Group theory

Definition of a group

$G = \{ g_1, g_2, g_3 \dots \}$

can be finite or infinite

and a group has an operation $*$

$g_1 * g_2 \to g_3$

$*$ can be multiplication or addition or composition of two function for example.

The set G together with $*$ is a group (we use the convention not to write $*$ as we do with multiplications)

i) associativity $(g_1 g_2) g_3 = g_1 (g_2 g_3)$

ii) $\exists$ identity element $e\, g = g \quad \forall\, g \in G$

iii) each element $g \in G$ has an inverse $g^{-1}\, g = e$ such that $g^{-1} \in G$

We can derive some properties from these axions

a) $g\, g^{-1} = e \Rightarrow g^{-1} g\, g^{-1} = e g^{-1} = g^{-1}$

we know $g^{-1} \cdot g = e$

$\times (g^{-1})^{-1}$ | $g\, g^{-1} = (g^{-1})^{-1} g^{-1} = e$

b) $ge = g$

$eg = g \Rightarrow ege = ge \Rightarrow ge = e^{-1} ge = ege$

$$ge = g(g^{-1}g) = eg = g$$

identity is unique

suppose we has two identy elements e and e_1

then $e e_1 = e_1$
$= e$ $\Big\} \Rightarrow e_1 = e$

inverce is unique

suppose $g_1 g = e$ $\quad g_2 g = e$

then $g_1 g = g_2 g$

$\Rightarrow g_1 g g_1 = g_2 g g_1$

$g_1 e = g_2 e \Rightarrow g_1 = g_2$

commutation

if $g_1 g_2 = g_2 g_1$ we say that g_1 and g_2 commute

if all multiplication of a group commute, we sy that the group is abelian otherwise the group is nonabelian.

Most group are nonabelian

Examples of groups

1) integers under addition, 0 is the identity
not that integers under multiplication is
not a group

2) integers $\neq 0 \bmod p$ under multiplication p
with p prime

$$1, 2, 3, \ldots, p-1$$

$(p-1)^2 = p^2 - 2p + 1 \bmod p = 1$

if $k\, l_1 \bmod p = k\, l_2 \bmod p$

then $k(l_1 - l_2) = 0 \bmod p$

$\Rightarrow$ p must be a divisor of k or $l_1 - l_2$
but both are less than p

example: $p = 7$

k | l	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

multiplication table

3) Rotations: O 3×3 matrix

$$O^T O = 1 \qquad \det O = 1$$

$$O^{-1} = O^T \qquad \mathbb{1} = (\sigma^1, \sigma_1)$$

$O = O_1 O_2$ then $(O_1 O_2)^T O_1 O_2 = O_2^T O_1^T O_1 O_2 = 1$

$\det(O_1 O_2) = \det O_1 \det O_2 = 1$

4) groups determined by generators

cyclic group $\{a^k\}$ $a^n = 1$ C_n

dihedral group $a^n = 1$, $b^2 = e$

$ab = e$

it has $2n$ elements

Properties of a group

Subgroup $H \subseteq G$ is subgroup

if $e \in H$ and if $h_1, h_2 \in H$ then

$h_1 h_2 \in H$

coset $H \subseteq G$

$$gH = \{gh_1, gh_2, \dots\}$$

is a coset

- if H is finite each coset has the same number of elements

$gh_1 = gh_2 \Rightarrow h_1 = h_2 \Rightarrow$ order of coset is order of H

- if two cosets intersect, they coincide

$\exists\, h_1, h_2$ such that $g_1 h_1 = g_2 h_2$

then $g_2 = g_1 h_1 h_2^{-1}$

$H \subseteq G$

first coset $g_1 H$

then take $g_2 \in G / g_1 H$

second coset $g_2 H$

then take $g_3 \in G / (g_1 H \cup g_2 H)$

third coset $g_3 H$

Until we have exhausted H

$\Rightarrow \quad G = \bigcup_\alpha g_\alpha H$

$\Rightarrow$ <u>Lagrange theorem</u>: the order of H is a divisor of G

<u>normal subgroup</u> H is a normal subgroup if $g^{-1} H g = H \quad \forall g \in G$

<u>Quotient group</u> G/H is a group if H is a normal subgroup

For a normal subgroup the left coset gH is equal to the right coset Hg: $gh = \underbrace{ghg^{-1}}_{\in H} g \in Hg$

$$g_1 h_1 g_2 h_2 = g_1 g_2 \underbrace{g_2^{-1} h_1 g_2}_{\in H \text{ for normal subgroup}} h_2$$

$$= g_1 g_2 H$$

Simple groups a group is simple if it has no normal subgroups other than e or G

eg cyclic groups are simple if n is prime

a^k, $k = 0, \ldots, n-1$

non trivial subgroup has general a^p with p a divisor of n

Conjugacy classes

g_1 conjugate with g_2 if

$$g_2 = g g_1 g^{-1}$$

notation $g_1 \sim g_2$

conjugacy class all elements that are conjugate

The set $g g_1 g^{-1}$ is a subgroup

$$H = \{ g g_1 g^{-1}, g \in G \}$$

it is a normal subgroup

Conjugacy class

$$\{ g_2 \mid g_2 = g_1^{-1} g g_1 , g_1 \in G \}$$

if $g_1 \in H g_1' \Rightarrow g_1 = h g_1'$

then $g_2 = g_1'^{-1} \underbrace{h^{-1} g h}_{g} g_1'$

$\Rightarrow g_2 \sim g$

$\Rightarrow$ order of conjugacy class is a divisor of G, In fact it is $|G|/|H|$

Example $U(n)$ $\quad U^+ U = 1$

$$u = V u V^{-1}$$

conjugacy classes are $U(n)$ matrices with the same eigenvalues

Permutations

permutation group S_n, $n!$ elements

$$\pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \qquad \pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$$

$$\pi_2 \circ \pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$$

cycle notation

$$\pi_1 = (1\,3)(2\,4)$$

$$\pi_2 = (1)(2\,4)(3)$$

$$\pi_2 \circ \pi_1 = (1\,3)(2)(4)$$

Any permutation with the same cycle length is in the same conjugacy class

eg $(1)(24)(3)$ in $(13)(2)(4)$

$$(1)(24)(3) = P^{-1}(13)(2)(4)P$$

$$P = \begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix} \quad P^{-1} = \begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}$$

$$P^{-1}((13)(2)(4))P = P^{-1}\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}$$

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

number of elements in conjugacy class

$$N_{r_1 r_2 \cdots} = \frac{n!}{1^{r_1} r_1! \, 2^{r_2} r_2! \cdots n^{r_n} n!}$$

$n = r_1 + 2r_2 + 3r_3 + \cdots + nr_n$

distribute n over $\binom{r_1}{\cdot}\cdot\binom{r_2}{\cdot}\cdot\binom{r_3}{\cdot}\cdot\binom{r_4}{\cdot}$

a cyclic permutation inside a cycle does not change the permutation divide by the length of each cycle. also the order of the cycles does not matter, divide by $r_k!$

sign of permutation: $\prod_k (\text{sg(cycle)})^{r_k}$

$(123) = (12)(23)$ is an even permutation

permutations can be written as the product of transposition (with repeated numbers)

$\text{sign}(\pi_1 \circ \pi_2) = \text{sign}\,\pi_1 \,\text{sign}\,\pi_2$

Alternating group: Subgroup of even permutations

A_n

A_n is simple for $n \geq 5$

$\Rightarrow$ Fifth order equation cannot be solved algebraically.

shown later independently by Galois

Any finite group is a subgroup of the permutation group

$g\{e, g_1, g_2, \ldots\} = \{g, gg_1, gg_2, \ldots\}$

permutation of group elements

$\text{sign}(\pi_1 \circ \pi_2) = \text{sign}\,\pi_1 \,\text{sign}\,\pi_2$

Alternating group: Subgroup of even permutations

A_n

A_n is simple for $n \geq 5$

$\Rightarrow$ Fifth order equation cannot be solved algebraically.

shown later independently by Galois

Any finite group is a subgroup of the permutation group

$g\{e, g_1, g_2, \ldots\} = \{g, gg_1, gg_2, \ldots\}$

permutation of group elements