Recall

For any prime power $q = p^n$

$\exists$ a field $\mathbb{F}_q$ w/

- $\# \mathbb{F}_q = q = p^n$

- $\mathbb{F}_q$ contains a "copy" of $\mathbb{F}_p$ $\left(1_{\mathbb{F}_q}, 1+1, \ldots\right)$

$(\mathbb{F}_q, +, \cdot)$ is abelian gp $\Rightarrow$ $\forall x \in \mathbb{F}_q$: $\operatorname{ord}(x) \mid q = p^n$

$\operatorname{ord}(x) = p^k$ $\Rightarrow$ $p^k \cdot x = 0$

$x + x + x + \cdots + x$

$= (1 + \cdots + 1) \cdot x = 0$

$\Rightarrow \underbrace{1 + \cdots + 1}_{p^k}$

$\Rightarrow$ $\operatorname{char} \mathbb{F}_q = p$

alternatively, $\mathbb{F}_q$ is a splitting field of

$x^{p^n} - x$ over $\mathbb{F}_p$

so $\operatorname{char} \mathbb{F}_q = p$

Moreover up to iso (of fields) any field $\mathbb{F}$ w/ $\# \mathbb{F} = p^n$ has iso $\mathbb{F} \cong \mathbb{F}_q$.

($\mathbb{F}_p := \mathbb{Z}_p = \{0, \cdots, p-1\}$

but $\mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}_p$)

- For a subfield inclusion $\mathbb{F} \subseteq \mathbb{k}$ we say that $\mathbb{k}$ is an extension of $\mathbb{F}$

Want: Classify all finite field extensions, ie, given a finite field $\mathbb{F}_q$, what are the possible subfields $\mathbb{F} \subseteq \mathbb{F}_q$?

$$\mathbb{F}_p \subseteq \mathbb{F}_q$$

Lemma: If p is prime,

$p^m - 1 \mid p^n - 1 \iff m \mid n.$

Proof: observe that $\forall x$

$$(x-1)\left(x^{n-1} + \dots + x + 1\right)$$

$$= x^n + x^{n-1} + \dots + x$$

$$- x^{n-1} - \dots - x - 1$$

$$= x^n - 1$$

$$(*) \quad \boxed{x^n - 1 = (x-1)\left(x^{n-1} + \dots + x + 1\right)}$$

If $m \mid n$, say $n = mk$,

then $x = p^m$

$$p^n - 1 = \left(p^m\right)^k - 1 \Rightarrow$$

$$= \left(p^m - 1\right)\left(\sum_{j=0}^{k-1} \left(p^m\right)^j\right)$$

$$\Rightarrow \boxed{p^m - 1 \mid p^n - 1}.$$

Conversely, if $p^m - 1 \mid p^n - 1$

and write $n = mq + r$ $(0 \le r < m)$

then

$$R \ni \frac{p^n - 1}{p^m - 1} = \frac{p^{mq+r} - p^{mq} + p^{mq} - 1}{p^m - 1}$$

$$= \frac{p^{mq+r} - p^{mq}}{p^m - 1} + \underbrace{\frac{p^{mq} - 1}{p^m - 1}}_{t}$$

$$= p^{mq} \frac{p^r - 1}{p^m - 1} + t \in R.$$

Now $t \in R$ since $m \mid mq$

$$\Rightarrow p^{mq} \cdot \frac{p^r - 1}{p^m - 1} \in \mathbb{Z}$$

$$\Rightarrow p^m - 1 \mid p^r - 1 .$$

but $r < m$

So $r = 0 \Rightarrow m \mid n$. //

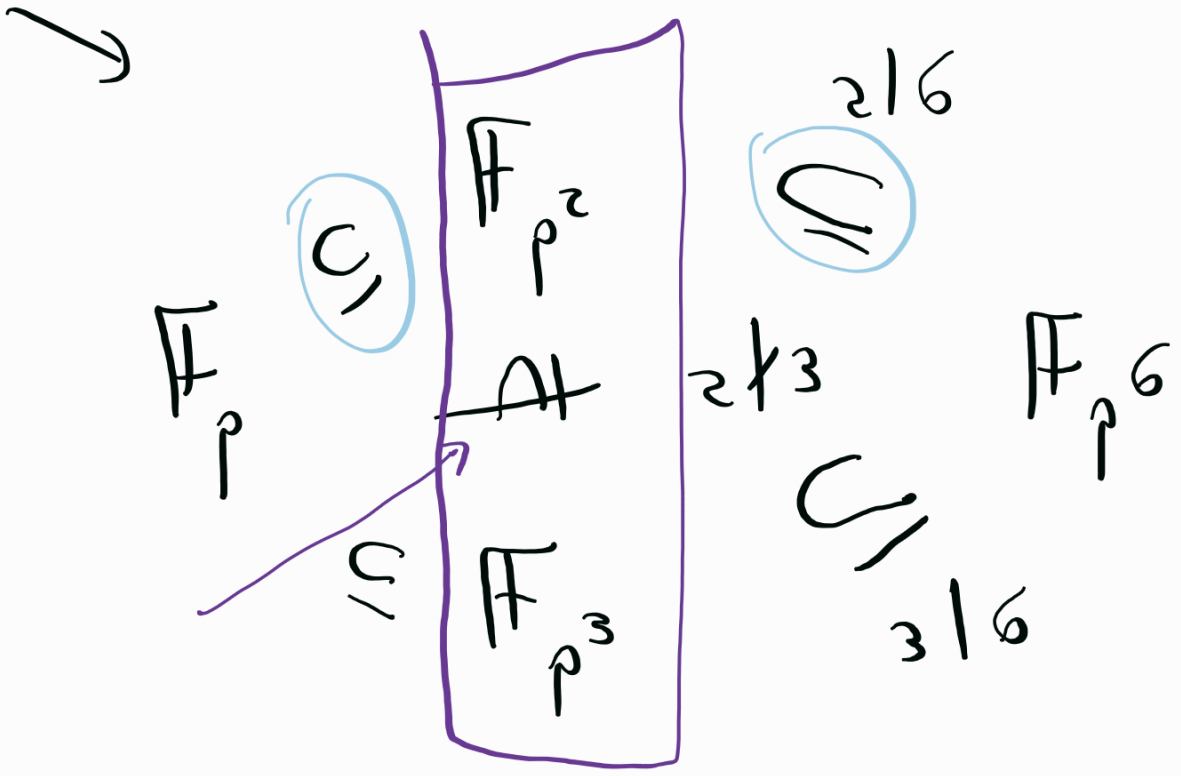
(classification of finite ext'n)

Thm: Let $q = p^n$ be a prime power. Then for every $m \mid n$ there is a unique subfield $\mathbb{F}$ of $\mathbb{F}_q$ w/

$$\# \mathbb{F} = p^m .$$

Moreover, every subfield of

$\mathbb{F}_q$ is of



Proof: Suppose $m \mid n$. The multiplicative gp $\mathbb{F}_q^\times$ is of order $q-1 = p^n - 1$.

By the lemma, $p^m - 1 \mid p^n - 1$.

By the converse Lagrange thm

$\exists$ a subgp $\mathbb{k}^\times \leq \mathbb{F}_q^\times$

$\#\mathbb{k}^\times = p^m - 1$

of order $\#\mathbb{K}^\times$.

Define $\mathbb{K} := \mathbb{K}^\times \cup \{0_{\mathbb{F}_q}\}$.

Observe that we can restrict addition and mult. in $\mathbb{F}_q$ to $\mathbb{K}$.

By Lagrange thm, every element in $\mathbb{K}^\times$ satisfies

$$\forall x \in \mathbb{K}^\times \quad x^{p^m - 1} = 1 \quad (\Leftrightarrow)$$

$$\forall x \in \mathbb{K} \quad x^{p^m} - x = 0 \quad (*)$$

If $a, b \in \mathbb{K}$. Then

$$(a+b)^{p^m} = a^{p^m} + b^{p^m}$$

$$= a + b$$

$$t^{p^m} = t$$

$\Rightarrow$ $a+b$ is a root of $x^{p^m} - x$ $\Rightarrow$

$a+b \in \mathbb{k}$.

Exercise $a \in \mathbb{k} \Rightarrow -a \in \mathbb{k}$

$\mathbb{k}$ is also closed under additive and mult. inverses.

To sum up, $\mathbb{k} \subseteq \mathbb{F}$ is a subfield of size p^m.

($m \mid n$).

If $\mathbb{F} \subseteq \mathbb{F}_q$ is a subfield.

Then by Lagrange $\#\mathbb{F} \mid \#\mathbb{F}_q = p^n$

so $\#\mathbb{F} = p^m$ for some m.

Now $\mathbb{F}^\times$ is (cyclic) of order $p^m - 1$ so the elements of $\mathbb{F}$ are precisely the roots of $x^{p^m} - x$ over $\mathbb{F}_q$.

Thus $\mathbb{F}$ is unique. //

$$\mathbb{F}_p = \mathbb{F}_{p^{1!}} \subseteq \mathbb{F}_{p^{2!}} \subseteq \mathbb{F}_{p^{3!}} \subseteq \cdots$$

$((n-1)! \mid n!)$

$q = p^d$

$$\mathbb{F}_q = \mathbb{F}_{q^{1!}} \subseteq \mathbb{F}_{q^{2!}} \subseteq \underline{\underline{\mathbb{F}_{q^{3!}}}} \subseteq \cdots$$

Def: The algebraic closure

A $\mathbb{F}_q$ is

$$\overline{\mathbb{F}}_q = \bigcup_{n=1}^{\infty} \mathbb{F}_{q^{n!}}$$

Proposition: $\overline{\mathbb{F}}_q$ is a field.

Proof: First $\mathbb{F}_p \subseteq \mathbb{F}_{q^{n!}}$ (subfield)

for any $n \Rightarrow \mathbb{F}_p \subseteq \overline{\mathbb{F}}_q$ (sets)

so we set $(0_{\overline{\mathbb{F}}_q}, 1_{\overline{\mathbb{F}}_q}) = (0_{\mathbb{F}_p}, 1_{\mathbb{F}_p})$

To define addition and multiplication, let $x, y \in \overline{\mathbb{F}}_q$.

Then $\exists\, n, k$ s.th $n \neq k$

$x \in \mathbb{F}_{q^{n!}}$, $y \in \mathbb{F}_{q^{k!}}$

$\subseteq$ subfield $\supseteq$

$\mathbb{F}_{q^{n!k!}}$

Clearly, if $x \in \bar{\mathbb{F}}_q$, say

$\ni x \in \mathbb{F}_{q^{n!}}$ then

$-x, x^{-1} \in \mathbb{F}_{q^{n!}} \Rightarrow -x, x^{-1} \in \bar{\mathbb{F}}_q$.

Associativity, commutativity and distributivity of $+, \cdot$ in $\bar{\mathbb{F}}_q$ follow from the corresponding axioms in each of the $\mathbb{F}_{q^{n!}}$

$$\Rightarrow \quad \overline{\mathbb{F}}_q = \bigcup_{n=1}^{\infty} \mathbb{F}_{q^{n!}}$$

is a field. //

char $\mathbb{F}$ is the min number s.th $1 + \dots + 1 = 0$

$$\mathbb{F}_p \subseteq \overline{\mathbb{F}}_q$$

$f(x) \in \mathbb{F}_p[x] \Rightarrow f \in \overline{\mathbb{F}}_p[x]$

Thm: Let $q = p^n$ be a prime power, and $f(x) \in \overline{\mathbb{F}}_q[x]$

Then f splits (to linear factors)

$$f(x) = a \cdot \prod_{i=1}^{n} (x - \alpha_i)$$

for $\alpha, \alpha_1, \ldots, \alpha_n \in \overline{\mathbb{F}}_q$.

Proof: f has finitely many coefficients, say $f(x) = \sum a_i x^i$

$a_0, a_1, \ldots, a_n \in \overline{\mathbb{F}}_q = \bigcup_{n=1}^{\infty} \mathbb{F}_{q^{n!}}$

$\Rightarrow \exists N$ s.th $\exists n(0)$: $a_0 \in \mathbb{F}_{q^{n(0)!}}$

$a_0, a_1, \ldots, a_n \in \mathbb{F}_{q^{N!}} \subseteq \overline{\mathbb{F}}_q$

ie $f(x) \in \mathbb{F}_{q^{N!}}[x]$.

a splitting field of f is $\mathbb{F}_{q^{N! \cdot d}}$ for

some d

but $\mathbb{F}_{q^{n!\,d}} \subseteq \mathbb{F}_{q^{n!}}$

is a subfield

$\Rightarrow$ f splits

in $\mathbb{F}_{q^{n!}}$ hence

also in $\overline{\mathbb{F}}_q$. //

$$\mathbb{F}_q \subseteq \mathbb{F}_{q^{2!}} \subseteq \dots \subseteq \mathbb{F}_{q^{n!}}$$

$$\mathbb{F}_{q^d} \subseteq \mathbb{F}_{q^{d!}}$$

$$\mathbb{F}_p[x]$$

$$\not\cong$$

$$\mathbb{F}_q[x]$$

→ Fundamental theorem of algebra: $\overline{\mathbb{R}} = \mathbb{C}$

Every polynomial $f \in \mathbb{C}[x]$ splits (to linear factors)

$$\mathbb{Q} \subseteq \overline{\mathbb{Q}} \subsetneq \mathbb{C}$$