Discrete Mathematics
Lecture 8

Liangfeng Zhang
School of Information Science and Technology
ShanghaiTech University

Field

DEFINITION: A **field** is a set $\mathbb{F}$ together with two binary operations $+$ and $\cdot$ such that:

- $\mathbb{F}$ is an abelian group with respect to the operation $+$;
- $\mathbb{F} \setminus \{0\}$ is an abelian group with respect to the operation $\cdot$;
- **Distributivity**: For all $a, b, c \in \mathbb{F}$, $a \cdot (b + c) = ab + ac$.

REMARK: additive identity 0; multiplicative identity: 1

EXAMPLE: $(\mathbb{R}, +, \cdot)$ is a field.

EXAMPLE: Let p be a prime. Then $(\mathbb{Z}_p, +, \cdot)$ is a field.

- $+$ is the addition of residue classes modulo p
- $\cdot$ is the multiplication of residue classes modulo p

Finite field: a field that contains finitely many elements.

Polynomials over $\mathbb{Z}_p$

DEFINITION: A **polynomial** of degree t over the finite field $\mathbb{Z}_p$ is a function of the form $f(X) = f_t X^t + \cdots + f_1 X + f_0$, where $f_0, f_1, \dots, f_t \in \mathbb{Z}_p$ and $f_t \neq 0$.

- $\deg(f(X))$: the **degree** of the polynomial $f(X)$
- $\mathbb{Z}_p[X] = \{f_t X^t + \cdots + f_1 X + f_0 : t \geq 0, f_0, \dots, f_t \in \mathbb{Z}_p\}$: the set of all polynomials over the finite field $\mathbb{Z}_p$

THEOREM: Let $f(X) = f_t X^t + \cdots + f_1 X + f_0 \in \mathbb{Z}_p[X]$ and $\alpha \in \mathbb{Z}_p$. Then there exists $q(X) = q_{t-1} X^{t-1} + q_{t-2} X^{t-2} + \cdots + q_0 \in \mathbb{Z}_p[X]$ such that $f(X) = (X - \alpha) q(X) + f(\alpha)$.

- $q_{t-1} = f_t$
- $q_{t-2} = f_{t-1} + f_t \alpha$
- $\vdots$
- $q_0 = f_1 + f_2 \alpha + \cdots + f_t \cdot \alpha^{t-2}$

Polynomials over $\mathbb{Z}_p$

EXAMPLE: If $f(X) = f_3X^3 + f_2X^2 + f_1X + f_0 \in \mathbb{Z}_p[X]$ and $\alpha \in \mathbb{Z}_p$, then $f(X) = (X - \alpha)Q(X) + f(\alpha)$ for

$$Q(X) = f_3X^2 + (f_2 + f_3\alpha)X + (f_1 + f_2\alpha + f_3\alpha^2).$$

DEFINITION: A field element $\alpha \in \mathbb{Z}_p$ is said to be a **root** of a polynomial $f(X) \in \mathbb{Z}_p[X]$ if $f(\alpha) = 0$.

EXAMPLE: $p = 11, f(X) = X^3 + 4X^2 + 3X + 3$.

- $\alpha = 1$ is a root of $f(X)$ as $f(1) = 1^3 + 4 \cdot 1^2 + 3 \cdot 1 + 3 = 0$
- $\alpha = 2$ is a root of $f(X)$ as $f(2) = 0$
- $\alpha = 4$ is a root of $f(X)$ as $f(4) = 0$
  - A polynomial of degree 3 has at most 3 roots.

Polynomials over $\mathbb{Z}_p$

THEOREM: A polynomial $f(X) \in \mathbb{Z}_p[X]$ has $\leq \deg(f)$ roots in $\mathbb{Z}_p$.

- Mathematical induction on $t = \deg(f(X))$
- $t = 0$: $f(X) = f_0$ ($f_0 \neq 0$) has 0 root
- $t = 1$: $f(X) = f_0 + f_1 X$ ($f_1 \neq 0$) has exactly 1 root in $\mathbb{Z}_p$
  - The root is $\alpha_1 = -f_1^{-1} \cdot f_0$
- Assume that the statement is true for $t < i$
- For $t = i$
  - $f(X)$ has 0 root: done
  - $f(X)$ has ≥ 1 roots in $\mathbb{Z}_p$
    - $\exists \alpha \in \mathbb{Z}_p$ such that $f(\alpha) = 0$
    - $f(X) = (X - \alpha)q(X) + f(\alpha) = (X - \alpha)q(X)$
      - $\deg\big(q(X)\big) = i - 1 < i$: $q(X)$ has $\leq i - 1$ roots in $\mathbb{Z}_p$
    - $(f(\beta) = 0) \wedge (\beta \neq \alpha) \Rightarrow q(\beta) = 0$
      - Except α, every root of $f(X)$ must be a root of $q(X)$
    - $f(X)$ has $\leq 1 + (i - 1) = i$ roots in $\mathbb{Z}_p$.

Order

DEFINITION: The **order** of a group G is the cardinality of G.

- $|\mathbb{Z}_n| = n, |\mathbb{Z}_p^*| = p - 1, |\mathbb{Z}| = \infty$

DEFINITION: when $|G| < \infty$, $\forall a \in G$, the **order** of a is the least integer $l > 0$ such that $a^l = 1$ ($la = 0$ for additive group)

EXAMPLE: Determine the orders of all elements of $\mathbb{Z}_7^*$ and $\mathbb{Z}_6$

- $\mathbb{Z}_7^* = \{1,2,3,4,5,6\}; o(1) = 1; o(2) = o(4) = 3; o(3) = o(5) = 6; o(6) = 2$
- $\mathbb{Z}_6 = \{0,1,2,3,4,5\};\ o(0) = 1, o(1) = o(5) = 6, o(2) = o(4) = 3, o(3) = 2$

THEOREM: Let G be a multiplicative Abelian group of order m. Then for any $a \in G$, $a^m = 1$.

- $G = \{a_1, \dots, a_m\}$
- If $i \neq j$, then $aa_i \neq aa_j$.
- $aa_1 \cdot aa_2 \cdots aa_m = a_1 a_2 \cdots a_m$
- $a^m = 1$

Subgroup

DEFINITION: Let $(G,\star)$ be an Abelian group. A subset $H \subseteq G$ is called a **subgroup** of G if $(H,\star)$ is also a group. $(H \leq G)$

- Multiplicative: $G = \mathbb{Z}_6^* = \{1,5\}, H = \{1\}$
- Additive: $G = \mathbb{Z}_6 = \{0,1,2,3,4,5\}; H = \{0,2,4\}$

THEOREM: Let $(G,\cdot)$ be an Abelian group. Let $\langle g \rangle = \{g^k : k \in \mathbb{Z}\}$ be a subset of G, where $g \in G$. Then $\langle g \rangle \leq G$.

- Closure: $g^a \cdot g^b = g^{a+b} \in \langle g \rangle$
- Associative: $g^a \cdot (g^b \cdot g^c) = g^{a+b+c} = (g^a \cdot g^b) \cdot g^c$
- Identity element: $g^0 \cdot g^a = g^a \cdot g^0 = g^a$
- Inverse: $g^a \cdot g^{-a} = g^{-a} \cdot g^a = g^0$
- Communicative: $g^a \cdot g^b = g^{a+b} = g^{b+a} = g^b \cdot g^a$

Cyclic Group

DEFINITION: Let $(G,\cdot)$ be an Abelian group. G is said to be **cyclic** if there exists $g \in G$ such that $G = \langle g \rangle$.

- g is called a **generator** of G.

EXAMPLE: $\mathbb{Z}_{10}^* = \{[1]_{10}, [3]_{10}, [7]_{10}, [9]_{10}\} = \langle [3]_{10} \rangle$

- $g = [3]_{10}$
- $g^0 = [1]_{10}, g^1 = [3]_{10}, g^2 = [9]_{10}, g^3 = [27]_{10} = [7]_{10}$

REMARK: Let G be a finite group and let $g \in G$. Then $\langle g \rangle$ can be computed as $\{g^1, g^2, \dots\}$

- If $G = \langle g \rangle$ is a cyclic group of order m, then

$$G = \{g^0, g^1, \dots, g^{m-1}\} = \{g^1, \dots., g^{m-1}, g^m\}.$$

THEOREM: For any prime p, the group $\mathbb{Z}_p^*$ is a cyclic group.

- proof omitted (beyond the scope of the course)

Cyclic Group

EXAMPLE: $\mathbb{Z}_p^*$ is a cyclic group and $G = \langle g \rangle$ is a cyclic subgroup.

- $p =$179769313486231590772930519078902473361797697894230657273430081157732675805500963132708477322407536021120113879871393357658789768814416622492847430639474124377767893424865485276302219601246094119453082952085005768838150682342462881473913110540827237163350510684586298239947245938479716304835356329624227998859
  - p is a prime; $\alpha = 2$
  - $\mathbb{Z}_p^* = \langle \alpha \rangle = \{\alpha^0, \alpha^1, \ldots, \alpha^{p-2}\} = \{\alpha^1, \ldots, \alpha^{p-2}, \alpha^{p-1}\}$ is a cyclic group of order $p - 1$
- $q =$89884656743115795386465259539451236680898848947115328636715040578866337902750481566354238661203768010560056939935696678829394884407208311246423715319737062188883946712432742638151109800623047059726541476042502884419075341171231440736956555270413618581675255342293149119973622969239858152417678164812113999429
  - $q = (p-1)/2$ is a prime; $g = \alpha^2 = 4$
  - $G = \langle g \rangle = \{g^0, g^1, \ldots, g^{q-1}\} = \{\alpha^0, \alpha^2, \ldots, \alpha^{2q-2}\} = \{\alpha^2, \ldots, \alpha^{2q-2}, \alpha^{2q}\}$ is a subgroup of $\mathbb{Z}_p^*$ of order q