群論在計數問題上之應用

關鍵字：群論、Burnside’s Lemma

作者：陳柏諺、陳聖諦、廖崇澔

指導教授：卓士堯教授

壹、摘要

我們最初從一個既定的命題出發，而後將其推廣至「容納 n 顆珠子，使用 k 種珠子」得到一條公式，再推廣此公式，使之對應到平面座標系並研究其性質。

貳、題目

給定兩自然數 n、k表於一可串入 n 個珠子的環中，以 k 種相異種類的珠子進行排列。若旋轉或翻轉後相同視為同種樣式，試求此環所有可能之樣式數。

參、研究動機

某次討論時，教授提到了一個這樣的題目："Considering rotation and reflection, how many different necklaces consisting of six beads can be formed by using five different kinds of beads?"。我們嘗試使用高中數學排列組合的方法來解決這個問題，卻發現過程十分繁雜。於是教授便教導我們將群論運用在計數問題上的方法，讓我們成功解決這道題目。然而這樣的方法只能在珠子個數、種類數都是常數的時候使用。這讓我們十分好奇：如果珠子個數、種類數都是變數的話，那麼將會有什麼一般化的公式能解決此問題呢？於是我們便決定展開一連串的研究以推廣這個運用群論解決組合問題的方法。

肆、定義及先備知識

一、群 *Group*

(一)群由一個集合及一個二元運算所組成。

(二)群具有以下性質：

1. 具有單位元素。
2. 對於每一元素，皆存在反元素。
3. 運算具有封閉性。
4. 運算具有結合律。

(三)若一群 G 包含 n 個元素，則稱其階(O*rder*)$|G| = n$。

(四)舉例

1. 整數加法群 $(\mathbb{Z}, +)$
2. 二面體群 *Dihedral group*

由一正 n 邊形在平面上所有旋轉及翻轉所構成的群，以D_n表示。

以D_4為例，D_4以正方形之旋轉及翻轉構成，$D_4 = \{1, \rho^1, \rho^2, \rho^3, \tau_1, \tau_2, \tau_3, \tau_4\}$，其中，$\rho$為逆時針旋轉$\frac{\pi}{2}$；$\tau_1$、$\tau_2$、$\tau_3$、$\tau_4$分別為以正方形四條相異的對稱軸翻轉。

二、群作用 *Group action*

令 X 為一集合，G 為一個群，則 G 在 X 的(左)群作用是一個映射 $*$：$G * X \to X$，且滿足：

(一) $\forall x \in X\ 1 * x = x$

(二) $\forall g_1, g_2 \in \mathrm{G}\ \forall x \in X\ g_1 * (g_2 * x) = (g_1 * g_2) * x$

若 G 在 X 上作用，則稱 X 為一個 G-*set*。

三、*Orbit*

令 X 為一個 G-*set*，$x \in X$。

(一)定義 x 的 *Orbit* 為$G * x = \{g * x \mid g \in G\}$。

注意到 X 可被所有 G 作用於 X 上的相異 *Orbits* 所分割

(二)對於$g \in G$，定義$F(g) = \{x \in X \mid g * x = x\}$。

四、*Burnside's lemma*

若 n 為「G 作用於一 *G-set* 上之相異 *Orbit* 的數量」，則可求得：

$$n = \frac{1}{|G|}\sum_{g\in G}|F(g)|$$

五、*Euler's phi function*

對一正整數 n，定義 $\varphi(n)$是小於或等於 n 中，與 n 互質的正整數數目。注意到其為積性函數，即對於兩互質自然數 a,b，有$\varphi(ab)=\varphi(a)\times\varphi(b)$。

若 n 可被質因數分解為 $n={p_1}^{q_1}\times{p_2}^{q_2}\times\cdots\times{p_r}^{q_r}$，則

$$\varphi(n)=n\prod_{i=1}^{r}\frac{p_i-1}{p_i}$$

伍、研究過程

若我們共有 k 種珠子，對於由 n 個珠子所構成的環型串珠$P_1P_2\cdots P_n$，令$b_1,b_2,\cdots,b_n$為小於等於 k 之正整數，依序代表$P_1,P_2,\cdots,P_n$各個頂點上所使用的珠子種類。任何依此方式構造的數列 $\langle b_i\rangle_{i=1}^{n}$ 皆可表示一種獨特的串珠排列方式。定義集合 $B_n=\{\langle b_i\rangle_{i=1}^{n}|b_i\in\mathbb{N},b_i\in[1,k]\}$，則 B_n可表示串珠在不考慮旋轉及翻轉下，所有排列方式的集合。顯然 $|B_n|=k^n$。

現考慮所有可能的旋轉及翻轉，可用一二面體群 $D_n=\{1,\rho,\rho^2,\cdots\cdots,\rho^{n-1},\tau_1,\tau_2,\dots,\tau_n\}$ 表示此串珠所有可能的旋轉或翻轉。其中ρ表示將此 n 邊形逆時針旋轉 $\frac{2\pi}{n}$，$\tau_1,\tau_2,\cdots,\tau_n$分別表示將此 n 邊形以 n 條相異對稱軸進行翻轉。考慮 D_n 在集合 B_n 上的群作用，所求之樣式數 $\mathcal{A}(n,k)$ 即為集合 B_n 被 D_n 所分割出 *Orbit* 數量的總和。

由 *Burnside's lemma*，有：$\mathcal{A}(n,k)=\frac{1}{|D_n|}\sum_{g\in D_n}|F(g)|$。

以$n=6$、ρ^2為例，$B_6=\left\{\langle b_i\rangle_{i=1}^{6}\middle|b_i\in\mathbb{N},b_i\in[1,k]\right\}$。對於任意 $x\in B_6$，若 x 滿足$\rho^2*x=x$，亦即 x 逆時針旋轉 $\frac{2\pi}{3}$ 後，各點$P_1,P_2,\cdots,P_6$上的珠子種類沒有改變(即串珠排列方式相同)，則 $x\in F(\rho^2)$。

操作後可得知，若旋轉前後串珠排列方式相同，則旋轉前P_1,P_3,P_5上的珠子種類必須相同，P_2,P_4,P_6上的珠子種類也必須相同。若珠子種類有 k 種，$|F(\rho^2)|=k^2$。

以此類推，則若要計算 $n=6$，$k=5$ 的串珠樣式數，須考慮二面體群 $D_6=\{1,\rho^1,\rho^2,\rho^3,\rho^4,\rho^5,\tau_1,\tau_2,\tau_3,\tau_4,\tau_5,\tau_6\}$在$B_6$上的群作用構造出的所有相異 *Orbits*，亦即 $\mathcal{A}(6,5)=\frac{1}{12}[|F(1)|+|F(\rho^1)|+|F(\rho^2)|+|F(\rho^3)|+|F(\rho^4)|+\left|F(\rho^5)\right|+|F(\tau_1)|+|F(\tau_2)|+|F(\tau_3)|+|F(\tau_4)|+|F(\tau_5)|+|F(\tau_6)|]$。在此將 τ_1、τ_2、τ_3 分別定義為以六邊形串珠過兩頂點的相異對稱軸進行翻轉，τ_4、τ_5、τ_6 分別定義為以六邊形串珠過兩對邊中點的相異對稱軸進行翻轉。則由前述的例子可計算出以下結果：

$$\begin{cases}|F(1)|=k^n=15625\\ |F(\rho^1)|=\left|F(\rho^5)\right|=k^1=5\\ |F(\rho^2)|=|F(\rho^4)|=k^2=25\\ |F(\rho^3)|=k^3=125\\ |F(\tau_1)|=|F(\tau_2)|=|F(\tau_3)|=k^4=625\\ |F(\tau_4)|=|F(\tau_5)|=|F(\tau_6)|=k^3=125\end{cases}$$

故$\mathcal{A}(6,5)=(15625+5+25+125+25+5+625\times3+125\times3)\div12$
$=18060\div12=1505$

在可串入六顆串珠的環中，若使用五種珠子總共有1505種方法。

接著考慮 n 與 k 皆為變數的情況。

一、考慮串珠之翻轉

(一) n 為奇數

若 $2 \nmid n$，則此正 n 邊形的 n 條對稱軸為各頂點的角平分線，令τ_i是以$\angle P_i$之角平分線為軸所進行的翻轉($i = 1, 2, 3, \cdots, n$)。

顯然$|F(\tau_i)| = k^{\frac{n+1}{2}}$，$\mathrm{i} = 1, 2, \cdots, n$。

故當 n 為奇數時， $\sum_{i=1}^{n} |F(\tau_i)| = nk^{\frac{n+1}{2}}$。

(二) n 為偶數

1. 以對角線為對稱軸

若$2 \mid n$，則此正 n 邊形的 n 條對稱軸中有 $\frac{n}{2}$ 條過 2 個頂點，令τ_i是以$\overleftrightarrow{P_i P_{i+\frac{n}{2}}}$為軸所進行的翻轉($i = 1,2,3, \cdots, \frac{n}{2}$)。

顯然$|F(\tau_i)| = k^{\frac{n}{2}+1}$，$i = 1, 2, 3, \cdots, \frac{n}{2}$。

當 n 為偶數，以對角線為軸時，$\sum_{i=1}^{n/2} |F(\tau_i)| = \frac{n}{2} k^{\frac{n}{2}+1}$。

2. 以中線為對稱軸

另外 $\frac{n}{2}$ 條對稱軸經過 2 個對邊，令M_i為$\overline{P_i P_{i+1}}$的中點($i = 1, 2, \cdots, n-1$)，M_n為$\overline{P_n P_1}$的中點，令τ_i是以$\overleftrightarrow{M_{i-\frac{n}{2}} M_i}$為軸所進行的翻轉($i = \frac{n}{2} + 1, \frac{n}{2} + 2, \cdots, n$)。

顯然$|F(\tau_i)| = k^{\frac{n}{2}}$，$i = \frac{n}{2} + 1, \frac{n}{2} + 2, \cdots, n$。

當 n 為偶數，以中線為軸時，$\sum_{i=\frac{n}{2}+1}^{n} |F(\tau_i)| = \frac{n}{2} k^{\frac{n}{2}}$。

(三)小結

1. 當 n 為奇數時， $\sum_{i=1}^{n} |F(\tau_i)| = nk^{\frac{n+1}{2}}$。
2. 當 n 為偶數時，$\sum_{i=1}^{n} |F(\tau_i)| = \frac{n}{2}(1+k)k^{\frac{n}{2}}$。

二、考慮串珠之旋轉

(一)引理I

令$\mathrm{a}, i, n \in \mathbb{Z}$，$d = gcd(i, n)$，則

x 的同餘方程式 $i \cdot x \equiv a (mod\, n)$有整數解 $\Leftrightarrow d \mid a$

1. 證明

($\Leftarrow$)： $\because d = gcd(i, n)$

$\therefore \exists\, x_0, y_0 \in \mathbb{Z}\ \mathrm{s.t.}\ d = ix_0 + ny_0$

$\therefore \exists\, \ell \in \mathbb{Z}\ \mathrm{s.t.}\ a = \ell d = \ell(ix_0 + ny_0)$

$\Rightarrow n(-y_0 \ell) + a = (\ell x_0)\, i$

$\Rightarrow i\, (\ell x_0) \equiv a (mod\, n)$■

($\Rightarrow$)： $\because i \cdot x \equiv a (mod\, n)$ 有整數解

$\therefore \exists\, x, y \in \mathbb{Z}\ \mathrm{s.t.}\ ix = ny + a$

$\Rightarrow a = ix - ny$

$\because d = gcd(i, n)\ \therefore d \mid \mathrm{i}, d \mid n$

$\Rightarrow d \mid ix - ny$

$\Rightarrow d \mid a$ ■

2. 推論

令$d=gcd(n,i)$，$rem_n(p_1+p_2)=(p_1+p_2)\div n$之餘數。

因為在被ρ^2作用後，各點上的珠子種類沒有改變，所以

$$\begin{cases} b_1=b_{rem(1+i)}=b_{rem(1+2i)}=b_{rem(1+3i)}=\cdots \\ b_2=b_{rem(2+i)}=b_{rem(2+2i)}=b_{rem(2+3i)}=\cdots \\ \vdots \\ b_d=b_{rem(d+i)}=b_{rem(d+2i)}=b_{rem(d+3i)}=\cdots \end{cases}$$

由引理I可得所有i的倍數除以n所得的餘數集合便是所有小於n的d的倍數所構成的集合，故：

$$\begin{cases} 1,rem(1+i),rem(1+2i),rem(1+3i)\cdots\in\{1,d+1,2d+1,\cdots,n-d+1\} \\ 2,rem(2+i),rem(2+2i),rem(2+3i)\cdots\in\{2,d+2,2d+2,\cdots,n-d+2\} \\ \vdots \\ d,rem(d+i),rem(d+2i),rem(d+3i)\cdots\in\{d,2d,3d,\cdots,n\} \end{cases}$$

故

$$\begin{cases} b_1=b_{d+1}=b_{2d+1}=\cdots=b_{n-d+1} \\ b_2=b_{d+2}=b_{2d+2}=\cdots=b_{n-d+2} \\ \vdots \\ b_d=b_{2d}=b_{3d}=\cdots=b_n \end{cases}$$

$\therefore\left|F(\rho^i)\right|=k^d=k^{\gcd(n,i)}$

(二)引理II

設$d,n\in\mathbb{N}$且$d\mid n$，$i\in\{1,2,\cdots,n\}$，則恰有$\varphi(\frac{n}{d})$個i值滿足$gcd(n,i)=d$。

1. 證明

若$gcd(n,i)=d$，則i為d的倍數且$\frac{n}{d}$與$\frac{i}{d}$互質，亦即$i\in\left\{d,2d,\cdots,\left(\frac{n}{d}\right)d\right\}$且$gcd\left(\frac{n}{d},\frac{i}{d}\right)=1$。因為$\frac{i}{d}\in\left\{1,2,\cdots,\frac{n}{d}\right\}$，而在此$\frac{n}{d}$個正整數中有$\varphi(\frac{n}{d})$個數與$\frac{n}{d}$互質，故恰有$\varphi(\frac{n}{d})$個$i$值滿足$gcd(n,i)=d$。

2. 推論

由引理II可推得，對於所有n的正因數d，皆存在$\varphi\left(\frac{n}{d}\right)$個小於等於$n$的正整數使$k^{gcd(n,i)}=k^d$，所以：

$$\sum_{i=0}^{n-1}\left|F(\rho^i)\right|=\sum_{i=1}^{n}\left|F(\rho^i)\right|=\sum_{i=1}^{n}k^{\gcd(n,i)}=\sum_{d|n}\varphi\left(\frac{n}{d}\right)k^d$$

三、總結

綜合以上，則對於$n\in\mathbb{N}$，$k\in\mathbb{N}$，

$$\mathcal{A}(n,k)=\frac{1}{|D_n|}\sum_{g\in D_n}|F(g)|=\frac{1}{2n}\left[\sum_{i=0}^{n-1}\left|F\left(\rho^i\right)\right|+\sum_{i=1}^{n}|F(\tau_i)|\right]$$

$$=\begin{cases} \frac{1}{2n}\left[\sum_{d|\mathrm{n}}\varphi\left(\frac{n}{d}\right)k^d+\frac{n}{2}(1+k)k^{\frac{n}{2}}\right], & 2\mid n \\ \frac{1}{2n}\left[\sum_{d|\mathrm{n}}\varphi\left(\frac{n}{d}\right)k^d+nk^{\frac{n+1}{2}}\right], & 2\nmid n \end{cases}$$

陸、討論

一、定義

給定一正整數 n，對於 $\mathcal{A}(n,x)$可得一 x 的多項式。現若將 n 的定義域擴展至任意非 0 整數，x 的定義域擴展至任意實數，我們可以將$\mathcal{A}(n,x)$重新定義並表示為以下連續函數：

$$y = a_n(x) = \begin{cases} \dfrac{1}{2n}\left[\displaystyle\sum_{d|\mathrm{n},\mathrm{dn}>0} \varphi\left(\frac{n}{d}\right)x^d + \frac{n}{2}(1+x)x^{\frac{n}{2}}\right], & 2 \mid n \\ \dfrac{1}{2n}\left[\displaystyle\sum_{d|\mathrm{n},\mathrm{dn}>0} \varphi\left(\frac{n}{d}\right)x^d + nx^{\frac{n+1}{2}}\right], & 2 \nmid n \end{cases}$$

注意到當 $n < 0$ 時，$d < 0$。

二、性質

進一步觀察，$y = a_n(x)$具有以下性質：

(一) $\forall n > 0$，$a_n(0) = 0$。

(二) $a_n(1)$有兩種情形：

1. 當 $n > 0$，$a_n(1) = 1$。
2. 當 $n < 0$，$a_n(1) = 0$。

(三) $a_n(-1)$有五種情形：

1. 當 $2 \mid n$，$a_n(-1) = 0$。
2. 當 $n \equiv 1 \ (mod\ 4)$時，若$n > 0$，$a_n(-1) = -1$。
3. 當 $n \equiv 1 \ (mod\ 4)$時，若$n < 0$，$a_n(-1) = 0$。

   注意到對於情形 2、3，$y = a_n(x)$為奇函數。
4. 當 $n \equiv 3 \ (mod\ 4)$，$n > 0$，$a_n(-1) = 0$。
5. 當 $n \equiv 3 \ (mod\ 4)$，$n < 0$，$a_n(-1) = -1$。

(四) $y = a_n(x) = 0$的解

1. 若$2 \mid n$，$n \neq 0$

$$y = a_n(x) = \frac{1}{2n}\left[\sum_{d|\mathrm{n}} \varphi\left(\frac{n}{d}\right)x^d + \frac{n}{2}(1+x)x^{\frac{n}{2}}\right]$$

$$\text{解：}\begin{cases} n > 0,\ \text{有二實數解}(0,0),(-1,0) \\ n = -2,-4,\ \text{有二實數解}(\pm 1,0) \\ n \leq -6,\ \text{有三實數解}(\pm 1,0),(\alpha,0),\alpha \in (0,1] \end{cases}$$

2. 對於$n \equiv 1 \ (mod\ 4)$

$$y = a_n(x) = \frac{1}{2n}\left[\sum_{d|\mathrm{n}} \varphi\left(\frac{n}{d}\right)x^d + nx^{\frac{n+1}{2}}\right]$$

$$\text{解：}\begin{cases} n > 0,\ \text{有一實數解}(0,0) \\ n = -3,\ \text{有二實數解}(\pm 1,0) \\ n \leq -7,\ \text{有四實數解}(\pm 1,0),(,\pm\alpha,0),\alpha \in (0,1) \end{cases}$$

3. 對於$n \equiv 3\ (mod\ 4)$

$$y = a_n(x) = \frac{1}{2n}\left[\sum_{d|\mathrm{n}} \varphi\left(\frac{n}{d}\right) x^d + nx^{\frac{n+1}{2}}\right]$$

$$解：\begin{cases} n > 0,\ 有三實數解(0,0),(-1,0),(\alpha,0),\alpha \in [-2,-1) \\ n = -1,\ 有一實數解(1,0) \\ n \le -5,\ 有二實數解(1,0),(\alpha,0),\alpha \in (0,1) \end{cases}$$

特別的是，α 與 n 在上述各情形皆存在嚴格遞增關係。

基於以上各性質，我們推測$a_n(x)$或許有特別的因式分解形式。

（五）對於不為 2 的質數 n，$a_n(x) = 0$ 的複數根呈一正 $\frac{n-1}{2}$ 邊形。

說明：對於不為 2 的質數 n，有

$$a_n(x) = \frac{1}{2n}\left[x^n + (n-1)x + nx^{\frac{n+1}{2}}\right]$$

而其有一般性因式分解

$$\frac{1}{2n} \cdot x \cdot \left(x^{\frac{n-1}{2}} + 1\right) \cdot [x^{\frac{n-1}{2}} + (n-1)]$$

顯然$a_n(x) = 0$ 之複根可形成一雙層正 $\frac{n-1}{2}$ 邊形。

柒、結論

若給定兩自然數 n、k，則一個可串入 n 個珠子的環中，以 k 種相異種類且數量足夠的珠子進行排列，考慮旋轉及翻轉，則此環所有可能之樣式數$\mathcal{A}(n,k)$可以表示為：

$$\mathcal{A}(n,k) = \begin{cases} \frac{1}{2n}\left[\sum_{d|\mathrm{n}} \varphi\left(\frac{n}{d}\right) k^d + \frac{n}{2}(1+k)k^{\frac{n}{2}}\right], & 2 \mid n \\ \frac{1}{2n}\left[\sum_{d|\mathrm{n}} \varphi\left(\frac{n}{d}\right) k^d + nk^{\frac{n+1}{2}}\right], & 2 \nmid n \end{cases}$$

捌、未來展望

一、更加地化簡$\mathcal{A}(n,k)$。

二、探討更多有關$a_n(x)$的複數根及因式分解形式。

三、研究其他種類的環。

玖、參考資料

[1]Nicholson, W. K. (2012). *Introduction to Abstract Algebra* (4th ed.). NJ: John Wiley & Sons.

[2]Fraleigh, J. B. (2003). *A First Course in Abstract Algebra* (7th ed.). NJ: Pearson.