Chapter 5 Pólya计数定理

目录

我们用一个简单的问题引出我们所要讨论的内容.

例 1 在苯环的每个碳原子处连上氢原子或甲基可以得到一些分子. 在相同的化学条件下可以得到多少个不同的分子?

读者易于枚举得到结果. 事实上本问题的困难之处在于, 如何判断两个"分子"在化学条件下是否相同. 或者说, 我们打破各点"对称性"后, 得到的哪些分子属于同一类, 如此进行分类的依据又是什么. 读者在思考后可能会得到对称, 旋转之类的答案. 下面我们从群的作用的方面具体地讨论.

1 置换群, 群在集合上的作用

1.1 置换群和轮换指标

定义 1 设$[n]=\{1,2,\ldots,n\}$, $[n]$到自身的一个双射称为$[n]$上的一个**置换**. $[n]$上的两个置换的乘积定义为它们的映射合成. $[n]$上的全体$n!$个置换在这样的乘法下构成一个群, 称为$[n]$上的(或n元)**对称群**, 记作S_n, 对称群的子群称为**置换群**.

我们举几个简单的例子.

例 2 对于$i,j=1,2,\ldots,n$, 定义$[n]$上的映射σ_i,τ_j如下:

$$\begin{aligned}\sigma_i(a)&=a+i\,(mod n),\\ \tau_j(a)&=-a+j\,(mod n),\end{aligned}\qquad a\in[n],$$

即σ_i,τ_j为$[n]$上的变量系数为1和-1的全体线性函数. 记

$$D_n=\left\{\sigma_i,\tau_j\mid i,j=1,2,\ldots,n\right\},$$

则D_n对置换的乘法封闭, 它是S_n的一个子群, 即$[n]$上的一个置换群, 称其为$[n]$上的**二面体群**. $\{\sigma_i\mid i=1,2,\ldots,n\}$也是$[n]$上的一个置换群, 它是由$\sigma_1$生成的循环群.

例 3 设$G=(V,E)$是一个图, G的一个自同构σ是顶点集V上的置换, 且满足对任意$x,y\in V,\{x,y\}\in E$当且仅当$\{\sigma(x),\sigma(y)\}\in E$. 图$G$的所有自同构在映射合成运算下构成一个群, 称为图$G$的**全自同构群**, 记为$\mathrm{Aut}(G)$.

用C_n表示n个顶点的圈图(即一个n边形图), 则它的全自同构群$\mathrm{Aut}(C_n) = D_n$. 事实上, 用$[n]$中的元素来表示C_n的顶点, 则对于顶点a, b, $\{a, b\}$为一条边, 或记为$a \sim b$, 当且仅当$a - b = \pm 1$. 首先容易验证

$$a \sim b \Leftrightarrow \sigma_i(a) \sim \sigma_i(b), \tau_j(a) \sim \tau_j(b) \Leftrightarrow \sigma_i, \tau_j \in \mathrm{Aut}(C_n).$$

另一方面, 任取$\pi \in \mathrm{Aut}(C_n)$, 设$\pi(1) = i$, 因为$1 \sim 2$, 有

$$\pi(2) = i + 1 \text{或} \pi(2) = i - 1.$$

从而归纳可证$\forall a \in [n], \pi(a) = a + (i-1)$或$\pi(a) = -a + (i+1)$. 从而$\pi \in D_n$. 故$\mathrm{Aut}(C_n) = D_n$.

其实自同构σ_i相当于正n边形绕其中心O沿逆时针方向旋转$\frac{2i\pi}{n}$角度, 自同构τ_j相当于此正n边形以直线L_j为轴作一次翻转, 其中当$j = 2t+1$是L_j是点O与边$\{t, t+1\}$中点的连线; 当$j = 2t$时L_j时点O与顶点t的连线.

我们下面用一类特殊置换的乘积来表示置换群里所有的置换.

定义 2 若置换群中一个置换σ满足

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

而

$$\sigma(j) = j, \forall j \neq i_1, \ldots, i_k,$$

则称σ为一个k-**轮换**, 记为$\sigma = (i_1 i_2 \ldots i_k)$.

置换群理论中一个熟知的基本事实是:$[n]$上人一个置换都可以表示为$[n]$中全部字符都出现的两两无公共字符的轮换的乘积, 且这种表示方式除了轮换的次序外是唯一的. 对$\sigma \in S_n$, 用$l_i(\sigma)$表示σ的轮换分解中i-轮换的个数, 则称$(l_1(\sigma), l_2(\sigma), \ldots, l_n(\sigma))$为$\sigma$的**轮换型号**(简称**型号**), 记为$\mathrm{type}(\sigma)$. 在上下文清楚的情况下, 也可吧$\sigma$的型号记为$(l_1, \ldots, l_n)$. 显然有

$$1 \cdot l_1(\sigma) + 2 \cdot l_2(\sigma) + \ldots + n \cdot l_n(\sigma) = n,$$

σ的轮换分解式中轮换的个数为$l_1(\sigma) + l_2(\sigma) + \ldots + l_n(\sigma)$.

定理 1 *(Cauchy*公式*)*对称群S_n中型号为$(l_1, \ldots, l_n)$的置换个数为

$$\frac{n!}{l_1! \ldots l_n! 1^{l_1} 2^{l_2} \ldots n^{l_n}}.$$

其证明我们在第一章例5中给出.

定义 3 设G是一个n元置换群, 定义G的**轮换指标**为变量$x_1,\ldots,x_n$的一个多项式

$$P_G(x_1,\ldots,x_n)=\frac{1}{|G|}\sum_{\sigma\in G}x_1^{l_1(\sigma)}x_2^{l_2(\sigma)}\ldots x_n^{l_n(\sigma)}.$$

例 4 由于

$$S_1=\{(1)\},S_2=\{(1)(2),(12)\},$$
$$S_3=\{(1)(2)(3),(12)(3),(13)(2),(23)(1),(123),(132)\}$$

所以

$$P_{S_1}(x_1)=x_1,P_{S_2}(x_1,x_2)=\frac{1}{2}\left(x_1^2+x_2\right),P_{S_3}(x_1,x_2,x_3)=\frac{1}{6}\left(x_1^3+3x_1x_2+2x_3\right).$$

例 5 设$\sigma=(12\ldots n)$, 求由σ生成的n阶循环群$\langle\sigma\rangle$的轮换指标.

解 1 $\langle\sigma\rangle=\left\{\sigma,\sigma^2,\ldots,\sigma^n\right\}$, 对$1\le k\le n$, 记$\gcd(k,n)$为$k$和$n$的最大公因数. 下计算type$\left(\sigma^k\right)$. 因为$\sigma$是一个$n$-轮换, 故当$\gcd(k,n)=1$时, σ^k也是一个n-轮换. 而当$k\mid n$时, σ^k是k个$\frac{n}{k}$轮换之积. 一般情形下, 设$d=\gcd(k,n)$, 则$\sigma^k=\left(\sigma^d\right)^{\frac{k}{d}}$. 由于$d\mid n$, σ^d是d个$\frac{n}{d}$-轮换的乘积. 又$\gcd\left(\frac{n}{d},\frac{k}{d}\right)=1$, 所以$\sigma^k=\left(\sigma^d\right)^{\frac{k}{d}}$仍是$d$个$\frac{n}{d}$-轮换的乘积. 故

$$l_i\left(\sigma^k\right)=\begin{cases}0, & i\ne\frac{n}{d},\\ d, & i=\frac{n}{d},\end{cases}$$

其中$d=\gcd(k,n)$. 所以

$$P_{\langle\sigma\rangle}(x_1,x_2,\ldots,x_n)=\frac{1}{n}\sum_{k-1}^{n}\left(x_{\frac{n}{\gcd(k,n)}}\right)^{\gcd(k,n)}.$$

由于满足$1\le k\le n$且$\gcd(k,n)=d$的正整数k的个数即为满足$1\le\frac{k}{d}\le\frac{n}{d}$且$\gcd\left(\frac{k}{d},\frac{n}{d}\right)=1$的正整数$\frac{k}{d}$的个数, 即为$\phi\left(\frac{n}{d}\right)$, 其中$\phi$为*Euler*函数, 因此

$$P_{\langle\sigma\rangle}(x_1,x_2,\ldots,x_n)=\frac{1}{n}\sum_{d\mid n}\phi\left(x_{\frac{n}{d}}\right)^d=\frac{1}{n}\sum_{j\mid n}\phi(j)^{x_j^{\frac{n}{j}}}.$$

例 6 考虑三维空间中正方体C的旋转群, 记为G, 即G是由三维空间中使正方体C变为自身的所有旋转组成的群. G中旋转有以下*5*类:

*(1)*单位元, 只有一个.

*(2)*绕C的相对两面中点的连线旋转180°, 这样的旋转有*3*个.

(3)绕C的相对两面的中点旋转90°, 因为有三对面, 左右两个方向, 故这样的旋转有6个.

(4)绕C的相对两棱的中点旋转180°, 这样的旋转有6个.

(5)绕C的相对两顶点连线旋转120°. 因为有左右两个方向, 4对顶点, 故这样的旋转有8个.

旋转群G诱导了正方体C的顶点集上的一个置换群G_1, C的棱集上的一个置换群G_2和C的面集上的一个置换群G_3, 可分别求得它们的轮换指标为

$$P_{G_1}(x_1,x_2,\ldots,x_8)=\frac{1}{24}\left(x_1^8+9x_2^4+6x_4^2+8x_1^2x_3^2\right),$$
$$P_{G_2}(x_1,x_2,\ldots,x_{12})=\frac{1}{24}\left(x_1^{12}+3x_2^6+8x_3^4+6x_4^3+6x_1^2x_2^5\right),$$
$$P_{G_3}(x_1,x_2,\ldots,x_6)=\frac{1}{24}\left(x_1^6+6x_2^3+8x_3^2+3x_1^2x_2^2+6x_1^2x_4\right).$$

定理 2 对称群S_n的轮换指标的普通生成函数为

$$\sum_{n=0}^{\infty}P_{S_n}(x_1,x_2,\ldots,x_n)\,t^n=\mathrm{e}^{t\frac{x_1}{1}+t^2\frac{x_2}{1}+\ldots+t^n\frac{x_n}{n}+\cdots}.$$

证明 1 由定义有

$$\begin{aligned}
&\sum_{n=0}^{\infty}P_{S_n}(x_1,x_2,\ldots,x_n)\,t^n=\sum_{n=0}^{\infty}\frac{t^n}{n!}\sum_{\sigma\in S_n}x_1^{l_1(\sigma)}x_2^{l_2(\sigma)}\ldots x_n^{l_n(\sigma)}\\
&=\sum_{n=0}^{\infty}\frac{t^n}{n!}\sum_{l_1+2l_2+\ldots+nl_n=n}\frac{n!}{1!2!\ldots n!1^{l_1}2^{l_2}\ldots n^{l_n}}x_1^{l_1}x_2^{l_2}\ldots x_n^{l_n}\\
&=\sum_{n=0}^{\infty}\sum_{l_1+2l_2+\ldots+nl_n=n}\frac{1}{1!2!\ldots n!1^{l_1}2^{l_2}\ldots n^{l_n}}(tx_1)^{l_1}\left(t^2x_2\right)^{l_2}\ldots(t^nx_n)^{l_n}\\
&=\sum_{l_1,l_2,\ldots,l_n,\ldots}\frac{1}{l_1!}\left(t\frac{x_1}{1}\right)\frac{1}{l_2!}\left(t^2\frac{x_2}{2}\right)\ldots\frac{1}{l_n!}\left(t^n\frac{x_n}{n}\right)\ldots\\
&=\sum_{l_1}\frac{1}{l_1!}\left(t\frac{x_1}{1}\right)\sum_{l_2}\frac{1}{l_2!}\left(t^2\frac{x_2}{2}\right)\ldots\sum_{l_n}\frac{1}{l_n!}\left(t^n\frac{x_n}{n}\right)\ldots\\
&=\mathrm{e}^{t\frac{x_1}{1}}\mathrm{e}^{t^2\frac{x_2}{2}}\ldots\mathrm{e}^{t^n\frac{x_n}{n}}\ldots.
\end{aligned}$$

1.2 群在集合上的作用

群在集合上的作用涉及部分抽象代数内容. 读者可以通过阅读附录了解一些抽象代数的简单知识, 从而便于理解下述内容.

定义 4 设G为一个群, X为一个集合, 所谓G在X上的一个**作用**指的是一个映射

$$G \times X \to X \quad (g, x) \to gx\,(g\,(x)),$$

满足$\mathrm{e}x = x$和$(g_1 g_2)\,x = g_1\,(g_2 x)$, 其中$\mathrm{e}$为群$G$的单位元, g_1, g_2为G中任意元素, x为X中任意元素.

等价地说, 群G在X上的一个作用也是G到X上的全变换群S_X的一个同态. 在这个同态下, G中每个元素的像是集合X上的一个置换, 所以有时也称G是作用在X上的一个置换群.

设G作用在X上, 对于$x \in X$, 称X的子集$O_x = \{gx \mid g \in G\}$为$x$**在$G$作用下的轨道**或过$x$的**$G$-轨道**(简称为**轨道**). 在$X$上定义关系~如下: 对$x, y \in X$, $x \sim y$当且仅当存在$g \in G$使得$y = gx$, 即$y \in O_x$. 容易验证~是X上的一个等价关系, 其等价类恰为O_x, 故有下述关于轨道的性质

(1)对$x, y \in X$, $x \sim y$当且仅当$O_x = O_y$;

(2)对$\forall x, y \in X$,, O_x与O_y相等或不交;

(3)在X的每一条轨道上取一个元素组成X的一个子集I, 称为X的轨道代表元集, 则$X = \bigcup_{x \in I} O_x$, 且这个并为不交并, 即给出了集合$X$的一个划分.

若G在X上的作用只有一个轨道, 即存在$x \in X$, 使得$X = O_x$, 则称这个作用**传递**. 进一步地, 若G在X上地作用传递, 且对任意$g \in G$, 有$g \neq e$, 以及任意$x \in X$, 有$gx \neq x$, 即G中非单位元没有不动点, 则称G在X上的作用在**正则**.

设群G作用在X上, 对于$x \in X$, 定义

$$G_x = \{g \in G \mid gx = x\},$$

称为群G作用下x的**稳定化子**. 容易验证, G_x为G的子群, 且过x的轨道O_x的长度(即$|O_x|$)等于G_x在G中的指数, 即$|O_x| = [G : G_x] = |G| \,/\, |G_x|$(假设$G$为有限的). 事实上, 取

$$H = \{gG_X \mid g \in G\},$$

即子群G_x在G中的全体左陪集所组成的集合, 定义$\phi : H \to O_x$为$\phi\,(gG_x) = gx$, 则ϕ为双射, 于是$|O_x| = |H|$. 显然, 若G在X上的作用正则, 则对任意$x \in X$, 有$G_x = \{\mathrm{e}\}$. 又$X = O_x$, 故$|G| = |X|$.

定理 3 ***Burnside*引理** 设群G作用在X上, 对于$g \in G$, 用$\psi\,(g) = \{x \in X \mid gx = x\}$表示被$g$固定的$X$中点的集合, 则$G$作用的轨道个数为

$$\frac{1}{|G|} \sum_{g \in G} |\psi\,(g)|.$$

证明 2 计算有序对(g,x)的个数, 其中$g \in G, x \in X$, 且$g(x) = x$. 一方面这个数为$\sum_{g\in G} |\varphi(g)|$; 另一方面, 对$x \in X$, 有$|G_x|$个$g \in G$固定$x$. 所以这个数又等于$\sum_{x\in X} |G_x|$. 由于$|G_x| = |G| / |O_x|$, 故

$$\sum_{g\in G} |\psi(g)| = \sum_{x\in X} |G_x| = |G| \sum_{x\in X} \frac{1}{|O_x|}.$$

又因G的轨道划分了X, 且$\sum_{y\in O_x} \frac{1}{|O_y|} = 1$, 故$\sum_{x\in X} \frac{1}{|O_x|}$为轨道的个数, 从而可得结论.

2 Pólya计数定理

Pólya计数定理是组合数学中一个十分有力的技术工具, 它主要研究一个由映射所构成的集合在某个群作用下的映射等价类数.

设A和C分别是n-集合和m-集合, 记$C^A = \{f \mid f : A \to C\}$为由$A$到$C$的全体映射组成的集合, 显然$\left|C^A\right| = |C|^{|A|} = m^n$. 有时候也称集合$C$中的元素为颜色, 并称映射$f \in C^A$为$A$中元素的一种染色(记元素$a$染成颜色$f(a)$). 这一凡是关于染色的计数问题都可以依这个观点解释为映射的计数问题.

设G是集合A上的一个置换群, G可以以如下方式自然地作用在映射集合C^A上: $gf = f \circ g^{-1}, g \in G, f \in C^A$. 容易验证这是一个群作用. 在这个群作用下, C^A中属于同一个G的轨道中的两个映射称为G-**等价**的(简称**等价**的). 因此, C^A中的一个G-轨道也可视为一个映射等价类, 我们要求的是G作用在C^A上的轨道的个数 (或A中元素用C中颜色染色时的互不等价等价的染色方法数). 为此, 先给出如下引理.

引理 1 设G时n-集合A上的一个置换群, 对于$g \in G$, $\text{type}(g) = (l_1(g), l_2(g), \ldots, l_n(g))$为$g$的轮换型号, 又记$k(g) = l_1(g) + l_2(g) + \ldots + l_n(g)$为$g$的轮换分解式中轮换的个数, 设$A_1, A_2, \ldots, A_{k(g)}$为$g$的轮换分解式中轮换的符号集, 用$\psi(g)$表示$C^A$中在$g$作用下保持不变的元素的集合, 则

(1)$\psi(g) = \left\{f \in C^A \mid f\text{在子集}A_1, A_2, \ldots, A_{k(g)}\text{上均取常数值}\right\}$;

(2)$|\psi(g)| = |C|^{k(g)} = m^{l_1(g)+l_2(g)+\ldots+l_n(g)}$.

引理的证明 1 任取$f \in \psi(g)$, 则有$gf = f \circ g^{-1} = f$, 从而对任意正整数r, 有$f = f \circ g^{-r}$. 故对任意$a \in A$, 有$f(a) = f(g^{-r}(a))$. 又对任意$a, b \in A$, a和b为g的同一个轮换中的符号, 当且仅当存在正整数r, 使得$a = g^r(b)$. 由此得到, 若$a, b \in A_j (1 \le j \le k(g))$, 则$f(a) = f(b)$, 即$f$在$g$的所有轮换符号

集$A_1, A_2, \ldots, A_{k(g)}$上均取常数值. 反之, 若$f(a) = f(b)$, 对$a, b \in A_j (1 \leq j \leq k(g))$均成立, 则对任意$a \in A$, 有$f(a) = f\left(g^{-1}(a)\right)$, 即$f = f \circ g^{-1} = gf$, 从而$f \in \psi(g)$. 所以

$$\psi(g) = \left\{ f \in C^A \mid f\text{在子集}A_1, A_2, \ldots, A_{k(g)}\text{上均取常数值} \right\}.$$

(2)$\psi(g)$中的映射可分别在$A_1, A_2, \ldots, A_{k(g)}$上取$C$任一元素为像, 故这样的映射共有$|C|^{k(g)}$个, 即$|\psi(g)| = m^{k(g)}$.

下面这个来源于Pólya的定理给出了上面所提问题的解答.'

定理 4 ***Pólya*计数定理** 设$|A| = n, |C| = m$, G为集合A上的一个置换群, $\mathcal{F}$为G作用在C^A上的轨道的集合, 则轨道个数为

$$\mathcal{F} = P_G(m, m, \ldots, m),$$

其中$P_G(x_1, x_2, \ldots, x_n)$是$A$上置换群$G$的轮换指标.

证明 3 由*Burnside*引理可得

$$|\mathcal{F}| = \frac{1}{|G|} \sum_{g \in G} |\psi(g)| = \frac{1}{|G|} \sum_{g \in G} \left(\prod_{i=1}^{n} m^{l_i(g)} \right) = P_G(m, m, \ldots, m).$$

我们回到最开始的问题. 在例1中, 群G为六个点上的二面体群D_6. 由

$$P_{D_6}(x_1, \ldots, x_6) = \frac{1}{12} \left(x_1^6 + 3x_1^2 x_2^2 + 4x_2^3 + 2x_3^2 + 2x_6 \right),$$

可知这样得到的不同的分子个数为

$$P_{D_6}(2, 2, \ldots, 2) = 13.$$

读者可以通过自己枚举的结果进行验证.

例 7 求m-集合C中元素的长度为n的可重复圆周排列的个数$C_m(n)$.

解 2 设$A = \{1, 2, \ldots, n\}$为圆周上(依次排列的)n个位置的集合, 则C中元素在位置集A上的一个重复排列相当于A到C的一个映射, 而两个这样的映射相应于同一个圆周排列当且仅当它们只相差定义域A上的一个循环移位. 因此, 置换群G就是A的全部循环移位所构成的群, 即有一个n-轮换$(12 \ldots n)$生成的n阶循环群. 这样, 集合C中元素的一个长度为n的可重复圆周排列就相当于群作用的一个轨道. 由*Pólya*计数定理得

$$C_m(n) = P_{\langle (12 \ldots n) \rangle}(m, m, \ldots, m) = \frac{1}{n} \sum_{d \mid n} \phi(d) m^{\frac{n}{d}} = \frac{1}{n} \sum_{d \mid n} \phi\left(\frac{n}{d}\right) m^d.$$

例 8 我们回顾允许重复的组合问题. 设x是一个正整数, 从x种不同物体种可以任意重复地选取n个, 则选法数为$\binom{n+x-1}{n}$. 这也可以看成一个映射问题. 设A是一个n-集合, B是一个x-集合, A种元素全部相同, B种元素各自不同, 则如上的一个可重复选取恰为一个从A到B的映射. 考虑映射集$B^{[n]} = \{f \mid f : [n] \to B\}$, $[n]$上的置换群为对称群S_n. 一个从A到B的映射恰为对称群S_n作用于映射集$B^{[n]}$的一条轨道. 由*Pólya*计数定理得到所求的选法数为

$$P_{S_n}(x, x, \ldots, x) = \frac{1}{n!} \sum_{\sigma \in S_n} x^{k(\sigma)} = \frac{1}{n!} \sum_{k=1}^{n} c(n,k)\, x^k,$$

其中$c(n,k)$为包含k个轮换的n元置换的个数(即无符号的第一类*Stirling*数). 故

$$\binom{n+x-1}{n} = \frac{1}{n!} \sum_{k=1}^{n} c(n,k)\, x^k.$$

即

$$\sum_{k=1}^{n} c(n,k)\, x^k = x(x+1)\ldots(x+n-1).$$

此式对任意正整数x成立. 等式两端又可堪称关于x的n次多项式, 所以上式对任意的x成立.

3 带权的Pólya计数定理与进一步推广

在有些计数问题种, 还需要进一步了解群G作用在C^A上时, 那些映成C中元素$c_1, \ldots, c_m$的A中元素的条数$\left|f^{-1}(c_1)\right|, \ldots, \left|f^{-1}(c_m)\right|$给定的那部分映射构成的$G$-轨道的个数. 例如, 我们在本章最初的问题中, 我们考虑其恰连接2个甲基的分子数. 解决这样的问题需要更一般的"带权的Burnside引理".

设群G作用在集合X上, w时定义在集合X上的一个数值函数, 称为权函数. 若w在X的各个轨道上均取常数值, 则可定义w在X的一轨道上的值为其中一元素上的值, 即$w(O_x) = w(x)$, 此时各轨道上的权之和可由下面的定理给出.

定理 5 带权的*Burnside*引理 设$O_1, O_2, \ldots, O_N$是群G作用在集合X上的全部轨道, w是X上的一个权函数, 它在各轨道上都取常数值(故w也同时被视为轨道集上的一个函数), 则所有轨道上的权之和可表示为

$$\sum_{i=1}^{N} w(O_i) = \frac{1}{|G|} \sum_{g \in G} \sum_{x \in \psi(g)} w(x).$$

证明 4 类似*Burnside*引理的证明, 有

$$\sum_{i=1}^{N} w(O_i) = \sum_{x\in X} \frac{w(x)}{|O_x|} = \frac{1}{G}\sum_{x\in X} |G_x| \cdot w(x) = \frac{1}{|G|}\sum_{x\in X} w(x)\left(\sum_{g\in G_x} 1\right)$$
$$= \frac{1}{|G|}\sum_{g\in G}\sum_{x\in\psi(g)} w(x).$$

我们取$w(x) = 1$即得Burnside引理. 与前面一样, 设A, C是两个集合, G是集合A上的一个置换群, w是集合C上的一个函数, 对$f \in C^A$, 定义

$$w(f) = \prod_{a\in A} w(f(a)).$$

当映射f_1, f_2等价时, 存在$g \in G$, 使得 $f_2 = f_1 \circ g^{-1}$. 因g是A上的一个置换, 故当a取遍A中所有元素时,$g^{-1}(a)$也取遍A中所有元素. 所以

$$w(f_2) = \prod_{a\in A} w(f_2(a)) = \prod_{a\in A} w\left(f_1\left(g^{-1}(a)\right)\right) = w(f_1).$$

即w在C^A的每个轨道上均取常数值, 从而w也可视为定义在轨道集合上的一个函数. 设$\mathcal{F}$为G作用在C^A上的轨道的集合, 则上面问题的带权形式为求所有轨道的权之和$\sum_{F\in\mathcal{F}} w(f)$ (当w恒为1时即为轨道的个数).

定理 6 带权的*Pólya*计数定理 设w是C上的一个权函数, 则w也可定义成为映射集C^A和轨道集$\mathcal{F}$上的函数, 且有

$$\sum_{F\in\mathcal{F}} w(F) = P_G\left(\sum_{c\in C} w(c), \sum_{c\in C} w(c)^2, \ldots, \sum_{c\in C} w(c)^n\right).$$

证明 5 对$g \in G$, 记

$$k = k(g) = l_1(g) + l_2(g) + \ldots + l_n(g).$$

对于任意$(c_1, c_2, \ldots, c_k) \in C^k$, 设$f_{c_1,c_2,\ldots,c_k}$为$C^A$中在符号集$A_i$上取常数值$c_i (i = 1, 2, \ldots, k)$的映射. 由引理*1 (1)*知

$$\psi(g) = \left\{f_{c_1,c_2,\ldots,c_k} \mid (c_1, c_2, \ldots, c_k) \in C^k\right\}.$$

又

$$w\left(f_{c_1,\ldots,c_k}\right) = \prod_{a\in A} w\left(f_{c_1,\ldots,c_k}(a)\right) = \prod_{i=1}^{k} w(c_i)^{|A_i|},$$

于是

$$\sum_{f\in\psi(g)} w(f) = \sum_{(c_1,\ldots,c_k)\in C^k} w\left(f_{c_1,c_2,\ldots,c_k}\right) = \sum_{(c_1,\ldots,c_k)\in C^k} \prod_{i=1}^{k} w(c_i)^{|A_i|}$$
$$= \prod_{i=1}^{k}\left(\sum_{c\in C} w(c)^{|A_i|}\right).$$

最后一个等式可以理解为一个以C为行角标集, 以$\{1,2,\ldots,k\}$为列角标集的矩阵中各行元素和的乘积等于其各列中任取一元素所能做成的各种可能的乘积之和.

由轮换型号的定义知, 数$|A_1|,\ldots,|A_k|$中恰有$l_i(g)$个等于$j(j=1,2,\ldots,n)$, 故把上式右端乘积中相同因子写成幂次的形式得

$$\sum_{f\in\psi(g)} w(f) = \prod_{j=1}^{n}\left(\sum_{c\in C} w(c)^j\right)^{l_j(g)}.$$

由带权的*Burnside*引理得

$$\sum_{F\in\mathcal{F}} w(F) = \frac{1}{|G|}\sum_{g\in G}\sum_{f\in\psi(g)} w(f) = \frac{1}{|G|}\sum_{g\in G}\prod_{j=1}^{n}\left(\sum_{c\in C} w(c)^j\right)^{l_j(g)}$$
$$= P_G\left(\sum_{c\in C} w(c), \sum_{c\in C} w(c)^2, \ldots, \sum_{c\in C} w(c)^n\right).$$

由此我们易得下述结论

定理 7 设$C=\{c_1,\ldots,c_m\}$, G是n-集合A上的一个置换群. 对满足$k_1+k_2+\ldots+k_m=n$的非负整数$k_1,k_2,\ldots,k_m$, 记$N(k_1,k_2,\ldots,k_m)$为C^A中恰把A中的ki个元素映成$c_i(i=1,2,\ldots,m)$的G-轨道的条数, 则有

$$P_G\left(\sum_{i=1}^{m} x_i, \sum_{i=1}^{m} x_i^2, \ldots, \sum_{i=1}^{m} x_i^n\right) = \sum_{k_1+k_2+\ldots+k_m=n} N(k_1,k_2,\ldots,k_m)\, x_1^{k_1}x_2^{k_2}\ldots x_m^{k_m}.$$

证明 6 定义集合C上的权函数w为

$$w(c_i) = x_i, i=1,2,\ldots,m,$$

其中$x_1,x_2,\ldots,x_m$为互相独立的未定元. 对$f\in C^A, i=1,2,\ldots,m$, f恰把A中k_i个元素映成c_i的充分必要条件为

$$w(f) = x_1^{k_1}x_2^{k_2}\ldots x_m^{k_m},$$

故$N(k_1,k_2,\ldots,k_m)$为C^A中权函数等于$x_1^{k_1}\ldots x_m^{k_m}$的$G$-轨道的条数. 将$\sum_{F\in\mathcal{F}}$中相同权函数的项合并, 可得

$$\sum_{F\in\mathcal{F}} w(F)=\sum_{k_1+k_2+\ldots+k_m=n} N(k_1,k_2,\ldots,k_m)\,x_1^{k_1}x_2^{k_2}\ldots x_m^{k_m}.$$

另一方面, 当$w(c_i)=x_i$时, 由带权的*Pólya*定理有

$$\sum_{F\in\mathcal{F}} w(F)=P_G\left(\sum_{i=1}^m x_i,\sum_{i=1}^m x_i^2,\ldots,\sum_{i=1}^m x_i^n\right).$$

以章首问题为例, 此时有

$$\begin{aligned}&P_{D_6}\left(x_1+x_2,x_1^2+x_2^2,\ldots,x_1^6+x_2^6\right)\\&=\frac{1}{12}\left((x_1+x_2)^6+3(x_1+x_2)^2\left(x_1^2+x_2^2\right)^2+4\left(x_1^2+x_2^2\right)^3+2\left(x_1^3+x_2^3\right)^2+2\left(x_1^6+x_2^6\right)\right)\end{aligned}$$

其中$x_1^2x_2^4$的系数为3, 故连接两个甲基的分子恰有3个.

更进一步地, 我们考虑在群在集合C和集合A上同时作用的情况.

定理 8 设G和H分别为n-集合A和有限集C上的置换群, 直积$G\times H$作用在C^A上, 当$f\in C^A$, 且$(\sigma,\tau)\in G\times H$时, 定义$(\sigma,\tau)f$如下:

$$((\sigma,\tau)f)(a)=\tau\left(f\circ\sigma^{-1}(a)\right).$$

则$G\times H$作用在C^A上的轨道数为

$$\frac{1}{|H|}\sum_{\tau\in H} P_G(m_1(\tau),m_2(\tau),\ldots,m_n(\tau))$$

其中

$$m_i(\tau):=\sum_{j\mid i} jl_j(\tau)$$

证明 7 由*Burnside*引理可得轨道数为

$$\frac{1}{|G||H|}\sum_{\sigma\in G,\tau\in H}\psi(\sigma,\tau),$$

其中$\psi(\sigma,\tau)=\left|\left\{f\in C^A\mid(\sigma,\tau)f=f\right\}\right|$. 我们下面只需要证明对任意$\tau\in H$, 有

$$\frac{1}{|G|}\sum_{\sigma\in G}\psi(\sigma,\tau)=P_G(m_1(\tau),\ldots,m_n(\tau)).$$

固定$\sigma \in G, \tau \in H$, 设$k = k(\sigma) = l_1(\sigma)+l_2(\sigma)+\ldots+l_n(\sigma)$, 并设$A_1, A_2, \ldots, A_k$为$\sigma$轮换分解式中的符号集.

一个映射$f : A \to C$被(σ, τ)固定, 当且仅当f在所有的$A_i, i = 1, 2, \ldots, k$上是固定的. 于是$\psi(\sigma, \tau)$是满足

$$f_i(\sigma(a)) = \tau(f_i(a)), \forall a \in A_i$$

的映射$f_i : A_i \to C$的数目的乘积, 其中$i = 1, 2, \ldots, k$. 设A_i有长度$|A_i|$并固定$a_0 \in A_i$. 设$\sigma \mid A_i$为σ在A_i上的限制. 假设$f_i : A_i \to C$被$(\sigma \mid A_i, \tau)$固定且$f(a_0) = c$, 则f完全被确定: $f_i\left(\sigma^l(a_0)\right) = \tau^l(c)$. 此外, $c = f_i(a_0) = f_i\left(\sigma^{|C_i|}(a_0)\right) = \tau^l(c)$, 因此我们看到$\tau$的包含$c$的轮换符号集有一定长度$l \mid |A_i|$.

反之, 若c是C的一个位于τ的轮换符号集上的元素, 其长度整除$|C_i|$, 则可以在C_i上由$f_i\left(\sigma^t(a_0)\right) := \tau^t(c)$定义一个映射$f_i$, 且这个$f_i$被$(\sigma \mid A_i, \tau)$固定(注意$f_i$定义是否良好).

总之, 对A_i, 固定的映射$f_i : A_i \to C$的数目于C的位于τ的长度整除$|A_i|$的圈中的元素相等. 这样的元素个数为

$$m_l = \sum_{j|l} j l_j(\tau),$$

从而得到原结论.

下面我们再考虑其带权形式.

定理 9 ***Pólya-De Bruijn* 计数定理** 设G作用在A上, H作用在C上, R为一个交换环且$w : C \to R$, w在H作用在B上的每个轨道中是常数. 定义$w(f) : \prod_{a \in A} w(f(a))$, 则$G \times H$作用于$C^A$上的轨道的一个代表系$\mathcal{F}$的和为

$$\sum_{F \in \mathcal{F}} w(F) = \frac{1}{|H|} \sum_{\tau \in H} P_G(M_1(\tau), M_2(\tau), \ldots, M_n(\tau)),$$

其中

$$M_i(\tau) = \sum_{\tau^i(c)=c} (w(c))^i.$$

De Bruijn给出了证明.

Pólya计数定理及其带权形式给出了有限集A到C的映射集C^A在A上的某个置换群G作用下的轨道(或某类轨道)的个数公式. 应用Pólya计数定理解决计数问题可如下进行:

(1)将所讨论的问题中的"安排"翻译成映射的语言, 从而确定映射的定义域A和值域C.

(2)确定映射的等价关系(即那些映射应属于同一个"安排"), 确定相应的A上的置换群G使这个等价关系就是G-等价关系, 从而使问题中的一个"安排"就相应于一个映射等价类, 即群作用下的一个轨道.

(3)求出置换群G的轮换指标$P_G(x_1, x_2, \ldots, x_n)$, 然后利用Pólya计数定理或其带权形式计算映射等价类的个数.

我们给出几个例子.

例 9 把正方体的顶点集V(或棱集E, 面集F)用m种颜色来染色, 其中称两种染色是等价的, 如果经过三维空间中某个把正方体变成自身的旋转后可使这两种染色成为一致的. 求他的互不等价的点染色方式数, 棱染色方式数和面染色方式数.

解 3 由例6中结果和*Pólya*计数定理, 其互不等价的点染色方式数为

$$P_{G_1}(m, \ldots, m) = \frac{m^8 + 17m^4 + 6m^2}{24},$$

互不等价的棱染色方式数为

$$P_{G_2}(m, \ldots, m) = \frac{m^{12} + 6m^7 + 3m^6 + 8m^4 + 6m^3}{24},$$

互不等价的面染色方式数为

$$P_{G_3}(m, \ldots, m) = \frac{m^6 + 3m^4 + 12m^3 + 8m^2}{24}.$$

若用红和蓝两种颜色来染色, 即$m = 2$, 其中恰有4个面染成红色, 2个面染成蓝色的互不等价的染色方式数为多项式

$$P_{G_3}\left(x_1 + x_2, x_1^2 + x_2^2, \ldots, x_1^6 + x_2^6\right)$$

中$x_1^4 x_2^2$的系数, 即为2.

例 10 把2个红球, 2个黄球和4个绿球放在1个圆盒子和3个方盒子中的方法数是多少?

解 4 取

$$A = \{R_1, R_2, Y_1, Y_2, G_1, G_2, G_3, G_4\}, G = S_2 \times S_2 \times S_4$$

$$C = \{r, s_1, s_2, s_3\}, H = S_1 \times S_3.$$

容易看出G的轮换指标是对称群的轮换符号集的指标的积, G是对称群之积, 因此

$$P_G = P_{S_2} \cdot P_{S_2} \cdot P_{S_4} = \frac{1}{2!2!4!}\left(x_1^2 + x_2\right)^2\left(x_1^4 + 6x_1^2x_2 + 3x_2^2 + 8x_1x_3 + 6x_4\right).$$

在H中有三种类型的置换. 若τ是恒等置换, 则

$$m_1(\tau) = 4, m_2(\tau) = 4, m_3(\tau) = 4, m_4(\tau) = 4.$$

如果τ互换$\{s_1, s_2, s_3\}$中的两个, 则

$$m_1(\tau) = 2, m_2(\tau) = 4, m_3(\tau) = 2, m_4(\tau) = 4.$$

如果τ只固定r, 则

$$m_1(\tau) = 1, m_2(\tau) = 1, m_3(\tau) = 4, m_4(\tau) = 1.$$

由定理8得, 方法数为656.

进一步地, 取$w(r) = r, w(s_1) = w_{s_2} = w_{s_3} = s$. 这里$R = \mathbb{Q}[r, s]$. t个球放到圆盒子且其余$8-t$个球放入方盒子中的方法数为

$$\frac{1}{6}\left(P_G\left(r + 3s, r^2 + 3s^2, \ldots, r^4 + 3s^4\right) + 3P_G\left(r + s, r^2 + 3s^2, r^3 + s^3, r^4 + 3s^4\right) + 2P_G\left(r, r^2, r^3 + 3s^3, r^4\right)\right).$$

中$r^t s^{8-t}$的系数.

例 11 求n个顶点的简单图(n阶简单图)的个数.

解 5 我们可求出n个顶点的标号图共有$2^{\frac{n(n-1)}{2}}$个. 下计数非标号图, 即两个同构的图被视为相同的. (设$G = (V(g), E(G)), H = (V(H), E(H))$是两个图. 一个从$G$到$H$的同构是一个双射$f: V(G) \to V(H)$,使得$f(E(G)) = E(H)$, 即对任意$u, v \in V(G)$, $\{u, v\} \in E(G)$当且仅当$\{f(u), f(v)\} \in E(H)$. 两图之间若有任意同构存在, 则称这两个图同构).

设图的顶点集为$[n] = \{1, 2, \ldots, n\}, D = \binom{[n]}{2}$. 即$[n]$的所有2-子集组成的集合. 易知$|D| = \frac{n(n-1)}{2}$, 则一个$n$阶标号图即为集合对$([n], E)$, 其中$E$为$D$的一个子集.

$[n]$上的对称群为S_n, 对于$g \in S_n$, g诱导出D上的置换π_g如下:

$$\pi_g(\{i, j\}) = \{g(i), g(j)\}, \forall \{i, j\} \in D.$$

记$G_n = \left\{\pi_g \mid g \in S_n\right\}$, 则$G_n$为$D$上的置换群. 若存在$g \in S_n$, 使得$\pi_g(E_1) = E_2$, 则标号图$([n], E_1)$与$([n], E_2)$同构, 即它们可看成相同的非标号图. 由*Pólya*计数定理知, n阶简单图的个数为$P_{G_n}(2, 2, \ldots, 2)$.

另一方面, 标号图也可看做映射$f_E : D \to \{0, 1\}$, 其定义为

$$f_E(\{i, j\}) = \begin{cases} 1, & \{i, j\} \in E, \\ 0, & \{i, j\} \notin E. \end{cases}$$

对$\{0, 1\}$赋权$w(0) = 1, w(1) = x$, 则恰有k条边的n阶简单图的个数为 $P_{G_n}\left(1 + x, 1 + x^2, \ldots, 1 + x^{\frac{n(n-1)}{2}}\right)$中$x^k$的系数.

一般地, n阶简单图的个数为

$$\sum_{l_1+2l_2+\ldots+nl_n=n} \frac{2^{N(l_1,\ldots,l_n)}}{l_1!l_2!\ldots l_n!1^{l_1}2^{l_2}\ldots n^{l_n}},$$

其中

$$N(l_1, \ldots, l_n) = \frac{1}{2}\left(\sum_{s,t=1}^{n} l_s l_t \gcd(s, t) - \sum_{s\text{为奇数}} l_s\right).$$

证明详见相关文献.

A 抽象代数基本概念

A.1 群

读者应熟知群的相关定义. 在此我们仍然提出作为参考.

定义 5 设集合A中的二元运算$\cdot : A \times A \to A$, 记作乘法. 若A的一个等价关系$\sim$满足

$$a \sim b, c \sim d \Rightarrow ac \sim bd, \forall a, b, c, d \in A,$$

则称$\sim$为A的一个**同余关系**. $a \in A$的等价类K_a此时也称a的**同余类**.

定义 6 设S为非空集合, 在S中定义了二元运算$\cdot : S \times S \to S$称为乘法, 其满足结合律, 即

$$(ab)c = a(bc), \forall a, b, c \in S,$$

则称$(S, \cdot)$为**半群**. 其简记作S. 下类似进行简记.

若半群S中存在元素1, 使得

$$1a = a1 = a, \forall a \in S,$$

则称M为**幺半群**, 1称为幺元, 易知其唯一.

若半群S的乘法满足交换律,即

$$ab = ba, \forall a, b \in S,$$

则S为**交换半群**, 或S是**可换的**.

定义 7 在非空集合G中定义二元运算$\cdot : G \times G \to G$, 称为乘法, 若满足以下条件

*(1)*结合律成立;

*(2)*存在**左幺元**,即$\exists e \in G$, 使得$ea = a, \forall a \in G$.

(3)$\forall a \in G$存在左逆元, 即$\exists b \in G$, 使得$ba = e$.

则称G是一个**群**. 若G中乘法还满足交换律, 则称G为**交换群**或***Abel*群**.

读者易于验证群满足下列性质.

定理 10 若b为a的左逆元, 则b也为a的右逆元, 从而b为a的逆元, 记为a^{-1}, 其是唯一的.

1也是G的右幺元, 从而为G的幺元, 其是唯一的.

群运算满足消去律. 群中方程$ax = b$的解存在且唯一.

定义 8 群G中所含元素个数$|G|$称为G的**阶**. 若$|G|$有限, 则称G为**有限群**. 若$|G|$无限, 则称G为**无限群**.

设a是群G的元素, 若$\forall k \in \mathbb{N}, a^k \neq 1$, 则称$a$的**阶为无穷**. 若$\exists k \in \mathbb{N}, a^k = 1$, 则$\min\left\{k | k \in \mathbb{N}, a^k = 1\right\}$称为$a$的**阶**.

设A, B是群G的两个子集, 约定$AB = \{ab | a \in A, b \in B\}$, $A^{-1} = \left\{a^{-1} | a \in A\right\}$. 特别地, 当$A = \{a\}$时, 记$AB = aB$, $BA = Ba$.

定义 9 群G的非空子集H若对G的运算也构成一个群, 则其称为G的**子群**. 其中$\{1\}$和G称为G的**平凡子群**, 其他的子群称为**非平凡子群**.

定义 10 设H是群G的子群, 又$a \in G$. 集合aH与Ha分别称为以a为代表的H的**左陪集**和**右陪集**.

易知对G的任意子群H, 其关于G中任意元素a确定一个等价关系, 其等价类为一左陪集aH, 从而左陪集族为G的一个划分. 右陪集类似.

定义 11 通常将G对上述等价关系的商集合, 即以左陪集为元素的集合记为G/H, 称为G对H的**左陪集空间**. G/H中元素个数$|G/H|$称为H在G中的**指数**, 记为$[G:H]$. 相应地可定义右陪集空间.

定理 11 设H是有限群G的子群, 则有

$$[G:1] = [G:H]\,[H:1],$$

因而子群H的阶是群G的阶的因子.

证明留给读者.

定义 12 对群G的元素a, $\langle a\rangle := \{a^n | n \in \mathbb{Z}\}$ 称为由a生成的G的子群(易验证其为群).

若群G中存在元素a, 使得$G = \langle a\rangle$, 则称G是**循环群**, a为G的一个**生成元**.

从而有推论

定理 12 有限群G的任一元素a的阶是G的阶的因子.

定理 13 设H是群G的子群, 则G中由

$$a\mathcal{R}b, \text{当} a^{-1}b \in H$$

所定义的关系$\mathcal{R}$为同余关系的充分必要条件为

$$ghg^{-1} \in H, \forall g \in G, h \in H.$$

此时称H为G的**正规子群**, 记为$H \lhd G$. 同时, 商集合G/H对同余关系$\mathcal{R}$导出的运算也构成一个群, 称为G对H的**商群**.

定义 13 设G_1, G_2为两个群(或半群, 幺半群), f是G_1到G_2的映射. 如果f满足

$$f(xy) = f(x)\,f(y), \forall x, y \in G_1,$$

则称f是G_1到G_2的一个**同态**. 若f还是满映射, 则称f为**满同态**, 或G_1**到**G_2**上的同态**, 此时也称G_1**与**G_2**同态**.

若f还是一一对应, 则称f为**同构**, 此时也称G_1与G_2**同构**, 记为$G_1 \cong G_2$.

例 12 设H是群G的正规子群, 记G到商群G/H的自然映射为

$$\pi : \pi(g) = gH, \forall g \in G,$$

则π为G到G/H上的同态, 称π为**自然同态**.

群同态与同构具有下述简单性质.

定理 14 若f是群G_1到群G_2的同态, g是群G_2到群G_3的同态, 则

(1)gf是G_1到G_3的同态;

*(2)*若f, g都是满同态*(*同构*)*, 则gf也是满同态*(*同构*)*.

定理 15 群的同构关系是一个等价关系.

定义 14 设X为非空集合, S_X表示X的所有可逆变换*(*即X到X的一一对应*)*的集合, 则S_X对变换的乘法构成一个群, 称为X的**全变换群**. id为其幺元.

S_X的子群称为X上的**变换群**.

下面我们证明任何群一定同构于一个变换群.

定义 15 设G是群. 对于$a \in G$, 可定义G上的两个变换L_a, R_a如下

$$L_a(x) = ax, R_a(x) = xa, \forall x \in G.$$

其分别称为由a决定的***左平移***和***右平移***.

易验证$L_G = \{L_a | a \in G\}, R_G = \{R_a | a \in G\}$都是$S_G$的子群.

定理 16 ***Cayley*定理** 设G是一个群, 则

$$G \cong L_G \cong R_G.$$

A.2 群的生成组和群在集合上的作用

设S是群G的非空子集, 以$\langle S \rangle$表示G的包含S的最小子群, 即S**生成的子群**. 显然,$\langle S \rangle$是G中所有包含S的子群之交.

定理 17 设S是群G的非空子集, 则

$$\langle S \rangle = \left\{ x_1 x_2 \dots x_m | x_i \in S \cup S^{-1}, 1 \le i \le m, m \in \mathbb{N} \right\}.$$

定义 16 若S为群G的子集, 且$G = \langle S \rangle$, 则称S为G的**生成组**. 若G有一个含有限个元素的生成组, 则称G是**有限生成的**.

定义 17 设集合$\{i_1, i_2, \ldots, i_r\}$为集合$\{1, 2, \ldots, n\}$的子集. 若$\sigma \in S_n$满足

$$\sigma\left(i_j\right) = i_{j+1}, 1 \leq j \leq r-1; \sigma(i_r) = i_1; \sigma(k) = k, k \notin \{i_1, \ldots, i_k\}.$$

则称σ为一个**长r的轮换**或**r轮换**, 此时记$\sigma = (i_1 i_2 \ldots i_r)$. 特别地, 将2轮换$(i, j)$称为**对换**.

若$\sigma = (i_1 i_2 \ldots i_r)$与$\tau = (j_1 j_2 \ldots j_s)$是两个轮换, 且

$$\{i_1, \ldots, i_r\} \cap \{j_1, \ldots, j_s\} = \varnothing,$$

则称σ与τ为不相交的轮换.

定理 18 设$a \in S_n$, 且$a = \sigma_1 \sigma_2 \ldots \sigma_k$, 其中$\sigma_i$为$r_i$轮换: 当$i \neq j$时$\sigma_i$与$\sigma_j$不相交, $1 \leq i, j \leq k$, 则a的阶为$r_1, r_2, \ldots, r_k$的最小公倍数$\operatorname{lcm}(r_1, \ldots, r_k)$

可归纳证明.

定理 19 令$S = \{(1i) | 2 \leq i \leq n\}$, 则$S_n = \langle S \rangle$.

证明 8 首先证明任何对换(ij)可写成S中元素之积. 事实上

$$(ij) = (1i)(1j)(1i).$$

其次用数学归纳法证明任何轮换$(i_1 \ldots i_r)$可写成对换之积,

$$(i_1 i_2 \ldots i_r) = (i_1 i_r)(i_1 i_{r-1}) \ldots (i_1 i_2).$$

证明留给读者.

最后证明$\forall a \in S_n$可写成轮换之积, 即可写成S中元素之积.

记S_n中幺元为id. 设$a \in S_n$, 令$\bar{F}_a = \{j | a(j) \neq j\}$. 显然有

$$\bar{F}_{\mathrm{id}} = \varnothing.$$

当$a \neq \mathrm{id}$时

$$\left|\bar{F}_a\right| \geq 2$$

当且仅当a为对换时等号成立. 不妨设$a \neq \mathrm{id}$. 下证存在轮换σ_1满足

$$\begin{cases} \bar{F}_a = \bar{F}_{\sigma_1} \cup \bar{F}_{\sigma^{-1} a}, \\ \bar{F}_{\sigma_1} \cap \bar{F}_{\sigma_1^{-1} a} = \varnothing. \end{cases}$$

由$a \neq \mathrm{id}$, 知$\exists i_1 \in \bar{F}_a$. 令

$$i_2 = a(i_1), \ldots, i_k = a(i_{k-1}).$$

由于$\bar{F}_a$是有限集, 故存在r使得$i_1, \ldots, i_{r-1}$互不相同, 而$i_r = i_t (1 \leq t \leq r-1)$. 现证$t = 1$. 否则有

$$a(i_{t-1}) = i_t = i_r = a(i_{r-1}).$$

从而$i_{t-1} = i_{r-1}$, 即$t = r$, 产生矛盾.

令$\sigma_1 = (i_1 i_2 \ldots i_{r-1})$, 显然

$$\sigma_1(i_k) = a(i_k), 1 \leq k \leq t, \bar{F}_{\sigma_1} = \{i_1, \ldots, i_{r-1}\} \subseteq \bar{F}_a.$$

再令$a_1 = \sigma_1^{-1} a$, 若$l \notin \bar{F}_a$, 则$l \notin \bar{F}_{\sigma_1^{-1}}$, 故$a_1(l) = l$, 因而$\bar{F}_{a_1} \subseteq \bar{F}_a$, 于是$\bar{F}_{a_1} \cup \bar{F}_{\sigma_1} \subseteq \bar{F}_a$. 反之, 若$l \notin \bar{F}_{a_1} \cup F_{\sigma_1}$, 则有$a_1(l) = \sigma_1(l) = l$, 故$a(l) = l$, 即$l \notin \bar{F}_a$. 从而$\bar{F}_a = \bar{F}_{\sigma_1} \cup \bar{F}_{\sigma^{-1} a}$.

设$i_k \in \bar{F}_{\sigma_1}$, 则有$a_1(i_k) = \sigma_{-1}^{-1} a(i_k) = \sigma_1^{-1} \sigma_1(i_k) = i_k$, 即$i_k \notin \bar{F}_{a_1}$, 从而$\bar{F}_{\sigma_1} \cap \bar{F}_{\sigma_1^{-1} a} = \varnothing$.

若$a \neq \sigma_1$, 则$\bar{F}_{\sigma_1^{-1} a} \neq \varnothing$. 再对$\sigma_1^{-1} a$用上述方法可得另一轮换$\sigma_2$与$\bar{F}_{\sigma_2^{-1} \sigma_1^{-1} a} \subset \bar{F}_{\sigma_1^{-1} a} \subset \bar{F}_a$. 由于$\bar{F}_a$是有限的, 从而存在$n$使得

$$\bar{F}_{\sigma_n^{-1} \sigma_{n-1}^{-1} \ldots \sigma_1^{-1} a} = \varnothing,$$

即$\sigma_n^{-1} \sigma_{n-1}^{-1} \ldots \sigma_1^{-1} a = \mathrm{id}$. 因而

$$a = \sigma_1 \sigma_2 \ldots \sigma_n.$$

即S_n中任何元素可表示为轮换之积, 故定理成立.

在上述证明的过程中容易发现$\sigma_1, \sigma_2, \ldots, \sigma_n$是两两不交的.

定义 18 设G是一个群, X是一个非空集合. 若$G \times X$到X的映射f满足

(1) $f(\mathrm{e}, x) = x, \forall x \in X$, e是$G$的幺元;

(2) $f(g_1 g_2, x) = f(g_1, f(g_2, x)), \forall g_1, g_2 \in G, x \in X$,

则称f决定了**群G在X上的一个作用**.

群G可以多种方式作用在一个集合X上. 不需要特别指出映射f(即固定好一种作用方式)时, 常记

$$f(g, x) = g(x), \forall g \in G, x \in X.$$

定义 19 设群G作用在集合X上. 若$\forall x, y \in X, \exists g \in G$, 使$y = g(x)$, 则称$G$在$X$上的作用是**可递的**, X称为(对于G的)**齐性空间**.

定义 20 设群G作用在集合X上, 若$g(x) = x, \forall g \in G, x \in X$,则称$G$在$X$上的作用是**平凡的**.

若当且仅当$g = \mathrm{e}$时$g(x) = x, \forall x \in X$,成立, 则称$G$在$X$上的作用是**有效的**.

定理 20 设群G作用在集合X上, $\forall g \in G$,

$$\sigma_g(x) = g(x), \forall x \in X$$

定义的σ_g是X的可逆变换, 即$\sigma_g \in S_X$.

又由$\sigma(g) = \sigma_g, \forall g \in G$ 定义的G到S_X的映射σ是一个同态映射.

G在X上的作用有效当且仅当σ是一一的.

反之, 若σ是群G到集合X的置换群S_X的同态, 则由

$$g(x) = \sigma(g)(x), \forall g \in G, x \in X$$

定义了G在X的作用, 此时$\sigma_g = \sigma(g)$.

证明详见抽象代数.

定义 21 设群G作用在集合X上, $x \in X$. 称X中的子集

$$O_x = \{g(x) | g \in G\}$$

为x的**轨道**.

G中子集$F_x = \{g | g \in G, g(x) = x\}$ 称为x的**迷向子群**(可自行证明其为子群).

定理 21 设群G作用在集合X上.

(1)在X中定义关系$\mathcal{R}$: $x\mathcal{R}y$当且仅当$\exists g \in G, y = g(x)$, 则$\mathcal{R}$为等价关系且$x$所在的等价类为$x$的轨道$O_x$;

(2)G在O_x上的作用是可递的, G在O_x上作用有效当且仅当F_x所包含的G的正规子群仅为{e}.

(3)若$y = g(x)(x, y \in X, g \in G)$, 则

$$F_{g(x)} = F_y = gF_xg^{-1} = \mathrm{ad}g(F_x).$$

其中

$$\mathrm{ad}g = L_gR_{g^{-1}}$$

称为由g决定的**内自同构**.

证明详见抽象代数.

定理说明, 群G作用在集合X上, 则可将X分解为轨道的不交并. G在每个轨道上的作用是可递的, 是否有效则由迷向子群所含的G的正规子群决定. 事实上, G在每个轨道上的作用相当于G在某个左陪集空间上的作用. 为说明这一点, 我们先引进作用等价的概念.

定义 22 *设群G作用在集合X与X'上, 若有X到X'上的一一对应ϕ, 使*

$$g(\phi(x)) = \phi(g(x)), \forall g \in G, x \in X,$$

*则称G在X, X'上的**作用等价**.*

作用等价可以自然地生成一个等价关系.

定理 22 *设群G在X上的作用可递, $x \in X$, 则G在X上的作用与G在G/F_x上的左平移作用等价.*