1 群

1.1 群的定义

若集合 $S \neq \varnothing$ 和 S 上的运算 $\cdot$ 构成的代数结构 $(S,\cdot)$ 满足以下性质：

- **封闭性**：$\forall a,b \in S, a\cdot b \in S \implies \cdot : S\times S \to S$
- 结合律：$\forall a,b,c \in S, (a\cdot b)\cdot c = a\cdot(b\cdot c)$
- 单位元：$\exists e \in S, \forall a \in S, e\cdot a = a\cdot e = a$
- **逆元（每个数都有）**：$\forall \boldsymbol{a} \in \boldsymbol{S}, \exists b \in S, \underline{a\cdot b = b\cdot a} = e$，称 b 为 a 的逆元，记为 a^{-1}

则称 $(S,\cdot)$ 为一个**群**（注意到 S 一定是非空的，有时直接把群写成 S）。有时记 $a\cdot b = ab$

例子：$\mathbb{Z} = \{\cdots,-2,-1,0,1,2,\cdots\}$ 和 $+$ 运算构成一个群。

一些其他定义：

- **有限群**：如果集合 S 是有限的，那么称之为有限群，而有限群的元素个数称作有限群的**阶**，记作 $|S|$。

1.2 群的简单性质

1. 一个群中的单位元唯一。
   证明：假设有两个单位元 e_1, e_2，有 $e_1 = e_1e_2 = e_2$。
2. 如果 $a\cdot x = e$，我们称 a 是 x 的左逆元；如果 $x\cdot b = e$，我们称 b 是 x 的右逆元。
   可以证明，在一个群中，每个元素的左逆元和右逆元是一样的（因此它是这个元素的逆元）
   证明：$ax = e = xb \implies a = ae = a\cdot(xb) = ax\cdot b = eb = b$
3. 一个群中 x 的逆元唯一。
   证明：如果有 x 两个逆元 a,b，那么我们有 $a = a\cdot(x\cdot b) = ax\cdot b = b$。
4. 群中有消去律存在。即 $\forall a,b,x \in G, ax = bx \Leftrightarrow a = b$。 $(a+c = b+c \implies a = b)$

   证明：两边同乘逆元。

在下面的讨论中，我们默认是在**有限群**上讨论。

1.3 子群及其衍生

- **子群**：对于一个群 $(G,\cdot)$，若 $H \subseteq G$，且 $(H,\cdot)$ 也是一个群，那么称 $(H,\cdot)$ 是 $(G,\cdot)$ 的一个**子群**，记为 $H \leq G$。
- **生成子群**：对于群 $(G,\cdot)$ 的子集 $T \subseteq G$，设

  $$T^* := \{T' \subseteq G \mid T \subseteq T' \text{ and } T' \leq G\}$$

  定义 T 的**生成子群**是

  $$\langle T \rangle := \bigcap_{T' \subseteq T^*} T'$$

  此时 T 是 $\langle T \rangle$ 的**生成集合**。
- （**循环群**：可由一个元素生成的群 H。$\exists x \in H, H = \langle x \rangle$（$x$ 代表 $\{x\}$））
- **陪集**：对于群 G 的一个子群 H 和 $a \in G$：

- 定义 H 的一个**左陪集**为 $_aH=\{ah \mid h\in H\}$。（$_2\mathbb{Z}=\{2k \mid k\in\mathbb{Z}\}$）
- 定义 H 的一个**右陪集**为 $H_a=\{ha \mid h\in H\}$。

注意陪集不一定是一个群，因为陪集显然可能没有单位元。

1.3.1 陪集的性质

陪集有一些重要的性质，我们下面只讨论右陪集的情况（左陪集同理）：

假设 $(G,\cdot)$ 是一个群，$H\leq G$：

1. $\boldsymbol{\forall a\in G, |H|=|H_a|}=|_aH|$。
   证明：$\forall h_1,h_2\in H$，$h_1\neq h_2 \implies ah_1\neq ah_2$（群的乘法消去律）
   对于不同的 h，ha 互不相同，因此 $|H|=|H_a|$。
2. $\forall a\in G, a\in H_a$。
   证明：因为 H 是群，所以 $e\in H$，所以 $ea\in H_a$ 即 $a\in H_a$。
3. $H_a=H\Leftrightarrow a\in H$
   证明：从左推到右，$a\in H_a \implies a\in H$。
   从右推到左，由群的封闭性 $H_a\subseteq H$，而 $|H|=|H_a|$，所以 $H_a=H$。
4. $\boldsymbol{H_a=H_b\Leftrightarrow ab^{-1}\in H}$。
   注意这个性质的右边也可以写成 $a\in H_b$ 或 $b\in H_a$。
   证明：从左推到右，$a\in H_a\Rightarrow a\in H_b(a=hb)\Rightarrow ab^{-1}\in H$。从右推到左，$H_{ab^{-1}}=H$，故 $H_a=H_b$。
5. $H_a\cap H_b\neq\varnothing\Rightarrow H_a=H_b$。
   这句话的意思是 H 的任意两个陪集要么相等，要么没有交集。
   证明：考虑 $c\in H_a\cap H_b$，那么 $\exists h_1,h_2\in H, h_1a=h_2b=c$，那么 $ab^{-1}=h_1^{-1}h_2\in H$，故 $H_a=H_b$。
6. H 的所有左（右）陪集的并是 G。

1.3.2 拉格朗日定理

若 $H\leq G$，那么 $|H|$ 整除 $|G|$。更准确地

$$|G|=|H|\cdot[G:H]$$

其中 $[G:H]$ **表示** G **中** H **不同的左（右）陪集数。**

证明：根据陪集的性质，H 的所有不同左（右）陪集大小相等且互不相交。

1.3.3 一些推论和应用

对于某个元素 $a\in G$，我们称 a 的**周期** $o(a)=\min\{x \mid a^x=e, x\in\mathbb{N}^*\}$

（$a^2=a\cdot a, a^3=a\cdot a\cdot a\cdots$）

在有限群内这个周期一定存在，否则我们令 $o(a)=+\infty$。

那么对于有限群 G，有以下推论：

- 对于 $a\in G$，有 $o(a)\mid |G|$。

  证明：$o(a)=|\langle a\rangle|$，显然 $\langle a\rangle\leq G$，由拉格朗日定理可知 $o(a)|\ |G|$。

- 对每个 $a\in G$，都有 $a^{|G|}=e$。

  证明：由前面的推论显然。

- 若 $|G|$ 为素数，则 G 是**循环群**。

  证明：对于 $a \neq e$，有 $|\langle a\rangle| \neq 1$ 整除 $|G|$，也就是 $|\langle a\rangle| = |G|$，因为 $\langle a\rangle \leq G$，所以 $\langle a\rangle = G$。

有一些的应用：

- 费马小定理：若 p 是质数，那么 $\forall a \not\equiv 0 \pmod p, a^{p-1} \equiv 1 \pmod p$。

  证明只要考虑群 $(\{1, 2, \cdots, p-1\}, \times \bmod p)$。
- 欧拉定理：若 $\gcd(a, p) = 1$，那么 $a^{\phi(p)} \equiv 1 \pmod p$。

  证明只要考虑群 $(\{x \mid x \in [1, p), \gcd(x, p) = 1\}, \times \bmod p)$。

2 置换群

2.1 置换的定义

- **映射（函数）**：A, B 集合非空，$\forall x \in A$ 依照对应规则 f 有 B 中唯一的元素 y 与之对应，那么就称 f 是 A 到 B 的映射，记作

$$\begin{aligned} f : A &\to B \\ x &\mapsto y \end{aligned}$$

- **单射**：映射 $f : A \to B$ 如果满足 $\forall a, b \in A, a \neq b \implies f(a) \neq f(b)$（$f(a) = f(b) \implies a = b$）
- **满射**：$B = f(A) = \{f(a) \mid a \in A\}$
- **双射**（一一对应）：既是单射，又是满射
- **置换**：有限集合到自身的双射（即一一对应）称为**置换**。不可重集合 $X = \{a_1, a_2, \cdots, a_n\}$ 上的置换可以表示为

$$\sigma = \begin{pmatrix} a_1, a_2, \ldots, a_n \\ a_{p_1}, a_{p_2}, \ldots, a_{p_n} \end{pmatrix}$$

表示将 a_i 映射为 a_{p_i}，即 $\sigma(a_i) = a_{p_i}$。其中 $p_1, p_2, \cdots, p_n$ 是 $1 \sim n$ 的一个排列。

如果我们没有强制 $a_1, a_2, \cdots, a_n$ 的排列顺序，那么显然这些列的顺序是不要紧的。

显然 X 上的所有不同置换的数量为 $n!$。记 X 上所有不同置换记作 S_X 或者 $\mathrm{Sym}(X)$。

2.2 置换的乘法

对于两个置换，$f = \begin{pmatrix} a_{p_1}, a_{p_2}, \ldots, a_{p_n} \\ a_{q_1}, a_{q_2}, \ldots, a_{q_n} \end{pmatrix}$ 和 $g = \begin{pmatrix} a_1, a_2, \ldots, a_n \\ a_{p_1}, a_{p_2}, \ldots, a_{p_n} \end{pmatrix}$，$f$ 和 g 的乘积记为 $f \circ g$（有时直接写成 fg），其值为

$$f \circ g = \begin{pmatrix} a_1, a_2, \ldots, a_n \\ a_{q_1}, a_{q_2}, \ldots, a_{q_n} \end{pmatrix}$$

即 $(f \circ g)(x) = f(g(x))$，简单来说就是先经过了 g 的映射再经过了 f 的映射（映射的复合）。

2.3 置换群

通常我们把在 $\{1,2,\cdots,n\}$ 上的所有置换构成的集合记为 S_n，即

$$S_n=\{双射\sigma:\{1,2,\cdots,n\}\to\{1,2,\cdots,n\}\}$$

易验证，所有置换关于置换的乘法满足封闭性、结合律、有单位元（**恒等置换/单位置换**，即每个元素映射成它自己）、有逆元（交换置换表示中的上下两行），因此集合 $(S_n,\circ)$ 构成一个群，称为 n **元对称群。**

这个群的任意一个子群即称为**置换群。**

2.4 循环置换

循环置换（也叫**轮换**）是集合 X 上特殊的置换：

- 如果记 $\sigma=(a_1,a_2,\ldots,a_m)$，那么定义

$$\begin{cases}\sigma(x)=x & x\in X,x\neq a_i(i=1,2,..,m)\\ \sigma(a_i)=a_{i+1} & i=1,2,..,m-1\\ \sigma(a_m)=a_1\end{cases}$$

（若两个循环置换的“a”不含有相同的元素，则称它们是**不相交**的）。

有如下定理：任意一个置换都可以分解为若干不相交的循环置换的乘积，例如

$$\begin{pmatrix}a_1,a_2,a_3,a_4,a_5\\a_3,a_1,a_2,a_5,a_4\end{pmatrix}=(a_1,a_3,a_2)\circ(a_4,a_5)$$

该定理的证明也非常简单。如果把元素视为图的节点，映射关系视为有向边，则每个节点的入度和出度都为 1，因此形成的图形必定是若干个环的集合，而一个环即可用一个循环置换表示。

3 轨道-稳定子定理

3.1 相关定义

- **群作用**：

  群 G 在集合 X 上的（左）群作用是一个**二元函数** $\alpha:G\times X\to X$，满足两个公理

$$\begin{cases}\alpha(e,x)=x & e是群G中的单位元\\ \alpha(g,\alpha(h,x))=\alpha(gh,x) & \forall g,h\in G\ \forall x\in X\end{cases}$$

  对于 $g\in G,x\in X$，通常记 $\alpha(g,x)=g\cdot x$ 或者 $g(x)$。公理就可以写成

$$\begin{cases}e(x)=x & e是群G中的单位元\\ g(h(x))=(gh)(x) & \forall g,h\in G\ \forall x\in X\end{cases}$$

  结论：取定 $g\in G$，实际上 $x\mapsto g(x)$ 是 $X\to X$ 的双射。
  例子：G 是置换群 $\leq S_X$，$\sigma\in G$，就可以定义 σ 作用于序列 $a=(a_1,a_2,\ldots,a_n)$ 得到 $\sigma(a)=(a_{\sigma(1)},a_{\sigma(2)},\ldots,a_{\sigma(n)})$。

- **稳定子、轨道、不动点集**：
  - 设 G 是作用于集合 X 的一个群，记 $\alpha(g,x)=g(x)$。
  - 对于每个 $x\in X$，我们定义

$$G^x = \{g \in G \mid g(x) = x\}$$
$$G(x) = \{g(x) \mid g \in G\}$$

其中 G^x 称为 x 的**稳定子**，$G(x)$ 称为 x 的**轨道**。

- 对于每个 $g \in G$，我们定义

$$X^g = \{x \in X \mid g(x) = x\}$$

称为 X 在 g 作用下的**不动点集合**。

（例子：定义 A, B 是两个有限集合，$X = B^A$ 表示所有从 A 到 B 的映射，G 是作用在 A 上的一个置换群。比如给正方体六个面染色，A 就是正方体六个面的集合，B 就是所有颜色的集合，X 就是不考虑本质不同的方案集合，即 $|X| = |B|^{|A|}$ ）

3.2 轨道-稳定子定理

定理：设 G 是作用于集合 X 的一个群，对任意的 $x \in X$ 都有

$$|G| = |G^x| \cdot |G(x)|$$

证明：step1. 首先可以证明 G^x 是 G 的一个子群，因为

- **封闭性**：若 $f, g \in G$ ，则 $(f \circ g)(x) = f(g(x)) = f(x) = x$ ，所以 $f \circ g \in G^x$。
- 结合律：显然置换的乘法满足结合律。
- 单位元：因为 $I(x) = x$ ，所以 $I \in G^x$ （I 为恒等置换）。
- 逆元：若 $g \in G^x$ ，则 $g^{-1}(x) = g^{-1}(g(x)) = (g^{-1} \circ g)(x) = I(x) = x$ ，所以 $g^{-1} \in G^x$。

step2. 由拉格朗日定理得 $|G| = |G^x| \cdot [G : G^x]$。下面只要证明 $|G(x)| = [G : G^x]$（直观理解这是很显然的，但是我们还是要证明一下）

- 令 $\varphi(g(x)) = {}_gG^x$，下面证明 φ 是**单射**，则 $|G(x)| \le [G : G^x]$。
  - $f(x) = g(x) \iff (f^{-1}g)(x) = x \iff f^{-1}g \in G^x \iff {}_fG^x =_g G^x$
  - 即 φ 是一个从 $G(x)$ 到左陪集的单射。
- 令 $\varphi'({}_gG^x) = g(x)$，同理证明 φ' 是**单射**，则 $|G(x)| \ge [G : G^x]$。

4 Burnside 引理

假设 G 是作用于有限集 X 的一个（置换）群

定义 X/G：表示 G 作用在 X 上产生的所有等价类的集合

- 设 $a, b \in X$，规定 a 与 b 等价（记为 $a \sim b$）的充要条件是
- $a \sim b \iff \exists h \in G, h(a) = b(\iff G(a) = G(b))$
  - 右边这个等价符号的证明：
    $\forall g \in G$，$g(b) = g(h(a)) = (gh)(a)\ (gh \in G) \implies G(b) \subseteq G(a)$
    同理根据 $h^{-1}(b) = a$ 可以推出 $G(a) \subseteq G(b)$
- $[x] = \{y \mid x \sim y\}$
- $X/G = \{[x] \mid x \in X\} = \{G(x) \mid x \in X\}$

X/G 其实就是，对于所有的 $x \in X$ **不同轨道的集合**，这些轨道必定是不交的。因此我们也将 $|X/G|$ 叫做 X 关于 G 的**轨道数**。

Burnside 引理：

$$|X/G| = \frac{1}{|G|}\sum_{g\in G}|X^g|$$

其中 $X^g = \{x \mid g(x) = x, x \in X\}$，我们称 X^g 是 X 在置换 g 下的**不动点**集合。

文字描述：X **关于置换群** G **的轨道数，等于** G **中每个置换下** X **不动点的个数的算术平均数。**

证明：（**Burnside 引理本质上是更换了枚举量，从而方便计数**）

$$\begin{aligned}
|X/G| &= \sum_{Y\in X/G} 1 \\
&= \sum_{Y\in X/G}\sum_{x\in Y}\frac{1}{|Y|} \\
&= \sum_{Y\in X/G}\sum_{x\in Y}\frac{1}{|G(x)|} \\
&= \sum_{x\in X}\frac{1}{|G(x)|}
\end{aligned}$$

根据轨道-稳定子定理，我们有 $|G| = |G^x|\cdot|G(x)|$，所以

$$\begin{aligned}
|X/G| &= \sum_{x\in X}\frac{1}{|G(x)|} \\
&= \frac{1}{|G|}\sum_{x\in X}\frac{|G|}{|G(x)|} \\
&= \frac{1}{|G|}\sum_{x\in X}|G^x| \\
&= \frac{1}{|G|}\sum_{x\in X}\sum_{g\in G}[g(x) = x] \\
&= \frac{1}{|G|}\sum_{g\in G}|X^g|
\end{aligned}$$

至此我们就证明了 Burnside 引理。

注意当 $X \subseteq B^A$ **时，Burnside 引理也是成立的。也就是说，我们给** A **到** B **的映射加上一些条件，Burnside 引理仍然成立。其原因就是上面的证明没有用到** $X = B^A$**。**

5 Pólya 定理

是 Burnside 引理的一种特殊形式。

定义 A, B 是两个有限集合，$X = B^A$ 表示所有从 A 到 B 的映射，G 是作用在 X 上的一个置换群。

$$|X/G| = \frac{1}{|G|}\sum_{g\in G}|B|^{c(g)}$$

$c(g)$ 表示置换 g 拆出的不相交轮换数量。

证明：在 Burnside 引理中，$g(x) = x$ 的充要条件是 x 将 g 中每个轮换内的元素都映射到了 B 中的同一个元素，所以 $|X^g| = |B|^{c(g)}$，即可得 Pólya 定理。

注意只有当 $X = B^A$ **成立时（也就是当** X **是** A **到** B **的所有映射时），Pólya 定理才成立，否则不一定成立。**