Section V.3. Splitting Fields, Algebraic Closure, and Normality (Supplement)

Note. In this supplement, we consider splitting fields of sets of an infinite number of polynomials. In the the process, we give a more detailed definition of "algebraically closed field" and an "algebraic closure" of a field than that given in the main notes for this section. If we are running low on time, this supplement can be skipped.

Theorem V.3.3. The following conditions on a field F are equivalent:

(i) Every nonconstant polynomial $f \in F[x]$ has a root in F;

(ii) every nonconstant polynomial $f \in F[x]$ splits over F;

(iii) every irreducible polynomial in $F[x]$ has degree one;

(iv) there is no algebraic extension field of F (except F itself);

(v) there exists a subfield K of F such that F is algebraic over K and every polynomial in $K[x]$ splits in $F[x]$.

Definition. A field F satisfying any of the equivalent conditions of Theorem V.3.3 is *algebraically closed.*

Note. By Theorem V.3.3(ii), we see that if F is algebraically closed and $f \in F[x]$ is of degree n, then f factors as $f = u_0(x-u_1)(x-u_2)\cdots(x-u_n)$ where the roots are $u_1, u_2, \ldots, u_n$. We will see in the appendix to this section (in Theorem V.3.19, The Fundamental Theorem of Algebra) that $\mathbb{C}$ is algebraically closed. The set, $\mathbb{A}$, of all algebraic (complex) numbers over $\mathbb{Q}$ form an algebraically closed field as shown in Fraleigh's Exercise 31.33 (*A First Course in Abstract Algebra*, 7th Edition). Many familiar fields are not algebraically closed. $\mathbb{Q}$ is not algebraically closed (consider x^2-2); $\mathbb{R}$ is not algebraically closed (consider x^2+1). In Exercise V.3.8 it is shown that no finite field is algebraically closed.

Theorem V.3.4. If F is an extension field of K, then the following conditions are equivalent:

(i) F is algebraic over K and F is algebraically closed;

(ii) F is a splitting field over K of the set of all (irreducible) polynomials in $K[x]$.

Definition. An extension field F of a field K that satisfies either of the (equivalent) conditions of Theorem V.3.4 is an *algebraic closure* of K.

Note. We will see below (in Theorem V.3.6) that "an" algebraic closure of K is unique (up to isomorphism).

Note. By the "algebraic" comment of Theorem V.3.4(i) (and the "splitting field" comment of condition (ii)) we have that an algebraic closure of K is "the smallest" algebraically closed field containing K. For example, the algebraic (complex) numbers $\mathbb{A}$ are the algebraic closure of $\mathbb{Q}$ (see the note in these class notes before Theorem V.3.4). Now $\mathbb{C}$ is also algebraically closed and contains $\mathbb{Q}$, but $\mathbb{C}$ is not the algebraic closure of $\mathbb{Q}$ ($\mathbb{C}$ is the algebraic closure of $\mathbb{R}$).

Note. The main result of this supplement is to prove that every field has an algebraic closure. The argument (given below in Lemma V.3.5 and Theorem V.3.6) is mostly set theoretic, as opposed to algebraic (another reason this supplement can be skipped, if pressed for time). We start by recalling some set theoretic results from Chapter 0.

Definition 0.8.3. Let α and β be cardinal numbers. The *sum* $\alpha+\beta$ is the cardinal number $|A \cup B|$, where A and B are disjoint sets such that $|A| = \alpha$ and $|B| = \beta$. The *product* $\alpha\beta$ is the cardinal number $|A \times B|$.

Definition 0.8.4. Let α, β be cardinal numbers and A, B sets such that $|A| = \alpha$, $|B| = \beta$. α is *less than or equal to* β, denoted $\alpha \leq \beta$ or $\beta \geq \alpha$, if A is equipollent with a subset of β (that is, there is an injective map $A \to B$).

Theorem 0.8.11. If α and β are cardinal numbers such that $0 \neq \beta \leq \alpha$ and α is infinite, then $\alpha\beta = \alpha$; in particular, $\alpha\aleph_0 = \alpha$ and if β is finite then $\aleph_0\beta = \aleph_0$.

Theorem 0.8.12(ii). Let A be a set and for each $n \in \mathbb{N}$ let $A^n = A \times A \times \cdots \times A$ (n factors). Then $|\cup_{n \in \mathbb{N}} A^n| = \aleph_0 |A|$.

Note. In *A First Course in Abstract Algebra*, 7th Edition, Fraleigh gives a proof that every field has an algebraic closure (see pages 290 and 291 and my online notes to Introduction to Modern Algebra 2, `http://faculty.etsu.edu/gardnerr/4127/notes/Algebraic-Closure.pdf`). Fraleigh's proof is very similar to Hungerford's proof of Theorem V.3.6. 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`).

Lemma V.3.5. If F is an algebraic extension field of K, then $|F| \leq \aleph_0 |K|$.

Note. We recall Zorn's Lemma since it is instrumental in the proof of the main objective of this supplement.

Zorn's Lemma. If A is a nonempty partially ordered set such that every chain in A has an upper bound in A, then A has a maximal element.

Note. Now for the main result of this supplement: The existence (and uniqueness) of an algebraic closure.

Theorem V.3.6. Every field K has an algebraic closure. Any two algebraic closures of K are K-isomorphic.

Note. Theorem V.3.6 allows us to show the existence of a splitting field for any set of polynomials over a given field.

Corollary V.3.7. If K is a field and S a set of polynomials (of positive degree) in $K[x]$, then there exists a splitting field of S over K.

Note. We now address two more results from Section V.3 which we excluded from the regular class notes. First, we give a proof of Theorem V.3.8 in the case of an infinite set of polynomials. Finally, we state and prove the "Generalized Theorem of Galois Theory."

Note. The uniqueness claim in Theorem V.3.6 requires the following. The case of a finite set of polynomials is given in the regular class notes, so we now give a proof for an infinite set of polynomials.

Theorem V.3.8. **(For S infinite.)** Let $\sigma : K \to L$ be an isomorphism of fields, $S = \{f_i\}$ a set of polynomials (of positive degree) in $K[x]$, and $S' = \{\sigma f_i\}$ the corresponding set of polynomials in $L[x]$. If F is a splitting field of S over K and M is a splitting field of S' over L, then σ is extendible to an isomorphism $F \cong M$.

Note. The original Fundamental Theorem of Galois Theory (Theorem V.2.5) deals with finite dimensional Galois extensions (so that $[F : K]$ is finite). Now that we have dealt with infinite sets of polynomials (namely, splitting fields of an infinite set of polynomials in Corollary V.3.9), we can address infinite dimensional Galois extensions. In doing so, we consider closed subgroups of the Galois group $\mathrm{Aut}_K F$. Recall that $H < \mathrm{Aut}_K F$ is closed if $H = H''$ (by Lemma V.2.6(iii), $H < H''$).

Theorem V.3.12. **(Generalized Fundamental Theorem of Galois Theory)** If F is an algebraic Galois extension field of K, then there is a one-to-one correspondence between the set of all intermediate fields of the extension and the set of all closed subgroups of the Galois group $\mathrm{Aut}_K F$ (given by $E \mapsto E' = \mathrm{Aut}_E F$) such that:

(ii)$'$ F is Galois over every intermediate field E, but E is Galois over K if and only if the corresponding subgroup E' is normal in $G = \mathrm{Aut}_K F$; in this case G/E' is (isomorphic to) the Galois group $\mathrm{Aut}_K E$ of E over K.

Note. The first part of the regular Fundamental Theorem of Galois Theory (Theorem V.2.5(i)) claims that $|\mathrm{Aut}_K F| = [F : K]$. This does not hold in the case of F being Galois over K but an infinite extension. This is shown by example in Exercise V.3.16. In the example, $K = \mathbb{Q}$, E is a splitting field of the set of polynomials $S = \{x^2 + 1 \mid a \in \mathbb{Q}\}$ (F can be taken to be the field $\mathbb{A}$ of all algebraic complex numbers). It is argued that $[E : \mathbb{Q}] < |\mathrm{Aut}_{\mathbb{Q}} E|$, so that part (i) of the regular Fundamental Theorem is violated.

Revised: 1/25/2016