2. Finite Groups

Lecture 3, Group Theory, Prof. Daniel Roggenkamp

Lecture notes by Janosh Riebesell, 22.04.2015

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

Remark:

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

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

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

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

Orders of subgroups divide the order of the group! [Lagrange's theorem]

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

$$\Rightarrow \exists n, m : g^n = g^m \Rightarrow \exists k \in \mathbb{N} : g^k = e$$
$$\Rightarrow \Gamma_g = \{e, g, g^2, ..., g^k = e\} \cong \mathbb{Z}_k$$

$$k =: \operatorname{ord}(g) = \operatorname{ord}(\Gamma_g)$$

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

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

$$\Rightarrow \operatorname{ord}(g) = |G| \quad \forall e \neq g \in G \quad \Rightarrow \quad \boxed{G \cong \mathbb{Z}_{|G|}}$$

Examples:

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

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

$$\Gamma_{S_i} = \{e = R_0, S_i\} \subset D_n,$$
$$\mathbb{Z}_n = \{R_0, ..., R_{n-1}\} = \Gamma_{R_1} \subset D_n,$$

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

Finite group $G = \{g_1, ..., g_n\}$. A group is specified by its *multiplication table* (you can describe all groups by giving the multiplication tables):

G	g_1	g_2	$\cdots$	g_i	$\cdots$	g_n
g_1	g_1g_1	g_1g_2	$\cdots$	g_1g_i	$\cdots$	g_1g_n
g_2	g_2g_1		$\ddots$			
$\vdots$	$\vdots$					
g_j	g_jg_1			g_jg_i		
$\vdots$	$\vdots$					
g_n	g_ng_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 the first row (column).

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

$$h(gg_i) = h\left(g_{\pi_g(i)}\right) = g_{\pi_h \circ \pi_g(i)}$$
$$\| $$
$$(hg)g_i = g_{\pi_{hg}(i)}$$

$$\Rightarrow \pi : g \mapsto \pi_g \text{ is a group homomorphism } G \to S_n$$

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

$$\to \pi : G \hookrightarrow S_n \text{ is injective}$$

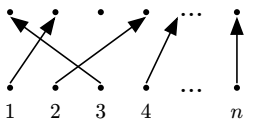
$$\Rightarrow G \cong \pi(G) \subset S_n \quad \text{all groups of order } n \text{ are subgroups of } S_n \text{ !}$$

Importance of S_n for physics:
- statistics of particles in quantum systems.
- representations of S_n govern the representation theory of SU(N).

Symmetric group:

$$S_n := \text{Bij}(S = \{1, ..., n\}), \quad |S_n| = n!$$

Notation:

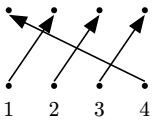


draw a row towards where the number goes

or

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

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

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


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

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

$$\pi : \mathbb{Z}_4 \to S_4, \quad g_i g_j = g_{i+j \bmod 4}$$

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

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

$$H = \left\{\pi_e, \pi_{[1]}, \pi_{[2]}, \pi_{[3]}\right\} \subset S_4, \quad H \cong \mathbb{Z}_4$$

- **Cycles:** special $\pi \in S_n$ which cyclically permute subsets of $S = \{1, ..., n\}$:

$$S_n \ni (s_0, ..., s_{k-1}) : \quad s_i \mapsto s_{i+1 \bmod k}$$
$$r \in S \setminus \{s_0, ..., s_{k-1}\} \mapsto r$$

$$(134) \in S_4 : \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}$$

  There is a k-fold ambiguity in notation: $(s_0, s_1, ..., s_{k-1}) = (s_1, s_2, ..., s_{k-1}, s_0)$.

  Non-intersecting cycles commute:

$$(s_1 ... s_k)(s'_1 ... s'_{k'}) = (s'_1 ... s'_{k'})(s_1 ... s_k) \quad \text{s.t.} \quad \{s_1 ... s_k\} \cap \{s'_1 ... s'_{k'}\} = \varnothing$$

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

  Proof: Choose any $\pi \in S_n$. Define an equivalence relation on $S = \{1, ..., n\}$:

$$x \sim y \quad \Leftrightarrow \quad \exists l \in \mathbb{N}_0 : y = \pi^l(x), \quad \Gamma_\pi \cong \mathbb{Z}_k \text{ for some } k$$

$$S = \bigcup_{\cdot} \text{equivalence classes} = \bigcup_{\cdot} \text{orbits under } \Gamma_\pi$$
$$S = S^0 \cup S^1 \cup ... \cup S^m, \quad S^i = \left\{s_i, \pi(s_i), \pi^2(s_i), ..., \pi^{n_i - 1}(s_i)\right\}, \quad n_i := |S^i|$$

$$\pi = \underbrace{(s_1, \pi(s_1), ..., \pi^{n_1-1}(s_1))(s_2, \pi(s_2), ...)(s_3, ...)...(s_m, \pi(s_m), ..., \pi^{n_m-1}(s_m))}_{\text{product of non-intersecting cycles}}$$

  Example:

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

$$S = \{1, 4, 2\} \cup \{3, 6\} \cup \{5\} \cup \{7\}, \quad \pi = (1, 4, 2)(3, 6)$$

Fact: Under conjugation, cycles of a particular length go to cycles of the same length.

$$\sigma \in S_n, \quad (s_1, ..., s_k) \in S_n, \quad \sigma(s_1, ..., s_k)\sigma^{-1} = (\sigma(s_1), ..., \sigma(s_k))$$

Proof:

$$\sigma(s_1 ... s_k)\sigma^{-1}(\sigma(s_i)) = \sigma(s_1, ..., s_k)(s_i) = \sigma(s_{i+1})$$
$$\Rightarrow \sigma(s_1, ..., s_k)\sigma^{-1} = (\sigma(s_1) ... \sigma(s_k)) \qquad \square$$

The conjugacy class is determined by the length structure of the cyclic decomposition.

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

$$\sum_i i k_i = n,$$

$$|C_{(k_1,\dots,k_n)}| = \frac{\overbrace{n!}^{\text{all permutations}}}{\prod_i \underbrace{i^{k_i}}_{\substack{\text{cyclic permutations}\\ \text{in cycles}}} \underbrace{k_i!}_{\substack{\text{permutations of cycles}\\ \text{of same length}}}},$$

where e.g. $(s_1 s_2 s_3) = (s_2 s_3 s_1)$ (i: length of the cycle, k_i: number of cycles with length i).

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

$$\lambda_i = \sum_{j=i}^{n} k_j \quad (\lambda_i \text{ is the number of cycles of length at least } i)$$

$$k_i = \lambda_i - \lambda_{i+1}, \quad \sum_{i=1}^{n} \lambda_i = \sum_{i=1}^{n} \sum_{j=i}^{n} k_j = \sum_j j k_j = n$$

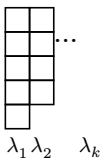
$(\lambda_1, ..., \lambda_n)$ is a partition of n.

Characterize conjugacy classes:

$$\begin{array}{c} \text{cycle structures} \to \left\{(k_1, ..., k_n) \mid k_i \geq 0, \sum i k_i = n\right\} \\ \updownarrow \text{1:1} \\ \text{partitions of } n \to \left\{(\lambda_1, ..., \lambda_n) \mid \lambda_1 \geq \lambda_2 \geq ... \geq \lambda_n \geq 0, \sum \lambda_i = n\right\} \\ \updownarrow \\ \text{conjugacy classes of } S_n \end{array}$$

Nice way to visualise partitions by means of *Young diagrams*.

The *Young diagram* associated to $(\lambda_1, ..., \lambda_k)$ is a picture of n boxes in columns of heights λ_i:



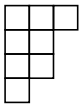
$\square$ ~ n boxes all together

Example: S_8: $(\cdot\,\cdot)(\cdot\,\cdot)(\cdot\,\cdot)(\cdot)$

$k_3 = 1$ $\quad$ $\lambda_1 = 4$

$k_2 = 2$ $\quad$ $\lambda_2 = 3$

$k_1 = 1$ $\quad$ $\lambda_3 = 1$



\# conjugacy classes of S_n = \# of partitions of $n = p(n)$:

$$\begin{aligned} p(1) &= 1 \\ p(2) &= 2, \quad 2 = 2+0, 1+1 \\ p(3) &= 3, \quad 3 = 3+0, 2+1, 1+1+1 \\ p(4) &= 5 \\ p(5) &= 7 \\ &\vdots \end{aligned}$$

Generating functions:

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

$$(1+x+x^2+...)(1+x^2+x^4+x^6+...)(1+x^3+x^6+x^9+...)...$$

- **Specific cycles:**
  - *transpositions:*

$$\sigma_i=(i,i+1):\quad\begin{cases}i\mapsto i+1\\ i+1\mapsto i\\ r\mapsto r,\quad r\neq i,i+1\end{cases}\qquad\sigma_i\sigma_i=e$$

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

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

$$\tilde{\pi}=\sigma_{n-1}\sigma_{n-2}...\sigma_i\pi,\quad\tilde{\pi}(n)=n.$$

If $\tilde{\pi}$ is a product of transpositions, then so is $\pi=\sigma_i\sigma_{i+1}...\sigma_{n-1}\tilde{\pi}$.
$S_2=\{e,(12)\}$ is generated by transpositions.

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

Define $\varphi:S_n\to\mathbb{Z}_2$:

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

$$\varphi(\pi)=\frac{p\big(x_{\pi(1)},...,x_{\pi(n)}\big)}{p(x_1,...,x_n)}\in\{\pm 1\},$$

$$\varphi(\pi\sigma)=\frac{p\big(x_{\pi\sigma(1)},...,x_{\pi\sigma(n)}\big)}{p(x_1,...,x_n)}=\underbrace{\frac{p\big(x_{\pi\sigma(1)},...,x_{\pi\sigma(n)}\big)}{p\big(x_{\sigma(1)},...,x_{\sigma(n)}\big)}}_{\varphi(\pi)}\cdot\underbrace{\frac{p\big(x_{\sigma(1)},...,x_{\sigma(n)}\big)}{p(x_1,...,x_n)}}_{\varphi(\sigma)},$$

$$\varphi(\sigma_i)=-1,\quad\varphi(\pi)=(-1)^{\text{length}(\pi)},$$
$$\ker(\varphi)=\{\pi\mid\varphi(\pi)=1\}=\{\pi\text{ of even length}\}\lhd S_n$$

A_n: *alternating group*, $S_n/A_n\cong\mathbb{Z}_2$.

Remark: Finite (simple) groups have been classified:
- cyclic groups $\mathbb{Z}_p$
- alternating groups
- simple groups of Lie type
- one of 26 sporadic groups (Monster)