

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

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 .

$$\begin{aligned} \text{If } \alpha, \beta \in L \text{ Then } (\alpha\beta)^{p^n} &= \alpha^{p^n} \beta^{p^n} = \alpha\beta \\ (\alpha + \beta)^{p^n} &= \alpha^{p^n} + \beta^{p^n} = \alpha + \beta \\ (\alpha^{-1})^{p^n} &= \alpha^{-1} \end{aligned}$$

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

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

L contains all roots of the pol-1,
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.

$$\text{So } |F| = p^n.$$

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

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

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

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

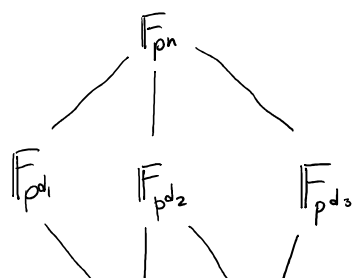
$$\text{so } x^{p^d} - x \mid x^{p^n} - x.$$

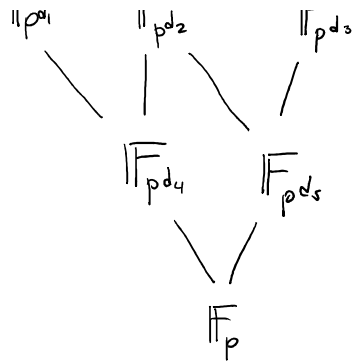
So the roots of $x^{p^d} - x$ are in \mathbb{F}_{p^n} .

$$\text{so } \mathbb{F}_{p^d} \overset{\text{subfield}}{\subseteq} \mathbb{F}_{p^n}$$

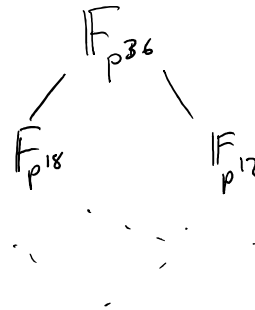
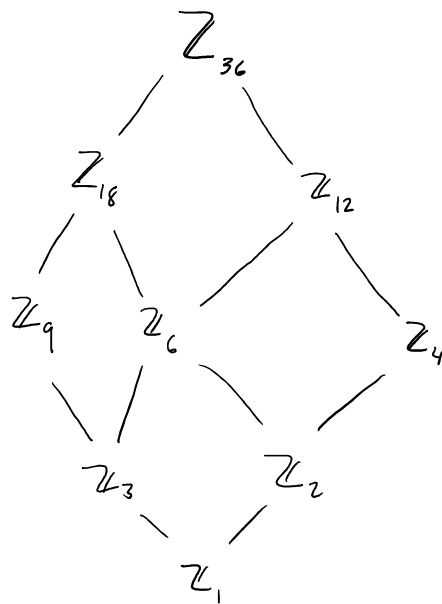
Theorem $\forall d \mid n$, \exists a unique subfield of \mathbb{F}_{p^n} isomorphic to \mathbb{F}_{p^d} , and \mathbb{F}_{p^n} has no other subfields.

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





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



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

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

So each irreducible factor of $x^{p^n} - x$ is the

minimal pol-1 of some such element,
and has degree $d \mid n$.

If $d \mid n$ and f is an irreducible pol-1

w/ degree d , then \forall root α of f ,

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

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

So

\hookrightarrow Theorem $\forall n$, $x^{p^n} - x = \prod_{d \mid n} \text{all } \overset{\text{monic}}{\text{irreducible pol-1s}} \overset{\text{over } \mathbb{F}_p}{\text{of degree } d}$

every such polynomial has exactly d roots.

$\forall d \mid n$, let $\psi(d) = \#$ of such pol-1s.

$$\text{Then } p^n = \sum_{d \mid n} d \psi(d) = \sum_{\substack{d \mid n \\ d < n}} d \psi(d) + n \psi(n)$$



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

eg

$p=2$, $n=2$, \mathbb{F}_4 . \mathbb{F}_2 is only subfield.

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

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

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

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

$\underbrace{\hspace{1.5cm}}_{\downarrow}$
 $1, \alpha, \alpha^2 = \mathbb{F}_4^\times$

$$p=3, \quad n=2$$

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

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

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

$$x^2 + 1 \text{ is irr.}$$

$$x^2 + x + 1 \text{ has } 1 \text{ as a root}$$

$$x^2 - x + 1 \text{ has } -1 \text{ as a root}$$

$$x^2 + x - 1 \text{ is irr.}$$

$$x^2 - x - 1 \text{ is irr.}$$

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