Further Results on Separability and Primitive Elements

Recall that if L/F is an extension of fields, we say that

- $f \in F[x]$ is **separable** if f has no repeated roots, i.e., $\gcd(f, f') = 1$.
- $\alpha \in L$ is **separable** over F if its minimal polynomial $f \in F[x]$ is separable.
- L/F is **separable** if every $\alpha \in L$ is separable over F.

I'll add another definition to this list:

- L/F is **purely inseparable** if for every $\beta \in L \smallsetminus F$, β is **not** separable over F.

For finite extensions L/F, we can characterize separability in terms of the **separable degree** $[L : F]_s$ (see Videos 17 and 18). In particular, $1 \leq [L : F]_s \leq [L : F]$, and if $[L : F] < \infty$, then:

$$L/F \text{ is separable } \iff [L : F]_s = [L : F],$$

and

$$L/F \text{ is purely inseparable } \iff [L : F]_s = 1.$$

(The first fact was proven in Video 17; the proof of the second uses similar ideas, but I'll leave it to you, the reader, to prove.) Thus, we can view "separable" and "purely inseparable" as the two extremes, with other field extensions — those that are neither separable nor purely inseparable, i.e., with $1 < [L : F]_s < [L : F]$ — lying in between.

That said, remember that if F is a **perfect field**, then every algebraic extension of F is separable. Every field of characteristic zero (like $\mathbb{Q}$) is perfect, and every finite field (like $\mathbb{F}_p$) is also perfect. (So is every algebraic extension of a finite field, and so is every algebraically closed field.) Therefore, if you want to construct field extensions L/F that are **not** separable, then your base field F has to be **both** infinite **and** of positive characteristic; the easiest one to write down is $F = \mathbb{F}_p(t)$, the field of rational functions with coefficients in $\mathbb{F}_p$.

The following result shows that every algebraic extension L/F can be factored into a separable extension and a purely inseparable extension.

Proposition. Let L/F be an algebraic extension. Define

$$K = \{\alpha \in L \,|\, \alpha \text{ is separable over } F\},$$

called the **separable closure of F in L**. Then:

(1) K is a field containing F.
(2) K/F is a separable extension.
(3) L/K is a purely inseparable extension.

The **separable closure** of a field F is the separable closure of F in $\overline{F}$, where $\overline{F}$ is an algebraic closure of F.

Proof. (1): Every $a \in F$ is separable over F, since it is a root of the polynomial $x - a \in F[x]$, which has no repeated roots. Thus, $F \subseteq K$.

Given $\alpha, \beta \in K$, then both α and β are separable over F (by definition of K), and thus, by the results of Video 18, the field $E = F(\alpha, \beta)$ is separable over F. In particular, since all four of $\alpha + \beta$, $\alpha - \beta$, $\alpha \cdot \beta$, and (if $\beta \neq 0$) α/β belong to E, they are all separable over F. Therefore, K is closed under $+, -, \cdot, \div$ and hence is a field.

(2): Now that we know K is a field, it is separable over F by its very definition.

(3): Given $\beta \in L \smallsetminus K$, suppose, towards a contradiction, that β is separable over K. Consider the field $K(\beta) \subseteq L$. From the results of Video 18, we have that $K(\beta)/K$ is separable and (since

K/F is separable) that therefore $K(\beta)/F$ is separable. In particular, $\beta \in K(\beta)$ is separable over F. Therefore, by definition of K, we have $\beta \in K$, a contradiction. Hence, β is **not** separable over K. QED Proposition

---

Example. We have seen before that if $f \in F[x]$ is irreducible, then either $\text{char}(F) = 0$ (in which case f is separable), or else $\text{char}(F) = p \geq 2$, and we have $f(x) = g\big(x^{p^e}\big)$ for some $g \in F[x]$ irreducible and separable and some integer $e \geq 0$.
In the latter case, if $f(x) = g\big(x^{p^e}\big)$, where $g \in F[x]$ is separable and irreducible over F, let's define β to be a root of f, and α to be a root of g. Let's also define $K = F(\alpha)$ and $L = F(\beta)$. So we have $L/K/F$, with:

- K/F is separable, since $K = F(\alpha)$ adjoins a root of the separable polynomial g, and
- L/K purely inseparable, since $L = K(\beta)$, where β is the (only) root of the inseparable polynomial $h(x) = x^{p^e} - \alpha \in K[x]$).

On a somewhat related note — related because the Primitive Element Theorem has a separability hypothesis — here is a curious fact, which appears as Theorem 5.4.5 in Cox's book. (But please note: the following theorem does NOT require the extension L/F to be separable.)

Theorem. Let L/F be a finite extension. The following are equivalent:
(1) L/F has a primitive element, i.e., $L = F(\alpha)$ for some $\alpha \in L$.
(2) There are only finitely many fields K such that $L/K/F$.

Proof. First observe that if $|F| < \infty$, then $|L| < \infty$ and L/F is separable, so that (1) is true by the Primitive Element Theorem, and (2) is true because L has only finitely many subsets, and hence only finitely many subfields. Thus, we may assume that $|F| = \infty$.

($\Longrightarrow$): Let $f \in F[x]$ be the minimal polynomial for α/F, and for each field K with $L/K/F$, let $f_K \in K[x]$ be the minimal polynomial for α/K.
Thus, for each such K, we have $f_K | f$ in $K[x]$, and hence $f_K | f$ in $L[x]$. Since f has only finitely many monic factors, there are therefore only finitely many possibilities for f_K.
For any such K, write $f_K = a_0 + a_1 x + \cdots + a_{m-1}x^{m-1} + x^m \in K[x]$, and let $E = F(a_0, \ldots, a_{m-1})$, so we have $L/K/E/F$. Since f_K is irreducible over K, then f_K is irreducible over the subfield E. That is, f_K must equal f_E, the minimal polynomial of α over E. Since $L = K(\alpha) = E(\alpha)$, then, we have

$$m = \deg(f_E) = [L : E] = [L : K][K : E] = \deg(f_K)[K : E] = m[K : E].$$

Therefore $[K : E] = 1$, and hence $K = E$. Since there are only finitely many polynomials f_K, and each determines a unique field $E = F(a_0, \ldots, a_{m-1})$, statement (2) follows. QED ($\Longrightarrow$)

($\Longleftarrow$): Let $r = \min\big\{m \geq 1 \big| \exists \alpha_1, \ldots, \alpha_m \in L \text{ s.t. } L = F(\alpha_1, \ldots, \alpha_m)\big\}$.
Suppose (towards contradiction) that $r \geq 2$. Write $L = F(\alpha_1, \ldots, \alpha_r)$, and define $M = F(\alpha_1, \alpha_2)$. For each $t \in F$, define $F_t = F(\alpha_1 + t\alpha_2)$. Thus, we have $L/M/F_t/F$. In particular, for each $t \in F$, F_t is one of the intermediate fields between F and L, of which there are only finitely many, by assumption. Therefore, since we assumed $|F| = \infty$, there exist distinct $s \neq t$ in F such that $F_s = F_t$.
Hence, both $\alpha_1 + s\alpha_2$ and $\alpha_1 + t\alpha_2$ belong to $F_s = F_t$. It follows that

$$\alpha_2 = \frac{1}{s-t}\big((\alpha_1 + s\alpha_2) - (\alpha_1 + t\alpha_2)\big) \in F_s.$$

It further follows that $\alpha_1 = (\alpha_1 + s\alpha_2) - s\alpha_2 \in F_s$ as well. Thus, $M = F(\alpha_1, \alpha_2) = F_s = F(\beta)$, where $\beta = \alpha_1 + s\alpha_2$, and therefore $L = M(\alpha_3, \ldots, \alpha_r) = F(\beta, \alpha_3, \ldots, \alpha_r)$, contradicting the minimality of $r \geq 2$. Hence, $r = 1$. QED