Thm Let E be an extension field of $\mathbb{Z}_p$ containing in some algebraic closure $\overline{\mathbb{Z}_p}$ of $\mathbb{Z}_p$, such that E has p^n elements.

Then $E = \{\text{zeros of } x^{p^n} - x \in \mathbb{Z}_p[x]\}$.

Pf. Let $E^* = \{\text{nonzero elts of } E\}$, which is a mult. group of $p^n - 1$ elements. $\Rightarrow \forall \alpha \in E^*$, $\text{order}(\alpha) \mid (p^n - 1) \Rightarrow$

$\alpha^{p^n-1} = 1 \in \mathbb{Z}_p. \Rightarrow \alpha(\alpha^{p^n-1} - 1) = 0 \Rightarrow \alpha^{p^n} - \alpha = 0.$

$\therefore E^* \subseteq \{\text{zeros of } x^{p^n} - x \in \mathbb{Z}_p[x]\}.$

Since $\left|\{\text{zeros of } x^{p^n} - x \in \mathbb{Z}_p[x]\}\right| \leq p^n$ $\Rightarrow E^* \cup \{0\} = E = \{\text{zeros of } x^{p^n} - x \text{ in } \mathbb{Z}_p[x]\}$.

$\blacksquare$

Defn: We say $x \in$ ring R is an $\underline{n^{th} \text{ root of unity}}$ $(n \in \mathbb{N})$ if $x^n = 1$. We say x is a $\underline{\text{primitive } n^{th} \text{ root of unity}}$ if $x^n = 1$ and $x^k \neq 1$ for $1 \leq k < n$.

Thm For every finite field F, $(F^*, \cdot)$ is cyclic.
[and thus any subgroup of F^* is cyclic.].

Proof: F^* is a finite abelian group, so by FTFGAG,

$$F^* \cong \mathbb{Z}_{p_1^{r_1}} \times \mathbb{Z}_{p_2^{r_2}} \times \cdots \times \mathbb{Z}_{p_k^{r_k}}$$

Let $m = \text{LCM of } \{p_i^{r_i}\}_{i=1}^{k} \Rightarrow \forall a \in F^*, \underline{a^m = 1}$.

But F^* has $p_1^{r_1} \cdot p_2^{r_2} \cdots p_k^{r_k}$ elements, and $m \leq p_1^{r_1} \cdots p_k^{r_k}$.

But There are at most m elements of F^* that satisfy $a^m - 1 = 0$

$\Rightarrow m \geq p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$

$\Rightarrow m = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k} \Rightarrow p_1, p_2, \ldots, p_k$ are distinct primes.

$\Rightarrow F^* \cong \mathbb{Z}_{p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}}$. ∎

[So if F is a finite field of p^n elements.
$(F^*, \cdot) \cong \mathbb{Z}_{p^n - 1}$. cyclic group of order $p^n - 1$.]

Cor. A finite extension of a finite field is a simple extension.

Proof: Let α be a generator of E^*, where $F \leq E$. (F: finite field)
Then $F(\alpha)$ contains all of E. ∎

[Note that this means $\alpha \in E \setminus F$.]

Lemma. Let F be a finite field of order p^n, with p prime, with algebraic closure $\overline{F}$. Then $x^{p^n} - x$ has p^n distinct zeros in $\overline{F}$.

Pf. Observe that $x^{p^n} - x$ splits (factors completely) over $\overline{F}$, so we just need to show the roots are distinct.

We check $f(x) = x^{p^n} - x$

$$\Rightarrow f'(x) = p^n x^{p^n - 1} - 1 = -1 \neq 0$$

$\therefore$ no multiple roots $\Rightarrow$ ∎

Lemma In a field F of characteristic p, $(\alpha + \beta)^{p^n} = \alpha^{p^n} + \beta^{p^n}$.

Pf: $$(\alpha + \beta)^{p^n} = \sum_{k=0}^{p^n} \binom{p^n}{k} \alpha^k \beta^{p^n - k} = \alpha^{p^n} + \beta^{p^n}.$$

all have factor of p except the first & last term. ∎

Thm For any prime p and any $n \in \mathbb{N}$, there exists a field of order p^n.

Pf. Let $F = \{\text{zeros of } x^{p^n} - x \text{ over } \mathbb{Z}_p\}$.
$\subseteq$ (splitting field of $x^{p^n} - x$).

We just need to check closure to show it is actually a field. Let $\alpha, \beta \in F$.

$$(\alpha+\beta)^{p^n} - (\alpha+\beta) = \alpha^{p^n} + \beta^{p^n} - \alpha - \beta = 0. \checkmark$$

$$\alpha^{p^n} - \alpha + \beta^{p^n} - \beta = 0 + 0 = 0.$$

closed under +

$$(\alpha-\beta)^{p^n} - (\alpha-\beta) = \begin{cases} \alpha^{p^n} - \beta^{p^n} - \alpha + \beta = 0 & \text{if } p \text{ is odd} \\ \alpha^{p^n} + \beta^{p^n} - \alpha + \beta = \alpha^{p^n} + \beta^{p^n} - \alpha - \beta = 0. & \text{if } p = 2 \end{cases}$$

$$(\alpha\beta)^{p^n} - \alpha\beta = \alpha^{p^n}\beta^{p^n} - \alpha\beta = \alpha\beta - \alpha\beta = 0. \checkmark$$

if $\beta \neq 0$

$$\left(\frac{\alpha}{\beta}\right)^{p^n} - \frac{\alpha}{\beta} = \frac{\alpha^{p^n}}{\beta^{p^n}} - \frac{\alpha}{\beta} = \frac{\alpha}{\beta} - \frac{\alpha}{\beta} = 0 \checkmark$$

$\therefore$ F is a field, and $|F| = p^n$. $\square$

Thm $\forall n \in \mathbb{N}$, p prime, a field F with $|F| = p^n$, $\forall k \geq 2$, $\exists$ irreducible polynomial in $F[x]$ of degree k.

Pf. F has p^n elements. $\exists$ a subfield $K \subseteq \overline{F}$ consisting of zeros of $x^{p^{kn}} - x$ — definitely a field, definitely $(p^n)^k$ elements.

We still need to check that $F \subseteq K$.

For $\alpha \in F$, α is a zero of $x^{p^n} - x$.

$$\Rightarrow \alpha^{p^{kn}} = \left(\underbrace{\alpha^{p^n}}_{\alpha}\right)^{p^{n(k-1)}} = \alpha^{p^{n(k-1)}} = \alpha^{p^{n(k-2)}} \cdots = \alpha$$

$\Rightarrow F \subseteq K$. Also $[K:F] = k$

K vector space over F has basis of k elements.

$K = \text{span}_F\{\beta_1, \dots, \beta_8\}$

$\Rightarrow |K| = |F|^8 = p^{n8} = p^{nk}$

$\Rightarrow 8 = k$

K is a simple extension

$K = F(\beta)$.

$\deg(\underbrace{\text{irr}(\beta, F)}_{\text{poly of deg } n \text{ that is irreducible}}) = k$ $\boxtimes$
