Finite Fields $\quad$ char $F = p \Rightarrow |F| = p^n$, $n = [F : \mathbb{F}_p]$

Then F is the spl. field of $x^{p^n} - x$

and consists of its roots.

Theorem $\forall$ prime p, $\forall n \in \mathbb{N}$, $\exists$ a field $\mathbb{F}_{p^n}$ of size p^n

and it's unique up to isomorphism

Proof Let F be the splitting field of $x^{p^n} - x$.

Let $L = \{\alpha \in F : \alpha^{p^n} = \alpha\} = \{\text{roots of } x^{p^n} - x\}$.

Claim L is a subfield of F.

If $\alpha, \beta \in L$ Then $(\alpha\beta)^{p^n} = \alpha^{p^n}\beta^{p^n} = \alpha\beta$

$$(\alpha+\beta)^{p^n} = \alpha^{p^n} + \beta^{p^n} = \alpha + \beta$$

$$(\alpha^{-1})^{p^n} = \alpha^{-1}.$$

$$L = \mathrm{Fix}(\Phi^n) = \{\alpha : \Phi^n(\alpha) = \alpha\}$$

where $\Phi(\alpha) = \alpha^p$ $\quad$ Frobenius endomorphism.

L contains all roots of the pol-l,

so $L = F$.

But $|L| = p^n$ since $(x^{p^n} - x)' = -1$ which has no roots so $x^{p^n} - x$ has no multiple roots.

So $|F| = p^n$.

Also, splitting fields are unique up to isomorphism, so $\mathbb{F}_{p^n}$ is unique up to isomorphism. $\square$

$\mathbb{F}_{p^n}^\times = \mathbb{F}_{p^n} \setminus \{0\}$ is cyclic, so $\exists\, \alpha$ s.t. $\{\alpha^k : k \in \mathbb{Z}\} = \mathbb{F}_{p^n}^\times$.

So $\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha)$, meaning $\mathbb{F}_{p^n}$ is a simple extn of $\mathbb{F}_p$.

So $\deg_{\mathbb{F}_p} \alpha = [\mathbb{F}_{p^n} : \mathbb{F}_p] = n$, so $\deg m_{\alpha, \mathbb{F}_p} = n$.

So $\exists$ an irreducible pol-l of degree n over $\mathbb{F}_p$.

$F = \mathbb{F}_{p^n}$ - subfields?

If $L \subseteq F$, Then $|L| = p^d$ for $d = [L : \mathbb{F}_p] \mid n$.

So $L = \mathbb{F}_{p^d}$ w/ $d \mid n$.

If $d \mid n$, Then $p^d - 1 \mid p^n - 1$

because $\dfrac{p^n-1}{p^d-1} = 1 + p^d + p^{2d} + \cdots + p^{(m-1)d}$ where $m = \frac{n}{d}$.

so $x^{p^d-1} - 1 \mid x^{p^n-1} - 1$ for the same reason

so $x^{p^d} - x \mid x^{p^n} - x$.

So the roots of $x^{p^d} - x$ are in $\mathbb{F}_{p^n}$.

So $\mathbb{F}_{p^d} \underset{\text{subfield}}{\subseteq} \mathbb{F}_{p^n}$

<u>Theorem</u> $\forall\, d \mid n$, $\exists$ a unique subfield of $\mathbb{F}_{p^n}$ isomorphic to $\mathbb{F}_{p^d}$, and $\mathbb{F}_{p^n}$ has no other subfields.

Diagram of Subfields of $\mathbb{F}_{p^n}$:

$$\begin{tikzcd}[arrows=dash]
 & \mathbb{F}_{p^n} \arrow[dl] \arrow[d] \arrow[dr] & \\
\mathbb{F}_{p^{d_1}} & \mathbb{F}_{p^{d_2}} & \mathbb{F}_{p^{d_3}}
\end{tikzcd}$$

$$
\begin{tikzcd}
\mathbb{F}_{p^{d_1}} & & \mathbb{F}_{p^{d_2}} & & \mathbb{F}_{p^{d_3}} \\
& \mathbb{F}_{p^{d_4}} \arrow[ul, dash] \arrow[ur, dash] & & \mathbb{F}_{p^{d_5}} \arrow[ul, dash] \arrow[ur, dash] & \\
& & \mathbb{F}_p \arrow[ul, dash] \arrow[ur, dash] & &
\end{tikzcd}
$$

Same as diagram of subgroups of $\mathbb{Z}_n$.

$$
\begin{tikzcd}
& & \mathbb{Z}_{36} \arrow[dl, dash] \arrow[dr, dash] & & \\
& \mathbb{Z}_{18} \arrow[dl, dash] \arrow[dr, dash] & & \mathbb{Z}_{12} \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{Z}_9 \arrow[dr, dash] & & \mathbb{Z}_6 \arrow[dl, dash] \arrow[dr, dash] & & \mathbb{Z}_4 \arrow[dl, dash] \\
& \mathbb{Z}_3 \arrow[dr, dash] & & \mathbb{Z}_2 \arrow[dl, dash] & \\
& & \mathbb{Z}_1 & &
\end{tikzcd}
\qquad
\begin{tikzcd}
& \mathbb{F}_{p^{36}} \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{F}_{p^{18}} & & \mathbb{F}_{p^{12}} \\
& \cdots &
\end{tikzcd}
$$

$x^{p^n} - x =$

each element $\cancel{x}^{0}$ of $\mathbb{F}_{p^n}$ is generating element of a subfield $\mathbb{F}_{p^d}$ with $d \mid n$.

So each irreducible factor of $x^{p^n} - x$ is the minimal pol-l of some such element, and has degree $d \mid n$.

If $d \mid n$ and f is an irreducible pol-l w/ degree d, then $\forall$ root α of f,

$[\mathbb{F}_p(\alpha) : \mathbb{F}_p] = d$ so $\mathbb{F}_p(\alpha) \subseteq \mathbb{F}_{p^n}$

so $f \mid x^{p^n} - x$.

So ↳ <u>Theorem</u> $\forall n$, $x^{p^n} - x = \prod_{d \mid n}$ all monic irreducible pol-ls over $\mathbb{F}_p$ of degree d

every such polynomial has exactly d roots.

$\forall d \mid n$, let $\psi(d) = \#$ of such pol-ls.

Then $p^n = \sum_{d \mid n} d\,\psi(d) = \underbrace{\sum_{\substack{d \mid n \\ d < n}} d\,\psi(d)}_{\text{can use}} + n\,\psi(n)$

can use to find $\psi(n)$ inductively.

<u>eg</u> $p=2$, $n=2$, $\mathbb{F}_4$. $\mathbb{F}_2$ is only subfield.

$4 = 2 + 2\psi(2)$, so $\psi(2) = 1$.

The irr. pol-l of degree 2 is $x^2 + x + 1$.

$$\mathbb{F}_4 = \mathbb{F}_2[x]/(x^2+x+1)$$

$$\mathbb{F}_4 = \{0, \underbrace{1, \alpha, \alpha+1}_{1, \alpha, \alpha^2 = \mathbb{F}_4^\times}\} \text{ with } \alpha^2 = -\alpha - 1 = \alpha + 1.$$

$p = 3$, $n = 2$

$9 = 3 + 2\psi(2)$ so $\psi(2) = 3$.

$x^2 \pm 1$, $x^2 \pm x \pm 1$.

$x^2 - 1 = (x+1)(x-1)$

$x^2 + 1$ is irr.

$x^2 + x + 1$ has 1 as a root

$x^2 - x + 1$ has -1 as a root

$x^2 + x - 1$ is irr.

$x^2 - x - 1$ is irr.

$$\mathbb{F}_9 = \mathbb{F}_3[x] / (x^2+1) = \mathbb{F}_3[x] / (x^2+x-1) = \mathbb{F}_3[x] / (x^2-x-1)$$