Finite fields!

K a finite field.

Then $|K| = p^n$ $\quad p = \mathrm{char}(K)$. $\quad \overbrace{\mathbb{F}_p \subset K}^{n}$

$K \cong \mathbb{F}_p[t]/f(t)$ $\quad f(t)$ 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 $p^n - 1$.

$\alpha \in K^\times \Rightarrow \alpha^{p^n-1} = 1$ $\quad \alpha$ satisfies $X^{p^n} - X = 0$

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

in $K[X]$.

$K = \mathbb{F}_p[t] / f(t)$ $\quad$ $f(t)$ irr. deg n.

$\alpha = t \in K$ $\quad$ 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 $x^{p^n} - x$.

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

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

In $K[x]$, $\quad x^{p^n} - x = \prod_{\alpha \in K} (x - \alpha)$ $\quad$ 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 $\underbrace{\text{deg } n \text{ over } \mathbb{F}_p}_{\text{size } p^n}$.

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

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

<u>Prop</u>: Any two finite fields of size p^n are isomorphic.

<u>Pf</u>: K, L finite fields of size p^n.

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

ring hom.

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

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

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

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

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

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

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

Ring hom aut. inj (fields) & aut. bij (same size).

$\square$

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

In $K[x]$ let's factor $\cancel{t^3+t+1}$ x^3+x+1.

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

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

R $\quad$ char $R = p$.

$$\begin{array}{ccc} R & \longrightarrow & R \\ \rotatebox{90}{$\in$} & & \rotatebox{90}{$\in$} \\ \varphi : x & \longmapsto & x^p \end{array}$$

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

$$\underbrace{\begin{gathered}\varphi(xy) = \varphi(x)\cdot\varphi(y) \\ \varphi(x+y) = \varphi(x) + \varphi(y)\end{gathered}}_{\text{ring hom.}}$$

$K = \mathbb{F}_5[t] \big/ (t^3+t+1)$ has Frobenius $\varphi : K \to K$.

$\mathbb{F}_5 \circlearrowleft \varphi = \mathrm{id}$

$$\begin{tikzcd} K \arrow[d, phantom, "\rotatebox{90}{$\in$}"] & & K \arrow[d, phantom, "\rotatebox{90}{$\in$}"] \\ t \arrow[rr, mapsto, "\varphi"] & & t^5 \arrow[d, mapsto, "\varphi"] \\ & & t^{25} \arrow[ull] \end{tikzcd}$$

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

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

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