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, $\operatorname{char}(K) = p > 0$ and $f \in K[t^p]$ is an irreducible polynomial over K. Prove that f is inseparable.

Solution. Suppose $f = \sum_{i=0}^{d} a_i t^{ip} \in K[t^p]$ is irreducible over K. By definition of the formal derivative, $\mathcal{D}f = \sum_{i=1}^{d} a_i p i t^{i(p-1)} = p\sum_{i=1}^{d} a_i i t^{i(p-1)} = 0$. Then by exercise 8.1 it follows that f is inseparable over K. □

Exercise 8.3. Let K be a field, $\operatorname{char}(K) = p > 0$ and $f \in K[t^p]$ is an irreducible polynomial over K. Prove that 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. We first notice that by Exercise 8.2, we have that f is inseparable over K. We know $f = \sum_{i=0}^{d} a_i t^{ip} \in K[t^p]$ so let $g(t^{p^n}) = \sum_{i=0}^{d} a_i \left(t^{p^n}\right)^i$, which is obviously equivalent to f for $n = 1 \in \mathbb{Z}_{\geq 0}$. Thus $f(t) = g\left(t^{p^n}\right)$ for some $g \in K[t]$ and $n \in \mathbb{Z}_{\geq 0}$.

Suppose then that g is reducible in $K[t]$, which is to say that $g = \overline{g}_1\overline{g}_2$ for $\overline{g}_1, \overline{g}_2 \in K[t] \setminus K$ of strictly lesser degree than g, and without loss of generality $\deg \overline{g}_1 \geq \deg \overline{g}_2 \geq 1$. Then

$$f(t) = g(t^p) = \overline{g}_1(t^p)\overline{g}_2(t^p) = f_1(t)f_2(t)$$

where $f_i(t) = \overline{g}_i(t^p) \in K[t^p]$ for $i = 1, 2$. Hence f is reducible if g is reducible, and by contrapositive the irreduciblity of f implies irreducibility of g.

If $\mathcal{D}g(t) \neq 0$, then g is separable and we are done. Else, assume we have shown that $f(t) = g_n\left(t^{p^{n+1}}\right) \in K[t^p]$ for $1 \leq k \leq n$. If $\mathcal{D}g_n(t) \neq 0$, then g_n is separable and we are done. Else, $g_n(t) = g_{n+1}(t^p)$ by Exercise 8.1.

Notice that $\deg f = \deg g_n\left(t^{p^n}\right) = (\deg g_n) \cdot p^n \in \mathbb{N}$ and we know $p \neq 0$, so obviously $\deg f > \deg g > \deg g_1 > \cdots > \deg g_n$ and $\deg g_n = \frac{\deg f}{p^n}$. Eventually we must have either $\mathcal{D}g_n \neq 0$ or $\deg g_n = 1$ and we note that in the latter case, $g_n \in K[t^p]$ contradicts that f is irreducible.

Hence our inductive procedure necessarily ends in some g_n with $\mathcal{D}g_n \neq 0$, whence g_n is separable over K. □

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

Solution. By theorem, we have that every element of $\mathbb{F}_q$ satisfies the equality $t^q = t$. Then $t^q - t = t(t^{q-1} - 1) = 0$ and we can factor out the zero root to see that every nonzero element of $\mathbb{F}_q$ satisfies the relationship $t^{q-1} = 1$. Thus, every element of $\mathbb{F}_q^*$ is a root of the polynomial $x^{q-1} - 1 = 0$. Moreover, we know $\mathbb{F}_q$ is a splitting field for $t^q - t$, so it follows that $\mathbb{F}_q^*$ is also a splitting field for $x^{q-1} - 1$. Hence $x^{q-1} - 1 = \prod_{\alpha \in \mathbb{F}_q^*}(x - \alpha)$. Then by comparing constant terms, we can see that

$$-1 = \prod_{\alpha \in \mathbb{F}_q^*}(-\alpha) = (-1)^{q-1} \prod_{\alpha \in \mathbb{F}_q^*} \alpha.$$

We know $q = p^n$ so obviously for $p > 2$ we have that $q - 1$ must be even, and hence $(-1)^{q-1} = 1$. If $p = 2$, then we have $q - 1$ must be odd and $(-1)^{q-1} = -1$, but we know $-1 = 1$ in characteristic 2. Hence we have $\prod_{\alpha \in \mathbb{F}_q^*} \alpha = -1$. □

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. By definition of trace, we have

$$\mathrm{Tr}(\alpha) = \sum_{i=0}^{n-1} \alpha^{p^i} = \sum_{i=0}^{n-1} (\beta - \beta^p)^{p^i}.$$

Since we are working in characteristic p, this simplifies to

$$\begin{aligned}\mathrm{Tr}(\alpha) &= \sum_{i=0}^{n-1} \beta^{p^i} - (\beta^p)^{p^i} = \sum_{i=0}^{n-1} \beta^{p^i} - \beta^{p^{i+1}} \\ &= (\beta - \beta^p) + (\beta^p - \beta^{p+1}) + \cdots + (\beta^{p^{n-2}} - \beta^{p^{n-1}}) + (\beta^{p^{n-1}} - \beta^{p^n}).\end{aligned}$$

Notice that all intermediate terms immediately cancel out, leaving us with $\mathrm{Tr}(\alpha) = \beta - \beta^{p^n}$. Recall that every $\gamma \in \mathbb{F}_q$ satisfies the equality $\gamma = \gamma^q$, and since $q = p^n$ we have $\beta^{p^n} = \beta$ over $\mathbb{F}_q$. Thus $\mathrm{Tr}(\alpha) = \beta - \beta = 0$. □

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. By definition of norm we have

$$\begin{aligned}\mathrm{Norm}(\alpha) &= \prod_{i=0}^{n-1} \alpha^{p^i} = \prod_{i=0}^{n-1} \left(\gamma^{1-p}\right)^{p^i} = \prod_{i=0}^{n-1} \frac{\gamma^i}{\gamma^{p^{i+1}}} \\ &= \left(\frac{\gamma}{\gamma^p}\right) \cdot \left(\frac{\gamma^p}{\gamma^{p^2}}\right) \cdot \left(\frac{\gamma^{p^2}}{\gamma^{p^3}}\right) \cdots \left(\frac{\gamma^{p^{n-1}}}{\gamma^{p^n}}\right)\end{aligned}$$

Similarly to before, everything cancels out except the numerator of the first term and the denominator of the last. Thus, $\mathrm{Norm}(\alpha) = \frac{\gamma}{\gamma^{p^n}}$ and we know $\gamma^{p^n} = \gamma$ so $\mathrm{Norm}(\alpha) = \frac{\gamma}{\gamma} = 1$. □

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

Solution. Given that $\alpha \in \mathbb{F}_p$ we know $\alpha^p = \alpha$, so $\alpha^{p^k} = (\alpha^p)^{p^{k-1}} = \alpha^{p^{k-1}}$ and by induction, we find that $\alpha^{p^k} = \alpha$ for all $k \in \mathbb{N}$. Thus $\mathrm{Tr}(\alpha) = \sum_{i=0}^{n-1} \alpha^{p^i} = \sum_{i=0}^{n-1} \alpha = n\alpha$. □

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

Solution. By the same reasoning as Exercise 8.5.3, we have $\mathrm{Norm}(\alpha) = \prod_{i=0}^{n-1} \alpha^{p^i} = \prod_{i=0}^{n-1} \alpha = \alpha^n$. □