Frobenius !

Power p operation.

In char_ p, defines a ring hom.

$(xy)^p = x^p \cdot y^p$ ✓

$(x+y)^p = x^p + y^p$ ← char p middle terms div by p.

$\mathbb{F}_p \xrightarrow{\varphi} \mathbb{F}_p$ identity.

$K \xrightarrow{\varphi} K$ finite field

K of size p^n.

φ inj (hom between fields)

surj (same size)

$\mathbb{F}_p[t] \xrightarrow{\varphi} \mathbb{F}_p[t]$

$t \longmapsto t^p$

K size p^n $\qquad$ $\varphi: K \to K$

$x^{p^n} = x$ for all $x \in K$.

$\iff \underbrace{\varphi \circ \varphi \circ \varphi \circ \cdots \circ \varphi}_{n \text{ times}} = \varphi^n$ is the identity on K.

e.g. $K = \mathbb{F}_5[t]/(t^3+t+1)$

Roots of x^3+x+1 in K.

t is a root

$$\begin{tikzcd} & t \arrow[dr] & \\ t^{25} \arrow[ur] & & t^5 \arrow[ll] \end{tikzcd}$$

Prop: n is the smallest pos. number s.t.

$\varphi^n = id$ on K.

Pf: Suppose $\varphi^m = id$, $m > 0$ $\qquad$ $x^{p^m} = x$ for all $x \in K$.

$\hookrightarrow$ p^n roots

$\Rightarrow p^m \geq p^n \Rightarrow m \geq n$.

$\square$.

Rem If a generator is fixed by a hom

$\Rightarrow$ the field is fixed.

(all elts of the field are fixed).

Ex. $K = \mathbb{F}_p[t]/(t^3+t+1)$ $t \mapsto t$

$\to$ everything $\mapsto$ itself.

$$\begin{array}{ccccc} K & \supset & L & \supset & \mathbb{F}_p \\ p^n & & p^m & & p^1 \\ \circlearrowright & & \circlearrowright & & \circlearrowright \end{array}$$

φ^n fixes everything here

φ^m fixes everything here

φ^1 fixes ---

$K = \mathbb{F}_p[t] / \text{irr deg } 6.$

t ⇝ all 6 roots
$+$ Frob ✓.

diff poly of deg 6.
irr. ↳ root gen. field of deg 6 ⇒ generates whole fields.
⇒ only 6^{th} power of Frob is back to itself

irred.
poly of deg 3.
↳ root. α look at $\mathbb{F}_p[\alpha] \subset K$.

$$\begin{array}{c} \mathbb{F}_p[\alpha] \\ \cup \; 3. \\ \mathbb{F}_p \end{array}$$

$\alpha, \varphi(\alpha), \varphi^2(\alpha)$ distinct & roots of your cubic.

—.

$K = \mathbb{F}_p[x] / $ irred. deg 6.

Does K contain roots of quadratic or cubics ?

$\Longleftrightarrow$ Does K contain subfields of size p^2 & p^3 ?

Prop: ~~If $m|n$ then~~

Let K be a field of size p^n.

If $m|n$, then K contains a subfield of size p^m.

& there is a unique such.

If $m \nmid n$ then K does not . . . . . .

Pf: Suppose m divides n. $\varphi = \text{Frob}$.

Consider $L = \{ \alpha \in K \text{ s.t. } \varphi^m(\alpha) = \alpha \}$.

L is a subfield. ✓ φ^m is a homomorphism.

A subfield of size p^m must be contained in L.

$$L = \{ \alpha \in K \mid \underbrace{\varphi^m(\alpha) = \alpha}_{} \}.$$ wish has size p^m.

$$\alpha^{p^m} = \alpha$$

so L has at most p^m elts. these are the roots of $X^{p^m} - X$ in K.

(Obs: $\not\exists$ If $m \mid n$ then $X^{p^m} - X$ divides $X^{p^n} - X$.)

p^m roots. $\Leftarrow$ $X^{p^m} - X$ also has distinct lin factors $\Leftarrow$ has p^n distinct factors over K

Converse: $K \supset L \supset \mathbb{F}_p$ ~~$\deg(K/L) = d$, say.~~

$$\underbrace{\overset{p^n}{K} \supset \underbrace{\overset{p^m}{L} \supset \overset{p}{\mathbb{F}_p}}_{m}}_{n} \Rightarrow m \mid n.$$