2.30 Proof that perfect fields give no repeated roots

Theorem 2.36. *Let $\mathbb{F}$ be a field. The field*

$$\mathbb{F} \textit{ is perfect}$$

if and only if $\mathbb{F}$ satisfies

$$\text{if } f(x) \in \mathbb{F}[x] \text{ and } f(x) \text{ is irreducible} \quad \text{then} \quad f(x) \text{ has no repeated roots.}$$

Proof. $\Rightarrow$: Assume $\mathbb{F}$ is perfect and let $m(x) \in \mathbb{F}[x]$.
To show: If $m(x) \in \mathbb{F}[x]$ has a repeated root then $m(x)$ is not irreducible.
Assume $\alpha \in \overline{\mathbb{F}}$ is a repeated root of $m(x)$.
Then

$$m(x) = (x-\alpha)^2 n(x) \qquad \text{and} \qquad m'(x) = \frac{dm}{dx} = (x-\alpha)^2 \frac{dn}{dx} + 2(x-\alpha)n(x),$$

giving that $m'(\alpha) = 0$.

Case $m'(x) \neq 0$: Since $\deg(m'(x)) < m(x)$ then $m(x)$ is not the minimal polynomial of α.
So $m(x)$ is a multiple of $m_{\alpha,\mathbb{F}}(x)$.
So $m(x)$ is not irreducible.

Case $m'(x) = 0$ and $\mathrm{char}(\mathbb{F}) = 0$. Then $\deg(m(x)) = 0$. So $m(x)$ is not irreducible.

Case $m'(x) = 0$ and $\mathrm{char}(\mathbb{F}) = p$ with $p > 0$. Then $m(x) = x^{kp} + c_{k-1}x^{(k-1)p} + \cdots + c_1 x^p + c_0$.
Let $b_{k-1} = F^{-1}(c_{k-1}), \ldots, b_0 = F^{-1}(c_0)$.
Then

$$\begin{aligned} m(x) &= x^{kp} + F(b_{k-1})x^{(k-1)p} + \cdots + F(b_1)x^p + F(b_0) \\ &= x^{kp} + b_{k-1})^p x^{(k-1)p} + \cdots + b_1^p x^p + b_0^p \\ &= (x^k + b_{k-1}x^{k-1} + \cdots + b_1 x + b_0)^p. \end{aligned}$$

So $m(x)$ is not irreducible.

$\Leftarrow$: Assume $\mathbb{F}$ is not perfect and $p = \mathrm{char}(\mathbb{F}) \in \mathbb{Z}_{>0}$.
To show: There exists $f(x) \in \mathbb{F}[x]$ such that $f(x)$ is irreducible and $f(x)$ has a multiple root.
Since $\mathbb{F}$ is not perfect then there exists $\alpha \in \mathbb{F}$ such that $\alpha^{1/p} \notin \mathbb{F}$.
Let

$$f(x) = m_{\alpha,\mathbb{F}}(x) = x^p - \alpha \qquad \text{be the minimal polynomial of } \alpha \text{ over } \mathbb{F}.$$

Since $f(x)$ is the minimal polynomial of α over $\mathbb{F}$ then $f(x)$ is irreducible.
Since $f(x) = x^p - \alpha = (x - \alpha^{1/p})^p$ then $f(x)$ has a multiple root. □