Recap.

1. group extension

$$1 \xrightarrow{f_0} G_1 \xrightarrow{f_1} G_2 \xrightarrow{f_2} G_3 \xrightarrow{f_3} 1$$

$$\mathrm{im}\, f_{i-1} = \ker f_i$$

$\{1\} = \mathrm{im}\, f_0 = \ker f_1 \Rightarrow f_1$ inj.

$\mathrm{im} f_1 = \ker f_2$

$\mathrm{im} f_2 = \ker f_3 \equiv G_3 \Rightarrow f_2$ surj.

$$\mu : G \to G'$$

$$1 \to N \cong \ker\mu \to G \to Q \cong \mathrm{im}\,\mu \to 1$$

$$G/N \cong Q$$

$N \cong A \subset Z(G)$. central extension.

2. Example: $\pi : SU(2) \to SO(3)$

$\ker \pi = \{\pm 1_2\} \cong \mathbb{Z}_2$

$$1 \to \mathbb{Z}_2 \to \underset{\cong Spin(3)}{SU(2)} \to SO(3) \to 1$$

$$1 \to \mathbb{Z}_2 \to Spin(n) \to SO(n) \to 1$$

$$1 \to \mathbb{Z}_2 \to \underline{G^{\text{Quantum}}} \to \underline{G^{\text{Classical}}} \to 1$$

$U(1)$

3. (finite) Heisenberg group Heis_N

$$[q, p] = i\hbar \Rightarrow \underline{e^{i\delta \hat{q}}}, \underline{e^{i\delta \hat{p}}}$$

$n=4$

$$P = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \qquad Q = \begin{pmatrix} 1 & & & \\ & \omega & & \\ & & \omega^2 & \\ & & & \omega^3 \end{pmatrix}$$

$$QP = \omega PQ, \quad \underline{\underline{P^n = Q^n = \mathbb{1}_n}}$$

$$\Rightarrow Q^l P^k = \omega^{kl} P^k Q^l$$

$$(\omega^{a_1} P^{b_1} Q^{c_1})(\omega^{a_2} P^{b_2} Q^{c_2}) = \omega^{a_1 + a_2} P^{b_1} \underline{Q^{c_1}} \cdot \underline{P^{b_2}} Q^{c_2}$$

$$= \omega^{a_1 + a_2 + c_1 b_2} P^{b_1 + b_2} Q^{c_1 + c_2}$$

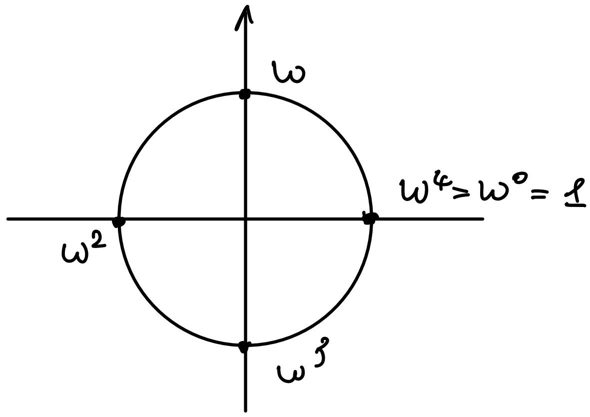
$$\pi : \text{Heis}_N \to \mathbb{Z}_N \times \mathbb{Z}_N$$

$$\omega^a P^b Q^c \mapsto (b \bmod N, c \bmod N)$$

$$\ker(\pi) = \{ \omega^a \cancel{P^{rN}} \cancel{Q^{sN}} \} \cong \mathbb{Z}_N \qquad (\omega^N = 1)$$

$$1 \to \underline{\underline{\mathbb{Z}_N}} \to \text{Heis}_N \to \underline{\mathbb{Z}_N} \times \underline{\mathbb{Z}_N} \to 1$$

$\Rightarrow$ Heisenberg group is a central extension of additive / translation group.



$(P \cdot \Psi)(\omega^k) := \Psi(\omega^{k-1})$ translation

$(Q\Psi)(\omega^k) := \omega^k \Psi(\omega^k)$ position operator

$(QP)\Psi(\omega^k) = \omega^k P\Psi(\omega^k) = \omega^k \Psi(\omega^{k-1})$

$(PQ)\Psi(\omega^k) = Q\Psi(\omega^{k-1}) = \omega^{k-1}\Psi(\omega^{k-1})$

$\Rightarrow QP = \omega PQ$

$N \to \infty$: $\mathbb{Z}_N \to U(1)$

$\mathbb{Z}_N \times \mathbb{Z}_N \to \mathbb{R} \times \mathbb{R}$

$1 \to U(1) \to \mathrm{Heis}(\mathbb{R} \times \mathbb{R}) \to \mathbb{R} \times \mathbb{R} \to 1$

4. Group actions $G \times X \to X$

① effective. $\forall g \neq 1.\ \exists x.$ s.t. $gx \neq x$

ineffective $\exists g \neq 1.\ \forall x,$ s.t. $gx = x$

② transitive. $\forall x, y \in X.\ \exists g.$ s.t. $y = gx$.

$\Rightarrow$ only one orbit

③ free. $\forall g \neq 1, \forall x., g \cdot x \neq x$

Def. ① stabilizer / isotropy group

$$\mathrm{Stab}_G(x) := \{ g \in G : g \cdot x = x \} \subset G$$
$$(G^x)$$

② $X^g = \mathrm{Fix}_X(g) = \{ x \in X : g \cdot x = x \} \subset X.$

5. Stabilizer - orbit theorem.

$$O_G(x) \longrightarrow G/G^x$$
$$g \cdot x \longmapsto g \cdot G^x$$

$$|O_G(x)| = [G : G^x] = |G|/|G^x|$$

Recall Lagrange theorem.

$[G : H] = |G|/|H|$. different.

in terms of group actions cosets are

right action of H on G.

$$O_H(g) = \{ gh , h \in H \} = gH$$

$$\mathrm{Stab}_H(g) \cong H^g = \{ \underline{g \cdot h = g} , h \in H \} = \{ 1 \}$$

$|gH| = \underline{[H : H^g]} = |H|/1 = |H| \quad \Rightarrow \quad \underline{\underline{|gH| = |H|}}$

7. Group action (cont.)

7.1. terminology. ; stabilizer - orbit theorem.

7.2. centralizer and normalizer.

① G acts on G by conjugation

$$O_G(h) = \{ g h g^{-1},\ g \in G \} =: C(h)$$

$$\mathrm{Stab}_G(h) \equiv G^h = \{ g \in G .\ \underline{g h g^{-1} = h} \} =: C_G(h)$$

$(gh = hg)$ centralizer subgroup.

$\Rightarrow$ extend to subset H

$$C_G(H) = \{ g \in G :\ g h g^{-1} = h,\ \forall h \in H \}$$

$$C_G(G) = Z(G)$$

$$|C(h)| = [G : G^h]$$

② G acts on $X = \{$ all subgroups $H < G \}$

$$O_G(H) = \{ g H g^{-1} .\ \forall g \in G \}$$

$$G^H = \{ g \in G :\ \underline{g H g^{-1} = H} \} =: N_G(H)$$

Normalizer subgroup.

a. $N_G(H)$ is a subgroup.

① $e \in N_G(H)$

② $g_1, g_2 \in N_G(H)$

②

$$(g_1 g_2^{-1}) H (g_1 g_2^{-1})^{-1} = g_1 (g_2^{-1} H g_2) g_1^{-1}$$
$$= g_1 H g_1^{-1} = H$$

$$\Rightarrow g_1 g_2^{-1} \in N_G(H)$$

b. $C_G(H) \subset N_G(H)$

c. $H \triangleleft N_G(H)$ $\quad$ $\forall g \in N_G(H) : gHg^{-1} = H$

$\Rightarrow N_G(H)$ is the largest subgroup of G in which H is normal.

$$|O_G(H)| = [G : N_G(H)]$$
$\uparrow$
conjugates of H

7.3. More on terminology of group actions.

1. $X = \{1, \dots, n\}$. $G = S_n$

① effective. ✓ $\quad (\forall \phi \neq 1.\ \exists x.\ \phi \cdot x \neq x)$

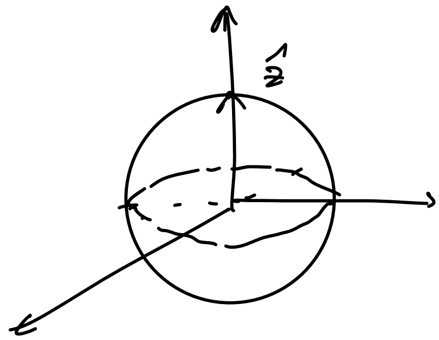
② transitive ✓

③ free ✗ $\quad (\forall \phi \neq 1.\ \forall x.\ \phi \cdot x \neq x)$

keep i fixed. $\cong S_{n-1}$

$\{ S_{n-i} \}$

2. $SO(3)$ acts on S^2



① effective. ✓

② transitive ✓

③ free ? ✗

$$\mathrm{Stab}_{SO(3)}(\hat{z}) = \left\{ \begin{pmatrix} \cos\phi & -\sin\phi & 0 \\ \sin\phi & \cos\phi & 0 \\ 0 & 0 & 1 \end{pmatrix}, \ \phi \in [0, 2\pi) \right\}$$

$$\cong SO(2)$$

$$\underbrace{\mathrm{Orb}_{SO(3)}(\hat{n})}_{= S^2} \cong SO(3) / SO(2)_{\hat{n}}$$

$$\underline{\pi_{\hat{n}}} : SO(3) \longrightarrow S^2$$

$$\underline{R} \longmapsto R\cdot\hat{n} = \hat{k} \in S^2$$

$$R_1 \hat{n} = R_2 \hat{n} = \hat{k} \qquad R_1 = R_2 \cdot R_0$$

$$R_0 \in \mathrm{Stab}(\hat{n}) \cong SO(2)_{\hat{n}}$$

3. $SU(2)$ acts on a qubit state space $\mathbb{C}^2$

a general $g \in SU(2)$

$$g = \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} \qquad |\alpha|^2 + |\beta|^2 = 1. \quad \alpha, \beta \in \mathbb{C}.$$

$$\begin{cases} \alpha = x_1 + i x_2 \\ \beta = x_3 + i x_4 \end{cases} \Rightarrow \sum_{i=1}^{4} x_i^2 = 1 \Rightarrow \underline{SU(2) \cong S^3}$$

We show it using stabilizer-orbit theorem.

The state space of a single qubit

$$|\varphi\rangle = z_1|0\rangle + z_2|1\rangle \qquad |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$\vec{z} = \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} \in \mathbb{C}^2$$

$$\{ \vec{z} \mid \vec{z}^{\,+} \vec{z} = (\bar{z}_1, \bar{z}_2) \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = |z_1|^2 + |z_2|^2 = 1 \} \cong S^3$$

$SU(2)$ acts on S^3 transitively

$$\left(g(\alpha, \beta, \gamma) = e^{-i\frac{\sigma_z}{2}\gamma} e^{-i\frac{\sigma_y}{2}\beta} e^{-\frac{i}{2}\sigma_z \alpha} \right)$$

Consider the stabilizer of $\hat{z} = |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$

$$\begin{pmatrix} \mu & \nu \\ -\bar{\nu} & \bar{\mu} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \mu \\ -\bar{\nu} \end{pmatrix} \equiv \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$\mathrm{Stab}_{SU(2)}(\hat{z}) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\mathrm{Orb}_{SU(2)}(\hat{z}) \equiv \underline{S^3} \cong SU(2)/\{1\} = \underline{SU(2)}$$

7.6 Centralizer subgroups & counting conjugacy classes

$$|C(h)| = [G : C_G(h)]$$

For a finite group

$$|C(g)| = \frac{|G|}{|C_G(g)|} \qquad (\text{stabilizer orbit})$$

$$|G| = \sum_{\substack{\text{distinct} \\ \text{conj. class } \{C(g)\}}} |C(g)| \qquad (\text{orbits partition group})$$

$$\Rightarrow |G| = \sum_{\{C(g)\}} \frac{|G|}{|C_G(g)|} \qquad \text{"class equation"}$$

Now consider the center

$$Z(G) = \{h \in G : hg = gh \ \forall g \in G\}$$

$$\forall g \in Z(G) \quad C(g) = \{hgh^{-1} \,.\, h \in G\} = \{g\}$$

$$|G| = \sum_{g \in Z(G)} |C(g)| + \sum_{\text{others}} |C(g)|$$

$$= |Z(G)| + \sum_{\substack{\{C(g)\} \\ g \notin Z(G)}} \frac{|G|}{|C_G(g)|}$$

common form of class equation

Theorem. If $|G| = p^n$, p prime. then

center is nontrivial. i.e. $Z(G) \neq \{1\}$

Proof: ① If $C_G(g) = G$. $\exists g \neq 1$ triwal.

② Lagrange theorem $\Rightarrow |C_G(g)| = p^{n-n_i}$ $0 < n_i < n$

$p \mid \underbrace{\sum \frac{|G|}{|C_G(g)|}}_{= p^{n_i}\ (n_i > 0)} \Rightarrow p \mid |Z(G)|$ i.e. $|Z(G)| \neq 1$.

Examples. $|G| = 8 = 2^3$

Abelian: $\mathbb{Z}_8$ $Z(\mathbb{Z}_8) = \mathbb{Z}_8$

non-abelian: Q $Z(Q) = \mathbb{Z}_2$

Theorem (Cauchy)

$p \mid |G|$, p prime $\Rightarrow \exists g \in G$. of order p

($g^p = 1$)

[HW] Lemma, G abelian, $p \mid |G|$. p prime

$\Rightarrow \exists g \in G$. of order p.

Proof. (by induction)

$|G| = p^m$. holds for $m=1$ ✓

If $g \notin Z(G)$, then $|C_G(g)| > 1$, then

① $p \mid |C_G(g)| \Rightarrow C_G(g)$ has an element of order p.

② $p \nmid |C_G(g)|$ ($\forall g \in G$). $|G| = [G : C_G(g)]\, |C_G(g)|$

$\Rightarrow p \mid [G : C_G(g)]$

$$|G| = |Z(G)| + \sum \frac{|G|}{|C_G(g)|}$$

$\Rightarrow p \mid |Z(G)|$

$\Rightarrow g \in Z(G)$ of order p.

7.5. Example applications of the stabilizer concept

1. Stabilizer code in Quantum information

(for details and more general error-correcting code. see "QC and QI". by Nielsen & Chuang)

Chapter 10 (10.5)

$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$

X. Y. Z gates / Pauli matrices $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

$$X|0\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle$$

$X|1\rangle = |0\rangle$ "bit-flip" ⑧

$Z|0\rangle = |0\rangle$ "phase-flip"

$Z|1\rangle = -|1\rangle$

Consider the Pauli group $P^n = (P_1)^{\otimes n}$

$P_1 = \{\pm I, \pm iI, \pm X, \pm iX, \pm Y, \pm iY, \pm Z, \pm iZ\}$

and its group action on the vector space spanned by n-qubit states. $\left(\begin{array}{l} G = P^n \\ X = (\mathbb{C}^2)^{\otimes n} \end{array} \right)$

Define $V_S = \{ \underline{|\varphi\rangle} : \underline{s|\varphi\rangle = |\varphi\rangle}, \forall s \in S \}$

where $S \subset P^n$ a subgroup.

V_S is the vector space stabilized by S

S is the stabilizer of space V_S.

For V_S to be nontrivial.

1. $\forall s_1, s_2 \in S$ $\quad s_1 s_2 = s_2 s_1$ $\quad S$ abelian

$s_1 s_2 |\varphi\rangle = s_1 |\varphi\rangle = |\varphi\rangle$
$s_2 s_1$

2. $\alpha I \in S.$ $\quad \alpha I |\varphi\rangle = |\varphi\rangle$ $\quad \alpha = 1$

i.e. $-I, \pm iI \notin S$

$(-I|\varphi\rangle = |\varphi\rangle \Rightarrow |\varphi\rangle = \vec{0})$