$.

Note. Let E be an extension field of field F. Let $\alpha_1, \alpha_2 \in E$. By Note 29.1 and Note 29.2, $F(\alpha_1)$ is the smallest extension field of F containing α_1. We can iterate the process to get $(F(\alpha_1))(\alpha_2)$ as the smallest extension field of F containing both α_1 and α_2. (This field is equivalent to $(F(\alpha_2))(\alpha_1)$.) This field is denoted $F(\alpha_1, \alpha_2)$.

Definition. Let E be an extension field of field F. Let $\alpha_1, \alpha_2, \ldots, \alpha_n \in E$. $F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ is the smallest extension field of F in E containing $\alpha_1, \alpha_2, \ldots, \alpha_n$. Field $F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ is the field that results from *adjoining* $\alpha_1, \alpha_2, \ldots, \alpha_n$ *to field* F in E.

Note. One can show that $F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ is the intersection of all subfields of E which contains F and $\alpha_1, \alpha_2, \ldots, \alpha_n$.

Example 31.9. In Example 31.8, we saw that $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$ are quite different (i.e., $\sqrt{2} \notin \mathbb{Q}(\sqrt{3})$ and $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$). So what *is* $\mathbb{Q}(\sqrt{2}, \sqrt{3})$? First, $\{1, \sqrt{2}\}$ is a basis of $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$. So $\dim(\sqrt{2}, \mathbb{Q}) = 2$. Now, let's adjoin $\sqrt{3}$ to $\mathbb{Q}(\sqrt{2})$. We claim $\{1, \sqrt{3}\}$ is a basis for $(\mathbb{Q}(\sqrt{2}))(\sqrt{3})$. Then as illustrated in the proof of Theorem 31.4, a basis for $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$. So $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$ and

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b, c, d \in \mathbb{Q}\}.$$

The text argues that $p(x) = x^4 - 10x^2 + 1$ is irreducible over $\mathbb{Q}$ and that $\sqrt{2} + \sqrt{3}$ is a zero of $p(x)$. Notice $\sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$ and the degree of p is $4 = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}]$.

Theorem 31.11. Let E be an algebraic extension of a field F. Then there exists a finite number of elements $\alpha_1, \alpha_2, \ldots, \alpha_n$ in E such that $E = F(\alpha_1, \alpha_2, \ldots, \alpha_m)$ if and only if E is a finite dimensional vector space over F (i.e., if and only if E is a finite extension of F).

Note. We now define the "algebraic closure" of a field F which is, in a sense, the largest field containing F which includes F and all zeros of polynomials in $F[x]$. We give a proof of the Fundamental Theorem of Algebra (based on complex analysis), and conclude this section in a supplement that gives a lengthy demonstration that any field has an algebraic closure.

Theorem 31.12. If E is an extension field of field F then

$$\overline{F}_E = \{\alpha \in E \mid \alpha \text{ is algebraic over } F\}$$

is a subfield of E, called the *algebraic closure of F in E*.

Corollary 31.13. The set of all algebraic numbers over $\mathbb{Q}$ in $\mathbb{C}$ forms a field.

Note. It is also true that the algebraic numbers over $\mathbb{Q}$ in $\mathbb{R}$ form a field. In fact, the (complex) algebraic numbers $\mathbb{A}$ over $\mathbb{Q}$ form an algebraically closed field (see Exercise 31.33).

Definition 31.14. A field F is *algebraically closed* if every nonconstant polynomial in $F[x]$ has a zero in F.

Note. The next result gives a cleaner classification of an algebraically closed field.

Theorem 31.15. A field F is algebraically closed if and only if every nonconstant polynomial in $F[x]$ factors in $F[x]$ into linear factors.

Note. The next result gives us the "largest field" idea in detail.

Corollary 31.16. An algebraically closed field F has no proper algebraic extensions; that is, no algebraic extensions E with $F < E$.

Note. The following result is a big deal and should probably be part of the book's "basic goal." The proof requires some heavy duty equipment and we give it in a supplement.

Theorem 31.17/31.22. Every field F has an *algebraic closure*; that is, an algebraic extension $\overline{F}$ that is algebraically closed.

Note. We now state and prove the Fundamental Theorem of Algebra (another big "goal" of this class). We will give a proof based on complex analysis. The text says (page 288) "There are algebraic proofs, but they are much longer." In fact, there are no *purely* algebraic proofs [*A History of Abstract Algebra*, Israel Kleiner, Birkhäuser (2007), page 12]. There are proofs which are mostly algebraic, but which borrow two results from analysis: **(A)** A positive real number has a square root; and **(B)** An odd degree polynomial in $\mathbb{R}[x]$ has a real zero. (**(A)** follows from the Axiom of Completeness of $\mathbb{R}$, and **(B)** follows from the Intermediate Value Theorem, which is also based on the Axiom of Completeness.) However, if we are going to use a result from analysis, the easiest approach is to use Liouville's Theorem from complex analysis. We give a few more details than the text, but for a complete treatment of a proof based on Liouville's Theorem, see my Complex Analysis (MATH 5510, MATH 5520) notes online: `http://faculty.etsu.edu/gardnerr/5510/notes.htm` (see Sections IV.3 and V.3). For a mostly algebraic proof, see my online notes for Modern Algebra 1 [MATH 5410]: `http://faculty.etsu.edu/gardnerr/5410/notes/V-3-A.pdf`

Philosophical Note. Should the Fundamental Theorem of Algebra be called the "Fundamental Theorem of *Algebra*" when there is no purely algebraic proof?

Definition. A function $f : \mathbb{C} \to \mathbb{C}$ is *analytic* at a point $z_0 \in \mathbb{C}$ if the derivative of $f(z)$, $f'(z)$, is continuous at z_0. f is an *entire function* if it is analytic for all z_0 in the entire complex plane (i.e., for all $z_0 \in \mathbb{C}$).

Theorem. Liouville's Theorem.
If $f : \mathbb{C} \to \mathbb{C}$ is an entire function and f is bounded on $\mathbb{C}$ (i.e., there exists $b \in \mathbb{R}$ such that $|f(z)| \le b$ for all $z \in \mathbb{C}$), then f is a constant function.

Note. So Liouville's Theorem says that there are no bounded analytic functions of a complex variable! (Well, other than constant functions.) This is certainly not the case for real valued functions of a real variable x—consider $f(x) = \sin x$. We have $|\sin x| \le 1$ for all $x \in \mathbb{R}$. Surprisingly, $f(z) = \sin z$ is an unbounded function in the complex plane.

Claim 1. If $f(z) \in \mathbb{C}[z]$ is a nonconstant polynomial (so $f(z) \notin \mathbb{C}$), then

$$\lim_{|z|\to\infty} |f(z)| = \infty \text{ and } \lim_{|z|\to\infty} \frac{1}{|f(z)|} = 0.$$

Claim 2. Let $f : \mathbb{C} \to \mathbb{C}$ be an entire function where f has no zeros in $\mathbb{C}$ (i.e., $f(z) \ne 0$ for all $z \in \mathbb{C}$). Suppose $\lim_{|z|\to\infty} \frac{1}{|f(z)|} = 0$. Then f is constant in $\mathbb{C}$.

Idea of the Proof. If $\displaystyle\lim_{|z|\to\infty} \frac{1}{|f(z)|} = 0$, then for $|z|$ sufficiently large, $\frac{1}{|f(z)|} \le 1$ (say this holds for $|z| > R$). Since f has no zeros in $\mathbb{C}$, then $1/f(z)$ is continuous. So $|1/f(z)|$ has a maximum value on the compact set $|z| \le R$ (this is the Extreme Value Theorem), say M. Then $|1/f(z)|$ is bounded by $\max\{1, M\}$ and so by Liouville's Theorem, $1/f(z)$ is constant and hence $f(z)$ is constant. $\square$

Theorem 31.18. Fundamental Theorem of Algebra.
The field $\mathbb{C}$ is algebraically closed.

Proof. Let $f(z) \in \mathbb{C}[z]$ be a nonconstant polynomial. Assume f has no zero in $\mathbb{C}$. Then $1/f(z)$ is an entire function and by Claim 1, $\displaystyle\lim_{|z|\to\infty} \frac{1}{|f(z)|} = 0$. By Claim 2, $f(z)$ is constant, a contradiction. This contradiction implies that the assumption that $f(z)$ has no zero is false. So $f(z)$ has a zero in $\mathbb{C}$ and $\mathbb{C}$ is algebraically closed.
$\blacksquare$

Note. We now introduce the ideas necessary to prove that every field has an algebraic closure (Theorem 31.17/31.22). We need some ideas from set theory. This material is given in supplemental notes.

Note. In Section 49 we will see that the algebraic closure of a field is unique in the following sense:
Corollary 49.5. Let $\overline{F}$ and $\overline{F}'$ be two algebraic closures of F. Then $\overline{F}$ is isomorphic to $\overline{F}'$ under an isomorphism leaving each element of F fixed.

Note. If we start with field $\mathbb{Q}$, then we have that $\mathbb{Q} \subset \mathbb{A}$ (where $\mathbb{A}$ is the field of algebraic complex numbers) and $\mathbb{Q} \subset \mathbb{C}$. Both $\mathbb{A}$ and $\mathbb{C}$ are algebraically closed—$\mathbb{A}$ is algebraically closed by Exercise 31.33, and $\mathbb{C}$ is algebraically closed by the Fundamental Theorem of Algebra (Theorem 31.18). *An* algebraic closure (or *the* algebraic closure, after we prove Corollary 49.5) of $\mathbb{Q}$ is $\mathbb{A}$. The complex numbers $\mathbb{C}$ are an algebraically closed extension field of $\mathbb{Q}$, but $\mathbb{C}$ is not an algebraic closure of $\mathbb{Q}$ since $\mathbb{C}$ is not an *algebraic extension* of $\mathbb{Q}$.

Revised: 3/21/2015