7 Group

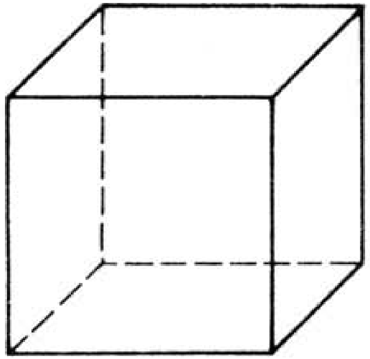
7-1 Turnable World

组合数学 Combinatorics

清华大学 马昱春
Tsinghua University
Associate Professor Ma

Permutation and Combination on the Blackboard

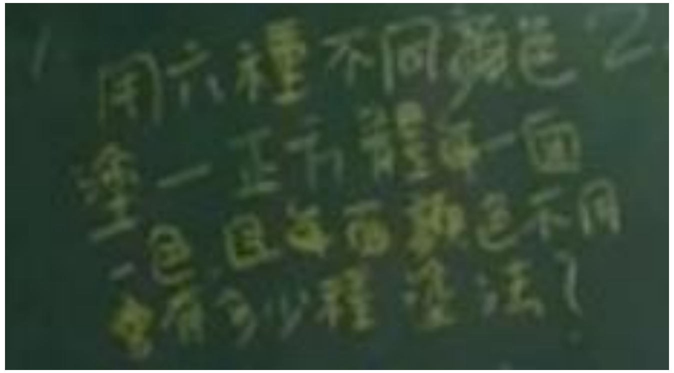
Use 6 different types of colors to paint a cube, each face with one color, whereas each is colored with a different color, how many painting ways are there?



$$6*5*P(4,4)/4\ /\ 6 = 30$$

Use 6 different colors to paint a cube, each side one color and **different sides may use the same color**, how many different kinds of coating are there?

黑板上排列組合　妳捨得解開嗎



1. 用六種不同顏色 2

塗一正方體每一面

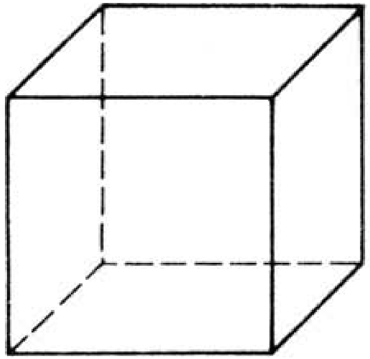
一色且每面顏色不同

共有多少種塗法?

Counting Rule

- Encountered difficulties during counting
  - – Difficulty in finding out the expression of general solutions
    - Bring in generating function
  - – Difficulty in distinguishing the classification, distinguishing similarity of nature, avoid repetitions and losses
    - Inclusion-exclusion principle to avoid double-counting
    - How to distinguish the classifciations?

Turnable World??



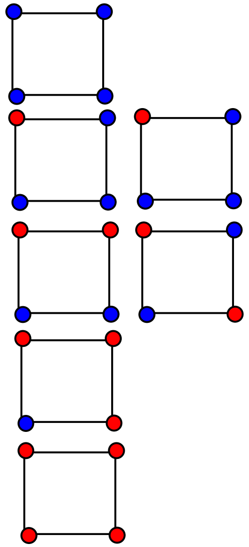
Turn-able World

- For Example
  - Use red and blue these 2 colors to paint the 4 corners of a square, how many different ways are there?

Quiz 2^4

  - If square is allowed to rotate, how many different ways are there?
  - Classification： Classify by red dot

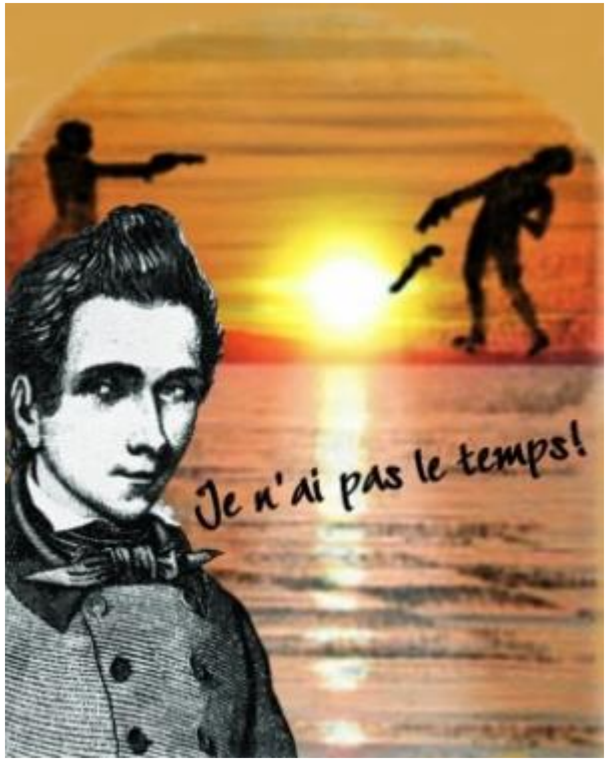
• 0 red dot	1 type
• 1 red dot	1 type
• 2 red dots	2 types
• 3 red dots	1 type
• 4 red dots	1 type



Total 6 types

- An early morning in the year of 1832……
- The revolution of French witnessed another duel……
- In a moment, a youth was shot in his abdomen by the opponent; and passed away……
- The whole world lost a great mind again.
- This 21 years old youth named Galois……

Group



Evariste Galois

- Évariste Galois(1811~1832)
- Galois introduced the new term of "group" and laid its foundation.
- he was able to determine a necessary and sufficient condition for a polynomial to be solvable by radicals, thereby solving a 350 years-standing problem.
- In 1846, Liouville realized the burst of genius ideas from the manuscript, he used several months trying to explain its meaning.
- **He is recognized as one of the two most romanticism figures in the history of mathematic**
- His death had caused the delayed of the mathematic development for decades
- This man was sent by God, hurriedly round the world, for only 21 years, but without any intension, he opened up a new generation for mathematic ……..

http://baike.baidu.com/view/251169.htm

Galois wrote in his research report in San Pedro Prison:

“**Classify** the arithmetical operation, learn to classify according to the degree of difficulty, but not according to their external characteristics, this is what I understand for the mathematicians’ task in the future, and this is the way I wish to go.”

The Concept of Group

Group

Definition A given **Set *G*** and **the binary operation** of *G*, satisfy the following condition is called group.

(a) 封闭性(Closure):

If $a, b \in G$, then exist $c \in G$, that $a \cdot b = c$.

(b) 结合律(Associativity):

Any $a, b, c \in G$, there is $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

Due to the establishment of associative law, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ can be noted as $a \cdot b \cdot c$.

(c) 有单位元(Identity):

Exist $e \in G$, any $a \in G$. $a \cdot e = e \cdot a = a$.

(d) 有逆元(Inverse):

Any $a \in G$, exist $b \in G$, $a \cdot b = b \cdot a = e$. note as $b = a^{-1}$.

The Concept of Group

Example 1*1=?

G={1} under normal multiplication is group

Example *G*={1,-1} under normal multiplication is group.

Proof： 1) Closure:1 × 1=1 (-1) × (-1)=1 (-1) × 1=-1 1 × (-1)=-1

2) Associativity: Founded

3) Identity: 1

4) Inverse: The inverse element of 1 is 1， the inverse element of -1 is -1

Example G={0,1,2,…,n-1}with the operation of the addition of *mod n* is group.

Proof：1) Closure: The remainder for the division of n can only be {0,1,2,…,n-1}，

Therefore closure is satisfied

2) Associativity: Satisfied

3) Identity: 0

4) Inverse: To any element a has (a+(n-a)) *mod* n = 0 ,

the inverse element of a is $a^{-1}=n-a$

The Concept of Group

Example All rigid items rotation in two dimensional Euclidean space

$T = \{Ta\}$ form a group. Among, $Ta = \begin{pmatrix} \cos a & \sin a \\ -\sin a & \cos a \end{pmatrix}$

Proof: 1) Closure: $TbTa = \begin{pmatrix} \cos b & \sin b \\ -\sin b & \cos b \end{pmatrix} \begin{pmatrix} \cos a & \sin a \\ -\sin a & \cos a \end{pmatrix}$

$$= \begin{pmatrix} \cos a \cos b - \sin a \sin b & \sin a \cos b + \cos a \sin b \\ -\sin a \cos b - \cos a \sin b & \cos a \cos b - \sin a \sin b \end{pmatrix}$$

$$= \begin{pmatrix} \cos(a+b) & \sin(a+b) \\ -\sin(a+b) & \cos(a+b) \end{pmatrix} = T(b+a)$$

1) Closure:

2)Associativity: Satisfied $(T_\alpha T_\beta)T_\gamma = T_\alpha(T_\beta T_\gamma) = T_\alpha T_\beta T_\gamma$

3) Identity: $T_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

4) Inverse Element: Inverse element of *Ta* is *T-a*

The Concept of Group

- If the number of group elements is limited, it is called finite group；
- If the number of group element is unlimited, it is called infinite group。
- The number of elements of finite group *G* is known as the order of group, noted as $|G|$。
- Set *G* as group, *H* is the subset of *G*, if *H* is still a group under *G* inherited operation, it is known as *G*’s subgroup.
- If any two elements *a* and b in group *G*, we have $ab=ba$. Then we call *G* as commutative group, or Abelian group.

The Concept of Group

(a) Unique Identity $e_1e_2 = e_2 = e_1$

(b) Cancellation Law stands $ab = ac \longrightarrow b = c$,

$$ba = \mathrm{ca} \longrightarrow \mathrm{b} = \mathrm{c}$$

(c) The unique inverse element of each element $aa^{-1}=a^{-1}a = e$,

$$ab^{-1} = ba^{-1} = e\ ,\ \ aa^{-1} = ab^{-1}\ ,\ a^{-1}=b$$

(d) $(ab....c)^{-1} = c^{-1}\ldots b^{-1}a^{-1}$.

$$c^{-1}\ldots b^{-1}a^{-1}\cdot ab\ldots c = e$$

The Concept of Group

（e） G is limited, $a\in G$, then exist the smallest positive integer r, that $a^r = e$ and $a^{-1} = a^{r-1}$.

Proof Let $|G|=g$, then $a,a^2 ,\ldots,a^g,a^{g+1}\in G$,

From the pigeonhole principle, there will be the identical items. Set $a^m =a^l$, $1\leq m < l\leq g+1$, $e=a^{l-m}$,$1\leq l-m\leq g$,

Let $l\text{-}m=r$. Then there is $a^r =a^{r-1}a=e$, which is $a^{-1}=a^{r-1}$.

Since there is positive integer r that $a^r = e$, among which we could find the smallest, assume to be r. r known as the order of a. It can be seen that $H=\{a,a^2 ,\ldots a^{r-1} ,a^r =e\}$ under its inherited operations is also a group.

7 Group

7-2 Permutation Group

清华大学 马昱春
Tsinghua University
Associate Professor Ma

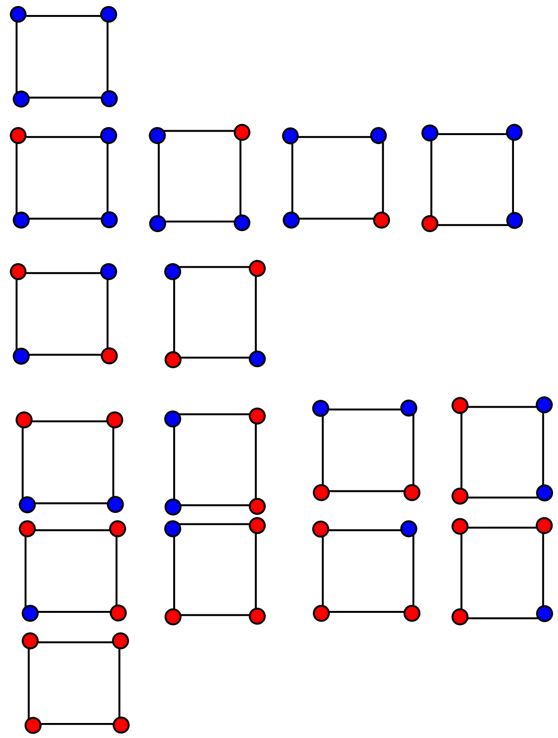
组合数学 Combinatorics

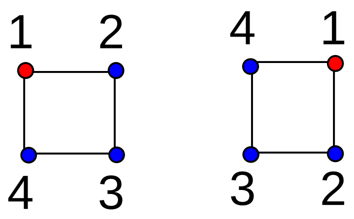
着色问题的等价类

- Use red and blue these 2 colors to paint the top 4 corners of a cube, how many different ways are there?

  2^4

- If square turning is allowed, how many different ways are there?
- **The representation for rotation?**





Rotate 90º
(1234) →(4123)

How to represent？

Permutation Group

- Permutation group is the most important finite group, all finite group can be represented by permutation group.
- Permute: 1-1 mapping on set [1,n] is called as *n-order* permutation. Represented as $\begin{pmatrix} 1 & 2 & \cdots & n \\ a1 & a2 & \cdots & an \end{pmatrix}$, $a_1a_2\ldots a_n$ is one of the arrangements in [1,*n*].
- *N*-order permutation contains *n* arrangement. The same permutation may have *n*! representations. For example, $p_1=\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} = \begin{pmatrix} 3 & 1 & 4 & 2 \\ 2 & 3 & 4 & 1 \end{pmatrix}$, *n* order permutation can be viewed as unary operation on [1, *n*], or a unary function.

Permutation Group: Permutation Set and **Binary Operation**

Permutation Group

- Permutation Multiplication $P_1=\begin{pmatrix}1 & 2 & 3 & 4\\ 3 & 1 & 2 & 4\end{pmatrix}$, $P_2=\begin{pmatrix}1 & 2 & 3 & 4\\ 4 & 3 & 2 & 1\end{pmatrix}$

  $P_1P_2=\begin{pmatrix}1 & 2 & 3 & 4\\ 3 & 1 & 2 & 4\end{pmatrix}\begin{pmatrix}3 & 1 & 2 & 4\\ 2 & 4 & 3 & 1\end{pmatrix}=\begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 4 & 3 & 1\end{pmatrix}$

  $P_2P_1=\begin{pmatrix}1 & 2 & 3 & 4\\ 4 & 3 & 2 & 1\end{pmatrix}\begin{pmatrix}4 & 3 & 2 & 1\\ 4 & 2 & 1 & 3\end{pmatrix}=\begin{pmatrix}1 & 2 & 3 & 4\\ 4 & 2 & 1 & 3\end{pmatrix}$.
- $P_2P_1 \neq P_1P_2$.
- Permutation does not satisfy commutative Law
- But it satisfied Associative Law

Permutation Group

- (1) Permutation Group

A permutation group is a group G whose elements are permutations of a given set [1,n] and whose group operation is the composition of permutations in G which are thought of as bijective functions from the set [1,n] to itself.

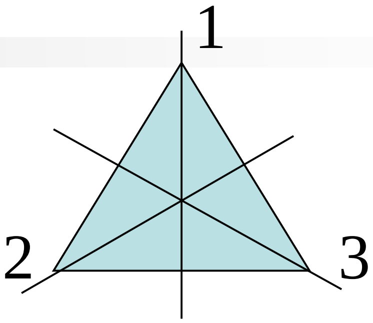
- (a) **Closure** $\begin{pmatrix}1 & 2 & \ldots & n\\ a_1 & a_2 & \ldots & a_n\end{pmatrix}\begin{pmatrix}a_1 & a_2 & \ldots & a_n\\ b_1 & b_2 & \ldots & b_n\end{pmatrix}=\begin{pmatrix}1 & 2 & \ldots & n\\ b_1 & b_2 & \ldots & b_n\end{pmatrix}$
- (b) **Associativity**
- $\left(\begin{pmatrix}1 & 2 & \ldots & n\\ a_1 & a_2 & \ldots & a_n\end{pmatrix}\begin{pmatrix}a_1 & a_2 & \ldots & a_n\\ b_1 & b_2 & \ldots & b_n\end{pmatrix}\right)\begin{pmatrix}b_1 & b_2 & \ldots & b_n\\ c_1 & c_2 & \ldots & c_n\end{pmatrix}=\begin{pmatrix}1 & 2 & \ldots & n\\ c_1 & c_2 & \ldots & c_n\end{pmatrix}$

$$=\begin{pmatrix}1 & 2 & \ldots & n\\ a_1 & a_2 & \ldots & a_n\end{pmatrix}\left(\begin{pmatrix}a_1 & a_2 & \ldots & a_n\\ b_1 & b_2 & \ldots & b_n\end{pmatrix}\begin{pmatrix}b_1 & b_2 & \ldots & b_n\\ c_1 & c_2 & \ldots & c_n\end{pmatrix}\right)$$

- (c) **Identity** e=$\begin{pmatrix}1 & 2 & \ldots & n\\ 1 & 2 & \ldots & n\end{pmatrix}$
- (d) **Inverse** $\begin{pmatrix}1 & 2 & \ldots & n\\ a_1 & a_2 & \ldots & a_n\end{pmatrix}^{-1}=\begin{pmatrix}a_1 & a_2 & \ldots & a_n\\ 1 & 2 & \ldots & n\end{pmatrix}$

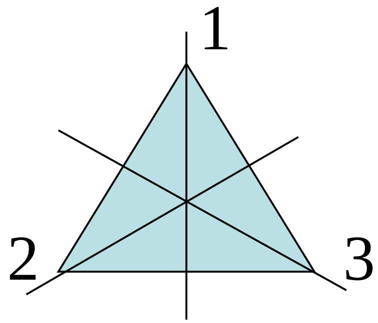
Permutation Group

- Example: Rotation group of Equilateral triangle.
- Fixed P1=$\begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix}$,



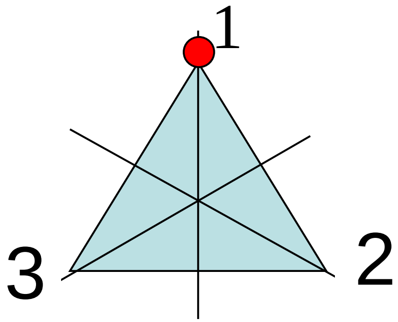
- Around the center rotation $\pm 120^{o}$

P2=$\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}$, P3=$\begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}$,



- Rotation around the axis of symmetry。

P4=$\begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix}$, P5=$\begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix}$, P6=$\begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}$,



Permutation Group

- All the permutations of [1,*n*] (total of *n*!) constitute a group, known as *n*-order symmetric group, noted as S_n.
- The 3 element permutation group of Set{1，2，3} forms S_3

$$P1=\begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix}\quad P2=\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}\quad P3=\begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}$$

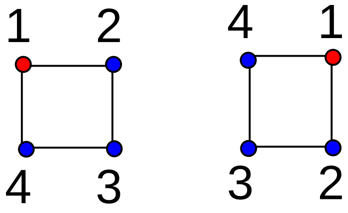
$$P4=\begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix}\quad P5=\begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix}\quad P6=\begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}$$

- Attention：Normally, the permutation group of [1,*n*] does not necessarily is referring to *Sn*, but it must be one of the subgroups of *Sn*.

Cycle, Odd Cycle and Even Cycle

$(a_1a_2\ldots a_m) = \begin{pmatrix} a_1a_2\ldots a_{m-1}a_m \\ a_2\,a_3\ldots a_m\;a_1 \end{pmatrix}$ known as cycle representation of permutation.

- Therefore $\begin{pmatrix} 12345 \\ 43152 \end{pmatrix}=(14523)$ $\begin{pmatrix} 12345 \\ 31254 \end{pmatrix}=(132)(45)$, $\begin{pmatrix} 12345 \\ 52314 \end{pmatrix}=(154)(2)(3)$.
- $(a_1a_2\ldots a_m)$ known as m order cycle； $(a_1a_2\ldots a_m)=(a_2a_3\ldots a_ma_1)=\ldots=(a_ma_1\ldots a_{m\text{-}1})$ contains m types representation.
- If 2 cycles do not have joint text, known as disjointed, the multiplication of disjointed cycles is exchangeable.
- If (132)(45)= (45)(132).
- If $p=(a_1a_2\ldots a_n)$, then p^n =(1)(2)…(n)=e.
  - If p=(123) p^2=(321) p^3=(1)(2)(3)



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

Rotate 90°
（1->4->3->2->1)

Cycle, Odd Cycle and Even Cycle

- Theorem Any permutation can be represented into the product of numerous disjointed cycles

- Proof For any given permutation p=$\begin{pmatrix} 1 & 2 & \dots & n \\ a_1 & a_2 & \dots & a_n \end{pmatrix}$, search from 1
- $1 \xrightarrow{p} a_{i1} \xrightarrow{p} a_{i2} \xrightarrow{p} \dots \xrightarrow{p} a_{ik} \xrightarrow{p} 1$ needs a cycle ($1\ a_{i1}\ a_{i2} \dots a_{ik}$),
- If ($1\ a_{i1}\ \dots\ a_{ik}$) contains all the text in [1, n], then the proposition hold.
- Otherwise, select 1 from in the remaining texts, continue the searching, there will be another cycle. Until all the texts belonged to the one of the cycles.

Because disjointed cycles are exchangeable, therefore except the arrangement of each cycle, any permutation contains its unique cycle representation.

Cycle, Odd Cycle and Even Cycle

- **Conjugate Class**

Normally, it can make any permutation p in S_n decomposed into numerous disjointed cycles composition.

$P=(a_1\ a_2\ldots a_{k1})(b_1\ b_2\ldots b_{k2})\ldots.(h_1\ h_2\ldots h_{kl})$

Among $k_1+k_2+\ldots+k_l = n$, set the number of occurrence of k order cycle as c_k, use $(k)^{ck}$ to represent, then the permutation format of S_n is

$$(1)^{c1}(2)^{c2}\ldots(n)^{cn}$$

$$\sum_{k=1}^{n} k*c_k= n$$

Cycle, Odd Cycle and Even Cycle

- S4={(1)(2)(3)(4),(12),(13),(14),(23),(24),(34),(123),(124),(132),(134),(142),(143),(234),(243), (1234), (1243), (1324), (1342), (1423),(1432),(12)(34),(13)(24),(14)(23)}.

Example: The format of (1)(2 3)(4 5 6 7) is $(1)^1(2)^1(4)^1$

- All permutations in S_n which contains the same format constitutes a conjugate class.

- Example $(2)^2$ in S4, there are 3 conjugate classes

- (12)(34),(13)(24),(14)(23).

$(1)^1$ $(3)^1$, there are 8 conjugate classes

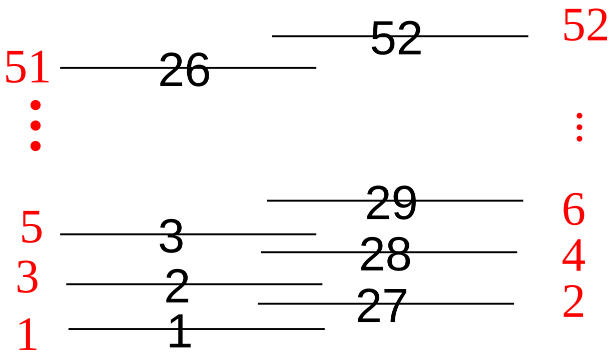
(123),(124),(132),(134),(142),(143),(234),(243),

Cycle, Odd Cycle and Even Cycle

Example A deck of cards, one split into 2, crossed insert into each other (shuffling), each operation is equaled to one permutation *p*.

$$i^p=\begin{cases}(i+1)/2, i=1,3,5,\dots,51.\\ i/2+26, i=2,4,6,\dots,52.\end{cases}$$

$p=\begin{pmatrix} i \\ i^p\end{pmatrix}$, i^{th} *position* occupied by i^p.



1 order cycle - 2
2 order cycle - 1
8 order cycle - 6

Put 1, then place 27, place 2, place 28………

How many rounds of operations are needed to restore all cards into its original order

p = (1) (2 27 14 33 17 9 5 3)
(4 28 40 46 49 25 13 7)
(6 29 15 8 30 41 21 11)
(10 31 16 34 43 22 37 19)
(12 32 42 47 24 38 45 23)(18 35)
(20 36 44 48 50 51 26 39) (52)

$p^8 = e$

Cycle, Odd Cycle and Even Cycle

- 2 order cycles is known as swap
- **Theorem** Any cycle can be represented by the product of swaps
- (1 2 …*n*)=(1 2)(1 3)…(1 *n*)
- Proof: Set（1 2 … *n*-1) = (1 2) (1 3) …(1 *n*-1)
- (1 2 3…*n*-1)(1 n)

$$=\begin{pmatrix}1 & 2 & 3 & \dots & n-1 \\ 2 & 3 & 4 & \dots\dots & 1\end{pmatrix}\begin{pmatrix}1 & 2 & 3 & \dots & n-1 & n \\ n & 2 & 3 & \dots & n-1 & 1\end{pmatrix}$$

$$=\begin{pmatrix}1 & 2 & 3 & \dots & n-1 & n \\ 2 & 3 & 4 & \dots\dots & 1 & n\end{pmatrix}\begin{pmatrix}2 & 3 & \dots & n-1 & 1 & n \\ 2 & 3 & \dots & n-1 & n & 1\end{pmatrix}$$

$$=\begin{pmatrix}1 & 2 & 3 & \dots & n-1 & n \\ 2 & 3 & 4 & \dots\dots & n & 1\end{pmatrix}=(1\ 2\ 3 \dots. n)$$

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

$$= (1\ 2)(1\ 3)$$

- The decomposition of each permutation is not unique
- (1 2 …n)=(2 3)(2 4)…(2 n)(2 1)
- (1 2 3) = (12)(13) = (12)(13)(31)(13)

Cycle, Odd Cycle and Even Cycle

- Any permutation represented as swap; its parity (odd or even) of the swapped unit is unique
- Proof: Set the representation of f as $f=\prod_{i<j}(x_i-x_j)$

Set $l,k(l<k)$ as positive constant integer, then

$$f=(x_l-x_k)A\prod_{i\neq l,k}(x_i-x_l)\,(x_i-x_k)$$

Term A does not contain the terms having x_k or x_l

If swapped the position of l and k, $(l\ \ k)f = -f$

Each swapping may change the sign of f, then the parity of the corresponding decomposition is unique.

Cycle, Odd Cycle and Even Cycle

Permutation is divided into 2 different types: Odd permutation and even permutation.

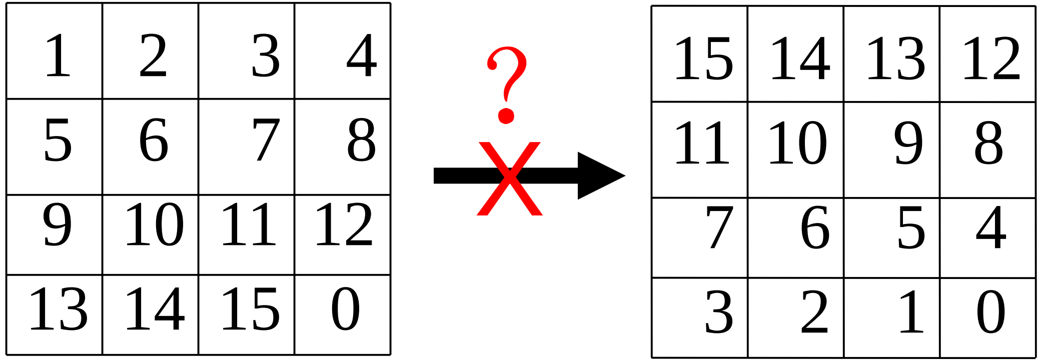
If a permutation can be decomposed as the product of odd number of position swapping, then it is odd permutation. If it can be decomposed as the product of even number of position swapping, it is even permutation.

S = (1)(25)(37)(46) 3 position swapping, odd permutation

S = (1) (2) (3) (4) (5) 0 position swapping, even permutation

Klotski of Number

- Example 0 represents empty space
  - Some layouts are obtained through the even-numbered of position swapping of the left image, some are obtained through odd-numbered of position swapping, but those obtained through odd-numbered of positing swapping; cannot be obtained through even-numbered of position swapping.
  - p=(0)(1 15)(2 14)(3 13)(4 12)(5 11)(6 10)(7 9)(8) odd permutation.
- If we limit any change to be the swapping "0" and the other number next to "0", is it possible to transform from the left image to the right one?
  - Start from the 0 over the right bottom corner back to bottom corner, in the horizontal direction, the vertical direction have done even-numbered times of change. An odd permutation does not equal to an even permutation.



1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	0

15	14	13	12
11	10	9	8
7	6	5	4
3	2	1	0

Cycle, Odd Cycle and Even Cycle

- All the permutation over [1,*n*] (total n!) structure a group, known as *n* order symmetric group, noted as *Sn*.
- Theorem All even permutations in *Sn* constitutes a sub-group which has its order as (*n*!)/2, known as alternating group, noted as *An*.

(1) Closure: The multiplication of two even permutations still gets a even permutation

(2) Associativity: The Associative Law of permutation group

(3) Identity: The identity element of permutation group is an even permutation

(4) Inverse: $(i\ k)^{-1} = (i\ k)$

Set $p = (i_1\ j_1)(i_2\ j_2)\ldots(i_{\mathrm{i}}\ j_{\mathrm{i}})$, then $p^{-1} = (i_i\ j_i)\ldots(i_1\ j_1)$

Therefore, A_n as group

Make $B_n=S_n-A_n$, $|B_n|+|A_n|=n!$,

Therefore, $(i\ j)\ B_n \subseteq A_n$, Hence $|B_n|\leq|A_n|$,

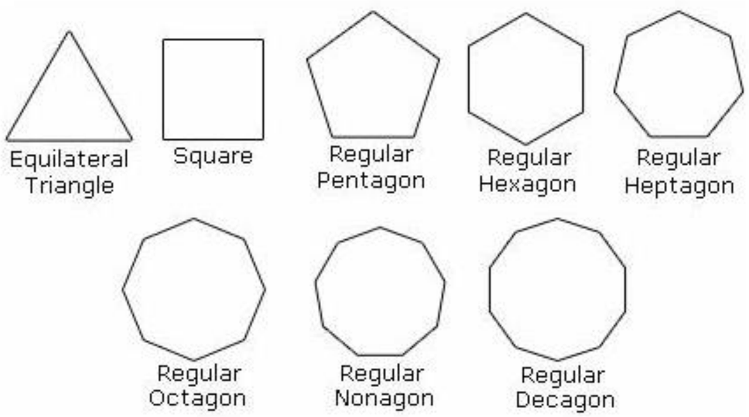
$(i\ j)\ A_n \subseteq B_n$, so$|A_n|\leq|B_n|$ $\therefore |A_n|=|B_n|=(n!)/2$

Cycle, Odd Cycle and Even Cycle

If 2 convex polygons have the same angles, have the same number of edges, these 2 polygons are called congruent polygons.

A regular convex polygon is a convex polygon which is equiangular (all angles are equal in measure) and equilateral (all sides have the same length).

The so-called regular polyhedron, is referring to each faces of the regular polyhedron are all equaled congruent regular polygon, and various polyhedral angles are all congruent polyhedral angles.



- Consider the following square Q with its corners labeled 1, 2, 3, 4 and edges labeled *a*, b, c and d.
  - There are 8 operations of Q of two types.
  - 4 rotations about the corner of the square through the angles of 0, 90, 180, and 270 degrees.

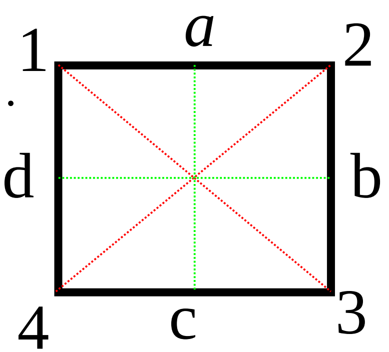
$$\rho_1 = I = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \qquad \rho_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$

$$\rho_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \qquad \rho_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}.$$

  - 4 reflections about the lines joining opposite corners and the lines joining the midpoints of opposite sides.

$$r_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} \qquad r_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$$

$$r_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \qquad r_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}.$$



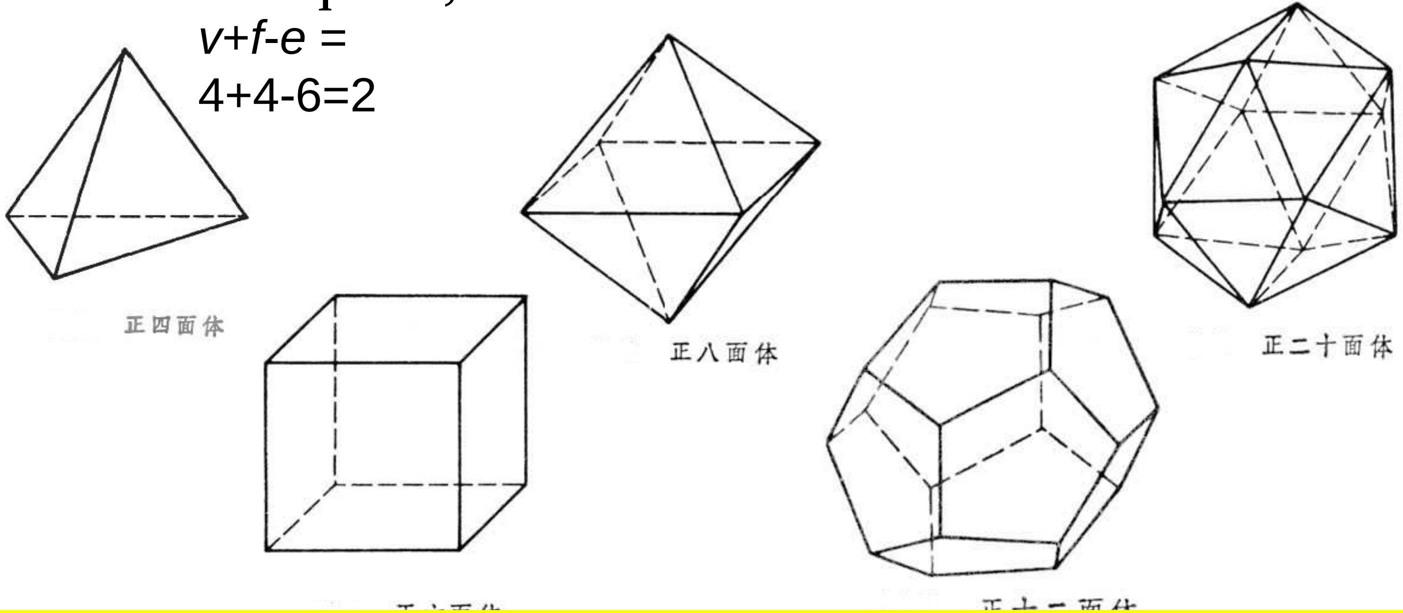
- The corner-symmetry group of a square is

$$G_C = \{p_4^0 = I, p_4, p_4^2, p_4^3, r_1, r_2, r_3, r_4\}.$$

Cycle, Odd Cycle and Even Cycle

From Euler’s polyhedron formula: There are 5 types of regular convex polyhedron, which are: Tetrahedron, Octahedron, Icosahedron, Hexahedron (Cube) and Dodecahedron.   The surface of tetrahedron, octahedron and icosahedron is triangle, each face of hexahedron is square, each face of dodecahedron is pentagons

v+*f*-*e* =
4+4-6=2

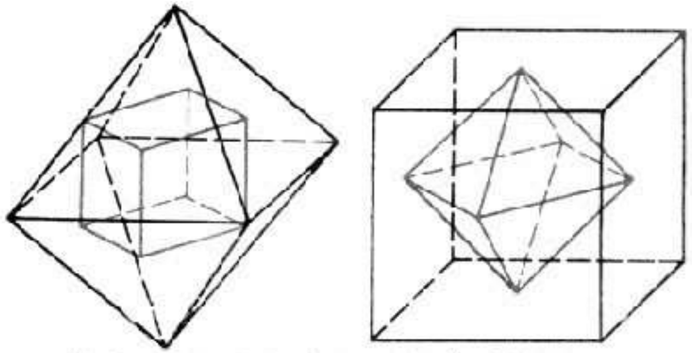


The sum value of any convex polyhedron vertices *v* and number of faces *f* is 2 more than the edge number *e*, which is *v*+*f*-*e* =2. This is **Euler's polyhedron formula**.

Cycle, Odd Cycle and Even Cycle

A polyhedron and those polyhedron which used its various surface center as top, is known as Mutual Dual Polyhedron.

Hexahedral and octahedral are mutual dual polyhedron of each other; Dodecahedron and icosahedron is each other mutual polyhedron of duality; The mutual dual polyhedron of a polyhedron is tetrahedron.



正六面体对正八面体的对偶图

A polyhedron can move in a 3D space. And after its movement, it is still occupying the same space position. All this type of movements compose a set. For 2 continuous movements, it may be denoted as the composition(multiplication) of movements. Under this composition with the movement set, it is a group known as polyhedral group.

From geometry, there are 5 types of polyhedral, which are tetrahedron, hexahedron, octahedron, dodecahedron, and icosahedron. Therefore, it then has tetrahedron group, hexa (octa)-hedron group and dode (ico)-hedron these 3 types.

Cycle, Odd Cycle and Even Cycle

The corner-symmetry group of a Tetrahedron

0o rotation: (A)(B)(C)(D)

Corner to the opposite side：

- A as the corner (AO_1):±120º (A)(*BCD*) and (A)(*BDC*)
- B as the corner :±120º (B) (*ACD*) and (B)(*ADC*)
- C as the corner :±120º (C) (*ABD*) and (C)(*ADB*)
- D as the corner :±120º (D) (*ABC*) and (D)(*ACB*)

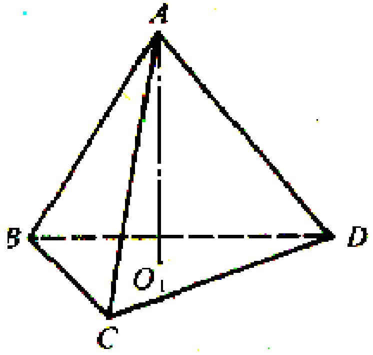
Total there are 8 three-term recurrence.

Connect the tetrahedron *A-BCD*'s 3 pairs of edge points as the axis of rotation:

Midpoints between opposite edge, 180o reflection: the permutation of (*AB*)(*CD*)，(*AC*)(*BD*)，(*AD*)(*BC*), Total 12 permutations compose a group, known as the corner-symmetry group of a Tetrahedron.

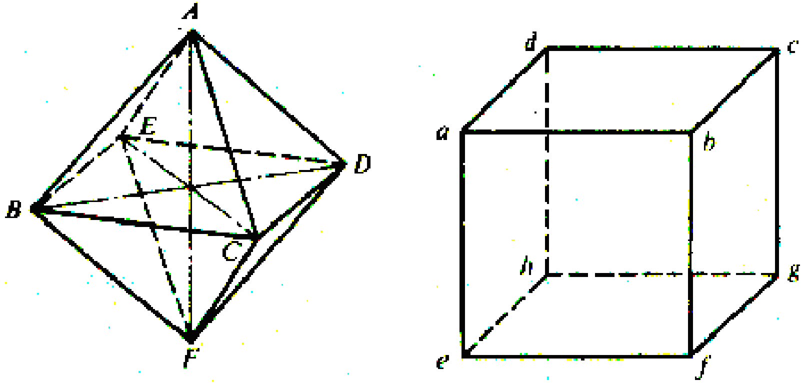
e, (*BCD*),(*BDC*),(*ACD*),(*ADC*)，(*ABD*)，(*ADB*)，(*ABC*)，(*ACB*) ,(*AB*)(*CD*)，(*AC*)(*BD*)，(*AD*)(*BC*),

•It has the same structure with the 4 characters *A*、*B*、C、*D*'s alternating group A_4. Therefore, 4-order alternating group A_4 is also known as tetrahedron group



Cycle, Odd Cycle and Even Cycle

Octahedron group or hexahedron group made up of 24 permutations, they are having the same structure as 4 symmetric groups S4. therefore octahedron group and hexahedron group is consistent, which are both 4-order symmetric group S4. Sometimes, 4-order symmetric group S4 is called as octahedron group or hexahedron group.



a 正八面体

b 正六面体

图 2

7 Group

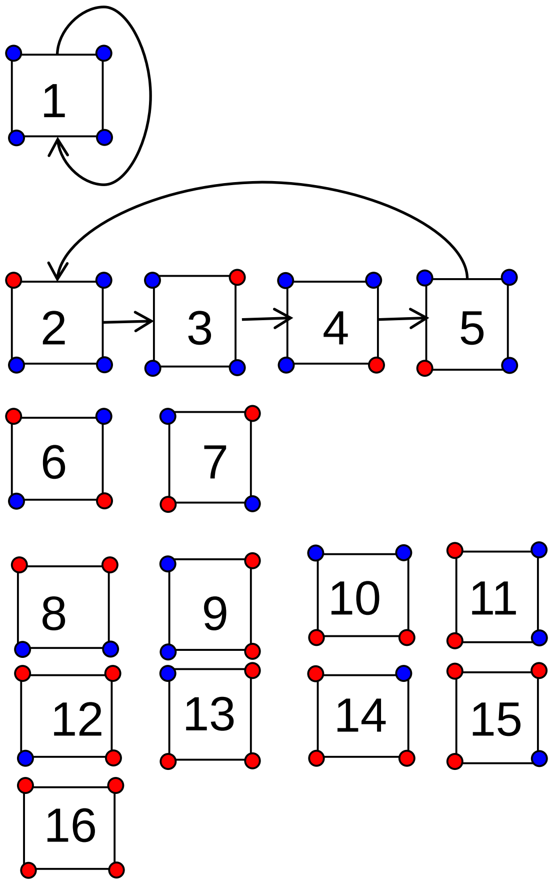
7-3 Burnside Lemma

组合数学 Combinatorics

清华大学 马昱春
Tsinghua University
Associate Professor Ma

Color Image and Solution

- Image: Static, for a specific location, if we use different colors to color it, then it will generate different images.
- Coloring solutions: If a coloring can be obtained by rotating or reflecting another coloring, then these two colorings are equivalent.
- Unchanged internal structure
  - Permutation: Transformation due to external force, such as rotation and reflection
  - Image constitutes a permutation group in its transformation
  - Image equivalence class in permutation group



The Coloring Problem of Equivalence Class

- Coloring 2 square vertices and consider only the rotation’s equivalence class number: 6
- |G|:Number of permutations
  - Only rotations considered: 4
- Permutation Group
  - *Rotate 0 degree: p_0*=(1)(2)(3)(4)(5)(6)(7)(8)(9)(10)(11)(12)(13)(14)(15)(16)
  - *rotate 90 degree:*

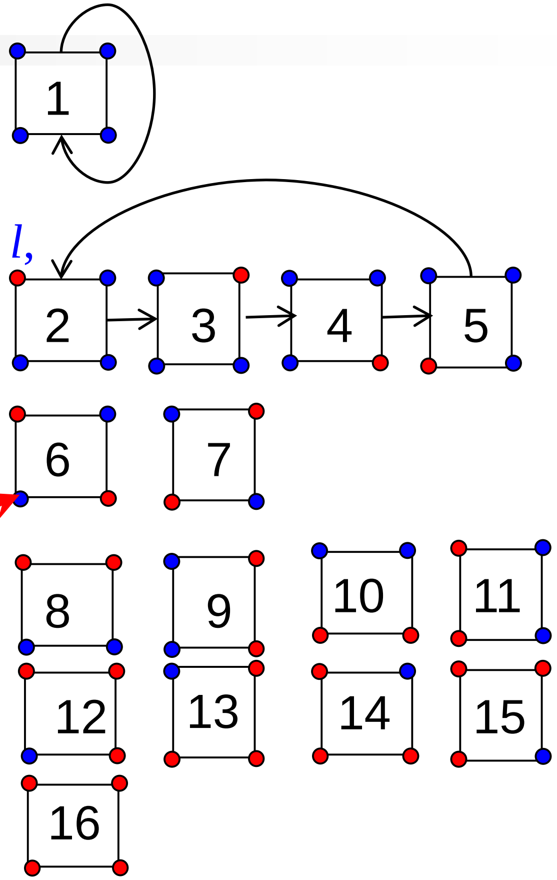
    p_1=(1)(2 3 4 5)(6 7)(8 9 10 11)(12 13 14 15)(16)
  - *rotate 180 degree:*

    p_2=(1)(2 4)(3 5)(6)(7)(8 10)(9 11)(12 14)(13 15)(16)
  - *rotate 270 degree:*

    p_3=((1)(2 5 4 3)(6 7)(8 11 10 9)(12 15 14 13)(16)

Permutation pi caused image *k* transformed into *l*, then *k* and *l* belonged to the same equivalence class

Permutation pi caused image *k unchanged*



Burnside Lemma

- K Stabilizer
- Set G as the permutation group of [1,n]. G is one of the subgroup of Sn. k∈[1,n], all the permutations which caused k element remained unchanged will compose a stabilizer of k, noted as Zk.
- For Example, G={e,(1 2),(3 4), (1 2)(3 4)}
- Z1={e,(3 4)}
- Z2={e,(3 4)}
- Z3=Z4={e,(1 2)}

The Coloring Problem of Equivalence Class

- Coloring 2 square vertices and consider only the rotation's equivalence class number: 6
- |G|: Number of Permutations
  - Only rotations considered: 4
- Permutation Group
  - *Rotate 0 degree: p_0*=(1)(2)(3)(4)(5)(6)(7)(8)(9)(10)(11)(12)(13)(14)(15)(16)
  - *rotate 90 degree:*

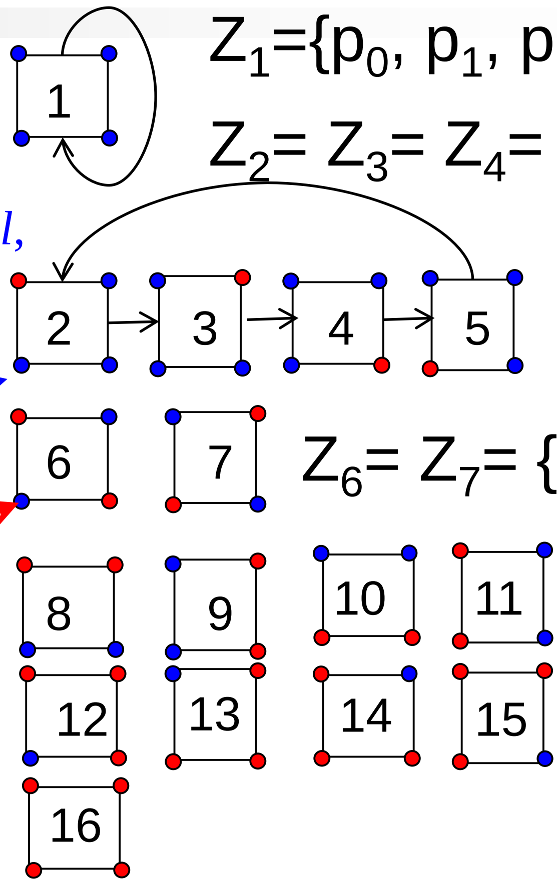
    p_1=(1)(2 3 4 5)(6 7)(8 9 10 11)(12 13 14 15)(16)
  - *rotate 180 degree:*

    p_2=(1)(2 4)(3 5)(6)(7)(8 10)(9 11)(12 14)(13 15)(16)
  - *rotate 270 degree:*

    p_3=((1)(2 5 4 3)(6 7)(8 11 10 9)(12 15 14 13)(16)

Permutation pi caused image *k* transformed into *l*, then *k* and *l* belonged to the same equivalence class

Permutation pi caused image *k unchanged*



Z_1={p_0, p_1, p_2, p_3}

Z_2= Z_3= Z_4= Z_5={p_0}

Z_6= Z_7= {p_0 , p_2}

Burnside Lemma

- Theorem Permutation group *G*’s *k* fixed displacement class *Zk* is G’s subgroup.

Closure： $k\xrightarrow{P_1}k\xrightarrow{P_2}k, k\xrightarrow{P_1P_2}k.$

Associativity: Natural.

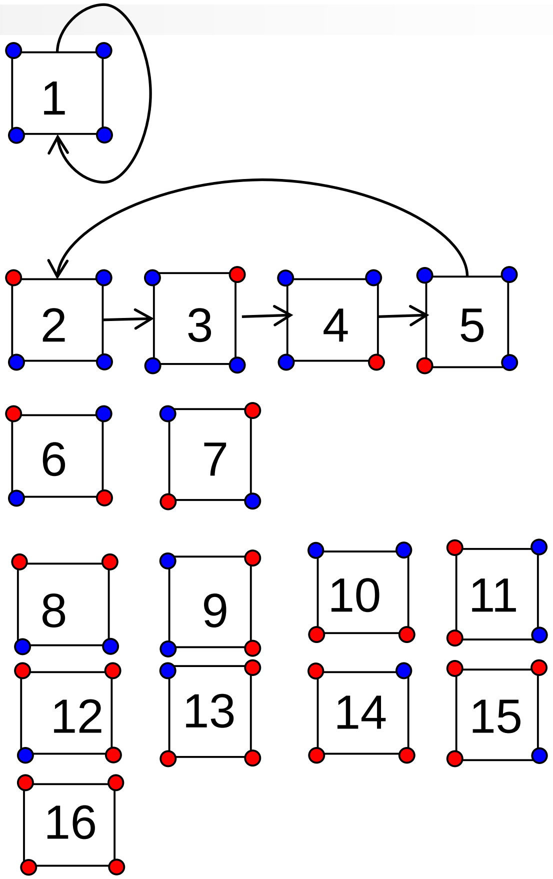
Contain Identity: G’s unit element belonged to Z_k.

Contain Inversion: $P\in Z_k, k\xrightarrow{P}k$, then $k\xrightarrow{P^{-1}}k, P^{-1}\in Z_k$.

$\therefore Z_k$ is the subgroup of G.

Burnside Lemma

- Equivalence Class (Orbit)
- Number k in $\{1,2\ldots.n\}$, if existing a permutation p_i which transforms k into l， then k and l belong to the same equivalence class, call this equivalence class as E_k
- Normally, in [1,n], G will decompose [1,n] into several equivalence class, to satisfy 3 rules of equivalence class.(a) Reflexivity; (b) Symmetry; (c) Transmission.
- G={(1)(2)(3)(4),(12),(34),(12)(34)}.Under G, 1 transformed into 2, 3 transformed into 4, but 1 will not transformed into 3. Z1=Z2={e,(34)}, Z3=Z4={e,(12)}.



E1=E2={1,2}　E3=E4={3 4}

The Coloring Problem of Equivalence Class

- Coloring 2 square vertices and consider only the rotation's equivalence class number: 6
- |G|: Number of permutations
  - Only rotations considered: 4
- Permutation Group
  - *Rotate 0 degree: p_0*=(1)(2)(3)(4)(5)(6)(7)(8)(9)(10)(11)(12)(13)(14)(15)(16)
  - *rotate 90 degree:*

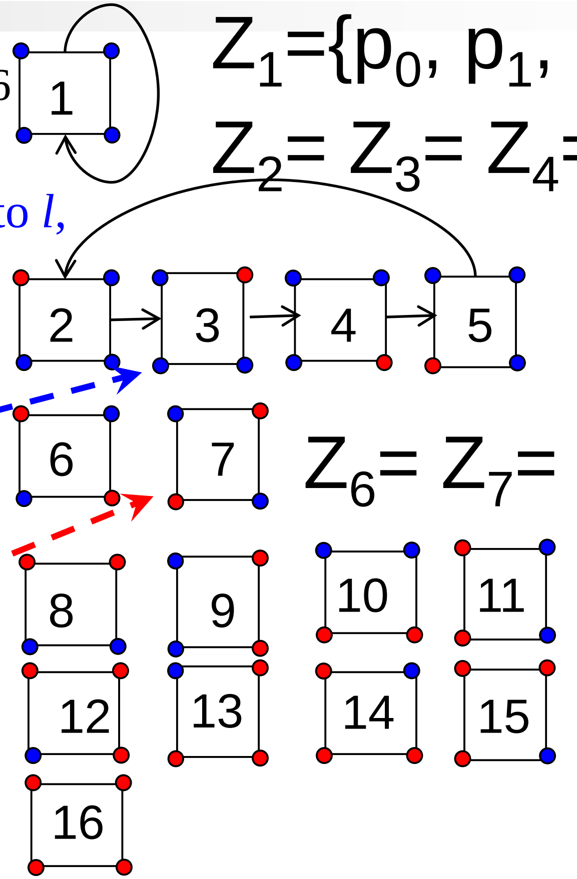
    p_1=(1)(2 3 4 5)(6 7)(8 9 10 11)(12 13 14 15)(16)
  - *rotate 180 degree:*

    p_2=(1)(2 4)(3 5)(6)(7)(8 10)(9 11)(12 14)(13 15)(16)
  - *rotate 270 degree:*

    p_3=((1)(2 5 4 3)(6 7)(8 11 10 9)(12 15 14 13)(16)

Permutation pi caused image *k* transformed into *l*, then *k* and *l* belonged to the same equivalence class

Permutation pi caused image *k unchanged*



$Z_1=\{p_0, p_1, p_2, p_3\}$

$Z_2= Z_3= Z_4= Z_5=\{p_0\}$

$Z_6= Z_7= \{p_0 , p_2\}$

$|E_1|*|Z_1|=4$

$|E_2|*|Z_2|=4$

……

$\boxed{|E_k|*|Z_k|=|G|?}$

Burnside Lemma

- Definition Review
  - Use G to represent group, every permutation in G is represented by ai
    $G=\{a_1,a_2\ldots.a_g\}=\{e,(1\ 2),(3\ 4),(1\ 2)(3\ 4)\}$
  - In each a_i in G, the number of k-order cycles is recorded as $c_k(ai)$

$a_1=e=(1)(2)(3)(4)$ $c_1(a1) = 4$ $(1)^4$

$a_4=(12)(34)$ $c_1(a4) = 0$ $c_2(a_4) = 2$ $(2)^2$

  - The set of all permutations in G that fix the element *k* is recorded as Z_k
  - $Z_1=\{e,(3\ 4)\}$ in G
  - The set of equivalent class of *k* to recorded as E_k
  - $E_1=E_2=\{1,2\}$ $E_3=E_4=\{3,4\}$

$|E_1|*|Z_1|=4$

$|E_2|*|Z_2|=4$

The Coloring Problem of Equivalence Class

- Coloring 2 square vertices and consider only the rotation's equivalence class number: 6
- |G|: Number of permutation
  - Only rotation considered: 4
- Permutation Group
  - *Rotate 0 degree:* p_0=(1)(2)(3)(4)(5)(6)(7)(8)(9)(10)(11)(12)(13)(14)(15)(16)
  - *rotate 90 degree:*

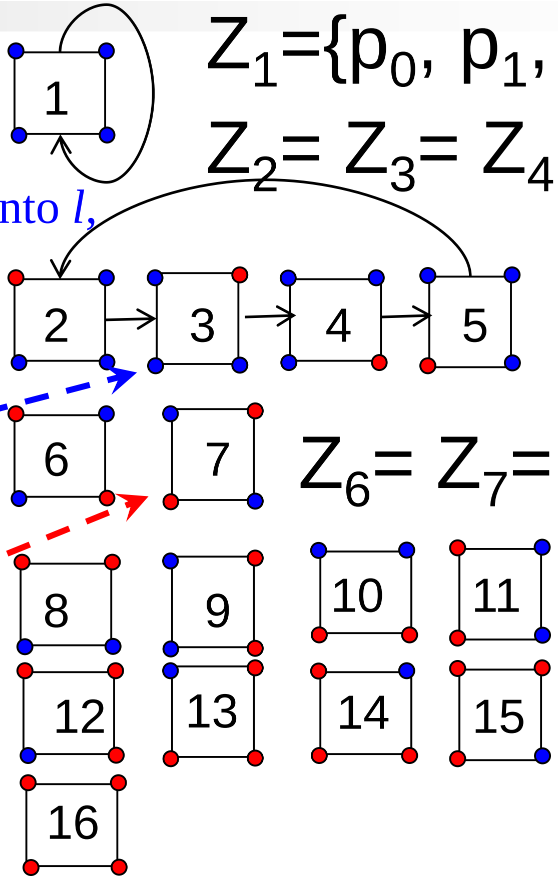
    p_1=(1)(2 3 4 5)(6 7)(8 9 10 11)(12 13 14 15)(16)
  - *rotate 180 degree:*

    p_2=(1)(2 4)(3 5)(6)(7)(8 10)(9 11)(12 14)(13 15)(16)
  - *rotate 270 degree:*

    p_3=((1)(2 5 4 3)(6 7)(8 11 10 9)(12 15 14 13)(16)

Permutation pi caused image *k* transformed into *l*, then *k* and *l* belonged to the same equivalence class

Permutation pi caused image *k unchanged*



$Z_1=\{p_0, p_1, p_2, p_3\}$

$Z_2= Z_3= Z_4= Z_5=\{p_0\}$

$Z_6= Z_7= \{p_0 , p_2\}$

$|E_1|*|Z_1|=4$

$|E_2|*|Z_2|=4$

……

$\boxed{|E_k|*|Z_k|=|G|?}$

Burnside Lemma

- **Theorem (Orbit-stabilizer theorem)** set G as the permutation group of $[1,n]$, E_k is $[1,n]$ under G's effect contains k's equivalence class, Z_k is k stablizer. There is $|E_k||Z_k|=|G|$.
- **Proof** Set$|E_k|=l$, $E_k=\{a_1(=k), a_2,\ldots,a_l\}$ $k=a_1\xrightarrow{p_i}a_i$, $i=1,2,\ldots,l$. $P=\{p_1,p_2,\ldots,p_l\}$

Cause $G_i=Z_kp_i,i=1,2,\ldots,l$. Hence, k in Z_kp_i's effects transformed into a_i

$G_i\subseteq G$(G on the decomposition of Z_k)$i\neq j,G_i\cap G_j=\Phi$.

$\boldsymbol{G_1+G_2+\ldots+G_l \subseteq G}$.

On the other hand, $p\in G$. $k\xrightarrow{p}a_j\xrightarrow{pj^{-1}}k$

$pp_j^{-1}\in Z_k$, $P\in Z_kp_j=G_j$.

$\therefore \boldsymbol{G \subseteq G_1+\ldots+G_l}$.

Thus, $G=G_1+G_2+\ldots+G_l$.

$|\mathrm{G}|=|\mathrm{G}_1|+|\mathrm{G}_2|+\ldots+|\mathrm{G}_l|=|Z_kp_1|+|Z_kp_2|+\ldots+|Z_kp_l|$

$= |Z_k| \cdot l= |Z_k| \cdot |E_k|$

Simple Example

$|E_k|*|Z_k|=|G|$

Example $G=\{e,(12),(34),(12)(34)\}$.

- $c_1(a_1)=4, c_1(a_2)=2,$
- $c_1(a_3)=2, c_1(a_4)=0.$
- $E_1=E_2=\{1, 2\}$ $E_3=E_4=\{3, 4\}$
- $S_{jk}=\begin{cases} 1, & k^{a_j}=k, \\ 0, & k^{a_j}\neq k. \end{cases}$

a_j \ S_{jk} \ k	1	2	3	4	$c_1(a_j)$	
(1)(2)(3)(4)	1	1	1	1	4	$(1)^4$
(12)(3)(4)	0	0	1	1	2	$(1)^2(2)^1$
(1)(2)(34)	1	1	0	0	2	$(1)^2(2)^1$
(12)(34)	0	0	0	0	0	$(2)^2$
$\lvert Z_k \rvert$ →	2	2	2	2	8	

The sum of row j obtains $c_1(a_j)$, the sum of column k obtains $|Zk|$

The sum of table elements

$$=\sum_{j=1}^{g}\sum_{k=1}^{n}S_{jk}=\sum_{k=1}^{n}|Z_k|=\sum_{j=1}^{g}c_1(a_j)$$

4.4 Burnside Lemma

- Generally, similar to the table is as the following table. Among *Sjk*= $\begin{cases}\mathbf{1},\ k^{a_j}=k, \\ \mathbf{0},\ k^{a_j}\neq k.\end{cases}$

Sjk \ k aj	1	2	…	n	c1(aj)
a1	S11	S12	…	S1n	c1(a1)
a2	S21	S22	…	S2n	c1(a2)
…	…	…		…	
ag	Sg1	Sg2	…	Sgn	c1(ag)
|Zk|	|Z1|	|Z2|	…	|Zn|	

$$\sum_{k=1}^{n}|Z_k|=\sum_{j=1}^{g}c_1(a_j)$$

$|E_k||Z_k|=|G|.$

$$\sum_{j=1}^{g}\sum_{k=1}^{n} S_{jk} = \sum_{k=1}^{n} |Z_k| = \sum_{j=1}^{g} c_1(a_j)$$

[1,*n*] divided into *l* number of <u>equivalence class.</u> [1,*n*]=$E_{a1}+E_{a2}+\ldots+E_{al}$.

- If *j*, *i* belonged to the same equivalence class, then $Ei=Ej$,$|Ei|=|Ej|$

Because $|E_i||Z_i|=|G|$, therefore $|Z_i|=|Z_j|$.

Each equivalence class $\sum_{i\in E_{aj}} |Z_i| = |E_{aj}||Z_{aj}|$

Total *l* equivalence class $\sum_{k=1}^{n} |Z_k| = \sum_{j=1}^{l}\sum_{i\in E_{aj}} |Z_i| = \sum_{j=1}^{l} |E_{aj}||Z_{aj}|$

$$= \sum_{j=1}^{l} |G| = l|G|$$

$$l = \frac{1}{|G|}\sum_{k=1}^{n} |Z_k| = \frac{1}{|G|}\sum_{j=1}^{g} c_1(a_j)$$

Burnside Lemma

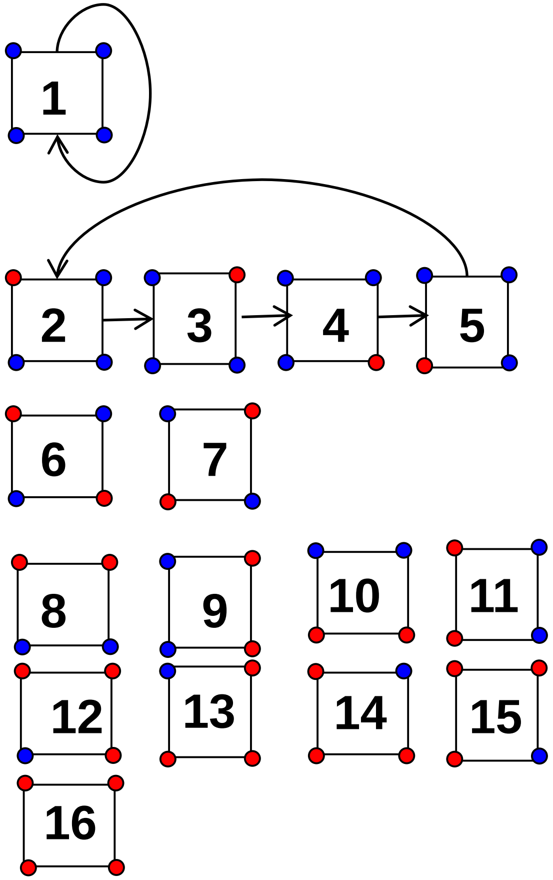
- Burnside Lemma (1897)
  - **Cauchy(1845)-Frobenius(1887) lemma**
  - Orbit-counting theorem
  - The result is not due to Burnside himself, who merely quotes it in his book 'On the Theory of Groups of Finite Order', attributing it instead to Frobenius(1887).

Set G={a1,a2,…ag} is the permutation group of the target group [1,n]. Each permutation is written into the product of disjointed cycles. $c_1(a_k)$ is number of the elements which are not changed by permutation $a_{k,}$ which is the number of cycles with the length of 1. G decomposes [1,n] into l number of equivalence classes that::

$$l = \frac{1}{|G|}\sum_{j=1}^{g} c_1(a_j)$$

$$\bullet\, l=[c_1(a_1)+c_1(a_2)+\ldots+c_1(a_g)]/|G| \;=\frac{1}{4}\sum_{f\in G}(16+2+4+2)=6$$

- Suppose to color the four corners of a regular square using two colors: red and blue. How many nonequivalent colorings are there if we only consider the rotation movements.
- |G|: Number of Permutation
  - Consider only rotation: 4
- c_1(f): Fixed Displacement Number
  - *Rotate 0 degree:* (1)(2)(3)(4)(5)(6)(7)(8)(9)(10)(11)(12)(13)(14)(15)(16)
  - *rotate 90 degree:* (1)(2 3 4 5)(6 7)(8 9 10 11)(12 13 14 15)(16)
  - *rotate 180 degree:* (1)(2 4)(3 5)(6)(7)(8 10)(9 11)(12 14)(13 15)(16)
  - *rotate 270 degree:* (1)(2 5 4 3)(6 7)(8 11 10 9)(12 15 14 13)(16)



Burnside Lemma

$$l = \frac{1}{|G|}\sum_{j=1}^{g} c_1(a_j)$$

- Solve by permutation group of the image set using Burnside Lemma
- But for coloring with multiple colors issue, theoretically it can be solved by Burnside, but it is extremely complicated

Use 6 different colors to paint a cube, each side one color, **different sides may use different colors**; how many different kinds of coating are there?

7 Group

7-4 Gossip of Group

组合数学 Combinatorics

清华大学 马昱春
Tsinghua University
Associate Professor Ma

What is Group

It is nothing, therefore it is everything

群(group)

A group is a set, G, together with an operation • (called the group law of G). To qualify as a group, the set and operation, (G, •), must satisfy four requirements known as the group axioms:

(a)封闭性(Closure):

(b)结合律(Associativity):

(c)有单位元(Identity):

(d)有逆元(Inverse):

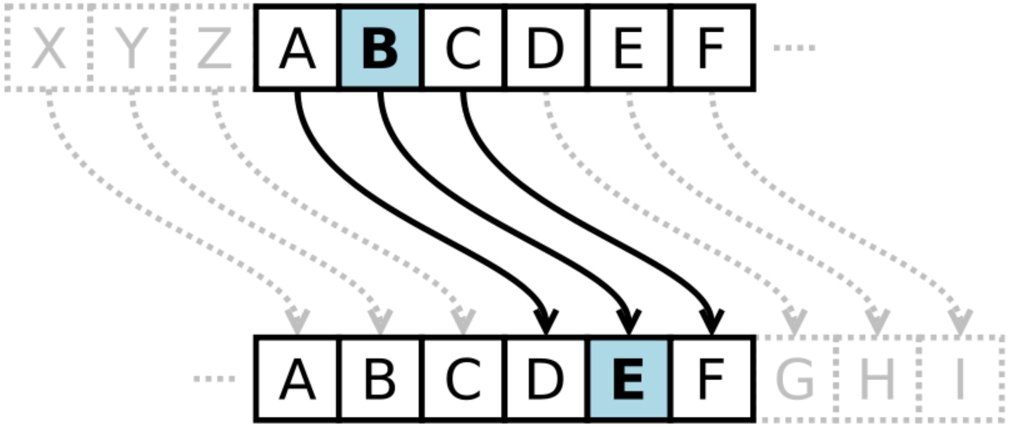
Abstract and corresponding to reality

Group

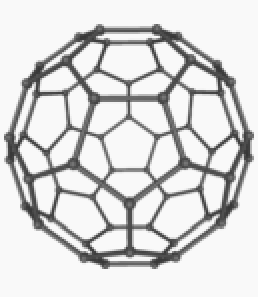
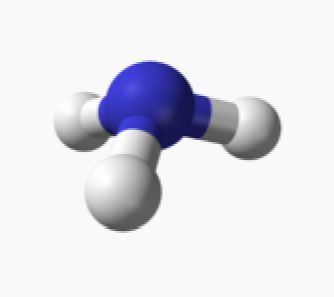
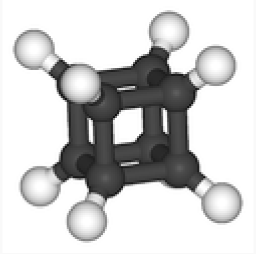
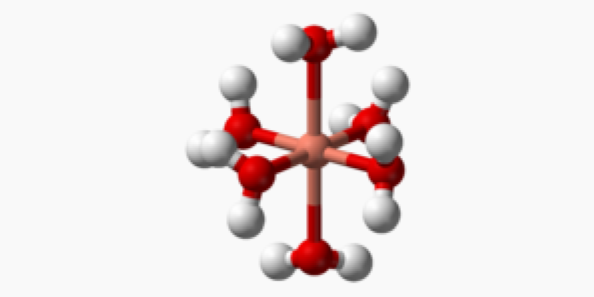
Rubik’s Cube Group:

The popular puzzle Rubik's cube invented in 1974 by Ernő Rubik has been used as an illustration of permutation groups.

旋转和翻转形成一个大二十面体的对称群。



The cyclic group Z26 underlies Caesar's cipher.

			
富勒烯展现了二十面体对称。	氨NH_3。它的对称群是6阶的，用120°旋转和反射生成的。	立方烷C_8H_8刻画了八面体对称。	六水合铜（II）配合物$[Cu(OH_2)_6]^{2+}$。相较于完美的对称形状，分子垂直膨胀大约22%（姜-泰勒效应）。

The Starting Point of the Century

- Galois was in touched with the concept of group when he was studying on the radical solution of the five degree univariate polynomial equation (一元五次方程).
  - For five times and higher univariate polynomial equation, Abel had proved that general formula does not exist.
  - Galois realized that the algebraic solution to a polynomial equation is related to the structure of a group of permutations associated with the roots of the polynomial, the Galois group of the polynomial.
  - Galois submitted his memoir on equation theory several times, but it was never published in his lifetime due to various events.
  - His first attempt was refused by Cauchy, but in February 1830 following Cauchy's suggestion he submitted it to the Academy's secretary Joseph Fourier, to be considered for the Grand Prix of the Academy. The reviewer for this memorandum is Cauchy. Although he had realized the importance of Galois's works, Cauchy did not accept the memorandum, but he suggested Galois to modify this memorandum and resubmit it to compete for the Academy Award for mathematics.
  - Unfortunately, Fourier died soon after, and the memoir was lost.

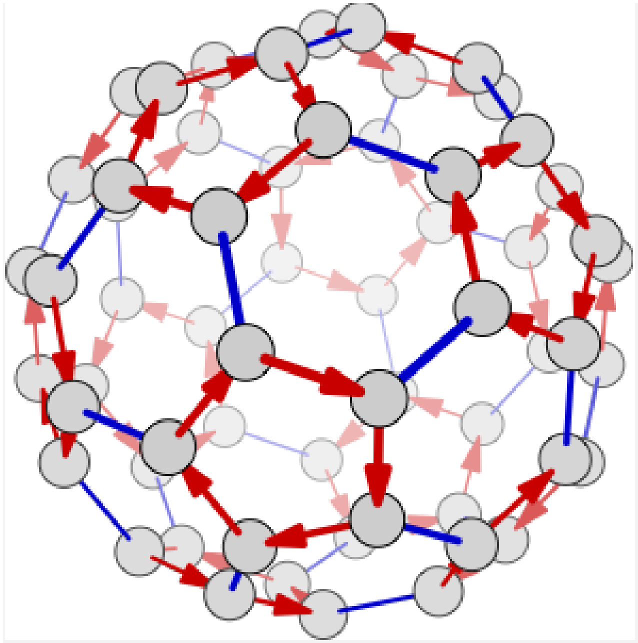
- Galois decided to place his last shot, but it was dismissed by Poisson, the reason was “cannot be understood”. When the news reached Galois, he had already imprisoned due to political struggle. At this time, there was only half a year before his duel.

- “Don’t cry, Alfred！ To die in my twenty years, I need all my courage.” This was the last sentence that he told his brother.
- The night before the duel (1832-5-29), Galois foreseen that he was going to die soon, he wrote all his ideas through the night
- “I have no time”、 “I have no time”。
- Please publicly request Jacobian or Gaussian on the importance of these theorems (not of the correctness of the theorem) to express their views

- In 1846, Liouville realized the burst of these genius ideas, he spent several months trying to explain its meaning.
- Bell said: “What he had written in his desperation before dawn, is enough for the next generation of mathematicians to work for decades.”
- “He once found the answer which tortured the mathematicians for centuries: Under what conditions an equation can be solved?”

The Development of Group

- Group is just symmetry. To research group, it is the study on various kinds of symmetry



交错群A_5的一个Cayley图（一种群的图示）

Normal Subgroup

Not only itself is a group, if it is “divided” to its original group, the result is still a group.

A group which is obtained by conducting “division” is known as Quotient Group(Factor Group)

Simple Group

Prime Number??

Group which cannot be further decomposed

Possible to find all simple groups?

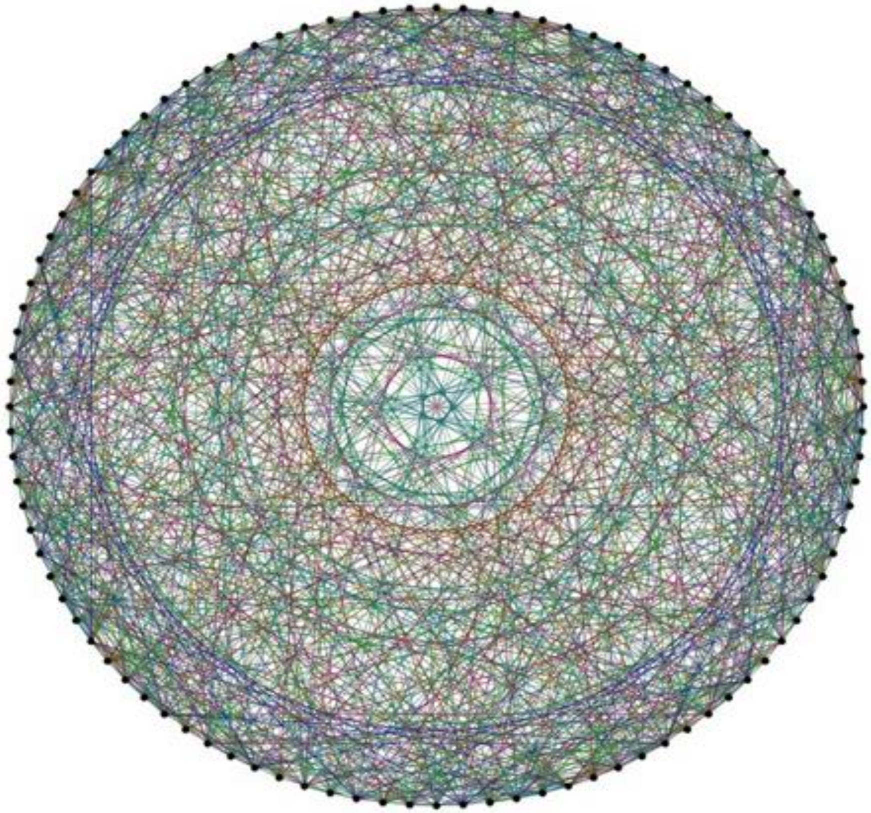
http://songshuhui.net/archives/57697

http://en.wikipedia.org/wiki/Simple_group

In 1823, mathematicia n>=5 are simple gro

unsolvable group

and group in



Higman-Sims图，可导出散在单群Higman-Sims群

Felix Klein
German Mathematician

In 1884, 16 Groups Lie type

Sophus Lie
Norway Mathematician

18 families of finite simple groups + 26 sporadic groups

All Finite Simple Group?

Classification Structure Analysis:

In 1872 - Sylow Theorem. Caused mathematicians to start understanding the in-depth structure of finite group.

In 1892 – Hölder: Clearly put forward the classification of finite simple groups.

100 years had passed……

The Journey of Hundred Years

- In 1983, Gorenstein announced finite simple group classification theorem was proven, the Group Theory Academy were as cheerful as a lark.
- All the evidence scattered in more than 500 papers in various journals, together almost over a million of pages, each paper had deal with each special case.
- The problem is, he was wrong.
- He thought one of the group which is called “quasi-thin group” was already well-handled, but the fact was not.
- In 2004, Aschbacher and Smith publish their work on quasithin groups (which are mostly groups of Lie type of rank at most 2 over fields of even characteristic), filling the last gap in the classification known at that time.
- The proof of the classification theorem consists of tens of thousands of pages in several hundred journal articles written by about 100 authors, published mostly between 1955 and 2004.
- 18 families of finite simple groups + 26 sporadic groups

Monster Group

- The largest sporadic group—— Monster Group
- In 1973, it was found out by Fischer and Griess separately.
- The largest sporadic simple group, “Monster Group” originated from its huge size.
- The number of accurate element of Monster Group is 808017424794512875886459904961710757005754368000000000, which is approximately $8*10^{53}$.
- The number of atoms of a solar system is about 10^{57}, merely higher 4 order of magnitude. If we use linear space and transform matrix to represent Monster Group, we need at least a 196883 dimensional linear space,
- Griess proposed a Griess algebra of the algebraic structure, and Monster Group just happened to be the auto-morphism group of algebraic structure. In other words, Monster Group happens to depict all the symmetry of the Griess algebra.
- The dimension of Griess algebras is 196884, 1 more than 196883.

Somewhere In Between

- The dimension of Griess algebras is 196884, 1 more than 196883
- Fourier series, in which each coefficient is an integer

$$j(\tau) = \frac{1}{q} + 744 + \boxed{196884}q + 21493760q^2 + 864299970q^3 + \cdots, q = e^{2\pi i\tau}$$

Coincident？ Relation？

$$j(\tau) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + 864299970q^3 + \cdots, q = e^{2\pi i\tau}$$

- In 1979, Conway and Norton put forward “Monstrous Moonshine”.
- It existed an infinite dimensional algebraic structure based on Monster Group, through the irreducible linear representations of Monster Group, it happened to give all Fourier expansion of j invariant. Whereas the effect of each element in Monster Group of the algebra structure, naturally gives the model type associated with certain group.

$$\begin{aligned} 1 &= 1 \\ 196884 &= 196883 + 1 \\ 21493760 &= 21296876 + 196883 + 1 \\ 864299970 &= 842609326 + 21296876 + 2\cdot 196883 + 2\cdot 1 \end{aligned}$$

- In 1992, Brocherds had completed the proof
- The proof had included mathematics and physics at the same time, which used No-ghost theorem in string theory to construct an essential algebraic structure;
- In 1998, Brocherds won the Fields prize due to this proof.
- From the bridge which formed through this theorem, mathematicians also realized that there are all kinds of connections among Monster Group, modular function and string theory.
- There are also crazy ideas around which mentioned that Monster Group may represent the ultimate symmetry of our universe.

Galois

- Évariste Galois(1811~1832)
- The theorem which proposed and insisted by Galois had proposed is a challenge to authority, to the generation; his “Group” had completed gone beyond the concept of mathematics which can be understood.
- His mathematic examiner once said, “This child is facing difficulties trying to express his thoughts, but he is very intelligence, and had reflected his extraordinary academic spirit”
- Excessive pursuit of simplicity is the somewhat cause of this regret.
- When you try to lead the reader away from ordinal thinking into a more confused field, clarity is absolutely necessary.