Recap groups. subgroups

1 (G, m, I, e) — set

$g_1(g_2 g_3) = (g_1 g_2) g_3$

m, I.

$m: G \times G \to G$

$I: G \to G$

uniqueness e, $\forall a \to a^{-1}$

2. subgroup. $H \subset G$. m, I

3. order $|G|$

4 direct product: $Z_2 \times Z_2 \to V$

5. $GL(n, K)$

$O(n, K)$ $AA^T = \mathbb{1}$ $(= A^T A = \mathbb{1})$

$SO(n, K)$ $\det A = 1$

$U(n) \subset GL(n, \mathbb{C})$ $AA^+ = \mathbb{1}$

$SU(n)$ $\det = 1$

$A J_{p.q} A^T = J_{p.q} \longrightarrow O(1.3)$

$\boxed{\det A = 1 \quad A \in Sp(2n)}$ $Sp(2n)$

Example (HW) $Sp(2n. k)$ & canonical transformations

$q^i . p_i \ (i=1,\cdots n)$ coordinates & momentum.

$f(\vec{q}.\vec{p}) \quad g(\vec{q},\vec{p})$.

Poisson bracket

$$\{f, g\} = \sum_{i=1}^{n} \left(\frac{\partial f}{\partial q^i}\frac{\partial g}{\partial p_i} - \frac{\partial f}{\partial p_i}\frac{\partial g}{\partial q^i} \right)$$

$$\Rightarrow \{q^i . q^j\} = \{p_i . p_j\} = 0$$

$$\{q^i . p_j\} = \delta^i_j$$

Canonical transform $\rightarrow \vec{Q}, \vec{P}$

$$\begin{pmatrix} Q^1 \\ Q^2 \\ \vdots \\ P^1 \\ P^2 \\ \vdots \end{pmatrix} = A \begin{pmatrix} q^1 \\ q^2 \\ \vdots \\ p^1 \\ p^2 \\ \vdots \end{pmatrix}$$

$$\{Q^i . Q^j\} = \{P_i . P_j\} \Rightarrow \{Q^i . P_j\} = \delta^i_j$$

$$\Leftrightarrow \underline{A \in Sp(2n)}$$

Definition: if X is a subset of G, then the smallest subgroup of G containing X, denoted $\langle X \rangle$, is called the subgroup generated by X. or we say X generates $\langle X \rangle$ ②

Remarks.

1. $G = \langle X \rangle$. X generates G.

   $|X| < \infty$. "finitely generated"

2. group preservation:

$$G = \langle g_1 \cdots g_n \mid \overset{\nearrow \text{relation}}{R_1 \cdots R_r} \rangle$$

$\uparrow$ generating elements

3. $1/e$ is usually not included.

Example:

$\mathbb{Z}_N$ or μ_N: $\langle A \mid A^N = 1 \rangle$

μ_N. $\langle \omega = e^{i\frac{2\pi}{N}} \mid \omega^N = 1 \rangle$

$\mathbb{Z}_N : \langle \bar{1} \mid (\bar{1})^N = \bar{0} \rangle$

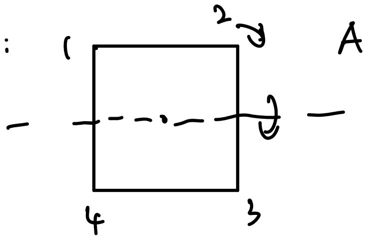
$\underbrace{\bar{1} + \bar{1} \cdots + \bar{1}}_{N}$

4-group: $\mathbb{Z}_2 \times \mathbb{Z}_2$: $\langle A, B \mid A^2 = B^2 = (AB)^2 = 1 \rangle$

$A^m B^n$: $\underline{1, A, B, AB}$ $A^2 B = B$

dihedral D_n : $\langle A, B \mid A^n = B^2 = (AB)^2 = 1 \rangle$ $D_2 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$

D_4 :



$A = C_n \qquad A^4 = 1$

$B^2 = 1$

<u>Example</u>: Quaternion group.

$$i^2 = j^2 = k^2 = -1 \qquad ij = -ji = k$$

$$jk = -kj = i$$

$$ki = -ik = j$$

$$Q = \{ \pm 1, \pm i, \pm j, \pm k \}$$

$$= \langle x, y \mid x^4 = 1,\ x^2 = y^2,\ y^{-1} x y = x^{-1} \rangle$$

$$= \langle i, j \rangle$$

Pauli matrices: $\sigma^1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $\sigma^2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$

$$\sigma^3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$\sigma^i \sigma^j = \delta^{ij} + i \epsilon^{ijk} \sigma^k \qquad ([\sigma^i, \sigma^j] = 2i \epsilon^{ijk} \sigma^k)$$

$$\Rightarrow i = -i\sigma^1, \quad j = -i\sigma^2 \quad k = -i\sigma^3$$

$$Q = \langle -i\sigma^1, -i\sigma^2 \rangle \subset SU(2)$$

Example Pauli group.

$$P_1 = \{\pm 1, \pm i, \pm\sigma^1, \pm\sigma^2, \pm\sigma^3, \pm i\sigma^1, \pm i\sigma^2, \pm i\sigma^3\}$$

$$= \langle \sigma^1 \sigma^2 \sigma^3 \rangle \qquad i = \sigma^1\sigma^2\sigma^3$$

$X \; Y \; Z$

Qubit two-dim. Hilbert space

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \qquad |\varphi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

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

X : "bit-flip"

NOT

$$X|1\rangle = |0\rangle$$

$$Z|0\rangle = |0\rangle$$

"phase-flip"

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

"Stabilizer codes" : "Toric code"

(Kitaev)

$\swarrow$ QI. $\downarrow$ Topology $\downarrow$ Group $\searrow$ Strongly correlated

3. Homomorphism & Isomorphism

<u>Definition</u>. Let (G, m, I, e) & (G', m', I', e') be two groups.

Homomorphism $\varphi : G \longrightarrow G'$, s.t. $\forall g_1, g_2 \in G$

$$\varphi(m(g_1, g_2)) = m'(\varphi(g_1), \varphi(g_2))$$

$$\left(\varphi(g_1 \cdot g_2) = \varphi(g_1) \cdot \varphi_2(g_2) \right)$$

$$\begin{tikzcd}
G \times G \arrow[r, "m"] \arrow[d, "\varphi \times \varphi"'] & G \arrow[d, "\varphi"] \\
G' \times G' \arrow[r, "m'"] & G'
\end{tikzcd}$$

"commutative diagram."

$$\varphi(e) = \varphi(e \cdot e) = \varphi(e)\varphi(e)$$
$$\Vert$$
$$a' = a' \cdot a'$$
$$a' = a' \cdot (a')^{-1} = e'$$

inversion:

$$\begin{tikzcd}
G \arrow[r, "I"] \arrow[d, "\varphi"'] & G \arrow[d, "\varphi"] \\
G' \arrow[r, "I'"] & G'
\end{tikzcd}$$

$$\varphi(e) = \varphi(g \cdot g^{-1})$$
$$= \varphi(g) \cdot \varphi(g^{-1})$$
$$= e'$$

$$\Rightarrow \varphi(g^{-1}) = (\varphi(g))^{-1}$$

Remarks :

1. $\varphi(g) = e'$. iff $\underline{g=e}$ $\quad$ φ is injective

$\|$ $\forall g_1, g_2 \in G$.

$\quad \varphi(g_1) = \varphi(g_2) \Rightarrow g_1 = g_2$

$$e' = \varphi(g_1)\cdot\varphi(g_2)^{-1} = \varphi(\underline{g_1 g_2^{-1}}) = \varphi(g_3 = e)$$

2. $\forall g' \in G'$. $\exists g \in G$. s.t. $\varphi(g) = g'$ $\quad$ surjective

3. (Def) φ is an isomorphism if both injec. & surjec. (bijective)

$$G \underset{\varphi^{-1}}{\overset{\varphi}{\rightleftarrows}} G'$$

φ^{-1} is also an isomorphism. (HW)

isomorphism defines an equivalence relation.

" isomorphic groups are the same ".

4. (Def) $G' = G$ $\quad \varphi : G \to G$

isomorphism $\rightarrow$ "automorphism"

Definition (kernel & image)

φ homo. $\varphi : G \longrightarrow H$

(a) kernel K

$$K = \ker \varphi := \{ g \in G : \varphi(g) = 1_H \}$$

(b) image

$$\operatorname{im} \varphi := \{ h \in H : \exists g \in G \text{ s.t. } \varphi(g) = h \}$$
$$= \varphi(G)$$

Remarks.

(a) $\varphi(G) \subset H$. is a subgroup.

① $\varphi(1_G) = 1_H$

② $\forall h_1 = \varphi(g_1)$, $h_2 = \varphi(g_2)$

$$h_1 h_2 = \varphi(g_1)\varphi(g_2) = \varphi(g_1 \cdot g_2) \in \varphi(G)$$

③ $h_1 = \varphi(g_1)$ $\quad 1_H = \varphi(g_1 \cdot g_1^{-1}) = \underbrace{\varphi(g_1)}_{h_1} \cdot \underbrace{\varphi(g_1^{-1})}_{h_2}$

$$\varphi(G) \ni h_2 = h_1^{-1}$$

(b) $K = \ker \varphi$ is a subgroup of G.

(c) φ is an isomorphism.

$\ker \varphi = \{1\}$ inj.

$\operatorname{im} \varphi = H$ surj.

<u>Example</u>. μ_N & $\mathbb{Z}_N$

$$\mu_N = \{1, \omega, \omega^2, \dots \omega^{N-1}\}$$

$$\mathbb{Z}_N = \{\bar{0}, \bar{1}, \dots \overline{N-1}\}$$

$$\varphi : \mathbb{Z}_N \to \mu_N$$

$$r' \in r + N\mathbb{Z}$$

$$\varphi(\bar{r} = r + N\mathbb{Z}) := e^{i\frac{2\pi}{N}r'}$$

① $\varphi(\bar{r}_1 + \bar{r}_2) = \varphi(\bar{r}_1)\varphi(\bar{r}_2)$ ✓

② $\varphi(\bar{r}) = 1 \Leftrightarrow \bar{r} = \bar{0}$ ✓

③ $\forall \omega^j \in \mu_N$, $\exists \varphi(\bar{r}_j) = \omega^j$ ✓

$\Big\}$ φ an isomorphism

<u>Example</u>. power map.

$$P_K : \mu_N \to \mu_N$$

$$P_K(z) = z^K$$

① $(z_1 z_2)^K = z_1^K z_2^K$ ✓

② isomorphism ? $\gcd(k, N) = 1$

$K = N\mathbb{Z}$ $\quad P_K(z) = 1$ $\quad$ trivial

$\mu_4 \longrightarrow \mu_4 \qquad k=2$

$$1 \longrightarrow 1$$
$$i = e^{i\frac{2\pi}{4}} \longrightarrow -1$$
$$-1 \longrightarrow 1$$
$$-i \longrightarrow -1$$

$\ker(p_2) = \{\pm 1\} \cong \mathbb{Z}_2$

$\operatorname{im}(p_2) = \{\pm 1\}$

$m_k : \mathbb{Z}_N \longrightarrow \mathbb{Z}_N$

$m_k(\bar{r}) = \overline{kr}$

$$\begin{array}{ccc} \mathbb{Z}_N & \xrightarrow[m_k]{m_{k_1}} & \mathbb{Z}_N \\ \downarrow \varphi & & \downarrow \varphi \\ \mu_N & \xrightarrow[p_{k_2}]{p_k} & \mu_N \end{array}$$

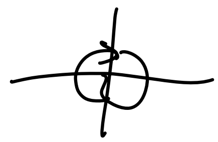
$\varphi \circ m_k = p_k \circ \varphi$

Commute iff $k_1 = k_2 \bmod N$.

<u>Example</u> $\varphi : U(1) \longrightarrow SU(2)$

$$\varphi(z) := \begin{pmatrix} z^N & 0 \\ 0 & z^{-N} \end{pmatrix}$$

$e^{i\theta} = t \in U(1)$



$(e^{i\theta})^N = 1$

$\ker(\varphi) \cong \mu_N$

Example $SU(2) \leftrightarrow SO(3)$ $\quad \mathbb{R}^3$

① $\mathbb{R}^3 \to 2\times 2$?

Def. homomorphism

$$h : \mathbb{R}^3 \to \mathcal{H}_2^0 \quad (\text{vector space of } 2\times 2 \text{ traceless matrices})$$

$$h(\vec{x}) = \vec{x}\cdot\vec{\sigma} = x_i \cdot \sigma^i = \begin{pmatrix} x^3 & x^1 - i x^2 \\ x^1 + i x^2 & -x^3 \end{pmatrix} \in \mathcal{H}_2^0$$

is an isomorphism.

② For a given $u \in SU(2)$. define homomorphism by conjugation:

$$C_u : \mathcal{H}_2^0 \to \mathcal{H}_2^0$$

$$C_u(m) := u m u^{-1} \quad (m \in \mathcal{H}_2^0)$$

$$\left(\begin{cases} tr(u m u^{-1}) = tr(m) = 0 \\ (u m u^{-1})^{+} = u m^{+} u^{-1} = u m u^{-1} \end{cases} \Rightarrow C_u(m) \in \mathcal{H}_2^0 \right)$$

Define $R(u) : \mathbb{R}^3 \longrightarrow \mathbb{R}^3$. s.t.

$$\begin{tikzcd} \mathbb{R}^3 \arrow[r, "\boxed{R(u)}"] \arrow[d, "h"'] & \mathbb{R}^3 \arrow[d, "h"] \\ \mathcal{H}_2^0 \arrow[r, "C_u"'] & \mathcal{H}_2^0 \end{tikzcd}$$

$h \circ \underline{R(u)} = C_u \circ h$

$(R(u) \cdot \vec{x}) \cdot \vec{\sigma} = u\, \vec{x} \cdot \vec{\sigma}\, u^{-1}$

$(\vec{x} \in \mathbb{R}^3)$

In other words. we define a homomorphism

$$R : SU(2) \longrightarrow GL(3, \mathbb{R})$$

s.t. $\forall \vec{x} \in \mathbb{R}^3$. $R(u)$ satisfy

$$\boxed{u\, \vec{x} \cdot \vec{\sigma} \cdot u^{-1} = (R(u)\, \vec{x}) \cdot \vec{\sigma}}$$

$u x_i \sigma^i u^{-1} = (R(u)_{ji}\, x_i) \cdot \sigma_j \qquad \forall \vec{x} \in \mathbb{R}$

$\Rightarrow u \sigma^i u^{-1} = R(u)_{ji}\, \sigma_j$

$$\begin{aligned}(u_1 u_2)\, \sigma_i\, (u_1 u_2)^{+} &= u_1 (R(u_2)_{ji}\, \sigma_j)\, u_1^{+} \\ &= R(u_1)_{ji} (u_1 \sigma_j u_1^{+}) \\ &= \underline{R(u_2)_{ji}\, R_{kj}(u_1)\, \sigma_k} \\ &= R(u_1 u_2)_{ki}\, \sigma_k\end{aligned}$$

$\Rightarrow R(u_1 u_2) = R(u_1) \cdot R(u_2)$

② $\vec{y} = R(u) \cdot \vec{x} \qquad \det(\vec{x} \cdot \vec{\sigma}) = -\vec{y}^{\,2}$

$\vec{y}^{\,2} = -\det((R(u) \cdot \vec{x}) \cdot \vec{\sigma}) = -\det(u\, \vec{x} \cdot \vec{\sigma}\, u^{-1}) = \vec{x}^{\,2}$

$\Rightarrow \quad R(u) \in O(3)$

② $\quad R(\mathbb{1}_2 \in SU(2)) = \mathbb{1}_3 \qquad R(u) \overset{?}{\in} SO(3)$

$$\mathrm{tr}(\sigma^i \sigma^j \sigma^k) = \epsilon_{ijk} \cdot (2i)$$

$$2i = \mathrm{tr}(\sigma^1 \underset{uu^+}{\hat{}} \sigma^2 \underset{uu^+}{\hat{}} \sigma^3 \overset{uu^+}{\hat{}}) = \mathrm{tr}(\underline{u\sigma^1 u^+}\,\underline{u\sigma^2 u^+}\,\underline{u\sigma^3 u^+})$$

$$= R_{i1}(u) R_{j2}(u) R_{k3}(u)\, \underline{\mathrm{tr}(\sigma^i \sigma^j \sigma^k)}$$

$$= (2i) \cdot \underline{\epsilon_{ijk} R_{i1}(u) R_{j2}(u) R_{k3}(u)}$$

$$= (2i)[\det R(u)]$$

$\Rightarrow \det R(u) = 1$

$\Rightarrow \quad R(u) \in SO(3)$

$R(u) = R(-u) \qquad SU(2)$ double cover of $SO(3)$

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