群论计数基础

x义x

HZXJHS

YYYY/MM/DD

头像的天线少了一根，不要在意（

目录

引言

只是主要课件的前置知识，不会讲的很深

引言

只是主要课件的前置知识，不会讲的很深

~~很深：比如什么给指导最喜欢的计算群论~~

群的定义

一个元素集合 G 和它上面的一个二元运算 $\times$，如果满足下面的性质，$(G, \times)$ 即可称为一个群。

群的定义

一个元素集合 G 和它上面的一个二元运算 $\times$，如果满足下面的性质，$(G, \times)$ 即可称为一个群。

- **封闭性**。$\forall a, b \in G, (a \times b) \in G$。说人话就是 G 内部的元素乘不出 G 外的元素。

群的定义

一个元素集合 G 和它上面的一个二元运算 $\times$，如果满足下面的性质，$(G, \times)$ 即可称为一个群。

- **封闭性**。$\forall a, b \in G, (a \times b) \in G$。说人话就是 G 内部的元素乘不出 G 外的元素。

- **结合律**。$(a \times b) \times c = a \times (b \times c)$。

群的定义

一个元素集合 G 和它上面的一个二元运算 $\times$，如果满足下面的性质，$(G,\times)$ 即可称为一个群。

- **封闭性**。$\forall a,b\in G,(a\times b)\in G$。说人话就是 G 内部的元素乘不出 G 外的元素。

- **结合律**。$(a\times b)\times c=a\times(b\times c)$。

- **存在单位元**。$\exists e\in G,\forall a\in G,a\times e=e\times a=a$。注意这**不**意味着 $\times$ 有交换律。立即得到其唯一性（$e_1\times e_2=e_1=e_2$）。

群的定义

一个元素集合 G 和它上面的一个二元运算 $\times$，如果满足下面的性质，$(G, \times)$ 即可称为一个群。

- **封闭性**。$\forall a, b \in G, (a \times b) \in G$。说人话就是 G 内部的元素乘不出 G 外的元素。

- **结合律**。$(a \times b) \times c = a \times (b \times c)$。

- **存在单位元**。$\exists e \in G, \forall a \in G, a \times e = e \times a = a$。注意这不意味着 $\times$ 有交换律。立即得到其唯一性（$e_1 \times e_2 = e_1 = e_2$）。

- **存在逆**。对于 $a \in G, \exists a^{-1} \in G, a \times a^{-1} = a^{-1} \times a = e$。立即得到其唯一性（$a_1^{-1} \times a \times a_2^{-1} = a_1^{-1} = a_2^{-1}$）。

太抽象了，举点例子

$\mathbb{Z}$ 连带加法构成一个群。

- 封闭性很直观。证明只需数学归纳法，不表。

- 结合律显然。事实上加法还具有交换律，这使得它成为一个交换群。

- 单位元是 0。

- 元素的逆即为其相反数。（$\mathbb{N}$ 连带加法不成为一个群，因为除了 0 的元素都没有逆。）

再举点例子

$\mathbb{Z}/\{0\}$ 连带乘法构成一个群。

$\mathbb{N}$ 连带异或构成一个群。值得注意的是任何元素的逆是它自身。

n 阶矩阵连带矩阵乘法构成一个群。值得注意的是它没有交换律。

重头戏：置换群

置换群的元素都是**置换**。置换可以看成一个函数，定义域为 $[1..n]$，取值恰好构成一个排列。一个排列构成一个置换。

一般把置换 f 写为

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

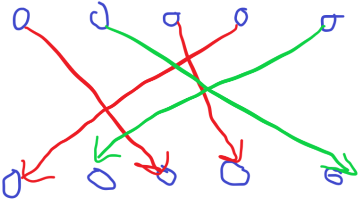
置换群的运算是置换的复合，$(f \times g)(i) = f(g(i))$。显然没有交换律。

循环拆分

我们知道，对于置换，一个经典的描述方法是把它看成一个二分图。比如置换

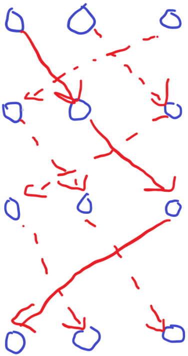
$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix}$$

就可以画为



循环拆分

我们注意到一些特殊的结构。如果只关注 $1, 3, 4$，那么我们重复这个置换 3 次，它会把 $1, 3, 4$ 都回到自身。



事实上，如果连边 $(1, f(1)), (2, f(2)), \ldots, (n, f(n))$，类似的结构会成为一个环，称为**循环**。

循环拆分

容易证明任何置换都可以被拆分为数个循环（可以是自环），这就是这个置换的**循环拆分**。对于刚才的例子，我们可以把这个置换写为

$$(134)(25)$$

注意，$(341)(25), (134)(52), (25)(134)$ 之类的表达也可以。但是 $(143)(25)$ 是不可以的，循环虽然没有起点但是有方向之分。

本质相同，等价类

研究置换群的意义在于它可以描述一类我们常说的“本质相同”。

考虑一类从 $\mathcal{M}$ 到 $\mathcal{B}$ 的映射，记为 $X = \mathcal{B}^{\mathcal{M}}$，称作**染色**。不妨认为 $\mathcal{M} = [1..n]$。

两个**染色** $\phi_1, \phi_2 \in X$ 被认为**本质相同**，如果存在映射 $g \in G, \phi_1 \circ g = \phi_2$。一系列两两本质相同的染色构成的集合称为**等价类**。等价类的集合称为 X/G。

Burnside 引理

等价类的数量等于各置换不动点数量的平均值。

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

其中 X^g 是 g 的不动点的集合，即 $\{x|x \in X, g \circ x = x\}$。

Pólya 定理：当 $\mathcal{B} = [1..c]$，$|X^g| = c^{g\text{的循环数}}$。

结语

啊这好像讲完了

下个课件见