Lecture 8

Note Title 1/17/2008

Finite fields:

Group: A set G with one binary operation $+$ $(+ : G \times G \to G)$ is a group if

(1) $+$ is associative

(2) There exists an element $0 \in G$ s.t. $a + 0 = a \quad \forall\, a \in G$. ($0$: identity)

(3) For every $a \in G$ $\exists\, -a \in G$ s.t. $a + (-a) = 0$

Commutative group $\Rightarrow$ $a + b = b + a \quad \forall\, a, b \in G$ (Abelian)

'$+$' : additive notation

$\to n \in \mathbb{N} \quad a \in G$

$$a + a + \cdots + a = na$$

(n times)

Ex: $Z_n = \{0, 1, 2, \ldots, n-1\}$ $+, \cdot \bmod n$

Z_n: group w.r.t. $+$

$Z_n \setminus \{0\} = Z_n^*$: group w.r.t. $\cdot$ (if n is prime

$\rightarrow Z_4^* = \{1, 2, 3\}$: Not a group w.r.t. $\cdot$

$3 \cdot 3 \bmod 4 = 1$ (2 has no inverse)

$3 = -1$

In general, Z_n^* : $a \mid n$ will not have an inverse.

$Z_p^* = \{1, 2, \ldots, p-1\}$ p: prime

Consider $a \cdot 1, a \cdot 2, a \cdot 3, \ldots, a \cdot (p-1) \bmod p$

$a \cdot i \neq a \cdot j \bmod p$

$\Rightarrow \exists\ k$ s.t. $a \cdot k = 1 \bmod p$.

Ex: $Z_5 = \{0, 1, 2, 3, 4\}$ $+, \cdot \bmod 5$

$Z_5^* = \{1, 2, 3, 4\}$ $1^{-1} = 1$, $2^{-1} = 3$, $3^{-1} = 2$, $4^{-1} = 4$

$2, 2^2 = 4, 2^3 = 3, 2^4 = 1, \ldots$

$3, 3^2 = 4, 3^3 = 2, 3^4 = 1, \ldots$

$4, 4^2 = 1, \ldots$

$Z_5 = \{0, 1, 2, 3, 4\}, +$

$-1 = 4, -2 = 3, -3 = 2, -4 = 1$

$1, 2 \cdot 1 = 2, 3 \cdot 1 = 3, 4 \cdot 1 = 4, 5 \cdot 1 = 0, \ldots$

$2, 2 \cdot 2 = 4, 3 \cdot 2 = 1, 4 \cdot 2 = 3, 5 \cdot 2 = 0, \ldots$

Order: G, $\cdot$

Defn: $a \in G$ $\quad \mathrm{ord}_G(a)$: smallest $n \in \mathbb{N}$ s.t. $a^n = 1 \in G$.

G: finite $\Rightarrow$ $\mathrm{ord}_G(a) \mid |G|$ for any $a \in G$.

Corollary: $a^{|G|} = 1$

Pf: $\mathrm{ord}_G(a) \mid |G| \Rightarrow a^{|G|} = a^{k(\mathrm{ord}_G(a))}$

$= \left(a^{\mathrm{ord}_G(a)}\right)^k = 1$

Ex: $\mathbb{Z}_p^* = \{1, 2, \ldots, p-1\}$ $\quad |\mathbb{Z}_p^*| = p-1$

$a \in \mathbb{Z}_p^*$ $\quad a^{p-1} = 1 \mod p$

Fields: A set F with two binary operations $+, \cdot$ is said to be a field if

(1) $(F, +)$: Abelian group (0 : additive identity)

(2) $(F^*, \cdot)$: Abelian group ($F^* = F \setminus \{0\}$)

(3) $a \cdot (b+c) = a \cdot b + a \cdot c \quad \forall a, b, c \in F$.

↳ distributive laws.

1 : multiplicative identity in F^*.

$\longrightarrow \quad 0 \cdot a = 0$

Finite fields: Field F with $|F|$ finite

Ex: 1) $F_5 = \{0, 1, 2, 3, 4\}$ $+, \cdot \bmod 5$

2) $F_p = \{0, 1, 2, \ldots, p-1\}$ $+, \cdot \bmod p$

3) $F_2 = \{0, 1\}$ $+, \cdot \bmod 2$

→ Can we find all finite fields?

Polynomials over a Field F:

$$a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \in F[x]$$

$a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$: polynomial

$a_i \in F$

$F[x]$: set of all polys over F.

+ over $F[x]$: easy
• over $F[x]$: extends from regular poly multiplication

Division:

$a(x), b(x) \in F[x]$

Divide $a(x)$ by $b(x)$ $\Rightarrow$? Find $q(x), r(x) \in F[x]$ s.t.

$$a(x) = q(x)b(x) + r(x)$$

$$\deg r(x) < \deg b(x)$$

$b(x) \overline{)\, a(x)}$ — !

—— ?

Ex: $F_5[x]$

$a(x) = x^4 + 2x^2 + x + 1$

$b(x) = x^2 + x + 1$

$$x^2+x+1 \;\overline{)\; x^4 + 2x^2 + x + 1 \;}\; x^2 + 4x + 2$$

$$x^4 + x^3 + x^2$$

$$4x^3 + x^2 + x + 1$$

$$4x^3 + 4x^2 + 4x$$

$$2x^2 + 2x + 1$$

$$2x^2 + 2x + 2$$

$$4$$

$a(x) = (x^2 + 4x + 2)\,b(x) + 4$