Recap :

1. $1 \to N \to G \to Q \to 1$

extension of Q by N.

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

Abelian. $\subset Z(G)$ central extension.

$$1 \to \mathbb{Z}_N \to \mathrm{Heis}_N \to \mathbb{Z}_N \times \mathbb{Z}_N \to 1$$

2. group actions : (left actions.)

$$G \to S_X$$

Conventions

$$\phi(g, x) = g \cdot x$$

$$\phi(g_2, \phi(g_1, x)) = g_2 \cdot (g_1 \cdot x) = (g_2 \cdot g_1) \cdot x$$

induced action on $F[X \to Y]$ $\quad f \in F$

$$\phi(g, f)(x) = f(g^{-1} \cdot x)$$

$$\phi(g_2, \phi(g_1, f))(x) = \phi(g_1, f)(g_2^{-1} x) = f(g_1^{-1} g_2^{-1} x)$$

$$(g_2 \cdot g_1 \cdot f)(g_2 \cdot g_1 x) = (g_1 f)(g_2^{-1} \cdot g_2 g_1 x) = f(g_1^{-1} g_1 x) = f(x)$$

① effective : $\forall g \neq 1$. "changes something" $\exists x . \ gx \neq x$

ineffective : $\exists g \neq 1$. nothing changes

② transitive : $\forall x . y \in X$. $\exists g . \ y = gx$

$\longrightarrow$ $\forall x . y \quad x \sim y$

single orbit.

③ free: $\forall g \neq 1$. "changes every thing" $g \cdot x \neq x$.

Defs.

① $Stab_G(x) = \{ g \in G : g \cdot x = x \} \subset G$. subgroup

② $Fix_X(g) = \{ x \in X : gx = x \} \subset X$

③ $Orb_G(x) = \{ g \cdot x \mid g \in G \} \subset X$

Theorem (orbit-stabilizer)

Let X be a G-set. Each left-coset of G^x ($= \mathrm{Stab}_G(x)$) ($x \in X$) is in a natural 1-1 correspondence with points in $O_G(x)$.

There exists a natural isomorphism

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

① Well defined.

$$g x = g' x$$
$$\Leftrightarrow (g'^{-1} g) x = x \Leftrightarrow g'^{-1} g \in G^x \Leftrightarrow g G^x = g' G^x$$

② surjective ✓

injective : $g \cdot G_x = g' \cdot G_x \Rightarrow g x = g' x$

For a finite group : $|O_G(x)| = [G : G^x] = |G| / |G^x|$

Example.

1. G acts on G by conjugation $h \in G$.

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

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

Definition. The centralizer of h in G

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

(1) $C_G(h)$ is a subgroup

① $e \in C_G(h)$: $eh = he$

② $\forall g_1, g_2 \in C_G(h)$ $(g_1 g_2^{-1})h = g_1 h g_2^{-1} = h g_1 g_2^{-1}$

$\Rightarrow (g_1 g_2^{-1}) \in C_G(h)$

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

$\uparrow$

number of conjugates of h

extend to subsets.

$$C_G(H) = \{g \in G \cdot gh = hg \ \ \forall h \in H\}$$

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

7.2 Practice with terminology of group actions

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

① effective. ✓ $(\forall \phi \neq 1, \ \underline{\exists x}, \ \phi \cdot x \neq x)$

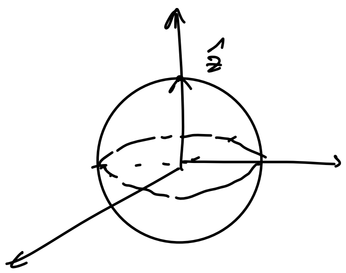
② transitive ✓

③ free ✗ $(\forall \phi \neq 1, \ \underline{\forall x}, \ \phi \cdot x \neq x)$

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

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

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



① effective. ✓

② transitive ✓

③ free ? ✗

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

$\cong SO(2)$

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

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

Previously. We know $g \in SU(2)$.

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

$$\begin{aligned} \alpha &= x_1 + i x_2 \\ \beta &= x_3 + i x_4 \end{aligned} \quad \longrightarrow \quad \Sigma\, x_i^2 = 1. \quad \cong S^3$$

$$\Rightarrow SU(2) \cong S^3$$

Now. from the perspective of orbit-stabilizer theorem:

$$|\psi\rangle = z_1 |0\rangle + z_2 |1\rangle$$

$$\vec{z} = \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} \in \mathbb{C}^2 \qquad |z_1|^2 + |z_2|^2 = 1 \qquad \vec{z} \text{ lives on } S^3$$

$SU(2)$ acts on S^3 transitively = One orbit

$$g(\alpha.\ \beta.\ \gamma) = e^{-i\frac{\sigma_3}{2}\gamma}\, e^{-i\frac{\sigma_2}{2}\beta}\, e^{-i\frac{\sigma_3}{2}\alpha}$$

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

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

$\mu = 1.\ \nu = 0$

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

$$\mathrm{Orb}_{SU(2)}(\hat{z}) \cong SU(2)/\{1\} = SU(2)$$

$$= S^3$$

7-3 centralizer subgroups and counting conj. cls.

(Moore §9)

1. Centralizer & normalizer

① G acts on G by conjugation

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

$Stab_G(h) \equiv G^h = \{g\in G.\ ghg^{-1}=h\} =: C_G(h)$

$(gh=hg)$ centralizer subgroup.

$\Rightarrow$ extend to subset H

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

$C_G(G) = Z(G)$

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

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

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

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

Normalizer subgroup.

- $N_G(H)$ is a subgroup.
  ① $e\in N_G(H)$

  ② $g_1, g_2\in N_G(H)$

$$(g_1g_2^{-1})H(g_1g_2^{-1})^{-1} = g_1(g_2^{-1}Hg_2)g_1^{-1}$$
$$= g_1Hg_1^{-1} = H$$

$\Rightarrow g_1g_2^{-1}\in N_G(H)$

2. counting conj. classes

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

$$Z(G) = \{ h \in G : hg = gh . \forall g \in G \} \quad \text{abelian subgrp.}$$

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

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

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

Theorem. If $|G| = p^n$, p prime. then center is nontrivial. i.e. $Z(G) \neq \{1\}$

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

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

$\Rightarrow$ center nontrivial

② Pick $g \neq 1 \notin Z(G)$. then

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

$p \mid \sum \frac{|G|}{|C_G(g)|} \Rightarrow p \mid |Z(G)|$ i.e. $|Z(G)| \neq 1$.

$= \sum p^{n_i}$ $(n_i > 0)$

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

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

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

D_4 $Z(D_4) = \mathbb{Z}_2$

Theorem (Cauchy)

If $p \mid |G|$. p a prime. then $\exists g \neq 1 \in G$. s.t. g of order p.

Proof by induction:

Lemma: the statement holds for abelian G.

Proof. $|G| = pm$.

the Lemma holds for $m=1$. since if $|G|=p$.

G is cyclic. as a result of Lagrange theorem

then any element $g \in G$ has order p ($g^p=1$)

Now suppose for a general $m>1$, $\exists h \in G$. s.t. h has order t, i.e. $h^t = 1$

① if $p \mid t$. then $h^{t/p}$ is of order p.

② else $\langle h \rangle$ is a normal subgroup. ($\because G$ is abelian)

$G/\langle h \rangle$ is an abelian group of order

$|G|/t = pm/t$ $\quad (\because |\langle h \rangle| = t)$

then m/t is an integer smaller than m.

by induction. $G/\langle h \rangle$ has an element

of order p

homomorphism φ: $G \longrightarrow G/\langle h \rangle$ a surjection.

$g \longmapsto g\langle h \rangle$

$\Rightarrow \exists\, g \neq 1$ s.t. $g\langle h\rangle$ has order p. then

$\varphi(g^p) = (g\langle h\rangle)^p = g^p\langle h\rangle = 1_{G/\langle h\rangle} = \langle h\rangle$

$g^p = h^x \in \langle h\rangle$

if $h^x = 1 \Rightarrow g^p = 1$

else $\exists y$. s.t. $(h^x)^y = 1 \Rightarrow g^{py} = 1 \Rightarrow (g^y)^p = 1$

$\underline{g^y \in G \text{ of order } p.}$

<u>Proof of general cases (G nonabelian)</u>:

$|G| = pm$. holds for $m=1$ ✓

If $g \notin Z(G)$, then $\underset{< |G|}{1 < |C_G(g)|}$, then of.

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

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

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

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

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

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

7.4 Example applications of the stabilizer concept

1. In solid state physics, we talk about "little group"

$\{ g \in P . \quad gk = k + K \}$

K reciprocal lattice

irreps of little group at k determine the bloch wave symmetry, band degeneracy.

2. Stabilizer code in Quantum information

(for details and more general error-correcting code, see § 10.5 "QC and QI". by Nielsen & Chuang)

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

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

$X|1\rangle = |0\rangle$ "bit-flip"

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

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

① Set up

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.

$G = P_n \qquad X = (\mathbb{C}^2)^{\otimes n}$

② Stabilizer subgroups and code spaces

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

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

$\begin{cases} V_S \text{ is the vector space stabilized by } S \quad \text{(Code space)} \\ S \text{ is the stabilizer of space } V_S. \end{cases}$

For V_S to be nontrivial,

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

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

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

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

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

$\dim V_S = 2^{n-r} \qquad n$: # physical qubits $\quad r$: independent generators