Groups 群

- $\mathbb{Z}$ under addition
  $\mathbb{Z} \setminus \{0\}$ under multiplication
  $\mathbb{Q}$ under addition
  $\mathbb{Q} \setminus \{0\}$ under multiplication
  $\mathbb{R}$ under addition
  $\mathbb{R} \setminus \{0\}$ under multiplication
  $\{0,1\}^*$ under concantenation
  $\{0,1\}^n$ under bitwise XOR
  2×2 real matrices under addition
  2×2 invertible, real matrices under multiplication

- A *group* is a set G and a binary operation $\circ$ defined on G such that:
  - (*Closure*) For all $g, h \in G$, $g \circ h$ is in G
  - (*Identity*) There is a unique element $e \in G$ such that $e \circ g = g$ for all $g \in G$
  - (*Inverse*) Every element $g \in G$ has an *inverse* $h \in G$ such that $g \circ h = e$
  - (*Associativity*) For all $f, g, h \in G$, $f \circ (g \circ h) = (f \circ g) \circ h$
- A *group* is called *abelian* if the further property holds.
  - (*Commutativity*) For all $g, g \in G$, $g \circ h = h \circ g$

阿贝尔群满足交换律

- The *order* of a finite group G is # of elements in G.

有限群G的order是G的元素个数$m=|G|$，且对$g\in G$，有$g^m=1$

- The group operation can be written *additively* or *multiplicatively*
  - I.e., instead of $g \circ h$, write $g + h$ or gh
  - Does *not* mean that the group operation corresponds to (integer) addition or multiplication
- Identity denoted by 0 or 1, respectively
- Inverse of g denoted by $-g$ or g^{-1}, respectively
- Group *exponentiation*: $m \cdot a$ or a^m, respectively

g的逆元g^{-1}是唯一的.

Example

- $\mathbb{Z}_N = \{0, 1, \ldots, N-1\}$ under addition modulo n
  - *Identity* is 0
  - *Inverse* of a is $-a$ mod N
  - *Associativity*, *commutativity* obvious
  - *Order* N
- What happens if we consider *multiplication* modulo N?
- $\mathbb{Z}_N$ is *not* a group under this operation!
  - 0 has no inverse
  - Even if we exclude 0, there is, e.g., *no* inverse of 2 modulo 4

- Consider instead the *invertible* elements modulo N, under multiplication modulo N
- $\mathbb{Z}_N^* = \{0 < x < N : \gcd(x, N) = 1\}$
  - *Closure*
  - *Identity* is 1
  - *Inverse* of a is a^{-1} mod N
  - *Associativity*, *commutativity* obvious
- If p is prime, then $\mathbb{Z}_p^* = \{1, 2, \ldots, p-1\}$
  - $\mathbb{Z}_p$ is a (prime) *field*

$\gcd(x,N)=1 \Rightarrow 1 = sx + tN \Rightarrow sx = 1 - tN$

$\Rightarrow sx \equiv 1 \pmod N$

只有当$\gcd(x,N)=1$时，$s=x^{-1}$才存在.

若G是群，set $H \subseteq G$ 是G的子群，当H在G的operation下也满足closure、identity、inverse、associativity.

每个群G都有子群{1}和G、平格子群H为$H \neq G$.

Permutation Group 排列群

- Let $s_n = < 1, 2, \ldots, n >$ denote a *sequence* of integers 1 through n. Denote by P_n the set of all *permutations* of the sequence s_n.

  For example, $s_3 = < 1, 2, 3 >$
  $P_3 = \{< 1,2,3 >, < 1,3,2 >, < 2,1,3 >, < 2,3,1 >, < 3,1,2 >, < 3,2,1 >\}$

- Define a binary operation $\circ$ on the elements of P_n: for $\rho, \pi \in P_n$, $\pi \circ \rho$ denotes a *re-permutation* of the elements of ρ according to the elements of π.

- Consider $s_3 = < 1, 2, 3 >$, and $P_3 = \{< p_1, p_2, p_3 > | p_1, p_2, p_3 \in s_3 \text{ with } p_1 \neq p_2 \neq p_3\}$.
- $\pi = < 3, 2, 1 >$, $\rho = < 1, 3, 2 >$, what is $\pi \circ \rho$?

  $\pi \circ \rho = < 2, 3, 1 > \in P_3$
- We can verify the other three properties.

  $\rho_1 \circ (\rho_2 \circ \rho_3) = (\rho_1 \circ \rho_2) \circ \rho_3$

  $< 1, 2, 3 > \circ \rho = \rho \circ < 1, 2, 3 > = \rho$

  For each $\rho \in P_3$, there exists another unique $\pi \in P_3$ such that

  $\rho \circ \pi = \pi \circ \rho = < 1, 2, 3 >$

$(P_n, \circ)$ is called a *permutation group*.
$(P_n, \circ)$ is not abelian.

$\pi = <3, 2, 1>$
$\rho = <1, 3, 2>$
$\pi \circ \rho = <2, 3, 1>$

排列群不是阿贝尔群

Group Z_N, Z_N^*

$Z_N \overset{def}{=} \{0, 1, 2, \ldots N-1\}$

$Z_N^* \overset{def}{=} \{b \in \{1, \ldots, N-1\} \mid gcd(b, N) = 1\}$

欧拉函数 $\varphi(N) = |Z_N^*|$

①若 $N = p$ 为质数，则 $\varphi(N) = \varphi(p) = p-1$

②若 $N = pq$ 为两质数之积，

对 $a \in \{1, \ldots, N-1\}$ 且 $gcd(a, N) \neq 1$，则必有 $p | a$ 或 $q | a$.

$\{1, \ldots, N-1\}$ 中能被 p 整除的恰有 $(q-1)$ 个：$p, 2p, 3p, \ldots, (q-1)p$

能被 q 整除的恰有 $(p-1)$ 个：$q, 2q, 3q, \ldots, (p-1)q$

则不能被 p、q 整除的个数有：

$(N-1) - (p-1) - (q-1) = pq - p - q + 1 = (p-1)(q-1)$

即 $\varphi(N) = (p-1)(q-1)$

③若 $N = \prod_i p_i^{e_i}$，$\{p_i\}$ 是不同质数且 $e_i \geq 1$，则 $\varphi(N) = \prod_i p_i^{e_i - 1}(p_i - 1)$

Ring 环

- If $(R, +)$ is an *abelian group*, we define one more operation (denoted as *multiplication* $\times$ for convenience) to have a *ring* $(R, +, \times)$ satisfying the following properties.

  Closure: R must be closed w.r.t. $\times$

  Associativity: $(a \times b) \times c = a \times (b \times c)$

  Distributivity: $a \times (b + c) = a \times b + a \times c$
  $(a + b) \times c = a \times c + b \times c$

Example:
$(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, $(\mathbb{M}_{n\times n}, +, \cdot)$?

环一定是阿贝尔群

环增加了乘法闭包、结合律、分配律

Commutative Ring, Integral Domain

- A *ring* is *commutative* if the multiplication operation is *commutative* for all elements in the ring. $(ab = ba)$

- An *integral domain* $(R, +, \times)$ is a *commutative ring* that satisfies the following two additional properties.

  Identity element for multiplication: $a1 = 1a = a$
  Nonzero product for any two nonzero elements:
  if $ab = 0$, then either a or b must be 0.

Example:
$(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$? yes
$(\mathbb{Z}_m, +, \times)$, $(\mathbb{M}_{n\times n}, +, \cdot)$? not integral domain

交换环需对乘法操作满足交换律.

整环在交换环基础上增加了单位元与Nonzero product

Group → Ring → Integral Domain → Field

Field 域

- A *field*, denoted by $(F, +, \times)$, is an *integral domain* whose elements satisfy the following additional property.

  Inverse for multiplication: For every $a \in F$, there exists an element b, denoted by a^{-1}, such that $ab = ba = 1$.
- **Example**:
  $(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$? No
  $(\mathbb{Z}_p, +, \times)$? Yes
- If $\mathbb{F}$ is finite, $\mathbb{F}$ is called a *finite field*.
- $\mathbb{F}_q = \mathbb{Z}_p = \{0, 1, \dots, p-1\}$ with the operations *addition*, *multiplication* of integers modulo p, is called a *prime field*
  - The properties can be verified

对+、×两种运算都定义了阿贝尔群

且定义了交换逆元.

Prime subfield and characteristic

- Consider a *finite field* $\mathbb{F}$, define
  $S_r = 1 + 1 + \cdots + 1$ as sum of r 1's for a positive integer r
  - Let p be the smallest positive number with $S_p = 0$. If such a p exists, it must be *prime*
  - If $p = a \cdot b$ with $0 < a, b < p$, then by *distributivity*, $0 = S_p = S_a \cdot S_b$. Then one of S_a, S_b must be 0, contradicting the minimality of p.
- This p is called the *characteristic* of the field $\mathbb{F}$.
- The subset $\{0, S_1, S_2, \dots, S_{p-1}\} \subseteq \mathbb{F}$ is *isomorphic* to $\mathbb{F}$ (prime field)
- Any finite field $\mathbb{F}$ is a *finite dimensional vector space* over $\mathbb{F}_p$, with $n = \dim_{\mathbb{F}_p}(\mathbb{F})$, $|\mathbb{F}| = p^n$, i.e., the cardinality of $\mathbb{F}$ must be a prime power

p是最小的正整数使得$S_p=0$. 若p存在则必为质数.

$\mathbb{F}_{p^m} \cong \mathbb{F}_p^m$

Finite fields

- For any prime power q, there is essentially only one finite field of order q. Any two finite fields of order q are the same except that the labelling used to represent the field elements may be different
- *Binary field* – *characteristic-2* finite fields $\mathbb{F}_{2^m}$
  - Elements are polynomials over $\mathbb{F}_2$ of degree $\leq m-1$
  - $\mathbb{F}_{2^m} := \{a_{m-1}x^{m-1} + a_{m-2}x^{m-2} + \cdots + a_2x^2 + a_1x + a_0 : \ a_i \in \mathbb{F}_2\}$
- An *irreducible polynomial* $f(x)$ of degree m is chosen: $f(x)$ cannot be factered as a product of binary polynomials each of degree less than m
  - *Addition*: usual
  - *Multiplication*: modulo $f(x)$

Representing elements in finite fields

① elements are polynomials over $\mathbb{F}_2$ of degree $\leq m-1$

② irreducible polynomial of degree m

对$\mathbb{F}_{2^4}$, $x^4+1=(x+1)^4$, $x^4+x^2+1=(x^2+x+1)^2$都可约

因为特征为2, 故$2x=0$, 所以$(x+1)^4=(x^2+2x+1)^2$

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

而$f(x)=x^4+x+1$不可约.