Supplement. Algebraic Closure of a Field

Note. In this supplement, we give some background material which is used in the proof of Fraleigh's Theorem 31.17/31.22 (Every field has an algebraic closure). All proofs require some set theoretic background.

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.

Note. The following result is a big deal and should probably be part of Fraleigh's "basic goal." This result simply claims the existence of an algebraic closure of a field but, as we'll see, neither the result nor its proof give insight as to *how* to construct the algebraic closure of a field.

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 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.

Definition 31.19. A *partial ordering* of a set S is given by a relation denoted $\leq$ defined for certain ordered pairs of elements of S such that the following are satisfied:

1. $a \leq a$ for all $a \in S$ (Reflexive Law).

2. If $a \leq b$ and $b \leq a$ then $a = b$ (Antisymmetric Law).

3. If $a \leq b$ and $b \leq c$ then $a \leq c$ (Transitive Law).

If for $a, b \in S$ we have either $a \leq b$ or $b \leq a$ then a and b are *comparable*. A subset $T \subseteq S$ is a *chain* if every two elements a and b in T are comparable. An element $u \in S$ is an *upper bound* for subset A of S if $a \leq u$ for all $a \in A$. An element m of S is *maximal* if there is no $s \in S$ such that $m \leq s$.

Example. Consider the sets $A = \varnothing$, $B = \{1\}$, $C = \{2\}$, $D = \{3\}$, $E = \{1,2\}$, $F = \{1,3\}$, and $G = \{2,3\}$. Define $S = \{A, B, C, D, E, F, G\}$. For sets X and Y in S, define $X \leq Y$ if $X \subseteq Y$. Then $A \leq X$ for all $X \in S$. Also, $B \leq E$, $B \leq F$, $C \leq E$, $C \leq G$, $D \leq F$ and $D \leq G$. The remaining pairs of sets are not comparable. Set S has no upper bound. Set $\{A, B, C, E\}$ has E as an upper bound. for set S, maximal elements are E, F, and G. Set $T = \{A, B, F\}$ is a chain in S.

Lemma 31.21. Zorn's Lemma.

If S is a partially ordered set such that every chain in S has an upper bound in S, then S has at least one maximal element.

Note. Zorn's Lemma is equivalent to the famous Axiom of Choice, which has some surprising consequences in measure theory (to drop some verbiage, a "non-Lebesgue-measurable set" and the "Banach-Tarski Paradox"). Zorn's Lemma can be used to show that every vector space has a basis (notice that the definition of vector space did not require the existence of a basis). We need Zorn's Lemma for the proof of Theorem 31.17/31.22.

Note. Russell's Paradox from set theory implies that there can be no "largest set" nor a "set of all sets." Russell's Paradox results from the 19th century approach to sets which did not have a clear way of constructing new sets from old ("sets" were still viewed informally). The fallout of Russell's Paradox was to inspire an axiomatic development of set theory (lead by Russell and Whitehead's *Principia Mathematica* of circa 1910). For more details on Russell's Paradox, see my notes on Analysis 1 (MATH 4217/5217):

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

Note. Georg Cantor (1845–1918) introduced the concept of the cardinality of an infinite set. We denote the cardinality of set A as $|A|$. Cantor's Theorem states that for *any* set A, the cardinality of the power set of set A, denoted $\mathcal{P}(A)$, is strictly greater than the cardinality of set A: $|\mathcal{P}(A)| > |A|$. For details, see my notes from Analysis 1 (MATH 4217/5217):

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

Note. Fraleigh gives a proof on pages 290 and 291. You can find an alternate proof in Hungerford's *Algebra* in Section V.3, but the proof requires a number of other results in Hungerford (some of them deep, set theoretic results). Another proof is given in Dummit and Foote's *Abstract Algebra*, 3rd Edition, John Wiley and Sons (2004), Section 13.4. This proof uses results concerning ideals and maximal ideals, but otherwise is pretty much independent of other results in the book. An additional interesting source is given by Hanspeter Fischer of Ball State University. His proof is given as a supplement to his notes and is posted online (see `http://www.cs.bsu.edu/homepages/fischer/math412/Closure.pdf`).

Note. The proof of Theorem 31.17/21.22 is unlike much of the rest of the content of this class because the proof is largely set-theoretic, instead of algebraic (though some of the details are algebraic which must be verified in order to apply the st theoretic approach). We break the proof into three parts. FIRST, in order to apply Zorn's Lemma we need to insure that all of the extension fields of field F we deal with are in the same set, Ω. SECOND, for any chain of fields, we construct an upper bound for the chain. THIRD, we show that the upper bound is a maximal element of the set of algebraic extension fields of F and that it is (with a proof by contradiction) algebraically closed. This "maximal element" approach will not necessarily guarantee uniqueness of the algebraic closure of field F.

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

Proof.

I. *Construction of a set Ω large enough to contain all algebraic extensions of field F.*

For a given field F, form a set A which has an element for every possible zero of a polynomial in $F[x]$:

$$A = \{\omega_{f,i} \mid f(x) \in F[x], i = 1, 2, \ldots, (\text{degree of } f)\}.$$

The idea here is that for any polynomial $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \in F[x]$, there are at most n zeros, one for such $\omega_{f,1}, \omega_{f,2}, \ldots, \omega_{f,n}$. So for every zero of every polynomial in $F[x]$ (and hence for every element of E an algebraic extension of F, see Definition 31.1) there is an element of S.

> The elements of a field are simply elements of a set. In the following arguments, we'll deal with fields consisting of elements of F and another set—we need not concern ourselves with what the elements of the other set *are*, simply that a field exists consisting of these elements.

Consider the power set $\mathcal{P}(A)$. By Cantor's Theorem (see above), $|\mathcal{P}(A)| > |A|$. Now, for each $a \in F$, we have a as a zero of $f_a(x) = x - a$ and so there is $\omega_{f_a,1} \in A$ and hence $\{\omega_{f_a,1}\} \in \mathcal{P}(A)$. Define set Ω as

$$\Omega = (\mathcal{P}(A) \setminus \cup_{a \in F}\{\omega_{f_a,1}\}) \cup \{a \mid a \in F\}.$$

That is, replace each $\{\omega_{f_a,1}\} \in \mathcal{P}(A)$ with $a \in F$. Then $F \subseteq \Omega$.

Now consider all possible fields that can be defined on the elements of Ω that are algebraic extensions of F. Denote the set of all such fields as $\mathcal{E}$. Since $\mathcal{E} \subseteq \mathcal{P}(\Omega)$, then set $\mathcal{E}$ actually exists.

> Recall from Russell's Paradox that we can't simply define a set in an arbitrary way, such as "the set of all sets" or "the set of all algebraic extensions of F," and that's why we take this approach of defining set A and considering power sets A and Ω.

Also, $F \in \mathcal{E}$, so $\mathcal{E}$ is nonempty.

Let E be an algebraic extension field of F with $\gamma \in E$ a zero of $f(x) \in F[x]$ and $\gamma \notin F$. Say $\deg(\gamma, F) = n$. Then every element of $F(\gamma)$ is of the form $a_0 + a_1\gamma + a_2\gamma^2 + \cdots + a_{n-1}\gamma^{n-1}$ by Theorem 29.18. Now pick $\omega \in \Omega$, $\omega \notin F$, and "rename" γ as ω. Also rename the element $a_0 + a_1\gamma + a_2\gamma^2 + \cdots + a_{n-1}\gamma^{n-1}$ of $F(\gamma)$ by distinct elements of Ω as the a_i range over F.

> For any infinite set, the set of all finite-tuples from the set has the same cardinality as the original set (though I need a reference for this result!). So set Ω is large enough to do this renaming with distinct elements of F.

The renamed $F(\gamma)$ (now "named" $F(\omega)$) is an algebraic extension field of F where $F(\omega) \subset \Omega$ and $f(\omega) = 0$.

For all algebraic extension fields E_j of F, with $E_j \subset \Omega$ (after the "renaming" above), form a set $S = \{E_j \mid j \in J\}$. Set S is partially ordered by subfield inclusion $\leq$. $F \in S$, so S is nonempty.

II. *Showing that every chain in S has an upper bound in S.*

Let $T = \{E_{j_k} \mid k \in K\}$ be a chain in S, and let $W = \cup_{k \in K} E_{j_k}$. We will (a) make W into a field, (b) show that W is an algebraic extension of F, and (c) show that W is an upper bound for T.

(a) The same *elements* of set W can form different fields under different binary operation $+$ and $\cdot$, so we need to define $+$ and $\cdot$ on W in a uniform way. Let $\alpha, \beta \in W$. Then $\alpha \in E_{j_1}$ and $\beta = E_{j_2}$ for some $E_{j_1}, E_{j_2} \in S$. Since T is a chain under subfield inclusion, one of these is a subfield of the other. Say, WLOG, $E_{j_1} \leq E_{j_2}$. Then $\alpha, \beta \in E_{j_2}$. So define (in W) the sum $\alpha +_W \beta$ as the sum $\alpha +_{j_2} \beta \in E_{j_2}$. Similarly define the product $\alpha \cdot_W \beta$ as $\alpha \cdot_{j_2} \beta \in E_{j_2}$. We simply denote these elements of W as $\alpha + \beta$ and $\alpha\beta$.

> Notice that these definitions of $+$ and $\cdot$ in W are well-defined. If $\alpha\beta \in E_{j_3}$ then, since T is a chain, then either $E_{j_2} \leq E_{j_3}$ or $E_{j_3} \leq E_{j_2}$. In either case, the sum and product of α and β are the same fields and so $+$ and $\cdot$ in W is unambiguously defined.

Now we verify that W is a field. We address this using the definition of a field as a commutative division ring (Definition 18.16). Since $+$ and $\cdot$ in W is defined using fields in chain T, then commutivity and associativity is inherited from the fields in T. For any $\alpha \in W$, we have $0, 1, \alpha \in E_{j_k}$ for some $E_{j_k} \in T$, and so $0 + \alpha = \alpha + 0 = \alpha$ and $1 \cdot \alpha = \alpha \cdot 1 = \alpha$ since E_{j_k} is a field. Also, if $\alpha \neq 0$, then there is $-\alpha, \alpha^{-1} \in E_{j_k}$ such that $\alpha + (-\alpha) = (-\alpha) + \alpha = 0$ and $\alpha\alpha^{-1} = \alpha^{-1}\alpha = 1$. For $\alpha, \beta, \gamma \in W$, since T is a chain, there is some $E_{j_k} \in S$ such that $\alpha, \beta, \gamma \in E_{j_k}$. then $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$ since E_{j_k} is a field, and do left distribution (and hence right distribution) holds in W. So W is a field.

(b) For any $\alpha \in W$, we have $\alpha \in E_{j_k}$ for some $E_{j_k} \in T$. Since E_{j_k} is an algebraic extension of F, then α is algebraic over F. So W is an algebraic extension field of field F. Therefore, $W \in S$.

(c) By construction, $E_{j_k} \leq W$ for all $E_{j_k} \in T$, so $W \in S$ is an upper bound for chain T.

III. *Showing that a maximal element of S is an algebraic closure of F.* Since for arbitrary chain T in S there is an upper bound W of T with $W \in S$, then the hypotheses of Zorn's Lemma are satisfied. Therefore, Zorn's Lemma implies that there is a maximal element $\overline{F}$ of S. We now show that $\overline{F}$ is algebraically closed. Let $f(x) \in F[x]$ where $f(x)$ is a nonconstant polynomial (i.e., $f(x) \notin \overline{F}$). ASSUME that $f(x)$ has no zero in $\overline{F}$. Then take $\omega \in \Omega$, where $\omega \notin \overline{F}$ and ω is a zero of $f(x)$, and form the field $\overline{F}(\omega) \subseteq \Omega$, as in Part I of the proof. Let $\beta \in \overline{F}(\omega)$. Then by Theorem 30.23, β is a zero of a polynomial $g(x) = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \cdots + \alpha_n x^n$ in $\overline{F}[x]$ where $\alpha_i \in \overline{F}$. Since $\overline{F} \in S$ (the set of all algebraic extensions of F) then $\overline{F}$ is an algebraic extension of F and so each α_i is algebraic over F. By Theorem 31.11 the field $F(\alpha_0, \alpha_1, \ldots, \alpha_n)$, we also see that $F(\alpha_0, \alpha_1, \ldots, \alpha_n, \beta)$ is a finite extension over $F(\alpha_0, \alpha_1, \ldots, \alpha_n)$ (again, by Theorem 31.11). In fact, by Theorem 31.4,

$$[F(\alpha_0, \alpha_1, \ldots, \alpha_n, \beta) : F] = [F(\alpha_0, \alpha_1, \ldots, \alpha_n, \beta) : F(\alpha_0, \alpha_1, \ldots, \alpha_n)][F(\alpha_0, \alpha_1, \ldots, \alpha_n) : F]$$

and so $F(\alpha_0, \alpha_1, \ldots, \alpha_n, \beta)$ is a finite extension of F. By Theorem 31.3, $F(\alpha_0, \alpha_1, \ldots, \alpha_n, \beta)$ is therefore an algebraic extension of F and so β is algebraic over F. Since $\beta \in \overline{F}(\omega)$ is arbitrary, then $\overline{F}(\omega)$ is an algebraic extension of F and so $\overline{F}(\omega) \in S$. But then $\overline{F} < \overline{F}(\omega)$ where $\overline{F}(\omega) \in S$, contradicting the choice of $\overline{F}$ as a maximal element of S. Therefore, the assumption that $f(x)$ has no zero in $\overline{F}[x]$ is false. Since $f(x) \in \overline{F}[x]$ is arbitrary, then we have shown that every nonconstant polynomial has a zero in $\overline{F}$. That is, $\overline{F}$ is algebraically closed. Since $F \leq \overline{F}$, then F has an algebraic closure $\overline{F}$ (that is, $\overline{F}$ is an algebraically closed extension field of F). ∎

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.

Revised: 2/16/2014