# 1

Since the roots of the polynomial are $\pm\sqrt{2}, \pm\sqrt{10}$, then the splitting field is given by $\mathbb{Q}(\sqrt{2}, \sqrt{10})$. Clearly, $\mathbb{Q}(\sqrt{2}+\sqrt{5})$ is a subset of the splitting field, we will show the opposite inclusion. Since the former contains $\sqrt{2}+\sqrt{5}$, it also contains

$$(\sqrt{2}+\sqrt{5})^2 = 7 + \sqrt{10}$$

and $-7 \in \mathbb{Q}$, so $\sqrt{10} \in \mathbb{Q}(\sqrt{2}+\sqrt{5})$. Then

$$(\sqrt{2}+\sqrt{5})\sqrt{10} = 2\sqrt{5} + 5\sqrt{2} \in \mathbb{Q}(\sqrt{2}+\sqrt{5}),$$

and subtracting $2(\sqrt{2}+\sqrt{5})$, we obtain $3\sqrt{2} \in \mathbb{Q}(\sqrt{2}+\sqrt{5})$. And since $1/3 \in \mathbb{Q}$, then in fact $\sqrt{2} \in \mathbb{Q}(\sqrt{2}+\sqrt{5})$. Hence, the splitting field $\mathbb{Q}(\sqrt{2}, \sqrt{10})$ is precisely $\mathbb{Q}(\sqrt{2}+\sqrt{5})$.

## 2

Given that $K$ is the splitting field for $f(x)$, then

$$f(x) = a(x-\alpha_1)\cdots(x-\alpha_n)$$

for some $a \in F^\times$ and $\alpha_1, \ldots, \alpha_n \in K$. Let $S = \{\alpha_1, \ldots, \alpha_n\}$, then we know $K = F(S)$. Given any $\alpha \in S$, we know $\alpha$ is a root of $f(x)$, so

$$m_{\alpha,F}(x) \mid f(x).$$

Since $\gcd(f(x), f'(x)) = 1$, then $f(x)$ is separable, so $m_{\alpha,F}(x)$ must also be separable (otherwise, $m_{\alpha,F}(x) \mid f(x)$ would imply $f(x)$ has multiple roots). That is, $\alpha$ is separable over $F$, so every element of $S$ is separable over $F$. And since $K = F(S)$, then $K/F$ is separable.

# 3

The proof is symmetric with respect to $\alpha$ and $\beta$; it suffices to show one direction. Suppose $m_{\alpha,F}(x)$ is irreducible over $(F(\beta))[x]$. We have

$$[F(\alpha,\beta):F] = [(F(\beta))(\alpha):F(\beta)][F(\beta):F],$$

where $[F(\beta):F] = \deg m_{\beta,F}(x)$. Since $m_{\alpha,F}(x) \in (F(\beta))[x]$ is monic, irreducible and has $\alpha$ as a root, then in fact, it is the minimal polynomial of $\alpha$ in $(F(\beta))[x]$. Therefore, we have

$$[F(\alpha,\beta):F] = (\deg m_{\alpha,F}(x))(\deg m_{\beta,F}(x)).$$

On the other hand, we have

$$[F(\alpha,\beta):F] = [(F(\alpha))(\beta):F(\alpha)][F(\alpha):F],$$

where $[F(\alpha):F] = \deg m_{\alpha,F}(x)$. Therefore, we have

$$[(F(\alpha))(\beta):F(\alpha)] = \deg m_{\beta,F}(x).$$

Now since $m_{\beta,F}(x) \in (F(\alpha))[x]$ has $\beta$ as a root and has the same degree as the extension $(F(\alpha))(\beta)/F(\alpha)$, then we must have $m_{\beta,F}(x)$ irreducible in $(F(\alpha))[x]$.

# 4

## (a)

Since $\theta_1 \in \overline{\mathbb{F}_p}$, then $\mathbb{F}_p(\theta_1)$ is a finite subfield of $\overline{\mathbb{F}_p}$. Then the minimal polynomial of $\theta_1$ over $\mathbb{F}_p$ divides $f(x)$. Since $f(x)$ is irreducible, then $m_{\theta_1,\mathbb{F}_p}(x) = a^{-1}f(x)$, where $a \in \mathbb{F}_p^\times$ is the leading coefficient of $f(x)$. In particular,

$$[\mathbb{F}_p(\theta_1) : \mathbb{F}_p] = \deg m_{\theta_1,\mathbb{F}_p}(x) = \deg f(x).$$

By the same argument.

$$[\mathbb{F}_p(\theta_2) : \mathbb{F}_p] = \deg m_{\theta_2,\mathbb{F}_p}(x) = \deg f(x).$$

This implies that $|\mathbb{F}_p(\theta_1)| = p^{\deg f(x)} = |\mathbb{F}_p(\theta_2)|$. Since both $F_p(\theta_1)$ and $\mathbb{F}_p(\theta_2)$ are subfields of $\overline{\mathbb{F}_p}$ with the same cardinality, then they must be precisely the same subfield, i.e., $\mathbb{F}_p(\theta_1) = \mathbb{F}_p(\theta_2)$.

## (b)

Since $K \subseteq \overline{\mathbb{F}_p}$ is the splitting field for $f(x)$ over $\mathbb{F}_p$, then $K = \mathbb{F}_p(S)$, where $S \subseteq \overline{\mathbb{F}_p}$ is the set of roots of $f(x)$ in $\overline{\mathbb{F}_p}$. For any pair $\theta_1, \theta_2 \in S$, from $(a)$, we know that $\mathbb{F}_p(\theta_1) = \mathbb{F}_p(\theta_2)$. Moreover, this means

$$\mathbb{F}_p(\theta_1, \theta_2) = \mathbb{F}_p(\theta_1).$$

Continuing inductively, suppose $\mathbb{F}_p(\theta_1, \ldots, \theta_{n-1}) = \mathbb{F}_p(\theta_1)$, for roots $\theta_1, \ldots, \theta_n \in S$. Then

$$\mathbb{F}_p(\theta_1, \ldots, \theta_n) = (\mathbb{F}_p(\theta_1, \ldots, \theta_{n-1}))(\theta_n) = \mathbb{F}_p(\theta_1, \theta_n) = \mathbb{F}_p(\theta_1).$$

Since $S$ has only finitely many roots, this induction shows that $K = \mathbb{F}_p(S) = \mathbb{F}_p(\theta)$ for any root $\theta \in S$. Then $m_{\theta,\mathbb{F}_p}(x) = a^{-1}f(x)$, where $a \in \mathbb{F}_p^\times$ is the leading coefficient of $f(x)$ (since $a^{-1}f(x) \in \mathbb{F}_p[x]$ monic, irreducible, and has $\theta$ as root), so

$$[K : \mathbb{F}_p] = [\mathbb{F}_p(\theta) : F] = \deg m_{\theta,\mathbb{F}_p}(x) = \deg f(x).$$

# 5

## (a)

By definition, $E \subseteq K$. Clearly, each $\alpha \in F$ is separable over $F$ since $m_{\alpha,F}(x) = x - \alpha \in F[x]$ has only $\alpha$ as a simple root. Therefore, as sets, $F \subseteq E \subseteq K$.

We now show $E$ is a field. Since $F \subseteq E$, then in particular, $0, 1 \in E$. If $\alpha, \beta \in E$, i.e., $\alpha, \beta$ are separable over $F$, then $F(\alpha, \beta)/F$ is a separable field extension of $F$. Since $F(\alpha, \beta)$ is a field containing $\alpha$ and $\beta$, then we know $\alpha - \beta, \alpha^{-1}\beta \in F(\alpha, \beta)$. Since $F(\alpha, \beta)$ is separable over $F$, then both $\alpha - \beta$ and $\alpha^{-1}\beta$ are separable over $F$. That is, both are contained in $E$, proving that $E$ is a field.

## (b)

Since $F$ is characteristic $p$, if $m_{\alpha,F}(x)$ is inseparable, we have shown its derivative will be identically zero. This means that all the powers of $x$ are multiples of $p$, so we can write it as a polynomial in $x^p$, say $m_{\alpha,F}(x) = f(x^p)$. Then either $f(x)$ is separable or its inseparable, if it is inseparable, we repeat the process until we obtain a separable function $g(x)$ such that $g(x^{p^m}) = m_{\alpha,F}(x)$. Then $\alpha^{p^m}$ is separable over $F$.

After this, it would remain to show that $n \geq m$ implies $\alpha^{p^n}$ is separable

## (c)