Lecture 9

Note Title 1/18/2008

$F[x]$: set of polys with coeffs from a field F

Division: $a(x) = q(x)b(x) + r(x)$, $\deg r(x) < \deg b(x)$

If $r(x) = 0$, $b(x) \mid a(x)$

($b(x)$ divides $a(x)$)

Ex: $a(x) = x^2 + 2x + 1 \in F_5[x]$

$= 2(3x^2 + x + 3)$ → trivial factorization

$= (x+1)(x+1)$

Finding linear factors of $a(x) \in F[x]$:

$a(\alpha) = 0$ for $\alpha \in F$ iff $(x - \alpha) \mid a(x)$.

Ex: 1) $x^2+1 \in F_2[x]$

$(x+1) \mid (x^2+1)$

$x^2+1 = (x+1)^2$ in $F_2[x]$

2) $x^2+1 \in F_3[x]$

↳ irreducible in $F_3[x]$

3) $x^2+x+1 \in F_2[x]$ $\quad$ $x^2+x+1 \in F_3[x]$

↳ irreducible $\quad$ ↳ $(x-1)^2$

4) $x^3+x+1 \in F_2[x]$ $\quad$ $x^4+x+1 \in F_2[x]$

↳ irreducible $\quad$ ↳ irreducible

⟶ For every $m \in \mathbb{N}$, there is at least one irreducible poly of degree m in $F_p[x]$, p: prime.

Construction of Finite fields:

→ Algebra, Michael Artin

We have seen F_p, p: prime

Suppose F_q exists for some q: finite

$0, 1 \in F_q$

$1+1 \in F_q$ $1+1+1 \in F_q$

$n = \overbrace{1+1+\cdots+1}^{n \text{ times}} \in F_q$

Since q: finite, $\exists$ smallest $n \in \mathbb{N}$ s.t.

$n = 0$ in F_q.

→ This smallest $n \in \mathbb{N}$ has to be prime.

Pf: $n = ab$ in $\mathbb{N}$ $\Rightarrow$ $n = ab$ in F_q

$0 = ab$

$\Rightarrow a = 0$ or $b = 0$ ✗

Characteristic of F_q: Smallest prime p for which $\underbrace{1+1+\cdots+1}_{p \text{ times}} = 0$ in F_q.

$$F_p = \{0, 1, 2, 3, \ldots, p-1\} \subseteq F_q.$$

p: prime

$\longrightarrow$ $F_p \subseteq F_q$ is actually the finite field F_p

$\longrightarrow$ F_q : vector space over F_p.

$\longrightarrow$ $a, b \in F_q$ $\quad a+b \in F_q$

addition in F_q $\Rightarrow$ call it vector addition

$a \in F_p$, $b \in F_q$ $\quad a \cdot b \in F_q$

mult. in F_q $\Rightarrow$ call it scalar mult.

→ F_q: finite-Dimensional vector space over F_p.

Suppose dimension $= m$.

$\Rightarrow \exists$ a basis $\{b_1, b_2, \ldots, b_m\}$ for F_q over F_p. ($b_i \in F_q$)

Arbitrary $\alpha \in F_q$ can be written as

$$\alpha = a_1 b_1 + a_2 b_2 + \cdots + a_m b_m$$

$$a_i \in F_p.$$

$$\Rightarrow q = p^m$$

Addition in F_q: $\alpha_1, \alpha_2 \in F_q$

$$\alpha_1 = a_{11} b_1 + a_{12} b_2 + \cdots + a_{1m} b_m$$

$$\alpha_2 = a_{21} b_1 + a_{22} b_2 + \cdots + a_{2m} b_m$$

$$\alpha_1 + \alpha_2 = (a_{11} + a_{21}) b_1 + \cdots + (a_{1m} + a_{2m}) b_m$$

Ex: $F_{16} = \{0000, 0001, 0010, 0011, \ldots$

$\ldots, 1111\}$

$0011 + 1111 = 1100$

$\longrightarrow$ F_q exists $\Rightarrow q = p^m$, p: characteristic

Construction of F_q, $q = p^m$, p: prime

$F_q = \{ a(x) \in F_p[x] : \deg a(x) \leq m-1 \}$ can be made into a field.

Addition: poly addition

$\pi(x)$: irreducible in $F_p[x]$, degree $= m$

Multiplication: poly. mult. mod $\pi(x)$

$\rightarrow$ Same proof as in F_p