Example 9.4. The condition $\mathrm{char}(F)=0$ or $\mathrm{char}(F)=p>m$ in Theorem 9.3(2) is crucial. For example let $f(x)=x^3-2\in\mathbb{Z}_3[x]$. Then

$$(x-2)^3 = x^3-3\cdot 2x^2-3\cdot 2^2x-2^3 = x^3-2=f(x)$$

Hence $E=\mathbb{Z}_3$ is a splitting field of f over $\mathbb{Z}_3$ and 2 has multiplicity 3 in $f(x)$. On the other hand $f'(x)=3x^2=0$ and so $f'(x)=f''(x)=f'''(x)=0$. Hence condition (1) of Theorem 9.3 fails.

Lemma 9.5. Let $f(x)\in F[x]$ be irreducible. Let E be a splitting field of f over F. Then f has multiple roots in E if and only if $f'(x)=0$.

Proof. Since f is irreducible, we have $\deg(f)\geq 1$. Hence there exists a root α of f in E. Then

$$f(x)=g(x)(x-\alpha) \qquad (*)$$

$$f'(x)=g'(x)(x-\alpha)+g(\alpha) \qquad (**)$$

for some $g(x)\in E[x]$. Let

$$f(x)=a_0+a_1x+\dots+a_nx^n,\quad a_n\neq 0.$$

Then $a_n^{-1}f(x)$ is the minimal polynomial of α over F. Since $\deg(f')<\deg(f)$, it follows that $f'(\alpha)=0 \iff f'(x)=0$. Hence we obtain

α is a multiple root of $f \overset{(*)}{\iff} g(\alpha)=0 \overset{(**)}{\iff} f'(\alpha)=0 \iff f'(x)=0$. $\square$

Corollary 9.6. Let $f(x)\in F[x]$ be irreducible. Let E be a splitting field of f over F.

(1) If $\mathrm{char}\,F=0$, then $f(x)$ has only simple roots in E.

(2) If $\mathrm{char}\,F=p>0$, then $f(x)$ has a multiple root in E if and only if $\exists\, g(x)\in F[x]$ with $f(x)=g(x^p)$.

Proof. Let $f(x)=a_0+a_1x+\cdots+a_nx^n$. Then
$$f'(x)=a_1+2a_2x+\cdots+na_nx^{n-1} \qquad (*).$$
(1) Assume to a contradiction that f has a multiple root in E. Then by Lemma 9.5 we have $f'(x)=0$ and so by $(*)$
$$a_1+2a_2x+\cdots+na_nx^{n-1}=0.$$
Since $\mathrm{char}(F)=0$, we conclude that $a_1=a_2=\cdots=a_n=0$ and so $f(x)=a_0$, contradicting f being irreducible.

(2) We have

$f(x)$ has a multiple root in $E \overset{\text{Lem 9.5}}{\Longleftrightarrow} f'(x)=0$

$\overset{(*)}{\Longleftrightarrow} ia_i=0 \quad \forall\ 1\le i\le n$

$\overset{\mathrm{char}(F)=p}{\Longleftrightarrow} a_i=0 \text{ if } p\nmid i$

$\Longleftrightarrow f(x)=a_0+a_px^p+a_{2p}x^{2p}+\cdots+a_{kp}x^{kp}$

$\Longleftrightarrow f(x)=g(x^p),\ g(x)=a_0+a_px+\cdots+a_{kp}x^k.$ $\square$

Theorem 9.7 Let $f(x)\in F[x]$ be irreducible. Let E be a splitting field of F. Then all roots of f in E have the same multiplicity.

Proof. Let $\alpha,\beta\in E$ be two distinct roots of f in E with multiplicities $m(\alpha)$, $m(\beta)$. We have the ring isomorphism
$$\sigma: F(\alpha) \longrightarrow F(\beta) \qquad (\sigma|_F=\mathrm{id}_F)$$
$$a_0+a_1\alpha+\cdots+a_n\alpha^n \longmapsto a_0+a_1\beta+\cdots+a_n\beta^n$$
We may assume that $F\subseteq F(\alpha)\subseteq \overline{F}$ so that $\overline{F(\alpha)}=\overline{F}$ (exercise). Similarly, $\overline{F(\beta)}=\overline{F}$. Therefore we have the field embeddings
$$\begin{tikzcd}
\overline{F}=\overline{F(\alpha)} \arrow[r, "\sigma^*"] & \overline{F(\beta)}=\overline{F} \\
 & F(\beta) \arrow[u, hook, "\iota_\beta"'] \\
F(\alpha) \arrow[uu, hook, "\iota_\alpha"] \arrow[ur, "\sigma", "\sim"'] &
\end{tikzcd}$$
,

where σ^* exists by Theorem 6.5 and $\sigma^*\circ\iota_\alpha=\iota_\beta\circ\sigma$. Then we have the ring homomorphism

$$\eta : \bar{F}[x] \longrightarrow \bar{F}[x]$$

$$p(x) = a_0 + a_1 x + \cdots + a_k x^k \longmapsto \eta(p(x)) = \sigma^*(a_0) + \sigma^*(a_1)x + \cdots + \sigma^*(a_k)x^k$$

In particular, $\eta(f(x)) = f(x)$ since $f(x) \in F[x]$, while

$$\sigma^*(\alpha) = \sigma^* \circ \iota_\alpha(\alpha) = \iota_\beta \circ \sigma(\alpha) = \iota_\beta(\beta) = \beta$$

implies $\eta((x-\alpha)^k) = (x-\beta)^k$. Then

$$f(x) = \eta(f(x)) = \eta(g(x)(x-\alpha)^{m(\alpha)}) = \eta(g(x))\,\eta((x-\alpha)^{m(\alpha)}) = \eta(g(x))(x-\beta)^{m(\alpha)}$$

implies $m(\alpha) \leq m(\beta)$. The same arguments on the opposite direction give $m(\beta) \leq m(\alpha)$ and so $m(\alpha) = m(\beta)$. ∎

By Theorem 9.7 we conclude that if $f(x) \in F[x]$ is irreducible and E is the splitting field of f over F, then

$$f(x) = a(x-\alpha_1)^k (x-\alpha_2)^k \cdots (x-\alpha_r)^k,$$

where $\alpha_1, \dots, \alpha_r$ are distinct roots of f, each with multiplicity k.