GroupAction10

2023年4月10日 星期一　　下午5:40

Cauthy's theorem

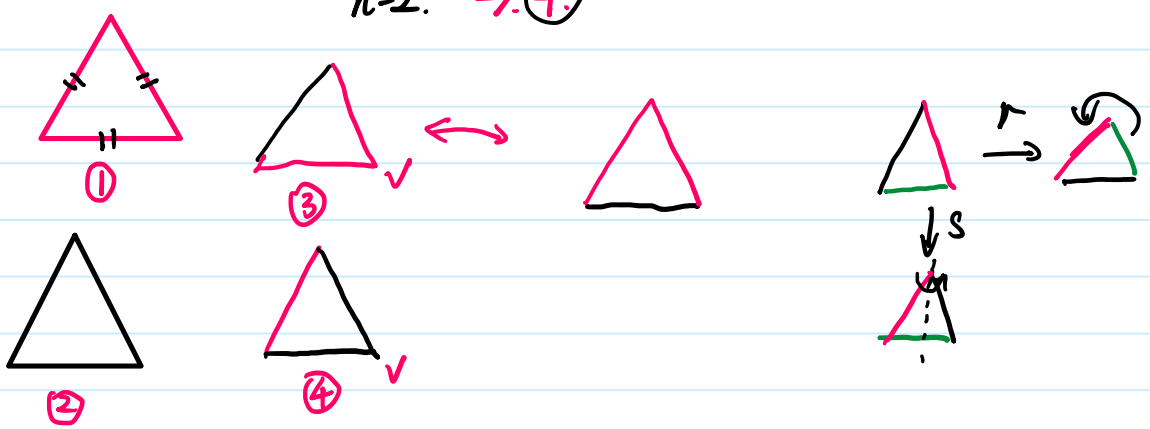
orbit counting formula.

Carley's theorem

Sylow's theorem.

How many essentially different ways can a triangle's edges be painted with n colours.　　equalateral

$n=2. \Rightarrow 4.$



n: The triangles sides might be coloured with 1, 2, 3 colourings.

$$n + C_n^2 \cdot 2 + C_n^3 = n + \frac{2n(n-1)}{2} + \frac{n(n-1)(n-2)}{6}$$

$$= \frac{n^3+3n^2+2n}{6}$$

$n=2.$　$\frac{8+12+4}{6} = 4.$

$S_3 = \{e, r, r^2, s, rs, rs^2\}$　conjugacy classes: $\{e\}$, $\{r, r^2\}$, $\{s, rs, rs^2\}$

$\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$ $\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$ $\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$ ...

S_3 acts on triangle. (Set: (R B Y))　3-space over $\mathbb{F}_n$.　$|\Omega| = n^3$.

3-space over n.

S_3 acts on triangle. (set: $(\underline{R},\underline{B},\underline{Y})$ $\begin{matrix}R&R&R\\B&B&Y\end{matrix}$ $|S| = n^3$.

$6 = 6\times 1$

$|G| = |\text{Stab}(s)| \times |\text{Orbit}(s)|$. $G \cong S_3$ S:

(R,R,R). $|\text{Stab}(s)| = |\{g: g\cdot s = s\}|$ $\forall g \in S_3$. $g\cdot(R,R,R) = (R,R,R)$

$G \geq |\text{Stab}(S)| = |S_3| = 6$.

$S \geq |\text{Orbit}(S)| = |\{g\cdot s\}| = |\{(R,R,R)\}| = 1$

(R,R,Y) $|\text{Stab}(s)| = |\{g; g\cdot s = s\}| = 2$ e. ✓ r. (Y,R,R) x.

r^2 x

$|\text{Orbit}(S)| = |\{g\cdot s\}| = 3$.

$r^2 s$. ✓

$(R,R,Y) = (R,R,Y) = r^2 s$ (R,R,Y) $(R\ Y\ R)_x$ $(R\ Y\ R)_x$

(Y,R,R) $(R\ Y\ R) = rs$

(R,Y,R) $(R\ Y\ R) = r$

$2\times 3 = 6$

(R,Y,B). $|\text{Stab}(S)| = 1$. (Y,B,R) ✓ (B,R,Y) ✓

e ✓ r r^2 x

$|\text{orb}(S)| = 6$. (B,Y,R) ✓ (R,B,Y) ✓ (Y,R,B) ✓

$g\cdot S = S$. $1\times 6 = 6$

$e\cdot S = S$

Orbit counting theorem: Let G be a finite group acting on a finite set S.

Then # orbits $= \frac{1}{|G|}\sum_{g\in G} |\text{fix}(g)|$ ✓

$\forall g\in G$. we define $\text{fix}(g) = |\{s\in S: g\cdot s = s\}|$.

$\text{stab}(s) = |\{g\in G: g\cdot s = s\}|$

proof: consider the set $A = \{(g,s): g\cdot s = s\} \subseteq G\times S$

count $|A|$ in two different ways. (double counting).

$$|A| = \sum_{g\in G} |\{s\in S : g\cdot s = s\}| = \sum_{s\in S} |\{g\in G : g\cdot s = s\}|$$

$$= \sum_{g\in G} |\mathrm{fix}(g)| = \sum_{s\in S} |\mathrm{Stab}(s)| \quad = N|G|$$

Orbits: $O_1, O_2 \cdots O_N$. then. orbits partition S.

$$\sum_{s\in S} |\mathrm{Stab}(s)| = \sum_{i=1}^{N} \sum_{s\in O_i} |\mathrm{Stab}(s)|$$

Orbit-stabilizer theorem:

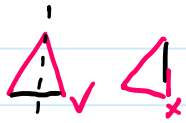
$$\sum_{i=1}^{n} \sum_{s\in O_i} |\mathrm{Stab}(s)| = \sum_{i=1}^{n} \sum_{s\in O_i} \frac{|G|}{|O_i|} = \sum_{i=1}^{n} |G| = N\cdot|G|.$$

$$\underbrace{\frac{|G|}{|O_i|} + \frac{|G|}{|O_i|} + \cdots \frac{|G|}{|O_i|}}_{|O_i|} = \frac{|G|}{|O_i|}\cdot|O_i| = |G|.$$

$$N = \frac{1}{|G|}\sum_{g\in G} |\mathrm{fix}(g)| = \#\text{ orbits}. \qquad \square$$

Continue.

	g	# conjugates.	s fixed by g	$\lvert\mathrm{fix}(g)\rvert$.	#
	e	1	all	n^3.	$1\cdot n^3$
n^3.	r, r^2	2	same colour.	n	$2\cdot n$
	s, rs r^2s.	3.	two colours.	n^2.	$3\cdot n^2$.



orbit counting formula: # orbits $= \frac{1}{|G|}\sum_{g\in G} |\mathrm{fix}(g)|$

$$= \frac{1}{6}\cdot(n^3 + 2n + 3n^2) \quad \triangle$$

How many different triples (x_1, x_2, x_3) of positive integers are there s.t.

$$\underbrace{x_1}_{1\sim 98} + \underbrace{x_2}_{1\sim 99-x_1} + x_3 = 100 \qquad \underbrace{x_1 \le x_2 \le x_3}_{\triangle}.$$

$x_1+x_2+x_3=100$ $\quad x_1\le x_2\le x_3$.

1-98 $\quad$ 1-(99-x_1)

$S=\{(x_1,x_2,x_3): x_i\ge 1, x_1+x_2+x_3=100\}$. $\Leftarrow S_3$.

$$|S|=\sum_{x_1=1}^{98}(99-x_1)=\frac{1}{2}\times 99\times 98=4851.$$

e (32) (21) (123)

$\begin{pmatrix}123\\123\end{pmatrix}$ $\begin{pmatrix}123\\132\end{pmatrix}$ $\begin{pmatrix}123\\213\end{pmatrix}$ $\begin{pmatrix}123\\231\\123\end{pmatrix}$

$\begin{pmatrix}123\\312\end{pmatrix}$ $\begin{pmatrix}123\\321\end{pmatrix}$

(132) (13).

g	# conjugates	s fixed by g	fix(g)	
e	1	(x_1,x_2,x_3)	4851	1×4851
(12) (13) (32)	3	(x_1,x_1,x_3)	49.	3×49
(123) (132)	2.	(x_1,x_1,x_1)	0.	0.

$2x_1+x_3=100$

1-49.

$3x_1=100$

orbit counting formula: $\frac{1}{6}\cdot(4851+147)=833.$

Cauchy. theorem: Let G be a finite group and let p be a prime dividing $|G|$. Then G has an element of order p.

proof: Let S denote the set:

$S=\{(g_1,\cdots g_p)\in G^p: g_1g_2\cdots g_p=e\}$.

$(e,e,e\cdots e)$.

p^α. $\alpha=1$

$|S|=|G|^{p-1}$: $g_p=(g_1\cdots g_{p-1})^{-1}$.

Let $\sigma=(1,2,\cdots p)$. $\quad \langle\sigma\rangle\cong C_p$.

$\sigma^2=(135\cdots)$.

$\sigma^3=\cdots$

$\in S$ group action:

$\sigma\cdot(g_1,g_2\cdots g_p)=(g_2,g_3\cdots g_p,g_1)\in S$.

$g_1g_2\cdots g_p=e$. $\quad g_1^{-1}=g_2g_3\cdots g_p$.

$g_2g_3\cdots g_p\cdot g_1=e$.

$(g_2,g_3,\cdots g_p,g_1)\in S$.

$g_2 g_3 \cdots g_p \cdot g_1 = e$.

$(g_2, g_3, \cdots g_p, g_1) \in S$.

$= p$.

orbits of action: $|G| = |Stab(s)| \times |Orb(s)|$.

$\Rightarrow$ $Orb(s)$ may have size 1 or p.

$\sigma \cdot (g_1, g_2, \cdots g_p) = (g_2, g_3 \cdots g_p, g_1) = (g_1, g_2, \cdots g_p)$.

$g_1 = g_2 = g_3 \cdots = g_p$ and $(g_1)^p = e$. $\{(e, \cdots e)\}$.

orbits patition S.

$$|S| = 1 \cdot k + l \cdot p = k + lp = |G|^{p-1}.$$

p divides $|G|$. $\Rightarrow$ p divides $|S|$. $\Rightarrow$ p divides k.

$k \geq 1$. there is at least one other singleton orbits. $g^p = e$.

$\{(g, g, \cdots g)\}$ $g \neq e$. $\square$

Theorem: Given a left action of a group G on a set S there is an associated homomorphism:

$$\rho: G \to Sym(S).$$

To each homomorphism $\rho: G \to Sym(S)$ there is an associated left action of G on S.

$s \xrightarrow{\rho_g} gs$, $\rho_{g^{-1}}$

proof: $g \in G$. $\rho_g: S \to S$ $\rho_g(s) = g \cdot s$. is a bijection

$\Rightarrow$.

$$\rho_{g^{-1}}(s) = g^{-1} \cdot s$$

$\rho: G \to Sym(S)$. $g \to \rho_g$. is a homomorphism.

$$\rho_{gh}(s) = gh \cdot s = g \cdot (h \cdot s) = \rho_g(\rho_h(s)) = (\rho_g \rho_h) \cdot (s).$$

$\rho_{gh}(s) = gh \cdot s = g \cdot (h \cdot s) = \rho_g(\rho_h(s)) = (\rho_g \rho_h) \cdot (s)$.

$\Leftarrow$ $\rho: G \to Sym(S)$ homomorphism

$g \cdot s = (\rho(g)) \cdot s$. $\forall s \in S$, $g, h \in G$. ① $e \cdot s = s$

$e \cdot s = (\rho(e))(s) = id(s) = s$.

② $(gh) \cdot s = g \cdot (h \cdot s)$.

$(gh) \cdot s = \rho(gh)(s) = \rho(g)[\rho(h)(s)] = g \cdot [\rho(h)(s)] = g \cdot (h \cdot s)$ □

Cayley's theorem: Every finite group is isomorphic to a subgroup of some permutation group S_n.

proof: G acts on itself: $g \cdot h = gh$ $\in G$ $\in G = S$.

$\rho: G \to Sym(G)$

① $(g_1 h_1)(g_2 h_2) g_3 h_3)$

② $h^{-1} h = e$. $g = h^{-1}$

③ $gh \cdot (g)^{-1} =$ $h^{-1} g^{-1} \in \rho(G)$

Let G be a finite group. $\rho(g_i)$ is a permutation of G. $g = h^{-1} \cdot g^{-1} \cdot h^{-1}$. $gh = h^{-1} g^{-1}$.

ρ is one-to-one:

$\rho(g_i) = \rho(g_j) \Rightarrow \rho(g_i)(e) = \rho(g_j)(e) \Rightarrow g_i e = g_j e \Rightarrow g_i = g_j$.

Hence G is isomorphic with the image of $\rho(G) \leq Sym(G) \cong S_n$. □.

Sylow's theorem: Let G be a group of order $p^\alpha m$.

where p is a prime, $m \geq 1$ p does not divide m.

(i). a subgroup of order p^α (Sylow p-subgroup). exists. ✓

(ii). All Sylow p-groups are conjugate in G.

$P_1 = g P_2 g^{-1}$.

(iii). group of order p^k. $k \geq 1$ p-group.

(iii). group of order p^k. $k \geq 1$. p-group.

subgroup of of order p^k $k \geq 1$ p-subgroup.

Any p-subgroup of G is contained in Sylow p-subgroup.

(iv): $n_p(G)$. the number of Sylow p-subgroups of G.

$n_p(G) \equiv 1 \bmod p$.