

Finite fields!

K a finite field.

Then $|K| = p^n$

$p = \text{char}(K)$

$\overbrace{\mathbb{F}_p}^n \subset K$

$K \cong \mathbb{F}_p[t] / f(t)$ $f(t)$ irred in $\mathbb{F}_p[t]$ deg n .

Conversely $\mathbb{F}_p[t] / f(t)$

— " —

gives a finite field
of size p^n .

K^\times is cyclic of order $p^n - 1$.

$$\alpha \in K^\times \Rightarrow \alpha^{p^n - 1} = 1$$

$$\forall \alpha \in K \Rightarrow \alpha^{p^n} = \alpha$$

α satisfies $X^{p^n} - X = 0$

$$\text{so } X^{p^n} - X = \prod_{\alpha \in K} (X - \alpha)$$

in $K[X]$.

$$K = \mathbb{F}_p[t] / f(t)$$

$f(t)$ irr. deg n .

$\alpha = t \in K$ satisfies a poly in $\mathbb{F}_p[x]$
min poly of α is $f(x)$

also satisfies $X^{p^n} - X = 0$.

$\Rightarrow f(x)$ divides $X^{p^n} - X$.

* Any irred poly in $\mathbb{F}_p[x]$ of deg n divides $X^{p^n} - X$.

Let K be any finite field of size p^n .

$$\text{In } K[x], \quad X^{p^n} - X = \prod_{\alpha \in K} (X - \alpha)$$

distinct
in linear
factors!

so how would $f(x)$ factor in $K[x]$?

$f(x)$ irred of deg n in $\mathbb{F}_p[x]$

Let K be any finite field of $\underbrace{\deg n \text{ over } \mathbb{F}_p}_{\text{size } p^n}$

(e.g. $K = \mathbb{F}_p[t]/f(t)$)

Then all irr. poly in $\mathbb{F}_p[x]$ of $\deg n$ factor
in distinct linear factors over K .

Prop: Any two finite fields of size p^n are isomorphic.

Pf: K, L finite fields of size p^n .

Know $K \cong \mathbb{F}_p[t]/f(t)$, want to find iso
ring hom.

$$\begin{array}{c} K \rightarrow L \\ \parallel \\ \mathbb{F}_p[t]/f(t) \end{array}$$

Ring hom $\mathbb{F}_p[t] / f(t) \xrightarrow{\varphi} L \leftarrow$

Step 0: $\mathbb{F}_p \longrightarrow L$ unique.

Step 1: $\mathbb{F}_p[t] \xrightarrow{\quad} L$ unique after choosing $t \mapsto \alpha \in L$

Step 2: $\mathbb{F}_p[t] / f(t) \xrightarrow{\quad} L$ exists iff $f(\alpha) = 0$.

~~For φ to exist~~ To construct φ we must
send t to a root of ~~$f(t)$~~ $f(x)$ in L .

we know that $f(x)$ must
have n roots in $L \Rightarrow n$ possible ring homs φ .

Ring hom aut. inj (fields) \Rightarrow aut. bij (same size).

□

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

In $K[x]$ let's factor ~~$t^3 + t + 1$~~ $x^3 + x + 1.$

$$(x^3 + x + 1) = (x - t) (\quad) (\quad)$$

Frobenius! \leftarrow operation of raising to p^{th} power.

R $\text{char } R = p.$

$$\varphi(0) = 0 \quad \varphi(1) = 1$$

$$\varphi(xy) = \varphi(x) \cdot \varphi(y)$$

$$\varphi(x+y) = \varphi(x) + \varphi(y)$$

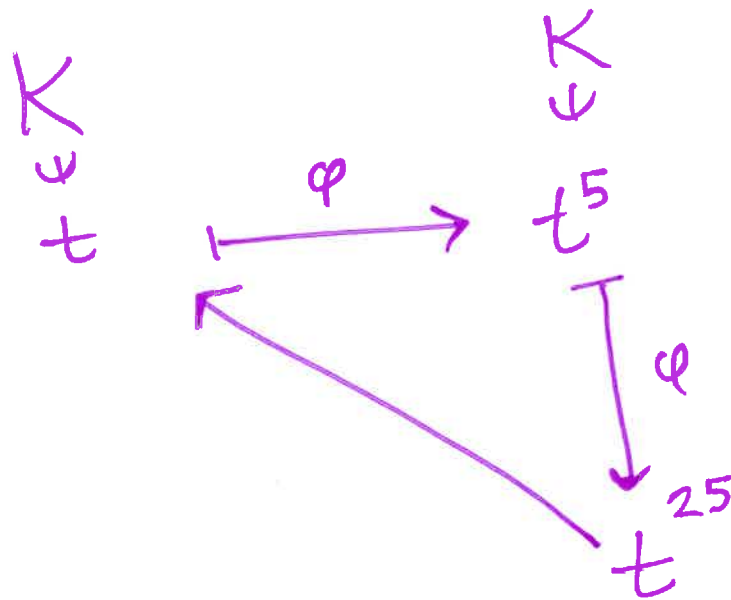
ring hom.

$$\varphi: \begin{matrix} R & \longrightarrow & R \\ \wr & & \wr \\ x & \longmapsto & x^p \end{matrix}$$

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

has Frobenius
 $\varphi: K \rightarrow K$.

$$\mathbb{F}_5 \ni \varphi = \text{id}$$



$$t^3 + t + 1 = 0$$

$$\varphi(t^3 + t + 1) = 0$$

$$\varphi(t)^3 + \varphi(t) + 1 = 0$$