Algebraically closed → think $\mathbb{C}$

↕ can have transcendental elements

Algebraic closure → think $\overline{\mathbb{Q}} \neq \mathbb{C}$

↑ only alg. elements. ↑ algebraic closure of $\mathbb{Q}$

Prop If F is a finite field, $\text{char}(F) = p$ then $|F| = p^n$ for some $n \in \mathbb{N}$.

Proof: Define a ring hom by

$$\phi : \mathbb{Z} \to F$$
$$n \mapsto n \cdot 1$$

$\text{char}(F) = p \quad \therefore \quad \ker\phi = p\mathbb{Z}$

$$\phi(\mathbb{Z}) \cong \mathbb{Z}/p\mathbb{Z}$$

↑ subfield of F

Let $K = \phi(\mathbb{Z}) \subset F$, Since F is a finite feild $\Rightarrow$ finite extension of K $\therefore$ alg. extension of K

$[F : K] = n$ = dimension of F as a K vector space

$\therefore \exists\ \alpha_1, \ldots, \alpha_n \in F$ ← basis

s.t.
for any $\alpha \in F$

$$\alpha = a_1\alpha_1 + \cdots + a_n\alpha_n \quad , \; a_i \in K$$

and $|K| = p$

$\therefore$ $\exists$ p^n linear combinations of the a_i's

$\therefore |F| = p^n$. ∎

Lemma Let p be prime, D an integral domain
$\text{Char}(D) = p$. Then

$$a^{p^n} + b^{p^n} = (a+b)^{p^n} \qquad \forall n \in \mathbb{N}$$

Proof: induction and binomial formula

Def Let F be a field. $f(x) \in F[x]$, $\deg(f) = n$
is **separable** if it has n **distinct** roots
in the splitting field of $f(x)$
that is $f(x)$ factors into **distinct** linear factors
in its splitting field.

- An extension E of F is a **separable extension** of F if **every** element in E is a root of a **separable** polynomial in $F[x]$.

Ex) • x^2-2 is separable over $\mathbb{Q}$ since

$$x^2-2 = (x-\sqrt{2})(x+\sqrt{2})$$

$\mathbb{Q}(\sqrt{2})$ is infact a separable extension

$$\mathbb{Q}(\sqrt{2}) = \{ a+b\sqrt{2} \mid a,b \in \mathbb{Q} \} \quad \therefore \quad \alpha \in \mathbb{Q}(\sqrt{2})$$

$$\alpha = a+b\sqrt{2}$$

- $b=0 \Rightarrow$ α is a root of $x-a$, is separable
- $b \neq 0 \Rightarrow$ α is a root of

$$x^2 - 2ax + a^2 - 2b^2 = (x-(a+b\sqrt{2}))(x-(a-b\sqrt{2}))$$

$\uparrow$ separable

Let $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in F[x]$

Def) The <u>derivative</u> of $f(x)$ is

$$f'(x) = a_1 + 2a_2 x + \cdots + n a_n x^{n-1}$$

<u>Lemma</u> : $f(x)$ is separable iff

$$\gcd(f(x), f'(x)) = 1$$

Proof: write $f(x)$ in factored form in splitting field

take divivitive, compare.

Thm For every prime p, every $n \in \mathbb{N}$

$\exists$ a finite field F with p^n elements; any such F is isomorphic to the splitting field of $f(x) = x^{p^n} - x$ over $\mathbb{Z}_p$.

Proof (sketch):

Let F be the splitting field of $f(x) = x^{p^n} - x$

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

$\gcd(f(x), f'(x)) = 1 \quad \therefore$ f is a sepeable polynomial

$\therefore$ f has p^n distinct roots

I claim that the collection of roots form a field, and in fact are the splitting field of $x^{p^n} - x$.

■

Def:

Galois field of order p^n = the unique finite with p^n elements (splitting field of $x^{p^n} - x$ over $\mathbb{Z}_p$)

$\| \quad GF(p^n)$

Thm: Every sub field of $GF(p^n)$ has p^m elements when $m \mid n$. Conversly if $m \mid n$ $\exists$ a unique sub field of $GF(p^n)$ isomorphic to $GF(p^m)$.

Proof: (sketch)

F a sub field of $E = GF(p^n)$

$\Rightarrow$ F is an extension of $K \cong \mathbb{Z}_p$

$\Rightarrow$ F contain p^m elements for some $m \leq n$

$$[E : K] = [E : F][F : k]$$

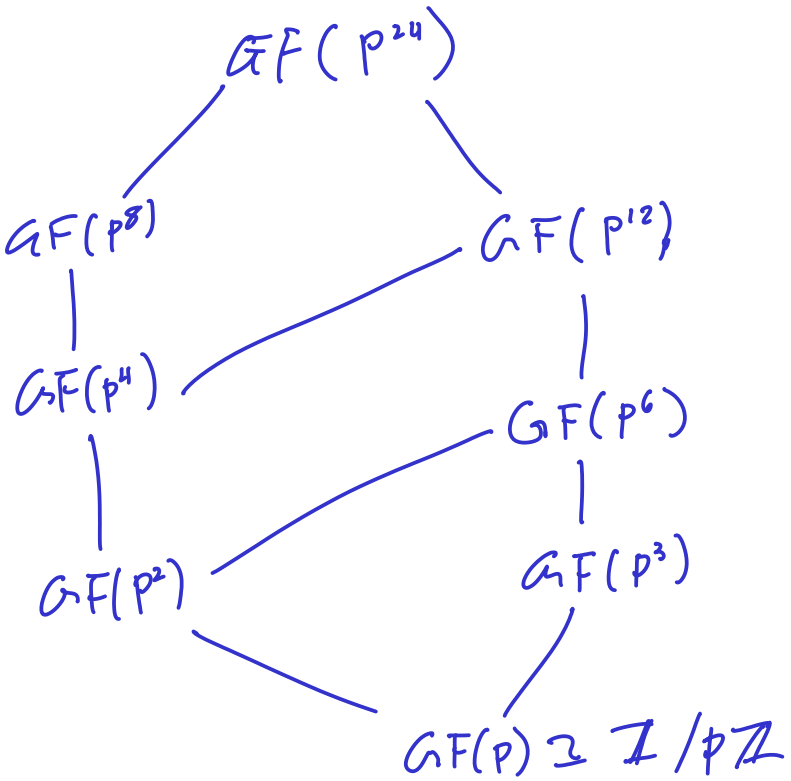
$$p^n = [E : F]\, p^m$$

$\Rightarrow$ $m \mid n$ since $[E : F]$ is an integer

Converse (Existence / Read)

$\blacksquare$

Ex) This lets us draw lattice pics



For each field F we have a multiplicative group of non-zero elements F^*.

- F^* is a cyclic group for F any finite field

Thm If G is a finite subgroup of F^* (for any F) then G is cyclic.

cor F^* is cyclic whenever F is a finite field

cor Every finite extension E of a finite field F is a simple extension.

Proof: Let α generates $E^* \Rightarrow E = F(\alpha)$. ∎