Section V.6. Separability

Note. Recall that in Definition V.3.10, an extension field F is a separable extension of K if every element of F is algebraic over K and every root of the irreducible polynomial of an element of F has all roots of multiplicity 1. This section starts with the definition of purely inseparable extensions. The degree of inseparability is defined and separability is explored in this setting of inseparability.

Definition V.6.1. Let F be an extension field of K. An algebraic element $u \in F$ is *purely inseparable* over K if its irreducible polynomial $f \in K[x]$ factors in $F[x]$ as $f = (x-u)^m$. F is a *purely inseparable extension* of K if every element of F is purely inseparable over K.

Note. So u is separable over K if the irreducible polynomial of u over F has n distinct roots in K where n is the degree of the irreducible polynomial. u is purely inseparable over K if the irreducible polynomial has exactly one root. Of course, these are extreme cases and an element may be *neither* separable *nor* purely inseparable; or it may be both separable *and* purely inseparable.

Example. This example of a purely inseparable extension is from Fraleigh (see Examples 51.4 and 52.2). Let p be prime, let $K = \mathbb{Z}_p$, and let $E = \mathbb{Z}_p(y)$ where y is an indeterminate. Consider the intermediate field $F = \mathbb{Z}_p(t)$ where $t = y^p$, so that $K \subset F \subset E$. Notice that $E = F(y) = \mathbb{Z}_p(t, y)$ is algebraic over F since y is a root of

$x^p - t \in F[x]$. Fraleigh's Exercise 51.10 shows that $x^p - t$ is irreducible in F. Since $F[x]$ is also of characteristic p, then by the Freshman's Cream (Exercise III.1.11) that $x^p - t = x^p - y^p = (x - y)^p$. So $y \in E$ is purely inseparable over $F = \mathbb{Z}_p(t)$. We'll see in Theorem V.6.4(v) that this is sufficient to show that $E = \mathbb{Z}_p(y)$ is purely inseparable over $F = \mathbb{Z}_p(t) = \mathbb{Z}_p(y^p)$.

Theorem V.6.2. Let F be an extension field of K. Then $u \in F$ is both separable and purely inseparable over K if and only if $u \in K$.

Note. Theorem V.6.2 is used in Section V.9, "Radical Extensions," in the proof of Theorem V.9.4. The remainder of this section is not necessary for what follows.

Note. Recall that every algebraic extension of a field of characteristic 0 is separable (see "Remarks" on page 261 and "Lemma" on page 5 of these class notes for Section V.3). So if u is a purely inseparable element of K where $\text{char}(K) = 0$ then, by the definition of purely inseparable, u is algebraic over K and so by "Remarks" and "Lemma" u is also separable over K. Then by Theorem V.6.2, $u \in K$. So the only purely inseparable elements of K, where $\text{char}(K) = 0$, are elements of K and so purely inseparable extensions of K are trivial if $\text{char}(K) = 0$. So we restrict our attention to purely inseparable extensions of fields of characteristic (prime) $p \neq 0$.

Lemma V.6.3. Let F be an extension field of K with $\text{char}(K) = p \neq 0$. If $u \in F$ is algebraic over K, then u^{p^n} is separable over K for some $n \geq 0$.

Note. Now we give conditions on extension F of K which are equivalent to purely inseparable.

Theorem V.6.4. If F is an algebraic extension field of a field K of characteristic $p \neq 0$ then the following statements are equivalent:

(i) F is purely inseparable over K;

(ii) the irreducible polynomial of any $u \in F$ is of the form $x^{p^n} - a \in K[x]$;

(iii) if $u \in F$, then $u^{p^n} \in K$ for some $n \geq 0$;

(iv) the only elements of F which are separable over K are the elements of K itself;

(v) F is generated over K by a set of purely inseparable elements.

Corollary V.6.5. If F is a finite dimensional purely inseparable extension field of K and $\text{char}(K) = p \neq 0$, then $[F : K] = p^n$ for some $n \geq 0$.

Lemma V.6.6. If F is an extension field of K, X is a subset of F such that $F = K(X)$, and every element of X is separable over K, then F is a separable extension of K.

Note. We now have the equipment to prove our "principal theorem on separability."

Theorem V.6.7. Let F be an algebraic extension field of K, let S be the set of all elements of F which are separable over K, and let P be the set of all elements of F which are purely inseparable over K.

(i) S is a separable extension field of K.

(ii) F is purely inseparable over S.

(iii) P is a purely inseparable extension field of K.

(iv) $P \cap S = K$.

(v) F is separable over P if and only if $F = SP$.

(iv) If F is normal over K, then S is Galois over K, F is Galois over P, and $\text{Aut}_K(S) \cong \text{Aut}_P(F) = \text{Aut}_K(F)$.

Note. "Clearly" S is the unique largest subfield of F which is separable over K. So S contains every intermediate field that is separable over K. Similarly, P is the unique largest subfield of F which is purely inseparable over K, so P contain every intermediate field that is inseparable over K. By the note after Theorem V.6.2, if $\text{char}(K) = 0$ then $S = F$ and $P = K$ and the results of Theorem V.6.7 are "flat."

Corollary V.6.8. If F is a separable extension of E and E is a separable extension field of K, then F is separable over K.

Note. Let F be a field of characteristic $p \neq 0$. Lemma V.5.5 shows that for each $n \geq 1$, the set $F^{p^n} = \{u^{p^n} \mid u \in F\}$ is the image of a field homomorphism which fixes the prime subfield of F (see Theorem V.5.1). By Exercise III.1.16, F^{p^n} is a field and so a subfield of F. Since every $u \in F$ is a root of $x^{p^n} - u^{p^n} \in F^{p^n}[x]$, then F is algebraic over F^{p^n}. By Theorem V.6.4 (the (iii)⇒(i) part), F is purely inseparable over F^{p^n}. Then by Exercise V.6.2, F is purely inseparable over every intermediate field. The next result relates an algebraic extension field of characteristic p to a composite filed involving F^{p^n}.

Corollary V.6.9. Let F be an algebraic extension field of K, with $\text{char}(K) = p \neq 0$. If F is separable over K, then $F = KF^{p^n}$ for each $n \geq 1$. If $[F : K]$ is finite and $F = KF^p$ (KF^p is the smallest subfield of F containing $K \cup F^p$), then F is separable over K. In particular, $u \in F$ is separable over K if and only if $K(u^p) = K(u)$.

Note. The following is needed in what follows (see Definition V.7.1, for example).

Definition V.6.10. Let F be an algebraic extension field of K and S the largest subfield of F separable over K (as in Theorem V.6.7). The dimension $[S : K]$ is called the *separable degree* of F over K and is denoted $[F : K]_s$. The dimension $[F : S]$ is called the *inseparable degree* (or *degree of inseparability*) of F over K and is denoted $[F : K]_i$.

Note 1. Since $K \subseteq S \subseteq F$, by Theorem V.1.2, we have $[F : K] = [F : S][S : K] = [F : K]_i[F : K]_s$. So F is separable over K (i.e., $S = F$) if and only if $[F : K] = [S : K] = [F : K]_s$ and $[F : S] = [S : S] = [S : K]_i = 1$. At the other extreme, F is purely inseparable over K (i.e., $S = K$; see Theorem V.6.7(ii)) if and only if $[S : K] = [K : K] = [F : K]_s = 1$ and $[F : K] = F : S] = [F : K]_i$.

Note 2. Let $[F : K]$ be finite and $\text{char}(K) = p \neq 0$. Let S be the largest subfield of F separable over K (as in Theorem V.6.7). By Theorem V.6.7(ii) F is purely inseparable over S and so $[F : S] = [F : S]_i$ by Note 1. By definition $[F : S] = [F : K]_i$. So $[F : S] = [F : K]_i = [F : S]_i$. Since F is finite dimensional, purely inseparable over S, and S is of characteristic a power of p (or so Hungerford seems to claim on page 286), then by Corollary V.6.5, $[F : S]_i$ is a power of p and so $[F : K]_i$ is a power of p.

Note. The following three results are used in the proof of Theorem V.7.3 in the next section. If we are pressed for time, we can skip Lemma V.6.11, Proposition V.6.12, Corollary V.6.13, and Corollary V.6.14 (as well as the proof of Theorem V.7.3).

Lemma V.6.11. Let F be an extension field of E, E an extension field of K, and N a normal extension field of K containing F. If r is the cardinal number of distinct E-monomorphisms mapping $F :\rightarrow N$ and t is the cardinal number of distinct K-monomorphisms mapping $E :\rightarrow N$, then rt is the cardinal number of distinct K-monomorphisms mapping $F \rightarrow N$.

Proposition V.6.12. Let F be a finite dimensional extension field of K and N a normal extension field of K containing F. The number of distinct K-monomorphisms mapping $F \to N$ is precisely $[F : K]_s$, the separable degree of F over K.

Corollary V.6.13. If F is an extension field of E and E is an extension field of K, then

$$[F : E]_s [E : K]_s = [F : K]_s \text{ and } [F : E]_i [E : K]_i = [F : K]_i.$$

Corollary V.6.14. Let $f \in K[x]$ be an irreducible monic polynomial over a field K, F a splitting field of f over K and u_i a root of f in F. Then

(i) every root of f has multiplicity $[K(u_1) : K]_i$ so that in $F[x]$

$$f(x) = ((x - u_1)(x - u_2) \cdots (x - u_n))^{[K(u_1):K]_i},$$

where $u_1, u_2, \ldots, u_n$ are all the distinct roots of f and $n = [K(u_1) : K]_s$;

(ii) $u_1^{[K(u_1):K]_i}$ is separable over K.

Note. The following result is independent of the other results in this section and is not referenced in the future material.

Proposition V.6.15. The Primitive Element Theorem.

Let F be a finite dimensional extension field of K.

(i) If F is separable over K, then F is a simple extension of K.

(ii) (Artin) More generally, F is a simple extension of K if and only if there are only finitely many intermediate fields.

Definition. The element $u \in F$ such that $F = K(u)$ as described in Proposition V.6.15 is a *primitive element* of the extension.

Revised: 2/14/2016