Recap.

1. Group: $(G. m. I. e)$

   1. $g_1(g_2g_3) = (g_1g_2)g_3$

   $\underline{m}$: $G \times G \to G$ $\quad$ e: $eg = ge$

   $\underline{I}$: $G \to G$ $\quad$ $g^{-1}g = gg^{-1} = e$

2. subgroup. $H \subset G$. $\quad$ $\underset{\sim}{m}$. $\underline{I}$. closed on H

3. order $|G|$ $\quad$ # elements in G

   $\hookrightarrow$ order of $g \in G$ $\quad$ $\underline{\underline{g^n = 1_G}}$ $\quad$ minimal n

   cyclic group $\mu_N = \{1, \omega, \ldots \omega^{N-1}\}$

   循环群 $\quad$ $N = 4$ $\quad$ $\omega_j = e^{i\frac{\pi}{2}j}$

   order $\omega_1 = 4$

   order of $\omega_2 = 2$

4. equivalence relation $a \sim b$ $\quad$ $[a] = \{x \in X \mid x \sim a\}$

5. direct product. $\mathbb{Z}_2 \times \mathbb{Z}_2 \to V$ $\quad$ Vier-group

   4-group

6. $GL(n, K)$

$$\left\{\begin{array}{lll} O(n. K) & AA^T = \mathbb{1} & \Rightarrow (\det A)^2 = 1 \\ SO(n. K) & \det A = 1 & \\ U(n) \in GL(n. \mathbb{C}) & AA^\dagger = \mathbb{1} & \Rightarrow |\det A| = \underline{1} \\ SU(n) & \det A = 1 & \end{array}\right.$$

$AJA^T = J$ $\qquad O(p,q)$. $\quad J = \begin{pmatrix} -\mathbb{1}_{p\times p} & 0 \\ 0 & \mathbb{1}_{q\times q} \end{pmatrix}$

$Sp(2n) \qquad J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$

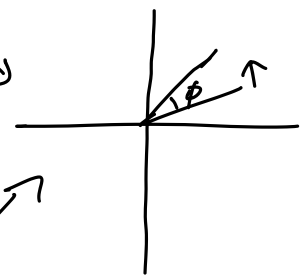
Examples.

1. $SO(2,\mathbb{R}) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \qquad \underline{a^2+b^2=1}$

$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \Rightarrow \begin{matrix} AA^T = 1 \\ \det A = 1 \end{matrix}$

$$R(\phi) = \begin{pmatrix} \cos\phi & -\sin\phi \\ \sin\phi & \cos\phi \end{pmatrix} = \underline{e^{-\phi J}} \qquad J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

$$R(\phi_1) R(\phi_2) = R(\phi_1+\phi_2)$$



2. $U(1)$: $\quad z(\phi) = \underline{e^{i\phi}}$

$$z(\phi_1) z(\phi_2) = z(\phi_1+\phi_2)$$

$$SO(2) \cong U(1) \sim S^1$$

$$e^{\phi J} \longleftrightarrow e^{i\phi}$$

$$z(\phi_1) z(\phi_2) = z(\phi_1+\phi_2)$$

$$R(\phi_1) R(\phi_2) = R(\phi_1+\phi_2)$$

3. $SU(2)$: $\quad g = \begin{pmatrix} z & -w^* \\ w & z^* \end{pmatrix} \qquad \underline{|z|^2 + |w|^2 = 1}$

$z = x_0 + i x_1$

$w = x_2 + i x_3$

$$\sum_{i=0}^{3} x_i^2 = 1 \sim S^3$$

4. $Sp(2n, k)$ $\quad A^T \underline{J} A = \underline{\underline{J}}$

$$\Rightarrow (\det A)^2 = 1 \qquad \det A = \pm 1$$

$$\Rightarrow \det A = 1$$

Pfaffian. antisymmetric J

普法夫值 $\Rightarrow \underset{\overset{\| \text{ symp.}}{J}}{Pf(A^T J A)} = \det(A) \cdot Pf(J)$

$pf(A)^2 = \det A$

$$\Rightarrow \det(A) = 1$$

5. $O(p, q)$ $\qquad \det(O(p,q)) = \pm 1$

$\hookrightarrow SO(p,q) \qquad \det = 1$

<u>Definition</u>: 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 <u>X generates $\langle X \rangle$</u>.

<u>Remarks</u>. 1. $G = \langle X \rangle$.

$|X| < \infty$ finitely generated

2. (Def) group presentation. 展示

$$G = \langle g_1, \cdots g_n \mid R_1 \cdots R_r \rangle$$

generating elements ↑ ↖ relations

$$\mu_N = \langle \underset{1}{\omega} = e^{i\frac{2\pi}{N}} \rangle$$

$Z = \langle 1 \rangle$ $$= \langle \omega \mid \omega^N = 1 \rangle$$

3. 1 / e is not included.

Why presentation? ⇒ show that there are at most $\log|G|$ generators

if $G = \langle g_1 \cdots g_\ell \rangle$. pick $g' \notin G$. $g \in G$. then

$gg' \notin G$. otherwise $g^{-1}(gg') \in G$. then $\forall f \in G\ g \notin G$.

⇒ adding one new generator at least doubles the # elements

Examples.

$Z_2 \times Z_2$

$I = (1, 1)$

$A = (-1, 1) \rightarrow A^2 = (1, 1)\quad A^3 = A$

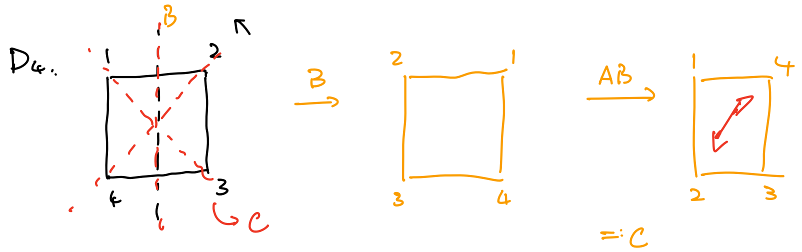
$B = (1, -1) \rightarrow B^2 = (1, 1)\quad B^3 = B$

$C = (-1, -1)\quad C^2 = 1$

$$\langle A, B \mid \underline{A^2 = B^2 = (AB)^2 = 1} \rangle$$

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

二面体群 dihedral group $D_n := \langle A, B \mid A^n = \underline{B^2 = (AB)^2} = 1 \rangle$



$D_2 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$

<u>Examples</u> Quaternion group 四元数群

$$\underline{i}^2 = \underline{j}^2 = \underline{k}^2 = -1$$

$$\begin{cases} \underline{ij} = \underline{-ji} = \underline{k} \\ jk = -kj = i \\ ki = -ik = j \end{cases}$$

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

$$= \langle a, b \mid a^4 = 1,\ a^2 = b^2,\ b^{-1} a b = a^{-1} \rangle$$

$$\cong \langle i, j \rangle$$

<u>Quiz</u> : $Z(Q)$?

$$Q/Z(Q) \cong D_2 \cong V_4 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$$

$$\underline{\sigma^i \sigma^j} = \delta^{ij} + \underset{\Delta}{i}\, \epsilon^{ijk} \underline{\sigma^k}$$

$$\underline{i} = -i\sigma^1 \qquad \underline{j} = -i\sigma^2 \qquad \underline{k} = -i\sigma^3$$

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

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

<u>Pauli group</u>

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

$$= \langle \sigma^1, \sigma^2, \sigma^3 \rangle$$

Qubit . two-dim Hilbert space

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

$\sigma^1 = X$

$$\begin{cases} X|0\rangle = \begin{pmatrix}0&1\\1&0\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}0\\1\end{pmatrix} = |1\rangle & \text{"bit-flip"} \\ X|1\rangle = |0\rangle & \text{NOT} \end{cases}$$

$$(\sigma^3 =) Z|0\rangle = |0\rangle \qquad \begin{pmatrix}1&\\&-1\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}1\\0\end{pmatrix}$$

$$Z|1\rangle = -|1\rangle \qquad \text{"phase-flip"}$$

$\Rightarrow \underline{P_n = P_1^{\otimes n}}$ for n qubits

"<u>Stabilizer codes</u>" $S \in P_n$ abelian.

code space $C = \{|\psi\rangle : g|\psi\rangle = |\psi\rangle . \ \forall g \in S\}$

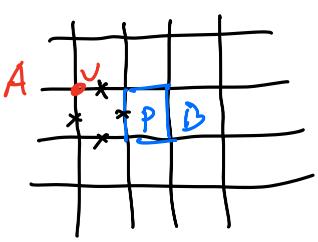
eg. $S = \langle Z_1 Z_2, \ Z_2 Z_3 \rangle \in P_3$ $\quad C = \mathrm{span}\{|000\rangle, |111\rangle\}$

① Nielsen & Chuang Quantum computing and Quantum information

Chap. 10.5

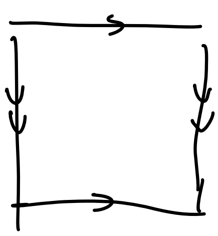
② Kitaev "<u>Toric</u> code" → strongly correlated

$H = -\sum A - \sum B$

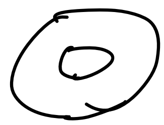


QI

Topology



→



$\mathbb{Z}_2 \times \mathbb{Z}_2$

$A = \prod_{e \in v} X_e \qquad B = \prod_{e \in P} Z_e$

3. Homomorplism & Isomorplism 同态 & 同构

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

be two groups.

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

$$\varphi(\underline{m}(g_1, g_2)) = \underline{m}'(\varphi(g_1), \varphi(g_2))$$

$$\varphi(g_1 \cdot g_2) = \varphi(g_1) \cdot \varphi(g_2)$$

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

Commutative diagram

交换图表

$$\underline{\varphi(e)} = \varphi(e \cdot e) = \underline{\varphi(e)}\,\underline{\varphi(e)}$$

$$\Rightarrow \varphi(e) = e'$$

Inversion:

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

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

$$\underline{\varphi(g^{-1})} = \underline{[\varphi(g)]^{-1}}$$

✓

Remarks:

1. $\varphi(g) = e'$ iff $g = e$. φ is injective

$\Updownarrow$ $\forall g_1, g_2 \in G$

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

$\Downarrow$

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

$\Rightarrow g_1 = g_2$

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

3. (Def) φ is an isomorphism if

it is ~~both~~ injective & surjective.

(bijective)

双射

$G \underset{\varphi^{-1}}{\overset{\varphi}{\rightleftarrows}} G'$ φ^{-1} is also an isomorphism

$\varphi^{-1}(g_1' g_2') = \varphi^{-1}(\varphi(g_1)\varphi(g_2)) = \varphi^{-1}(\varphi(g_1 g_2)) = g_1 g_2 = \varphi^{-1}(g_1')\varphi^{-1}(g_2')$

isomorphism defines an equivalence relation

"isomorphic groups are the same"

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

isomorphism $\Rightarrow$ "automorphism"

自同构

$\mu_4 \cong \mathbb{Z}_4$

$\mathbb{Z}_4 \longrightarrow \mathbb{Z}_4$

$\bar{0} \longleftrightarrow \bar{0}$

$\bar{1}$ $\bar{1}$

$\bar{2}$ $\bar{2}$

$\bar{3}$ $\bar{3}$

$\bar{x} \longmapsto 3\bar{x}$

$\bar{x} \longmapsto k \cdot \bar{x}$

? $\gcd(k, N) = 1$