Recap:

1 $(G, \underline{m}, \underline{I}, e)$

$$\begin{cases} \underline{m} : G \times G \to G \\ \underline{I} : G \to G \\ \exists e \end{cases}$$

$\underline{m}$ associtivity) semigroup

$\exists e$) unital monoid

$\exists g^{-1}$) group

topological group $\quad \underline{m}, \underline{I}$ cont.

Lie group $\quad \underline{m}, \underline{I}$ real analytic
local coord

2. $|G|$, $\# G$ $\quad |G| < \infty$ finite group

3. N^{th}-root $\quad \mu_N = \{1, \omega, \dots, \omega^{N-1}\} = \langle z \in \mathbb{C} \mid z^N = 1 \rangle$

μ_N "$\cong$" $\mathbb{Z}_N$

4. $G \times G$: $\quad (g_1, g_2) \cdot (g_1', g_2') = (g_1 \cdot g_1', g_2 g_2')$

klein 4-group. $\mathbb{Z}_2 \times \mathbb{Z}_2$

$$\begin{cases} (1, 1) \\ (1, -1) \\ (-1, 1) \\ (-1, -1) \end{cases}$$

5. Abelian & non-abelian groups

6. $GL(n,k)$: invertible $n\times n$ over field $k=\mathbb{R},\mathbb{C}$

$$Z(G) = \{ z\in G \mid zg = gz,\ \forall g\in G \}$$

$$Z(GL(n,k)) = \{ A : A=\lambda \mathbb{1}_n,\ \lambda\in k^* \}$$

7. $SL(n,k) = \{ A\in GL \mid \det A = 1 \}$

$O(n,k) = \{ \quad AA^T = 1 \}$ $\quad \det A = \pm 1$

$SO(n,k) = \{ \quad \det A = 1 \}$

$U(n) := \{ A\in GL(n,\mathbb{C}) \mid AA^\dagger = 1 \}$ $\quad |\det A| = 1$

$SU(n) := \{ \quad \det A = 1 \}$

bilinear form.

$$O(p,q) = \{ A\in GL(p+q,\mathbb{R}) \mid A^T J_{p,q} A = J_{p,q} \}$$

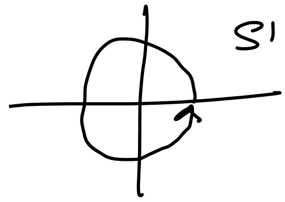
$$J_{pq} = \left(\begin{array}{c|c} -1_p & \\ \hline & 1_q \end{array}\right)$$

$O(1,d)$ $\quad d+1$ Lorentz

$$Sp(2n,k) = \{ A\in GL(2n,k) \mid A^T J A = J \}$$

$$J = \begin{pmatrix} 0 & 1_n \\ -1_n & 0 \end{pmatrix} \qquad \det A = 1$$

$SO(2)$ "$\simeq$" $U(1)$



S^1

$$SU(2) \to S^3$$

$$g = \begin{pmatrix} z & -w^* \\ w & z^* \end{pmatrix}$$

$$z = x_0 + i x_1$$

$$w = x_2 + i x_3$$

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

$SU(3)$

Example. $Sp(2n, k)$ and canonical transformations.

$q^i, p_i \quad (i=1, \dots n)$

$f(\vec{q}, \vec{p})$ & $g(\vec{q}, \vec{p})$. define Poisson braket

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

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

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

transformation of coord & momentum

$$\begin{pmatrix} Q^1 \\ Q^2 \\ \vdots \\ Q^n \\ P_1 \\ \vdots \\ P_n \end{pmatrix} = A \begin{pmatrix} q^1 \\ \vdots \\ q^n \\ p_1 \\ \vdots \\ p_n \end{pmatrix}$$

$$\Rightarrow \{Q^i, Q^j\} = \{P_i, P_j\} = 0$$

$$\{Q^i, P_j\} = \delta^i_j$$

$\Leftrightarrow \quad A \subset Sp(2n, \mathbb{R})$

$\leftarrow$

$\rightarrow$

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

Remarks

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

   X are the generators of G

   $|x| < \infty$, G "finitely generated"

2. Finitely generated group. can be presented by its generators & relations the generators satisfy.

$$G = \langle g_1 \cdots g_n \mid R_1, R_2 \cdots R_r \rangle$$

$$\to \quad g_i^m g_j^n = 1$$

3. 1 is usually $\notin X$

Examples: $\mathbb{Z}_n$ or μ_n: $\langle A \mid A^n = 1 \rangle$

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

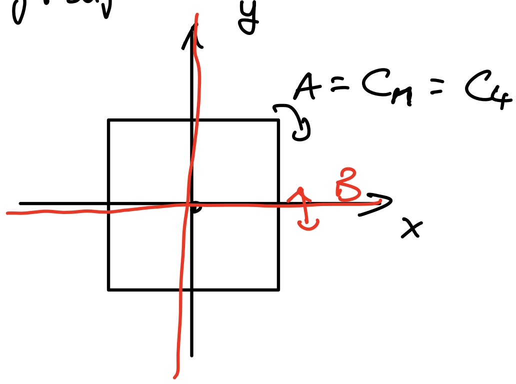
$A^m B^n$: $\boxed{1, A, B, AB}$. $AB^2 = A$ - -

$(1,1)$ $\quad (1,-1)$ $\quad (-1,1)$ $\quad (-1,-1)$

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

dihedral group $\qquad D_2$ "$\simeq$" $\mathbb{Z}_2 \otimes \mathbb{Z}_2$

D_4:



Example $\quad$ Quaternion group (1843)

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

$\underline{j}\,\underline{k} = -\underline{k}\,\underline{j} = \underline{i}$

$\underline{k}\,\underline{i} = -\underline{i}\,\underline{k} = \underline{j}$

$Q = \{\pm 1, \pm \underline{i}, \pm \underline{j}, \pm \underline{k}\} = \langle x, y \mid x^4 = 1,\ x^2 = y^2,\ y^{-1} x y = x^{-1} \rangle$

$= \langle \underline{i}\, \underline{j} \rangle$

$\underline{i}\,\underline{j} = \underline{k}$

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

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

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

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

$Q = \{\pm 1, \pm i\sigma^1, \pm i\sigma^2, \pm i\sigma^3\} \equiv \langle -i\sigma^1, -i\sigma^2 \rangle$

$\subset SU(2)$

<u>Example</u> Pauli group

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

$\equiv \langle \sigma^1, \sigma^2, \sigma^3 \rangle$ $\qquad$ $\underline{i} = \sigma^1\sigma^2\sigma^3$

important in Quantum info. & computation.

$X = \sigma^1$

$Z = \sigma^3$

$Y = \sigma^2$

$Y = i\sigma^2$

spin-½. (two-level) $|0\rangle, |1\rangle$

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

$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$ $\qquad$ $|\alpha|^2 + |\beta|^2 = \underline{1}$

$X = \sigma^1$

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

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

"bit-flip"

NOT-gate

$Z = \sigma^3$ $\quad Z|0\rangle = |0\rangle$ $\quad$ "phase-flip"

$Z|1\rangle = -|1\rangle$ $\quad \begin{pmatrix} 1 & \\ & -1 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = -\begin{pmatrix} 0 \\ 1 \end{pmatrix}$

Pauli group n-qubit

$$\underline{P_n} = (P_1)^n = \underbrace{P_1 \times P_1 \times \cdots P_1}_{n}$$

(Def). Let $\underline{S}$ be a subgroup of P_n. define

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

V_S is the vector space <u>stabilized by S</u>

S is the <u>stabilizer</u> of 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 subgroup of P_n)

$$\begin{cases} s_1 s_2|\varphi\rangle = s_1|\varphi\rangle = |\varphi\rangle \\ s_2 s_1|\varphi\rangle = s_2|\varphi\rangle = |\varphi\rangle \end{cases}$$

$s_1 s_2 = -s_2 s_1 \rightarrow |\varphi\rangle = -|\varphi\rangle \quad |\varphi\rangle = 0$

2. $-1 \notin S$ $\quad |\varphi\rangle = -|\varphi\rangle \Rightarrow |\varphi\rangle = 0$

Example : Stabilizer code

Quantum info. $\alpha|0\rangle + \beta|1\rangle \rightarrow \boxed{\text{noisy channel}} \rightarrow \begin{cases} \alpha|0\rangle + \beta|1\rangle \ ? \\ \alpha|1\rangle + \beta|0\rangle \ ? \end{cases}$

3-qubit code : $\alpha|000\rangle + \beta|111\rangle \rightarrow \boxed{} \rightarrow$

encode 1-qubit $|0\rangle$ $|1\rangle$ $\alpha|001\rangle + \beta|110\rangle$ $(p \ll 1)$

$\underbrace{|000\rangle}_{}$ SS $\underbrace{|111\rangle}_{}$ SS

Quantum error correction: $E = X$:

detectable error: $\exists s \in S$, s.t. E anticommute with s

$s|\varphi\rangle = |\varphi\rangle$

$s(E|\varphi\rangle) = -Es|\varphi\rangle = -E|\varphi\rangle$ $\quad E|\varphi\rangle \in V_S^{\perp}$

undecetable error:

$E \in N(S) = \{ g : gs = sg, \ \forall s \in S \}$ "normalizer group"

$S \leq N(S)$

3-qubit bit-flip code

$S \equiv \{ I, Z_1Z_2, Z_2Z_3, Z_1Z_3 \} \equiv \langle Z_1Z_2, Z_2Z_3 \rangle$

$V_S = \{ |000\rangle, |111\rangle \}$

$$\dim V_S = 2^1 = 2^{3-2}$$

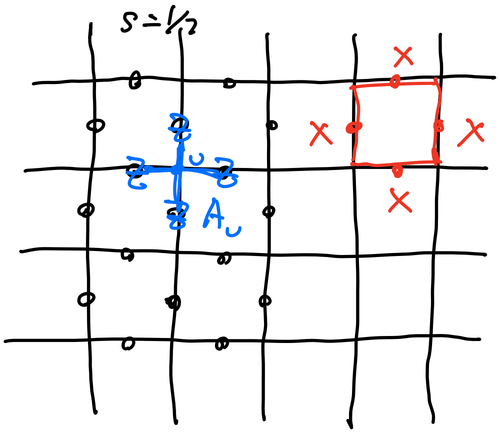
\# qubit

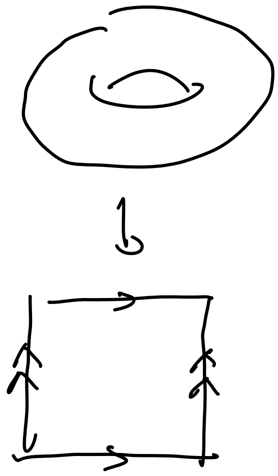
\# generator

Z_1Z_2	Z_2Z_3	Error
+1	+1	✓
+1	−1	3 flip
−1	+1	1 flip
−1	−1	2 flip

$\langle Z_1Z_2\rangle$

Example Toric code (Kitaev)

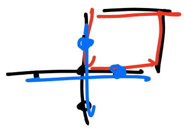




$$A_v = \prod_{j \in star(v)} Z_j \qquad B_p = \prod_{j \in plaquette} X_j$$

$$[A_v, A_{v'}] = 0 \qquad [B_p, B_{p'}] = 0$$

$$[A_v, B_p] = 0$$



$$H = -\sum_v A_v - \sum_p B_p$$

$A^2 = 1 \quad B^2 = 1$

$\Downarrow$

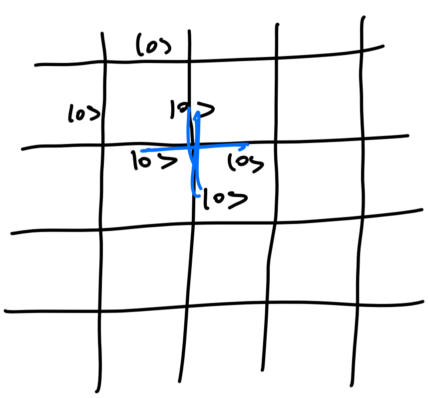
± 1

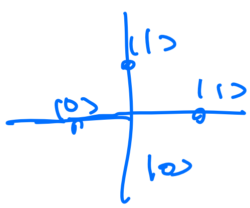
$$\boxed{\begin{aligned} A|\varphi\rangle &= |\varphi\rangle \\ B|\varphi\rangle &= |\varphi\rangle \end{aligned}}$$

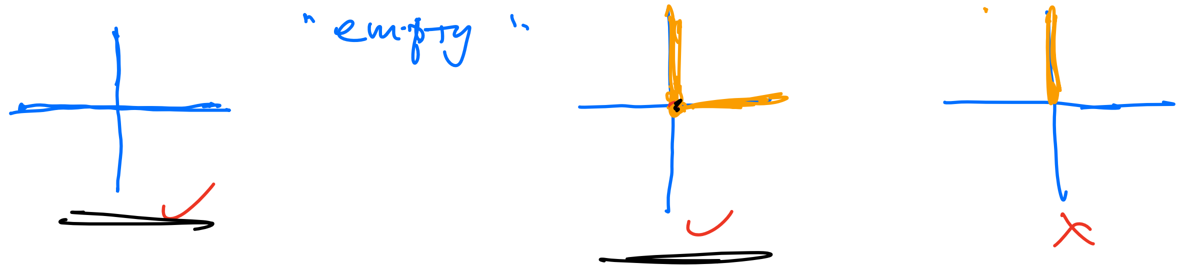
$A = \prod Z_j$

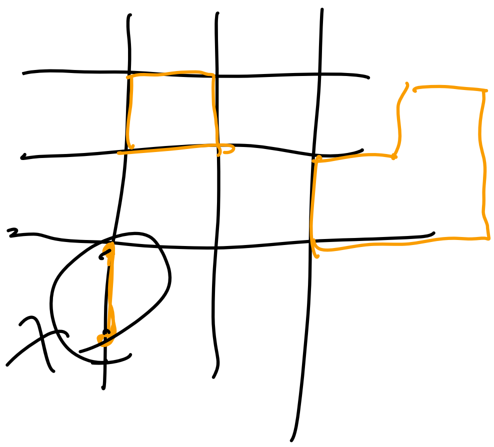
$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

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





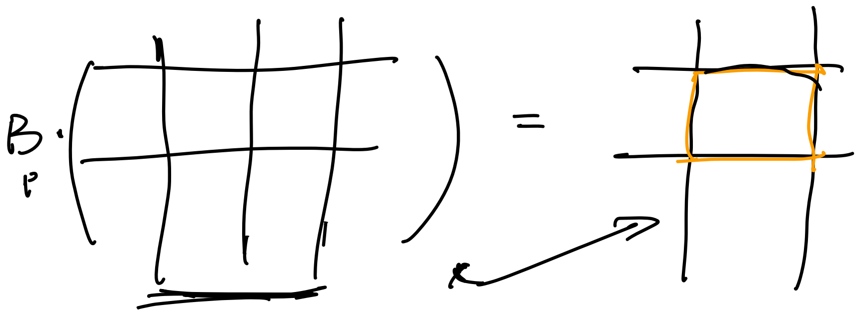




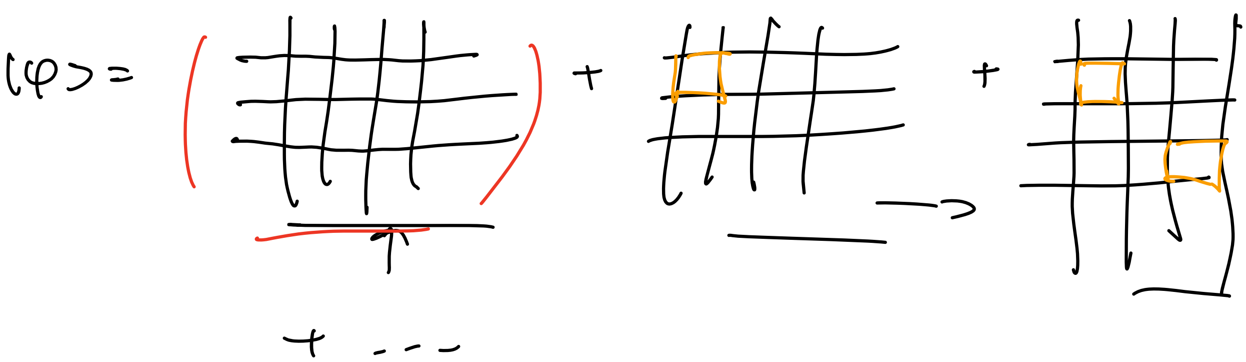
A : large degeneracy of closed loops

$B_p = \prod X \qquad X|0\rangle = |1\rangle$

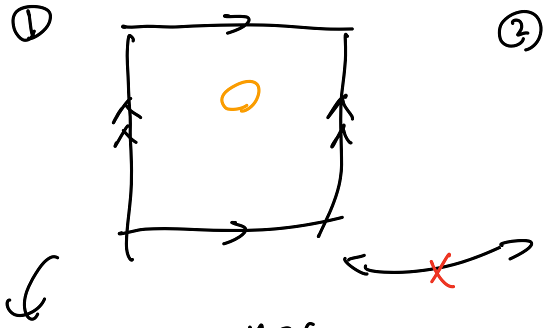
$\qquad\qquad\qquad X|1\rangle = |0\rangle$



$B_p |\varphi\rangle = |\varphi\rangle$

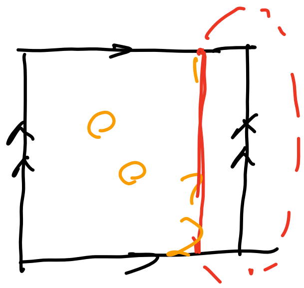


(equal weights superposition of all loop configurations)

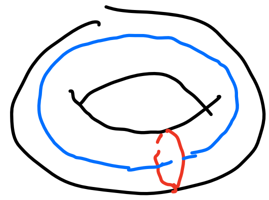
① 

$|00\rangle$

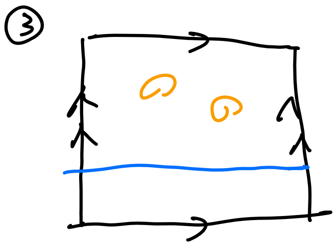
not connected by application of B_p's

② 

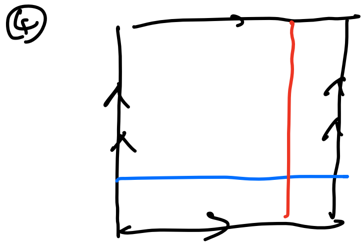
$|10\rangle$



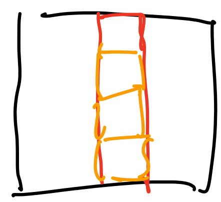
$Z_2 \times Z_2$

③ 

$|01\rangle$

④ 

$|11\rangle$

 $=$ ①

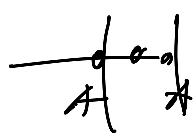
$\dim V \langle A_v, B_p \rangle = 4$ ✓

$$\dim = \frac{2^{2N}}{2^{2N-2}} = 2^2$$ ✓

$$\left\{ \begin{array}{ll} A|\varphi\rangle = \pm|\varphi\rangle & N \\ B|\varphi\rangle = \pm|\varphi\rangle & N \end{array} \right.$$

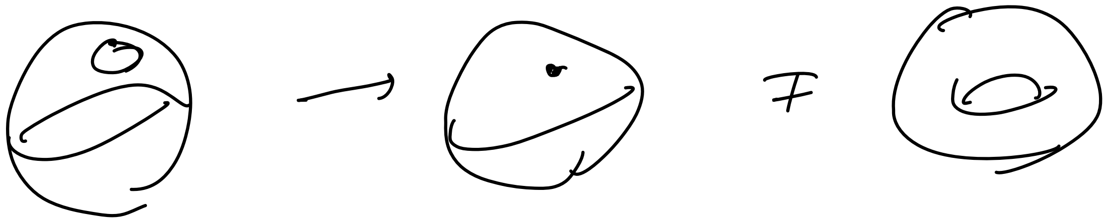
$A = \Pi Z$

$B = \Pi X$



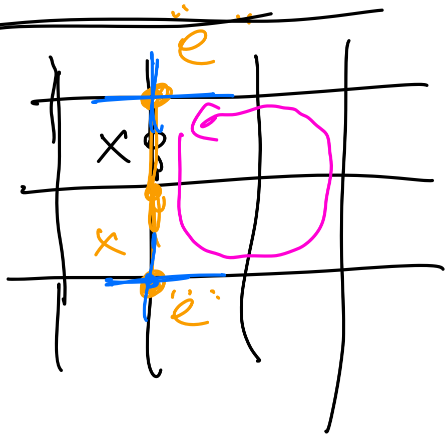
$\prod_v A_v = \prod_p B_p = 1$

$2N$ − two constraints



"topological order"

anyon excitations

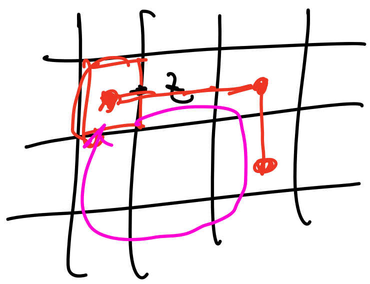


charge excitation

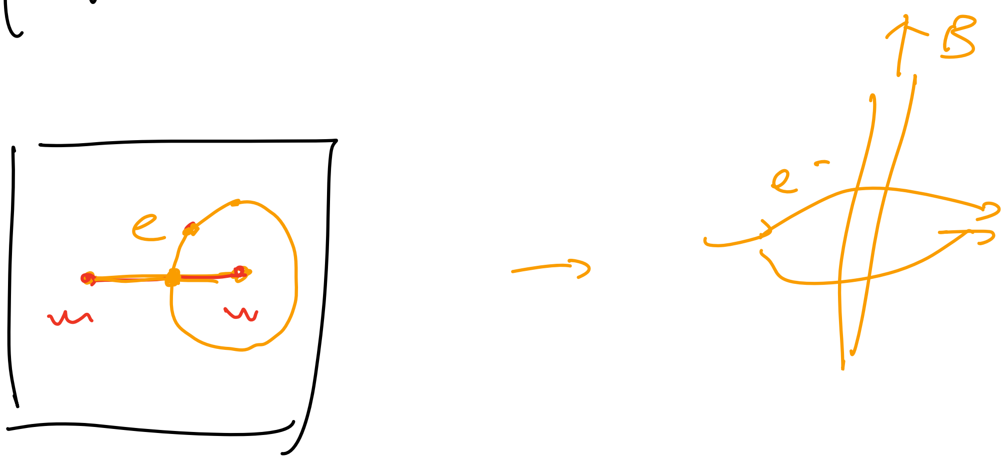
fractionalized excitations

(in pairs)

bosons



flux excitation



acquires a phase -1

due to $XZ = -ZX$