Section X.51. Separable Extensions

Note. Let E be a finite field extension of F. Recall that $[E : F]$ is the degree of E as a vector space over F. For example, $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$ since a basis for $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbb{Q}$ is $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$. Recall that the number of isomorphisms of E onto a subfield of $\overline{F}$ leaving F fixed is the index of E over F, denoted $\{E : F\}$. We are interested in when $[E : F] = \{E : F\}$. When this equality holds (again, for *finite* extensions) E is called a separable extension of F.

Definition 51.1. Let $f(x) \in F[x]$. An element α of $\overline{F}$ such that $f(\alpha) = 0$ is a *zero of* $f(x)$ *of multiplicity* ν if ν is the greatest integer such that $(x - \alpha)^\nu$ is a factor of $f(x)$ in $F[x]$.

Note. I find the following result unintuitive and surprising! The backbone of the (brief) proof is the Conjugation Isomorphism Theorem and the Isomorphism Extension Theorem.

Theorem 51.2. Let $f(x)$ be irreducible in $F[x]$. Then all zeros of $f(x)$ in $\overline{F}$ have the same multiplicity.

Note. The following follows from the Factor Theorem (Corollary 23.3) and Theorem 51.2.

Corollary 51.3. If $f(x)$ is irreducible in $F[x]$, then $f(x)$ has a factorization in $\overline{F}[x]$ of the form

$$a \prod_i (x - \alpha_i)^\nu,$$

where the α_i are the distinct zeros of $f(x)$ in $\overline{F}$ and $a \in F$.

Note 1. By Theorem 48.3 (The Conjugation Isomorphisms Theorem) and Corollary 48.5, we know that given a simple extension $F(\alpha)$ of F, there is one extension of the identity isomorphism ι mapping F into F for every distinct zero of $\mathrm{irr}(\alpha, F)$ (namely $\psi_{\alpha,\beta}$) and these are the only extensions of ι (by the uniqueness part of Corollary 48.5). Therefore, $\{F(\alpha) : F\}$ is the number of distinct zeros of $\mathrm{irr}(\alpha, F)$.

Theorem 51.6. If E is a finite extension of F, then $\{E : F\}$ divides $[E : F]$. (In the proof we see that $[e : F]/\{E : F\} = \prod v_i$.)

Definition 51.7. A finite extension E of F is a *separable extension field of* F if $\{E : F\} = [E : F]$. An element α of $\overline{F}$ is a *separable element over* F if $F(\alpha)$ is a separable extension of F. An irreducible polynomial $f(x) \in F[x]$ is a *separable polynomial over* F if every zero of $f(x)$ in $\overline{F}$ is separable over F.

Note 2. Now that we know $\{E : F\}$ divides $[E : F]$, we are interested in when these two quantities are equal. In this case, $\prod v_i = 1$ and each zero of $\mathrm{irr}(\alpha_i, F(\alpha_1, \alpha_2, \ldots, \alpha_{i-1}))$ must be of multiplicity $v_i = 1$. So element α is a separable element over F if and only if $\mathrm{irr}(\alpha, F)$ has all zeros of multiplicity 1.

Note 3. From the Note 2 above, we see that an irreducible polynomial $f(x) \in F[x]$ is a separable polynomial over F if and only if $f(x)$ has all zeros of multiplicity 1.

Theorem 51.9. If K is a finite extension of E and E is a finite extension of F, that is $F \leq E \leq K$, then K is separable over F if and only if K is separable over E and E is separable over F.

Note. Of course, Theorem 51.9 can be inductively extended to a "tower" of extension fields: $F \leq E_1 \leq E_2 \leq \cdots \leq E_n \leq K$. In addition, the concept of "E is a separable extension field of F" can be extended to infinite extensions (though Fraleigh does not explore this in any depth; these ideas are restricted to Exercise 51.12).

Corollary 51.10. If E is a finite extension of F, then E is separable over F if and only if each $\alpha \in E$ is separable over F.

Note. Next, we will show that α *fails* to be a separable element over F only if F is an infinite field of characteristic $p \neq 0$ (in Theorems 51.13 and 51.14). By Note 2 above, α is not a separable element over F if it is a zero of $\mathrm{irr}(\alpha, F)$ of multiplicity ≥ 2. Recall that $\alpha \in \mathbb{C}$ is a zero of multiplicity m of $f(x) \in \mathbb{C}[x]$ if and only if $f(\alpha) = f'(\alpha) = f''(\alpha) = \cdots = f^{(m)}(\alpha) = 0$ and $f^{(m+1)}(\alpha) \neq 0$. This topic of separable elements in a field can be explored using "formal derivatives" (see Exercises 51.15 through 51.22). However, Fraleigh follows a shorter path.

Lemma 51.11. Let $\overline{F}$ be an algebraic closure of F and let

$$f(x) = x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1 x + a_0$$

be any monic polynomial in $\overline{F}[x]$. If $(f(x))^m \in F[x]$ and $m \cdot 1 = 1 + 1 + \cdots + 1 \neq 0$ in F, then $f(x) \in F[x]$ (that is, $a_i \in F$ for all i).

Definition 51.12. A field is *perfect* if every finite extension is a separable extension.

Theorem 51.13. Every field of characteristic zero is perfect.

Theorem 51.14. Every finite field is perfect.

Note. Combining Theorems 51.13 and 51.14 we see that fields of characteristic zero (such as $\mathbb{Q}$ and $\mathbb{R}$) and finite fields only have separable finite extensions. So for an example of a "nonseparable" extension, we must either consider infinite extensions or finite extensions of an infinite field of characteristic $p \neq 0$.

Theorem 51.15. The Primitive Element Theorem.
Let E be a finite separable extension of a field F. Then there exists $\alpha \in E$ such that $E = F(\alpha)$. That is, a finite separable extension of a field is a simple extension. The element α is a *primitive element*.

Corollary 51.16. A finite extension of a field of characteristic zero is a simple extension.

Note. Comparing Corollary 33.6 and Corollary 51.16, we see that a finite extension of (1) a finite field, and of (2) a field of characteristic zero, are both simple.

Exercise 51.3. Corollary 51.16 implies that the finite extension $\mathbb{Q}(\sqrt{2},\sqrt{3})$ of field of characteristic zero $\mathbb{Q}$ is a simple extension. Find $\alpha \in \mathbb{R}$ such that $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\alpha)$.

Solution. Let $\alpha = \sqrt{2}+\sqrt{3}$. Then $\alpha^3 = 11\sqrt{2}+9\sqrt{3}$. So $\sqrt{2} = (\alpha^3 - 9\alpha)/2$ and $\sqrt{3} = (\alpha^3 - 11\alpha)/(-2)$; hence $\sqrt{2},\sqrt{3} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$. Therefore $\mathbb{Q}(\sqrt{2},\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}+\sqrt{3})$. Also, $\sqrt{2}+\sqrt{3} \in \mathbb{Q}(\sqrt{2},\sqrt{3})$ and so $\mathbb{Q}(\sqrt{2}+\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2},\sqrt{3})$. Hence $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$.

Revised: 5/1/2015