

## 2. FINITE GROUPS

A group  $G$  is finite if  $|G| < \infty$ .  $|G|$  is called the order of  $G$ .

Remark: (i)  $H \subset G$  subgroup  $\Rightarrow |H| < \infty$

$$G = \bigcup_{g \in G/H} gH, \text{ multiplication is bijection } \Rightarrow |gH| = |H|$$

$$\Rightarrow |G| = |G/H| \cdot |H|$$

$|G/H| = [G : H]$  is sometimes called the index of  $H$  in  $G$ .

Orders of subgroups divide the order of the group!

[Lagrange's theorem]

$$(ii) g \in G : \Gamma_g := \{g^i \mid i \in \mathbb{Z}\} \subset G$$

$$|\Gamma_g| < \infty$$

$$\Rightarrow \exists n, m : g^n = g^m \Rightarrow \exists k \in \mathbb{N} : g^k = e$$

$$\Rightarrow \Gamma_g = \{e, g, g^2, \dots, g^k = e\} \cong \mathbb{Z}_k$$

$$k = \text{ord}(g) = \text{ord}(\Gamma_g)$$

$$\text{Lagrange theorem} \Rightarrow \text{ord}(g) \mid |G|$$

What does this mean if  $|G|$  is prime?

$$\Rightarrow \text{ord}(g) = |G| \quad \forall e \neq g \in G$$

$$\Rightarrow \boxed{G \cong \mathbb{Z}_{|G|}}$$

Examples:

$$(i) \mathbb{Z}_{pq} \supset \mathbb{Z}_p \text{ generated by } [p] \\ \supset \mathbb{Z}_q \text{ generated by } [q]$$

$$(ii) |D_n| = 2n$$

$$\Gamma_{s_i} = \{e = R_0, s_i\} \subset D_n$$

$$\mathbb{Z}_n = \{R_0, \dots, R_{n-1}\} \\ \uparrow \\ \Gamma_{R_1}$$

$$\Gamma_{R_2} \cong \Gamma_{R_1}, n \text{ odd} \quad n = pq, \Gamma_{R_p} \cong \mathbb{Z}_q$$

Finite group  $G = \{g_1, \dots, g_n\}$

Group is specified by multiplication table:

you can describe all groups by giving the multiplication tables.

| $G$      | $g_1$     | $g_2$     | $\dots$ | $g_i$     | $\dots$ | $g_n$     |
|----------|-----------|-----------|---------|-----------|---------|-----------|
| $g_1$    | $g_1 g_1$ | $g_1 g_2$ | $\dots$ | $g_1 g_i$ | $\dots$ | $g_1 g_n$ |
| $g_2$    | $g_2 g_1$ |           |         |           |         |           |
| $\vdots$ | $\vdots$  |           |         |           |         |           |
| $g_j$    | $g_j g_1$ |           |         | $g_j g_i$ |         |           |
| $\vdots$ | $\vdots$  |           |         |           |         |           |
| $g_n$    | $g_n g_1$ |           |         |           |         |           |

Example:

| $D_3$ | $R_0$ | $R_1$ | $R_2$ | $S_0$ | $S_1$ | $S_2$ |
|-------|-------|-------|-------|-------|-------|-------|
| $R_0$ | $R_0$ | $R_1$ | $R_2$ | $S_0$ | $S_1$ | $S_2$ |
| $R_1$ | $R_1$ | $R_2$ | $R_0$ | $S_1$ | $S_2$ | $S_0$ |
| $R_2$ | $R_2$ | $R_0$ | $R_1$ | $S_2$ | $S_0$ | $S_1$ |
| $S_0$ | $S_0$ | $S_2$ | $S_1$ | $R_0$ | $R_2$ | $R_1$ |
| $S_1$ | $S_1$ | $S_0$ | $S_2$ | $R_1$ | $R_0$ | $R_2$ |
| $S_2$ | $S_2$ | $S_1$ | $S_0$ | $R_2$ | $R_1$ | $R_0$ |

Note: since multiplication is a bijection in  $G \Rightarrow$  all rows (columns) are permutations of first row (column).

$$g: g_i \mapsto g g_i = g_{\pi_g(i)} \quad \pi_g \in S_n$$

$$h(g g_i) = h(g_{\pi_g(i)}) = g_{\pi_h \circ \pi_g(i)}$$

$$(hg) g_i = g_{\pi_{hg}(i)}$$

$\Rightarrow \pi: g \mapsto \pi_g$  is group homomorphism

$$G \rightarrow S_n$$

$$\pi_g = e \in S_n \Rightarrow \pi_g(i) = i \quad \forall i \Rightarrow g = e$$

$\rightarrow \pi: G \hookrightarrow S_n$  is injective

$\Rightarrow G \cong \pi(G) \subset S_n$  all groups of order  $n$  are subgroups of  $S_n$ !

Importance of  $S_n$  for physics:

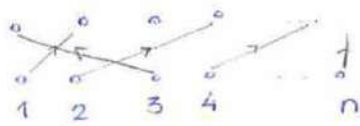
- statistics of particles in quantum systems.
- represent. of  $S_n$  govern the representation theory of  $SU(N)$ .

• Symmetric Group:

$$S_n := B_j (S = \{1, \dots, n\})$$

$$|S_n| = n!$$

Notation:



~ draw a row <sup>towards</sup> where the number goes

or

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

Example:  $S_4 \ni \pi$  cyclic permutation of  $(1, 2, 3, 4)$

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = \begin{array}{cccc} \circ & \circ & \circ & \circ \\ \nearrow & \nearrow & \nearrow & \nearrow \\ \circ & \circ & \circ & \circ \\ 1 & 2 & 3 & 4 \end{array}$$

Example: What is a Cayley subgroup of  $\mathbb{Z}_4$ ?

$$g_i = [i], \quad g_0 = e, \quad g_1 = [1], \quad g_2 = [2], \quad g_3 = [3]$$

$$\pi: \mathbb{Z}_4 \rightarrow S_4$$

$$g_i g_j = g_{i+j \bmod 4}$$

$$\pi_e = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \quad \pi_{[1]} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

$$\pi_{[2]} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \quad \pi_{[3]} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$

$$H = \{ \pi_e, \pi_{[1]}, \pi_{[2]}, \pi_{[3]} \} \subset S_4$$

$$\cong \mathbb{Z}_4$$

- Cycles:

special  $\pi \in S_n$  which cyclically permute subsets of  $S = \{1 \dots n\}$

$$S_k \ni (s_0, \dots, s_{k-1}) : s_i \mapsto s_{i+1 \bmod k}$$

$$r \in S_n \setminus \{s_0, \dots, s_{k-1}\} \mapsto r$$

$$\begin{pmatrix} 1 & 3 & 4 \\ \curvearrowright & \curvearrowright & \curvearrowright \\ 3 & 2 & 1 \end{pmatrix} \in S_4 \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}$$

There is a  $k$ -fold ambiguity in notation:  $(s_0, s_1, \dots, s_k) = (s_1, s_2, \dots, s_k, s_0)$

Non intersecting cycles commute:

$$(s_1 \dots s_k) (s'_1 \dots s'_{k'}) = (s'_1 \dots s'_{k'}) (s_1 \dots s_k)$$

$$\text{s.t. } \{s_1 \dots s_k\} \cap \{s'_1 \dots s'_{k'}\} = \emptyset$$

Important fact:

All  $\pi \in S_n$  can be written as product of non-intersecting cycles!

Choose any  $\pi \in S_n$

Define equivalent relation on  $S = \{1, \dots, n\}$

$$x \sim y \iff \exists \ell \in \mathbb{N}_0 : y = \pi^\ell(x)$$

$$\Gamma_\pi \cong \mathbb{Z}_k \text{ for some } k$$

$S = \bigcup$  equivalence classes  
" orbits under  $\Gamma_\pi$

$$S = S^0 \cup S^1 \cup \dots \cup S^m$$

$$S^i = \{s_i, \pi(s_i), \pi^2(s_i), \dots, \pi^{n_i-1}(s_i)\} \quad , \quad n_i = |S^i|$$

$$\pi = (s_1, \pi(s_1) \dots \pi^{n_1-1}(s_1)) (s_2, \pi(s_2) \dots \pi^{n_2-1}(s_2)) \dots (s_m, \pi(s_m) \dots \pi^{n_m-1}(s_m))$$

↑  
product of non-intersecting cycles

Example:

$$T = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 1 & 6 & 2 & 5 & 3 & 7 \end{pmatrix}$$

$$S = \{1, 4, 2\} \cup \{3, 6\} \cup \{5\} \cup \{7\}$$

$$\pi = (1, 4, 2) (3, 6)$$

Fact: under conjugation: cycles of particular length go to cycles of the same length.

$$\sigma \in S_n \quad (s_1, \dots, s_k) \in S_n$$

$$\sigma(s_1, \dots, s_k) \sigma^{-1} = (\sigma(s_1), \dots, \sigma(s_k))$$

$$\sigma(s_1, \dots, s_k) \sigma^{-1}(\sigma(s_i)) = \sigma(s_1, \dots, s_k)(s_i) = \sigma(s_{i+1})$$

$$\Rightarrow \sigma(s_1, \dots, s_k) \sigma^{-1} = (\sigma(s_1), \dots, \sigma(s_k)) \quad \perp$$

Conjugacy class is determined by the length-structure of the cyclic ~~group~~ decomp.

Conjugacy classes are characterized by cycle structure:  $(k_1, \dots, k_n)$ , where  $k_i \geq 0$  is number of cycles of length  $i$ .

$$\sum i k_i = n$$

$$|C(k_1, \dots, k_n)| = \frac{n!}{\prod_i i^{k_i} k_i!}$$

$\swarrow$  all permutations  
 $\nwarrow$  cycle permutations in cycles  
 $\nearrow$  length of the cycle  
 $\nearrow$  permutations of cycles of same length  
 $\nwarrow$  no. of cycles with length  $i$

$(s_1 s_2 s_3) = (s_2 s_3 s_1)$

Reparametrisation:  $(k_1, \dots, k_n) \mapsto (\lambda_1, \dots, \lambda_n)$

$$\lambda_i = \sum_{j=i}^n k_j$$

$\lambda_i$  is the number of cycles of length at least  $i$

$$k_i = \lambda_i - \lambda_{i+1}$$

$$\sum_{i=1}^n \lambda_i = \sum_{i=1}^n \sum_{j=i}^n k_j = \sum_{j=1}^n i k_j = n$$

$(\lambda_1, \dots, \lambda_n)$  is a partition of  $n$ .

Characterize conjugacy classes

Cycle structures  $\rightarrow \{(k_1, \dots, k_n) \mid k_i \geq 0, \sum i k_i = n\}$

$\updownarrow$  1:1

partitions of  $n \rightarrow \{(\lambda_1, \dots, \lambda_n) \mid \lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_n \geq 0, \sum \lambda_i = n\}$

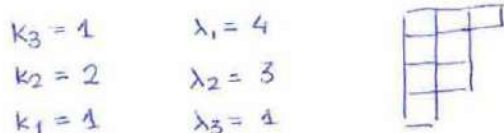
nice way to visualise partitions by means of Young diagrams

$\updownarrow$  conjugacy classes of  $S_n$

Young diagram associated to  $(\lambda_1, \dots, \lambda_k)$  is a picture of  $n$  boxes in columns of heights  $\lambda_i$ :



Example:  $S_8: (\dots)(\dots)(\dots)(\dots)$



# conjugacy classes of  $S_n$ ?

"
   
# of partitions of  $n = p(n)$

$$p(1) = 1$$

$$p(2) = 2 \quad 2 = 2+0, 1+1$$

$$p(3) = 3 \quad 3 = 3+0, 2+1, 1+1+1$$

$$p(4) = 5$$

$$p(5) = 7$$

:

Generating functions:

$$\prod_{k \geq 1} \left( \frac{1}{1-x^k} \right) = \prod_k \sum_{i \geq 0} x^{ki} = \sum_n x^n p(n)$$

$$(1+x+x^2+\dots)(1+x^2+x^4+x^6+\dots) \times \\ \times (1+x^3+x^6+x^9+\dots) \dots$$

- Specific cycles:

- transpositions:

$$\sigma_i = (i, i+1): \begin{array}{l} i \mapsto i+1 \\ i+1 \mapsto i \\ r \mapsto r, \quad r \neq i+1 \end{array}$$

$$\sigma_i \sigma_i = e$$

$S_n$  is generated by transpositions (all  $\pi \in S_n$  can be ~~written~~ written by products of transpositions)

Take  $\pi \in S_n$ ,  $\pi(n) = i$

$$\tilde{\pi} = \sigma_{n-1} \sigma_{n-2} \dots \sigma_i \pi$$

$$\tilde{\pi}(n) = n$$

If  $\tilde{\pi}$  is product of transpositions, then  $S_0$  is  $\pi = \sigma_1 \sigma_{i+1} \dots \sigma_{k-1} \tilde{\pi}$

$S_2 = \{e, (12)\}$  is generated by transp.

$$\text{length}(\pi) = \min \{k \mid \pi = \sigma_{i_1} \dots \sigma_{i_k}\}$$

Define:  $\psi: S_n \rightarrow \mathbb{Z}_2$

$$\rho(x_1, \dots, x_n) = \prod_{i < j} (x_i - x_j)$$

$$\psi(\pi) = \frac{\rho(x_{\pi(1)} \dots x_{\pi(n)})}{\rho(x_1 \dots x_n)} \in \{\pm 1\}$$

$$\psi(\pi\sigma) = \frac{\rho(x_{\pi\sigma(1)} \dots x_{\pi\sigma(n)})}{\rho(x_1 \dots x_n)} = \frac{\rho(x_{\sigma(1)} \dots x_{\sigma(n)})}{\rho(x_{\sigma(1)} \dots x_{\sigma(n)})} \cdot \frac{\rho(x_{\pi(1)} \dots x_{\pi(n)})}{\rho(x_1 \dots x_n)} = \psi(\sigma) \psi(\pi)$$

$$\psi(\sigma_i) = -1$$

$$\psi(\pi) = (-1)^{\text{length}(\pi)}$$

$$\text{Ker}(\psi) = \{\pi \mid \psi(\pi) = 1\}$$

$$= \{\pi \text{ of even length}\} \triangleleft S_n$$

An alternating group

$$S_n / A_n \cong \mathbb{Z}_2$$

Remark: Finite group (simple) have been classified

- cyclic group  $\mathbb{Z}_n$
- alternating group
- simple group of Lie-type
- one of 26 sporadic groups (Monster)