Separable Degree

Dummit and Foote introduce the separable degree fairly late in Chapter 14 (page 650). Moreover the definition they give is not the usual one, but the usual definition is useful and important. I can recommend Lang's *Algebra* for a better treatment of separability. But here are the basic facts.

Let E/F be a field extension, and let $\Omega \supset F$ be another field. By an *embedding* of E into Ω over F, we mean a field homomorphism $\phi : E \longrightarrow \Omega$ such that $\phi(x) = x$ for $x \in F$. The term embedding is used since ϕ is automatically injective, so ϕ isomorphically maps E onto its image and hence "embeds" E into Ω.

In Galois theory, a useful point of view is to take Ω to be some sufficiently large field containing F and to study embeddings of E into Ω over F. If Ω is "sufficiently large," then "all" embeddings of E will end up in Ω. Let us define these terms.

Definition 1. *Let E/F be a finite extension. A field $\Omega \supset F$ is sufficiently large for the extension E/F if whenever $\Omega' \supseteq \Omega$ is a bigger field and $\phi : E \longrightarrow \Omega'$ is an embedding over F, we automatically have $\phi(E) \subseteq \Omega$.*

An example of a field that is always sufficiently large for any finite extension E/F is the algebraic closure of F. But actually a much smaller field will do if E/F is finite.

Proposition 1. *Let E/F be a finite field extension, and let $\Omega_0 \supset E$ be a splitting field over F. Then Ω_0 is sufficiently large for the extension E/F.*

Proof. Let $\Omega' \supseteq \Omega_0$ be a larger field and let $\phi : E \longrightarrow \Omega'$ be an embedding over F. Let $\alpha \in E$. Then α is a root of an irreducible polynomial $f \in F[X]$. By Exercise 5 in Section 13.4 (HW2) f splits completely in Ω since Ω_0 is a splitting field over F. Now $\phi(\alpha)$ is another root of f, so $\phi(\alpha) \in \Omega_0$. This proves $\phi(E) \subseteq \Omega_0$. □

1 Separable degree

Definition 2. *Let E/F be a finite extension. The separable degree $[E : F]_s$ is the number of distinct embeddings $E \longrightarrow \Omega$ for Ω a sufficiently large field.*

This definition doesn't depend on Ω since *by definition* of the term "sufficiently large," increasing the size of Ω does not increase the number of embeddings if Ω.

Proposition 2. *Let $E \supset K \supset F$. Assume E/F is a finite extension. Then*

$$[E : F]_s = [E : K]_s[K : F]_s.$$

Proof. Let $[K : F]_s = m$ and $[E : K]_s = n$. Let $\phi_1, \cdots, \phi_m$ be the distinct embeddings of K into Ω over F, and let $\psi_1, \cdots, \psi_n$ be the number of distinct embeddings of E into F over K. Let Ω_0 be a splitting field over F containing E.

We fix one of the ϕ_i.

Lemma 3. *The number of distinct embeddings τ of E into Ω over F such that the restriction of τ to K is ϕ_i is n.*

Proof. Extend ϕ_i to an embedding $\tilde{\phi}_i : \Omega_0 \longrightarrow \Omega_0$ using Theorem 27 in Section 13.4 of Dummit and Foote. We can do this since if Ω_0 is a splitting field of $f \in F[X]$ over F, it is also a splitting field of f over K, and also a splitting field of f over $\phi_i(K)$. Clearly $\tilde{\phi}_i : \Omega_0 \longrightarrow \Omega_0$ is injective. Now consider $\tilde{\phi}_i^{-1}\tau : E \longrightarrow \Omega$. The restriction of this map to K is the identity. Indeed, if $x \in K$ then by assumption $\tau(x) = \phi_i(x)$, so

$$\tilde{\phi}_i^{-1}\tau(x) = \phi_i^{-1}\phi_i(x) = x.$$

Thus $\tilde{\phi}_i^{-1}\tau$ is an embedding of $E \longrightarrow \Omega$ over K, that is, $\tilde{\phi}_i^{-1}\tau = \psi_j$ for some j. Thus $\tau = \tilde{\phi}_i\psi_j$ for some j, proving that there are exactly n possible τ. □

Now we may enumerate the embeddings $\tau : E \longrightarrow \Omega$ as follows. For each $i = 1, \cdots, m$, we see that there are exactly n that extend $\phi_i : K \longrightarrow \Omega$, or mn total. Thus $[E : F]_s = mn = [E : K]_s[K : F]_s$. □

Proposition 4. *Let $E = F(\alpha)$ where $\alpha \in E$ is the root of an irreducible polynomial $f \in F[X]$. Then $[E : F]_s$ is the number of distinct roots of f, while $[E : F]$ is the degree of f. Therefore $[E : F]_s \leqslant [E, F]$ with equality if and only if the polynomial f is separable.*

Proof. We may assume f is monic. Let $n = \deg(f)$ and write

$$f(X) = \prod_{i=1}^{n}(x - \alpha_i)$$

Let Ω be a sufficiently large field for E/F and let Ω' be a splitting field for f containing Ω. For each i there is an embedding $\phi_i : F(\alpha) \longrightarrow \Omega'$ such that $\phi_i(\alpha) = \alpha_i$ by Theorem 6 in Section 13.1. Since Ω is sufficiently large, we have $\phi_i(E) \subseteq \Omega$. Moreover if $\phi : F(\alpha) \longrightarrow \Omega$ is any embedding it sends α to some α_i, so ϕ is one of the ϕ_i. And finaly, note that $\phi_i = \phi_j$ if and only if $\alpha_i = \alpha_j$. So $[E : F]_s$ equals the number of distinct ϕ_i, that is, the number of distinct α_i. Thus $[E : F]_s \leqslant n$ with equality if and only if f is separable. □

Proposition 5. *If E/F is any finite extension, $[E : F]_s \leqslant [E : F]$.*

Proof. If E/F is a simple extension, that is, if $E = F(\alpha)$ for some α, this follows from Proposition 4. In the general case, let $\alpha_1, \cdots, \alpha_k \in E$ such that $E = F(\alpha_1, \cdots, \alpha_n)$. Then E can be built up from F by a sequence of simple extensions:

$$F \subset F(\alpha_1) \subset F(\alpha_1, \alpha_2) \subset \cdots \subset F(\alpha_1, \cdots, \alpha_n) = E.$$

We have $[F(\alpha_1, \cdots, \alpha_k) : F(\alpha_1, \cdots, \alpha_{k-1})]_s \leqslant [F(\alpha_1, \cdots, \alpha_k) : F(\alpha_1, \cdots, \alpha_{k-1})]$. Multiplying these inequalities together we obtain $[E : F]_s \leqslant [E : F]$. □

We define the finite extension E/F to be *separable* if $[E : F]_s = [E : F]$. This is equivalent to the definition in Dummit and Foote, as we will soon show.

Proposition 6. *Let $E \supseteq K \supseteq F$ be finite extensions. Then E/F is separable if and only if both extensions E/K and K/F are separable.*

Proof. We have $[E : K]_s[K : F]_s = [E : F]_s \leqslant [E : F] = [E : K][K : F]$. From this it is clear that $[E : F]_s = [E : F]$ if and only if both $[E : K]_s = [E : K]$ and $[K : F]_s = [K : F]$. □

Proposition 7. *Let E/F be a finite extension. Then E/F is separable if and only if every $\alpha \in E$ is a root of a separable polynomial in $F[X]$.*

This shows that our definition of separability is equivalent to Dummit and Foote's.

Proof. Assume that E/F is separable. Then by Proposition 6 the extension $F(\alpha)/F$ is separable for every $\alpha \in E$, and by Proposition 4 this implies that α is a root of a separable polynomial.

Conversely, suppose that every $\alpha \in E$ is the root of a separable polynomial. We will show that E/F is separable. We will prove this by induction on degree, so assume that this statement is true for extensions of degree $< [E : F]$. If $E = F$, separability is clear. Otherwise, $\alpha \in E - F$, and let $K = F(\alpha)$. Since α is a root of a separable polynomial over F, by Proposition 4 the extension $F(\alpha)/F$ is separable. To use Proposition 6, we must show that E/K is separable. Now every element of E is a root of a separable polynomial over F, hence over K. Since $[E : K] < [E : F]$, induction on degree shows that E/K is separable, as required. □