Thm. For any p prime, $n \in \mathbb{N}$, if E, E' are two fields of order p^n, then $E \cong E'$.

Pf. Both E & E' contain an isomorphic copy of $\mathbb{Z}_p$. $\{0, 1, 1+1, \ldots, \underbrace{1+1+\cdots+1}_{p-1 \text{ times}}\} \cong \mathbb{Z}_p$.

Then E = splitting field of $x^{p^n} - x$ over this $\mathbb{Z}_p$.

$$E \cong \mathbb{Z}_p[x] / \langle f(x) \rangle$$

E^* generated by $\alpha \in E$, $f(x)$ min poly of α.

$\uparrow$ irreducible factor of $x^{p^n} - x$ of degree n that the generator of E^* satisfies.

Since $f(x)$ is a factor of $x^{p^n} - x$, and

E' = splitting field of $x^{p^n} - x$ over $(\mathbb{Z}_p)'$,

$\exists$ a root $\beta \in E'$ of $f(x)$, and so $f(x)$ is the min poly. of β over $(\mathbb{Z}_p)'$.

$$\Rightarrow (\mathbb{Z}_p)'[x] / \langle \underset{\deg n}{f(x)} \rangle \text{ is isomorphic to}$$

$(\mathbb{Z}_p')(\beta)$ = a subfield of E', but it's the same order (p^n) as E'. So $\mathbb{Z}_p'(\beta) = E'$. Thus $E' \cong [\mathbb{Z}_p)'[x] / \langle f(x) \rangle$

$$\cong \mathbb{Z}_p[x] / \langle f(x) \rangle \cong E.$$

$\boxed{\text{QED}}$

Explicitly the isomorphism $E \to E'$ maps $0 \mapsto 0'$, $1 \mapsto 1'$, $\alpha \mapsto \beta$ (and the rest follows).

Galois Theory.

Terminology: Let E be an algebraic extension of the field F. We say $\alpha, \beta \in E$ are conjugate over F if $\operatorname{irr}(\alpha, F) = \operatorname{irr}(\beta, F)$.

Thm. Let F be a field, and let α, β be alg. over F with $\deg(\alpha, F) = n$. The map $\psi_{\alpha,\beta} : F(\alpha) \to F(\beta)$ defined by

$$\psi_{\alpha,\beta}(c_0 + c_1\alpha + c_2\alpha^2 + \dots + c_{n-1}\alpha^{n-1}) =$$

$$c_0 + c_1\beta + c_2\beta^2 + \dots + c_{n-1}\beta^{n-1},$$

for each $c_i \in F$, is an isomorphism if and only if α & β are conjugate over F.

Proof: ($\Rightarrow$) If $\psi_{\alpha,\beta}$ is an isomorphism, then if $\operatorname{irr}(\alpha, F) = a_0 + a_1 x + \dots + a_n x^n$, then

$$\psi_{\alpha,\beta}(\underbrace{a_0 + a_1\alpha + \dots + a_n\alpha^n}_{=0}) = a_0 + a_1\beta + \dots + a_n\beta^n = 0$$

So β is also a root of $\operatorname{irr}(\alpha, F)$.

$\Rightarrow \operatorname{irr}(\beta, F) \mid \operatorname{irr}(\alpha, F)$. But since $\operatorname{irr}(\alpha, F)$ & $\operatorname{irr}(\beta, F)$ are monic and irreducible,

$\operatorname{irr}(\beta, F) = \operatorname{irr}(\alpha, F)$. ✓ (i.e. α, β are conjugate).

($\Leftarrow$) Suppose α, β are conjugate, i.e. $\underbrace{\operatorname{irr}(\alpha, F) = \operatorname{irr}(\beta, F)}_{= p(x)}$.

Then $\phi_\alpha : F[x] \to F(\alpha)$ has the same kernel $\langle p(x) \rangle$

as $\phi_\beta : F[x] \to F(\beta)$.

$$\Rightarrow F(\alpha) \cong F[x]/\langle p(x) \rangle \cong F(\beta).$$

We map $F[x]/\langle p(x) \rangle$ to $F(\alpha)$ by

$$f(x) + \langle p(x) \rangle \overset{\psi_\alpha}{\underset{\cong}{\longmapsto}} f(\alpha)$$

$$f(x) + \langle p(x) \rangle \overset{\psi_\beta}{\underset{\cong}{\longmapsto}} f(\beta)$$

$$\psi_\beta \circ \psi_\alpha^{-1} : F(\alpha) \to F(\beta)$$

$$f(\alpha) \underset{\cong}{\longmapsto} f(\beta)$$

This is exactly $\psi_{\alpha,\beta}$. $\blacksquare$

Corollary: If an isomorphism

$$\tau : F(\alpha)^{\subseteq \overline{F}} \to E^{\subseteq \overline{F}}$$ maps

F to F (ie, $\tau(a) = a \ \forall a \in F$), then

$\tau(\alpha)$ is a conjugate of α.

AND $\tau = \psi_{\alpha\beta}$, where $\beta = \tau(\alpha)$.

Corollary: Let $f(x) \in \mathbb{R}[x]$. If $f(a+bi) = 0$, then $f(a-bi) = 0$.

Pf: $\operatorname{irr}(i, \mathbb{R}) = \operatorname{irr}(-i, \mathbb{R}) = x^2+1$.

The Cor applies with $\tau : \mathbb{R}(i) \to \mathbb{R}(-i)$

$\tau(i) = -i$. ∎
