

# 浅谈置换群

codgician

2020.03.14

# 关系

- 集合的笛卡尔积 (Cartesian product):

$$A \times B = \{(a, b) \mid a \in A, b \in B\}$$

- 设  $A$  是集合, 集合  $A \times A$  的每个子集  $R$  叫做集合  $A$  上的一个**关系** (relation)。
- 若  $(a, b) \in R$ , 则称  $a$  和  $b$  有关系  $R$ , 记作  $aRb$ 。

# 等价关系

若集合  $A$  上的关系  $\sim$  满足如下条件:

- **自反性**:  $\forall a \in A, a \sim a$ ;
- **对称性**:  $\forall a, b \in A$ , 若  $a \sim b$  则  $b \sim a$ ;
- **传递性**:  $\forall a, b \in A$ , 若  $a \sim b, b \sim c$ , 则  $a \sim c$ ;

则称  $\sim$  是**等价关系** (equivalence relation)

$$a \sim b := a \equiv b \pmod{7}$$

- 自反性? 对称性? 传递性?
- 看起来可以把所有自然数分成 7 类.....

# 等价类

设  $\sim$  是  $A$  上的等价关系,  $\forall a \in A$ ,  $[a]$  表示  $A$  中与  $a$  等价的全部元素构成的集合:

$$[a] = \{b \sim a \mid b \in A\}$$

称  $[a]$  为  $a$  所在的**等价类** (equivalence class)。

若  $a, b \in A$  且  $[a] \cap [b] \neq \emptyset$ , 则  $[a] = [b]$ 。

**若**  $a, b \in A$  **且**  $[a] \cap [b] \neq \emptyset$ , **则**  $[a] = [b]$ 。

- 假设  $k_1 \in [a]$  且  $k_1 \notin [b]$ ,  $k_2 \in [a] \cap [b]$ ;
- 则有  $k_1 \sim a$ ,  $k_2 \sim a$ ,  $k_2 \sim b$ ;
- 由传递性得  $k_1 \sim b$ , 与假设不符。

若  $a, b \in A$  且  $[a] \cap [b] \neq \emptyset$ , 则  $[a] = [b]$ 。

- 集合  $A$  可看作一些两两不相交的等价类的并：

$$A = \bigcup_{a \in R} [a] \quad (\text{两两不相交之并})$$

- $A$  上的每个等价关系给出集合  $A$  的一个**划分** (partition)。



# 群 $(G, \cdot)$

$G$  是非空集合, 且二元运算满足:

- 结合律:  $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
- 单位元  $e$ :  $\forall a \in G, ea = ae = a$
- 逆元:  $\forall a \in G, \exists b \in G$  s.t.  $ab = ba = e$

# 群 $(G, \cdot)$

$G$  是非空集合, 且二元运算满足:

- 结合律:  $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
- 单位元  $e$ :  $\forall a \in G, ea = ae = a$
- 逆元:  $\forall a \in G, \exists b \in G$  s.t.  $ab = ba = e$

若满足交换律, 则称为**交换群**

- 左右逆元相等:

- 设  $x$  是  $a$  的左逆元,  $y$  是  $a$  的右逆元, 有:

$$x = xe = x(ay) = (xa)y = y$$

- 满足消去律:

- $\forall a, b, c \in G, ab = ac \Leftrightarrow b = c$

# 子群

设  $(G, \cdot)$  为群,  $H$  是  $G$  的子集, 若  $(H, \cdot)$  成群, 则称  $H$  为  $G$  的子群 (subgroup), 记作  $H \leq G$ ;

# 陪集

设  $H \leq G$ , 对于  $x \in G$ :

- $H$  的一个**左陪集** (left coset)  $xH$ :

$$xH = \{x \cdot h \mid h \in H\}$$

- $H$  的一个**右陪集** (right coset)  $Hx$ :

$$Hx = \{h \cdot x \mid h \in H\}$$

$$xH = \{x \cdot h \mid h \in H\}$$

$$xH = \{x \cdot h \mid h \in H\}$$

$$x \sim y := x \in yH$$

- **自反性:**  $x \in xH$ ;
- **对称性:** 若  $y \in xH$ , 则  $x \in yH$ ;
- **传递性:** 若  $z \in yH$ ,  $y \in xH$ , 则  $z \in xH$ 。

- 若  $xH \cap yH \neq \emptyset$ , 则  $xH = yH$ ;
- 利用陪集可以对群  $G$  进行划分 (陪集分解) :

$$G = \bigcup_{g \in R} gH \text{ (两两不相交之并)}$$



- 对于  $a, b \in H, g \in G$ , 由消去律  $a \neq b \Leftrightarrow ga \neq gb$ ;
- 因此,  $\forall g \in R, |gH| = |H|$ :

$$|G| = \sum_{g \in R} |gH| = \sum_{g \in R} |H| = |R| \cdot |H|$$

# 拉格朗日定理

设  $G$  为有限群,  $H \leq G$ , 则:

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

其中  $[G : H]$  称为群  $H$  对于群  $G$  的**指数** (index)。

# 置换

一个集合的**置换** (permutation) 即从该集合映射至自身的双射。

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

$$\text{复合运算: } (f \circ g)(x) = f(g(x))$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 1 & 3 & 6 & 2 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 1 & 3 & 6 & 2 \end{pmatrix}$$

$$1 \rightarrow 4 \rightarrow 3$$

$$2 \rightarrow 5 \rightarrow 6$$

任一置换都能被划分成若干不交的映射链？

# 轮换表示法

$$\begin{pmatrix} a_1 & a_2 & \dots & a_n \\ a_2 & a_3 & \dots & a_1 \end{pmatrix} \xRightarrow{\text{记作}} (a_1 \ a_2 \ \dots \ a_n)$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 1 & 3 & 6 & 2 \end{pmatrix} = (1 \ 4 \ 3) \cdot (2 \ 5 \ 6)$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 1 & 3 & 6 & 2 \end{pmatrix} = (1 \ 4 \ 3) \cdot (2 \ 5 \ 6)$$

**若不计轮换内外的次序，对于任意置换的不交轮换分解是唯一的吗？**



- 对于恒等置换, 显然分解是唯一的;
- 对于非恒等置换,  $\exists i$  s.t.  $\sigma(i) \neq i$ .
  - $i \rightarrow \sigma(i) \rightarrow \sigma^2(i) \rightarrow \dots$
  - 由抽屉原理,  $\exists t_1 < t_2$  s.t.  $\sigma^{t_1}(i) = \sigma^{t_2}(i)$
  - 令  $t$  为使得  $\sigma^t(i) = i$  的最小正整数, 则:

$$(i \ \sigma(i) \ \dots \ \sigma^{t-1}(i))$$

是一个轮换。

- 对于每个这样的  $i$  都如此操作即可构造出一个唯一的不相交轮换分解式：
  - 每个元素在分解式中恰好出现 1 次；
  - 每个元素所属的轮换是固定的。

# 轮换的幂运算

# 轮换的幂运算

$(1\ 2\ 3\ 4\ 5\ 6)$

# 轮换的幂运算

$$\begin{aligned} & (1\ 2\ 3\ 4\ 5\ 6)^2 \\ &= (1\ 3\ 5) \cdot (2\ 4\ 6) \end{aligned}$$

# 轮换的幂运算

$$\begin{aligned} & (1\ 2\ 3\ 4\ 5\ 6)^3 \\ &= (1\ 4) \cdot (2\ 5) \cdot (3\ 6) \end{aligned}$$

# 轮换的幂运算

$$\begin{aligned} & (1\ 2\ 3\ 4\ 5\ 6)^4 \\ &= (1\ 5\ 3) \cdot (2\ 6\ 4) \end{aligned}$$

$$\sigma = (a_0 \ a_1 \ \dots \ a_{n-1})$$

- $\sigma^t(a_i) = a_{[(i+t) \bmod n]}$
- 令  $k \in \mathbb{N}^*$  s.t.  $\sigma^{tk}(a_i) = a_i$ :



$$\sigma = (a_0 \ a_1 \ \dots \ a_{n-1})$$

- $\sigma^t(a_i) = a_{[(i+t) \bmod n]}$
- 令  $k \in \mathbb{N}^*$  s.t.  $\sigma^{tk}(a_i) = a_i$ :

$$i + tk \equiv i \pmod{n}$$

$$\sigma = (a_0 \ a_1 \ \dots \ a_{n-1})$$

- $\sigma^t(a_i) = a_{[(i+t) \bmod n]}$
- 令  $k \in \mathbb{N}^*$  s.t.  $\sigma^{tk}(a_i) = a_i$ :

$$tk \equiv 0 \pmod{n}$$

最小正整数解:  $k = \frac{n}{\gcd(n,t)}$

$$\sigma = (a_0 \ a_1 \ \dots \ a_{n-1})$$

- $\sigma^t$  可表示为  $\gcd(n, t)$  个长为  $\frac{n}{\gcd(n, t)}$  的轮换;
- $a_i$  所在轮换里第  $j$  个元素为  $a_{(i+jt) \bmod n}$ 。

$$\sigma = (a_0 \ a_1 \ \dots \ a_{n-1})$$

- $\sigma^t$  可表示为  $\gcd(n, t)$  个长为  $\frac{n}{\gcd(n, t)}$  的轮换;
- $a_i$  所在轮换里第  $j$  个元素为  $a_{(i+jt) \bmod n}$ 。
  - $a_i$  所在轮换内元素下标模  $\gcd(n, t)$  均为  $i$ ;
  - $a_0, a_1, \dots, a_{\gcd(n, t)-1}$  一定位于不同轮换。

# 置换群

$n$  个元的所有置换，在复合运算  $\circ$  下成群，称作  $n$  元**对称群** (symmetric group)，记作  $S_n$

- **结合律**：  $(\sigma \circ \tau) \circ \phi = \sigma \circ (\tau \circ \phi)$
- **单位元**：恒等置换  $\epsilon \circ x = x$ ;
- **逆元**：置换是双射，故必然存在逆置换。

# 群在集合上的作用

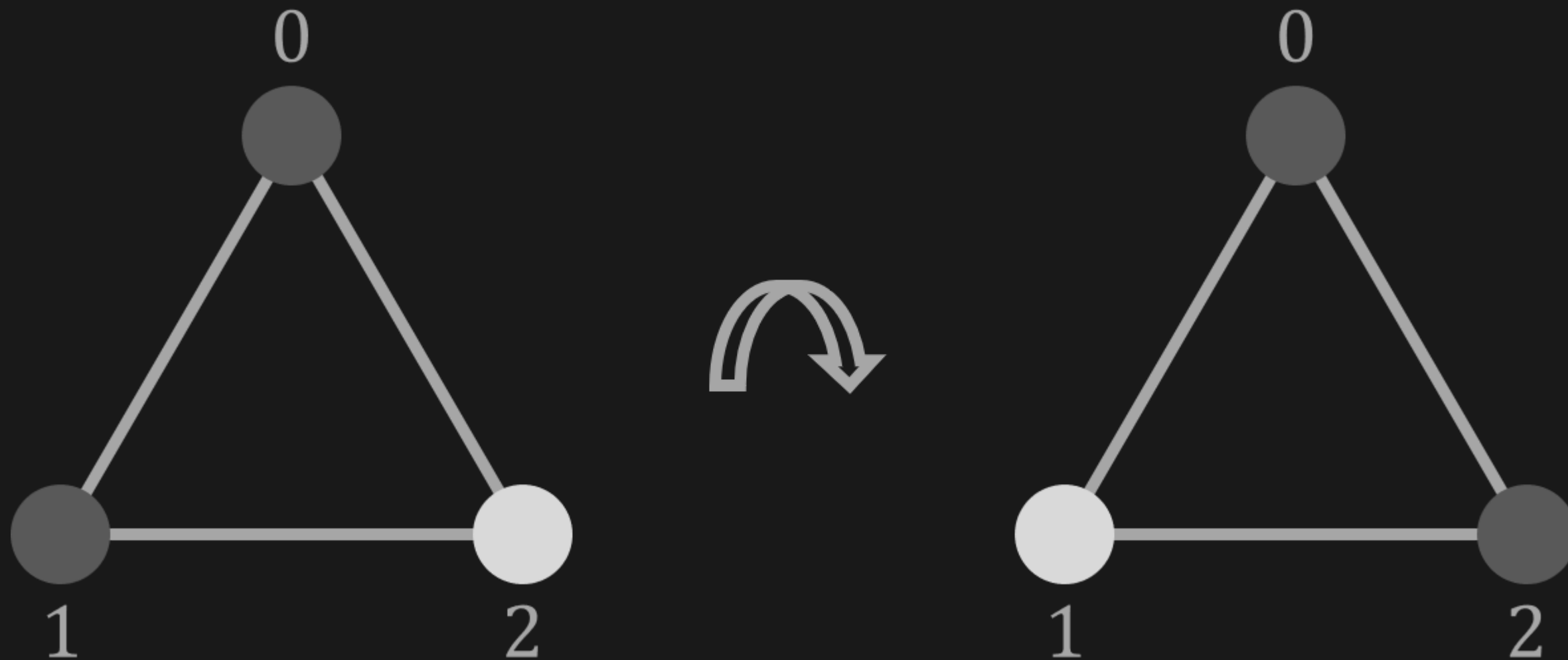
$$\phi : G \times M \longrightarrow M$$

$$(\sigma, x) \longmapsto \sigma \circ x$$

- $\forall x \in M$  满足:
  - **单位元**:  $\exists \epsilon \in G$  s.t.  $\epsilon \circ x = x$
  - **结合律**:  $\tau \circ (\sigma \circ x) = (\tau \circ \sigma) \circ x$

用黑白两色对等边三角形顶点染色，若可通过旋转得到的方案算相同方案，求方案数？

用黑白两色对等边三角形顶点染色，若可通过旋转得到的方案算相同方案，求方案数？



在旋转意义下同构



用黑白两色对等边三角形顶点染色，若可通过旋转得到的方案算相同方案，求方案数？

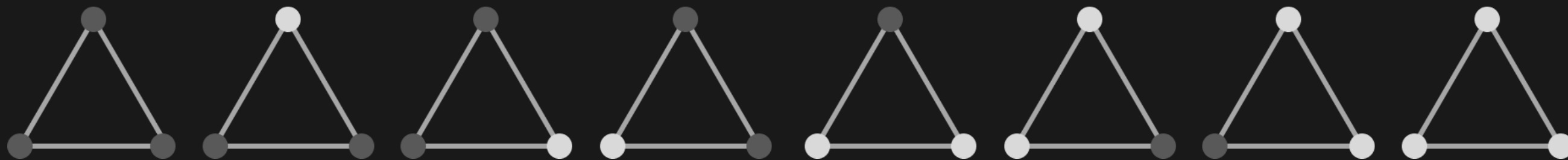
$$G = \{\text{顺时针旋转 } 0^\circ, 120^\circ, 240^\circ\}$$

$$M = \{\text{不考虑同构时的染色方案}\}$$

用黑白两色对等边三角形顶点染色，若可通过旋转得到的方案算相同方案，求方案数？

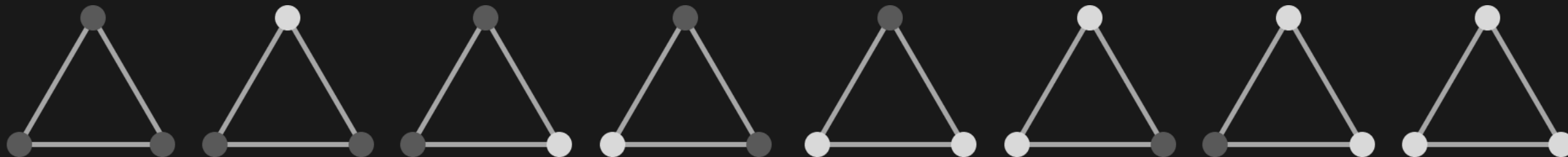
$G = \{\text{顺时针旋转 } 0^\circ, 120^\circ, 240^\circ\}$

$M = \{\text{不考虑同构时的染色方案}\}$

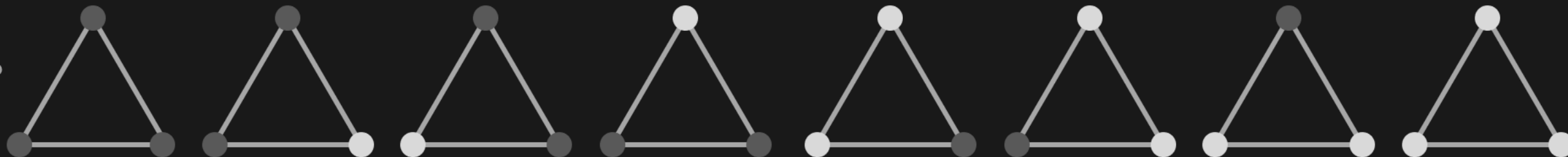


不考虑同构时的染色方案

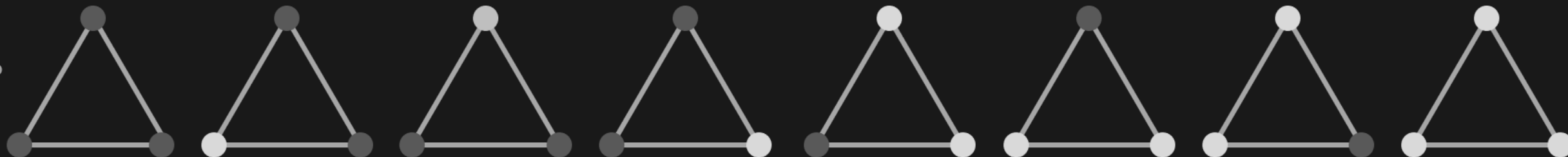
0°



120°

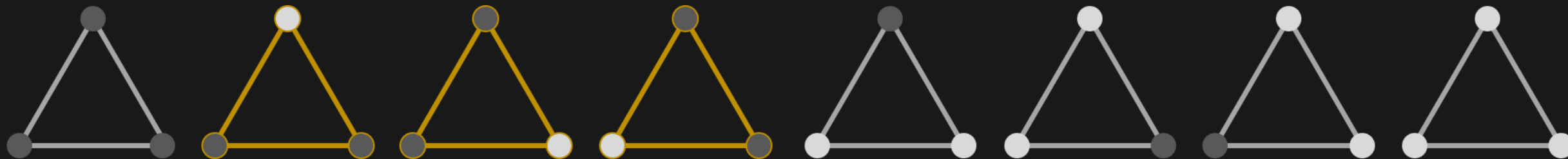


240°

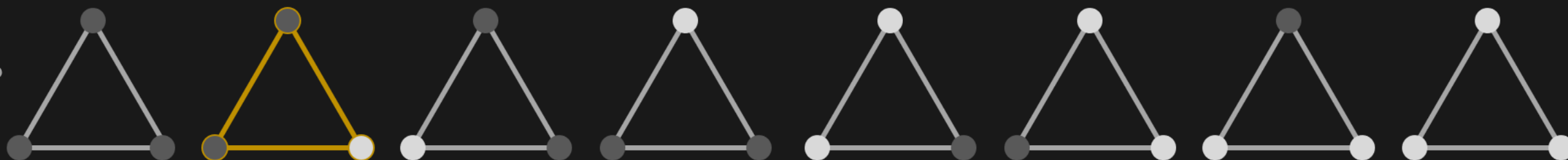


$$G \times M$$

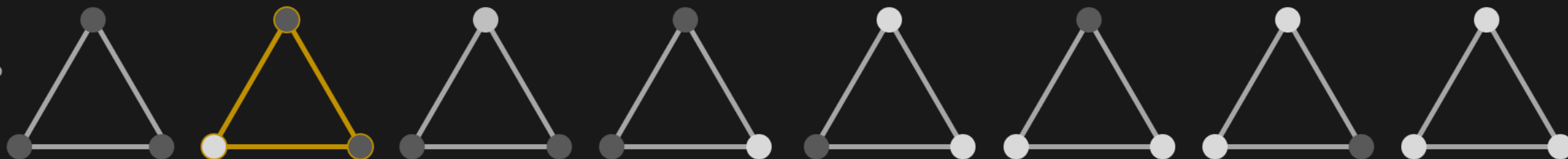
$0^\circ$



$120^\circ$

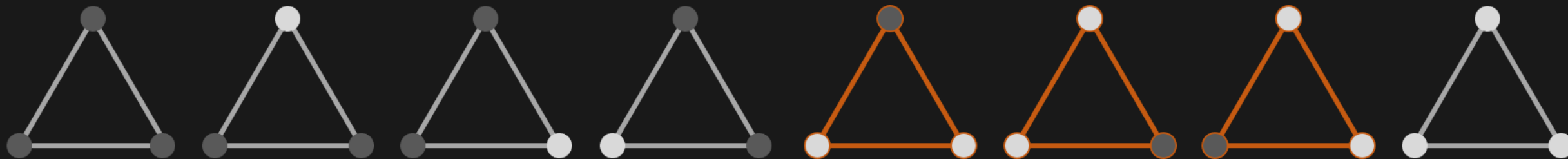


$240^\circ$

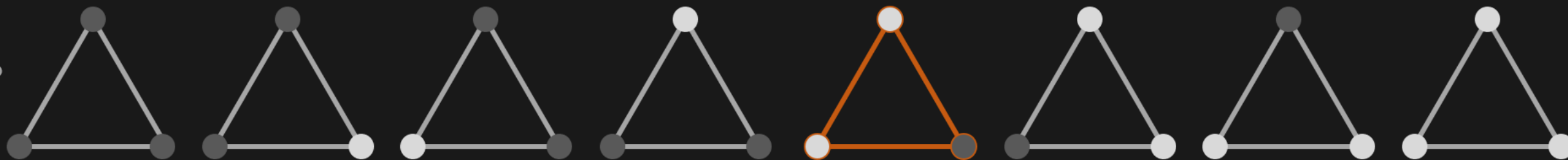


等价类?

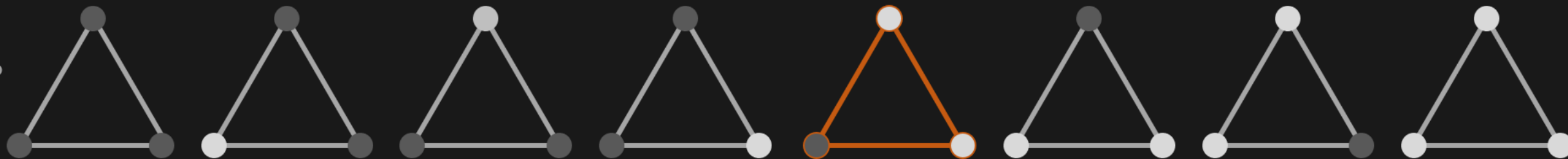
0°



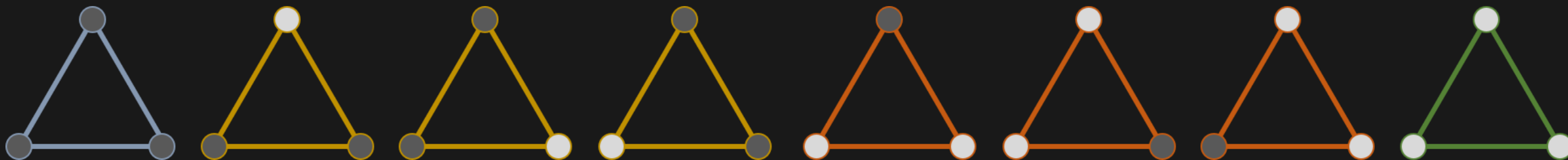
120°



240°



等价类?



- 一种等价关系?
- 借助该等价关系对集合进行划分?
- 有多少不同的等价类?

# 轨道

群  $G$  作用于集合  $M$  上,  $x \in M$ , 称  $M$  的子集

$$\text{orb}_G(x) = \{\sigma \circ x \mid \sigma \in G\}$$

为  $x$  在  $G$  作用下的**轨道** (orbit), 简称过  $x$  的轨道。

# 轨道

群  $G$  作用于集合  $M$  上,  $x \in M$ , 称  $M$  的子集

$$\text{orb}_G(x) = \{\sigma \circ x \mid \sigma \in G\}$$

为  $x$  在  $G$  作用下的**轨道** (orbit), 简称过  $x$  的轨道。

- $G$  中置换作用于元素  $x$  所能得到的不同结果;
- $|\text{orb}_G(x)|$ : 对于元素  $x$  而言,  $G$  中本质不同置换的种数。



$$\text{orb}_G(x) = \{\sigma \circ x \mid \sigma \in G\}$$

$$x \sim y := x \in \text{orb}_G(y)$$

- **自反性:**  $x \in \text{orb}_G(x)$ ;
- **对称性:** 若  $y \in \text{orb}_G(x)$ , 则  $x \in \text{orb}_G(y)$ ;
- **传递性:** 若  $z \in \text{orb}_G(y)$ ,  $y \in \text{orb}_G(x)$ , 则  $z \in \text{orb}_G(x)$ 。

- 若  $\text{orb}_G(x) \cap \text{orb}_G(y) \neq \emptyset$ , 则  $\text{orb}_G(x) = \text{orb}_G(y)$ ;
- 在  $M$  的每一条轨道上取一个元素组成  $M$  的一个子集  $R$ , 称为  $M$  的**轨道的代表元集**, 则:

$$M = \bigcup_{x \in R} \text{orb}_G(x)$$

并且此中各  $\text{orb}_G(x)$  互不相交。

# 稳定子

设群  $G$  作用于集合  $M$ , 对  $x \in M$ , 称

$$\text{stab}_G(x) = \{\sigma \mid \sigma \in G, \sigma \circ x = x\}$$

为群  $G$  作用下  $x$  的**稳定子** (stabilizer)。

# 稳定子

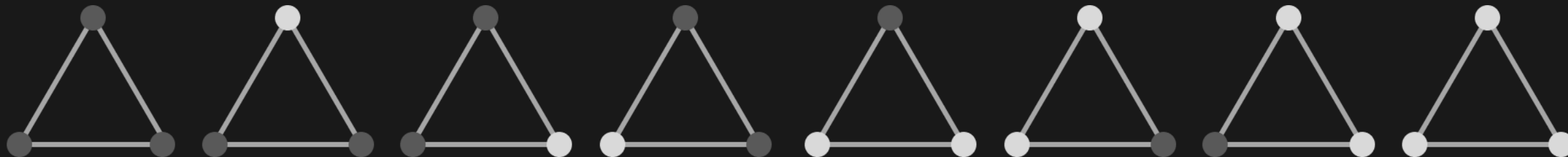
设群  $G$  作用于集合  $M$ , 对  $x \in M$ , 称

$$\text{stab}_G(x) = \{\sigma \mid \sigma \in G, \sigma \circ x = x\}$$

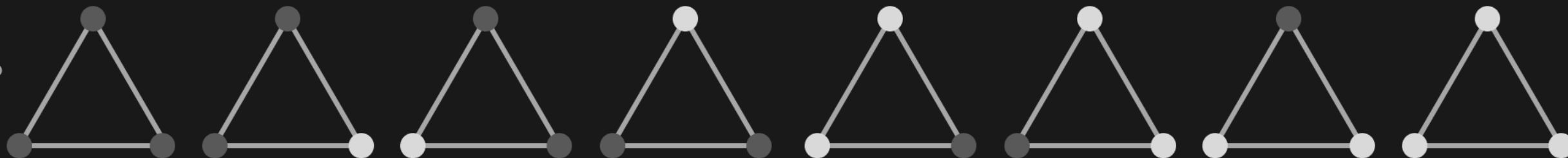
为群  $G$  作用下  $x$  的**稳定子** (stabilizer)。

- 所有作用于  $x$  后结果仍然为  $x$  的置换。

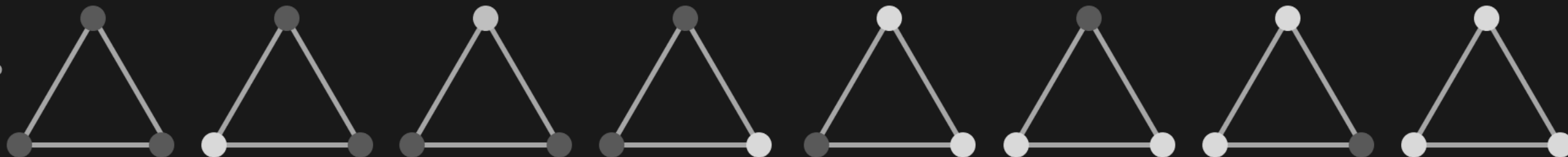
0°



120°



240°



$$G \times M$$

$$\text{stab}_G(x) = \{\sigma \circ x = x \mid \sigma \in G\} \leq G$$

$$\text{stab}_G(x) = \{\sigma \circ x = x \mid \sigma \in G\} \leq G$$

- **封闭性**:  $\forall \sigma, \tau \in \text{stab}_G(x), \sigma \circ \tau \circ x = \sigma \circ x = x$ , 故  $(\sigma \circ \tau) \in \text{stab}_G(x)$ ;
- **结合律**: 显然置换的复合满足结合律;
- **单位元**: 恒等置换  $\epsilon \circ x = x$ ;
- **逆元**:  $\forall \sigma \in \text{stab}_G(x), \sigma^{-1} \circ x = \sigma^{-1} \circ (\sigma \circ x) = \epsilon(x) = x$ 。

$$\text{stab}_G(x) = \{\sigma \circ x = x \mid \sigma \in G\} \leq G$$



$$\text{stab}_G(x) = \{\sigma \circ x = x \mid \sigma \in G\} \leq G$$

- 既然是子群，那可以用来对  $G$  进行左陪集划分；

$$\text{stab}_G(x) = \{\sigma \circ x = x \mid \sigma \in G\} \leq G$$

- $\beta\text{stab}_G(x)$  里的元素相当于作用于  $x$  时  $G$  中所有与  $\beta$  等价的置换:

$$\beta\text{stab}_G(x) = \{(\beta \circ \sigma) \circ x = \beta \circ x \mid \sigma \in G\}$$

$$\text{stab}_G(x) = \{\sigma \circ x = x \mid \sigma \in G\} \leq G$$

- $\beta\text{stab}_G(x)$  里的元素相当于作用于  $x$  时  $G$  中所有与  $\beta$  等价的置换:

$$\beta\text{stab}_G(x) = \{\tau \circ x = \beta \circ x \mid \tau \in G\}$$

$$\text{stab}_G(x) = \{\sigma \circ x = x \mid \sigma \in G\} \leq G$$

- $\beta\text{stab}_G(x)$  里的元素相当于作用于  $x$  时  $G$  中所有与  $\beta$  等价的置换:

$$\beta\text{stab}_G(x) = \{\tau \circ x = \beta \circ x \mid \tau \in G\}$$

$$|G| = |\text{stab}_G(x)| \cdot [G : \text{stab}_G(x)]$$

- $|\text{orb}_G(x)|$ : 对  $x$  而言,  $G$  中所有本质不同置换种数。
  - 也就是不同的上述陪集的种数!

# 轨道-稳定子定理

设有限群  $G$  作用于集合  $M$ ,  $x \in M$ , 则:

$$|G| = |\operatorname{stab}_G(x)| \cdot |\operatorname{orb}_G(x)|$$

# BURNSIDE 引理

设有限群  $G$  作用于有限集  $M$  上, 则轨道数:

$$|M/G| = \frac{1}{|G|} \sum_{\sigma \in G} |\text{fix}(\sigma)|$$

其中  $\text{fix}(\sigma)$  代表  $\sigma$  的不动元构成的集合:

$$\text{fix}(\sigma) = \{x \mid x \in M, \sigma \circ x = x\}$$

# 证明

$$\text{stab}_G(x) = \{\sigma \mid \sigma \in G, \sigma \circ x = x\}$$

$$\text{fix}(\sigma) = \{x \mid x \in M, \sigma \circ x = x\}$$

$$\sum_{x \in M} |\text{stab}_G(x)| = \sum_{\sigma \in G} |\text{fix}(\sigma)|$$

- 每个轨道对轨道数贡献为 1, 故  $x \in M$  对答案的贡献为  $\frac{1}{|\text{orb}_G(x)|}$  :

$$\begin{aligned} |M/G| &= \sum_{x \in M} \frac{1}{|\text{orb}_G(x)|} \\ &= \sum_{x \in M} \frac{|\text{stab}_G(x)|}{|G|} \quad (\text{轨道-稳定子定理}) \\ &= \frac{1}{|G|} \sum_{\sigma \in G} |\text{fix}(\sigma)| \end{aligned}$$



对正六边形的 6 个顶点，一半涂黑一半涂白。若经旋转可得到的方案算相同方案，求方案数？

对正六边形的 6 个顶点，一半涂黑一半涂白。若经旋转可得到的方案算相同方案，求方案数？

$$M = \{\text{不计同构的涂色方案}\} \quad |M| = \binom{6}{3} = 20$$

$$G = \{\text{顺时针旋转 } 0^\circ, 60^\circ, 120^\circ, 180^\circ, 240^\circ, 300^\circ\}$$

记 6 个顶点分别为  $A_1, A_2, \dots, A_6$

旋转  $0^\circ$

$$\begin{pmatrix} A_1 & A_2 & A_3 & A_4 & A_5 & A_6 \\ A_1 & A_2 & A_3 & A_4 & A_5 & A_6 \end{pmatrix}$$

将这一置换作用于  $M$  中的任意元素都不会使该元素发生变化，故不动元有 20 个。

旋转  $60^\circ$

$$\begin{pmatrix} A_1 & A_2 & A_3 & A_4 & A_5 & A_6 \\ A_6 & A_1 & A_2 & A_3 & A_4 & A_5 \end{pmatrix}$$

若要成为不动元，则应当满足：

$$A_1 = A_2 = \cdots = A_6$$

故没有不动元

旋转  $120^\circ$

$$\begin{pmatrix} A_1 & A_2 & A_3 & A_4 & A_5 & A_6 \\ A_5 & A_6 & A_1 & A_2 & A_3 & A_4 \end{pmatrix}$$

若要成为不动元，则应当满足：

$$A_1 = A_3 = A_5, A_2 = A_4 = A_6$$

故不动元数量为 2

旋转  $180^\circ$

$$\begin{pmatrix} A_1 & A_2 & A_3 & A_4 & A_5 & A_6 \\ A_4 & A_5 & A_6 & A_1 & A_2 & A_3 \end{pmatrix}$$

若要成为不动元，则应当满足：

$$A_1 = A_4, A_2 = A_5, A_3 = A_6$$

故没有不动元

- 旋转  $60^\circ$  与 旋转  $300^\circ$  情形相似;
- 旋转  $120^\circ$  与 旋转  $240^\circ$  情形相似。

$$\text{轨道数: } \frac{1}{6}(20 + 2 + 2) = 4$$

# PÓLYA 计数定理

- 将置换表示为若干轮换乘积，若轮换内元素颜色均相同即为不动元（这样才能保证每一个点变成新点后的颜色与原先一致）；
- 记染色可选的颜色数为  $m$ ， $c(\sigma)$  为置换  $\sigma$  被分解为不交轮换乘积的个数，则：



# PÓLYA 计数定理

- 将置换表示为若干轮换乘积，若轮换内元素颜色均相同即为不动元（这样才能保证每一个点变成新点后的颜色与原先一致）；
- 记染色可选的颜色数为  $m$ ， $c(\sigma)$  为置换  $\sigma$  被分解为不交轮换乘积的个数，则：

$$\text{fix}(\sigma) = m^{c(\sigma)}$$

# PÓLYA 计数定理

- 将置换表示为若干轮换乘积，若轮换内元素颜色均相同即为不动元（这样才能保证每一个点变成新点后的颜色与原先一致）；
- 记染色可选的颜色数为  $m$ ， $c(\sigma)$  为置换  $\sigma$  被分解为不交轮换乘积的个数，则：

$$|M/G| = \frac{1}{|G|} \sum_{\sigma \in G} m^{c(\sigma)}$$

# 小结

- 关系 | 等价关系 | 等价类
  - 对集合分类：等价类  $[a]$  内的元素都与存在  $a$  等价关系；
- 群 | 子群 | 陪集
  - 对群分类：陪集  $gH$  里的所有元素都与  $g$  存在等价关系；
- 群在集合上的作用
  - 轨道：  $M$  的子集，在  $G$  作用下与  $x$  等价的元素；
  - 稳定子：  $G$  的子群，对于  $x$  而言  $G$  中等价的置换；
  - 轨道-稳定子定理 | Burnside 引理 | Pólya 计数法

# 项链染色

长为  $n$  的环,  $m$  种颜色对环上元素染色, 经旋转或翻转都算作相同方案

$$n, m \leq 10^9$$

# 分析

$$G = \{ \text{顺时针旋转 } \frac{2\pi}{n}, \dots, (n-1)\frac{2\pi}{n}, 2\pi, \\ \text{过每一条对称轴的翻转} \}$$

$$M = \{ \text{不考虑同构的所有染色方案} \}$$

$$G \text{ 作用于 } M$$

# 分析

$$G = \{ \text{顺时针旋转 } \frac{2\pi}{n}, \dots, (n-1)\frac{2\pi}{n}, 2\pi, \\ \text{过每一条对称轴的翻转} \}$$

$$M = \{ \text{不考虑同构的所有染色方案} \}$$

$G$  作用于  $M$

$G$  中复合运算封闭吗?

若将环上的元素按顺时针编号： $0, 1, \dots, (n - 1)$

- 顺时针旋转  $k \frac{2\pi}{n}$ ： $\sigma_k(i) = (i + k) \bmod n$ ;
- 沿过点  $a$  的对称轴翻转：

$$\tau_a(i) = \begin{cases} i & i = a \text{ or } a \text{ 对面的点} \\ (2a - i) \bmod n & \text{otherwise} \end{cases}$$

若将环上的元素按顺时针编号： $0, 1, \dots, (n - 1)$

- 顺时针旋转  $k \frac{2\pi}{n}$ ： $\sigma_k(i) = (i + k) \bmod n$ ;
- 沿过点  $a$  的对称轴翻转：

$$\tau_a(i) = \begin{cases} i & i = a \text{ or } a \text{ 对面的点} \\ (2a - i) \bmod n & \text{otherwise} \end{cases}$$

- 注：若  $n$  为偶数，则翻转对称轴可能同时过两条边的中点。这等同于共有  $2n$  个点且不考虑此类对称轴的情况，故下面暂不考虑这种对称轴。



若将环上的元素按顺时针编号： $0, 1, \dots, (n - 1)$

- 顺时针旋转  $k \frac{2\pi}{n}$ ： $\sigma_k(i) = (i + k) \bmod n$ ;
- 沿过点  $a$  的对称轴翻转：

$$\tau_a(i) = \begin{cases} i & i = a \text{ or } a \text{ 对面的点} \\ (2a - i) \bmod n & \text{otherwise} \end{cases}$$

- 考虑  $i \neq a$  的情况 ( $i = a$  显然封闭) , 若  $2 \mid k$ :

$$\sigma_k \circ \tau_a \circ i = (2a - i + k) \bmod n = \tau_{(a + \frac{k}{2}) \bmod n} i$$

若将环上的元素按顺时针编号： $0, 1, \dots, (n - 1)$

- 顺时针旋转  $k \frac{2\pi}{n}$ ： $\sigma_k(i) = (i + k) \bmod n$ ;
- 沿过点  $a$  的对称轴翻转：

$$\tau_a(i) = \begin{cases} i & i = a \text{ or } a \text{ 对面的点} \\ (2a - i) \bmod n & \text{otherwise} \end{cases}$$

- 考虑  $i \neq a$  的情况 ( $i = a$  显然封闭) , 若  $2 \nmid k$ :

$$\sigma_k \circ \tau_a \circ i = (2a - i + k) \bmod n = \tau_{(a + \frac{n+k}{2})} \bmod n$$

# 旋转

- 旋转置换一共  $n$  种;
- 旋转  $\frac{2\pi}{n}$  时只能分解成一个不交轮换;
- 旋转  $i\frac{2\pi}{n}$  可看作前者的  $i$  次幂, 故可拆成  $\gcd(n, i)$  个轮换:

$$\sum_{\sigma} |\text{fix}(\sigma)| = \sum_{i=1}^n m^{\gcd(n, i)}$$

$$\begin{aligned}
\sum_{g \in G} | \operatorname{fix}(\sigma) | &= \sum_{i=1}^n m^{\operatorname{gcd}(n,i)} \\
&= \sum_{d|n} m^d \sum_{i=1}^n [\operatorname{gcd}(n, i) = d] \\
&= \sum_{d|n} m^d \sum_{i=1}^{\frac{n}{d}} [\operatorname{gcd}(\frac{n}{d}, i) = 1] \\
&= \sum_{d|n} m^d \cdot \varphi(\frac{n}{d})
\end{aligned}$$

# 翻转

- 翻转置换一共  $n$  种。
- $n$  为偶数：
  - $\frac{n}{2}$  条过点的对称轴:  $c(\tau) = \frac{n}{2} + 1$
  - $\frac{n}{2}$  条过边的对称轴:  $c(\tau) = \frac{n}{2}$

$$\sum_{\tau} |\text{fix}(\tau)| = \frac{n}{2} \cdot m^{\frac{n}{2}+1} + \frac{n}{2} \cdot m^{\frac{n}{2}}$$

- $n$  为奇数:

- $n$  条 既过点又过边的对称轴:  $c(\tau) = \frac{n+1}{2}$

$$\sum_{\tau} |\text{fix}(\tau)| = n \cdot m^{\frac{n+1}{2}}$$

# 结论

$$\begin{aligned} |M/G| &= \frac{\sum_{\sigma} |\text{fix}(\sigma)| + \sum_{\tau} |\text{fix}(\tau)|}{2n} \\ &= \frac{1}{2n} \sum_{d|n} m^d \cdot \varphi\left(\frac{n}{d}\right) \\ &\quad + \frac{1}{2n} \begin{cases} \frac{n}{2} \cdot m^{\frac{n}{2}+1} + \frac{n}{2} \cdot m^{\frac{n}{2}} & 2 \mid n \\ n \cdot m^{\frac{n+1}{2}} & 2 \nmid n \end{cases} \end{aligned}$$

复杂度:  $\mathcal{O}(d(n) \cdot \sqrt{n})$ ,  $d(n)$  代表  $n$  的约数个数。

# 南昌 J. SUMMON

现要从 4 种不同的水晶中取  $n$  个围成一个圈，但有  $m$  个限制条件：每条限制条件要求某四种水晶不能在围成的圈中连续出现。通过旋转可互相得到的方案算作一种方案，问有多少种本质不同的方案？（结果模 998244353）

$$n \leq 10^5, m \leq 256$$



# 分析

$$G = \{\text{顺时针旋转}\frac{2\pi}{n}, \dots, (n-1)\frac{2\pi}{n}, 2\pi\}$$

$$M = \{\text{满足限制且不计同构的染色方案}\}$$

# 分析

$$G = \{\text{顺时针旋转 } \frac{2\pi}{n}, \dots, (n-1)\frac{2\pi}{n}, 2\pi\}$$

$$M = \{\text{满足限制且不计同构的染色方案}\}$$

- 单单把每一个轮换内的所有元素染成相同颜色可能破坏限制条件;
- 无法直接应用 Pólya 计数定理。

- 旋转  $\frac{2\pi}{n}$  只能分解成一个不交轮换;
- 旋转  $i\frac{2\pi}{n}$  可看作前者的  $i$  次幂, 因此:
  - 可表示为  $\gcd(n, i)$  个不交轮换之积;
  - 标号模  $\gcd(n, i)$  结果相同的点在同一轮换内。

- 旋转  $\frac{2\pi}{n}$  只能分解成一个不交轮换;
- 旋转  $i\frac{2\pi}{n}$  可看作前者的  $i$  次幂, 因此:
  - 可表示为  $\gcd(n, i)$  个不交轮换之积;
  - 标号模  $\gcd(n, i)$  结果相同的点在同一轮换内。

**对于旋转  $i\frac{2\pi}{n}$  这一置换, 只需确定前  $\gcd(n, i)$  个元素的颜色即可知道该置换下不动元数量!**

## DP 求不动元数量

- 记  $v\langle a, b, c, d \rangle$  代表是否允许  $a, b, c, d$  四种颜色相邻;

$$v\langle a, b, c, d \rangle = \begin{cases} 0 & \text{不允许 } a, b, c, d \text{ 相邻} \\ 1 & \text{允许 } a, b, c, d \text{ 相邻} \end{cases}$$

- 记  $\text{dp}\langle i, a, b, c \rangle$  代表  $i$  个元素排成一排, 最后 3 个元素的颜色分别为  $a, b, c$  的方案数:

$$\text{dp}\langle i, a, b, c \rangle = \sum_k v\langle k, a, b, c \rangle \cdot \text{dp}\langle i - 1, k, a, b \rangle$$

- 记  $\text{dp}\langle i, a, b, c \rangle$  代表  $i$  个元素排成一排，最后 3 个元素的颜色分别为  $a, b, c$  的方案数：

$$\text{dp}\langle i, a, b, c \rangle = \sum_k v\langle k, a, b, c \rangle \cdot \text{dp}\langle i - 1, k, a, b \rangle$$

- 枚举前 3 个元素的颜色  $\langle a, b, c \rangle$  :
  - 只初始化  $\text{dp}\langle 3, a, b, c \rangle = 1$ ;
  - $\text{dp}\langle m + 3, a, b, c \rangle$  即为  $m$  个元素围成环时不动元方案数。

# 矩阵快速幂优化 DP

$$\text{dp}\langle i, a, b, c \rangle = \sum_k \mathbf{v}\langle k, a, b, c \rangle \cdot \text{dp}\langle i - 1, k, a, b \rangle$$

$$\begin{bmatrix} \text{dp}\langle i, 1, 1, 1 \rangle \\ \text{dp}\langle i, 1, 1, 2 \rangle \\ \vdots \\ \text{dp}\langle i, 4, 4, 4 \rangle \end{bmatrix} = T \cdot \begin{bmatrix} \text{dp}\langle i - 1, 1, 1, 1 \rangle \\ \text{dp}\langle i - 1, 1, 1, 2 \rangle \\ \vdots \\ \text{dp}\langle i - 1, 4, 4, 4 \rangle \end{bmatrix}$$



# 矩阵快速幂优化 DP

$$\text{dp}\langle i, a, b, c \rangle = \sum_k \mathbf{v}\langle k, a, b, c \rangle \cdot \text{dp}\langle i - 1, k, a, b \rangle$$

$$\begin{bmatrix} \text{dp}\langle i, 1, 1, 1 \rangle \\ \text{dp}\langle i, 1, 1, 2 \rangle \\ \vdots \\ \text{dp}\langle i, 4, 4, 4 \rangle \end{bmatrix} = T \cdot \begin{bmatrix} \text{dp}\langle i - 1, 1, 1, 1 \rangle \\ \text{dp}\langle i - 1, 1, 1, 2 \rangle \\ \vdots \\ \text{dp}\langle i - 1, 4, 4, 4 \rangle \end{bmatrix}$$

$$\text{dp}\langle i, a, b, c \rangle = \sum_{\langle j, k, l \rangle} T[a, b, c][j, k, l] \cdot \text{dp}\langle i - 1, j, k, l \rangle$$

# 矩阵快速幂优化 DP

$$\text{dp}\langle i, a, b, c \rangle = \sum_k \mathbf{v}\langle k, a, b, c \rangle \cdot \text{dp}\langle i - 1, k, a, b \rangle$$

$$\begin{bmatrix} \text{dp}\langle i, 1, 1, 1 \rangle \\ \text{dp}\langle i, 1, 1, 2 \rangle \\ \vdots \\ \text{dp}\langle i, 4, 4, 4 \rangle \end{bmatrix} = T \cdot \begin{bmatrix} \text{dp}\langle i - 1, 1, 1, 1 \rangle \\ \text{dp}\langle i - 1, 1, 1, 2 \rangle \\ \vdots \\ \text{dp}\langle i - 1, 4, 4, 4 \rangle \end{bmatrix}$$

$$T[a, b, c][k, a, b] = \mathbf{v}\langle k, a, b, c \rangle$$

- 枚举前三 3 个元素的颜色  $\langle a, b, c \rangle$  时, 初始化:

$$\begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{bmatrix}, \dots, \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix}$$

- 等价于  $T^n$  直接乘上单位矩阵;
- $T^n$  主对角线元素之和即为所有不动元数量。

# 结论

- 记  $T^i$  对角线元素之和为  $f(i)$
- 旋转  $i \frac{2\pi}{n}$  下不动元个数为  $f(\gcd(n, i))$

# 结论

$$\begin{aligned}\sum_{\sigma \in G} |\text{fix}(\sigma)| &= \sum_{i=1}^n f(\gcd(n, i)) \\ &= \sum_{d|n} f(d) \cdot \sum_{i=1}^n [\gcd(n, i) = d] \\ &= \sum_{d|n} f(d) \cdot \varphi\left(\frac{n}{d}\right)\end{aligned}$$

- 复杂度:  $\mathcal{O}(d(n) \cdot 64^3 \log n)$ , 其中  $d(n)$  代表  $n$  的约数个数。

# 无向图同构计数

$n$  个点无向完全图,  $m$  种颜色给边染色, 求本质不同的染色方案数。

$$n \leq 60, m \leq 10^3$$

# 无向图同构计数

$n$  个点无向完全图,  $m$  种颜色给边染色, 求本质不同的染色方案数。

$$n \leq 60, m \leq 10^3$$

- 两张图若**对点重标号**后可以重合即为同构;
- 把边的不存在当作一种颜色可将其推广至一般无向图同构。

# 分析

$G = S_n$  ( $n$ 阶对称群),  $|S_n| = n!$

$M = \{\text{不计同构的无向图染色方案}\}$

- 置换是对点的置换，而染色是对边染色；
- 两点确定一条边，分析边两端点的情况。



# 两端在同一轮换内的边

$$\sigma = (1 \ 3 \ 5 \ 6) \cdot (2 \ 4)$$

# 两端在同一轮换内的边

$$\sigma = (1 \ 3 \ 5 \ 6) \cdot (2 \ 4)$$

- 对于两端点位于同一点轮换内的边：
  - $\langle 1, 3 \rangle \rightarrow \langle 3, 5 \rangle \rightarrow \langle 5, 6 \rangle \rightarrow \langle 6, 1 \rangle$
  - $\langle 1, 5 \rangle \rightarrow \langle 3, 6 \rangle$
  - $\langle 2, 4 \rangle$

$$(a_0 \ a_1 \ \dots \ a_{l-1})$$

$$\langle a_i, a_j \rangle \longrightarrow \langle a_{(i+1) \bmod l}, a_{(j+1) \bmod l} \rangle \longrightarrow \dots$$

$$(a_0 \ a_1 \ \dots \ a_{l-1})$$

$$\langle a_i, a_j \rangle \rightarrow \langle a_{(i+1) \bmod l}, a_{(j+1) \bmod l} \rangle \rightarrow \dots$$

$$\begin{cases} i + t \equiv i \pmod{l} \\ j + t \equiv j \pmod{l} \end{cases}$$

$$(a_0 \ a_1 \ \dots \ a_{l-1})$$

$$\langle a_i, a_j \rangle \rightarrow \langle a_{(i+1) \bmod l}, a_{(j+1) \bmod l} \rangle \rightarrow \dots$$

$$t \equiv 0 \pmod{m}$$

最小正整数解  $t = l$ , 则边轮换长度至多为  $l$ 。

$$(a_0 \ a_1 \ \dots \ a_{l-1})$$

$$\langle a_i, a_j \rangle \longrightarrow \langle a_{(i+1) \bmod l}, a_{(j+1) \bmod l} \rangle \longrightarrow \dots$$

$$(a_0 \ a_1 \ \dots \ a_{l-1})$$

$$\langle a_i, a_j \rangle \longrightarrow \langle a_{(i+1) \bmod l}, a_{(j+1) \bmod l} \rangle \longrightarrow \dots$$

$$\begin{cases} i + t \equiv j \pmod{l} \\ j + t \equiv i \pmod{l} \end{cases}$$

$$(a_0 \ a_1 \ \dots \ a_{l-1})$$

$$\langle a_i, a_j \rangle \rightarrow \langle a_{(i+1) \bmod l}, a_{(j+1) \bmod l} \rangle \rightarrow \dots$$

$$2i \equiv 2j \pmod{m}$$

- 若  $2 \nmid l$ , 则  $i \equiv j \pmod{l}$ , 无法构成边;
- 若  $2 \mid l$ , 则  $i \equiv j \pmod{\frac{l}{2}}$ , 最小非负  $t = \frac{l}{2}$ 。



$$(a_0 \ a_1 \ \dots \ a_{l-1})$$

- 对于边  $\langle a_i, a_j \rangle$  所在的边轮换：
  - 若  $2 \mid l$  且  $|j - i| = \frac{l}{2}$ , 则其大小为  $\frac{l}{2}$ ;
  - 否则其大小为  $l$ ;
- $|j - i| \bmod l$  相同的边在同一边轮换内, 故边轮换个数为  $\lfloor \frac{l}{2} \rfloor$ 。

# 两端在不同轮换内的边

$$\sigma = (1\ 3\ 5\ 6) \cdot (2\ 4)$$

- 两点在不同点轮换里的边：
  - $\langle 1, 2 \rangle \rightarrow \langle 3, 4 \rangle \rightarrow \langle 5, 2 \rangle \rightarrow \langle 6, 4 \rangle$
  - $\langle 1, 4 \rangle \rightarrow \langle 3, 2 \rangle \rightarrow \langle 5, 4 \rangle \rightarrow \langle 6, 2 \rangle$

$$(a_0 \ a_1 \ \dots \ a_{l-1}) \cdot (b_0 \ b_1 \ \dots \ b_{s-1})$$

$$\langle a_i, b_j \rangle \longrightarrow \langle a_{(i+1) \bmod l}, b_{(j+1) \bmod s} \rangle \longrightarrow \dots$$

$$(a_0 \ a_1 \ \dots \ a_{l-1}) \cdot (b_0 \ b_1 \ \dots \ b_{s-1})$$

$$\langle a_i, b_j \rangle \rightarrow \langle a_{(i+1) \bmod l}, b_{(j+1) \bmod s} \rangle \rightarrow \dots$$

$$\begin{cases} i + t \equiv i \pmod{l} \\ j + t \equiv j \pmod{s} \end{cases}$$

- 每个边轮换大小为  $\text{lcm}(l, s)$ , 共  $\frac{ls}{\text{lcm}(l, s)} = \text{gcd}(l, s)$  个。

# 点轮换与边轮换的关系

$$\sigma = \prod_{i=1}^k c_i \quad (\text{轮换 } c_i \text{ 长度为 } l_i)$$

- 可表示成边轮换的个数:

$$\sum_{i=1}^k \left\lfloor \frac{l_i}{2} \right\rfloor + \sum_{i=1}^k \sum_{j=i+1}^k \gcd(l_i, l_j)$$

# 点轮换与边轮换的关系

$$\sigma = \prod_{i=1}^k c_i \quad (\text{轮换 } c_i \text{ 长度为 } l_i)$$

- 可表示成边轮换的个数:

$$\sum_{i=1}^k \left\lfloor \frac{l_i}{2} \right\rfloor + \sum_{i=1}^k \sum_{j=i+1}^k \gcd(l_i, l_j)$$

- 不动元? 每个边轮换内的边染色情况应当相同;
- $|S_n| = n!$ , 没办法枚举每一个置换.....

# 点轮换与边轮换的关系

$$\sigma = \prod_{i=1}^k c_i \quad (\text{轮换 } c_i \text{ 长度为 } l_i)$$

- 可表示成边轮换的个数:

$$\sum_{i=1}^k \left\lfloor \frac{l_i}{2} \right\rfloor + \sum_{i=1}^k \sum_{j=i+1}^k \gcd(l_i, l_j)$$

- 边轮换的个数只跟每个点轮换的大小有关系;
- 枚举点轮换大小的情况 ( $n$  的拆分方案) ?

# 剪枝

- 枚举  $n$  的拆分方案:

$$n = \sum_{i=1}^k l_i \quad (l_1 \leq l_2 \leq \cdots \leq l_k)$$

- 每一种拆分方案对应多少点置换?



- $n$  个点分配到轮换内（多重组合数）：

$$\frac{n!}{\prod_{i=1}^k l_i!}$$

- 再考虑轮换内的顺序（圆排列）：
  - 比如 (1 2 3) 和 (1 3 2) 算不同的置换

$$\frac{n!}{\prod_{i=1}^k l_i!} \cdot \prod_{i=1}^k (l_i - 1)!$$

- 对于长度相等的轮换，其之间的顺序不计。
  - 记共有  $s$  种不同长度的轮换，其中第  $i$  种轮换的长度为  $q_i$ ，则：

$$\frac{n!}{\prod_{i=1}^k l_i} \cdot \prod_{i=1}^s \frac{1}{q_i!}$$

# 结论

- 对  $n$  的每一种拆分方案:  $n = \sum_{i=1}^k l_i$ 
  - $l_1 \leq l_2 \leq \cdots \leq l_k$ ;
  - 记共有  $s$  种不同长度的轮换, 其中第  $i$  种轮换的长度为  $q_i$ ;
  - 其对应的点轮换数量为:

$$\frac{n!}{\left(\prod_{i=1}^k l_i\right) \cdot \left(\prod_{i=1}^s q_i!\right)}$$

$$\frac{1}{|G|} \sum_{\sigma \in G} |\text{fix}(\sigma)|$$

$$= \frac{1}{n!} \cdot \sum \frac{n!}{\left(\prod_{i=1}^k l_i\right) \cdot \left(\prod_{i=1}^s q_i!\right)} \cdot m^{\sum_{i=1}^k \left\lfloor \frac{l_i}{2} \right\rfloor + \sum_{i=1}^k \sum_{j=i+1}^k \text{gcd}(l_i, l_j)}$$

- 复杂度  $\mathcal{O} \left( \sum_{p \in \text{Partition}(n)} \text{len}^2(p) \cdot \log n \right)$
- 其实题目数据范围内  $\text{Partition}(n)$  大小不大.....所以  $\mathcal{O}$ (能过)。

## 思路回顾

- 置换是对点的置换，均可分解成点轮换之积；
- 染色对边染色，同一边轮换内边染色方案相同；
- 点轮换和边轮换之间的关系？
- 只关心边轮换个数，其只与点轮换的大小情况有关，枚举点轮换的大小情况.....

谢谢大家

# 相关题目 #1

- HDU 1817: Necklace of Beads
- HDU 3547: DIY Cube
- HDU 3441: Rotation
- POJ 2888: Magic Bracelet
- 洛谷 P1446: Cards



## 相关题目 #2

- 洛谷 P4128: 有色图
- ICPC 2014 鞍山 K: Colorful Toy
- HDU 6360: Kaleidoscope
- ICPC 2019 南昌 J: Summon
- ICPC 2019 银川 M: Crazy Cake

# 参考资料

- 近世代数引论/冯克勤,李尚志,章璞编著.-3版.-合肥: 中国科学技术大学出版社,2009.12
- 近世代数初步/石生明.-2版.-北京: 高等教育出版社,2006.3
- Contemporary Abstract Algebra/Joseph A. Gallian.-8th Edition
- 群论初探 - nosta - 博客园