群和环

群的定义

- 对一个具有一个二元运算的代数系统 $\langle G, \circ \rangle$ ，若满足
  1. 结合律
  2. 具有单位元
  3. 每个元素都具有逆元

  则称为一个 **群** 。若不满足 2,3 点则称为 **半群** ，若满足 2 但不满足 3 则称为 **幺半群** ，或 **独异点** 。若群满足交换律，则称为 **Abel 群（交换群）** 。

  Note : 运算性质按照基本程度可以排为： 结合律 > 交换律 > 分配率； 代数常数按照基本程度可以排为： 单位元 > 逆元 > 零元
- 半群的例子：所有 n 阶矩阵和矩阵乘法构成的代数系统。

群的性质

- 群自动满足消去律。
- 元素的阶数：若 $a \in G,\ \ a^r = e$ 则 a 的阶数为 r 记作 $|a| = r$ 。其中 e 为单位元。
  - $\forall k \in \mathbb{Z},\ \ a^k = e \text{ iff } \ r|k$
  - $|a^{-1}| = |a|$
  - $|a^t| = \frac{r}{gcd(t,r)}$

子群

- 定义：如果一个群(G)的非空子集(H)关于群中的运算构成群，则这个子集被称为原来群的子群。记作 $H \leq G$
- 判定定理：充要条件
  1. $\forall a, b \in H,\ \ ab \in H$ and $\forall a \in H,\ \ a^{-1} \in H$
  2. $\forall a, b \in H,\ \ ab^{-1} \in H$
  3. 若 H 是有限集，则只需要 $\forall a \in H,\ \ ab \in H$
- 由元素 a 生成的子群定义为：

  $$H = \{a^k | k \in \mathbb{Z}\}$$

  由子集 B 生成的子群定义为：

  $$\langle B \rangle = \cap\{H | B \subseteq H,\ H \leq G\}$$

陪集

- 定义：设 H 是群 G 的子群，$a \in G$ 则

  $$Ha = \{ha | h \in H\}$$

  称为子群 H 在 G 中的右陪集，a 称为 Ha 的代表元素。
- 性质：
  - 若 $a \in H$ ，则 $Ha = H$ (实质上就是 $Ha = He$ ，利用了陪集中任何元素都可以当代表元素的性质。)
  - $\forall a \in G,\ \ a \in Ha$
  - H 的每一个不同的陪集都有 $|H|$ 个元素。
- 判定定理：下列命题彼此等价（说明了陪集中任何元素都可以当代表元）
  - $Ha = Hb$
  - $a \in Hb$
  - $ab^{-1} \in H$
- 拉格朗日定理：设 G 是有限群，H 是子群，则

  $$|G| = |H|\dot{|}G : H|$$

  其中 $|G : H|$ 表示 H 在 G 中的陪集数。

循环群

- 定义：设 G 是循环群，a 是代表元。
  - n 阶循环群：$G = \{a^0 = e, a^1, a^2, \ldots, a^{n-1}\}$
  - 无限循环群：$G = \{a^0 = e, a^{\pm 1}, a^{\pm 2}, \cdots\}$
- 如何求生成元
  - 对于 n 阶循环群：对于任何不大于 n 且与 n 互素的正整数 r ，a^r 都是 G 的生成元。
  - 对于无限循环群，生成元只有 $a,\ a^{-1}$
- 循环群的子群
  - 无限循环群的子群除了 $\{e\}$ 以外还是无限循环群。
  - n 阶循环群的子群也是循环群，且对 n 的每一个正因子 d 都有一个 d 阶子群。事实上由 $a^{n/d}$ 生成的子群就是这个唯一的子群。

置换群

- 定义：设 $S = \{1, 2, \ldots, n\}$ ，S 上的任何双射函数 $\sigma : S \to S$ 称为 S 上的 n 元置换。一般将 n 元置换 σ 记作

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

- k 阶轮换：设 σ 是 $S = \{1, 2, \ldots, n\}$ 上的 n 元置换，若

$$\sigma(i_1) = i_2, \sigma(i_2) = i_3, \cdots, \sigma(i_{k-1}) = i_k, \sigma(i_k) = i_1$$

  将这个置换记为轮换表达式 $\sigma_1 = (i_1\ i_2\ \cdots\ i_k)$ 。若 k 等于 2 ，则称 σ 为对换。
  一个置换可以写成一系列的不交的轮换表达式之积（抽屉原理），**轮换表达式在不考虑顺序的情况下是唯一的**。同时所有的轮换表达式可以利用

$$\sigma = (i_1\ i_2\ \cdots i_n) = (i_1\ i_2)(i_1\ i_3)\cdots(i_1\ i_n)$$

  来转换成为一系列对换表达式的乘积。**一个置换表示成对换的方式不一定唯一，但是对换表达式的个数的奇偶性是一定的，根据这个性质将置换分成及置换和偶置换。**
- Polya 定理：
  设 $N = \{1, 2, \ldots, n\}$ 是被着色物体的集合，$G = \{\sigma_1, \sigma_2, \cdots, \sigma_g\}$ 是 N 上的置换群，用 m 种颜色对 N 中的元素进行着色，则在 G 的作用下不同的着色方案是

$$M = \frac{1}{|G|} \sum_{k=1}^{g} m^{c(\sigma_k)}$$

  其中 $c(\sigma_k)$ 是置换 σ_k 的轮换表达式中包含 1 阶轮换在内的轮换个数。

环和域

- 环的定义：设 $R = \langle R, +, \cdot \rangle$ 是代数系统，如果
  1. $\langle R, + \rangle$ 构成交换群
  2. $\langle R, \cdot \rangle$ 构成半群
  3. $\cdot$ 运算关于 $+$ 运算满足分配律

  则称该代数系统是一个环
- 环的例子：所有 n 阶矩阵和矩阵加法，矩阵乘法构成的系统。
- 设 $R = \langle R, +, \cdot \rangle$
  - 若环中的乘法满足交换律，则称为交换环
  - 若环中的乘法存在单位元，则称为含幺环
  - 若 $\forall a, b \in R,\ \ ab = 0 \text{ iff } a = 0 \text{ or } b = 0$ 则称 R 为无零因子环。
  - 无零因子的交换幺环称为整环
  - 若 R 是整环，且 $\forall a \in R^* = R - \{0\}$ 有 $a^{-1} \in R$ 则称 R 为域。