Exercise 8.1. Let $K \subseteq L$ be a splitting field extension for some $f \in K[t] \setminus K$. Then the following are equivalent:

(i) f has a repeated root over L;

(ii) $\exists \alpha \in L$ s.t. $0 = f(\alpha) = (\mathcal{D}f)(\alpha)$;

(iii) $\exists g \in K[t]$, $\deg g \geq 1$ s.t. g divides both f and $\mathcal{D}f$.

Solution. ((i) $\implies$ (ii)) Suppose $f \in K[t] \setminus K$ has a repeated root in L. That is, $f = \prod_{i=0}^{d}(t - \alpha_i)^{r_i}$ where $\alpha_0, \ldots, \alpha_d \in L$ are roots of f, $r_j = n \geq 2$ for some j, and without loss of generality we can say $j = 0$. Then $f = gh$ over L where $g, h \in L[t] \setminus L$ of strictly smaller degree such that $g = (t - \alpha_0)^n$ and $h = \prod_{i=1}^{d}(t - \alpha_i)^{r_i}$, whence

$$\begin{aligned}
\mathcal{D}f &= \mathcal{D}(g)h + g\mathcal{D}(h) \\
&= n(t - \alpha_0)^{n-1}h + (t - \alpha_0)^n h' \\
&= (t - \alpha_0)[n(t - \alpha_0)^{n-2}h + (t - \alpha_0)^{n-1}h'].
\end{aligned}$$

Thus $f(\alpha_0) = \mathcal{D}f(\alpha_0) = 0$.

((i) $\impliedby$ (ii)) Suppose $f \in K[t] \setminus K$ does *not* have repeated a root in L. That is, $f = \prod_{i=0}^{d}(t - \alpha_i)$ where $\alpha_0, \ldots, \alpha_d \in L$ are distinct roots of f. Let $R_f = \{\alpha_0, \ldots, \alpha_d\}$ be the set of all roots of f. Then it is easy to see that

$$\mathcal{D}f(t) = \sum_{i=1}^{d} \left(\prod_{j \neq i} (t - \alpha_j) \right) \quad \implies \quad \mathcal{D}f(\alpha_k) = \prod_{j \neq k} (\alpha_k - \alpha_j) \neq 0, \quad \forall \alpha_k \in R_f$$

since $\alpha_j \neq \alpha_k$ for all $j \neq k$, so $\nexists \alpha \in L$ such that $0 = f(\alpha) = (\mathcal{D}f)(\alpha)$.

((ii) $\implies$ (iii)) Suppose $\exists \alpha \in L$ such that $\mathcal{D}f(\alpha) = f(\alpha) = 0$ for some $f \in K[t] \setminus K$. By definition of formal derivative, we know $\mathcal{D}f \in K[t]$. Moreover we are given that L is a splitting field extension for f, so $L : K$ must be finite and hence algebraic. Thus $\exists \mu_\alpha^K \in K[t]$, and by theorem we have that $\mu_\alpha^K \mid f$ and $\mu_\alpha^K \mid \mathcal{D}f$.

((iii) $\implies$ (ii)) Suppose $\exists g \in K[t]$ with $\deg g \geq 1$ such that g divides both f and $\mathcal{D}f$. We know that $f = \prod_{i=0}^{d}(t - \alpha_i)^{r_i}$ where $\alpha_0, \ldots, \alpha_d \in L$ are roots of f and $r_i \in \mathbb{N}$ for all i. Thus for g to divide f it must be divisible by some factor $(t - \alpha_j)$ of f for some j. It follows that $\mathcal{D}f$ must also be divisible by $(t - \alpha_j)$, whence α_j is a root of both $\mathcal{D}f$ and f.

Thus we have that (i) $\iff$ (ii) $\iff$ (iii). □

Exercise 8.2. Let K be a field, $\mathrm{char}(K) = p > 0$ and $f \in K[t^p]$ is an irreducible polynomial over K. Prove that f is inseparable.

Solution. Suppose $f = \sum_{i=0}^{d} a_i t^{ip} \in K[t^p]$. It follows that $\mathcal{D}f = \sum_{i=1}^{d} a_i p i t^{i(p-1)} = p \sum_{i=1}^{d} a_i i t^{i(p-1)} = 0$.

□

Exercise 8.3. Let K be a field, $\mathrm{char}(K) = p > 0$ and $f \in K[t^p]$ is an irreducible polynomial over K. Prove that if there is $g \in K[t]$ and a non-negative n such that $f(t) = g\left(t^{p^n}\right)$ and g is an irreducible and separable polynomial.

Solution. □

Exercise 8.4. Prove that $\prod_{\alpha \in \mathbb{F}_q^*} \alpha = -1$

Solution. □

Exercise 8.5.1. Let $\alpha \in \mathbb{F}_q$ and $\alpha = \beta - \beta^p$ for some $\beta \in \mathbb{F}_q$. Prove that $\mathrm{Tr}(\alpha) = 0$.

Solution. □

Exercise 8.5.2. Let $\alpha \in \mathbb{F}_q$ and $\alpha = \gamma^{1-p}$ for some nonzero $\gamma \in \mathbb{F}_q$. Prove that $\mathrm{Norm}(\alpha) = 1$.

Solution. □

Exercise 8.5.3. Let $\alpha \in \mathbb{F}_p \subseteq \mathbb{F}_{p^n}$. Prove that $\mathrm{Tr}(\alpha) = n\alpha$.

Solution. □

Exercise 8.5.4. Let $\alpha \in \mathbb{F}_p \subseteq \mathbb{F}_{p^n}$. Prove that $\mathrm{Norm}(\alpha) = \alpha^n$.

Solution. □