Note Title

$\mathbb{F}_2[x]$, $\mathbb{F}_3[x]$

$\mathbb{F}_4$: finite field with 4 elements

$$\mathbb{F}_4 = \{0, 1, \alpha, 1+\alpha\} \quad \alpha^2 = \alpha + 1$$

$1+1=0$ $+$: mod 2

'α' : indeterminate

$$F_9 = \{0, 1, 2, \alpha, 2\alpha, \alpha+1, \alpha+2, 2\alpha+1, 2\alpha+2\}$$

$1,\ 1+1=2,\ 1+1+1=0$

$$\alpha^2+1=0$$

Finite field F : ?

$\{0, 1$

$1,\ 1+1,\ 1+1+1,\ \ldots\ldots$ has to repeat

'p': called characteristic of F

$\exists$ minimum 'p' s.t.

$$\underbrace{1+1+\cdots+1}_{(p \text{ times})} = 0 \text{ in } F.$$

Fact: Characteristic of a finite field is prime.

Pf: Suppose $p = rs$

$$0 = \underbrace{1 + 1 + \cdots + 1}_{p \text{ times}} = \underbrace{(1+1+\cdots+1)}_{r \text{ times}}\underbrace{(1+1+\cdots+1)}_{s \text{ times}}$$

$\downarrow$

get a contradiction

QED

F contains $\{\underbrace{0, 1, 2, \ldots, p-1}, \ldots\}$

Fact:

$\{0, 1, 2, \ldots, p-1\} \subseteq F$ is isomorphic to $\mathbb{Z}_p$.

$p = 7$

$$\underbrace{(1+1+1)(1+1+1+1)}_{\text{in } F} \longleftrightarrow \overbrace{3 \cdot 4 \bmod 7}^{\text{in } \mathbb{Z}_7}$$

$$= 5$$

$$\updownarrow$$

$1+1+1+1+1$ in F

Fact: F is a finite-dimensional vector space over $\{0, 1, 2, \ldots, p-1\} \leftrightarrow \mathbb{Z}_p$

Pf: easy. check the axioms

m: dim of F over $\mathbb{Z}_p$

$$\Rightarrow \boxed{|F| = p^m}$$

Basis of F over $\mathbb{Z}_p$: $\{\alpha_1, \alpha_2, \ldots\ldots, \alpha_m\}$

$$F = \{ a_1\alpha_1 + a_2\alpha_2 + \cdots + a_m\alpha_m : a_i \in \mathbb{Z}_p \}$$

→ addition : easy

→ multiplication : ?

Construction of $\mathbb{F}_{p^m}$:

$\mathbb{Z}_p[x]$

$\updownarrow$

$\pi(x)$: irreducible, degree-m in $\mathbb{F}_p[x]$

↓

(Such a poly exists)

$$F_{p^m} = \{ a_0 + a_1\alpha + \dots + a_{m-1}\alpha^{m-1} : a_i \in \mathbb{Z}_p, \underbrace{\pi(\alpha) = 0}_{\alpha^m \text{ : in terms of } 1, \alpha, \dots, \alpha^{m-1}} \}$$

'α': indeterminate

<u>Pf:</u> $+, \times$: modulo $\pi(\alpha)$

$a(\alpha), b(\alpha) \in F_{p^m}$ $\quad a(\alpha) \times b(\alpha)$ in F_{p^m} $= a(\alpha) b(\alpha) \bmod \pi(\alpha)$

$\longrightarrow$ same proof as for $\mathbb{Z}_p$