

Frobenius!

Power p operation.

In char p , defines a ring hom.

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

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

K of size p^n .

φ inj (hom between fields)
surj (same size)

$$(xy)^p = x^p \cdot y^p \quad \checkmark$$

$$(x+y)^p = x^p + y^p \quad \leftarrow \text{char } p$$

middle terms
div by p .

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

$t \mapsto t^p$

K size p^n

$$\varphi: K \rightarrow K$$

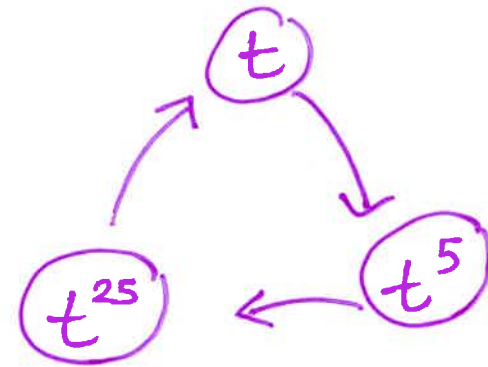
$$x^{p^n} = x \quad \text{for all } x \in K.$$

$$\Leftrightarrow \underbrace{\varphi \circ \varphi \circ \varphi \dots \circ \varphi}_{n \text{ times}} = \text{id} \quad \text{is the identity on } K.$$

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

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

t is a root



Prop: n is the smallest pos. number st.

$$\varphi^n = \text{id} \quad \text{on } K.$$

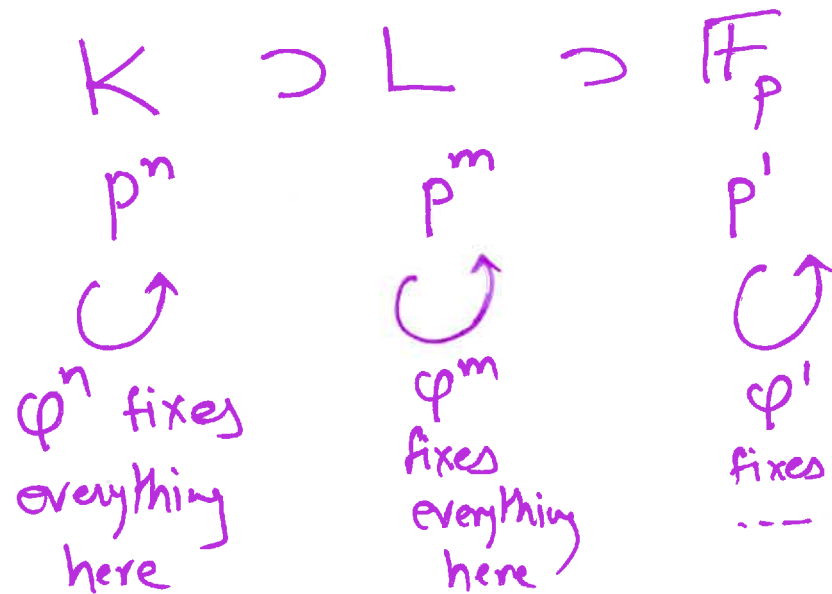
Pf: Suppose $\varphi^m = \text{id}$, $m > 0$ $x^{p^m} = x$ for all $x \in K$.

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

$\square.$

Rem If a generator is fixed by a hom
 \Rightarrow the field is fixed.
(all elts of the field are fixed).

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



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

$t \mapsto$ all 6 roots
+ Frob ✓.

diff poly of deg 6.

irr. \hookrightarrow root gen. field of deg 6 \Rightarrow generates whole fields

\Rightarrow only 6th power of Frob is back to itself.

irred.
poly of deg 3.

\hookrightarrow root. α look at $\mathbb{F}_p[\alpha] \subset K.$
 \cup 3.
 \mathbb{F}_p

$\alpha, \varphi(\alpha), \varphi^2(\alpha)$

distinct
& roots of
your cubic.

—.

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

Does K contain roots of quadratic or cubics?

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

Prop: ~~If $m \mid n$ then~~

Let K be a field of size p^n .

$\left\{ \begin{array}{l} \text{If } m \mid n, \text{ then } K \text{ contains a subfield of size } p^m \\ \text{ \& there is a unique such.} \end{array} \right.$

If $m \nmid n$ then K does not

Pf: Suppose m divides n .

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

$\varphi = \text{Frob.}$

L is a subfield. \checkmark φ^m is a homomorphism.

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

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

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

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

(Obs: ~~*~~ 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.~~
 $\underbrace{p^n}_{n} \supset \underbrace{p^m}_m \supset p$
 $\Rightarrow m \mid n.$