FINITE FIELDS

(1) Let K be a finite field. | Let $p = \mathrm{Char}(K)$ prime number.

Want : $|K| = p^n$.

R any ring. $\exists!$ ring hom

$\mathbb{Z} \to R$ $\quad$ $\mathbb{Z}/n\mathbb{Z} \hookrightarrow R$

$\mathrm{Ker} = n\mathbb{Z}$, $n \geq 0$. $\quad$ $n =$ Char. of R.

If R domain $\Rightarrow$ n prime. or $n = 0$.

K finite field $p = \mathrm{Char}(K)$

$$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \hookrightarrow K$$

So K is an extension of $\mathbb{F}_p$

finite ext^n because K is finite.

Let $n = \deg_{\mathbb{F}_p} K \Rightarrow |K| = p^n$.

$\deg_{\mathbb{F}_p}(K)$.

Char K

$\square$

Next. $K \cong \mathbb{F}_p[t]/(f(t))$ for some irred. $f(t) \in \mathbb{F}_p[t]$.

Need: There exists $\alpha \in K$ such that

$K = \mathbb{F}_p[\alpha]$. $\leftarrow$ smallest sub ring of K containing $\mathbb{F}_p$ & α

($\mathbb{F}_p[t] \to K$ $\quad t \mapsto \alpha$

eval at $t = \alpha$

surj. & $f(t)$ is gen of kernel.)

[~~Let's prove that $\mathbb{F}_p^\times = \mathbb{F}_p - \{0\}$ under $\times$ is a cyclic group.~~

~~(If α generates $\mathbb{F}_p^\times$, then $\mathbb{F}_p^\times = \{1, \alpha, \alpha^2, \alpha^3, \dots\}$~~]

Let $K^\times = K - \{0\}$ K our fin field size p^n

<u>Claim</u>: $K^\times$ is a cyclic gp under $\times$.

α generator $\Rightarrow K^\times = \{1, \alpha, \alpha^2, \ldots, \alpha^{p^n-2}\}$

$\Rightarrow K = \mathbb{F}_p[\alpha]$.

<u>Pf</u> of <u>Claim</u> :- Remember every finite abelian gp (Algebra 1) is iso. to a product of cyclic gps

$$\cong C_{d_1} \times C_{d_2} \times \cdots \times C_{d_k} \quad \text{where}$$

$$d_1 \mid d_2 \mid \cdots \mid d_k.$$

Size $= d_1 \cdot d_2 \cdot \cdots \cdot d_k$ & every elt g in the gp satisfies $g^{d_k} = 1$

Suppose $K^{\times} \cong \underbrace{C_{d_1} \times \cdots \times C_{d_k}}$

Then $|K^{\times}| = d_1 d_2 \cdots d_k$

& every $x \in K^{\times}$ satisfies $X^{d_k} - 1 = 0$

poly of deg d_k

Has at most d_k distinct roots $\Leftarrow$ poly of deg d_k

We already see $d_1 \cdot d_2 \cdot \cdots \cdot d_k$ roots $\leftarrow$ elts of $K^{\times}$!

$\Rightarrow \quad d_1 \cdot d_2 \cdots d_k = d_k \Rightarrow d_1 = d_2 = \cdots = d_{k-1} = 1$

---

deg n poly $\Rightarrow$ at most n roots

$\uparrow$ <u>any field</u>

α root $\Rightarrow$ $(X - \alpha)$ factor. $\leftarrow$ div. with remainder.

$\square$

K finite field $\Rightarrow$ K size p^n

& $\exists\ \alpha \in K^\times$ that generates $K^\times$ multiplicatively

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

min poly of α.

$$x^{p^n-1} - 1 = 0$$

$$x^{p^n} - x = \prod_{a \in K} (x - a) \quad \text{in } K[x].$$

$\Rightarrow$ $f(t)$ divides $\cancel{x^{p^n} - x}$ $t^{p^n} - t$ in $\mathbb{F}_p[t]$.