Content:

Big goal	Prove all splitting fields are unique.
Theorem	If E is a field with p^n elements, then E is a splitting field for $f(x)$ over $\mathbb{Z}_p$.
Notation	$\varphi: F \to F'$ is an isomorphism $\varphi^*: F[x] \to F'[x]$ is an isomorphism induced by φ Denote $\varphi^*(f(x)) = f^*(x)$. $\overline{\varphi}: F[x]/(f(x)) \to F'[x]/(f^*(x))$ is an isomorphism
Question	If $p(x)$ is irreducible in $F[x]$ is $p^*(x)$ irreducible in $F'[x]$?
Question	If $p(x)$ is irreducible in $F[x]$, α is a root of $p(x)$ in some E/F, α' is a root of $p^*(x)$ in some E'/F', is $F(\alpha) \cong F'(\alpha')$?
Question	What can we say about the isomorphism ψ?
Question	If $f(x) \in F[x]$, E is a splitting field for $f(x)$ over F, α is a root of $f(x)$ in E, is E a splitting field for $f(x)$ over $F(\alpha)$?
Theorem	If $f(x) \in F[x]$ where F is a field, E is a splitting field for $f(x)$ over F, $\varphi: F \to F'$ is an isomorphism, $\varphi^*: F[x] \to F'[x]$ is an isomorphism induced by φ, E' is a splitting field for $f^*(x)$ over F', then $\Phi: E \to E'$ such that Φ extends φ and $\overline{\varphi}$ is an isomorphism.
Corollary	If E, E' are splitting fields for $f(x)$ over F then $E \cong E'$.
Corollary	Any 2 fields of order p^n are isomorphic.

Big goal Prove all splitting fields are unique.

Theorem Let E be a field with p^n elements. Then E is a splitting field for $f(x) = x^{p^n} - x$ over $\mathbb{Z}_p$.

Proof:

Let E be a field such that $|E| = p^n$. Then $|E^*| = p^n - 1$.

Since E* is a multiplicative group, then

$\forall\, c \in E^*$, $c^{p^n - 1} = 1$ (by Lagrange).

So $c^{p^n} = c\ \forall\, c \in E^*$.

In fact, $0^{p^n} = 0$, so $c^{p^n} = c\ \forall\, c \in E$.

Thus, all elements in E are roots of $f(x) = x^{p^n} - x$.

And since $\deg f(x) = p^n \Rightarrow f(x)$ has at most p^n roots,

then E contains all the roots of $f(x)$.

That is, a is a root of $f(x) \Leftrightarrow a \in E$.

Thus, $f(x)$ splits over E.

Moreover, since all elements in E are roots, E must be the smallest field in which $f(x)$ splits. So E is a splitting field for $f(x) = x^{p^n} - x$.

Notation $\varphi: F \to F'$ is an isomorphism.

$\varphi^*: F[x] \to F'[x]$ is an isomorphism induced by φ.

Denote $\varphi^*(f(x)) = f^*(x)$.

Proof: (See Proposition 3.48)

Define $\varphi^*: F[x] \to F'[x]$ by $\varphi^*(r_0 + r_1x + \cdots) = \varphi(r_0) + \varphi(r_1)x + \cdots$.

To show φ^* is well-defined and injective,

let $f, g \in F[x]$ where $f(x) = a_0 + a_1x + \cdots + a_nx^n$, and

$g(x) = b_0 + b_1x + \cdots + b_mx^m$.

Then $\varphi^*(f) = \varphi(a_0) + \varphi(a_1)x + \cdots + \varphi(a_n)x^n$ and

$\varphi^*(g) = \varphi(b_0) + \varphi(b_1)x + \cdots + \varphi(b_m)x^m$.

Thus, since φ is well-defined and injective,

$\varphi^*(f) = \varphi^*(g) \Leftrightarrow \varphi(a_i) = \varphi(b_i) \ \forall\, i,\ 0 \le i \le \max\{n, m\} \Leftrightarrow a_i = b_i \ \forall\, i$.

$\therefore$ φ^* is well-defined and injective.

To show φ^* is a homomorphism, define f and g as above and assume, without loss of generality, that $n \ge m$. Note that $b_i = 0 \ \forall\, i > m$.

We note that since φ is a homomorphism, we have

$$\varphi^*(f+g) = \varphi^*\left(\sum_{i=0}^{n}(a_i + b_i)x^i\right)$$

$$= \sum_{i=0}^{n}\varphi(a_i + b_i)x^i$$

$$= \sum_{i=0}^{n}\varphi(a_i)x^i + \sum_{i=0}^{n}\varphi(b_i)x^i$$

$$= \varphi^*\left(\sum_{i=0}^{n}a_ix^i\right) + \varphi^*\left(\sum_{i=0}^{n}b_ix^i\right)$$

$= \varphi^*(f) + \varphi^*(g)$. And

$$\varphi^*(fg) = \varphi^*\left(\sum_{i=0}^{n+m}c_ix^i\right) \text{ where } c_i = \sum_{j=0}^{i}a_jb_{j-i}$$

$$= \sum_{i=0}^{n}\varphi(c_i)x^i \text{ where } \varphi(c_i) = \sum_{j=0}^{i}\varphi(a_jb_{j-i}) = \sum_{j=0}^{i}\varphi(a_j)\varphi(b_{j-i})$$

$$= \sum_{i=0}^{n}\varphi(a_i)x^i \bullet \sum_{i=0}^{n}\varphi(b_i)x^i$$

$$= \varphi^*\left(\sum_{i=0}^{n}a_ix^i\right) \bullet \varphi^*\left(\sum_{i=0}^{n}b_ix^i\right)$$

$= \varphi^*(f)\varphi^*(g)$.

$\therefore$ φ^* is a homomorphism.

To show φ^* is surjective, let $f' \in F'[x]$.

Then $f' = r_0' + r_1'x + \cdots + r_n'x^n$ for some $r_i' \in F'$.

Since φ is surjective, then $\exists\, r_i \in F$ such that $\varphi(r_i) = r_i'$ for each i.

Thus $\varphi^*(r_0 + r_1x + \cdots + r_nx^n) = \varphi(r_0) + \varphi(r_1)x + \cdots + \varphi(r_n)x^n$

$= r_0' + r_1'x + \cdots + r_n'x^n$.

$\therefore$ φ^* is surjective, hence φ^* is a bijection.

$\overline{\varphi}: F[x]/(f(x)) \to F'[x]/(f^*(x))$ is an isomorphism

Proof:

Define $\overline{\varphi}: F[x]/(f(x)) \to F'[x]/(f^*(x))$ by
$\overline{\varphi}(r(x) + (f(x))) = r^*(x) + (f^*(x))$.
Since cosets are not always uniquely represented, we need to check that $\overline{\varphi}$ is well-defined. To show is well-defined, choose $r_1(x), r_2(x) \in F[x]$ such that
$r_1(x) + (f(x)) = r_2(x) + (f(x))$. Then $r_1(x) - r_2(x) \in (f(x))$.
So $\varphi^*(r_1(x) - r_2(x)) \in \varphi^*((f(x)))$.
Claim: $\varphi^*((f(x))) = (f^*(x))$.
Let $g^*(x) \in \varphi^*((f(x)))$.
Then $\exists\, g(x) \in (f(x))$ such that $\varphi^*(g(x)) = g^*(x)$.
So $g(x) = f(x)h(x)$ for some $h(x) \in F[x]$. And
$g^*(x) = \varphi^*(g(x)) = \varphi^*(f(x)h(x)) = \varphi^*(f(x))\varphi^*(h(x)) \in (\varphi^*(f(x)))$.
For the reverse containment, let $g'(x) \in (f^*(x))$.
Then $g'(x) = f^*(x)h'(x)$ for some $h'(x) \in F'[x]$.
Since φ^* is surjective, then
$\exists\, h(x) \in F[x]$ such that $h^*(x)) = h'(x)$.
And $g'(x) = f^*(x)h^*(x)) = \varphi^*(f(x)h(x)) \in \varphi^*((f(x)))$ since
$f(x)h(x) \in (f(x))$.
$\therefore\ \varphi^*((f(x))) = (f^*(x))$.
Thus $\varphi^*(r_1(x) - r_2(x)) = \varphi^*(r_1(x)) - \varphi^*(r_2(x)) \in \varphi^*((f(x))) = (f^*(x))$.
And since $\deg f^*(x)$ is minimal in $(f^*(x))$,
$\deg \varphi^*(r_1(x)) = \deg r_1(x) < \deg f(x) = \deg f^*(x)$, and
$\deg \varphi^*(r_2(x)) = \deg r_2(x) < \deg f(x) = \deg f^*(x)$, we have that
$\varphi^*(r_1(x)) = \varphi^*(r_2(x))$, hence
$\varphi^*(r_1(x)) + (f^*(x))) = \varphi^*(r_2(x)) + (f^*(x)))$.
$\therefore\ \overline{\varphi}(r_1(x) + (f(x))) = \overline{\varphi}(r_2(x) + (f(x)))$
$\therefore\ \overline{\varphi}$ is well-defined.

To show is injective, choose $r_1(x), r_2(x) \in F[x]$ such that
$\overline{\varphi}(r_1(x) + (f(x))) = \overline{\varphi}(r_2(x) + (f(x)))$.
Then $\varphi^*(r_1(x)) + (f^*(x)) = \varphi^*(r_2(x)) + (f^*(x))$.
Thus $\varphi^*(r_1(x)) - \varphi^*(r_2(x)) \in (f^*(x))$.
Since $f^*(x)$ is of minimal degree in $(f^*(x))$,
$\deg \varphi^*(r_1(x)) = \deg r_1(x) < \deg f(x) = \deg f^*(x)$, and
$\deg \varphi^*(r_2(x)) = \deg r_2(x) < \deg f(x) = \deg f^*(x)$,
then $\varphi^*(r_1(x)) - \varphi^*(r_2(x)) = 0$, (Lecture Notes 1/27/10),
hence $\varphi^*(r_1(x)) = \varphi^*(r_2(x))$.
And since φ^* is injective, then $r_1(x) = r_2(x)$, hence
$r_1(x) + (f(x)) = r_2(x) + (f(x))$.
$\therefore\ \overline{\varphi}$ is injective.

The surjective and homomorphic properties of $\overline{\varphi}$ can be easily shown and are left to the reader.

Question (1) If $p(x)$ is irreducible in $F[x]$ is $p^*(x)$ irreducible in $F'[x]$? Yes.

Proof:
Assume $p(x)$ is irreducible in $F[x]$.
Suppose $p^*(x) = a(x)b(x)$ where $a(x), b(x) \in F'[x]$.
Since φ^* is onto, $\exists\, g(x), h(x) \in F[x]$ such that
$g^*(x) = a(x)$, $h^*(x) = b(x)$.
Thus $\varphi^*(p(x)) = \varphi^*(g(x))\varphi^*(h(x)) = \varphi^*(g(x)h(x))$.
And $p(x) = g(x)h(x)$ as φ^* is injective.
Since $p(x)$ is irreducible, $g(x)$ or $h(x)$ is a unit in $F[x]$.
Without loss of generality, assume $g(x) = c$ for some $c \in F^\times$
(i.e. nonzero elements of F).
Then $g^*(x) = \varphi^*(g(x)) = \varphi^*(c) = \varphi(c) \in F'$.
Thus, $g^*(x)$ is a unit, so $p^*(x)$ is irreducible.

Question (2) If $p(x)$ is irreducible in $F[x]$, α is a root of $p(x)$ in some E/F, α' is a root of $p^*(x)$ in some E'/F', is $F(\alpha) \cong F'(\alpha')$? Yes.

Proof:
$F(\alpha) \cong F[x]/(p(x)) \cong F'[x]/(p^*(x)) \cong F'(\alpha')$?

Question (3) What can we say about the isomorphism ψ?
Define $\bar{\bar{\varphi}}$: F[x]/(p(x)) → F[x] by $\bar{\bar{\varphi}}\,(r(x) + (p(x))) = r(x)$.
Define φ_α: $F[x] \to F(\alpha)$ by $r(x) = r(\alpha)$.
Define $\bar{\bar{\varphi}}_\alpha$: $F[x]/(p(x)) \to F(\alpha)$ by $\bar{\bar{\varphi}}_\alpha(r(x) + (p(x))) = \bar{\bar{\varphi}}(\varphi_\alpha(r(x)))$
Define ψ: $F(\alpha) \to F'(\alpha')$ by $\psi(f(x)) = \bar{\bar{\varphi}}_{\alpha'}\,(\bar{\varphi}\,(\bar{\bar{\varphi}}_\alpha^{-1}(w))$.
So our map looks like

$$\begin{array}{ccccc} & \bar{\bar{\varphi}}_\alpha & & \bar{\varphi} & & \bar{\bar{\varphi}}_{\alpha'} & \\ & \leftarrow & & \rightarrow & & \rightarrow & \\ F(\alpha) & \cong F[x]/(p(x)) & & \cong F'[x]/(p^*(x)) & & \cong F'(\alpha') & \\ \alpha & \longmapsto x + (p(x)) & & \mapsto x + (p^*(x)) & & \mapsto & \alpha' \end{array}$$

Note that $\psi(c_0 + c_1x + c_2x^2) = \varphi(c_0) + \varphi(c_1)x + \varphi(c_2)x^2$.
$c_0 + c_1\alpha + c_2\alpha^2 \mapsto c_0 + c_1x + c_2x^2 + (p(x)) \mapsto \varphi(c_0) + \varphi(c_1)x + \varphi(c_2)x^2 + (p^*(x)) \mapsto \varphi(c_0) + \varphi(c_1)\alpha' + \varphi(c_2)\alpha'^2$.
$\psi(\alpha) = \alpha'$
$\alpha \mapsto x + (p(x)) \mapsto x + (p^*(x)) \mapsto \alpha'$
And $\psi(c) = \varphi(c)$, where $c \in F$,
$c \mapsto c + (p(x)) \mapsto \varphi(c) + (p^*(x))) \mapsto \varphi(c) \in F'$.

So ψ extends φ and sends α to α'.

Question (4) If $f(x) \in F[x]$, E is a splitting field for $f(x)$ over F, α is a root of $f(x)$ in E, is E a splitting field for $f(x)$ over $F(\alpha)$?
(i.e. Is E the smallest splitting field over F?) Yes.

Proof:
Let $\alpha, \alpha_2, \ldots, \alpha_n$ be the roots of $f(x)$. Let $E = F(\alpha, \alpha_2, \ldots, \alpha_n)$.
A splitting field for $f(x)$ over $F(\alpha)$ is $F(\alpha)(\alpha, \alpha_2, \ldots, \alpha_n) = E$.

Theorem Let $f(x) \in F[x]$ where F is a field.

Let E be a splitting field for $f(x)$ over F.
Let $\varphi: F \to F'$ be an isomorphism, $\varphi^*: F[x] \to F'[x]$ be the map induced by φ.
Let E' be a splitting field for $f^*(x)$ over F'.
Then $\exists\ \Phi: E \to E'$ such that Φ extends φ and Φ is an isomorphism.

Proof:
Let $[E:F] = d$.
We will proceed by induction on d.

Suppose $d = 1$. Then $E = F$ (Lecture Notes 3/17/10).
Thus $f(x) = c(x - a_1)(x - a_2) \cdots (x - a_n) \in F[x]$.
Since, for each i, $\varphi^*(x - a_i)$ is irreducible in $F'[x]$ by Question (1),
for each i, $\varphi^*(x - a_i)$ is linear and
$f^*(x) = \varphi^*(c')\varphi^*(x - a_1)\varphi^*(x - a_2) \cdots \varphi^*(x - a_n)$ by homomorphic properties of φ^*, then $f^*(x)$ splits over F'. Thus $E' = F'$. Then $\Phi = \varphi$.

Assume $d > 1$, and the result holds for any splitting field of degree $< d$.
Since $[E:F] > 1$, then $E \neq F$, (Lecture Notes 3/17/10).
So $\exists\ \alpha \in E$ such that $\alpha \notin F$ and $f(\alpha) = 0$.
Let $p(x)$ be an irreducible factor of $f(x)$ such that $p(\alpha) = 0$.
Recall Lecture Notes 3/10/10, (If E/F is an extension, $a \in E$ where a is algebraic over F, $p(x)$ is an irreducible polynomial in $F[x]$ such that a is a root, deg $p(x) = n$, then $\cdots [F(a):F] = n$.)
$[F(\alpha):F] = \deg p(x) > 1$, since $\alpha \notin F$.
Let $\alpha' \in E'$ such that $p^*(\alpha') = 0$.
Then $F(\alpha) \cong F'(\alpha')$, by Question (2) above.
In particular, we have $\psi: F(\alpha) \to F'(\alpha')$ such that ψ extends φ by Question (3).
Since E is a splitting field for $f(x)$ over F, then E is a splitting field for $f(x)$ over $F(\alpha)$ by Question (4) above.
Similarly E' is a splitting field for f^* over $F'(\alpha')$.

> Note that we now have that
> E is a splitting field for $f(x)$ over $F(\alpha)$;
> $\psi: F(\alpha) \to F'(\alpha')$ is an isomorphism, $\psi^*: F(\alpha)[x] \to F'(\alpha')[x]$ is the map induced by ψ;
> and E' is a splitting field for $f^*(x)$ over $F'(\alpha')$.

Also since $d = [E:F] = [E:F(\alpha)][F(\alpha):F]$ and $[F(\alpha):F] > 1$, then $[E:F(\alpha)] < d$.
By our induction hypothesis, there is $\Phi: E \to E'$ an isomorphism that extends ψ.
However ψ extends φ. Thus Φ extends φ.

Corollary If E, E' are splitting fields for $f(x)$ over F then $E \cong E'$.

Proof:
Let E, E' be splitting fields for $f(x)$ over F.
Define $\varphi: F \to F$ by $\varphi(a) = a$.
And define $\varphi^*: F[x] \to F[x]$ by $\varphi^*(f(x)) = f(x)$.
Then by the theorem above, we have
$\exists\, \Phi: E \to E'$ such that Φ extends φ and Φ is an isomorphism.
Hence $E \cong E'$.

Corollary Any 2 fields of order p^n are isomorphic.

Proof:
Each of the fields must be a splitting field for $f(x) = x^{p^n} - x$ over $\mathbb{Z}_p$.
Hence, they're isomorphic.