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

Note. The topic of this section is the identification and construction of Galois extensions. Our attention is turned to factoring polynomials and finding their roots. We restrict our attention to finite collections of polynomials and omit the part of this section concerning roots of infinite collections of polynomials. After this section, we have the equipment to give a mostly-algebriac proof of the Fundamental Theorem of Algebra.

Definition. Let F be a field and $f \in F[x]$ a polynomial of positive degree. f is said to *split* over F if f can be written as a product of linear factors in $F[x]$; that is, $f = u_0(x - u_1)(x - u_2) \cdots (x - u_n)$ with $u_i \in F$. (So f splits over F if field F contains all roots of f.)

Definition V.3.1. Let K be a field and $f \in K[x]$ a polynomial of positive degree. An extension field F of K is a *splitting field* over K *of polynomial* f if f splits in $F[x]$ where $F = K(u_1, u_2, \ldots, u_n)$ with $u_1, u_2, \ldots, u_n$ the roots of f in F. Let S be a set of polynomials of positive degree in $K[x]$. An extension field F of K is a *splitting field* over K *of the set* S of polynomials if every polynomial in S splits in $F[x]$ and F is generated over K by the roots of all the polynomials in S.

Example. Polynomial $x^2 - 2 \in \mathbb{Q}[x]$ has two roots, but the simple extension $\mathbb{Q}(\sqrt{2})$ is the splitting field since it contains both roots. Polynomial $x^3 - 2 \in \mathbb{Q}[x]$ has three roots in $\mathbb{C}$, but the simple extension $\mathbb{Q}(\sqrt[3]{2})$ is not the splitting field for $x^3 - 2$ since it contains neither complex root.

Note. If field F is a splitting field of set S of polynomials over K, then $F = K(X)$ where set X is the set of all roots of the polynomials in set S (here, $S \subset K[x]$). By Theorem V.1.12, F is algebraic over K. If set S is finite, say $S = \{f_1, f_2, \ldots, f_n\}$ then the set of roots for the polynomials in S is the same as the set of roots for the single polynomial $f_1 f_2 \cdots f_n$. So when we consider splitting fields of a set S of polynomials, we are really only interested in the cases where S contains one polynomial or S contains infinitely many polynomials. In these notes, we only consider the situation concerning the case where S contains a finite number of polynomials (or equivalently, a single polynomial). We have not yet established the existence of splitting fields and the following result starts this process.

Theorem V.3.2. If K is a field and $f \in K[x]$ has degree $n \geq 1$, then there exists a splitting field F of f with dimension $[F : K] \leq n!$.

Definition. A field F in which every nonconstant polynomial $f \in F[x]$ has a root in F is *algebraically closed*. If F is an extension field of field K such that F is algebraic over K and F is algebraically closed, then F is an *algebraic closure* of field K.

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 as shown in Fraleigh's *A First Course in Abstract Algebra*, 7th Edition, Exercise 31.33, and $\mathbb{C}$ is algebraically closed by the Fundamental Theorem of Algebra, as shown in the appendix to this section. *An* algebraic closure (soon to be called *the* algebraic closure, after we prove Corollary V.3.9) 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 $\mathbb{Q}$.

Note. By the Factor Theorem, Theorem III.6.6, we see that if every $f \in F[x]$ has a root in F, then each such f can be factored into a product of linear terms. That is, every nonconstant f splits over F. This also means that there is no (proper) algebraic extension field of F.

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

Note. The proof of Theorem V.3.6 requires Zorn's Lemma. The result is largely set-theoretic, as opposed to algebraic. You can find a proof in the Supplement to these notes. Another self-contained proof can be found in the following notes:

`http://faculty.etsu.edu/gardnerr/4127/notes/Algebraic-Closure.pdf`

Note. We now turn our attention to the uniqueness of splitting fields.

Theorem V.3.8. (For S finite.) 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. Now we show the uniqueness of an algebraic closure.

Corollary V.3.9. Let K be a field and S a set of polynomials (of positive degree) in $K[x]$. Then any two splitting fields of S over K are K-isomorphic. In particular, any two algebraic closures of K are K-isomorphic.

Definition. Let K be a field and $f \in K[x]$ where f is not the zero polynomial. Let c be a root of f. Then $f(x) = (x-c)^m g(x)$ where $g(c) \neq 0$ (see page 161 or page 5 of these notes for Section III.6). Then c is a *simple root* if $m = 1$; c is a *multiple root* if $m > 1$.

Definition V.3.10. Let K be a field and $f \in K[x]$ an irreducible polynomial. The polynomial f is *separable* if in some splitting field of f over K every root of f is a simple root. If F is an extension field of K and $u \in F$ is algebraic over K, then element u is *separable* over K provided its irreducible polynomial is separable. If every element of F is separable over K, then F is a *separable extension* of K.

Note. By Theorem III.6.10(i), an irreducible polynomial in $K[x]$ is separable if and only if its derivative is nonzero. By Exercise III.6.3(a), if $\text{char}(K) = 0$ then for any irreducible polynomial f (any polynomial, in fact) we have $f' \neq 0$, so if $\text{char}(K) = 0$ then every irreducible polynomial is separable. By Corollary V.3.9, a separable polynomial has no multiple zeros in *any* splitting field f over K (since all splitting fields of f over K are K-isomorphic). We therefore have:

Lemma. Every algebraic extension field of a field of characteristic 0 is separable.

Theorem V.3.11. If F is an extension field of K, then the following statements are equivalent.

(i) F is algebraic and Galois over K.

(ii) F is separable over K and F is a splitting field over K of a set S of polynomials in $K[x]$.

(iii) F is a splitting field over K of a set T of separable polynomials in $K[x]$.

Definition V.3.13. An algebraic extension field F of K is *normal* over K (or a *normal extension*) if every irreducible polynomial in $K[x]$ that has a root in F actually splits in $F[x]$.

Theorem V.3.14. If F is an algebraic extension field of K, then the following statements are equivalent.

(i) F is normal over K.

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

(iii) If $\overline{K}$ is algebraically closed, contains K, and contains F, then for any K-monomorphism of fields $\sigma : F \to \overline{K}$ (that is, σ is a one to one homomorphism

and σ fixes K elementwise), then $\text{Im}(\sigma) = F$ so that σ is actually a K-automorphism of F (that is, $\sigma \in \text{Aut}_K(F)$).

Corollary V.3.15. Let F be an algebraic extension field of K. Then F is Galois over K if and only if F is normal and separable over K. If $\text{char}(K) = 0$, then F is Galois over K if and only if F is normal over K.

Note. The following result will play a role in our proof of the Fundamental Theorem of Algebra in the appendix to this section.

Theorem V.3.16. If E is an algebraic extension field of K, then there exists an extension field F of E such that:

(i) F is normal over K;

(ii) No proper subfield of F containing E is normal over K;

(iii) If E is separable over K, then F is Galois over K;

(iv) $[F : K]$ is finite if and only if $[E : K]$ is finite.

The field F is uniquely determined up to an E-isomorphism.

Definition. The field F of Theorem V.3.16 is the *normal closure* of E over K.