Theorem 22.1 (Classification of finite fields)

For each prime p and $n \in \mathbb{Z}^+$, $\exists!$ field E with $|E| = p^n$.

E is "the" splitting field of $x^{p^n} - x$ over $\mathbb{Z}_p$.

Existence $\quad f(x) = x^{p^n} - x \qquad f'(x) = -1$.

Thm 20.5 $\Rightarrow$ $f(x)$ has exactly p^n distinct zeros in E.

Exercise: the zeros of $f(x)$ form a field.

Consequently $E = \{\text{zeros of } f(x)\}$ and $|E| = p^n$.

Uniqueness $\quad$ Let K be a field, $|K| = p^n$.

The additive order of 1 divides p^n and is prime. (Thm 13.4)

Thus char $K = p$, and by Cor 1 of Thm 15.5, $\mathbb{Z}_p \approx \langle 1 \rangle \subseteq K$.

For $a \in K^*$, Lagrange's Theorem $\Rightarrow$ $|a| \mid p^n - 1$.

Therefore $\quad a^{p^n} = a^{p^n-1} \cdot a = 1 \cdot a = a$,

and a is a zero of $x^{p^n} - x$.

K contains p^n distinct zeros of $x^{p^n} - x$ and so is "the" splitting field of $x^{p^n} - x$ over $\langle 1 \rangle \approx \mathbb{Z}_p$. (Cor to Thm 20.4.)

We name $E = GF(p^n)$ "Galois Field"

Theorem 22.2 Let p be prime, $n \in \mathbb{Z}^+$.

$$(GF(p^n), +) \approx \underbrace{\mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p}_{n \text{ factors}}$$

$$(GF(p^n)^*, \cdot) \approx \mathbb{Z}_{p^n-1}.$$

Proof

Additive structure: $\mathrm{char}(GF(p^n)) = p \Rightarrow p \cdot a = 0 \ \forall a$.
Additive order of every element is 1 or p.
Only possibility in Thm. 11.1 is $\mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p$.

Multiplicative structure:

$(GF(p^n)^*, \cdot) \approx \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_k}$ (Ex. 11, Ch. 11)
where $n_{i+1} \mid n_i$ for all i.

Let $a = (a_1, a_2, \ldots, a_k) \in \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_k}$.

$n_1 \cdot a = 0$ in $\mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_k}$ (addition)
$a^{n_1} = 1$ in $GF(p^n)^*$ (multiplication)

Every $a \in GF(p^n)^*$ is a root of $x^{n_1} - 1$,
so $p^n - 1 \leq n_1$ by Cor. 3 of Thm 16.2.

$|\langle(1,0,\ldots,0)\rangle| = n_1$ divides $n_1 \cdot n_2 \cdot \cdots \cdot n_k = p^n - 1$,
and so $n_1 = p^n - 1$ and

$$GF(p^n)^* \approx \mathbb{Z}_{p^n-1}. \qquad \square$$

<u>Exercise</u> The basis of $GF(p^n)$ over $GF(p)$ has n elements, by considering the standard basis $\mathcal{B} = \{(1,0,\dots,0), \dots, (0,\dots,0,1)\} \subseteq \underbrace{\mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p}_{n \text{ times}}$.

<u>Corollary 1</u> $[GF(p^n) : GF(p)] = \dim_{GF(p)} GF(p^n)$

$$= \dim_{\mathbb{Z}_p} \underbrace{\mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p}_{n \text{ times}} = n.$$

<u>Corollary 2</u> Let a generate $GF(p^n)^*$.

Then

$$[GF(p)(a) : GF(p)] = [GF(p^n) : GF(p)] = n,$$

and a is algebraic of degree n over $GF(p)$.

Exercise Let p be prime, and $m, n \in \mathbb{Z}^+$. Assume $m \mid n$. Then

$$p^n - 1 = (p^m - 1)(\underbrace{p^{n-m} + p^{n-2m} + \cdots + p^m + 1}_{t})$$

Therefore $GF(p^n)^*$ has an element of order $p^m - 1$ (any generator to t^{th} power).

Exercise $K = \{x \in GF(p^n) \mid x^{p^m} = x\}$ is a subfield of $GF(p^n)$.

The subfield of order p^m is unique; otherwise $x^{p^m} - x$ has $> p^m$ zeros in $GF(p^n)$.

$m \mid n$ is required, since if F is a subfield of $GF(p^n)$,

$$[GF(p^n):GF(p)] \overset{\text{Cor 1 Thm 22.2}}{=} n \underset{\text{Thm 21.5}}{=} [GF(p^n):F]\underbrace{[F:GF(p)]}_{m}$$

and so $m = [F:GF(p)]$ divides n, and $|F| = p^m$.
(This page is Theorem 22.3.)