Recap.

1. $(G.\ m.\ I.\ e)$

   1. $g_1(g_2 g_3) = (g_1 g_2) g_3$

      $\underline{m}: G \times G \longrightarrow G$

      $\underline{I}: G \longrightarrow G$

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

3. order $|G|$ $\# G$.

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

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

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

   order $\omega_1 = 4$

   order of $\omega_2 = 2$

4. direct product. $\mathbb{Z}_2 \times \mathbb{Z}_2 \longrightarrow V$ Vier-group

   4-group

5. $GL(n, K)$

   $O(n.K)$ $AA^T = \mathbb{1} \Rightarrow (\det A)^2 = 1$

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

   $U(n) \in GL(n. \mathbb{C})$ $AA^+ = \mathbb{1} \Rightarrow |\det A| = \underline{1}$

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

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

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

Examples:

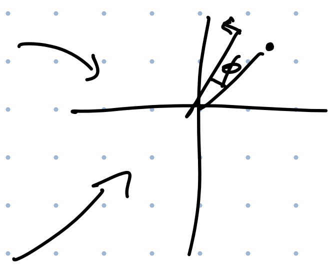
1. $SO(2,\mathbb{R}) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \qquad \underline{a^2+b^2=1}$

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

$\det A = 1$

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

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



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

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

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

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

$z = x_0 + i x_1$

$w = x_2 + i x_3$

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

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

$$\Rightarrow \underset{\substack{\parallel \\ J}}{Pf(A^T J A)} = \det(A) \cdot Pf(J)$$

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

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

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

<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.

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

generating elements

relations

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

$$\mathbb{Z} = \langle 1 \rangle \qquad = \langle \omega \mid \omega^N = 1 \rangle$$

3. $1 / e$ is not included.

Examples.

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

$I = (1, 1)$

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

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

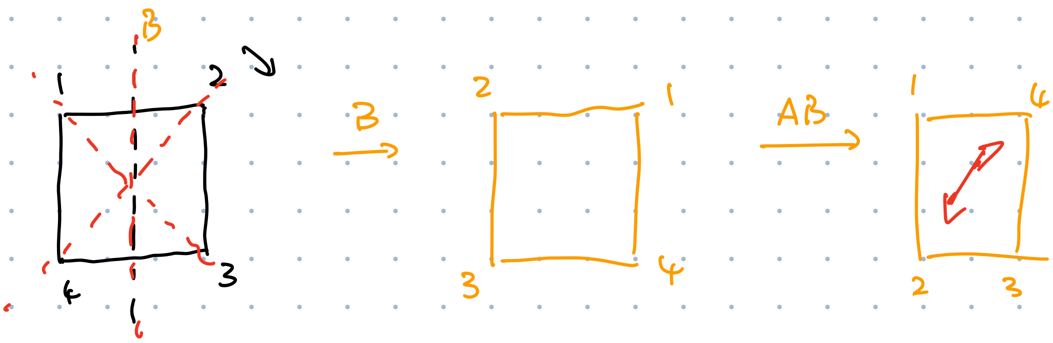
$C = (-1, -1) \quad C^2 = 1$

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

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

dihedral group $D_n := \langle A, B \mid A^n = B^2 = (AB)^2 = 1 \rangle$

D_4:



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

Examples Quaternion group

$$i^2 = j^2 = k^2 = -1 \qquad \begin{cases} ij = -ji = k \\ jk = -kj = i \\ ki = -ik = j \end{cases}$$

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

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

$$\equiv \langle i, j \rangle$$

$$\sigma^i \sigma^j = \delta^{ij} + i \epsilon^{ijk} \sigma^k$$

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

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

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

Pauli group

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

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

↳ adding one generating element,

at least doubles the group elements

$\# X \sim \log |G|$

Qubit. two-dim Hilbert space

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

$$\sigma^1 = X$$

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

"bit-flip"

NOT

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

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

"phase-flip"

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

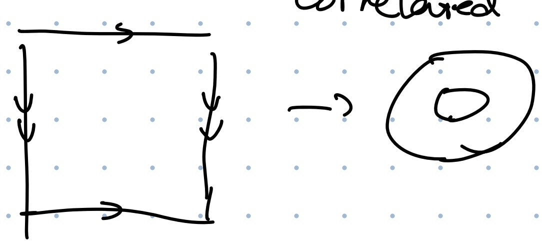
"<u>Stabilizer codes</u>"

① Nielsen & Chuang Quantum computing and Quantum information Chap. 10.5

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

QI

Topology



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

3. Homomorphism & Isomorphism

Definition. Let (G, m, I, e), & (G', m', I', e')

be two groups.

Homomorphism $\varphi : G \to G'$. 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

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

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

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)

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

isomorphism defines an equivalence relation

"isomorphic groups are the same"

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

isomorphism $\Rightarrow$ "automorphism"

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

$\mathbb{Z}_4 \to \mathbb{Z}_4$

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

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

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

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

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

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

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

Definition (kernel & image)

φ homomorphism $\varphi : G \longrightarrow H$

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

$$h_1 h_2 = \varphi(g_1)\varphi(g_2) = \varphi(\underline{g_1 g_2}) \in \varphi(G) \quad ✓$$

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

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

(c) φ is an isomorphism:

$\ker \varphi = \{1_G\}$ injective

$\operatorname{im} \varphi = H$ surjective

Example $\mu_N \cong \mathbb{Z}_N$

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

$$\bar{r} = r + N\mathbb{Z} \mapsto e^{i\frac{2\pi}{N} r'} \qquad r' \in r + N\mathbb{Z}.$$

isomorphism

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

$+_{\mathbb{Z}_N}$ $\quad \cdot_{\mu_N}$

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

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

Example. P_k power map

$$P_k : \mu_N \to \mu_N$$

$$z \mapsto z^k$$

① $(z_1 z_2)^k = z_1^k \cdot z_2^k$ homo.

② isomorphism. $\gcd(k, N) = 1$?

$k = N\mathbb{Z}$ $\quad P_k(z) = 1$ trivial

$\mu_4 \to \mu_4 \quad k = 2$

$\ker(P_2) = \{\pm 1\}$

$\mathrm{im}(P_2) = \{\pm 1\}$ $\cong \mathbb{Z}_2$

③ $U(1) \cong SO(2, \mathbb{R})$

Next week. $SU(2) \longleftrightarrow SO(3)$