group, tensor, spinor

Joey Yu Hsu, MD

since 2024/05

Contents

1 coloring

1.1 single coloring

```
\def\zl{ {\color{blue} z_l} }
```

also can be put into “preamble”

$$0=\frac{\partial}{\partial z_l}\left(\|h(z_{l-1})\cdot w_l - z_l\| + \lambda\|h(z_l)\cdot w_{l+1} - z_{l+1}\|\right)$$

1.2 recolor = coloring with regular expression (= RegEx = re)

```
\usepackage{expl3,xparse}
\usepackage{xcolor}


\ExplSyntaxOn
\NewDocumentCommand{\recolor}{m}
{
    \tl_set:Nn \l_tmpa_tl { #1 }
    \regex_replace_all:nnN { 2 } { \c{ensuremath}{\c{color}{red}{2}} } \l_tmpa_tl
    \tl_use:N \l_tmpa_tl
}
\ExplSyntaxOff
```

$$c^2 = a^2 + b^2$$

Part I
group theory

2 basic definition

定義 2.1. group

$$\begin{array}{l} G \text{ is a group} \\ \Updownarrow \end{array}$$

$$G=(G,\cdot)=(G,\cdot_G)=\left\{ g \left| \begin{array}{lrl} g_1\cdot g_2 = g_1g_2\in G & \forall g_1,g_2\in G & (c)\ \cdot_G \text{ closure} \\ g_1(g_2g_3)=(g_1g_2)g_3=g_1g_2g_3 & \forall g_1,g_2,g_3\in G & (a)\ \cdot_G \text{ associativity} \\ e\cdot g=eg=g=ge=g\cdot e & \exists e=e_G\in G,\forall g\in G & (id)\text{ identity element} \\ \bar{g}\cdot g=\bar{g}g=e=g\bar{g}=g\cdot\bar{g} & \forall g\in G,\exists\bar{g}\in G & (in)\text{ inverse element} \end{array} \right. \right\}$$

定理 2.2.

$$\begin{array}{r} \forall g\in G \\ g\neq e\in G \end{array} \Rightarrow \forall \tilde{g}\in G\,[g\tilde{g}\neq\tilde{g}]$$

定理 2.3.

$$\begin{array}{r} \forall g_1,g_2\in G \\ g_1\neq g_2 \end{array} \Rightarrow \forall g\in G\,[g_1g\neq g_2g]$$

定理 2.4. *rearrangement theorem*

$$\forall g\in G\,[\{g\tilde{g}|\tilde{g}\in G\}=G]$$

Proof. proof idea $f = g(\overline{g}f) = gg^{-1}f = ef = f$

$$\forall g \in G, \exists \overline{g} \in G \left[\overline{g}g = e = g\overline{g} \right]$$

$$\Downarrow$$

$$\forall f \in G \left[f = ef \stackrel{e=g\overline{g}}{=} (g\overline{g})\, f \stackrel{(a)}{=} g(\overline{g}f) \right] \Rightarrow \quad \forall f \in G\, [f = g(\overline{g}f)] \stackrel{(c)\overline{g}f\in G}{\Rightarrow} f \in \{g\widetilde{g} | \widetilde{g} \in G\}$$

$$\Downarrow$$

$$\forall f \in G\, [f \in \{g\widetilde{g} | \widetilde{g} \in G\}]$$

$$\Downarrow$$

$$G \subseteq \{g\widetilde{g} | \widetilde{g} \in G\}$$

$$\{g\widetilde{g} | \forall \widetilde{g} \in G\} \subseteq G \because (c) \cdot_G \text{ closure}$$

$$\Downarrow$$

$$G = \{g\widetilde{g} | \widetilde{g} \in G\}$$

□

推論 2.5.

$$\begin{cases} \forall g \in G\, [g \in \{g\widetilde{g} | \widetilde{g} \in G\}] & (l)\ \textit{lossless} = \textit{complete} \\ \forall g_1, g_2 \in G = \{g\widetilde{g} | \widetilde{g} \in G\} \\ g_1 \neq g_2 \end{cases} \Rightarrow g_1\widetilde{g} \neq g_2\widetilde{g} \quad (r)\ \textit{repeatless} = \textit{rearrange}$$

定義 2.6. exponentiation or power

$$g^n = \overbrace{g \cdot_G g \cdot_G \cdots \cdot_G g}^{n} = \overbrace{g \cdot g \cdot \cdots \cdot g}^{n} = \overbrace{g \cdot \cdots \cdot g}^{n} = \overbrace{g \cdots g}^{n} \qquad n \in \mathbb{N}$$

$$g^{-n} = \overline{g}^n = \overbrace{\overline{g} \cdot_G \overline{g} \cdot_G \cdots \cdot_G \overline{g}}^{n} = \overbrace{\overline{g} \cdot \overline{g} \cdot \cdots \cdot \overline{g}}^{n} = \overbrace{\overline{g} \cdot \cdots \cdot \overline{g}}^{n} = \overbrace{\overline{g} \cdots \overline{g}}^{n} \qquad n \in \mathbb{N}$$

$$\overline{g}g = e = g\overline{g}$$

$$g^0 = g^n\overline{g}^n = \overline{g}^n g^n = \left(\overline{g}^{n-1}\overline{g}\right)\left(gg^{n-1}\right) = \overline{g}^{n-1}(\overline{g}g)\, g^{n-1} = \overline{g}^{n-1}(e)\, g^{n-1} = \cdots = e$$

$$g^0 = e$$

$$g^k = \begin{cases} g^k & k > 0 \\ e & k = 0 \\ \overline{g}^{|k|} = g^{-|k|} & k < 0 \end{cases} \qquad k \in \mathbb{Z}$$

定義 2.7. infinite group vs. finite group

$$\begin{array}{ccc} G \text{ is a group} & & G \text{ is a group} \\ \exists H \subsetneq G \left[|G| = |H| \right] & & \nexists H \subsetneq G \left[|G| = |H| \right] \\ \Updownarrow & \leftarrow \rightarrow & \Updownarrow \\ G \text{ is an infinite group} & & G \text{ is a finite group} \end{array}$$

定義 2.8. discrete group vs. Lie group

$$\begin{array}{ccc} G \text{ is a group} & & G \text{ is a group} \\ \exists H \subseteq \mathbb{Z} \left[|G| = |H| \right] & & \nexists H \subseteq \mathbb{Z} \left[|G| = |H| \right] \\ \Updownarrow & \leftarrow \rightarrow & \Updownarrow \\ G \text{ is a discrete group} & & G \text{ is a Lie group} \end{array}$$

定義 2.9. commutative group = Abelian group

$$\begin{array}{cc} G \text{ is a group} & A \text{ is a group} \\ \forall g_1, g_2 \in G\, [g_1 g_2 = g_2 g_1] & \forall a_1, a_2 \in A\, [a_1 a_2 = a_2 a_1] \\ \Updownarrow & \Updownarrow \\ G \text{ is a commutative group} & A \text{ is a commutative group} \\ \Updownarrow & \Updownarrow \\ G \text{ is an Abelian group} & A \text{ is an Abelian group} \end{array}$$

定義 2.10. trivial group

$$\{e\} = \{e_G\} = \left\{g^0\right\} \quad g \in G = (G, \cdot) = (G, \cdot_G) \text{ is a group}$$

3 finite group

3.1 cyclic group

定義 3.1. cyclic group

$$\begin{aligned} \mathbb{Z}_n = (\mathbb{Z}_n, +) = (\mathbb{Z}_n, +_{\mathbb{Z}_n}) &\overset{\text{def.}}{=} \{0, 1, 2, \cdots, n-1\} && n \in \mathbb{N} \\ &= \{0, 1, \cdots, n-1\} \qquad = \left\{\overbrace{0, 1, \cdots, n-1}^{n}\right\} \\ &= \{0, \cdots, n-1\} \qquad = \left\{\overbrace{0, \cdots, n-1}^{n}\right\} \end{aligned}$$

$$\forall g_1, g_2 \in \mathbb{Z}_n \begin{bmatrix} g_1 + g_2 = g_1 +_{\mathbb{Z}_n} g_2 \overset{\text{def.}}{=} (g_1 +_{\mathbb{Z}} g_2) \mod n & (g_1 +_{\mathbb{Z}_n} g_2) - (g_1 +_{\mathbb{Z}} g_2) = n \cdot_{\mathbb{Z}} k = nk \quad k \in \mathbb{Z} \\ = g_1 \% g_2 & \text{some programming language} \\ \equiv (g_1 +_{\mathbb{Z}} g_2) \mod n & (g_1 +_{\mathbb{Z}} g_2) \mod n < n \\ = r & \mod \text{ is integer modular arithmetic or modulus} \\ & g_1 +_{\mathbb{Z}} g_2 = nk + r \quad \mathbb{Z} \ni r < n \end{bmatrix}$$

$\mathbb{Z}_2$

$$\begin{aligned} \mathbb{Z}_2 = (\mathbb{Z}_2, +) = (\mathbb{Z}_2, +_{\mathbb{Z}_n}) &= \{0, 1\} && \mathbb{Z}_n = (\mathbb{Z}_n, +) = (\mathbb{Z}_n, +_{\mathbb{Z}_n}), 2 = n \in \mathbb{N} \\ 0 + 0 &= (0 \mod 2) = 0 \\ 0 + 1 &= (1 \mod 2) = 1 \\ 1 + 0 &= (1 \mod 2) = 1 \\ 1 + 1 &= (2 \mod 2) = 0 \end{aligned}$$

$+_{\mathbb{Z}_2}$	0	1
0	0	1
1	1	0

$\mathbb{Z}_3$

$$\mathbb{Z}_3 = (\mathbb{Z}_3, +) = (\mathbb{Z}_3, +_{\mathbb{Z}_n}) = \{0, 1, 2\} \qquad \mathbb{Z}_n = (\mathbb{Z}_n, +) = (\mathbb{Z}_n, +_{\mathbb{Z}_n}), 3 = n \in \mathbb{N}$$

$$\begin{matrix} +_{\mathbb{Z}_n} & 0 & 1 & 2 \\ 0 & (0 \mod 3) & (1 \mod 3) & (2 \mod 3) \\ 1 & (1 \mod 3) & (2 \mod 3) & (3 \mod 3) \\ 2 & (2 \mod 3) & (3 \mod 3) & (4 \mod 3) \end{matrix} \rightarrow \begin{matrix} +_{\mathbb{Z}_3} & 0 & 1 & 2 \\ 0 & 0 & 1 & 2 \\ 1 & 1 & 2 & 0 \\ 2 & 2 & 0 & 1 \end{matrix}$$

定理 3.2.

$$\forall n \in \mathbb{N} \begin{bmatrix} +_{\mathbb{Z}_n} \textit{ commutative} \Rightarrow & \mathbb{Z}_n \textit{ is an Abelian group} \\ & \Updownarrow \\ & \mathbb{Z}_n \textit{ is a commutative group} \end{bmatrix}$$

complex multiplication

定理 3.3.

$$\mathrm{e}^{\mathrm{i}\frac{2\pi}{n}k_1}\mathrm{e}^{\mathrm{i}\frac{2\pi}{n}k_2} = \mathrm{e}^{\mathrm{i}\frac{2\pi}{n}k_1} \cdot_{\mathbb{C}} \mathrm{e}^{\mathrm{i}\frac{2\pi}{n}k_2} = \mathrm{e}^{\mathrm{i}\frac{2\pi}{n}(k_1+k_2) \mod n} \qquad \begin{aligned} \forall k_1, k_2 \in \mathbb{Z} \\ |k_1|, |k_2| < n \in \mathbb{N} \end{aligned}$$

$\mathbb{Z}_n$

$$\begin{aligned}
\mathbb{Z}_n = (\mathbb{Z}_n, +) &= (\mathbb{Z}_n, +_{\mathbb{Z}_n}) &&= \{0, 1, 2, \cdots, n-1\} && n \in \mathbb{N} \\
\mathbb{Z}_n = (\mathbb{Z}_n, \cdot) &= (\mathbb{Z}_n, \cdot_{\mathbb{C}}) &&= \left\{ \mathrm{e}^{\mathrm{i}\frac{2\pi}{n}0}, \mathrm{e}^{\mathrm{i}\frac{2\pi}{n}1}, \mathrm{e}^{\mathrm{i}\frac{2\pi}{n}2}, \cdots, \mathrm{e}^{\mathrm{i}\frac{2\pi}{n}(n-1)} \right\} && \mathrm{e}^{\mathrm{i}\frac{2\pi}{n}(nk)} = 1 \quad \forall k \in \mathbb{Z} \\
\mathbb{Z}_n = (\mathbb{Z}_n, \cdot) &= (\mathbb{Z}_n, \cdot_G) &&= \{g^0, g^1, g^2, \cdots, g^{n-1}\} \\
& &&= \{e, g, g^2, \cdots, g^{n-1}\} && g^n = e \\
& &&= \left\{ g^k \middle| \begin{array}{l} g^n = g^0 = e = e_G \in G \\ k \in \mathbb{Z} \end{array} \right\} && g \text{ is a generating element} \\
& &&= \langle g \rangle && \text{or a generator of the group} \\
\mathbb{Z}_n & &&\overset{\text{e.g.}}{=} \left\langle \mathrm{e}^{\mathrm{i}\frac{2\pi}{n}} \right\rangle
\end{aligned}$$

$\mathbb{Z}_2$

$$\begin{aligned}
\mathbb{Z}_2 = (\mathbb{Z}_2, +) &= (\mathbb{Z}_2, +_{\mathbb{Z}_n}) &&= \{0, 2-1\} && = \{0, 1\} \\
\mathbb{Z}_2 = (\mathbb{Z}_2, \cdot) &= (\mathbb{Z}_2, \cdot_{\mathbb{C}}) &&= \left\{ \mathrm{e}^{\mathrm{i}\frac{2\pi}{2}0}, \mathrm{e}^{\mathrm{i}\frac{2\pi}{2}(2-1)} \right\} = \{\mathrm{e}^{\mathrm{i}0}, \mathrm{e}^{\mathrm{i}\pi}\} && = \{1, -1\}
\end{aligned}$$

$\mathbb{Z}_3$

$$\begin{aligned}
\mathbb{Z}_3 = (\mathbb{Z}_3, +) &= (\mathbb{Z}_3, +_{\mathbb{Z}_n}) &&= \{0, 1, 3-1\} && = \{0, 1, 2\} \\
\mathbb{Z}_3 = (\mathbb{Z}_3, \cdot) &= (\mathbb{Z}_3, \cdot_{\mathbb{C}}) &&= \left\{ \mathrm{e}^{\mathrm{i}\frac{2\pi}{3}0}, \mathrm{e}^{\mathrm{i}\frac{2\pi}{3}1}, \mathrm{e}^{\mathrm{i}\frac{2\pi}{3}(3-1)} \right\} = \left\{ \mathrm{e}^{\mathrm{i}0}, \mathrm{e}^{\mathrm{i}\frac{2\pi}{3}}, \mathrm{e}^{\mathrm{i}\frac{4\pi}{3}} \right\} && = \left\{ 1, \frac{-1}{2} + \mathrm{i}\frac{\sqrt{3}}{2}, \frac{-1}{2} - \mathrm{i}\frac{\sqrt{3}}{2} \right\}
\end{aligned}$$

$\mathbb{Z}_4$

$$\begin{aligned}
\mathbb{Z}_4 = (\mathbb{Z}_4, +) &= (\mathbb{Z}_4, +_{\mathbb{Z}_n}) &&= \{0, 1, 2, 4-1\} && = \{0, 1, 2, 3\} \\
\mathbb{Z}_4 = (\mathbb{Z}_4, \cdot) &= (\mathbb{Z}_4, \cdot_{\mathbb{C}}) &&= \left\{ \mathrm{e}^{\mathrm{i}\frac{2\pi}{4}0}, \mathrm{e}^{\mathrm{i}\frac{2\pi}{4}1}, \mathrm{e}^{\mathrm{i}\frac{2\pi}{4}2}, \mathrm{e}^{\mathrm{i}\frac{2\pi}{4}(4-1)} \right\} = \left\{ \mathrm{e}^{\mathrm{i}0}, \mathrm{e}^{\mathrm{i}\frac{\pi}{2}}, \mathrm{e}^{\mathrm{i}\pi}, \mathrm{e}^{\mathrm{i}\frac{3\pi}{2}} \right\} && = \{1, \mathrm{i}, -1, -\mathrm{i}\}
\end{aligned}$$

3.2 permutation group or symmetric group

定義 3.4. permutation

$$N = \{1, 2, \cdots, n\} = \{1, \cdots, n\} = \left\{ \overbrace{1, \cdots, n}^{n} \right\} \qquad \text{finite set by } n \in \mathbb{N}$$

$$\begin{aligned}
\sigma \in N^N \Leftrightarrow \sigma : N \to N \Leftrightarrow N \xrightarrow{\sigma} N & \qquad \text{autofunction over } N = \mathbb{N}_{\leq n \in \mathbb{N}} = \mathbb{N}_{\leq n} \\
\sigma(N) = N & \qquad \sigma(N) \text{ range equals codomain } N \Leftrightarrow \sigma \text{ is a permutation}
\end{aligned}$$

定義 3.5. permutation group = symmetric group

$$S_n = (S_n, \cdot_{S_n}) = (S_n, \circ) = \left\{ \sigma \middle| \begin{array}{c} n \in \mathbb{N} \\ N = \left\{ \overbrace{1, \cdots, n}^{n} \right\} \\ \sigma \in N^N \\ \sigma(N) = N \end{array} \right\} = \left\{ \sigma \middle| \begin{array}{c} n \in \mathbb{N} \\ N = \{1, \cdots, n\} \\ \sigma : N \to N \\ \forall \sigma_i, \sigma_j \in S_n \left[\sigma_i \sigma_j = \sigma_i \circ \sigma_j \right] \\ \forall m_1, m_2 \in N \left[m_1 \neq m_2 \Leftrightarrow \sigma(m_1) \neq \sigma(m_2) \right] \end{array} \right\}$$

S_1

$$\begin{aligned}
\sigma(1) &= 1 \\
S_1 &= \{\sigma\} = \{e\} = \{e_{S_1}\} = \{\mathrm{id}\} \\
\sigma\sigma(1) &= \sigma \cdot_{S_n} \sigma(1) = \sigma \circ \sigma(1) = \sigma(\sigma(1)) = \sigma(1) = 1 = \sigma(1) \\
\sigma\sigma(1) &= \sigma(1) \\
\sigma\sigma &= \sigma = \sigma \cdot_{S_n} \sigma = \sigma \circ \sigma
\end{aligned}$$

$$\begin{aligned}
S_1 &= \left\{ \begin{array}{ccc} & \sigma & \\ 1 & \to & 1 = \sigma(1) \end{array} \right\} = \left\{ \begin{array}{ccc} & \sigma_1 & \\ 1 & \to & 1 = \sigma_1(1) \end{array} \right\} \\
&= \left\{ \begin{array}{c} 1 \\ \downarrow \\ 1 \end{array} \right\} = \left\{ \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\}
\end{aligned}$$

$$\begin{array}{cc} \cdot_{S_n} & \sigma \\ \sigma & \sigma \end{array} \leftrightarrow \begin{array}{cc} \circ & \sigma_1 \\ \sigma_1 & \sigma_1 \end{array} \leftrightarrow \begin{array}{cc} \circ & \sigma_1 \\ \sigma_1 & e \end{array} \leftrightarrow \begin{array}{cc} \cdot_{S_n} & \sigma_1 \\ \sigma_1 & e_{S_1} \end{array} \leftrightarrow \begin{array}{cc} \circ & e \\ e & e \end{array}$$

S_2

$$\begin{array}{rccccccccccccc} S_2 & =\{ & & \sigma_1 & & & , & & \sigma_2 & & & \}=\{ & e & , & \sigma_2 & \} \\ & & 1 & \to & 1 & =\sigma_1(1) & & 1 & \to & 2 & =\sigma_2(1) & & \| & & & \\ & & 2 & \to & 2 & =\sigma_1(2) & & 2 & \to & 1 & =\sigma_2(2) & & e_{S_2} & & & \\ & =\{ & \sigma_1 & \begin{array}{c}1\\ \downarrow\\ 1\end{array} & \begin{array}{c}2\\ \downarrow\\ 2\end{array} & & , & \sigma_2 & \begin{array}{c}1\\ \downarrow\\ 2\end{array} & \begin{array}{c}2\\ \downarrow\\ 1\end{array} & & \}=\{ & \begin{pmatrix}1 & 2\\ 1 & 2\end{pmatrix} & , & \begin{pmatrix}1 & 2\\ 2 & 1\end{pmatrix} & \} \end{array}$$

$$\begin{aligned}
\sigma_1\sigma_1(1) =& \sigma_1 \cdot_{S_n} \sigma_1(1) = \sigma_1 \circ \sigma_1(1) = \sigma_1(\sigma_1(1)) = \sigma_1(1) = 1 = \sigma_1(1) \\
\sigma_1\sigma_1(2) =& \sigma_1 \cdot_{S_n} \sigma_1(2) = \sigma_1 \circ \sigma_1(2) = \sigma_1(\sigma_1(2)) = \sigma_1(2) = 2 = \sigma_1(2) \\
\sigma_1\sigma_1 =& \sigma_1 \\
\sigma_2\sigma_1(1) =& \sigma_2 \cdot_{S_n} \sigma_1(1) = \sigma_2 \circ \sigma_1(1) = \sigma_2(\sigma_1(1)) = \sigma_2(1) = 2 = \sigma_2(1) \\
\sigma_2\sigma_1(2) =& \sigma_2 \cdot_{S_n} \sigma_1(2) = \sigma_2 \circ \sigma_1(2) = \sigma_2(\sigma_1(2)) = \sigma_2(2) = 1 = \sigma_2(2) \\
\sigma_2\sigma_1 =& \sigma_2 \\
\sigma_1\sigma_2(1) =& \sigma_1 \cdot_{S_n} \sigma_2(1) = \sigma_1 \circ \sigma_2(1) = \sigma_1(\sigma_2(1)) = \sigma_1(2) = 2 = \sigma_2(1) \\
\sigma_1\sigma_2(2) =& \sigma_1 \cdot_{S_n} \sigma_2(2) = \sigma_1 \circ \sigma_2(2) = \sigma_1(\sigma_2(2)) = \sigma_1(1) = 1 = \sigma_2(2) \\
\sigma_1\sigma_2 =& \sigma_2 \\
\sigma_2\sigma_2(1) =& \sigma_2 \cdot_{S_n} \sigma_2(1) = \sigma_2 \circ \sigma_2(1) = \sigma_2(\sigma_2(1)) = \sigma_2(2) = 1 = \sigma_1(1) \\
\sigma_2\sigma_2(2) =& \sigma_2 \cdot_{S_n} \sigma_2(2) = \sigma_2 \circ \sigma_2(2) = \sigma_2(\sigma_2(2)) = \sigma_2(1) = 2 = \sigma_1(2) \\
\sigma_2\sigma_2 =& \sigma_1
\end{aligned}$$

$$\begin{aligned}
\sigma_1\sigma_i = \sigma_i\sigma_1 = \sigma_i \Rightarrow& \sigma_1 = e = e_{S_2} = \overline{\sigma}_1 = \sigma_1^{-1} \\
\sigma_2\sigma_2 = \sigma_1 \Rightarrow& \sigma_2 = \overline{\sigma}_2 = \sigma_2^{-1}
\end{aligned}$$

$$\begin{array}{ccc} \cdot_{S_n} & \sigma_1 & \sigma_2 \\ \sigma_1 & \sigma_1 & \sigma_2 \\ \sigma_2 & \sigma_2 & \sigma_1 \end{array} \leftrightarrow \begin{array}{ccc} \circ & \sigma_1 & \sigma_2 \\ \sigma_1 & e & \sigma_2 \\ \sigma_2 & \sigma_2 & e \end{array} \leftrightarrow \begin{array}{ccc} \circ & e & \sigma_2 \\ e & e & \sigma_2 \\ \sigma_2 & \sigma_2 & e \end{array}$$

$S_2 = \mathbb{Z}_2$

$$\begin{aligned}
\mathbb{Z}_2 = (\mathbb{Z}_2, +) \quad &= (\mathbb{Z}_2, +_{\mathbb{Z}_n}) &&= \{0, 2-1\} &&= \{0, 1\} \\
\mathbb{Z}_2 = (\mathbb{Z}_2, \cdot) \quad &= (\mathbb{Z}_2, \cdot_{\mathbb{C}}) &&= \left\{ e^{i\frac{2\pi}{2}0}, e^{i\frac{2\pi}{2}(2-1)} \right\} = \{e^{i0}, e^{i\pi}\} &&= \{1, -1\} \\
S_2 = \mathbb{Z}_2 = (S_2, \cdot_{S_n}) \quad &= (S_2, \circ) &&= \{\sigma_1, \sigma_2\} = \{e_{S_2}, \sigma_2\} &&= \{e, \sigma_2\}
\end{aligned}$$

$|S_n| = n!$

$$|S_n| = \mathrm{P}_n^n = n! = n \cdot (n-1) \cdot \cdots \cdot 2 \cdot 1 = \overbrace{n(n-1)\cdots 1}^{n} = n(n-1)\cdots 1$$

$$
\begin{aligned}
S_n &= (S_n, \cdot_{S_n}) = (S_n, \circ) \\
&= \left\{ \sigma \,\middle|\, \begin{array}{l} n \in \mathbb{N} \\ N = \left\{ \overbrace{1, \cdots, n}^{n} \right\} \\ \sigma \in N^N \\ \sigma(N) = N \end{array} \right\} = \left\{ \sigma \,\middle|\, \begin{array}{c} n \in \mathbb{N} \\ N = \{1, \cdots, n\} \\ \sigma : N \to N \\ \forall \sigma_i, \sigma_j \in S_n \left[\sigma_i \sigma_j = \sigma_i \circ \sigma_j\right] \\ \forall m_1, m_2 \in N \left[m_1 \neq m_2 \Leftrightarrow \sigma(m_1) \neq \sigma(m_2) \right] \end{array} \right\} \\
&\underset{I}{=} \left\{ \sigma \,\middle|\, \sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix} = \begin{pmatrix} \overbrace{1 \quad \cdots \quad n}^{n} \\ \sigma(1) \quad \cdots \quad \sigma(n) \end{pmatrix} = \begin{pmatrix} 1 & \cdots & n \\ \sigma(1) & \cdots & \sigma(n) \end{pmatrix} \right\} && \text{two-line notation} \\
&= \left\{ \sigma \,\middle|\, \sigma = \sigma(1)\sigma(2)\cdots\sigma(n) = \overbrace{\sigma(1)\sigma(2)\cdots\sigma(n)}^{n} = \sigma(1)\cdots\sigma(n) = [\sigma(1)\cdots\sigma(n)] \right\} && \text{one-line notation} \\
&= \left\{ \sigma \,\middle|\, \sigma = c_1 c_2 \cdots c_{n_\sigma} = \overbrace{c_1 c_2 \cdots c_{n_\sigma}}^{n_\sigma} = c_1 \cdots c_{n_\sigma} = \overbrace{\underbrace{c_{11} c_{12} \cdots c_{1 n_1}}_{c_1} \cdots \underbrace{c_{n_\sigma 1} c_{n_\sigma 2} \cdots c_{n_\sigma n_{n_\sigma}}}_{c_{n_\sigma}}}^{n_\sigma} \right\} && \text{cycle notation} \\
&= \left\{ \sigma \,\middle|\, \sigma = s_1 s_2 \cdots s_{N_\sigma} = \overbrace{s_1 s_2 \cdots s_{N_\sigma}}^{N_\sigma} = s_1 \cdots s_{N_\sigma} = \overbrace{\underbrace{(s_{11} s_{12})}_{s_1} \cdots \underbrace{(s_{N_\sigma 1} s_{N_\sigma 2})}_{s_{N_\sigma}}}^{N_\sigma} \right\} && \text{swap notation}
\end{aligned}
$$

two-line notation

$$
\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix} = \begin{pmatrix} 2 & 1 & \cdots & n \\ \sigma(2) & \sigma(1) & \cdots & \sigma(n) \end{pmatrix}, \cdots
$$

定義 3.6. S_3

$$
\begin{array}{lccccccll}
S_3 = \{ & \sigma_1, & \sigma_2, & \sigma_3, & \sigma_4, & \sigma_5, & \sigma_6 & \} & \\
\quad = \{ & \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, & \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, & \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, & \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, & \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, & \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} & \} & \text{two-line notation} \\
\quad = \{ & [123], & [231], & [312], & [213], & [132], & [321] & \} & \text{one-line notation} \\
\quad = \{ & 123, & 231, & 312, & 213, & 132, & 321 & \} & \text{one-line notation, simplified} \\
\quad = \{ & (1)(2)(3), & (123), & (132), & (12)(3), & (1)(23), & (31)(2) & \} & \text{cycle notation} \\
\quad = \{ & (), & (123), & (132), & (12), & (23), & (31) & \} & \text{cycle notation, simplified}
\end{array}
$$

$$
\begin{array}{lll}
\sigma_6 \sigma_3 & & = \sigma_6 \circ \sigma_3 \\
= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} & & = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \\
\qquad \| & & \\
= \begin{pmatrix} 3 & 1 & 2 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} & & \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 3 & 1 & 2 \\ 1 & 3 & 2 \end{pmatrix} \\
\quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} & & \\
= \begin{pmatrix} 3 & 1 & 2 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} & & = \sigma_5
\end{array}
$$

$\cdot_{S_n}$	[123]	[231]	[312]	[213]	[132]	[321]
[123]	[123]	[231]	[312]	[213]	[132]	[321]
[231]	[231]					
[312]	[312]					
[213]	[213]					
[132]	[132]					
[321]	[321]					

$\leftrightarrow$

$\circ$	e	[231]	[312]	[213]	[132]	[321]
e	e	[231]	[312]	[213]	[132]	[321]
[231]	[231]					
[312]	[312]					
[213]	[213]					
[132]	[132]					
[321]	[321]					

cycle notation= cyclic notation

$$\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}=\begin{pmatrix}1&2&3\\\downarrow&\nearrow&\nwarrow\!\downarrow\\3&1&2\end{pmatrix}=(1\to3\to2\to1)=(1321)=(132)$$

$$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}=\begin{pmatrix}1&2&3\\\downarrow\!\nearrow&\downarrow\!\nearrow&\downarrow\\2&3&1\end{pmatrix}=(1\to2\to3\to1)=(1231)=(123)$$

$$\begin{aligned}
\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}&=(1\to1)(2\to2)(3\to3)=(11)(22)(33) &&=(1)(2)(3)\\
\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}&=(1\to2\to3\to1)=(1231) &&=(123)=(231)=(312)\\
\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}&=(1\to3\to2\to1)=(1321) &&=(132)=(321)=(213)\\
\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}&=(1\to2\to1)(3\to3)=(121)(33) &&=(12)(3)=(21)(3)=(3)(21)=(3)(12)\\
\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}&=(1\to1)(2\to3\to2)=(11)(232) &&=(1)(23)=(1)(32)=(32)(1)=(23)(1)\\
\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}&=(1\to3\to1)(2\to2)=(131)(22) &&=(13)(2)=(31)(2)=(2)(31)=(2)(31)
\end{aligned}$$

$$\begin{aligned}
(123)(321)&=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\\
&\qquad\quad\|\\
&=\begin{pmatrix}3&1&2\\1&2&3\end{pmatrix}\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} \qquad \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}=\begin{pmatrix}3&1&2\\1&2&3\end{pmatrix}\\
&=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\\
&\begin{pmatrix}3&1&2\\1&2&3\end{pmatrix}=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}=e \qquad =e_{S_3}\\
(123)(321)&=e
\end{aligned}$$

$$(321)^{-1}=\overline{(321)}=(123) \qquad (123)^{-1}=\overline{(123)}=(321)$$

$$\begin{aligned}
(321)(123)&=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\\
&\qquad\quad\|\\
&=\begin{pmatrix}2&3&1\\1&2&3\end{pmatrix}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} \qquad \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}=\begin{pmatrix}2&3&1\\1&2&3\end{pmatrix}\\
&=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\\
&\begin{pmatrix}2&3&1\\1&2&3\end{pmatrix}=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}=e \qquad =e_{S_3}
\end{aligned}$$

$$\begin{aligned}
\sigma&=c_1c_2\cdots c_{n_\sigma}=\overbrace{c_1c_2\cdots c_{n_\sigma}}^{n_\sigma}=c_1\cdots c_{n_\sigma}=\overbrace{c_1\cdots c_{n_\sigma}}^{n_\sigma} \qquad c_i\cap c_j=\emptyset\\
&=\underbrace{c_{11}c_{12}\cdots c_{1n_1}}_{c_1}\underbrace{c_{21}c_{22}\cdots c_{2n_2}}_{c_2}\cdots\underbrace{c_{n_\sigma1}c_{n_\sigma2}\cdots c_{n_\sigma n_{n_\sigma}}}_{c_{n_\sigma}} \qquad c_{ij_1}\cap c_{ij_2}=\emptyset\\
&=\underbrace{c_{11}c_{12}\cdots c_{1n_1}}_{c_1}\cdots\underbrace{c_{n_\sigma1}c_{n_\sigma2}\cdots c_{n_\sigma n_{n_\sigma}}}_{c_{n_\sigma}}\\
&=\overbrace{\underbrace{c_{11}c_{12}\cdots c_{1n_1}}_{c_1}\cdots\underbrace{c_{n_\sigma1}c_{n_\sigma2}\cdots c_{n_\sigma n_{n_\sigma}}}_{c_{n_\sigma}}}^{n_\sigma}
\end{aligned}$$

$$\sum_{i=1}^{n_\sigma}n_i=n \qquad \forall n\in\mathbb{N},\forall\sigma\in S_n$$

$(ab)(bcd) = (abcd) \quad (a-b)(b-c)(c-d)(d-a) \neq 0$

Proof.

$$
\begin{aligned}
(ab)(bcd) &= \begin{pmatrix} a & b \\ b & a \end{pmatrix} \begin{pmatrix} b & c & d \\ c & d & b \end{pmatrix} \\
&= \begin{pmatrix} a & b \\ b & a \end{pmatrix} \begin{pmatrix} a & b & c & d \\ a & c & d & b \end{pmatrix} && \begin{pmatrix} b & c & d \\ c & d & b \end{pmatrix} = \begin{pmatrix} a & b & c & d \\ a & c & d & b \end{pmatrix} \\
&= \begin{pmatrix} a & b \\ b & a \end{pmatrix} \begin{pmatrix} a & d & b & c \\ a & b & c & d \end{pmatrix} && \begin{pmatrix} a & b & c & d \\ a & c & d & b \end{pmatrix} = \begin{pmatrix} a & d & b & c \\ a & b & c & d \end{pmatrix} \\
&\begin{pmatrix} a & d & b & c \\ a & b & c & d \end{pmatrix} \\
&= \begin{pmatrix} a & b \\ b & a \end{pmatrix} = \begin{pmatrix} a & d & b & c \\ b & a & c & d \end{pmatrix} = \begin{pmatrix} a & b & c & d \\ b & c & d & a \end{pmatrix} && = (abcd)
\end{aligned}
$$

□

swap

$$
\begin{aligned}
(ab)(bc)(ca) &= \begin{pmatrix} a & b \\ b & a \end{pmatrix} \begin{pmatrix} b & c \\ c & b \end{pmatrix} \begin{pmatrix} c & a \\ a & c \end{pmatrix} \\
&= \begin{pmatrix} c & a & b \\ c & b & a \end{pmatrix} \begin{pmatrix} b & a & c \\ c & a & b \end{pmatrix} \begin{pmatrix} b & c & a \\ b & a & c \end{pmatrix} \\
&\begin{pmatrix} b & c & a \\ b & a & c \end{pmatrix} \\
&\begin{pmatrix} b & a & c \\ c & a & b \end{pmatrix} \\
&= \begin{pmatrix} c & a & b \\ c & b & a \end{pmatrix} = \begin{pmatrix} b & c & a \\ c & b & a \end{pmatrix} = \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix} = (bc)
\end{aligned}
$$

$$
\begin{aligned}
(ab)(bc) &= \begin{pmatrix} a & b \\ b & a \end{pmatrix} \begin{pmatrix} b & c \\ c & b \end{pmatrix} \\
&= \begin{pmatrix} c & a & b \\ c & b & a \end{pmatrix} \begin{pmatrix} b & a & c \\ c & a & b \end{pmatrix} \\
&\begin{pmatrix} b & a & c \\ c & a & b \end{pmatrix} \\
&= \begin{pmatrix} c & a & b \\ c & b & a \end{pmatrix} = \begin{pmatrix} b & a & c \\ c & b & a \end{pmatrix} = \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix} = (abc)
\end{aligned}
$$

$$
\begin{aligned}
\sigma =& s_1 s_2 \cdots s_{N_\sigma} = \overbrace{s_1 s_2 \cdots s_{N_\sigma}}^{N_\sigma} = s_1 \cdots s_{N_\sigma} = \overbrace{s_1 \cdots s_{N_\sigma}}^{N_\sigma} \quad s_i \cap s_{i+1} = \{s_{(i)2}\} \\
=& \underbrace{(s_{11} s_{12})}_{s_1} \underbrace{(s_{21} s_{22})}_{s_2} \cdots \underbrace{(s_{N_\sigma 1} s_{N_\sigma 2})}_{s_{N_\sigma}} \quad s_{(i)2} = s_{(i+1)1} \\
=& \underbrace{(s_{11} s_{12})}_{s_1} \cdots \underbrace{(s_{N_\sigma 1} s_{N_\sigma 2})}_{s_{N_\sigma}} \\
=& \overbrace{\underbrace{(s_{11} s_{12})}_{s_1} \cdots \underbrace{(s_{N_\sigma 1} s_{N_\sigma 2})}_{s_{N_\sigma}}}^{N_\sigma}
\end{aligned}
$$

$$
\sigma \begin{cases} \text{is an even permutation} & N_\sigma \in 2\mathbb{N} - 2 \\ \text{is an odd permutation} & N_\sigma \in 2\mathbb{N} - 1 \end{cases} \Leftrightarrow \sigma \begin{cases} \text{even} & N_\sigma \in 2\mathbb{Z}_{\geq 0} \\ \text{odd} & N_\sigma \in 2\mathbb{N} - 1 \end{cases} \quad \forall \sigma \in S_n
$$

定義 3.7. alternating group

$$
A_n = \left\{ \sigma \,\middle|\, \begin{matrix} \sigma \in S_n \\ N_\sigma \in 2\mathbb{Z}_{\geq 0} \end{matrix} \right\}
$$

3.3 dihedral group

D_3

$$
\begin{array}{lclclclclclcl}
1 & : & \langle \cos 0, \sin 0 \rangle & = & \left\langle \cos \frac{2\pi}{3}0, \sin \frac{2\pi}{3}0 \right\rangle & = & \langle 1, 0 \rangle & = & \begin{bmatrix} 1 \\ 0 \end{bmatrix} & : & e^{i\frac{2\pi}{3}0} & = & 1 + i0 \\
2 & : & \left\langle \cos \frac{2\pi}{3}, \sin \frac{2\pi}{3} \right\rangle & = & \left\langle \cos \frac{2\pi}{3}1, \sin \frac{2\pi}{3}1 \right\rangle & = & \left\langle \frac{-1}{2}, \frac{\sqrt{3}}{2} \right\rangle & = & \begin{bmatrix} \frac{-1}{2} \\ \frac{\sqrt{3}}{2} \end{bmatrix} & : & e^{i\frac{2\pi}{3}1} & = & \frac{-1}{2} + i\frac{\sqrt{3}}{2} \\
3 & : & \left\langle \cos \frac{4\pi}{3}, \sin \frac{4\pi}{3} \right\rangle & = & \left\langle \cos \frac{2\pi}{3}2, \sin \frac{2\pi}{3}2 \right\rangle & = & \left\langle \frac{-1}{2}, \frac{-\sqrt{3}}{2} \right\rangle & = & \begin{bmatrix} \frac{-1}{2} \\ \frac{-\sqrt{3}}{2} \end{bmatrix} & : & e^{i\frac{2\pi}{3}2} & = & \frac{-1}{2} + i\frac{-\sqrt{3}}{2}
\end{array}
$$

$$
() = (1)\,(2)\,(3) \quad : \begin{cases}
\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} & (1) \\
\begin{bmatrix} \frac{-1}{2} \\ \frac{\sqrt{3}}{2} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} \frac{-1}{2} \\ \frac{\sqrt{3}}{2} \end{bmatrix} & (2) \\
\begin{bmatrix} \frac{-1}{2} \\ \frac{-\sqrt{3}}{2} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} \frac{-1}{2} \\ \frac{-\sqrt{3}}{2} \end{bmatrix} & (3)
\end{cases}
\qquad
\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} \cos \frac{2\pi}{3}0 & -\sin \frac{2\pi}{3}0 \\ \sin \frac{2\pi}{3}0 & \cos \frac{2\pi}{3}0 \end{bmatrix}
$$

$$
(123) = (12)\,(23) \quad : \begin{cases}
\begin{bmatrix} \frac{-1}{2} \\ \frac{\sqrt{3}}{2} \end{bmatrix} = \begin{bmatrix} \frac{-1}{2} \\ \frac{\sqrt{3}}{2} \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} & (12) \\
\begin{bmatrix} \frac{-1}{2} \\ \frac{-\sqrt{3}}{2} \end{bmatrix} = \begin{bmatrix} \frac{-1}{2} & \frac{-\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & \frac{-1}{2} \end{bmatrix} \begin{bmatrix} \frac{-1}{2} \\ \frac{\sqrt{3}}{2} \end{bmatrix} & (23)
\end{cases}
\qquad
\begin{bmatrix} \frac{-1}{2} & \frac{-\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & \frac{-1}{2} \end{bmatrix} = \begin{bmatrix} \cos \frac{2\pi}{3}1 & -\sin \frac{2\pi}{3}1 \\ \sin \frac{2\pi}{3}1 & \cos \frac{2\pi}{3}1 \end{bmatrix}
$$

$$
(132) = (13)\,(32) \quad : \begin{cases}
\begin{bmatrix} \frac{-1}{2} \\ \frac{-\sqrt{3}}{2} \end{bmatrix} = \begin{bmatrix} \frac{-1}{2} \\ \frac{-\sqrt{3}}{2} \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} & (13) \\
\begin{bmatrix} \frac{-1}{2} \\ \frac{\sqrt{3}}{2} \end{bmatrix} = \begin{bmatrix} \frac{-1}{2} & \frac{\sqrt{3}}{2} \\ \frac{-\sqrt{3}}{2} & \frac{-1}{2} \end{bmatrix} \begin{bmatrix} \frac{-1}{2} \\ \frac{-\sqrt{3}}{2} \end{bmatrix} & (32)
\end{cases}
\qquad
\begin{bmatrix} \frac{-1}{2} & \frac{\sqrt{3}}{2} \\ \frac{-\sqrt{3}}{2} & \frac{-1}{2} \end{bmatrix} = \begin{bmatrix} \cos \frac{2\pi}{3}2 & -\sin \frac{2\pi}{3}2 \\ \sin \frac{2\pi}{3}2 & \cos \frac{2\pi}{3}2 \end{bmatrix}
$$

$$
(12) = (12)\,(3) \quad : \begin{cases}
\begin{bmatrix} \frac{-1}{2} \\ \frac{\sqrt{3}}{2} \end{bmatrix} = \begin{bmatrix} \frac{-1}{2} & 0 \\ \frac{\sqrt{3}}{2} & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} & (12) \\
\begin{bmatrix} \frac{-1}{2} \\ \frac{-\sqrt{3}}{2} \end{bmatrix} = \begin{bmatrix} \frac{-1}{2} & \frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & \frac{1}{2} \end{bmatrix} \begin{bmatrix} \frac{-1}{2} \\ \frac{-\sqrt{3}}{2} \end{bmatrix} & (3)
\end{cases}
\qquad
\begin{bmatrix} \frac{-1}{2} & \frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & \frac{1}{2} \end{bmatrix} = \begin{bmatrix} \cos \frac{2\pi}{3}1 & \sin \frac{2\pi}{3}1 \\ \sin \frac{2\pi}{3}1 & -\cos \frac{2\pi}{3}1 \end{bmatrix}
$$

$$
(23) = (23)\,(1) \quad : \begin{cases}
\begin{bmatrix} \frac{-1}{2} \\ \frac{-\sqrt{3}}{2} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} \frac{-1}{2} \\ \frac{\sqrt{3}}{2} \end{bmatrix} & (23) \\
\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} & (1)
\end{cases}
\qquad
\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} \cos \frac{2\pi}{3}0 & \sin \frac{2\pi}{3}0 \\ \sin \frac{2\pi}{3}0 & -\cos \frac{2\pi}{3}0 \end{bmatrix}
$$

$$
(31) = (31)\,(2) \quad : \begin{cases}
\begin{bmatrix} \frac{-1}{2} \\ \frac{-\sqrt{3}}{2} \end{bmatrix} = \begin{bmatrix} \frac{-1}{2} \\ \frac{-\sqrt{3}}{2} \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} & (31) \\
\begin{bmatrix} \frac{-1}{2} \\ \frac{\sqrt{3}}{2} \end{bmatrix} = \begin{bmatrix} \frac{-1}{2} & \frac{-\sqrt{3}}{2} \\ \frac{-\sqrt{3}}{2} & \frac{1}{2} \end{bmatrix} \begin{bmatrix} \frac{-1}{2} \\ \frac{\sqrt{3}}{2} \end{bmatrix} & (2)
\end{cases}
\qquad
\begin{bmatrix} \frac{-1}{2} & \frac{-\sqrt{3}}{2} \\ \frac{-\sqrt{3}}{2} & \frac{1}{2} \end{bmatrix} = \begin{bmatrix} \cos \frac{2\pi}{3}2 & \sin \frac{2\pi}{3}2 \\ \sin \frac{2\pi}{3}2 & -\cos \frac{2\pi}{3}2 \end{bmatrix}
$$

$$
\begin{array}{llllll}
D_3 = \{ & (), & (123), & (132), & & \\
 & (12), & (23), & (31), & \} & = S_3 \\
= \{ & [123], & [231], & [312], & & \\
 & [213], & [132], & [321], & \} & = S_3 \\
= \{ & \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, & \begin{bmatrix} \frac{-1}{2} & \frac{-\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & \frac{-1}{2} \end{bmatrix}, & \begin{bmatrix} \frac{-1}{2} & \frac{\sqrt{3}}{2} \\ \frac{-\sqrt{3}}{2} & \frac{-1}{2} \end{bmatrix}, & & \\
 & \begin{bmatrix} \frac{-1}{2} & \frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & \frac{1}{2} \end{bmatrix}, & \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, & \begin{bmatrix} \frac{-1}{2} & \frac{-\sqrt{3}}{2} \\ \frac{-\sqrt{3}}{2} & \frac{1}{2} \end{bmatrix} & \} & \text{matrix representation} \\
= \{ & \begin{bmatrix} \cos 0 & -\sin 0 \\ \sin 0 & \cos 0 \end{bmatrix}, & \begin{bmatrix} \cos\frac{2\pi}{3} & -\sin\frac{2\pi}{3} \\ \sin\frac{2\pi}{3} & \cos\frac{2\pi}{3} \end{bmatrix}, & \begin{bmatrix} \cos\frac{4\pi}{3} & -\sin\frac{4\pi}{3} \\ \sin\frac{4\pi}{3} & \cos\frac{4\pi}{3} \end{bmatrix}, & & \rho_k = \begin{bmatrix} \cos\frac{2\pi}{3}k & -\sin\frac{2\pi}{3}k \\ \sin\frac{2\pi}{3}k & \cos\frac{2\pi}{3}k \end{bmatrix} \\
 & \begin{bmatrix} \cos\frac{2\pi}{3} & \sin\frac{2\pi}{3} \\ \sin\frac{2\pi}{3} & -\cos\frac{2\pi}{3} \end{bmatrix}, & \begin{bmatrix} \cos 0 & \sin 0 \\ \sin 0 & -\cos 0 \end{bmatrix}, & \begin{bmatrix} \cos\frac{4\pi}{3} & \sin\frac{4\pi}{3} \\ \sin\frac{4\pi}{3} & -\cos\frac{4\pi}{3} \end{bmatrix} & \} & \pi_k = \begin{bmatrix} \cos\frac{2\pi}{3}k & \sin\frac{2\pi}{3}k \\ \sin\frac{2\pi}{3}k & -\cos\frac{2\pi}{3}k \end{bmatrix} \\
= \{ & \rho_0, & \rho_1, & \rho_2, & & \text{rotations} \\
 & \pi_0, & \pi_1, & \pi_2 & \} & \text{reflections} \\
= \{ & \rho_k & | & \rho_{k+3} = \rho_k & & \\
 & \pi_k & | & \pi_{k+3} = \pi_k & \} &
\end{array}
$$

$$
\begin{aligned}
\cos\alpha\cos\beta &= \frac{+\cos(\alpha+\beta)+\cos(\alpha-\beta)}{2} \\
\sin\alpha\sin\beta &= \frac{-\cos(\alpha+\beta)+\cos(\alpha-\beta)}{2} \\
\sin\alpha\cos\beta &= \frac{+\sin(\alpha+\beta)+\sin(\alpha-\beta)}{2} \\
\cos\alpha\sin\beta &= \frac{+\sin(\alpha+\beta)-\sin(\alpha-\beta)}{2}
\end{aligned}
$$

$$
\rho_i\rho_j = \begin{bmatrix} \cos\frac{2\pi}{3}i & -\sin\frac{2\pi}{3}i \\ \sin\frac{2\pi}{3}i & \cos\frac{2\pi}{3}i \end{bmatrix} \begin{bmatrix} \cos\frac{2\pi}{3}j & -\sin\frac{2\pi}{3}j \\ \sin\frac{2\pi}{3}j & \cos\frac{2\pi}{3}j \end{bmatrix} = \begin{bmatrix} \cos\frac{2\pi}{3}(i+j) & -\sin\frac{2\pi}{3}(i+j) \\ \sin\frac{2\pi}{3}(i+j) & \cos\frac{2\pi}{3}(i+j) \end{bmatrix} = \rho_{i+j} \qquad \rho_i\rho_j = \rho_{i+j}
$$

$$
\rho_i\pi_j = \begin{bmatrix} \cos\frac{2\pi}{3}i & -\sin\frac{2\pi}{3}i \\ \sin\frac{2\pi}{3}i & \cos\frac{2\pi}{3}i \end{bmatrix} \begin{bmatrix} \cos\frac{2\pi}{3}j & \sin\frac{2\pi}{3}j \\ \sin\frac{2\pi}{3}j & -\cos\frac{2\pi}{3}j \end{bmatrix} = \begin{bmatrix} \cos\frac{2\pi}{3}(i+j) & \sin\frac{2\pi}{3}(i+j) \\ \sin\frac{2\pi}{3}(i+j) & -\cos\frac{2\pi}{3}(i+j) \end{bmatrix} = \pi_{i+j} \qquad \rho_i\pi_j = \pi_{i+j}
$$

$$
\pi_i\rho_j = \begin{bmatrix} \cos\frac{2\pi}{3}i & \sin\frac{2\pi}{3}i \\ \sin\frac{2\pi}{3}i & -\cos\frac{2\pi}{3}i \end{bmatrix} \begin{bmatrix} \cos\frac{2\pi}{3}j & -\sin\frac{2\pi}{3}j \\ \sin\frac{2\pi}{3}j & \cos\frac{2\pi}{3}j \end{bmatrix} = \begin{bmatrix} \cos\frac{2\pi}{3}(i-j) & \sin\frac{2\pi}{3}(i-j) \\ \sin\frac{2\pi}{3}(i-j) & -\cos\frac{2\pi}{3}(i-j) \end{bmatrix} = \pi_{i-j} \qquad \pi_i\rho_j = \pi_{i-j}
$$

$$
\pi_i\pi_j = \begin{bmatrix} \cos\frac{2\pi}{3}i & \sin\frac{2\pi}{3}i \\ \sin\frac{2\pi}{3}i & -\cos\frac{2\pi}{3}i \end{bmatrix} \begin{bmatrix} \cos\frac{2\pi}{3}j & \sin\frac{2\pi}{3}j \\ \sin\frac{2\pi}{3}j & -\cos\frac{2\pi}{3}j \end{bmatrix} = \begin{bmatrix} \cos\frac{2\pi}{3}(i-j) & -\sin\frac{2\pi}{3}(i-j) \\ \sin\frac{2\pi}{3}(i-j) & \cos\frac{2\pi}{3}(i-j) \end{bmatrix} = \rho_{i-j} \qquad \pi_i\pi_j = \rho_{i-j}
$$

$$
\begin{aligned}
\rho_{k+3} &= \rho_k \\
\pi_{k+3} &= \pi_k \\
\rho_i\rho_j &= \rho_{i+j} \\
\rho_i\pi_j &= \pi_{i+j} \\
\pi_i\rho_j &= \pi_{i-j} \\
\pi_i\pi_j &= \rho_{i-j}
\end{aligned}
$$

$$
\begin{aligned}
D_3 &= S_3 \\
\rho_0 &\leftrightarrow [123] \\
\rho_1 &\leftrightarrow [231] \\
\rho_2 &\leftrightarrow [312] \\
\pi_0 &\leftrightarrow [213] \\
\pi_1 &\leftrightarrow [132] \\
\pi_2 &\leftrightarrow [321]
\end{aligned}
$$

$\cdot_{D_3}$	ρ_0	ρ_1	ρ_2	π_0	π_1	π_2
ρ_0	ρ_{0+0}	ρ_{0+1}	ρ_{0+2}	π_{0+0}	π_{0+1}	π_{0+2}
ρ_1	ρ_{1+0}	ρ_{1+1}	ρ_{1+2}	π_{1+0}	π_{1+1}	π_{1+2}
ρ_2	ρ_{2+0}	ρ_{2+1}	ρ_{2+2}	π_{2+0}	π_{2+1}	π_{2+2}
π_0	π_{0-0}	π_{0-1}	π_{0-2}	ρ_{0-0}	ρ_{0-1}	ρ_{0-2}
π_1	π_{1-0}	π_{1-1}	π_{1-2}	ρ_{1-0}	ρ_{1-1}	ρ_{1-2}
π_2	π_{2-0}	π_{2-1}	π_{2-2}	ρ_{2-0}	ρ_{2-1}	ρ_{2-2}

$\rightarrow$

$\cdot_{D_3}$	ρ_0	ρ_1	ρ_2	π_0	π_1	π_2
ρ_0	ρ_0	ρ_1	ρ_2	π_0	π_1	π_2
ρ_1	ρ_1	ρ_2	ρ_3	π_1	π_2	π_3
ρ_2	ρ_2	ρ_3	ρ_4	π_2	π_3	π_4
π_0	π_0	π_{-1}	π_{-2}	ρ_0	ρ_{-1}	ρ_{-2}
π_1	π_1	π_0	π_{-1}	ρ_1	ρ_0	ρ_{-1}
π_2	π_2	π_1	π_0	ρ_2	ρ_1	ρ_0

$\rho_{k+3} = \rho_k \downarrow \pi_{k+3} = \pi_k$

$\cdot_{D_3}$	ρ_0	ρ_1	ρ_2	π_0	π_1	π_2
ρ_0	ρ_0	ρ_1	ρ_2	π_0	π_1	π_2
ρ_1	ρ_1	ρ_2	ρ_0	π_1	π_2	π_0
ρ_2	ρ_2	ρ_0	ρ_1	π_2	π_0	π_1
π_0	π_0	π_2	π_1	ρ_0	ρ_2	ρ_1
π_1	π_1	π_0	π_2	ρ_1	ρ_0	ρ_2
π_2	π_2	π_1	π_0	ρ_2	ρ_1	ρ_0

$\xleftarrow{S_3 = D_3}$

$\cdot_{S_3}$	[123]	[231]	[312]	[213]	[132]	[321]
[123]	[123]	[231]	[312]	[213]	[132]	[321]
[231]	[231]	[312]	[123]	[132]	[321]	[213]
[312]	[312]	[123]	[231]	[321]	[213]	[132]
[213]	[213]	[321]	[132]	[123]	[312]	[231]
[132]	[132]	[213]	[321]	[231]	[123]	[312]
[321]	[321]	[132]	[213]	[312]	[231]	[123]

$\downarrow$

$+_{\mathbb{Z}_3}$	0	1	2	π_0	π_1	π_2
0	0	1	2	π_0	π_1	π_2
1	1	2	0	π_1	π_2	π_0
2	2	0	1	π_2	π_0	π_1
π_0	π_0	π_2	π_1	ρ_0	ρ_2	ρ_1
π_1	π_1	π_0	π_2	ρ_1	ρ_0	ρ_2
π_2	π_2	π_1	π_0	ρ_2	ρ_1	ρ_0

$\leftarrow$

$+_{\mathbb{Z}_3}$	0_ρ	1_ρ	2_ρ	0_π	1_π	2_π
0_ρ	0_ρ	1_ρ	2_ρ	0_π	1_π	2_π
1_ρ	1_ρ	2_ρ	0_ρ	1_π	2_π	0_π
2_ρ	2_ρ	0_ρ	1_ρ	2_π	0_π	1_π
0_π	0_π	2_π	1_π	0_ρ	2_ρ	1_ρ
1_π	1_π	0_π	2_π	1_ρ	0_ρ	2_ρ
2_π	2_π	1_π	0_π	2_ρ	1_ρ	0_ρ

$$
\begin{aligned}
D_3 &= \{\rho_0, \rho_1, \rho_2, \pi_0, \pi_1, \pi_2\} && = \{\rho_{0,3}, \rho_{1,3}, \rho_{2,3}, \pi_{0,3}, \pi_{1,3}, \pi_{2,3}\} \\
&= \left\{ \begin{array}{c} \rho_k \\ \pi_k \end{array} \middle| \begin{array}{l} \rho_k = \begin{bmatrix} +\cos\frac{2\pi}{3}k & -\sin\frac{2\pi}{3}k \\ +\sin\frac{2\pi}{3}k & +\cos\frac{2\pi}{3}k \end{bmatrix} \\ \pi_k = \begin{bmatrix} +\cos\frac{2\pi}{3}k & +\sin\frac{2\pi}{3}k \\ +\sin\frac{2\pi}{3}k & -\cos\frac{2\pi}{3}k \end{bmatrix} \end{array} \right\} && k \in \{0,1,2\} \\
D_n &= \left\{ \begin{array}{c} \rho_k \\ \pi_k \end{array} \middle| \begin{array}{l} \rho_k = \begin{bmatrix} +\cos\frac{2\pi}{n}k & -\sin\frac{2\pi}{n}k \\ +\sin\frac{2\pi}{n}k & +\cos\frac{2\pi}{n}k \end{bmatrix} \\ \pi_k = \begin{bmatrix} +\cos\frac{2\pi}{n}k & +\sin\frac{2\pi}{n}k \\ +\sin\frac{2\pi}{n}k & -\cos\frac{2\pi}{n}k \end{bmatrix} \end{array} \right\} && \begin{array}{r} \forall n \in \mathbb{N} \\ k \in \{0, \cdots, n-1\} \end{array} \\
&= \left\{ \begin{array}{c} \rho_{k,n} \\ \pi_{k,n} \end{array} \middle| \begin{array}{l} \rho_{k,n} = \begin{bmatrix} +\cos\frac{2\pi}{n}k & -\sin\frac{2\pi}{n}k \\ +\sin\frac{2\pi}{n}k & +\cos\frac{2\pi}{n}k \end{bmatrix} \\ \pi_{k,n} = \begin{bmatrix} +\cos\frac{2\pi}{n}k & +\sin\frac{2\pi}{n}k \\ +\sin\frac{2\pi}{n}k & -\cos\frac{2\pi}{n}k \end{bmatrix} \end{array} \right\} && \begin{array}{r} \forall n \in \mathbb{N} \\ k \in \{0, \cdots, n-1\} \end{array} \\
D_2 &= \left\{ \begin{array}{c} \rho_k \\ \pi_k \end{array} \middle| \begin{array}{l} \rho_k = \begin{bmatrix} +\cos\frac{2\pi}{2}k & -\sin\frac{2\pi}{2}k \\ +\sin\frac{2\pi}{2}k & +\cos\frac{2\pi}{2}k \end{bmatrix} \\ \pi_k = \begin{bmatrix} +\cos\frac{2\pi}{2}k & +\sin\frac{2\pi}{2}k \\ +\sin\frac{2\pi}{2}k & -\cos\frac{2\pi}{2}k \end{bmatrix} \end{array} \right\} && k \in \{0, 2-1\} = \{0,1\} \\
&= \left\{ \begin{array}{c} \rho_k \\ \pi_k \end{array} \middle| \begin{array}{l} \rho_k = \begin{bmatrix} +\cos\pi k & -\sin\pi k \\ +\sin\pi k & +\cos\pi k \end{bmatrix} \\ \pi_k = \begin{bmatrix} +\cos\pi k & +\sin\pi k \\ +\sin\pi k & -\cos\pi k \end{bmatrix} \end{array} \right\} && k \in \{0,1\} \\
&= \{ \begin{bmatrix} \cos 0 & -\sin 0 \\ \sin 0 & \cos 0 \end{bmatrix}, \begin{bmatrix} \cos\pi & -\sin\pi \\ \sin\pi & \cos\pi \end{bmatrix}, && = \{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \\
&\qquad \begin{bmatrix} \cos 0 & \sin 0 \\ \sin 0 & -\cos 0 \end{bmatrix}, \begin{bmatrix} \cos\pi & \sin\pi \\ \sin\pi & -\cos\pi \end{bmatrix} \} && \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \} \\
&= \{\rho_0, \rho_1, && = \{\rho_0, \rho_1, \pi_0, \pi_1\} \\
&\qquad \pi_0, \pi_1\} && = \{\rho_{0,2}, \rho_{1,2}, \pi_{0,2}, \pi_{1,2}\} \\
D_1 &= \{ \begin{bmatrix} \cos 0 & -\sin 0 \\ \sin 0 & \cos 0 \end{bmatrix}, && = \{\rho_0, \pi_0\} \\
&\qquad \begin{bmatrix} \cos 0 & \sin 0 \\ \sin 0 & -\cos 0 \end{bmatrix} \} && = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \right\} = \{\rho_{0,1}, \pi_{0,1}\}
\end{aligned}
$$

4 subgroup

定義 4.1. subgroup

$$
\begin{aligned}
G = (G, \cdot) = (G, \cdot_G) &\ \text{ is a group} \\
G \supseteq H &\neq \emptyset \\
h_1 \cdot h_2 = h_1 h_2 &\in H && \forall h_1, h_2 \in H \quad (c) \cdot \text{closure} \\
h^{-1} = \overline{h} &\in H && \forall h \in H \quad (in)\,\text{inverse} \\
&\Updownarrow \\
H &\leq G \\
&\Updownarrow \\
H &\text{ is a subgroup of } G \quad \overset{\text{need to be proved}}{\Rightarrow} \quad H = (H, \cdot) = (H, \cdot_G) \ \text{ is a group}
\end{aligned}
$$

trivial subgroups

$$\{e\} = \{e_G\} \le G$$
$$G = G \le G$$

$$C_3 = \quad \mathbb{Z}_3 \le D_3 = S_3$$
$$\mathbb{Z}_2 \le S_3 = D_3 \qquad \mathbb{Z}_2 \le S_n \quad \forall n \in \mathbb{N}_{\ge 2}$$

$\cdot_{D_3}$	ρ_0	ρ_1	ρ_2	π_0	π_1	π_2
ρ_0	ρ_{0+0}	ρ_{0+1}	ρ_{0+2}	π_{0+0}	π_{0+1}	π_{0+2}
ρ_1	ρ_{1+0}	ρ_{1+1}	ρ_{1+2}	π_{1+0}	π_{1+1}	π_{1+2}
ρ_2	ρ_{2+0}	ρ_{2+1}	ρ_{2+2}	π_{2+0}	π_{2+1}	π_{2+2}
π_0	π_{0-0}	π_{0-1}	π_{0-2}	ρ_{0-0}	ρ_{0-1}	ρ_{0-2}
π_1	π_{1-0}	π_{1-1}	π_{1-2}	ρ_{1-0}	ρ_{1-1}	ρ_{1-2}
π_2	π_{2-0}	π_{2-1}	π_{2-2}	ρ_{2-0}	ρ_{2-1}	ρ_{2-2}

$\rightarrow$

$\cdot_{D_3}$	ρ_0	ρ_1	ρ_2	π_0	π_1	π_2
ρ_0	ρ_0	ρ_1	ρ_2	π_0	π_1	π_2
ρ_1	ρ_1	ρ_2	ρ_3	π_1	π_2	π_3
ρ_2	ρ_2	ρ_3	ρ_4	π_2	π_3	π_4
π_0	π_0	π_{-1}	π_{-2}	ρ_0	ρ_{-1}	ρ_{-2}
π_1	π_1	π_0	π_{-1}	ρ_1	ρ_0	ρ_{-1}
π_2	π_2	π_1	π_0	ρ_2	ρ_1	ρ_0

$$\rho_{k+3} = \rho_k \downarrow \pi_{k+3} = \pi_k$$

$\cdot_{D_3}$	ρ_0	ρ_1	ρ_2	π_0	π_1	π_2
ρ_0	ρ_0	ρ_1	ρ_2	π_0	π_1	π_2
ρ_1	ρ_1	ρ_2	ρ_0	π_1	π_2	π_0
ρ_2	ρ_2	ρ_0	ρ_1	π_2	π_0	π_1
π_0	π_0	π_2	π_1	ρ_0	ρ_2	ρ_1
π_1	π_1	π_0	π_2	ρ_1	ρ_0	ρ_2
π_2	π_2	π_1	π_0	ρ_2	ρ_1	ρ_0

$\xleftarrow{S_3=D_3}$

$\cdot_{S_3}$	[123]	[231]	[312]	[213]	[132]	[321]
[123]	[123]	[231]	[312]	[213]	[132]	[321]
[231]	[231]	[312]	[123]	[132]	[321]	[213]
[312]	[312]	[123]	[231]	[321]	[213]	[132]
[213]	[213]	[321]	[132]	[123]	[312]	[231]
[132]	[132]	[213]	[321]	[231]	[123]	[312]
[321]	[321]	[132]	[213]	[312]	[231]	[123]

$\downarrow$

$+_{\mathbb{Z}_3}$	0	1	2	π_0	π_1	π_2
0	0	1	2	π_0	π_1	π_2
1	1	2	0	π_1	π_2	π_0
2	2	0	1	π_2	π_0	π_1
π_0	π_0	π_2	π_1	ρ_0	ρ_2	ρ_1
π_1	π_1	π_0	π_2	ρ_1	ρ_0	ρ_2
π_2	π_2	π_1	π_0	ρ_2	ρ_1	ρ_0

$\leftarrow$

$+_{\mathbb{Z}_3}$	0_ρ	1_ρ	2_ρ	0_π	1_π	2_π
0_ρ	0_ρ	1_ρ	2_ρ	0_π	1_π	2_π
1_ρ	1_ρ	2_ρ	0_ρ	1_π	2_π	0_π
2_ρ	2_ρ	0_ρ	1_ρ	2_π	0_π	1_π
0_π	0_π	2_π	1_π	0_ρ	2_ρ	1_ρ
1_π	1_π	0_π	2_π	1_ρ	0_ρ	2_ρ
2_π	2_π	1_π	0_π	2_ρ	1_ρ	0_ρ

$\Downarrow$

$$\mathbb{Z}_3 = \{0,1,2\}$$
$$= \{0_\rho, 1_\rho, 2_\rho\} = \{[123],[231],[312]\} = \{(),(123),(132)\}$$
$$= \left\{ \mathrm{e}^{\mathrm{i}\frac{2\pi}{n}0}, \mathrm{e}^{\mathrm{i}\frac{2\pi}{n}1}, \mathrm{e}^{\mathrm{i}\frac{2\pi}{n}2}, \cdots, \mathrm{e}^{\mathrm{i}\frac{2\pi}{n}(n-1)} \right\} \overset{n=3}{=} \left\{ \mathrm{e}^{\mathrm{i}\frac{2\pi}{3}0}, \mathrm{e}^{\mathrm{i}\frac{2\pi}{3}1}, \mathrm{e}^{\mathrm{i}\frac{2\pi}{3}2} \right\}$$
$$= \left\{ e, g, g^2, \cdots, g^{n-1} \right\} = \left\{ g^0, g^1, g^2 \right\} = \left\{ e, g, g^2 \right\}, g^n = e$$

$\Downarrow$

$$\mathbb{Z}_3 \le D_3 = S_3$$

$\Uparrow$

$\cdot_{S_3}$	()	(123)	(132)	(12)	(23)	(31)
()	()	(123)	(132)	(12)	(23)	(31)
(123)	(123)	(132)	()	(23)	(31)	(12)
(132)	(132)	()	(123)	(31)	(12)	(23)
(12)	(12)	(31)	(23)	()	(132)	(123)
(23)	(23)	(12)	(31)	(123)	()	(132)
(31)	(31)	(23)	(12)	(132)	(123)	()

$\rightarrow$

$+_{\mathbb{Z}_2}$	0	(123)	(132)	1	(23)	(31)
0	0	(123)	(132)	1	(23)	(31)
(123)	(123)	(132)	()	(23)	(31)	(12)
(132)	(132)	()	(123)	(31)	(12)	(23)
1	1	(31)	(23)	0	(132)	(123)
(23)	(23)	(12)	(31)	(123)	()	(132)
(31)	(31)	(23)	(12)	(132)	(123)	()

or

$+_{\mathbb{Z}_2}$	0	(123)	(132)	(12)	1	(31)
0	0	(123)	(132)	(12)	1	(31)
(123)	(123)	(132)	()	(23)	(31)	(12)
(132)	(132)	()	(123)	(31)	(12)	(23)
(12)	(12)	(31)	(23)	()	(132)	(123)
1	1	(12)	(31)	(123)	0	(132)
(31)	(31)	(23)	(12)	(132)	(123)	()

or

$+_{\mathbb{Z}_2}$	0	(123)	(132)	(12)	(23)	1
0	0	(123)	(132)	(12)	(23)	1
(123)	(123)	(132)	()	(23)	(31)	(12)
(132)	(132)	()	(123)	(31)	(12)	(23)
(12)	(12)	(31)	(23)	()	(132)	(123)
(23)	(23)	(12)	(31)	(123)	()	(132)
1	1	(23)	(12)	(132)	(123)	0

$\Downarrow$

$\Leftarrow$

$$\mathbb{Z}_2 \le S_3 = D_3$$

$\Downarrow$

$$\mathbb{Z}_2 \le S_n \quad \forall n \in \mathbb{N}_{\ge 2}$$

$S_2 = \mathbb{Z}_2 \leq S_3 = D_3$

$$\begin{array}{rlllll}
\mathbb{Z}_2 = (\mathbb{Z}_2, +) & = (\mathbb{Z}_2, +_{\mathbb{Z}_n}) & = \{0, 2-1\} & & = \{0, 1\} \\
= \mathbb{Z}_2 = (\mathbb{Z}_2, \cdot) & = (\mathbb{Z}_2, \cdot_{\mathbb{C}}) & = \left\{ \mathrm{e}^{\mathrm{i}\frac{2\pi}{2}0}, \mathrm{e}^{\mathrm{i}\frac{2\pi}{2}(2-1)} \right\} = \{\mathrm{e}^{\mathrm{i}0}, \mathrm{e}^{\mathrm{i}\pi}\} & & = \{1, -1\} \\
= S_2 = \mathbb{Z}_2 = (S_2, \cdot_{S_n}) & = (S_2, \circ) & = \{\sigma_1, \sigma_2\} = \{e_{S_2}, \sigma_2\} & & = \{e, \sigma_2\} \\
= C_{2,1} & = (\mathbb{Z}_2, \cdot_{S_3}) & = \{[123], [213]\} = \{(), (12)\} & & \\
= C_{2,2} & = (\mathbb{Z}_2, \cdot_{S_3}) & = \{[123], [132]\} = \{(), (23)\} & & \\
= C_{2,3} & = (\mathbb{Z}_2, \cdot_{S_3}) & = \{[123], [321]\} = \{(), (31)\} & & \\
E_3 & = (\mathbb{Z}_1, \cdot_{S_3}) & = \{e\} = \{[123]\} = \{()\} & e = e_{S_3} &
\end{array}$$

$\mathbb{Z}_2 \leq \mathbb{Z}_4$

$$\mathbb{Z}_4 = \left\{ e, a, a^2, a^3 \middle| a^4 = e \right\}$$

$$\begin{array}{ccccc}
\cdot_{\mathbb{Z}_4} & e & a & a^2 & a^3 \\
e & e & a & a^2 & a^3 \\
a & a & a^2 & a^3 & a^4 \\
a^2 & a^2 & a^3 & a^4 & a^5 \\
a^3 & a^3 & a^4 & a^5 & a^6
\end{array}
\to
\begin{array}{ccccc}
\cdot_{\mathbb{Z}_4} & e & a & a^2 & a^3 \\
e & e & a & a^2 & a^3 \\
a & a & a^2 & a^3 & e \\
a^2 & a^2 & a^3 & e & a \\
a^3 & a^3 & e & a & a^2
\end{array}
\to
\begin{array}{ccccc}
+_{\mathbb{Z}_2} & 0 & a & 1 & a^3 \\
0 & 0 & a & 1 & a^3 \\
a & a & a^2 & a^3 & e \\
1 & 1 & a^3 & 0 & a \\
a^3 & a^3 & e & a & a^2
\end{array}$$

$$\Downarrow$$

$$\{e, a^2\} \quad = \quad \{0, 1\} = \mathbb{Z}_2 \leq \mathbb{Z}_4$$

$\mathbb{Z}_2 \leq \mathbb{Z}_{2n}$

$$\mathbb{Z}_{2n} = \left\{ e, a, \cdots, a^n, \cdots, a^{2n-1} \middle| a^{2n} = e \right\} \quad \forall n \in \mathbb{N}$$

$$\begin{array}{ccccccc}
\cdot_{\mathbb{Z}_{2n}} & e & a & \cdots & a^n & \cdots & a^{2n-1} \\
e & e & a & \cdots & a^n & \cdots & a^{2n-1} \\
a & a & a^2 & \cdots & a^{n+1} & \cdots & a^{2n} \\
\vdots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\
a^n & a^n & a^{n+1} & \cdots & a^{2n} & \cdots & a^{3n-1} \\
\vdots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\
a^{2n-1} & a^{2n-1} & a^{2n} & \cdots & a^{3n-1} & \cdots & a^{4n-2}
\end{array}
\to
\begin{array}{ccccccc}
\cdot_{\mathbb{Z}_{2n}} & e & a & \cdots & a^n & \cdots & a^{2n-1} \\
e & e & a & \cdots & a^n & \cdots & a^{2n-1} \\
a & a & a^2 & \cdots & a^{n+1} & \cdots & a^{2n} \\
\vdots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\
a^n & a^n & a^{n+1} & \cdots & a^{2n} & \cdots & a^{2n+(n-1)} \\
\vdots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\
a^{2n-1} & a^{2n-1} & a^{2n} & \cdots & a^{2n+(n-1)} & \cdots & a^{2(n-1)}
\end{array}$$

$$\downarrow$$

$$\begin{array}{ccccccc}
+_{\mathbb{Z}_2} & 0 & a & \cdots & 1 & \cdots & a^{2n-1} \\
0 & 0 & a & \cdots & 1 & \cdots & a^{2n-1} \\
a & a & a^2 & \cdots & a^{n+1} & \cdots & e \\
\vdots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\
1 & 1 & a^{n+1} & \cdots & 0 & \cdots & a^{n-1} \\
\vdots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\
a^{2n-1} & a^{2n-1} & e & \cdots & a^{n-1} & \cdots & e
\end{array}
\leftarrow
\begin{array}{ccccccc}
\cdot_{\mathbb{Z}_{2n}} & e & a & \cdots & a^n & \cdots & a^{2n-1} \\
e & e & a & \cdots & a^n & \cdots & a^{2n-1} \\
a & a & a^2 & \cdots & a^{n+1} & \cdots & e \\
\vdots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\
a^n & a^n & a^{n+1} & \cdots & e & \cdots & a^{n-1} \\
\vdots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\
a^{2n-1} & a^{2n-1} & e & \cdots & a^{n-1} & \cdots & e
\end{array}$$

$$\Downarrow$$

$$\mathbb{Z}_{2n} \geq \mathbb{Z}_2 = \{0, 1\} \quad = \quad \{e, a^n\}$$

$\mathbb{Z}_2 \nleq \mathbb{Z}_{2n+1}$

$$\mathbb{Z}_1 = \{e\} = \{0\}$$

$$\mathbb{Z}_{2n+1} = \left\{ e, a, \cdots, a^k, \cdots, a^{2n} \middle| \begin{array}{rl} a^{2n+1} = e & (id) \\ k \in \mathbb{N}_{\leq 2n} & (xp) \end{array} \right\} \quad \forall n \in \mathbb{N}$$

$$(xp) \Rightarrow \left\{ e, a^k \middle| k \in \mathbb{N}_{\leq 2n} \right\} \in \left\{ \left\{ e, a^k \middle| 1 \leq k \leq 2n \right\} \right\}$$

even $2\mathbb{N} \ni 2k \neq 2n+1 \in 2\mathbb{N}+1$ odd

$$\Rightarrow 2 \leq 2k \leq 2 \cdot 2n < 2(2n+1)$$

$$\Downarrow$$

$$2k \neq 2(2n+1) \Rightarrow 2n+1 \nmid 2k$$

$$a^{2k} = \left(a^k\right)^2 \neq \left(a^{2n+1}\right)^m \overset{(id)}{=} (e)^m = e \qquad m \in \mathbb{Z}_{\geq 0}$$

$$\left(a^k\right)^2 \neq e \qquad \Rightarrow \mathbb{Z}_2 \nleq \mathbb{Z}_{2n+1}$$

$2\mathbb{Z} \leq \mathbb{Z}$

$$\begin{aligned}
\mathbb{Z} =& \{\cdots, -3, -2, -1, 0, +1, +2, +3, \cdots\} = \{\cdots, -3, -2, -1, 0, 1, 2, 3, \cdots\} = \{k | k \in \mathbb{Z}\} \\
2\mathbb{Z} =& \{\cdots, -6, -4, -2, 0, +2, +4, +6, \cdots\} = \{\cdots, -6, -4, -2, 0, 2, 4, 6, \cdots\} = \{2k | k \in \mathbb{Z}\} \\
2\mathbb{Z} \subset& \mathbb{Z} \\
2k_1 + 2k_2 =& 2(k_1 + k_2) \in 2\mathbb{Z} \\
-2k = \overline{2k} =& 2(-k) \in 2\mathbb{Z} \\
&\Downarrow \\
2\mathbb{Z} \leq& \mathbb{Z}
\end{aligned}$$

$n\mathbb{Z} \leq \mathbb{Z}$

$$\begin{aligned}
\mathbb{Z} =& \{\cdots, -3, -2, -1, 0, +1, +2, +3, \cdots\} = \{\cdots, -3, -2, -1, 0, 1, 2, 3, \cdots\} = \{k | k \in \mathbb{Z}\} \\
n\mathbb{Z} =& \{\cdots, -3n, -2n, -n, 0, n, 2n, 3n, \cdots\} = \left\{ nk \middle| \begin{aligned} k \in& \mathbb{Z} \\ n \in& \mathbb{N} \end{aligned} \right\} \\
n\mathbb{Z} \subseteq& \mathbb{Z} \\
nk_1 + nk_2 =& n(k_1 + k_2) \in n\mathbb{Z} \\
-nk = \overline{nk} =& n(-k) \in n\mathbb{Z} \\
&\Downarrow \\
n\mathbb{Z} \leq& \mathbb{Z} \\
|n\mathbb{Z}| \not<& \infty
\end{aligned}$$

$\{0\} \leq \mathbb{Z}$

$$\begin{aligned}
\{0\} \subset& \mathbb{Z} \\
0 + 0 =& 0 \in \{0\} \\
-0 = \overline{0} =& 0 \in \{0\} \\
&\Downarrow \\
\{0\} \leq& \mathbb{Z} \\
|\{0\}| =& 1 < \infty
\end{aligned}$$

$\mathbb{Z}_n \leq U(1)$

$$\begin{aligned}
\mathbb{Z}_n = (\mathbb{Z}_n, \cdot) = (\mathbb{Z}_n, \cdot_{\mathbb{C}}) =& \left\{ \mathrm{e}^{\mathrm{i}\frac{2\pi}{n}0}, \mathrm{e}^{\mathrm{i}\frac{2\pi}{n}1}, \mathrm{e}^{\mathrm{i}\frac{2\pi}{n}2}, \cdots, \mathrm{e}^{\mathrm{i}\frac{2\pi}{n}(n-1)} \right\} \qquad \forall n \in \mathbb{N} \\
=& \left\{ \mathrm{e}^{\mathrm{i}\frac{2\pi}{n}k} \middle| k \in \mathbb{N}_{<n} \right\} \\
=& \left\{ \mathrm{e}^{\mathrm{i}\frac{2\pi}{n}k} \middle| k \in \mathbb{N}_{\leq n-1} \right\} \\
=& \left\{ \mathrm{e}^{\mathrm{i}\frac{2\pi}{n}k} \middle| k \in \{0, 1, \cdots, n-1\} \right\} \\
\subset& U(1) = \{\mathrm{e}^{\mathrm{i}\theta} | \theta \in [0, 2\pi]\} \\
\mathrm{e}^{\mathrm{i}\frac{2\pi}{n}k_1} \mathrm{e}^{\mathrm{i}\frac{2\pi}{n}k_2} =& \mathrm{e}^{\mathrm{i}\frac{2\pi}{n}(k_1+k_2)} = \mathrm{e}^{\mathrm{i}\frac{2\pi}{n}(k_1+k_2) \mod n} \in \mathbb{Z}_n \\
\mathrm{e}^{-\mathrm{i}\frac{2\pi}{n}k} = \mathrm{e}^{\mathrm{i}\frac{2\pi}{n}(-k)} =& \mathrm{e}^{\mathrm{i}\frac{2\pi}{n}(-k)} \cdot 1 = \mathrm{e}^{\mathrm{i}\frac{2\pi}{n}(-k)} \mathrm{e}^{\mathrm{i}\frac{2\pi}{n}n} = \mathrm{e}^{\mathrm{i}\frac{2\pi}{n}(n-k)} \in \mathbb{Z}_n \\
&\Downarrow \\
\mathbb{Z}_n \leq& U(1)
\end{aligned}$$

$D_n \leq S_n$

$$D_n = \left\{ \begin{matrix} \rho_{k,n} \\ \pi_{k,n} \end{matrix} \middle| \begin{aligned} \rho_{k,n} =& \begin{bmatrix} +\cos\frac{2\pi}{n}k & -\sin\frac{2\pi}{n}k \\ +\sin\frac{2\pi}{n}k & +\cos\frac{2\pi}{n}k \end{bmatrix} \\ \pi_{k,n} =& \begin{bmatrix} +\cos\frac{2\pi}{n}k & +\sin\frac{2\pi}{n}k \\ +\sin\frac{2\pi}{n}k & -\cos\frac{2\pi}{n}k \end{bmatrix} \end{aligned} \right\} \qquad \begin{aligned} &\forall n \in \mathbb{N} \\ k \in \{0, \cdots, n-1\} =& \mathbb{Z}_{[0,n)} \end{aligned}$$

$$
\begin{aligned}
|D_1| = 2\cdot 1 = 2 > 1 = 1! = |S_1| & \qquad n = 1\\
|D_2| = 2\cdot 2 = 4 > 2 = 2! = |S_2| & \qquad n = 2\\
|D_3| = 2\cdot 3 = 6 = 6 = 3! = |S_3| & \qquad n = 3\\
|D_n| = 2n < n! = |S_n| & \qquad \forall n \in \mathbb{N}_{>3}\\
\Downarrow & \qquad D_n \text{ do not change neighbors}\\
D_n \subseteq S_n & \qquad \forall n \in \mathbb{N}_{>3}\\
\Downarrow & \qquad D_n \text{ are groups}\\
D_n \leq S_n & \qquad \forall n \in \mathbb{N}_{>3}
\end{aligned}
$$

$A_n \leq S_n$

$$
\begin{aligned}
A_n &= \left\{\sigma \middle| \begin{matrix}\sigma \in S_n\\ N_\sigma \in 2\mathbb{Z}_{\geq 0}\end{matrix}\right\} \subseteq S_n\\
\sigma\widetilde{\sigma} &= \overbrace{\underbrace{(s_{11}s_{12})}_{s_1}\cdots\underbrace{(s_{N_\sigma 1}s_{N_\sigma 2})}_{s_{N_\sigma}}}^{N_\sigma}\overbrace{\underbrace{(\widetilde{s}_{11}\widetilde{s}_{12})}_{\widetilde{s}_1}\cdots\underbrace{(\widetilde{s}_{\widetilde{N}_\sigma 1}\widetilde{s}_{\widetilde{N}_\sigma 2})}_{\widetilde{s}_{N_\sigma}}}^{\widetilde{N}_\sigma} && \begin{matrix}\forall\sigma \in A_n \Rightarrow N_\sigma \in 2\mathbb{Z}_{\geq 0}\\ \forall\widetilde{\sigma} \in A_n \Rightarrow \widetilde{N}_\sigma \in 2\mathbb{Z}_{\geq 0}\end{matrix}\\
&= \overbrace{\underbrace{(s_{11}s_{12})}_{s_1}\cdots\underbrace{(s_{N_\sigma 1}s_{N_\sigma 2})}\underbrace{(\widetilde{s}_{11}\widetilde{s}_{12})}_{\substack{\widetilde{s}_1\\ s_{N_\sigma}}}\cdots\underbrace{(\widetilde{s}_{\widetilde{N}_\sigma 1}\widetilde{s}_{\widetilde{N}_\sigma 2})}_{\widetilde{s}_{N_\sigma}}}^{N_\sigma+\widetilde{N}_\sigma} && N_\sigma + \widetilde{N}_\sigma \in 2\mathbb{Z}_{\geq 0}\\
&\in A_n\\
\sigma^{-1} = \overline{\sigma} &= \overline{\overbrace{\underbrace{(s_{11}s_{12})}_{s_1}\cdots\underbrace{(s_{N_\sigma 1}s_{N_\sigma 2})}_{s_{N_\sigma}}}^{N_\sigma}} = \overbrace{\underbrace{(s_{N_\sigma 2}s_{N_\sigma 1})}_{\overline{s}_{N_\sigma}}\cdots\underbrace{(s_{12}s_{11})}_{\overline{s}_1}}^{N_\sigma} && \forall\sigma \in A_n \Rightarrow N_\sigma \in 2\mathbb{Z}_{\geq 0}\\
&\in A_n\\
&\Downarrow\\
A_n &\leq S_n
\end{aligned}
$$

定理 4.2. *finite cyclic subgroup*

$$
\begin{aligned}
(G, \cdot_G) = (G, \cdot) = G & \textit{ is a group}\\
|G| < \infty & \qquad G \textit{ is a finite group}\\
g \in G &\\
\langle g\rangle = \{g^n | n \in \mathbb{N}\} & \qquad \forall g \in G\\
\Downarrow &\\
\langle g\rangle \leq G & \qquad \langle g\rangle \textit{ is a finite cyclic subgroup of } G\textit{, generated by } g \in G
\end{aligned}
$$

Proof. $g = e = e_G$,

$$\langle e\rangle = \{e\} = \{e_G\} \leq G \quad \text{is one of trivial subgroups}$$

$g \neq e = e_G$,

$$\begin{aligned}
\langle g\rangle &= \{g^n | n \in \mathbb{N}\} = \{g^1, g^2, \cdots\} = \{g, g^2, \cdots, g^n, \cdots\} && n \in \mathbb{N} \\
&\subseteq G && g^n \in G \\
|\langle g\rangle| &\leq |G| < \infty && \Rightarrow |\langle g\rangle| < \infty \\
\langle g\rangle &: \mathbb{N} \to G && \Leftrightarrow \langle g\rangle \in G^{\mathbb{N}}
\end{aligned}$$

$$\Downarrow \text{pigeonhole principle} = \text{Dirichlet drawer principle} \qquad \Leftarrow |\mathbb{N}| \not< \infty \wedge \begin{matrix} |G| < \infty \\ |\langle g\rangle| < \infty \end{matrix}$$

$$\exists n_1 \neq n_2 \left[g^{n_1} = g^{n_2} \right] \qquad n_1, n_2 \in \mathbb{N}$$

$$\Downarrow \text{without loss of generality, let } n_1 < n_2$$

$$\exists n_1 < n_2 \left[g^{n_2} = g^{n_1} \right]$$

$$\begin{aligned}
& g^{n_2}\overline{g^{n_1}} = g^{n_1}\overline{g^{n_1}} = g^{n_1}g^{-n_1} = g^{n_1-n_1} = g^0 = e = e_G && \forall G \text{ is a group}, \forall g^{n_2} \in G, \exists \overline{g^{n_2}} \in G \\
&= g^{n_2}g^{-n_1} = g^{n_2-n_1} = g^{|n_2-n_1|} && n_1 < n_2 \Rightarrow 0 < n_2 - n_1 = |n_2 - n_1| \\
& g^{|n_2-n_1|} = e \\
& \downarrow \\
& \operatorname{ord}\langle g\rangle \overset{\text{def.}}{=} \min\{|n_2 - n_1|\} \in \mathbb{N} && \min\{|n_2-n_1|\} \text{ is the order of } \langle g\rangle \\
& \langle g\rangle = \left\{g^1, g^2, \cdots, g^{\operatorname{ord}\langle g\rangle}, \cdots\right\} = \{g, g^2, \cdots, e, \cdots\} && g^{\operatorname{ord}\langle g\rangle} = e
\end{aligned}$$

$$\begin{aligned}
\langle g\rangle &= \left\{g^1, g^2, \cdots, g^{\operatorname{ord}\langle g\rangle-1}, g^{\operatorname{ord}\langle g\rangle}, g^{\operatorname{ord}\langle g\rangle+1}, \cdots\right\} = \{g, g^2, \cdots, \overline{g}, e, g, \cdots\} \\
&= \left\{g^1, g^2, \cdots, g^{\operatorname{ord}\langle g\rangle-1}, g^{\operatorname{ord}\langle g\rangle}\right\} = \{g, g^2, \cdots, \overline{g}, e\}
\end{aligned}$$

$$\exists \overline{g^k} = g^{\operatorname{ord}\langle g\rangle-k} \left[g^k g^{\operatorname{ord}\langle g\rangle-k} = g^{k+\operatorname{ord}\langle g\rangle-k} = g^{\operatorname{ord}\langle g\rangle} = e \right], \forall k \in \{1, \cdots, \operatorname{ord}\langle g\rangle\} = \mathbb{N}_{\leq \operatorname{ord}\langle g\rangle}$$

$$\begin{aligned}
\langle g\rangle &\subseteq G \\
g^{n_1}g^{n_2} &= g^{n_1+n_2} \in \langle g\rangle && \forall n_1, n_2 \in \mathbb{N}\,[n_1 + n_2 \in \mathbb{N}] \\
\exists \overline{g^k} = g^{\operatorname{ord}\langle g\rangle-k} \Big[\overline{g^k}g^k &= g^{\operatorname{ord}\langle g\rangle-k}g^k = g^{\operatorname{ord}\langle g\rangle} = e \Big] && \forall k \in \{1, \cdots, \operatorname{ord}\langle g\rangle\} = \mathbb{N}_{\leq \operatorname{ord}\langle g\rangle} \\
&\Downarrow \\
\langle g\rangle &\leq G
\end{aligned}$$

□

定義 4.3. order of a group element

$$\forall g \in G \text{ is a group}, \forall m \in \mathbb{N}\,[g^m = e = e_G \Rightarrow \exists!\min\{m\} \in \mathbb{N}\,[\operatorname{ord} g = \min\{m\}]]$$

$$\begin{aligned}
\langle g\rangle &= \left\{g^1, g^2, \cdots, g^{\operatorname{ord}\langle g\rangle-1}, g^{\operatorname{ord}\langle g\rangle}, g^{\operatorname{ord}\langle g\rangle+1}, \cdots\right\} = \{g, g^2, \cdots, \overline{g}, e, g, \cdots\} \\
&= \left\{g^1, g^2, \cdots, g^{\operatorname{ord}\langle g\rangle-1}, g^{\operatorname{ord}\langle g\rangle}\right\} = \{g, g^2, \cdots, \overline{g}, e\} \\
&= \{g, g^2, \cdots, e\} = \left\{g, g^2, \cdots, g^{\min\{m\}}\right\} = \{g, g^2, \cdots, g^{\operatorname{ord} g}\} \\
|\langle g\rangle| &= \left|\{g, g^2, \cdots, g^{\operatorname{ord} g}\}\right| = \left|\left\{g, g^2, \cdots, g^{\operatorname{ord}\langle g\rangle}\right\}\right| \\
&= \operatorname{ord} g = \operatorname{ord}\langle g\rangle && \langle g\rangle \neq \emptyset = \{\} \\
\operatorname{ord}\langle g\rangle &= \operatorname{ord} g = |\langle g\rangle| \in \mathbb{N} && |\langle g\rangle| \in \mathbb{N} \neq \mathbb{Z}_{\geq 0}
\end{aligned}$$

$\mathbb{Z}_4$

$$\begin{aligned}
\mathbb{Z}_4 &= \{0, 1, 2, 3\} && = \mathbb{Z}_{[0,4)} = (\mathbb{Z}_4, +_{\mathbb{Z}_n}) \\
&= \{e, g, g^2, g^3\} && = (\mathbb{Z}_4, \cdot) = (\mathbb{Z}_4, \cdot_G) \\
&= \{g, g^2, g^3, e\} \\
&= \{g^1, g^2, g^3, g^4\} = \langle g\rangle && g^4 = e \\
&= \{a^1, a^2, a^3, a^4\} \\
&= \{a^1, a^2, a^3, e\} && a^4 = e \\
&= \{e, a, a^2, a^3\}
\end{aligned}$$

ord

$$
\begin{array}{llllll}
g = e & g^1 = e^1 = e & \mathrm{ord} g = \mathrm{ord} e = 1 & & & \\
\prec & & & & & \\
g \neq e & g^1 = g \neq e & g^2 \neq e & g^3 \neq e & g^4 = e & \mathrm{ord} g = 4 \\
g^2 \neq e & \left(g^2\right)^1 = g^2 \neq e & \left(g^2\right)^2 = g^4 = e & \mathrm{ord} g^2 = 2 & & \\
g^3 \neq e & \left(g^3\right)^1 = g^3 \neq e & \begin{aligned} \left(g^3\right)^2 &= g^6 \\ &= g^4 g^2 \\ &= e g^2 \\ &= g^2 \neq e \end{aligned} & \begin{aligned} \left(g^3\right)^3 &= g^9 \\ &= \left(g^4\right)^2 g \\ &= e^2 g \\ &= e g \\ &= g \neq e \end{aligned} & \begin{aligned} \left(g^3\right)^4 &= \left(g^4\right)^3 \\ &= e^3 = e \end{aligned} & \mathrm{ord} g^3 = 4 \\
\prec & & & & & \\
g^4 = e & \left(g^4\right)^1 = e^1 = e & \mathrm{ord} g^4 = \mathrm{ord} e = 1 & & &
\end{array}
$$

$$
\mathrm{ord} \langle g \rangle = |\langle g \rangle| = \mathrm{ord} g = \begin{cases} 1 & g = e \\ \begin{cases} 2 & g^2 = e \\ 4 & g^2 \neq e \end{cases} & g \neq e \end{cases}
$$

定理 4.4. *subgroup intersection*

$$
\begin{aligned} H_1 &\leq G \\ H_2 &\leq G \end{aligned} \Leftrightarrow H_1, H_2 \leq G \Rightarrow H_1 \cap H_2 \leq G \Leftrightarrow (H_1 \cap H_2) \leq G
$$

定義 4.5. central subgroup

$$
C(G) = \left\{ c \middle| \begin{aligned} & & c \in G \\ cg &= gc & \forall g \in G \end{aligned} \right\}
$$

$C(G) \leq G$

$\forall c_1, c_2 \in C(G) = (C(G), \cdot) = (C(G), \cdot_G)\, [c_1 c_2 \in C(G)]$

$$
\begin{aligned}
c_1 c_2 g &\overset{c_2 \in C(G)}{=} c_1 g c_2 \overset{c_1 \in C(G)}{=} g c_1 c_2 & \forall g \in G, \forall c_1, c_2 \in C(G) \\
c_1 c_2 g &= g c_1 c_2 & \\
(c_1 c_2) g &= g (c_1 c_2) & \Rightarrow c_1 c_2 \in C(G) \\
&\Downarrow & \\
c_1 c_2 &\in C(G) & \forall c_1, c_2 \in C(G)
\end{aligned}
$$

$$
\begin{array}{lr}
\overline{c} c = e = e_G & \forall g \in G, \forall c \in C(G), \exists \overline{c} = c^{-1} \in G \\
\overline{c} g \overline{g} c = (\overline{c} g)(\overline{g} c) = \overline{c} (g \overline{g}) c = \overline{c} e c = \overline{c} c = e & \Rightarrow \left(g^{-1} c\right)^{-1} = \overline{\overline{g} c} = \overline{(\overline{g} c)} = \overline{c} g = c^{-1} g \quad (1) \\
g \overline{c} c \overline{g} = (g \overline{c})(c \overline{g}) = g (\overline{c} c) \overline{g} = g e \overline{g} = g \overline{g} = e & \Rightarrow \left(c g^{-1}\right)^{-1} = \overline{c \overline{g}} = \overline{(c \overline{g})} = g \overline{c} = g c^{-1} \quad (2) \\
\overline{c} g \overset{(1)}{=} \overline{\overline{g} c} \overset{\overline{g} c = c \overline{g}}{=} \overline{c \overline{g}} \overset{(2)}{=} g \overline{c} & \because c \in C(G), \overline{g} \in G \therefore \overline{g} c = c \overline{g} \\
\overline{c} g = g \overline{c} & \Rightarrow \overline{c} \in C(G) \\
\Downarrow & \\
\overline{c} \in C(G) & \forall c \in C(G)
\end{array}
$$

$$
\begin{aligned}
C(G) = \left\{ c \middle| \begin{aligned} & & c \in G \\ cg &= gc & \forall g \in G \end{aligned} \right\} &\subseteq G & C(G) \subseteq G \\
c_1 c_2 &\in C(G) & \forall c_1, c_2 \in C(G) \\
\overline{c} &\in C(G) & \forall c \in C(G) \\
&\Downarrow & \\
C(G) &\leq G &
\end{aligned}
$$

5 coset

定義 5.1. left coset

$$
\begin{aligned}
H &\leq G & G \text{ is a group} \\
&\Downarrow & \\
gH &\overset{\text{def.}}{=} \{gh | h \in H\} & \forall g \in G \\
&\Updownarrow & \\
gH &\text{ is a left coset of } G &
\end{aligned}
$$

$$gH = \{gh | h \in H \le G\} \qquad G \text{ is a group} \quad \forall g \in G$$

定義 5.2. right coset

$$\begin{aligned} &H \le G && G \text{ is a group} \\ &\Downarrow && \\ &Hg \overset{\text{def.}}{=} \{hg | h \in H\} && \forall g \in G \\ &\Updownarrow && \\ &Hg \text{ is a right coset of } G && \end{aligned}$$

$$Hg = \{hg | h \in H \le G\} \qquad G \text{ is a group} \quad \forall g \in G$$

$\mathbb{Z}_2 \le \mathbb{Z}_4$

$$\begin{aligned}
\mathbb{Z}_4 &= \{0, 1, 2, 3\} && = \mathbb{Z}_{[0,4)} = (\mathbb{Z}_4, +_{\mathbb{Z}_n}) \\
&= \{e, g, g^2, g^3\} && = (\mathbb{Z}_4, \cdot) = (\mathbb{Z}_4, \cdot_G) \\
&= \{g, g^2, g^3, e\} && \\
&= \{g^1, g^2, g^3, g^4\} = \langle g \rangle && g^4 = e \\
&= \{a^1, a^2, a^3, a^4\} && \\
&= \{a^1, a^2, a^3, e\} && a^4 = e \\
&= \{e, a, a^2, a^3\} \supset \{e, a^2\} = (\mathbb{Z}_2, \cdot) = (\mathbb{Z}_2, \cdot_G) && = \mathbb{Z}_2 \\
\mathbb{Z}_2 \le \mathbb{Z}_4 \Rightarrow \mathbb{Z}_2 &= \{e, a^2\} && \\
e\mathbb{Z}_2 &= \{ee, ea^2\} = \{e, a^2\} && = \mathbb{Z}_2 \\
a\mathbb{Z}_2 &= \{ae, aa^2\} = \{a, a^3\} && = a\mathbb{Z}_2 \\
a^2\mathbb{Z}_2 &= \{a^2e, a^2a^2\} = \{a^2, a^4\} = \{a^2, e\} = \{e, a^2\} && = \mathbb{Z}_2 \\
a^3\mathbb{Z}_2 &= \{a^3e, a^3a^2\} = \{a^3, a^5\} = \{a^3, a\} = \{a, a^3\} && = a\mathbb{Z}_2 \\
a^4\mathbb{Z}_2 &= e\mathbb{Z}_2 = \{e, a^2\} && = \mathbb{Z}_2 \\
\mathbb{Z}_4\mathbb{Z}_2 &= \{g\mathbb{Z}_2 | g \in \mathbb{Z}_4\} && \\
&= \{e\mathbb{Z}_2, a\mathbb{Z}_2, a^2\mathbb{Z}_2, a^3\mathbb{Z}_2\} && \\
&= \{\mathbb{Z}_2, a\mathbb{Z}_2\} &&
\end{aligned}$$

$C_3 = \mathbb{Z}_3 \le D_3 = S_3$

$$\begin{array}{ccccccc}
\cdot_{D_3} & \rho_0 & \rho_1 & \rho_2 & \pi_0 & \pi_1 & \pi_2 \\
\rho_0 & \rho_0 & \rho_1 & \rho_2 & \pi_0 & \pi_1 & \pi_2 \\
\rho_1 & \rho_1 & \rho_2 & \rho_0 & \pi_1 & \pi_2 & \pi_0 \\
\rho_2 & \rho_2 & \rho_0 & \rho_1 & \pi_2 & \pi_0 & \pi_1 \\
\pi_0 & \pi_0 & \pi_2 & \pi_1 & \rho_0 & \rho_2 & \rho_1 \\
\pi_1 & \pi_1 & \pi_0 & \pi_2 & \rho_1 & \rho_0 & \rho_2 \\
\pi_2 & \pi_2 & \pi_1 & \pi_0 & \rho_2 & \rho_1 & \rho_0
\end{array}
\xrightarrow{e=\rho_0}
\begin{array}{ccccccc}
\cdot_{D_3} & e & \rho_1 & \rho_2 & \pi_0 & \pi_1 & \pi_2 \\
e & e & \rho_1 & \rho_2 & \pi_0 & \pi_1 & \pi_2 \\
\rho_1 & \rho_1 & \rho_2 & e & \pi_1 & \pi_2 & \pi_0 \\
\rho_2 & \rho_2 & e & \rho_1 & \pi_2 & \pi_0 & \pi_1 \\
\pi_0 & \pi_0 & \pi_2 & \pi_1 & e & \rho_2 & \rho_1 \\
\pi_1 & \pi_1 & \pi_0 & \pi_2 & \rho_1 & e & \rho_2 \\
\pi_2 & \pi_2 & \pi_1 & \pi_0 & \rho_2 & \rho_1 & e
\end{array}$$

$$e \ne \rho = \rho^1 = \rho_1 \downarrow \rho^2 = (\rho_1)^2 = \rho_2$$

$$\begin{array}{ccccccc}
+_{\mathbb{Z}_3} & 0 & 1 & 2 & \pi_0 & \pi_1 & \pi_2 \\
0 & 0 & 1 & 2 & \pi_0 & \pi_1 & \pi_2 \\
1 & 1 & 2 & 0 & \pi_1 & \pi_2 & \pi_0 \\
2 & 2 & 0 & 1 & \pi_2 & \pi_0 & \pi_1 \\
\pi_0 & \pi_0 & \pi_2 & \pi_1 & e & \rho^2 & \rho \\
\pi_1 & \pi_1 & \pi_0 & \pi_2 & \rho & e & \rho^2 \\
\pi_2 & \pi_2 & \pi_1 & \pi_0 & \rho^2 & \rho & e
\end{array}
\xleftarrow{\mathbb{Z}_3 \le D_3}
\begin{array}{ccccccc}
\cdot_{D_3} & e & \rho & \rho^2 & \pi_0 & \pi_1 & \pi_2 \\
e & e & \rho & \rho^2 & \pi_0 & \pi_1 & \pi_2 \\
\rho & \rho & \rho^2 & e & \pi_1 & \pi_2 & \pi_0 \\
\rho^2 & \rho^2 & e & \rho & \pi_2 & \pi_0 & \pi_1 \\
\pi_0 & \pi_0 & \pi_2 & \pi_1 & e & \rho^2 & \rho \\
\pi_1 & \pi_1 & \pi_0 & \pi_2 & \rho & e & \rho^2 \\
\pi_2 & \pi_2 & \pi_1 & \pi_0 & \rho^2 & \rho & e
\end{array}$$

$$D_3 = \left\{ \begin{array}{c|c} \begin{array}{c} \rho_{k,n} \\ \pi_{k,n} \end{array} & \begin{array}{l} \rho_{k,n} = \begin{bmatrix} +\cos\frac{2\pi}{n}k & -\sin\frac{2\pi}{n}k \\ +\sin\frac{2\pi}{n}k & +\cos\frac{2\pi}{n}k \end{bmatrix} \\ \pi_{k,n} = \begin{bmatrix} +\cos\frac{2\pi}{n}k & +\sin\frac{2\pi}{n}k \\ +\sin\frac{2\pi}{n}k & -\cos\frac{2\pi}{n}k \end{bmatrix} \end{array} \quad \forall k \in \mathbb{Z}_{[0,3)} \end{array} \right\} \qquad n = 3$$

$$= \{\rho_0, \rho_1, \rho_2, \pi_0, \pi_1, \pi_2\} \qquad = (D_3, \cdot) = (D_3, \cdot_G)$$

$$= \{e, \rho_1, \rho_2, \pi_0, \pi_1, \pi_2\} \qquad e = \rho_0$$

$$= \{e, \rho, \rho^2, \pi_0, \pi_1, \pi_2\} \supset \{e, \rho, \rho^2\} = \mathbb{Z}_3 \qquad e \neq \rho = \rho^1 = \rho_1, \quad \rho^2 = (\rho_1)^2 = \rho_2$$

$$\mathbb{Z}_3 \leq D_3 \Rightarrow \mathbb{Z}_3 = \{0, 1, 2\} \qquad = \mathbb{Z}_{[0,3)} = (\mathbb{Z}_3, +_{\mathbb{Z}_n})$$

$$= \{e, g, g^2\} \qquad = (\mathbb{Z}_4, \cdot) = (\mathbb{Z}_4, \cdot_G)$$

$$= \{g, g^2, e\}$$

$$= \{g^1, g^2, g^3\} = \langle g \rangle \qquad g^3 = e$$

$$= \{a^1, a^2, a^3\}$$

$$= \{a^1, a^2, e\} \qquad a^3 = e$$

$$= \{e, a, a^2\}$$

$$= \{e, \rho, \rho^2\} = (\mathbb{Z}_3, \cdot_{D_3}) \subset D_3 \qquad \rho^3 = e$$

$$C_3 = \mathbb{Z}_3 = \{e, \rho, \rho^2\} \subset D_3$$

$$e\mathbb{Z}_3 = \{ee, e\rho, e\rho^2\} = \{e, \rho, \rho^2\} \qquad = \mathbb{Z}_3$$

$$\rho\mathbb{Z}_3 = \{\rho e, \rho\rho, \rho\rho^2\} = \{\rho, \rho^2, \rho^3\} = \{\rho, \rho^2, e\} = \{e, \rho, \rho^2\} \qquad = \mathbb{Z}_3$$

$$\rho^2\mathbb{Z}_3 = \{\rho^2 e, \rho^2\rho, \rho^2\rho^2\} = \{\rho^2, \rho^3, \rho^4\} = \{\rho^2, e, \rho\} = \{e, \rho, \rho^2\} \qquad = \mathbb{Z}_3$$

$$\rho^3\mathbb{Z}_3 = e\mathbb{Z}_3 = \{e, \rho, \rho^2\} \qquad = \mathbb{Z}_3$$

$$\pi_0\mathbb{Z}_3 = \{\pi_0 e, \pi_0\rho, \pi_0\rho^2\} = \{\pi_0\rho_0, \pi_0\rho_1, \pi_0\rho_2\} \qquad \pi_i\rho_j = \pi_{i-j}, \quad \pi_i = \pi_{3+i}$$

$$= \{\pi_0, \pi_{-1}, \pi_{-2}\} = \{\pi_0, \pi_2, \pi_1\} = \{\pi_0, \pi_1, \pi_2\} \qquad = \pi_0\mathbb{Z}_3$$

$$\pi_1\mathbb{Z}_3 = \{\pi_1 e, \pi_1\rho, \pi_1\rho^2\} = \{\pi_1\rho_0, \pi_1\rho_1, \pi_1\rho_2\}$$

$$= \{\pi_1, \pi_0, \pi_{-1}\} = \{\pi_1, \pi_0, \pi_2\} = \{\pi_0, \pi_1, \pi_2\} \qquad = \pi_0\mathbb{Z}_3$$

$$\pi_2\mathbb{Z}_3 = \{\pi_2 e, \pi_2\rho, \pi_2\rho^2\} = \{\pi_2\rho_0, \pi_2\rho_1, \pi_2\rho_2\}$$

$$= \{\pi_2, \pi_1, \pi_0\} = \{\pi_0, \pi_1, \pi_2\} \qquad = \pi_0\mathbb{Z}_3$$

$$D_3\mathbb{Z}_3 = \{g\mathbb{Z}_3 | g \in D_3\}$$

$$= \{e\mathbb{Z}_3, \rho\mathbb{Z}_3, \rho^2\mathbb{Z}_3, \pi_0\mathbb{Z}_3, \pi_1\mathbb{Z}_3, \pi_2\mathbb{Z}_3\}$$

$$= \{\mathbb{Z}_3, \pi_0\mathbb{Z}_3\}$$

$$= \{e\mathbb{Z}_3, \pi_i\mathbb{Z}_3\} \qquad i \in \{0, 1, 2\} = \mathbb{Z}_{[0,3)}$$

$4\mathbb{Z} \leq \mathbb{Z}$

$$\begin{aligned}
\mathbb{Z} =& \{\cdots, -3, -2, -1, 0, +1, +2, +3, \cdots\} = \{k|k \in \mathbb{Z}\} \\
4\mathbb{Z} =& \{\cdots, -12, -8, -4, 0, +4, +8, +12, \cdots\} = \{4k|k \in \mathbb{Z}\} \\
4\mathbb{Z} \subset& \mathbb{Z} \\
4k_1 + 4k_2 =& 4(k_1 + k_2) \in 4\mathbb{Z} \\
-4k = \overline{4k} =& 4(-k) \in 4\mathbb{Z} \\
& \Downarrow \\
4\mathbb{Z} \leq& \mathbb{Z}
\end{aligned}$$

$$\begin{aligned}
5 + 4\mathbb{Z} =& \{\cdots, 5 + (-12), 5 + (-8), 5 + (-4), 5 + 0, 5 + 4, 5 + 8, 5 + 12, \cdots\} \\
=& \{\cdots, -7, -3, 1, 5, 9, 13, 17, \cdots\} && = 1 + 4\mathbb{Z} \\
4 + 4\mathbb{Z} =& \{\cdots, 4 + (-12), 4 + (-8), 4 + (-4), 4 + 0, 4 + 4, 4 + 8, 4 + 12, \cdots\} \\
=& \{\cdots, -8, -4, 0, 4, 8, 12, 16, \cdots\} && = 0 + 4\mathbb{Z} \\
3 + 4\mathbb{Z} =& \{\cdots, 3 + (-12), 3 + (-8), 3 + (-4), 3 + 0, 3 + 4, 3 + 8, 3 + 12, \cdots\} \\
=& \{\cdots, -9, -5, -1, 3, 7, 11, 15, \cdots\} && = -3 + 4\mathbb{Z} \\
2 + 4\mathbb{Z} =& \{\cdots, 2 + (-12), 2 + (-8), 2 + (-4), 2 + 0, 2 + 4, 2 + 8, 2 + 12, \cdots\} \\
=& \{\cdots, -10, -6, -2, 2, 6, 10, 14, \cdots\} && = -2 + 4\mathbb{Z} \\
1 + 4\mathbb{Z} =& \{\cdots, 1 + (-12), 1 + (-8), 1 + (-4), 1 + 0, 1 + 4, 1 + 8, 1 + 12, \cdots\} \\
=& \{\cdots, -11, -7, -3, 1, 5, 9, 13, \cdots\} && = -1 + 4\mathbb{Z} \\
0 + 4\mathbb{Z} =& \{\cdots, 0 + (-12), 0 + (-8), 0 + (-4), 0 + 0, 0 + 4, 0 + 8, 0 + 12, \cdots\} \\
=& \{\cdots, -12, -8, -4, 0, 4, 8, 12, \cdots\} && = 4\mathbb{Z} \\
-1 + 4\mathbb{Z} =& \{\cdots, -1 + (-12), -1 + (-8), -1 + (-4), -1 + 0, -1 + 4, -1 + 8, -1 + 12, \cdots\} \\
=& \{\cdots, -13, -9, -5, -1, 3, 7, 11, \cdots\} && = 3 + 4\mathbb{Z} \\
-2 + 4\mathbb{Z} =& \{\cdots, -2 + (-12), -2 + (-8), -2 + (-4), -2 + 0, -2 + 4, -2 + 8, -2 + 12, \cdots\} \\
=& \{\cdots, -14, -10, -6, -2, 2, 6, 10, \cdots\} && = 2 + 4\mathbb{Z} \\
-3 + 4\mathbb{Z} =& \{\cdots, -3 + (-12), -3 + (-8), -3 + (-4), -3 + 0, -3 + 4, -3 + 8, -3 + 12, \cdots\} \\
=& \{\cdots, -15, -11, -7, -3, 1, 5, 9, \cdots\} && = 1 + 4\mathbb{Z} \\
-4 + 4\mathbb{Z} =& \{\cdots, -4 + (-12), -4 + (-8), -4 + (-4), -4 + 0, -4 + 4, -4 + 8, -4 + 12, \cdots\} \\
=& \{\cdots, -16, -12, -8, -4, 0, 4, 8, \cdots\} && = 0 + 4\mathbb{Z} \\
-5 + 4\mathbb{Z} =& \{\cdots, -5 + (-12), -5 + (-8), -5 + (-4), -5 + 0, -5 + 4, -5 + 8, -5 + 12, \cdots\} && = -1 + 4\mathbb{Z} \\
=& \{\cdots, -17, -13, -9, -5, -1, 3, 7, \cdots\} \\
& \vdots
\end{aligned}$$

$$\begin{array}{ccccccccc}
\{\cdots, -8, -4, +0, +4, +8, \cdots\} & + & 4\mathbb{Z} & = & \{4 + 4\mathbb{Z}\} & = & \{0 + 4\mathbb{Z}\} & = & \{4\mathbb{Z}\} \\
\cup & & & & \cup \\
\{\cdots, -9, -5, -1, +3, +7, \cdots\} & + & 4\mathbb{Z} & = & \{3 + 4\mathbb{Z}\} \\
\cup & & & & \cup \\
\{\cdots, -10, -6, -2, +2, +6, \cdots\} & + & 4\mathbb{Z} & = & \{2 + 4\mathbb{Z}\} \\
\cup & & & & \cup \\
\{\cdots, -11, -7, -3, +1, +5, \cdots\} & + & 4\mathbb{Z} & = & \{1 + 4\mathbb{Z}\} \\
\| & & & & \| \\
\mathbb{Z} & + & 4\mathbb{Z} & = & \left\{ \begin{array}{c} 4\mathbb{Z}, \\ 1 + 4\mathbb{Z}, \\ 2 + 4\mathbb{Z}. \\ 3 + 4\mathbb{Z} \end{array} \right\}
\end{array}$$

$$\begin{aligned}
\mathbb{Z} + 4\mathbb{Z} =& \{k + 4\mathbb{Z}|k \in \mathbb{Z}\} = \{4\mathbb{Z}, 1 + 4\mathbb{Z}, 2 + 4\mathbb{Z}.3 + 4\mathbb{Z}\} \\
=& \{\cdots, -3 + 4\mathbb{Z}, -2 + 4\mathbb{Z}, -1 + 4\mathbb{Z}, 0 + 4\mathbb{Z}, 1 + 4\mathbb{Z}, 2 + 4\mathbb{Z}, 3 + 4\mathbb{Z}, \cdots\}
\end{aligned}$$

L_g: left shift

$$H \overset{L_g}{\to} gH$$

定理 5.3. *according to the rearrangement theorem*

$$\begin{aligned} H \leq& G \\ H =& G \end{aligned} \Rightarrow gH = H \quad \forall g \in G$$

定理 5.4.

$$H \le G \Rightarrow hH = H \quad \forall h \in H$$

$$H \le G \Rightarrow gH = H \quad \forall g \in H$$

$$H \le G \Rightarrow \{\forall g \in H\,[gH = H]\}$$

$$\begin{array}{ccc} g \in H \Rightarrow gH = H & \Leftrightarrow & gH \ne H \Rightarrow g \notin H \\ & \text{let } H \le G & \\ gH = H \Rightarrow g \in H & \Leftrightarrow & g \notin H \Rightarrow gH \ne H \\ g \cdot e = ge \in H & & \end{array}$$

$$\begin{array}{c} H \le G \\ \Downarrow \\ g \in H \Leftrightarrow gH = H \\ \Updownarrow \\ g \notin H \Leftrightarrow gH \ne H \end{array}$$

定理 5.5.

$$\begin{array}{ccc} H \le G & \wedge & g_1, g_2 \in G \\ & \Downarrow & \\ g_1H = g_2H & \Leftrightarrow & \overline{g}_2 g_1 \in H \\ & \Updownarrow & \\ g_1H \ne g_2H & \Leftrightarrow & \overline{g}_2 g_1 \notin H \end{array}$$

Proof.

$$\begin{aligned} g_1H &= g_2H & \exists e = e_H = e_G \in H \subseteq G \\ g_1 = g_1 \cdot e = g_1 e &= g_2 h & \exists h \in H \\ g_1 &= g_2 h & \\ \overline{g}_2 g_1 &= \overline{g}_2 g_2 h = eh = h & \\ \overline{g}_2 g_1 &= h \in H & \overline{g}_2 g_1 \in H \end{aligned}$$

□

$$\overline{g_2} g_1 \in H \Rightarrow g_1H = g_2H$$

定理 5.6. *coset mutually exclusive theorem*

$$\begin{array}{ccc} H \le G & \wedge & g_1, g_2 \in G \\ & \Downarrow & \\ g_1H \ne g_2H & \Rightarrow & g_1H \cap g_2H = \emptyset \end{array}$$

Proof.

$$\begin{aligned} g_1H \cap g_2H &\ne \emptyset \\ &\Downarrow \\ \exists g_1h_1 = g_2h_2 &\in g_1H \cap g_2H \\ &\Downarrow \\ g_1h_1 &= g_2h_2 \\ g_1 = g_1e = g_1h_1\overline{h}_1 &= g_2h_2\overline{h}_1 \\ g_1 &= g_2h_2\overline{h}_1 \\ &\Downarrow \end{aligned}$$

$$\begin{aligned} g_1H = \{g_1h | h \in H\} &= \left\{g_2h_2\overline{h}_1h \middle| h \in H\right\} \\ &= \left\{g_2\left(h_2\overline{h}_1h\right) \middle| h \in H\right\} \qquad \widetilde{h} = h_2\overline{h}_1h \in H \\ &\overset{\text{rearrangement theorem}}{=} \left\{g_2\widetilde{h} \middle| \widetilde{h} \in H\right\} = g_2H \quad \Rightarrow\Leftarrow g_1H \ne g_2H \end{aligned}$$

□

定理 5.7. *coset partitioning group*

$$
\begin{aligned}
H \leq & G \\
g_j \in & G \\
& \Downarrow
\end{aligned}
$$

$$
\begin{aligned}
G = \bigcup_{g \in G} gH = \bigcup_{j} g_j H &= \begin{cases} \bigcup_{j=1}^{n} g_j H & |G| = n \in \mathbb{N} \\ \bigcup_{j \in J} g_j H & |G| = |J|, J \in \{\mathbb{N}, \mathbb{Z}, [0,1], \mathbb{R}, \cdots\} \end{cases} \\
&= \begin{cases} g_1 H \cup g_2 H \cup \cdots \cup g_n H & |G| = n \in \mathbb{N} \\ \bigcup_{j \in J} g_j H & |G| = |J|, J \in \{\mathbb{N}, \mathbb{Z}, [0,1], \mathbb{R}, \cdots\} \end{cases} && \exists m \in \mathbb{N}_{\leq n} [g_m = e = e_H = e_G] \\
&= \begin{cases} g_1 H \cup g_2 H \cup \cdots & |G| = n \in \mathbb{N} \\ \bigcup_{j \in J} g_j H & J \in \{\mathbb{N}, \mathbb{Z}, [0,1], \mathbb{R}, \cdots\} \end{cases} && \wedge g_i H \neq g_j H \Rightarrow g_i H \cap g_j H = \emptyset
\end{aligned}
$$

$\mathbb{Z}_2 \leq \mathbb{Z}_4$

$$
\begin{aligned}
\mathbb{Z}_4 &= \{0,1,2,3\} && = \mathbb{Z}_{[0,4)} = (\mathbb{Z}_4, +_{\mathbb{Z}_n}) \\
&= \{e, g, g^2, g^3\} && = (\mathbb{Z}_4, \cdot) = (\mathbb{Z}_4, \cdot_G) \\
&= \{g, g^2, g^3, e\} \\
&= \{g^1, g^2, g^3, g^4\} = \langle g \rangle && g^4 = e \\
&= \{a^1, a^2, a^3, a^4\} \\
&= \{a^1, a^2, a^3, e\} && a^4 = e \\
&= \{e, a, a^2, a^3\} \supset \{e, a^2\} = (\mathbb{Z}_2, \cdot) = (\mathbb{Z}_2, \cdot_G) && = \mathbb{Z}_2 \\
\mathbb{Z}_2 \leq \mathbb{Z}_4 \Rightarrow \mathbb{Z}_2 &= \{e, a^2\} \\
e\mathbb{Z}_2 &= \{ee, ea^2\} = \{e, a^2\} && = \mathbb{Z}_2 \\
a\mathbb{Z}_2 &= \{ae, aa^2\} = \{a, a^3\} && = a\mathbb{Z}_2 \\
a^2\mathbb{Z}_2 &= \{a^2 e, a^2 a^2\} = \{a^2, a^4\} = \{a^2, e\} = \{e, a^2\} && = \mathbb{Z}_2 \\
a^3\mathbb{Z}_2 &= \{a^3 e, a^3 a^2\} = \{a^3, a^5\} = \{a^3, a\} = \{a, a^3\} && = a\mathbb{Z}_2 \\
a^4\mathbb{Z}_2 &= e\mathbb{Z}_2 = \{e, a^2\} && = \mathbb{Z}_2 \\
\mathbb{Z}_4\mathbb{Z}_2 &= \{g\mathbb{Z}_2 | \forall g \in \mathbb{Z}_4\} \\
&= \{e\mathbb{Z}_2, a\mathbb{Z}_2, a^2\mathbb{Z}_2, a^3\mathbb{Z}_2\} \\
&= \{\mathbb{Z}_2, a\mathbb{Z}_2\}
\end{aligned}
$$

$$
\begin{aligned}
\mathbb{Z}_4 = \bigcup_{g \in \mathbb{Z}_4} g\mathbb{Z}_2 &= e\mathbb{Z}_2 \cup a\mathbb{Z}_2 \cup a^2\mathbb{Z}_2 \cup a^3\mathbb{Z}_2 && \begin{aligned} e\mathbb{Z}_2 = a^2\mathbb{Z}_2 &= \mathbb{Z}_2 \\ a\mathbb{Z}_2 = a^3\mathbb{Z}_2 &= a\mathbb{Z}_2 \end{aligned} \\
&= \mathbb{Z}_2 \cup a\mathbb{Z}_2 \\
&= e\mathbb{Z}_2 \cup a\mathbb{Z}_2 = e\mathbb{Z}_2 \cup a^3\mathbb{Z}_2 = a^2\mathbb{Z}_2 \cup a\mathbb{Z}_2 = a^2\mathbb{Z}_2 \cup a^3\mathbb{Z}_2
\end{aligned}
$$

$C_3 = \mathbb{Z}_3 \leq D_3 = S_3$

$$D_3 = \left\{ \begin{matrix} \rho_{k,n} \\ \pi_{k,n} \end{matrix} \middle| \begin{matrix} \rho_{k,n} = \begin{bmatrix} +\cos\frac{2\pi}{n}k & -\sin\frac{2\pi}{n}k \\ +\sin\frac{2\pi}{n}k & +\cos\frac{2\pi}{n}k \end{bmatrix} \\ \pi_{k,n} = \begin{bmatrix} +\cos\frac{2\pi}{n}k & +\sin\frac{2\pi}{n}k \\ +\sin\frac{2\pi}{n}k & -\cos\frac{2\pi}{n}k \end{bmatrix} \end{matrix} \quad \forall k \in \mathbb{Z}_{[0,3)} \right\} \qquad n = 3$$

$$= \{\rho_0, \rho_1, \rho_2, \pi_0, \pi_1, \pi_2\} \qquad = (D_3, \cdot) = (D_3, \cdot_G)$$

$$= \{e, \rho_1, \rho_2, \pi_0, \pi_1, \pi_2\} \qquad e = \rho_0$$

$$e \neq \rho = \rho^1 = \rho_1$$

$$= \{e, \rho, \rho^2, \pi_0, \pi_1, \pi_2\} \supset \{e, \rho, \rho^2\} = \mathbb{Z}_3$$

$$\rho^2 = (\rho_1)^2 = \rho_2$$

$$\mathbb{Z}_3 \leq D_3 \Rightarrow \mathbb{Z}_3 = \{0, 1, 2\} \qquad = \mathbb{Z}_{[0,3)} = (\mathbb{Z}_3, +_{\mathbb{Z}_n})$$

$$= \{e, g, g^2\} \qquad = (\mathbb{Z}_4, \cdot) = (\mathbb{Z}_4, \cdot_G)$$

$$= \{g, g^2, e\}$$

$$= \{g^1, g^2, g^3\} = \langle g \rangle \qquad g^3 = e$$

$$= \{a^1, a^2, a^3\}$$

$$= \{a^1, a^2, e\} \qquad a^3 = e$$

$$= \{e, a, a^2\}$$

$$= \{e, \rho, \rho^2\} = (\mathbb{Z}_3, \cdot_{D_3}) \subset D_3 \qquad \rho^3 = e$$

$$C_3 = \mathbb{Z}_3 = \{e, \rho, \rho^2\} \subset D_3$$

$$e\mathbb{Z}_3 = \{ee, e\rho, e\rho^2\} = \{e, \rho, \rho^2\} \qquad = \mathbb{Z}_3$$

$$\rho\mathbb{Z}_3 = \{\rho e, \rho\rho, \rho\rho^2\} = \{\rho, \rho^2, \rho^3\} = \{\rho, \rho^2, e\} = \{e, \rho, \rho^2\} \qquad = \mathbb{Z}_3$$

$$\rho^2\mathbb{Z}_3 = \{\rho^2 e, \rho^2\rho, \rho^2\rho^2\} = \{\rho^2, \rho^3, \rho^4\} = \{\rho^2, e, \rho\} = \{e, \rho, \rho^2\} \qquad = \mathbb{Z}_3$$

$$\rho^3\mathbb{Z}_3 = e\mathbb{Z}_3 = \{e, \rho, \rho^2\} \qquad = \mathbb{Z}_3$$

$$\pi_i\rho_j = \pi_{i-j}$$

$$\pi_0\mathbb{Z}_3 = \{\pi_0 e, \pi_0\rho, \pi_0\rho^2\} = \{\pi_0\rho_0, \pi_0\rho_1, \pi_0\rho_2\}$$

$$\pi_i = \pi_{3+i}$$

$$= \{\pi_0, \pi_{-1}, \pi_{-2}\} = \{\pi_0, \pi_2, \pi_1\} = \{\pi_0, \pi_1, \pi_2\} \qquad = \pi_0\mathbb{Z}_3$$

$$\pi_1\mathbb{Z}_3 = \{\pi_1 e, \pi_1\rho, \pi_1\rho^2\} = \{\pi_1\rho_0, \pi_1\rho_1, \pi_1\rho_2\}$$

$$= \{\pi_1, \pi_0, \pi_{-1}\} = \{\pi_1, \pi_0, \pi_2\} = \{\pi_0, \pi_1, \pi_2\} \qquad = \pi_0\mathbb{Z}_3$$

$$\pi_2\mathbb{Z}_3 = \{\pi_2 e, \pi_2\rho, \pi_2\rho^2\} = \{\pi_2\rho_0, \pi_2\rho_1, \pi_2\rho_2\}$$

$$= \{\pi_2, \pi_1, \pi_0\} = \{\pi_0, \pi_1, \pi_2\} \qquad = \pi_0\mathbb{Z}_3$$

$$D_3\mathbb{Z}_3 = \{g\mathbb{Z}_3 | g \in D_3\}$$

$$= \{e\mathbb{Z}_3, \rho\mathbb{Z}_3, \rho^2\mathbb{Z}_3, \pi_0\mathbb{Z}_3, \pi_1\mathbb{Z}_3, \pi_2\mathbb{Z}_3\}$$

$$= \{\mathbb{Z}_3, \pi_0\mathbb{Z}_3\}$$

$$= \{e\mathbb{Z}_3, \pi_i\mathbb{Z}_3\} \qquad i \in \{0, 1, 2\} = \mathbb{Z}_{[0,3)}$$

$$e\mathbb{Z}_3 = \rho\mathbb{Z}_3 = \rho^2\mathbb{Z}_3 = \mathbb{Z}_3$$

$$D_3 = \bigcup_{g \in D_3} g\mathbb{Z}_3 = e\mathbb{Z}_3 \cup \rho\mathbb{Z}_3 \cup \rho^2\mathbb{Z}_3 \cup \pi_0\mathbb{Z}_3 \cup \pi_1\mathbb{Z}_3 \cup \pi_2\mathbb{Z}_3$$

$$\pi_0\mathbb{Z}_3 = \pi_1\mathbb{Z}_3 = \pi_2\mathbb{Z}_3 = \pi_i\mathbb{Z}_3$$

$$= \mathbb{Z}_3 \cup \pi_i\mathbb{Z}_3 \qquad i \in \{0, 1, 2\} = \mathbb{Z}_{[0,3)}$$

$$= \cdots \qquad 3 \cdot 3 = 9 \text{ possibilities of combinations}$$

$$4\mathbb{Z} \leq \mathbb{Z}$$

$$\mathbb{Z} + 4\mathbb{Z} = \{k + 4\mathbb{Z} | k \in \mathbb{Z}\} = \{4\mathbb{Z}, 1 + 4\mathbb{Z}, 2 + 4\mathbb{Z}.3 + 4\mathbb{Z}\}$$
$$= \{\cdots, -3 + 4\mathbb{Z}, -2 + 4\mathbb{Z}, -1 + 4\mathbb{Z}, 0 + 4\mathbb{Z}, 1 + 4\mathbb{Z}, 2 + 4\mathbb{Z}, 3 + 4\mathbb{Z}, \cdots\}$$

$$\mathbb{Z} = \bigcup_{k \in \mathbb{Z}} (k + 4\mathbb{Z}) = (4\mathbb{Z}) \cup (1 + 4\mathbb{Z}) \cup (2 + 4\mathbb{Z}) \cup (3 + 4\mathbb{Z})$$

定理 5.8.

$$\begin{aligned} H \le & G \\ g \ne & e = e_H = e_G \\ gH = & \{gh \mid h \in H\} \quad \forall g \in G \\ & \Downarrow \\ |gH| = & |H| \end{aligned}$$

定理 5.9. *coset theorem = Langrange coset theorem = Lagrange theorem bridge between group theory and number theory*

$$\begin{aligned} H \le & G \\ |G| < & \infty \\ & & |gH| = |H| \\ & \Downarrow & G = \bigcup_{g \in G} gH \\ & & g_i H \ne g_j H \Rightarrow g_i H \cap g_j H = \emptyset \\ |G| / |H| \in \mathbb{N} & & \Rightarrow |H| \mid |G| \Leftrightarrow |G| = n|H| \quad n \in \mathbb{N} \end{aligned}$$

$$\begin{aligned} G & \text{ is a group} \\ |G| = & p \in \mathbb{P} \end{aligned} \Rightarrow \{H \mid H \le G\} = \{\{e\}, G\}$$

$$\begin{aligned} G & \text{ is a group} \\ |G| = & p \in \mathbb{P} \\ g \ne & e = e_G \\ \langle g \rangle = & \{g^n \mid n \in \mathbb{N}\} \\ & \Downarrow \\ \langle g \rangle \le & G \\ \langle g \rangle \in & \{H \mid H \le G\} = \{\{e\}, G\} \\ \langle g \rangle \ne & \{e\} \\ & \Downarrow \\ \langle g \rangle = & G \\ & \Downarrow \mathrm{ord} \langle g \rangle = |\langle g \rangle| \\ \mathrm{ord} \langle g \rangle = & \mathrm{ord} G \\ = & |\langle g \rangle| = |G| = p \in \mathbb{P} \\ \mathrm{ord} \langle g \rangle = & p \in \mathbb{P} \end{aligned}$$

5.1 left coset space

定義 5.10. indexed set

$$\begin{aligned} \{a_i\}_{i \in I} &= \{a_i \mid i \in I\} = \{\cdots, a_i, \cdots\} & i \in I \\ &= \bigcup_{i \in I} \{a_i\} & i \in I \\ &= \begin{cases} \bigcup_{i=1}^{n} \{a_i\} & \left|\{a_i\}_{i \in I}\right| = n \in \mathbb{N} \\ \bigcup_{i \in I} \{a_i\} & I \in \{\mathbb{N}, \mathbb{Z}, [0,1], \mathbb{R}, \cdots\} \end{cases} \end{aligned}$$

$$\begin{aligned} \{a_i\}_{i \in \mathbb{N}} &= \{a_i \mid i \in \mathbb{N}\} = \{a_1, a_2, \cdots, a_i, \cdots\} = \{a_1, a_2, a_3, \cdots\} & i \in \mathbb{N} \\ = \{a_n\}_{n \in \mathbb{N}} &= \{a_n \mid n \in \mathbb{N}\} = \{a_1, a_2, \cdots, a_n, \cdots\} = \{a_1, a_2, a_3, \cdots\} & n \in \mathbb{N} \\ &= \bigcup_{i \in \mathbb{N}} \{a_i\} = \bigcup_{n \in \mathbb{N}} \{a_n\} = \begin{cases} \bigcup_{i=1}^{n} \{a_i\} & \left|\{a_i\}_{i \in \mathbb{N}}\right| = n \in \mathbb{N} \\ \bigcup_{n \in \mathbb{N}} \{a_n\} & \left|\{a_i\}_{i \in \mathbb{N}}\right| = |\mathbb{N}| \end{cases} \\ \{a_i\}_{i=1}^{n} &= \bigcup_{i=1}^{n} \{a_i\} = \{a_1, a_2, \cdots, a_n\} = \{a_1, \cdots, a_n\} & \forall n \in \mathbb{N} \end{aligned}$$

$$
\begin{aligned}
\{a_i\}_{i\in\mathbb{Z}_{\geq 0}} &= \{a_i | i \in \mathbb{Z}_{\geq 0}\} = \{a_0, a_1, a_2, \cdots, a_i, \cdots\} = \{a_0, a_1, a_2, a_3, \cdots\} && i \in \mathbb{Z}_{\geq 0} \\
= \{a_k\}_{k\in\mathbb{Z}_{\geq 0}} &= \{a_k | k \in \mathbb{Z}_{\geq 0}\} = \{a_0, a_1, \cdots, a_k, \cdots\} = \{a_0, a_1, a_2, \cdots\} && k \in \mathbb{Z}_{\geq 0} \\
= \{a_\mu\}_{\mu\in\mathbb{Z}_{\geq 0}} &= \{a_\mu | \mu \in \mathbb{Z}_{\geq 0}\} = \{a_0, a_1, \cdots, a_\mu, \cdots\} = \{a_0, a_1, a_2, \cdots\} && \mu \in \mathbb{Z}_{\geq 0} \\
&= \bigcup_{i\in\mathbb{Z}_{\geq 0}} \{a_i\} = \bigcup_{\mu\in\mathbb{Z}_{\geq 0}} \{a_\mu\} = \begin{cases} \bigcup_{\mu=0}^{n-1} \{a_\mu\} & \left|\{a_\mu\}_{\mu\in\mathbb{Z}_{\geq 0}}\right| = n \in \mathbb{N} \\ \bigcup_{\mu\in\mathbb{Z}_{\geq 0}} \{a_\mu\} & \left|\{a_\mu\}_{\mu\in\mathbb{Z}_{\geq 0}}\right| = |\mathbb{Z}_{\geq 0}| = |\mathbb{N}| \end{cases}
\end{aligned}
$$

定義 5.11. indexed sequence

$$
\langle a_i \rangle_{i\in I} = \langle a_i | i \in I \rangle = \langle \cdots, a_i, \cdots \rangle \quad i \in I
$$

$$
\begin{aligned}
\langle a_i \rangle_{i\in\mathbb{N}} &= \langle a_i | i \in \mathbb{N} \rangle = \langle a_1, a_2, \cdots, a_i, \cdots \rangle = \langle a_1, a_2, a_3, \cdots \rangle && i \in \mathbb{N} \\
= \langle a_n \rangle_{n\in\mathbb{N}} &= \langle a_n | n \in \mathbb{N} \rangle = \langle a_1, a_2, \cdots, a_n, \cdots \rangle = \langle a_1, a_2, a_3, \cdots \rangle && n \in \mathbb{N} \\
&= \left\langle \mathop{,}_{i\in\mathbb{N}} a_i \right\rangle = \left\langle \mathop{,}_{n\in\mathbb{N}} a_n \right\rangle = \begin{cases} \left\langle \mathop{,}_{i=1}^{n} a_i \right\rangle & \left|\langle a_i \rangle_{i\in\mathbb{N}}\right| = n \in \mathbb{N} \\ \left\langle \mathop{,}_{i\in\mathbb{N}} a_i \right\rangle & \left|\langle a_i \rangle_{i\in\mathbb{N}}\right| = |\mathbb{N}| \end{cases} \\
\langle a_i \rangle_{i=1}^{n} &= \left\langle \mathop{,}_{i=1}^{n} a_i \right\rangle = \langle a_1, a_2, \cdots, a_n \rangle = \langle a_1, \cdots, a_n \rangle && \forall n \in \mathbb{N}
\end{aligned}
$$

定義 5.12. indexed tuple

$$
(x_i)_{i\in I} = (x_i | i \in I) = (\cdots, x_i, \cdots) \quad i \in I
$$

$$
\begin{aligned}
\boldsymbol{x} = x_i = (x_i)_{i\in\mathbb{N}} &= (x_i | i \in \mathbb{N}) = (x_1, x_2, \cdots, x_i, \cdots) = (x_1, x_2, x_3, \cdots) && i \in \mathbb{N} \\
= (x_n)_{n\in\mathbb{N}} &= (x_n | n \in \mathbb{N}) = (x_1, x_2, \cdots, x_n, \cdots) = (x_1, x_2, x_3, \cdots) && n \in \mathbb{N} \\
&= \left(\mathop{,}_{i\in\mathbb{N}} x_i \right) = \left(\mathop{,}_{n\in\mathbb{N}} x_n \right) \\
= \langle x_i \rangle_{i\in\mathbb{N}} &= \begin{pmatrix} x_1 & x_2 & \cdots & x_i & \cdots \end{pmatrix}^{\mathsf{T}} = \begin{bmatrix} x_1 & x_2 & \cdots & x_i & \cdots \end{bmatrix}^{\mathsf{T}} && i \in \mathbb{N} \\
&= \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_i \\ \vdots \end{pmatrix} = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_i \\ \vdots \end{bmatrix} && i \in \mathbb{N} \\
\langle x_i \rangle_{i=1}^{n} &= \left\langle \mathop{,}_{i=1}^{n} x_i \right\rangle = \langle x_1, x_2, \cdots, x_n \rangle = \langle x_1, \cdots, x_n \rangle && \forall n \in \mathbb{N} \\
&\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} && \forall n \in \mathbb{N}
\end{aligned}
$$

$$
\begin{aligned}
\boldsymbol{x} = x_\mu = (x_i)_{i\in\mathbb{Z}_{\geq 0}} &= (x_i | i \in \mathbb{Z}_{\geq 0}) = (x_0, x_1, x_2, \cdots, x_i, \cdots) = (x_0, x_1, x_2, x_3, \cdots) && i \in \mathbb{Z}_{\geq 0} \\
= (x_k)_{k\in\mathbb{Z}_{\geq 0}} &= (x_k | k \in \mathbb{Z}_{\geq 0}) = (x_0, x_1, \cdots, x_k, \cdots) = (x_0, x_1, x_2, \cdots) && k \in \mathbb{Z}_{\geq 0} \\
= (x_\mu)_{\mu\in\mathbb{Z}_{\geq 0}} &= (x_\mu | \mu \in \mathbb{Z}_{\geq 0}) = (x_0, x_1, \cdots, x_\mu, \cdots) = (x_0, x_1, x_2, \cdots) && \mu \in \mathbb{Z}_{\geq 0} \\
&= \left(\underset{i\in\mathbb{Z}_{\geq 0}}{,} x_i \right) = \left(\underset{\mu\in\mathbb{Z}_{\geq 0}}{,} x_n \right) \\
= \langle x_\mu \rangle_{\mu\in\mathbb{Z}_{\geq 0}} &= \begin{pmatrix} x_0 & x_1 & \cdots & x_\mu & \cdots \end{pmatrix}^\mathsf{T} = \begin{bmatrix} x_0 & x_1 & \cdots & x_\mu & \cdots \end{bmatrix}^\mathsf{T} && \mu \in \mathbb{Z}_{\geq 0} \\
&= \begin{pmatrix} x_0 \\ x_1 \\ \vdots \\ x_\mu \\ \vdots \end{pmatrix} = \begin{bmatrix} x_0 \\ x_1 \\ \vdots \\ x_\mu \\ \vdots \end{bmatrix} && \mu \in \mathbb{Z}_{\geq 0} \\
\langle x_\mu \rangle_{\mu=0}^{n-1} &= \left\langle \underset{\mu=0}{\overset{n-1}{,}} x_\mu \right\rangle = \langle x_0, x_1, \cdots, x_{n-1} \rangle = \langle x_0, \cdots, x_{n-1} \rangle && \forall n \in \mathbb{N} \\
&= \begin{pmatrix} x_0 \\ x_1 \\ \vdots \\ x_{n-1} \end{pmatrix} = \begin{bmatrix} x_0 \\ x_1 \\ \vdots \\ x_{n-1} \end{bmatrix} = \begin{pmatrix} x_0 \\ \vdots \\ x_{n-1} \end{pmatrix} = \begin{bmatrix} x_0 \\ \vdots \\ x_{n-1} \end{bmatrix} && \forall n \in \mathbb{N}
\end{aligned}
$$

定義 5.13. left coset space

$$
\begin{aligned}
& && G \text{ is a group} \\
G/H &= \{gH | g \in G\} && \forall H \leq G \\
&= \bigcup_{g\in G} \{gH\} && \forall H \leq G \\
&= \{gH\}_{g\in G} && \forall H \leq G
\end{aligned}
$$

$$
G = \bigcup_{g\in G} gH \quad \forall H \leq G
$$

$\mathbb{Z}_2 \leq \mathbb{Z}_4$

$$
\begin{aligned}
\mathbb{Z}_4 &= \{0, 1, 2, 3\} && = \mathbb{Z}_{[0,4)} = (\mathbb{Z}_4, +_{\mathbb{Z}_n}) \\
&= \{e, g, g^2, g^3\} && = (\mathbb{Z}_4, \cdot) = (\mathbb{Z}_4, \cdot_G) \\
&= \{g, g^2, g^3, e\} \\
&= \{g^1, g^2, g^3, g^4\} = \langle g \rangle && g^4 = e \\
&= \{a^1, a^2, a^3, a^4\} \\
&= \{a^1, a^2, a^3, e\} && a^4 = e \\
&= \{e, a, a^2, a^3\} \supset \{e, a^2\} = (\mathbb{Z}_2, \cdot) = (\mathbb{Z}_2, \cdot_G) && = \mathbb{Z}_2 \\
\mathbb{Z}_2 \leq \mathbb{Z}_4 \Rightarrow \mathbb{Z}_2 &= \{e, a^2\} \\
e\mathbb{Z}_2 &= \{ee, ea^2\} = \{e, a^2\} && = \mathbb{Z}_2 \\
a\mathbb{Z}_2 &= \{ae, aa^2\} = \{a, a^3\} && = a\mathbb{Z}_2 \\
a^2\mathbb{Z}_2 &= \{a^2e, a^2a^2\} = \{a^2, a^4\} = \{a^2, e\} = \{e, a^2\} && = \mathbb{Z}_2 \\
a^3\mathbb{Z}_2 &= \{a^3e, a^3a^2\} = \{a^3, a^5\} = \{a^3, a\} = \{a, a^3\} && = a\mathbb{Z}_2 \\
a^4\mathbb{Z}_2 &= e\mathbb{Z}_2 = \{e, a^2\} && = \mathbb{Z}_2 \\
\mathbb{Z}_4/\mathbb{Z}_2 = \mathbb{Z}_4\mathbb{Z}_2 &= \{g\mathbb{Z}_2 | g \in \mathbb{Z}_4\} \\
&= \{e\mathbb{Z}_2, a\mathbb{Z}_2, a^2\mathbb{Z}_2, a^3\mathbb{Z}_2\} \\
&= \{\mathbb{Z}_2, a\mathbb{Z}_2\} \\
\mathbb{Z}_4 = \bigcup_{g\in\mathbb{Z}_4} g\mathbb{Z}_2 &= e\mathbb{Z}_2 \cup a\mathbb{Z}_2 \cup a^2\mathbb{Z}_2 \cup a^3\mathbb{Z}_2 && \begin{aligned} e\mathbb{Z}_2 = a^2\mathbb{Z}_2 &= \mathbb{Z}_2 \\ a\mathbb{Z}_2 = a^3\mathbb{Z}_2 &= a\mathbb{Z}_2 \end{aligned} \\
&= \mathbb{Z}_2 \cup a\mathbb{Z}_2 \\
&= e\mathbb{Z}_2 \cup a\mathbb{Z}_2 = e\mathbb{Z}_2 \cup a^3\mathbb{Z}_2 = a^2\mathbb{Z}_2 \cup a\mathbb{Z}_2 = a^2\mathbb{Z}_2 \cup a^3\mathbb{Z}_2
\end{aligned}
$$

$$2 = 4/2 = \left|\{e, a, a^2, a^3\}\right| / \left|\{e, a^2\}\right| = |\mathbb{Z}_4| / |\mathbb{Z}_2| = |\mathbb{Z}_4/\mathbb{Z}_2| = |\{\mathbb{Z}_2, a\mathbb{Z}_2\}| = 2$$

$C_3 = \mathbb{Z}_3 \leq D_3 = S_3$

$$D_3 = \left\{ \begin{matrix} \rho_{k,n} \\ \pi_{k,n} \end{matrix} \middle| \begin{matrix} \rho_{k,n} = \begin{bmatrix} +\cos\frac{2\pi}{n}k & -\sin\frac{2\pi}{n}k \\ +\sin\frac{2\pi}{n}k & +\cos\frac{2\pi}{n}k \end{bmatrix} \\ \pi_{k,n} = \begin{bmatrix} +\cos\frac{2\pi}{n}k & +\sin\frac{2\pi}{n}k \\ +\sin\frac{2\pi}{n}k & -\cos\frac{2\pi}{n}k \end{bmatrix} \end{matrix} \quad \forall k \in \mathbb{Z}_{[0,3)} \right\} \qquad n = 3$$

$$\begin{aligned}
&= \{\rho_0, \rho_1, \rho_2, \pi_0, \pi_1, \pi_2\} && = (D_3, \cdot) = (D_3, \cdot_G) \\
&= \{e, \rho_1, \rho_2, \pi_0, \pi_1, \pi_2\} && e = \rho_0 \\
& && e \neq \rho = \rho^1 = \rho_1 \\
&= \{e, \rho, \rho^2, \pi_0, \pi_1, \pi_2\} \supset \{e, \rho, \rho^2\} = \mathbb{Z}_3 && \rho^2 = (\rho_1)^2 = \rho_2 \\
\mathbb{Z}_3 \leq D_3 \Rightarrow \mathbb{Z}_3 &= \{0, 1, 2\} && = \mathbb{Z}_{[0,3)} = (\mathbb{Z}_3, +_{\mathbb{Z}_n}) \\
&= \{e, g, g^2\} && = (\mathbb{Z}_3, \cdot) = (\mathbb{Z}_3, \cdot_G) \\
&= \{g, g^2, e\} \\
&= \{g^1, g^2, g^3\} = \langle g \rangle && g^3 = e \\
&= \{a^1, a^2, a^3\} \\
&= \{a^1, a^2, e\} && a^3 = e \\
&= \{e, a, a^2\} \\
&= \{e, \rho, \rho^2\} = (\mathbb{Z}_3, \cdot_{D_3}) \subset D_3 && \rho^3 = e \\
C_3 = \mathbb{Z}_3 &= \{e, \rho, \rho^2\} \subset D_3 \\
e\mathbb{Z}_3 &= \{ee, e\rho, e\rho^2\} = \{e, \rho, \rho^2\} && = \mathbb{Z}_3 \\
\rho\mathbb{Z}_3 &= \{\rho e, \rho\rho, \rho\rho^2\} = \{\rho, \rho^2, \rho^3\} = \{\rho, \rho^2, e\} = \{e, \rho, \rho^2\} && = \mathbb{Z}_3 \\
\rho^2\mathbb{Z}_3 &= \{\rho^2 e, \rho^2\rho, \rho^2\rho^2\} = \{\rho^2, \rho^3, \rho^4\} = \{\rho^2, e, \rho\} = \{e, \rho, \rho^2\} && = \mathbb{Z}_3 \\
\rho^3\mathbb{Z}_3 &= e\mathbb{Z}_3 = \{e, \rho, \rho^2\} && = \mathbb{Z}_3 \\
& && \pi_i\rho_j = \pi_{i-j} \\
\pi_0\mathbb{Z}_3 &= \{\pi_0 e, \pi_0\rho, \pi_0\rho^2\} = \{\pi_0\rho_0, \pi_0\rho_1, \pi_0\rho_2\} && \pi_i = \pi_{3+i} \\
&= \{\pi_0, \pi_{-1}, \pi_{-2}\} = \{\pi_0, \pi_2, \pi_1\} = \{\pi_0, \pi_1, \pi_2\} && = \pi_0\mathbb{Z}_3 \\
\pi_1\mathbb{Z}_3 &= \{\pi_1 e, \pi_1\rho, \pi_1\rho^2\} = \{\pi_1\rho_0, \pi_1\rho_1, \pi_1\rho_2\} \\
&= \{\pi_1, \pi_0, \pi_{-1}\} = \{\pi_1, \pi_0, \pi_2\} = \{\pi_0, \pi_1, \pi_2\} && = \pi_0\mathbb{Z}_3 \\
\pi_2\mathbb{Z}_3 &= \{\pi_2 e, \pi_2\rho, \pi_2\rho^2\} = \{\pi_2\rho_0, \pi_2\rho_1, \pi_2\rho_2\} \\
&= \{\pi_2, \pi_1, \pi_0\} = \{\pi_0, \pi_1, \pi_2\} && = \pi_0\mathbb{Z}_3 \\
D_3/\mathbb{Z}_3 = D_3\mathbb{Z}_3 &= \{g\mathbb{Z}_3 | g \in D_3\} \\
&= \{e\mathbb{Z}_3, \rho\mathbb{Z}_3, \rho^2\mathbb{Z}_3, \pi_0\mathbb{Z}_3, \pi_1\mathbb{Z}_3, \pi_2\mathbb{Z}_3\} \\
&= \{\mathbb{Z}_3, \pi_0\mathbb{Z}_3\} \\
&= \{e\mathbb{Z}_3, \pi_i\mathbb{Z}_3\} && i \in \{0, 1, 2\} = \mathbb{Z}_{[0,3)} \\
& && e\mathbb{Z}_3 = \rho\mathbb{Z}_3 = \rho^2\mathbb{Z}_3 = \mathbb{Z}_3 \\
D_3 = \bigcup_{g \in D_3} g\mathbb{Z}_3 &= e\mathbb{Z}_3 \cup \rho\mathbb{Z}_3 \cup \rho^2\mathbb{Z}_3 \cup \pi_0\mathbb{Z}_3 \cup \pi_1\mathbb{Z}_3 \cup \pi_2\mathbb{Z}_3 && \pi_0\mathbb{Z}_3 = \pi_1\mathbb{Z}_3 = \pi_2\mathbb{Z}_3 = \pi_i\mathbb{Z}_3 \\
&= \mathbb{Z}_3 \cup \pi_i\mathbb{Z}_3 && i \in \{0, 1, 2\} = \mathbb{Z}_{[0,3)} \\
&= \cdots && 3 \cdot 3 = 9 \text{ possibilities of combinations}
\end{aligned}$$

$$2 = 6/3 = \left|\{e, \rho, \rho^2, \pi_0, \pi_1, \pi_2\}\right| / \left|\{e, \rho, \rho^2\}\right| = |D_3| / |\mathbb{Z}_3| = |D_3/\mathbb{Z}_3| = |\{e\mathbb{Z}_3, \pi_i\mathbb{Z}_3\}| = 2$$

$4\mathbb{Z} \leq \mathbb{Z}$

$$\begin{aligned}
\mathbb{Z}/4\mathbb{Z} = \mathbb{Z} + 4\mathbb{Z} = \{k + 4\mathbb{Z} | k \in \mathbb{Z}\} &= \{4\mathbb{Z}, 1 + 4\mathbb{Z}, 2 + 4\mathbb{Z}.3 + 4\mathbb{Z}\} \\
&= \{\cdots, -3 + 4\mathbb{Z}, -2 + 4\mathbb{Z}, -1 + 4\mathbb{Z}, 0 + 4\mathbb{Z}, 1 + 4\mathbb{Z}, 2 + 4\mathbb{Z}, 3 + 4\mathbb{Z}, \cdots\}
\end{aligned}$$

$$\mathbb{Z} = \bigcup_{k \in \mathbb{Z}} (k + 4\mathbb{Z}) = (4\mathbb{Z}) \cup (1 + 4\mathbb{Z}) \cup (2 + 4\mathbb{Z}) \cup (3 + 4\mathbb{Z})$$

6 normal subgroup

定義 **6.1.** normal subgroup

$$
\begin{aligned}
H &\leq G \\
gH &= Hg && \forall g \in G \\
&\Downarrow \\
H &\trianglelefteq G \\
&\Updownarrow \\
&H \text{ is a normal subgroup of } G
\end{aligned}
$$

trivial subgroups are normal subgroups

$$
\begin{aligned}
\{e\} &\leq G \\
G &\leq G && \{e\}, G \leq G \\
g\{e\} &= \{e\} g && \forall g \in G \\
gG &= Gg && \forall g \in G \\
&\Downarrow \\
\{e\} &\trianglelefteq G \\
G &\trianglelefteq G && \{e\}, G \trianglelefteq G \\
&\Updownarrow \\
&\text{trivial groups } \{e\}, G \text{ are normal subgroups of } G
\end{aligned}
$$

central subgroup is a normal subgroup

$$
\begin{aligned}
C(G) &\leq G \\
g \cdot C(G) = gC(G) &= C(G)g = C(G) \cdot g && \forall g \in G \\
&\Downarrow \\
C(G) &\trianglelefteq G \\
&\Updownarrow \\
&\text{central subgroup } C(G) \text{ is a normal subgroup of } G
\end{aligned}
$$

$C_3 = \mathbb{Z}_3 \trianglelefteq S_3 = D_3$

$$
\begin{aligned}
\rho_{k+3} &= \rho_k \\
\pi_{k+3} &= \pi_k \\
\rho_i \rho_j &= \rho_{i+j} \\
\rho_i \pi_j &= \pi_{i+j} \\
\pi_i \rho_j &= \pi_{i-j} \\
\pi_i \pi_j &= \rho_{i-j}
\end{aligned}
$$

$$
\begin{aligned}
C_3 = \mathbb{Z}_3 &= \{0,1,2\} \\
&= \{0_\rho, 1_\rho, 2_\rho\} = \{[123],[231],[312]\} = \{(),(123),(132)\} && \leq S_3 \\
&= \left\{e^{i\frac{2\pi}{n}0}, e^{i\frac{2\pi}{n}1}, e^{i\frac{2\pi}{n}2}, \cdots, e^{i\frac{2\pi}{n}(n-1)}\right\} \overset{n=3}{=} \left\{e^{i\frac{2\pi}{3}0}, e^{i\frac{2\pi}{3}1}, e^{i\frac{2\pi}{3}2}\right\} \\
&= \{e, g, g^2, \cdots, g^{n-1}\} = \{g^0, g^1, g^2\} = \{e, g, g^2\}, g^n = e \\
&= \{e, \rho, \rho^2\} = \{\rho_0, \rho_1, \rho_2\} = \{\rho_j | j \in \{0,1,2\}\} && \leq D_3 = \{\rho_k, \pi_k\} = \{\rho_{k,3}, \pi_{k,3}\} \\
\rho_i \mathbb{Z}_3 &= \{\rho_i\rho_j | j \in \{0,1,2\}\} \\
&= \{\rho_{i+j} | j \in \{0,1,2\}\} \overset{i+j=j+i}{=} \{\rho_{j+i} | j \in \{0,1,2\}\} \\
&= \{\rho_j\rho_i | j \in \{0,1,2\}\} = \mathbb{Z}_3\rho_i && \Rightarrow \rho_i\mathbb{Z}_3 = \mathbb{Z}_3\rho_i \\
\pi_i \mathbb{Z}_3 &= \{\pi_i\rho_j | j \in \{0,1,2\}\} \\
&= \{\pi_{i-j} | j \in \{0,1,2\}\} \overset{\pi_{k+3}=\pi_k}{=} \{\pi_{3+i-j} | j \in \{0,1,2\}\} \\
&= \{\pi_{i+(3-j)} | 3-j \in \{3,2,1\}\} = \{\pi_{(3-j)+i} | 3-j \in \{3,2,1\}\} && i+(3-j) = (3-j)+i \\
&= \{\rho_{3-j}\pi_i | 3-j \in \{3,2,1\}\} = \{\rho_{3-j} | 3-j \in \{3,2,1\}\}\pi_i && \rho_i\pi_j = \pi_{i+j} \\
&= \{\rho_j | j \in \{0,1,2\}\}\pi_i = \mathbb{Z}_3\pi_i && \Rightarrow \pi_i\mathbb{Z}_3 = \mathbb{Z}_3\pi_i \\
&\Downarrow \\
\rho_i\mathbb{Z}_3 &= \mathbb{Z}_3\rho_i \\
\pi_i\mathbb{Z}_3 &= \mathbb{Z}_3\pi_i && \Rightarrow g\mathbb{Z}_3 = \mathbb{Z}_3 g \quad \forall g \in D_3 \\
&\Downarrow \\
&\mathbb{Z}_3 \leq D_3 = S_3 \\
g\mathbb{Z}_3 &= \mathbb{Z}_3 g \quad \forall g \in D_3 && \Rightarrow \mathbb{Z}_3 \trianglelefteq D_3 = S_3 \\
& && \Updownarrow \\
& && \mathbb{Z}_3 \trianglelefteq S_3 = D_3
\end{aligned}
$$

$\mathbb{Z}_2 \ntrianglelefteq S_3 = D_3$

定義 6.2. set mulitplication and set inverse

$$
\begin{aligned}
S^{-1} &= \overline{S} = \{\overline{s} | s \in S\} = \{s^{-1} | s \in S\} \\
gS &= \{gs | s \in S\} \qquad \{sg | s \in S\} = Sg \\
S_1S_2 &= \left\{ s_1s_2 \middle| \begin{matrix} s_1 \in S_1 \\ s_2 \in S_2 \end{matrix} \right\}
\end{aligned}
$$

定理 6.3. *subgroup or group multiplication closure and inverse closure*

$$
\begin{aligned}
H &\leq G \\
&\Downarrow \\
HH &= H \qquad\qquad HH = \left\{ h_1h_2 \middle| \begin{matrix} h_1 \in H \\ h_2 \in H \end{matrix} \right\} \\
&\wedge \\
H^{-1} = \overline{H} &= H \quad H^{-1} = \overline{H} = \{\overline{h} | h \in H\} = \{h^{-1} | h \in H\}
\end{aligned}
$$

$$
H \leq G \Rightarrow \begin{cases} HH = H & \text{group multiplication closure} \\ \overline{H} = H & \text{group inverse closure} \end{cases}
$$

定理 6.4.

$$
\begin{aligned}
N &\trianglelefteq G \\
g_1, g_2 &\in G \\
&\Downarrow \\
(g_1N)(g_2N) &= (g_1g_2)N
\end{aligned}
$$

Proof.

$$
\begin{aligned}
(g_1N)(g_2N) &= (g_1Ng_2)(N) & (g_1n_1)(g_2n_2) &= (g_1n_1g_2)n_2 \\
&= (g_1g_2N)(N) & &\overset{N \trianglelefteq G \Rightarrow gn=ng}{=} (g_1g_2n_1)n_2 \\
&= (g_1g_2)(NN) & &= (g_1g_2)(n_1n_2) \\
&= (g_1g_2)(N) & N \leq G \Rightarrow NN = N &\Leftarrow HH = H \Leftarrow H \leq G \\
(g_1N)(g_2N) &= (g_1g_2)N
\end{aligned}
$$

□

定理 6.5.

$$\begin{aligned} N &\trianglelefteq G \\ g &\in G \\ &\Downarrow \\ (gN)^{-1} = \overline{(gN)} &= \overline{g}N = g^{-1}N \end{aligned}$$

Proof.

$$\begin{aligned} \overline{(gN)} = \overline{\{gn\}} &= \{\overline{gn}\} & \overline{S} = \{\overline{s} | s \in S\} \\ &= \{\overline{n}\overline{g}\} & \overline{gn}gn = \overline{n}\overline{g}gn = e \\ &= \overline{N}\overline{g} \\ &= N\overline{g} & \overline{N} = N \Leftarrow N \leq G \\ &= \overline{g}N & gN = Ng \Leftarrow N \trianglelefteq G \\ \overline{(gN)} &= \overline{g}N \end{aligned}$$

□

定理 6.6.

$$N \trianglelefteq G \Rightarrow (N)(gN) = NgN = gN$$

Proof.

$$\begin{aligned} (N)(gN) &= (N)(Ng) & gN = Ng \Leftarrow N \trianglelefteq G \\ &= (NN)g & (n_1)(n_2 g) = (n_1 n_2) g \\ &= Ng & NN = N \Leftarrow N \leq G \\ &= gN & gN = Ng \Leftarrow N \trianglelefteq G \end{aligned}$$

□

6.1 quotient group

$$\begin{aligned} &G \text{ is a group} \\ &\Updownarrow \\ G = (G, \cdot) = (G, \cdot_G) = &\left\{ g \left| \begin{array}{lll} g_1 \cdot g_2 = g_1 g_2 \in G & \forall g_1, g_2 \in G & (c)\ \cdot_G \text{ closure} \\ g_1(g_2 g_3) = (g_1 g_2) g_3 = g_1 g_2 g_3 & \forall g_1, g_2, g_3 \in G & (a)\ \cdot_G \text{ associativity} \\ e \cdot g = eg = g = ge = g \cdot e & \exists e = e_G \in G, \forall g \in G & (id) \text{ identity element} \\ \overline{g} \cdot g = \overline{g}g = e = g\overline{g} = g \cdot \overline{g} & \forall g \in G, \exists \overline{g} \in G & (in) \text{ inverse element} \end{array} \right. \right\} \end{aligned}$$

定義 6.7. quotient group

$$\begin{aligned} G/N = GN &= (G/N, \cdot_{\text{group}}) = (GN, \cdot_{\text{set}}) \\ &= \left\{ gN \left| \begin{array}{lll} (g_1 N)(g_2 N) = (g_1 g_2) N \in G/N & \forall g_1 N, g_2 N \in G/N & (c)\ \cdot_{\text{group}} \text{ closure} \\ g_1 N (g_2 N g_3 N) = (g_1 N g_2 N) g_3 N = g_1 g_2 g_3 N & \forall g_1 N, g_2 N, g_3 N \in G/N & (a)\ \cdot_{\text{group}} \text{ associativity} \\ (N)(gN) = NgN = gN = (gN)N = (gN)(N) & \exists N = e_{G/N} \in G/N, \forall gN \in G/N & (id) \text{ identity element} \\ \overline{(gN)}(gN) = \overline{gN}gN = N\overline{g}gN = NeN = NN = N & \forall gN \in G/N, \exists \overline{gN} \in G/N & (in) \text{ inverse element} \end{array} \right. \right\} \\ &\Downarrow \\ G/N &= \{gN | g \in G\} \text{ is a group} \qquad \forall N \trianglelefteq G \\ &\Updownarrow \text{def.} \\ G/N &\text{ is a quotient group} \end{aligned}$$

$$|G/N| = |G| / |N| \overset{\text{if } |N|>1 \text{ or } G/N \neq \{e\}}{<} |G|$$

quotient group vs. left coset space

- quotient group

$$\begin{aligned} & & G \text{ is a group} \\ G/N &= \{gN | g \in G\} & \forall N \trianglelefteq G \\ &= \bigcup_{g \in G} \{gN\} & \forall N \trianglelefteq G \\ &= \{gN\}_{g \in G} & \forall N \trianglelefteq G \end{aligned}$$

$$G = \bigcup_{g \in G} gN \quad \forall N \trianglelefteq G$$

$$|G/N| = |G| \, / \, |N|$$

- left coset space

$$\begin{aligned} & & & G \text{ is a group} \\ G/H &= \{gH | g \in G\} & & \forall H \leq G \\ &= \bigcup_{g \in G} \{gH\} & & \forall H \leq G \\ &= \{gH\}_{g \in G} & & \forall H \leq G \end{aligned}$$

$$G = \bigcup_{g \in G} gH \quad \forall H \leq G$$

$$|G/H| = |G| \, / \, |H|$$

$S_3 = D_3 \triangleright C_3 = \mathbb{Z}_3 \triangleright E_3$

$\cdot_{D_3}$	ρ_0	ρ_1	ρ_2	π_0	π_1	π_2
ρ_0	ρ_0	ρ_1	ρ_2	π_0	π_1	π_2
ρ_1	ρ_1	ρ_2	ρ_0	π_1	π_2	π_0
ρ_2	ρ_2	ρ_0	ρ_1	π_2	π_0	π_1
π_0	π_0	π_2	π_1	ρ_0	ρ_2	ρ_1
π_1	π_1	π_0	π_2	ρ_1	ρ_0	ρ_2
π_2	π_2	π_1	π_0	ρ_2	ρ_1	ρ_0
$\cdot_{S_3}$	e	(123)	(132)	$(3)(12)$	$(1)(23)$	$(2)(31)$
e	e	(123)	(132)	$(3)(12)$	$(1)(23)$	$(2)(31)$
(123)	(123)	(132)	e	$(1)(23)$	$(2)(31)$	$(3)(12)$
(132)	(132)	e	(123)	$(2)(31)$	$(3)(12)$	$(1)(23)$
$(3)(12)$	$(3)(12)$	$(2)(31)$	$(1)(23)$	e	(132)	(123)
$(1)(23)$	$(1)(23)$	$(3)(12)$	$(2)(31)$	(123)	e	(132)
$(2)(31)$	$(2)(31)$	$(1)(23)$	$(3)(12)$	(132)	(123)	e

$\cdot_{S_3}$	$[123]$	$[231]$	$[312]$	$[213]$	$[132]$	$[321]$
$[123]$	$[123]$	$[231]$	$[312]$	$[213]$	$[132]$	$[321]$
$[231]$	$[231]$	$[312]$	$[123]$	$[132]$	$[321]$	$[213]$
$[312]$	$[312]$	$[123]$	$[231]$	$[321]$	$[213]$	$[132]$
$[213]$	$[213]$	$[321]$	$[132]$	$[123]$	$[312]$	$[231]$
$[132]$	$[132]$	$[213]$	$[321]$	$[231]$	$[123]$	$[312]$
$[321]$	$[321]$	$[132]$	$[213]$	$[312]$	$[231]$	$[123]$
$\cdot_{S_3}$	$()$	(123)	(132)	(12)	(23)	(31)
$()$	$()$	(123)	(132)	(12)	(23)	(31)
(123)	(123)	(132)	$()$	(23)	(31)	(12)
(132)	(132)	$()$	(123)	(31)	(12)	(23)
(12)	(12)	(31)	(23)	$()$	(132)	(123)
(23)	(23)	(12)	(31)	(123)	$()$	(132)
(31)	(31)	(23)	(12)	(132)	(123)	$()$
$\cdot_{D_3}$	e	ρ	ρ^2	π_0	π_1	π_2
e	e	ρ	ρ^2	π_0	π_1	π_2
ρ	ρ	ρ^2	e	π_1	π_2	π_0
ρ^2	ρ^2	e	ρ	π_2	π_0	π_1
π_0	π_0	π_2	π_1	e	ρ^2	ρ
π_1	π_1	π_0	π_2	ρ	e	ρ^2
π_2	π_2	π_1	π_0	ρ^2	ρ	e

$S_3 = \{$	$\sigma_1,$	$\sigma_2,$	$\sigma_3,$	$\sigma_4,$	$\sigma_5,$	σ_6	$\}$	
$= \{$	$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix},$	$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix},$	$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$	$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$	$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},$	$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$	$\}$	two-line notation
$= \{$	$[123],$	$[231],$	$[312],$	$[213],$	$[132],$	$[321]$	$\}$	one-line notation
$= \{$	$123,$	$231,$	$312,$	$213,$	$132,$	321	$\}$	one-line notation, simplified
$= \{$	$(1)(2)(3),$	$(123),$	$(132),$	$(12)(3),$	$(1)(23),$	$(31)(2)$	$\}$	cycle notation
$= \{$	$(),$	$(123),$	$(132),$	$(12),$	$(23),$	(31)	$\}$	cycle notation, simplified
$D_3 = \{$	$\rho_0,$	$\rho_1,$	$\rho_2,$	$\pi_0,$	$\pi_1,$	π_2	$\}$	
$= \{$	$e,$	$\rho,$	$\rho^2,$	$\pi_0,$	$\pi_1,$	π_2	$\}$	

$$|S_3| = 3! = 6 = 2 \cdot 3 = |D_3|$$

$$\begin{aligned} C_3 = \mathbb{Z}_3 &= \{\rho_0\} \cup \{\rho_1, \rho_2\} & &= \{\rho_0, \rho_1, \rho_2\} \\ &= \{[123]\} \cup \{[231], [312]\} & &= \{[123], [231], [312]\} \\ &= \{()\} \cup \{(123), (132)\} & &= \{(), (123), (132)\} \end{aligned}$$

$$|\mathbb{Z}_3| = |C_3| = 3$$

$$
\begin{aligned}
D_3/C_3 = S_3/\mathbb{Z}_3 &= \{\sigma\mathbb{Z}_3 | \sigma \in S_3\} & &= S_3\mathbb{Z}_3 \\
&= \{[123]\,\mathbb{Z}_3, [213]\,\mathbb{Z}_3\} & &= \{()\mathbb{Z}_3, (12)\,\mathbb{Z}_3\} \\
&= \{[123]\,\mathbb{Z}_3, [132]\,\mathbb{Z}_3\} & &= \{()\mathbb{Z}_3, (23)\,\mathbb{Z}_3\} \\
&= \{[123]\,\mathbb{Z}_3, [321]\,\mathbb{Z}_3\} & &= \{()\mathbb{Z}_3, (31)\,\mathbb{Z}_3\} \\
&= \{eC_3, \pi_i C_3\} & &= D_3 C_3 \\
&= \{\rho_0 C_3, \pi_0 C_3\} \\
&= \{\rho_0 C_3, \pi_1 C_3\} \\
&= \{\rho_0 C_3, \pi_2 C_3\} \\
&= \{\{[123], [231], [312]\}, \{[213], [132], [321]\}\} \\
&= \{\{(), (123), (132)\}, \{(12), (23), (31)\}\} \\
&= \{\{\rho_0, \rho_1, \rho_2\}, \{\pi_0, \pi_1, \pi_2\}\} \\
&= \left\{\left\{e, \rho, \rho^2\right\}, \{\pi_0, \pi_1, \pi_2\}\right\}
\end{aligned}
$$

$$|D_3/C_3| = |S_3/\mathbb{Z}_3| = |D_3| \,/\, |C_3| = |S_3| \,/\, |\mathbb{Z}_3| = 6/3 = 2$$

$$C_3 = \mathbb{Z}_3 \trianglelefteq S_3 = D_3$$

$$C_3 = \mathbb{Z}_3 \triangleleft S_3 = D_3$$

$$S_3 = D_3 \triangleright C_3 = \mathbb{Z}_3$$

$$S_3 \triangleright C_3$$

$$E_3 = \{e\} = \{\rho_0\} = \{[123]\} = \{()\} \subset \{(), (123), (132)\} = C_3$$

$$|E_3| = 1$$

$$
\begin{aligned}
C_3/E_3 = \mathbb{Z}_3/E_3 &= \{\sigma E_3 | \sigma \in \mathbb{Z}_3\} \\
&= \{[123]\,E_3, [231]\,E_3, [312]\,E_3\} & &= \{\{[123]\}, \{[231]\}, \{[312]\}\} \\
&= \{()E_3, (123)\,E_3, (132)\,E_3\} & &= \{\{()\}, \{(123)\}, \{(132)\}\} \\
&= \{\rho_0 E_3, \rho_1 E_3, \rho_2 E_3\} & &= \{\{\rho_0\}, \{\rho_1\}, \{\rho_2\}\} \\
&= \left\{eE_3, \rho E_3, \rho^2 E_3\right\} & &= \left\{\{e\}, \{\rho\}, \left\{\rho^2\right\}\right\}
\end{aligned}
$$

$$|C_3/E_3| = |\mathbb{Z}_3/E_3| = |C_3| \,/\, |E_3| = |\mathbb{Z}_3| \,/\, |E_3| = 3/1 = 3$$

$$E_3 \trianglelefteq C_3 = \mathbb{Z}_3 \trianglelefteq S_3 = D_3$$

$$E_3 \triangleleft C_3 = \mathbb{Z}_3 \triangleleft S_3 = D_3$$

$$S_3 = D_3 \triangleright C_3 = \mathbb{Z}_3 \triangleright E_3$$

$$S_3 \triangleright C_3 \triangleright E_3$$

$$S_4 \rhd A_4 \rhd H_4 \rhd C_2 \rhd E_4$$

$$
\begin{array}{llllllll}
S_4 = \{ & \sigma_1, & \sigma_2, & \sigma_3, & \sigma_4, & \sigma_5, & \sigma_6, & \\
& \sigma_1, & \sigma_2, & \sigma_3, & \sigma_4, & \sigma_5, & \sigma_6, & \\
& \sigma_1, & \sigma_2, & \sigma_3, & \sigma_4, & \sigma_5, & \sigma_6, & \\
& \sigma_1, & \sigma_2, & \sigma_3, & \sigma_4, & \sigma_5, & \sigma_6 & \} \\
= \{ & \begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}, & \begin{pmatrix}1&2&3&4\\2&3&1&4\end{pmatrix}, & \begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix}, & \begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix}, & \begin{pmatrix}1&2&3&4\\1&3&2&4\end{pmatrix}, & \begin{pmatrix}1&2&3&4\\3&2&1&4\end{pmatrix}, & \\
& \begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}, & \begin{pmatrix}1&2&3&4\\2&3&1&4\end{pmatrix}, & \begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix}, & \begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix}, & \begin{pmatrix}1&2&3&4\\1&3&2&4\end{pmatrix}, & \begin{pmatrix}1&2&3&4\\3&2&1&4\end{pmatrix}, & \\
& \begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}, & \begin{pmatrix}1&2&3&4\\2&3&1&4\end{pmatrix}, & \begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix}, & \begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix}, & \begin{pmatrix}1&2&3&4\\1&3&2&4\end{pmatrix}, & \begin{pmatrix}1&2&3&4\\3&2&1&4\end{pmatrix}, & \\
& \begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}, & \begin{pmatrix}1&2&3&4\\2&3&1&4\end{pmatrix}, & \begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix}, & \begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix}, & \begin{pmatrix}1&2&3&4\\1&3&2&4\end{pmatrix}, & \begin{pmatrix}1&2&3&4\\3&2&1&4\end{pmatrix} & \} \\
= \{ & [123], & [231], & [312], & [213], & [132], & [321], & \\
& [123], & [231], & [312], & [213], & [132], & [321], & \\
& [123], & [231], & [312], & [213], & [132], & [321], & \\
& [123], & [231], & [312], & [213], & [132], & [321] & \} \\
= \{ & 123, & 231, & 312, & 213, & 132, & 321, & \\
& 123, & 231, & 312, & 213, & 132, & 321, & \\
& 123, & 231, & 312, & 213, & 132, & 321, & \\
& 123, & 231, & 312, & 213, & 132, & 321 & \} \\
= \{ & (1)(2)(3), & (123), & (132), & (12)(3), & (1)(23), & (31)(2), & \\
& (1)(2)(3), & (123), & (132), & (12)(3), & (1)(23), & (31)(2), & \\
& (1)(2)(3), & (123), & (132), & (12)(3), & (1)(23), & (31)(2), & \\
& (1)(2)(3), & (123), & (132), & (12)(3), & (1)(23), & (31)(2) & \} \\
= \{ & (), & (123), & (132), & (12), & (23), & (31), & \\
& (), & (123), & (132), & (12), & (23), & (31), & \\
& (), & (123), & (132), & (12), & (23), & (31), & \\
& (), & (123), & (132), & (12), & (23), & (31) & \}
\end{array}
$$

6.2 simple group

定義 6.8. simple group

G is a group
G does not have no nontrivial normal groups $\quad \forall N \trianglelefteq G \, [N \in \{\{e\}, G\}]$
$\Downarrow$
G is a simple group

定義 6.9. finite simple group

G is a group
G does not have no nontrivial normal groups $\quad \forall N \trianglelefteq G \, [N \in \{\{e\}, G\}]$
$|G| < \infty$
$\Downarrow$
G is a simple group

finite simple group : finite group theory $\sim$ prime number : number theory

classification of finite simple groups

- cyclic groups of prime order $\mathbb{Z}_{\mathbb{P}}$
- alternating groups of degree at least 5 $A_{n \geq 5}$
  - Galois theory
- Lie groups = group with properties of manifold
- derived subgroups of Lie groups
- 26 sporadic groups
  - monster group

7 conjugate class

定義 7.1. conjugate class

$$[g] = \left\{hg\overline{h}\middle|h \in G\right\} \qquad \begin{array}{r}G \text{ is a group}\\ \forall g \in G\end{array}$$

$$\begin{aligned}
&[g] \ni eg\overline{e} = ege = (eg)\,e = (g)\,e = ge = g\\
&\Downarrow\\
&g = eg\overline{e} \in [g]\\
&\Downarrow\\
&g \in [g]
\end{aligned}$$

$$\widetilde{g} \in [g] = \left\{hg\overline{h}\middle|h \in G\right\} \qquad \begin{array}{r}G \text{ is a group}\\ \forall g \in G\end{array}$$

$$\Downarrow$$

$$\widetilde{g} = hg\overline{h}$$

$$\overline{h}\widetilde{g}h = \overline{h}hg\overline{h}h = ege = g$$

$$g = \overline{h}\widetilde{g}h = \overline{h}\widetilde{g}\overline{\overline{h}} \in \left\{\overline{h}\widetilde{g}\overline{\overline{h}}\middle|h \in G\right\} = \left\{h\widetilde{g}\overline{h}\middle|h \in G\right\} = [\widetilde{g}] \qquad \begin{array}{r}G \text{ is a group}\\ \forall \widetilde{g} \in G\end{array}$$

$$\Downarrow$$

$$g \in [\widetilde{g}]$$

$$\overline{h\widetilde{h}}h\widetilde{h} = \overline{\widetilde{h}}\overline{h}h\widetilde{h} = \overline{\widetilde{h}}\left(\overline{h}h\right)\widetilde{h} = \overline{\widetilde{h}}\,(e)\,\widetilde{h} = \overline{\widetilde{h}}\widetilde{h} = e$$

$$\begin{cases} g \in [\widetilde{g}] & \Rightarrow g = h\widetilde{g}\overline{h} = h\widetilde{h}\widetilde{\widetilde{g}}\overline{\widetilde{h}}\overline{h} \overset{\overline{h\widetilde{h}}=\overline{\widetilde{h}}\overline{h}}{=} h\widetilde{h}\widetilde{\widetilde{g}}\overline{h\widetilde{h}} \in \left\{h\widetilde{h}\widetilde{\widetilde{g}}\overline{h\widetilde{h}}\middle|h\widetilde{h} \in G\right\} = \left[\widetilde{\widetilde{g}}\right] \\ \widetilde{g} \in \left[\widetilde{\widetilde{g}}\right] & \Rightarrow \widetilde{g} = \widetilde{h}\widetilde{\widetilde{g}}\overline{\widetilde{h}} \Uparrow \end{cases} \Rightarrow g \in \left[\widetilde{\widetilde{g}}\right]$$

$$[e] = \left\{he\overline{h}\middle|h \in G\right\} = \left\{h\overline{h}\middle|h \in G\right\} = \{e|h \in G\} = \{e\} \qquad \begin{array}{r}G \text{ is a group}\\ e = e_G \in G\end{array}$$

$$[e] = \{e\}$$

$$[c] = \left\{hc\overline{h}\middle|h \in G\right\} = \left\{ch\overline{h}\middle|ch = hc \quad \forall h \in G \quad\right\} = \{ce|h \in G\} = \{c\} \qquad \forall c \in C\,(G)$$

$$[c] = \{c\}$$

$$g \in [\widetilde{g}] = \left\{h\widetilde{g}\overline{h}\middle|h \in G\right\} \qquad \begin{array}{r}G \text{ is a group}\\ \widetilde{g} \in G\end{array}$$

$$\exists h \in G\left[g = h\widetilde{g}\overline{h}\right]$$

$$g = h\widetilde{g}\overline{h}$$

$$\begin{aligned}
g^n &= \overbrace{h\widetilde{g}\overline{h}h\widetilde{g}\overline{h}\cdots h\widetilde{g}\overline{h}}^{n} = h\overbrace{\widetilde{g}e\widetilde{g}e\cdots e\widetilde{g}}^{n}\overline{h} = h\overbrace{\widetilde{g}\widetilde{g}\cdots\widetilde{g}}^{n}\overline{h} = h\widetilde{g}^n\overline{h} \in [\widetilde{g}^n] && \forall n \in \mathbb{N}\\
g^n &\in [\widetilde{g}^n] && \forall n \in \mathbb{N}\\
g^{-n} = \overline{g}^n = \overline{g^n} &= \overline{h\widetilde{g}^n\overline{h}} = \overline{\overline{h}}\overline{\widetilde{g}}^n\overline{h} = h\overline{\widetilde{g}}^n\overline{h} = h\widetilde{g}^{-n}\overline{h} && \forall n \in \mathbb{N}\\
g^m &\in [\widetilde{g}^m] && \forall m \in \mathbb{Z}
\end{aligned}$$

$$D_3 = S_3$$

$\cdot_{D_3}$	ρ_0	ρ_1	ρ_2	π_0	π_1	π_2
ρ_0	ρ_0	ρ_1	ρ_2	π_0	π_1	π_2
ρ_1	ρ_1	ρ_2	ρ_0	π_1	π_2	π_0
ρ_2	ρ_2	ρ_0	ρ_1	π_2	π_0	π_1
π_0	π_0	π_2	π_1	ρ_0	ρ_2	ρ_1
π_1	π_1	π_0	π_2	ρ_1	ρ_0	ρ_2
π_2	π_2	π_1	π_0	ρ_2	ρ_1	ρ_0

$\rightarrow$

$\cdot_{S_3}$	[123]	[231]	[312]	[213]	[132]	[321]
[123]	[123]	[231]	[312]	[213]	[132]	[321]
[231]	[231]	[312]	[123]	[132]	[321]	[213]
[312]	[312]	[123]	[231]	[321]	[213]	[132]
[213]	[213]	[321]	[132]	[123]	[312]	[231]
[132]	[132]	[213]	[321]	[231]	[123]	[312]
[321]	[321]	[132]	[213]	[312]	[231]	[123]

$\downarrow$

$\cdot_{S_3}$	()	(123)	(132)	(12)	(23)	(31)
()	()	(123)	(132)	(12)	(23)	(31)
(123)	(123)	(132)	()	(23)	(31)	(12)
(132)	(132)	()	(123)	(31)	(12)	(23)
(12)	(12)	(31)	(23)	()	(132)	(123)
(23)	(23)	(12)	(31)	(123)	()	(132)
(31)	(31)	(23)	(12)	(132)	(123)	()

$\downarrow$

$\cdot_{S_3}$	e	(123)	(132)	(3) (12)	(1) (23)	(2) (31)
e	e	(123)	(132)	(3) (12)	(1) (23)	(2) (31)
(123)	(123)	(132)	e	(1) (23)	(2) (31)	(3) (12)
(132)	(132)	e	(123)	(2) (31)	(3) (12)	(1) (23)
(3) (12)	(3) (12)	(2) (31)	(1) (23)	e	(132)	(123)
(1) (23)	(1) (23)	(3) (12)	(2) (31)	(123)	e	(132)
(2) (31)	(2) (31)	(1) (23)	(3) (12)	(132)	(123)	e

$\nwarrow$

$\cdot_{D_3}$	ρ_0	ρ_1	ρ_2	π_0	π_1	π_2	$\cdot_{S_3}$	[123]	[231]	[312]	[213]	[132]	[321]
ρ_0	ρ_0	ρ_1	ρ_2	π_0	π_1	π_2	[123]	[123]	[231]	[312]	[213]	[132]	[321]
ρ_1	ρ_1	ρ_2	ρ_0	π_1	π_2	π_0	[231]	[231]	[312]	[123]	[132]	[321]	[213]
ρ_2	ρ_2	ρ_0	ρ_1	π_2	π_0	π_1	[312]	[312]	[123]	[231]	[321]	[213]	[132]
π_0	π_0	π_2	π_1	ρ_0	ρ_2	ρ_1	[213]	[213]	[321]	[132]	[123]	[312]	[231]
π_1	π_1	π_0	π_2	ρ_1	ρ_0	ρ_2	[132]	[132]	[213]	[321]	[231]	[123]	[312]
π_2	π_2	π_1	π_0	ρ_2	ρ_1	ρ_0	[321]	[321]	[132]	[213]	[312]	[231]	[123]
$\cdot_{S_3}$	e	(123)	(132)	(3) (12)	(1) (23)	(2) (31)	$\cdot_{S_3}$	()	(123)	(132)	(12)	(23)	(31)
e	e	(123)	(132)	(3) (12)	(1) (23)	(2) (31)	()	()	(123)	(132)	(12)	(23)	(31)
(123)	(123)	(132)	e	(1) (23)	(2) (31)	(3) (12)	(123)	(123)	(132)	()	(23)	(31)	(12)
(132)	(132)	e	(123)	(2) (31)	(3) (12)	(1) (23)	(132)	(132)	()	(123)	(31)	(12)	(23)
(3) (12)	(3) (12)	(2) (31)	(1) (23)	e	(132)	(123)	(12)	(12)	(31)	(23)	()	(132)	(123)
(1) (23)	(1) (23)	(3) (12)	(2) (31)	(123)	e	(132)	(23)	(23)	(12)	(31)	(123)	()	(132)
(2) (31)	(2) (31)	(1) (23)	(3) (12)	(132)	(123)	e	(31)	(31)	(23)	(12)	(132)	(123)	()

$\mathbb{Z}_3 \leq D_3 = S_3$

$$D_3 = \left\{ \begin{array}{l|l} \rho_{k,n} & \rho_{k,n} = \begin{bmatrix} +\cos\frac{2\pi}{n}k & -\sin\frac{2\pi}{n}k \\ +\sin\frac{2\pi}{n}k & +\cos\frac{2\pi}{n}k \end{bmatrix} \\ \pi_{k,n} & \pi_{k,n} = \begin{bmatrix} +\cos\frac{2\pi}{n}k & +\sin\frac{2\pi}{n}k \\ +\sin\frac{2\pi}{n}k & -\cos\frac{2\pi}{n}k \end{bmatrix} \end{array} \quad \forall k \in \mathbb{Z}_{[0,3)} \right\} \qquad n = 3$$

$$\begin{aligned}
&= \{\rho_0, \rho_1, \rho_2, \pi_0, \pi_1, \pi_2\} && = (D_3, \cdot) = (D_3, \cdot_G) \\
&= \{e, \rho_1, \rho_2, \pi_0, \pi_1, \pi_2\} && e = \rho_0 \\
& && e \neq \rho = \rho^1 = \rho_1 \\
&= \left\{e, \rho, \rho^2, \pi_0, \pi_1, \pi_2\right\} \supset \left\{e, \rho, \rho^2\right\} = \mathbb{Z}_3 && \rho^2 = (\rho_1)^2 = \rho_2
\end{aligned}$$

$$\begin{aligned}
\mathbb{Z}_3 \leq D_3 \Rightarrow \mathbb{Z}_3 &= \{0, 1, 2\} && = \mathbb{Z}_{[0,3)} = (\mathbb{Z}_3, +_{\mathbb{Z}_n}) \\
&= \left\{e, g, g^2\right\} && = (\mathbb{Z}_3, \cdot) = (\mathbb{Z}_3, \cdot_G) \\
&= \left\{g, g^2, e\right\} \\
&= \left\{g^1, g^2, g^3\right\} = \langle g \rangle && g^3 = e \\
&= \left\{a^1, a^2, a^3\right\} \\
&= \left\{a^1, a^2, e\right\} && a^3 = e \\
&= \left\{e, a, a^2\right\} \\
&= \left\{e, \rho, \rho^2\right\} = (\mathbb{Z}_3, \cdot_{D_3}) \subset D_3 && \rho^3 = e \\
D_3/\mathbb{Z}_3 = D_3\mathbb{Z}_3 &= \{g\mathbb{Z}_3 | g \in D_3\} \\
&= \left\{e\mathbb{Z}_3, \rho\mathbb{Z}_3, \rho^2\mathbb{Z}_3, \pi_0\mathbb{Z}_3, \pi_1\mathbb{Z}_3, \pi_2\mathbb{Z}_3\right\} \\
&= \{\mathbb{Z}_3, \pi_0\mathbb{Z}_3\} \\
&= \{e\mathbb{Z}_3, \pi_i\mathbb{Z}_3\} && i \in \{0, 1, 2\} = \mathbb{Z}_{[0,3)} \\
& && e\mathbb{Z}_3 = \rho\mathbb{Z}_3 = \rho^2\mathbb{Z}_3 = \mathbb{Z}_3 \\
D_3 = \bigcup_{g \in D_3} g\mathbb{Z}_3 &= e\mathbb{Z}_3 \cup \rho\mathbb{Z}_3 \cup \rho^2\mathbb{Z}_3 \cup \pi_0\mathbb{Z}_3 \cup \pi_1\mathbb{Z}_3 \cup \pi_2\mathbb{Z}_3 && \pi_0\mathbb{Z}_3 = \pi_1\mathbb{Z}_3 = \pi_2\mathbb{Z}_3 = \pi_i\mathbb{Z}_3 \\
&= \mathbb{Z}_3 \cup \pi_i\mathbb{Z}_3 && i \in \{0, 1, 2\} = \mathbb{Z}_{[0,3)} \\
&= \cdots && 3 \cdot 3 = 9 \text{ possibilities of combinations}
\end{aligned}$$

$$\mathbb{Z}_3 \trianglelefteq S_3 = D_3$$

$$\begin{aligned}
\rho_{k+3} &= \rho_k \\
\pi_{k+3} &= \pi_k \\
\rho_i\rho_j &= \rho_{i+j} \\
\rho_i\pi_j &= \pi_{i+j} \\
\pi_i\rho_j &= \pi_{i-j} \\
\pi_i\pi_j &= \rho_{i-j}
\end{aligned}$$

$$\begin{aligned}
\mathbb{Z}_3 &= \{0,1,2\} \\
&= \{0_\rho, 1_\rho, 2_\rho\} = \{[123],[231],[312]\} = \{(),(123),(132)\} && \leq S_3 \\
&= \left\{e^{i\frac{2\pi}{n}0}, e^{i\frac{2\pi}{n}1}, e^{i\frac{2\pi}{n}2}, \cdots, e^{i\frac{2\pi}{n}(n-1)}\right\} \overset{n=3}{=} \left\{e^{i\frac{2\pi}{3}0}, e^{i\frac{2\pi}{3}1}, e^{i\frac{2\pi}{3}2}\right\} \\
&= \{e, g, g^2, \cdots, g^{n-1}\} = \{g^0, g^1, g^2\} = \{e, g, g^2\}, g^n = e \\
&= \{e, \rho, \rho^2\} = \{\rho_0, \rho_1, \rho_2\} = \{\rho_j | j \in \{0,1,2\}\} && \leq D_3 = \{\rho_k, \pi_k\} = \{\rho_{k,3}, \pi_{k,3}\} \\
\rho_i\mathbb{Z}_3 &= \{\rho_i\rho_j | j \in \{0,1,2\}\} \\
&= \{\rho_{i+j} | j \in \{0,1,2\}\} \overset{i+j=j+i}{=} \{\rho_{j+i} | j \in \{0,1,2\}\} \\
&= \{\rho_j\rho_i | j \in \{0,1,2\}\} = \mathbb{Z}_3\rho_i && \Rightarrow \rho_i\mathbb{Z}_3 = \mathbb{Z}_3\rho_i \\
\pi_i\mathbb{Z}_3 &= \{\pi_i\rho_j | j \in \{0,1,2\}\} \\
&= \{\pi_{i-j} | j \in \{0,1,2\}\} \overset{\pi_{k+3}=\pi_k}{=} \{\pi_{3+i-j} | j \in \{0,1,2\}\} \\
&= \{\pi_{i+(3-j)} | 3-j \in \{3,2,1\}\} = \{\pi_{(3-j)+i} | 3-j \in \{3,2,1\}\} && i+(3-j) = (3-j)+i \\
&= \{\rho_{3-j}\pi_i | 3-j \in \{3,2,1\}\} = \{\rho_{3-j} | 3-j \in \{3,2,1\}\}\pi_i && \rho_i\pi_j = \pi_{i+j} \\
&= \{\rho_j | j \in \{0,1,2\}\}\pi_i = \mathbb{Z}_3\pi_i && \Rightarrow \pi_i\mathbb{Z}_3 = \mathbb{Z}_3\pi_i \\
&\Downarrow \\
\rho_i\mathbb{Z}_3 &= \mathbb{Z}_3\rho_i \\
\pi_i\mathbb{Z}_3 &= \mathbb{Z}_3\pi_i && \Rightarrow g\mathbb{Z}_3 = \mathbb{Z}_3 g \quad \forall g \in D_3 \\
&\Downarrow \\
\mathbb{Z}_3 &\leq D_3 = S_3 \\
g\mathbb{Z}_3 &= \mathbb{Z}_3 g \quad \forall g \in D_3 && \Rightarrow \mathbb{Z}_3 \trianglelefteq D_3 = S_3 \\
& && \Updownarrow \\
& && \mathbb{Z}_3 \trianglelefteq S_3 = D_3
\end{aligned}$$

$$\begin{aligned}
& & \rho_0 &= e \\
\rho_{k+3} &= \rho_k & \rho_0 &= \rho_3 \\
\pi_{k+3} &= \pi_k & k+x = 3 &\Rightarrow x = 3-k \\
\rho_i\rho_j &= \rho_{i+j} & \rho_k\rho_x = \rho_{k+x} = \rho_3 = \rho_0 &\Rightarrow \overline{\rho}_k = \rho_{3-k} = \rho_{-k} \\
\rho_i\pi_j &= \pi_{i+j} \\
\pi_i\rho_j &= \pi_{i-j} & k-x = 0 &\Rightarrow x = k \\
\pi_i\pi_j &= \rho_{i-j} & \pi_k\pi_x = \rho_{k-x} = \rho_0 &\Rightarrow \overline{\pi}_k = \pi_k
\end{aligned}$$

$$\rho_0 = e = he\overline{h} = h\overline{h} = e$$

$$x, y \in \{0,1,2\}$$

$$hg\overline{h} \overset{g=\rho_x}{=} h\rho_x\overline{h} \overset{h=\rho_y}{=} \rho_y\rho_x\overline{\rho}_y = \rho_y\rho_x\rho_{-y} = \rho_{y+x}\rho_{-y} = \rho_{y+x-y} = \rho_x = \rho_{3+x}$$

$$hg\overline{h} \overset{g=\rho_x}{=} h\rho_x\overline{h} \overset{h=\pi_y}{=} \pi_y\rho_x\overline{\pi}_y = \pi_y\rho_x\pi_y = \pi_{y-x}\pi_y = \rho_{y-x-y} = \rho_{-x} = \rho_{3-x}$$

$$hg\overline{h} \overset{g=\pi_x}{=} h\pi_x\overline{h} \overset{h=\rho_y}{=} \rho_y\pi_x\overline{\rho}_y = \rho_y\pi_x\rho_{-y} = \pi_{y+x}\rho_{-y} = \pi_{y+x-(-y)} = \pi_{2y+x}$$

$$hg\overline{h} \overset{g=\pi_x}{=} h\rho_x\overline{h} \overset{h=\pi_y}{=} \pi_y\pi_x\overline{\pi}_y = \pi_y\pi_x\pi_y = \rho_{y-x}\pi_y = \pi_{y-x+y} = \pi_{2y-x}$$

$$\rho_0 = e \in [e] = [\rho_0] = [\rho_{0+3}] = [\rho_{0+3k}] = [\rho_{3k}] = \{e\} = \{\rho_0\} \quad \forall k \in \mathbb{Z}$$

$$\rho_1 \in [\rho_1] = [\rho_{3-1}] = [\rho_2] = \{\rho_1, \rho_2\}$$

$$\pi_{2y+x} \in [\pi_{2y+x}] = [\pi_{2y+x \mod 3}] = [\pi_{2y-x \mod 3}] = \{\pi_0, \pi_1, \pi_2\}$$

$\cdot_{D_3}$	ρ_0	ρ_1	ρ_2	π_0	π_1	π_2
ρ_0	ρ_0	ρ_1	ρ_2	π_0	π_1	π_2
ρ_1	ρ_1	ρ_2	ρ_0	π_1	π_2	π_0
ρ_2	ρ_2	ρ_0	ρ_1	π_2	π_0	π_1
π_0	π_0	π_2	π_1	ρ_0	ρ_2	ρ_1
π_1	π_1	π_0	π_2	ρ_1	ρ_0	ρ_2
π_2	π_2	π_1	π_0	ρ_2	ρ_1	ρ_0
$\cdot_{S_3}$	e	(123)	(132)	$(3)(12)$	$(1)(23)$	$(2)(31)$
e	e	(123)	(132)	$(3)(12)$	$(1)(23)$	$(2)(31)$
(123)	(123)	(132)	e	$(1)(23)$	$(2)(31)$	$(3)(12)$
(132)	(132)	e	(123)	$(2)(31)$	$(3)(12)$	$(1)(23)$
$(3)(12)$	$(3)(12)$	$(2)(31)$	$(1)(23)$	e	(132)	(123)
$(1)(23)$	$(1)(23)$	$(3)(12)$	$(2)(31)$	(123)	e	(132)
$(2)(31)$	$(2)(31)$	$(1)(23)$	$(3)(12)$	(132)	(123)	e

$\cdot_{S_3}$	$[123]$	$[231]$	$[312]$	$[213]$	$[132]$	$[321]$
$[123]$	$[123]$	$[231]$	$[312]$	$[213]$	$[132]$	$[321]$
$[231]$	$[231]$	$[312]$	$[123]$	$[132]$	$[321]$	$[213]$
$[312]$	$[312]$	$[123]$	$[231]$	$[321]$	$[213]$	$[132]$
$[213]$	$[213]$	$[321]$	$[132]$	$[123]$	$[312]$	$[231]$
$[132]$	$[132]$	$[213]$	$[321]$	$[231]$	$[123]$	$[312]$
$[321]$	$[321]$	$[132]$	$[213]$	$[312]$	$[231]$	$[123]$
$\cdot_{S_3}$	$()$	(123)	(132)	(12)	(23)	(31)
$()$	$()$	(123)	(132)	(12)	(23)	(31)
(123)	(123)	(132)	$()$	(23)	(31)	(12)
(132)	(132)	$()$	(123)	(31)	(12)	(23)
(12)	(12)	(31)	(23)	$()$	(132)	(123)
(23)	(23)	(12)	(31)	(123)	$()$	(132)
(31)	(31)	(23)	(12)	(132)	(123)	$()$

$D_3 = S_3$

$$
\begin{aligned}
D_3 &= [e] \cup [\rho_1] \cup [\pi_0] = \{\rho_0\} \cup \{\rho_1, \rho_2\} \cup \{\pi_0, \pi_1, \pi_2\} \\
&= [e] \cup [\rho_2] \cup [\pi_1] = \{\rho_0\} \cup \{\rho_1, \rho_2\} \cup \{\pi_0, \pi_1, \pi_2\} \\
&= [\rho_0] \cup [\rho_2] \cup [\pi_2] = \{\rho_0\} \cup \{\rho_1, \rho_2\} \cup \{\pi_0, \pi_1, \pi_2\} \\
= S_3 &= [[123]] \cup [[231]] \cup [[213]] = \{[123]\} \cup \{[231], [312]\} \cup \{[213], [132], [321]\} \\
&= [[123]] \cup [[312]] \cup [[132]] = \{[123]\} \cup \{[231], [312]\} \cup \{[213], [132], [321]\} \\
&= [[123]] \cup [[312]] \cup [[321]] = \{[123]\} \cup \{[231], [312]\} \cup \{[213], [132], [321]\} \\
&= [()] \cup [(123)] \cup [(12)] = \{()\} \cup \{(123), (132)\} \cup \{(12), (23), (31)\} \\
&= [()] \cup [(132)] \cup [(23)] = \{()\} \cup \{(123), (132)\} \cup \{(12), (23), (31)\} \\
&= [()] \cup [(132)] \cup [(31)] = \{()\} \cup \{(123), (132)\} \cup \{(12), (23), (31)\}
\end{aligned}
$$

$\mathbb{Z}_3 \trianglelefteq S_3 = D_3$

$$
\begin{aligned}
\mathbb{Z}_3 &= [e] \cup [\rho_1] &&= \{\rho_0\} \cup \{\rho_1, \rho_2\} \\
&= [[123]] \cup [[231]] &&= \{[123]\} \cup \{[231], [312]\} \\
&= [()] \cup [(123)] &&= \{()\} \cup \{(123), (132)\}
\end{aligned}
$$

S_n

$S_n = (S_n, \cdot_{S_n}) = (S_n, \circ)$

$$
= \left\{ \sigma \left| \begin{array}{c} n \in \mathbb{N} \\ N = \left\{ \overbrace{1, \cdots, n}^{n} \right\} \\ \sigma \in N^N \\ \sigma(N) = N \end{array} \right. \right\} = \left\{ \sigma \left| \begin{array}{c} n \in \mathbb{N} \\ N = \{1, \cdots, n\} \\ \sigma : N \to N \\ \forall \sigma_i, \sigma_j \in S_n \, [\sigma_i \sigma_j = \sigma_i \circ \sigma_j] \\ \forall m_1, m_2 \in N \left[m_1 \neq m_2 \Leftrightarrow \sigma(m_1) \neq \sigma(m_2) \right] \end{array} \right. \right\}
$$

$$
= \left\{ \sigma \middle| \sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix} = \left(\overbrace{\begin{matrix} 1 & \cdots & n \\ \sigma(1) & \cdots & \sigma(n) \end{matrix}}^{n} \right) = \begin{pmatrix} 1 & \cdots & n \\ \sigma(1) & \cdots & \sigma(n) \end{pmatrix} \right\} \quad \text{two-line notation}
$$

$$
= \left\{ \sigma \middle| \sigma = \sigma(1)\sigma(2)\cdots\sigma(n) = \overbrace{\sigma(1)\sigma(2)\cdots\sigma(n)}^{n} = \sigma(1)\cdots\sigma(n) = [\sigma(1)\cdots\sigma(n)] \right\} \quad \text{one-line notation}
$$

$$
= \left\{ \sigma \middle| \sigma = c_1 c_2 \cdots c_{n_\sigma} = \overbrace{c_1 c_2 \cdots c_{n_\sigma}}^{n_\sigma} = c_1 \cdots c_{n_\sigma} = \overbrace{\underbrace{c_{11} c_{12} \cdots c_{1n_1}}_{c_1} \cdots \underbrace{c_{n_\sigma 1} c_{n_\sigma 2} \cdots c_{n_\sigma n_{n_\sigma}}}_{c_{n_\sigma}}}^{n_\sigma} \right\} \quad \text{cycle notation}
$$

$$
= \left\{ \sigma \middle| \sigma = s_1 s_2 \cdots s_{N_\sigma} = \overbrace{s_1 s_2 \cdots s_{N_\sigma}}^{N_\sigma} = s_1 \cdots s_{N_\sigma} = \overbrace{\underbrace{(s_{11} s_{12})}_{s_1} \cdots \underbrace{(s_{N_\sigma 1} s_{N_\sigma 2})}_{s_{N_\sigma}}}^{N_\sigma} \right\} \quad \text{swap notation}
$$

$$
\begin{aligned}
\sigma =& c_1 c_2 \cdots c_{n_\sigma} = \overbrace{c_1 c_2 \cdots c_{n_\sigma}}^{n_\sigma} = c_1 \cdots c_{n_\sigma} = \overbrace{c_1 \cdots c_{n_\sigma}}^{n_\sigma} \qquad c_i \cap c_j = \emptyset \\
=& \underbrace{c_{11} c_{12} \cdots c_{1n_1}}_{c_1} \underbrace{c_{21} c_{22} \cdots c_{2n_2}}_{c_2} \cdots \underbrace{c_{n_\sigma 1} c_{n_\sigma 2} \cdots c_{n_\sigma n_{n_\sigma}}}_{c_{n_\sigma}} \qquad c_{ij_1} \cap c_{ij_2} = \emptyset \\
=& \underbrace{c_{11} c_{12} \cdots c_{1n_1}}_{c_1} \cdots \underbrace{c_{n_\sigma 1} c_{n_\sigma 2} \cdots c_{n_\sigma n_{n_\sigma}}}_{c_{n_\sigma}} \\
=& \overbrace{\underbrace{c_{11} c_{12} \cdots c_{1n_1}}_{c_1} \cdots \underbrace{c_{n_\sigma 1} c_{n_\sigma 2} \cdots c_{n_\sigma n_{n_\sigma}}}_{c_{n_\sigma}}}^{n_\sigma}
\end{aligned}
$$

$$
\sum_{i=1}^{n_\sigma} n_i = n \qquad \forall n \in \mathbb{N}, \forall \sigma \in S_n
$$

cycle type

$$n_i$$

$$
[n_i] = [n_1 n_2 \cdots n_{n_\sigma}] = \left[1^{k_1} 2^{k_2} \cdots n^{k_n}\right] = \left[\ell^{k_\ell}\right]
$$

$$
S_3 \ni (3)\,(12) \to [n_i] = [n_1 n_2 \cdots n_{n_\sigma}] \overset{n_\sigma = 2}{=} [n_1 n_2] \overset{n_1=1, n_2=2}{=} [1 \cdot 2] = \left[1^1 2^1\right] = \left[1^{k_1} 2^{k_2} \cdots n^{k_n}\right] = \left[\ell^{k_\ell}\right]
$$

$$
\begin{aligned}
S_n \ni e = (1)\,(2)\,(3) \cdots (n) \to [n_i] = [n_1 n_2 \cdots n_{n_\sigma}] \\
\overset{n_\sigma = n}{=} [n_1 n_2 \cdots n_n] \overset{n_1=1, n_2=1, \cdots, n_n=1}{=} [1 \cdot 1 \cdot \cdots \cdot 1] = [1^n] = \left[1^{k_1} 2^{k_2} \cdots n^{k_n}\right] = \left[\ell^{k_\ell}\right]
\end{aligned}
$$

Young diagram
S_4: $\left[1^4\right] \times 1, \left[1^2 2\right] \times 6, \left[1^1 3^1\right] \times 8, \left[2^2\right] \times 3, \left[4^1\right] \times 6$
D_n

$$
D_n = \begin{cases} [\rho_{0,n}] \cup [\rho_{1,n}] \cup [\pi_{2m,n}] \cup [\pi_{2m-1,n}] & m \in \mathbb{Z}_{\left[0, \frac{n}{2}\right]}, n \in 2\mathbb{N} \\ [\rho_{0,n}] \cup [\rho_{1,n}] \cup [\pi_{m,n}] & m \in \mathbb{Z}_{[0, n-1]}, n \in 2\mathbb{N} - 1 \end{cases}
$$

$N \trianglelefteq G$

$$
\begin{aligned}
hN\overline{h} =& h\overline{h}N = eN = N \\
N =& hN\overline{h} = \left\{ hn\overline{h} \middle| \begin{matrix} n \in N \\ h \in G \end{matrix} \right\} = \bigcup_{n \in N} [n] \\
N =& \bigcup_{n \in N} [n] \\
[n] \subseteq& N \qquad\qquad\qquad \forall n \in N
\end{aligned}
$$

$$
\begin{array}{ccccccccc}
G & = & (g_0 N = eN = N) & \cup & (g_1 N) & \cup & (g_2 N) & \cup & \cdots \\
 & & \| & & & & & & \\
 & & [n_0] = [e] & & & & & & \\
 & & \cup & & & & & & \\
 & & [n_1] & & & & & & \\
 & & \cup & & & & & & \\
 & & [n_2] & & & & & & \\
 & & \cup & & & & & & \\
 & & \vdots & & & & & &
\end{array}
$$

8 homomorphism

- homomorphism 同態 = 均態 = 均形
- endomorphism 内同態 = 内態 = 内形 = 内均形
- isomorphism 同構 = 同形
- automorphism 自同構 = 自構 = 同形 = 自同形

定義 8.1. homomorphism

$$\begin{aligned}
&G \text{ is a group} && \Rightarrow G = (G, \cdot_G) \\
&g, \widetilde{g} \in G && \\
&\acute{G} \text{ is a group} && \Rightarrow \acute{G} = \left(\acute{G}, \cdot_{\acute{G}}\right) \\
&\acute{g}, \widetilde{\acute{g}} \in \acute{G} && \\
&\varphi : G \to \acute{G} && \Leftrightarrow G \xrightarrow{\varphi} \acute{G} \Leftrightarrow \varphi \in \acute{G}^G \\
& && \exists! \acute{g} = \varphi(g), \exists! \widetilde{\acute{g}} = \varphi(\widetilde{g}) \\
&\varphi(g \cdot_G \widetilde{g}) = \varphi(g) \cdot_{\acute{G}} \varphi(\widetilde{g}) && = \acute{g} \cdot_{\acute{G}} \widetilde{\acute{g}} \\
&\Downarrow && \\
&G \simeq \acute{G} && \text{homomorphism vs. isomorphism } G \cong \acute{G} \\
&\Updownarrow && \\
&G, \acute{G} \text{ have homomorphism} && \text{homomorphism map } \varphi
\end{aligned}$$

preserving the correspnding identity element

$$\begin{aligned}
\varphi(g) &= \varphi(e_G \cdot_G g) = \varphi(e \cdot_G g) = \varphi(e) \cdot_{\acute{G}} \varphi(g) \\
\varphi(g) &= \varphi(e) \cdot_{\acute{G}} \varphi(g) \\
&\Downarrow \\
\varphi(e) &= \acute{e} = e_{\acute{G}}
\end{aligned}$$

preserving the correspnding inverse element

$$\begin{aligned}
\acute{e} = e_{\acute{G}} = \varphi(e) &= \varphi(e_G) = \varphi(\overline{g} \cdot_G g) = \varphi(\overline{g}) \cdot_{\acute{G}} \varphi(g) \\
e_{\acute{G}} &= \varphi(\overline{g}) \cdot_{\acute{G}} \varphi(g) \\
&\Downarrow \\
\varphi(g^{-1}) = \varphi(\overline{g}) &= \overline{\varphi(g)} = [\varphi(g)]^{-1}
\end{aligned}$$

定義 8.2. endomorphism

$$\begin{aligned}
&G \text{ is a group} && \Rightarrow G = (G, \cdot_G) \\
&g, \widetilde{g} \in G && \\
&\varphi : G \to G && \Leftrightarrow G \xrightarrow{\varphi} G \Leftrightarrow \varphi \in G^G \\
& && \exists! \acute{g} = \varphi(g), \exists! \widetilde{\acute{g}} = \varphi(\widetilde{g}) \\
&\varphi(g \cdot_G \widetilde{g}) = \varphi(g) \cdot_{\acute{G}} \varphi(\widetilde{g}) && = \acute{g} \cdot_{\acute{G}} \widetilde{\acute{g}} \\
&\Downarrow && \\
&G \simeq G && \text{endomorphism vs. isomorphism } G \cong \acute{G} \\
&\Updownarrow && \\
&G \text{ has endomorphism} && \text{endomorphism map } \varphi
\end{aligned}$$

範例 8.3. $\mathcal{V} \simeq \acute{\mathcal{V}} \because \exists L : \mathcal{V} \to \acute{\mathcal{V}}$ linear map over two vector spaces(= additive Abelian groups + scalar multiplication)

$$\begin{aligned}
&\mathcal{V} \text{ is an additive Abelian group} && \Leftarrow \mathcal{V} = (\mathcal{V}, +_{\mathcal{V}}) = (\mathcal{V}, +_{\mathcal{V}}, \cdot_{\mathbb{F}\times\mathcal{V},\mathbb{F}}) \\
&\boldsymbol{v}, \widetilde{\boldsymbol{v}} \in \mathcal{V} \\
&\acute{\mathcal{V}} \text{ is an additive Abelian group} && \Leftarrow \acute{\mathcal{V}} = \left(\acute{\mathcal{V}}, +_{\acute{\mathcal{V}}}\right) = \left(\acute{\mathcal{V}}, +_{\acute{\mathcal{V}}}, \cdot_{\mathbb{F}\times\acute{\mathcal{V}},\mathbb{F}}\right) \\
&\acute{\boldsymbol{v}}, \widetilde{\acute{\boldsymbol{v}}} \in \acute{\mathcal{V}} \\
&L : \mathcal{V} \to \acute{\mathcal{V}} && \Leftrightarrow \mathcal{V} \xrightarrow{L} \acute{\mathcal{V}} \Leftrightarrow \varphi \in \acute{\mathcal{V}}^{\mathcal{V}} \\
& && \exists! \acute{\boldsymbol{v}} = L(\boldsymbol{v}), \exists! \widetilde{\acute{\boldsymbol{v}}} = L(\widetilde{\boldsymbol{v}}) \\
& && \text{linear map } L : L\left(\lambda \boldsymbol{v} +_{\mathcal{V}} \widetilde{\lambda}\widetilde{\boldsymbol{v}}\right) = \lambda L(\boldsymbol{v}) + \widetilde{\lambda}_{\acute{\mathcal{V}}} L(\widetilde{\boldsymbol{v}}) \\
& && \Downarrow \\
& && L(\boldsymbol{v} +_{\mathcal{V}} \widetilde{\boldsymbol{v}}) = L(\boldsymbol{v}) +_{\acute{\mathcal{V}}} L(\widetilde{\boldsymbol{v}}) \\
L(\boldsymbol{v} +_{\mathcal{V}} \widetilde{\boldsymbol{v}}) = &L(\boldsymbol{v}) +_{\acute{\mathcal{V}}} L(\widetilde{\boldsymbol{v}}) && = \acute{\boldsymbol{v}} \cdot_{\acute{\mathcal{V}}} \widetilde{\acute{\boldsymbol{v}}} \\
&\Downarrow \\
\mathcal{V} \simeq &\acute{\mathcal{V}} && \text{homomorphism vs. isomorphism } \mathcal{V} \cong \acute{\mathcal{V}} \\
&\Updownarrow \\
&\mathcal{V}, \acute{\mathcal{V}} \text{ have homomorphism} && \text{homomorphism map } L
\end{aligned}$$

preserving the correspnding identity element

$$L(\mathbf{0}_{\mathcal{V}}) = L(\mathbf{0}) = \acute{\mathbf{0}} = \mathbf{0}_{\acute{\mathcal{V}}}$$

preserving the correspnding inverse element

$$\begin{gathered}
L(\boldsymbol{v}) = \acute{\boldsymbol{v}} \\
\Downarrow \\
L(\overline{\boldsymbol{v}}) = L(-\boldsymbol{v}) = -\acute{\boldsymbol{v}} = \overline{\acute{\boldsymbol{v}}}
\end{gathered}$$

定義 8.4. general linear group

$$\begin{aligned}
GL_n = (GL_n, \cdot_{\mathcal{M}}) &= \left\{ A \middle| \begin{array}{r} A \in \mathcal{M}_{n\times n} \Leftrightarrow A = [a_{ij}]_{n\times n} \\ \forall A \in GL_n \left[\exists A^{-1} \in GL_n\right] \end{array} \right\} \\
&= \left\{ [a_{ij}]_{n\times n} \middle| \forall [a_{ij}]_{n\times n} \in GL_n \left[\exists \left([a_{ij}]_{n\times n}\right)^{-1} \in GL_n\right] \right\} \qquad \forall n \in \mathbb{N} \\
&= \left\{ \begin{array}{c} [a_{ij}]_{n\times n}, \\ \left([a_{ij}]_{n\times n}\right)^{-1} \end{array} \middle| \forall a_{ij} \right\} = \left\{ \begin{array}{c} A, \\ A^{-1} \end{array} \middle| \begin{array}{r} A \in \mathcal{M}_{n\times n} \\ \forall A \in GL_n \left[\exists A^{-1} \in GL_n\right] \end{array} \right\}
\end{aligned}$$

$$\begin{aligned}
GL(n, \mathbb{F}) = GL_n(\mathbb{F}) = (GL_n(\mathbb{F}), \cdot_{\mathcal{M}}) &= \left\{ A \middle| \begin{array}{r} A \in \mathcal{M}_{n\times n}(\mathbb{F}) \Leftrightarrow \begin{cases} a_{ij} \in \mathbb{F} \\ A = [a_{ij}]_{n\times n} \end{cases} \\ \forall A \in GL_n \left[\exists A^{-1} \in GL_n\right] \end{array} \right\} \\
&= \left\{ [a_{ij}]_{n\times n} \middle| \begin{array}{r} a_{ij} \in \mathbb{F} \\ \forall [a_{ij}]_{n\times n} \in GL_n \left[\exists \left([a_{ij}]_{n\times n}\right)^{-1} \in GL_n\right] \end{array} \right\} \qquad \forall n \in \mathbb{N} \\
&= \left\{ \begin{array}{c} [a_{ij}]_{n\times n}, \\ \left([a_{ij}]_{n\times n}\right)^{-1} \end{array} \middle| a_{ij} \in \mathbb{F} \right\} = \left\{ \begin{array}{c} A, \\ A^{-1} \end{array} \middle| \begin{array}{r} A \in \mathcal{M}_{n\times n}(\mathbb{F}) \\ \forall A \in GL_n(\mathbb{F}) \left[\exists A^{-1} \in GL_n(\mathbb{F})\right] \end{array} \right\}
\end{aligned}$$

$$\begin{aligned}
GL(n, \mathbb{R}) = GL_n(\mathbb{R}) = (GL_n(\mathbb{R}), \cdot_{\mathcal{M}}) &= \left\{ A \middle| \begin{array}{r} A \in \mathcal{M}_{n\times n}(\mathbb{R}) \Leftrightarrow \begin{cases} a_{ij} \in \mathbb{R} \\ A = [a_{ij}]_{n\times n} \end{cases} \\ \forall A \in GL_n \left[\exists A^{-1} \in GL_n\right] \end{array} \right\} \\
&= \left\{ [a_{ij}]_{n\times n} \middle| \begin{array}{r} a_{ij} \in \mathbb{R} \\ \forall [a_{ij}]_{n\times n} \in GL_n \left[\exists \left([a_{ij}]_{n\times n}\right)^{-1} \in GL_n\right] \end{array} \right\} \qquad \forall n \in \mathbb{N} \\
&= \left\{ \begin{array}{c} [a_{ij}]_{n\times n}, \\ \left([a_{ij}]_{n\times n}\right)^{-1} \end{array} \middle| a_{ij} \in \mathbb{R} \right\} = \left\{ \begin{array}{c} A, \\ A^{-1} \end{array} \middle| \begin{array}{r} A \in \mathcal{M}_{n\times n}(\mathbb{R}) \\ \forall A = [a_{ij}]_{n\times n} \left[\exists A^{-1} \in GL_n\right] \end{array} \right\} \\
&= \left\{ [a_{ij}]_{n\times n} \middle| \begin{array}{r} a_{ij} \in \mathbb{R} \\ \det [a_{ij}]_{n\times n} \neq 0 \end{array} \right\} = \left\{ [a_{ij}]_{n\times n} \middle| \begin{array}{r} a_{ij} \in \mathbb{R} \\ \det [a_{ij}]_{n\times n} \in \mathbb{R}_{\neq 0} \end{array} \right\}
\end{aligned}$$

$$GL(n,\mathbb{C})=GL_n(\mathbb{C})=(GL_n(\mathbb{C}),\cdot_{\mathcal{M}})=\left\{A\middle|\begin{array}{r}A\in\mathcal{M}_{n\times n}(\mathbb{C})\Leftrightarrow\begin{cases}a_{ij}\in\mathbb{C}\\A=[a_{ij}]_{n\times n}\end{cases}\\\forall A\in GL_n\left[\exists A^{-1}\in GL_n\right]\end{array}\right\}$$

$$=\left\{[a_{ij}]_{n\times n}\middle|\begin{array}{r}a_{ij}\in\mathbb{C}\\\forall[a_{ij}]_{n\times n}\in GL_n\left[\exists\left([a_{ij}]_{n\times n}\right)^{-1}\in GL_n\right]\end{array}\right\}\quad\forall n\in\mathbb{N}$$

$$=\left\{\begin{array}{c}[a_{ij}]_{n\times n},\\\left([a_{ij}]_{n\times n}\right)^{-1}\end{array}\middle|a_{ij}\in\mathbb{C}\right\}=\left\{\begin{array}{c}A,\\A^{-1}\end{array}\middle|\begin{array}{r}A\in\mathcal{M}_{n\times n}(\mathbb{C})\\\forall A\in GL_n(\mathbb{C})\left[\exists A^{-1}\in GL_n(\mathbb{C})\right]\end{array}\right\}$$

範例 8.5. $GL_2(\mathbb{R})\simeq\mathbb{R}_{\neq0}\because\exists\det:GL(2,\mathbb{R})=GL_2(\mathbb{R})\to\mathbb{R}_{\neq0}\subset\mathbb{R}$

$GL_2(\mathbb{R})$ is a multiplicative group $\Leftarrow GL_2(\mathbb{R})=(GL_2(\mathbb{R}),\cdot_{\mathcal{M}})$

$$=\left\{\begin{array}{c}A,\\A^{-1}\end{array}\middle|\begin{array}{r}A\in\mathcal{M}_{2\times2}(\mathbb{R})\\\forall A\in GL_2(\mathbb{R})\left[\exists A^{-1}\in GL_2(\mathbb{R})\right]\end{array}\right\}$$

$M,\widetilde{M}\in GL_2(\mathbb{R})$

$\mathbb{R}_{\neq0}$ is a multiplicative group $\Rightarrow\mathbb{R}_{\neq0}=(\mathbb{R}_{\neq0},\cdot_{\mathbb{R}})$

$r,\widetilde{r}\in\mathbb{R}$

$\det:GL_2(\mathbb{R})\to\mathbb{R}_{\neq0}\subset\mathbb{R}$ $\Leftrightarrow GL_2(\mathbb{R})\overset{\det}{\to}\mathbb{R}\Leftrightarrow\det\in\mathbb{R}^{GL_2(\mathbb{R})}$

$\exists!r=\det(M)=\det M,\exists!\widetilde{r}=\det\left(\widetilde{M}\right)=\det\widetilde{M}$

$$\det\left(M\cdot_{\mathcal{M}}\widetilde{M}\right)=\det\left(M\widetilde{M}\right)=\det(M)\cdot_{\mathbb{R}}\det\left(\widetilde{M}\right)=\det M\det\widetilde{M}\qquad=r\cdot_{\mathbb{R}}\widetilde{r}=r\widetilde{r}$$

$\Downarrow$

$GL_2(\mathbb{R})\simeq\mathbb{R}_{\neq0}$ homomorphism not mentioned isomorphism here

$\Updownarrow$

$GL_2(\mathbb{R})$,$\mathbb{R}_{\neq0}$ have homomorphism homomorphism map $\det$

範例 8.6. $\mathbb{R}\simeq U(1)\because\exists\exp\mathrm{i}:\mathbb{R}\to U(1)$

$\mathbb{R}$ is a additive group $\Leftarrow\mathbb{R}=(\mathbb{R},+_{\mathbb{R}})$

$\theta,\widetilde{\theta}\in\mathbb{R}$

$U(1)$ is a multiplicative group $\Leftarrow U(1)=(U(1),\cdot_{\mathbb{C}})=\{|z|=1|\forall z\in\mathbb{C}\}$

$=\left\{\mathrm{e}^{\mathrm{i}\theta}\middle|\forall\theta\in\mathbb{R}\right\}$

$u,\widetilde{u}\in U(1)$

$\exp\mathrm{i}:\mathbb{R}\to U(1)$ $\Leftrightarrow\mathbb{R}\overset{\exp\mathrm{i}}{\to}U(1)\Leftrightarrow\exp\mathrm{i}\in U(1)^{\mathbb{R}}$

$\exists!u=\exp\mathrm{i}(\theta)=\mathrm{e}^{\mathrm{i}\theta},\exists!\widetilde{u}=\exp\mathrm{i}\left(\widetilde{\theta}\right)=\mathrm{e}^{\mathrm{i}\widetilde{\theta}}$

$$\exp\mathrm{i}\left(\theta+_{\mathbb{R}}\widetilde{\theta}\right)=\mathrm{e}^{\mathrm{i}\left(\theta+\widetilde{\theta}\right)}=\mathrm{e}^{\mathrm{i}\theta}\mathrm{e}^{\mathrm{i}\widetilde{\theta}}=\exp\mathrm{i}(\theta)\cdot_{\mathbb{C}}\exp\mathrm{i}\left(\widetilde{\theta}\right)\qquad=u\cdot_{\mathbb{C}}\widetilde{u}=u\widetilde{u}$$

$\Downarrow$

$\mathbb{R}\simeq U(1)$ homomorphism not mentioned isomorphism here

$\Updownarrow$

$\mathbb{R}$,$U(1)$ have homomorphism homomorphism map $\exp\mathrm{i}$

$\exp\mathrm{i}(0)=\exp\mathrm{i}(2\pi)=\exp\mathrm{i}(2\pi k)=1\quad\forall k\in\mathbb{Z}\Rightarrow\exp\mathrm{i}$ is not 1-1 or 1-to-1

範例 8.7. $S_n\simeq\mathbb{Z}_2\because\exists\mathrm{sign}=\mathrm{sgn}:S_n\to\mathbb{Z}_2$

$$\begin{aligned}\sigma&=s_1s_2\cdots s_{N_\sigma}=\overbrace{s_1s_2\cdots s_{N_\sigma}}^{N_\sigma}=s_1\cdots s_{N_\sigma}=\overbrace{s_1\cdots s_{N_\sigma}}^{N_\sigma}\quad s_i\cap s_{i+1}=\{s_{(i)2}\}\\&=\underbrace{(s_{11}s_{12})}_{s_1}\underbrace{(s_{21}s_{22})}_{s_2}\cdots\underbrace{(s_{N_\sigma1}s_{N_\sigma2})}_{s_{N_\sigma}}\qquad s_{(i)2}=s_{(i+1)1}\\&=\underbrace{(s_{11}s_{12})}_{s_1}\cdots\underbrace{(s_{N_\sigma1}s_{N_\sigma2})}_{s_{N_\sigma}}\\&=\overbrace{\underbrace{(s_{11}s_{12})}_{s_1}\cdots\underbrace{(s_{N_\sigma1}s_{N_\sigma2})}_{s_{N_\sigma}}}^{N_\sigma}\end{aligned}$$

$$\sigma\begin{cases}\text{is an even permutation} & N_\sigma\in 2\mathbb{N}-2\\ \text{is an odd permutation} & N_\sigma\in 2\mathbb{N}-1\end{cases}\Leftrightarrow\sigma\begin{cases}\text{even} & N_\sigma\in 2\mathbb{Z}_{\geq 0}\\ \text{odd} & N_\sigma\in 2\mathbb{N}-1\end{cases}\quad\forall\sigma\in S_n$$

S_n is a group $\Leftarrow S_n=(S_n,\cdot_{S_n})=(S_n,\circ)$

$\sigma,\widetilde{\sigma}\in S_n$

$\mathbb{Z}_2$ is a group $\Leftarrow \mathbb{Z}_2=(\mathbb{Z}_2,\cdot_{\mathbb{C}})=\left\{\mathrm{e}^{\mathrm{i}\frac{2\pi}{2}0},\mathrm{e}^{\mathrm{i}\frac{2\pi}{2}(2-1)}\right\}$

$=\{\mathrm{e}^{\mathrm{i}0},\mathrm{e}^{\mathrm{i}\pi}\}$

$=\{-1,+1\}$

$\acute{\sigma},\widetilde{\acute{\sigma}}\in\mathbb{Z}_2$

$\mathrm{sign}=\mathrm{sgn}:S_n\to\mathbb{Z}_2$ $\Leftrightarrow S_n\overset{\mathrm{sgn}}{\to}\mathbb{Z}_2\Leftrightarrow\mathrm{sgn}\in\mathbb{Z}_2^{S_n}$

$$\mathrm{sgn}(\sigma)=\begin{cases}+1 & \sigma\text{ even}\Leftrightarrow N_\sigma\in 2\mathbb{Z}_{\geq 0}\\ -1 & \sigma\text{ odd}\Leftrightarrow N_\sigma\in 2\mathbb{N}-1\end{cases}$$

$\exists!\acute{\sigma}=\mathrm{sgn}(\sigma),\exists!\widetilde{\acute{\sigma}}=\mathrm{sgn}(\widetilde{\sigma})$

$\mathrm{sgn}(\sigma\cdot_{S_n}\widetilde{\sigma})=\mathrm{sgn}(\sigma\widetilde{\sigma})=\mathrm{sgn}(\sigma)\,\mathrm{sgn}(\widetilde{\sigma})=\mathrm{sgn}(\sigma)\cdot_{\mathbb{C}}\mathrm{sgn}(\widetilde{\sigma})$ $=\acute{\sigma}\cdot_{\mathbb{C}}\widetilde{\acute{\sigma}}$

$\Downarrow$

$S_n\simeq\mathbb{Z}_2$ homomorphism not mentioned isomorphism here

$\Updownarrow$

$S_n,\mathbb{Z}_2$ have homomorphism homomorphism map sgn

8.1 isomorphism

8.2 homomorphism kernel

Part II

tensor

9 tensor algebra

9.1 vector space

$$\mathbb{F}^n \in \{\mathbb{R}^n, \mathbb{C}^n, \mathbb{R}^\infty, \cdots\} \qquad \widetilde{\mathfrak{V}}, \mathfrak{V} \subseteq \mathcal{V} \subseteq \mathbb{F}^n \in \{\mathbb{R}^n, \mathbb{C}^n, \cdots\}$$

$$\mathcal{V} \ni \boldsymbol{v} = v^j \boldsymbol{v}_j = \sum_j v^j \boldsymbol{v}_j \qquad \boldsymbol{v}_j \in \mathfrak{V} = \{\boldsymbol{v}_j\} = \{\boldsymbol{v}_j\}_j$$

$$= \begin{cases} v^1 \boldsymbol{v}_1 + \cdots + v^n \boldsymbol{v}_n & = \sum_{j=1}^{n} v^j \boldsymbol{v}_j \\ \cdots + v^j \boldsymbol{v}_j + \cdots & = \sum_{j \in J} v^j \boldsymbol{v}_j \end{cases} \qquad = \begin{cases} \{\boldsymbol{v}_j\}_{j=1}^n \\ \{\boldsymbol{v}_j\}_{j \in J} & J \in \{\mathbb{N}, \mathbb{Z}, \mathbb{R}, \cdots\} \end{cases}$$

$$= \begin{cases} v^1 \begin{bmatrix} | \\ \boldsymbol{v}_1 \\ | \end{bmatrix} + \cdots + v^n \begin{bmatrix} | \\ \boldsymbol{v}_n \\ | \end{bmatrix} & = \begin{bmatrix} | & & | \\ \boldsymbol{v}_1 & \cdots & \boldsymbol{v}_n \\ | & & | \end{bmatrix} \begin{bmatrix} v^1 \\ \vdots \\ v^n \end{bmatrix} \\ \cdots + v^j \begin{bmatrix} | \\ \boldsymbol{v}_j \\ | \end{bmatrix} + \cdots & = \begin{bmatrix} & | & \\ \cdots & \boldsymbol{v}_j & \cdots \\ & | & \end{bmatrix} \begin{bmatrix} \vdots \\ v^j \\ \vdots \end{bmatrix} \end{cases} = \begin{bmatrix} \vdots \\ \boldsymbol{v}_j \\ \vdots \end{bmatrix}^{\intercal} \begin{bmatrix} \vdots \\ v^j \\ \vdots \end{bmatrix} = V\,[\boldsymbol{v}]_V \qquad [\boldsymbol{v}]_V \in \begin{cases} \mathbb{F}^n \\ \mathbb{F}^{|J|} \end{cases}$$

$$= \widetilde{v}^j \widetilde{\boldsymbol{v}}_j = \sum_j \widetilde{v}^j \widetilde{\boldsymbol{v}}_j \qquad \widetilde{\boldsymbol{v}}_j \in \widetilde{\mathfrak{V}} = \{\widetilde{\boldsymbol{v}}_j\} = \{\widetilde{\boldsymbol{v}}_j\}_j$$

$$= \begin{cases} \widetilde{v}^1 \widetilde{\boldsymbol{v}}_1 + \cdots + \widetilde{v}^n \widetilde{\boldsymbol{v}}_n & = \sum_{j=1}^{n} \widetilde{v}^j \widetilde{\boldsymbol{v}}_j \\ \cdots + \widetilde{v}^j \widetilde{\boldsymbol{v}}_j + \cdots & = \sum_{j \in J} \widetilde{v}^j \widetilde{\boldsymbol{v}}_j \end{cases} \qquad = \begin{cases} \{\widetilde{\boldsymbol{v}}_j\}_{j=1}^n \\ \{\widetilde{\boldsymbol{v}}_j\}_{j \in J} & J \in \{\mathbb{N}, \mathbb{Z}, \mathbb{R}, \cdots\} \end{cases}$$

$$= \begin{cases} \widetilde{v}^1 \begin{bmatrix} | \\ \widetilde{\boldsymbol{v}}_1 \\ | \end{bmatrix} + \cdots + \widetilde{v}^n \begin{bmatrix} | \\ \widetilde{\boldsymbol{v}}_n \\ | \end{bmatrix} & = \begin{bmatrix} | & & | \\ \widetilde{\boldsymbol{v}}_1 & \cdots & \widetilde{\boldsymbol{v}}_n \\ | & & | \end{bmatrix} \begin{bmatrix} \widetilde{v}^1 \\ \vdots \\ \widetilde{v}^n \end{bmatrix} \\ \cdots + \widetilde{v}^j \begin{bmatrix} | \\ \widetilde{\boldsymbol{v}}_j \\ | \end{bmatrix} + \cdots & = \begin{bmatrix} & | & \\ \cdots & \widetilde{\boldsymbol{v}}_j & \cdots \\ & | & \end{bmatrix} \begin{bmatrix} \vdots \\ \widetilde{v}^j \\ \vdots \end{bmatrix} \end{cases} = \begin{bmatrix} \vdots \\ \widetilde{\boldsymbol{v}}_j \\ \vdots \end{bmatrix}^{\intercal} \begin{bmatrix} \vdots \\ \widetilde{v}^j \\ \vdots \end{bmatrix} = \widetilde{V}\,[\boldsymbol{v}]_{\widetilde{V}} \qquad [\boldsymbol{v}]_{\widetilde{V}} \in \begin{cases} \mathbb{F}^n \\ \mathbb{F}^{|J|} \end{cases}$$

$$
\begin{aligned}
\boldsymbol{v} &= V\left[\boldsymbol{v}\right]_V = \widetilde{V}\left[\boldsymbol{v}\right]_{\widetilde{V}} \\
v^i &= V^i{}_j v^j = \widetilde{V}^i{}_j \widetilde{v}^j \\
v^k &= V^k{}_i v^i = \widetilde{V}^k{}_j \widetilde{v}^j \\
&\qquad \left[\boldsymbol{v}\right]_V = V^{-1}\widetilde{V}\left[\boldsymbol{v}\right]_{\widetilde{V}} = \overline{V}\widetilde{V}\left[\boldsymbol{v}\right]_{\widetilde{V}} \qquad = F\left[\boldsymbol{v}\right]_{\widetilde{V}} \\
&\qquad v^i = \left(V^k{}_i\right)^{-1}\widetilde{V}^k{}_j\widetilde{v}^j = \overline{V^k{}_i}\widetilde{V}^k{}_j\widetilde{v}^j \qquad = F^i{}_j\widetilde{v}^j \\
&\qquad = \left(V^{-1}\right)^i{}_k\widetilde{V}^k{}_j\widetilde{v}^j = \overline{V}^i{}_k\widetilde{V}^k{}_j\widetilde{v}^j \qquad = F^i{}_j\widetilde{v}^j \\
&\qquad \left(V^{-1}\right)^i{}_k\widetilde{V}^k{}_j = \overline{V}^i{}_k\widetilde{V}^k{}_j \qquad = F^i{}_j \\
F^i{}_j &= \left(V^{-1}\right)^i{}_k\widetilde{V}^k{}_j \\
&\quad \left(V^{-1}\right)^i{}_k = \left(V^k{}_i\right)^{-1} \\
&\qquad \left[\boldsymbol{v}\right]_{\widetilde{V}} = \widetilde{V}^{-1}V\left[\boldsymbol{v}\right]_V \qquad = B\left[\boldsymbol{v}\right]_V \\
&\qquad \widetilde{v}^j = \left(\widetilde{V}^k{}_j\right)^{-1}V^k{}_i v^i \qquad = B^j{}_i v^i \\
&\qquad = \left(\widetilde{V}^{-1}\right)^j{}_k V^k{}_i v^i \qquad = B^j{}_i v^i \\
&\qquad \left(\widetilde{V}^{-1}\right)^j{}_k V^k{}_i \qquad = B^j{}_i \\
B^j{}_i &= \left(\widetilde{V}^{-1}\right)^j{}_k V^k{}_i \\
&\quad \left(\widetilde{V}^{-1}\right)^j{}_k = \left(\widetilde{V}^k{}_j\right)^{-1}
\end{aligned}
$$

$$
\begin{aligned}
v^i\boldsymbol{v}_i &= \widetilde{v}^j\widetilde{\boldsymbol{v}}_j = \left(\widetilde{V}^k{}_j\right)^{-1}V^k{}_i v^i\widetilde{\boldsymbol{v}}_j = B^j{}_i v^i\widetilde{\boldsymbol{v}}_j \qquad \widetilde{v}^j = \left(\widetilde{V}^k{}_j\right)^{-1}V^k{}_i v^i = B^j{}_i v^i \\
v^i\boldsymbol{v}_i &= \left(\widetilde{V}^k{}_j\right)^{-1}V^k{}_i v^i\widetilde{\boldsymbol{v}}_j = B^j{}_i v^i\widetilde{\boldsymbol{v}}_j \qquad \cancel{v^i} \\
\boldsymbol{v}_i &= \left(\widetilde{V}^k{}_j\right)^{-1}V^k{}_i\widetilde{\boldsymbol{v}}_j = B^j{}_i\widetilde{\boldsymbol{v}}_j \\
\widetilde{v}^j\widetilde{\boldsymbol{v}}_j &= v^i\boldsymbol{v}_i = \left(V^k{}_i\right)^{-1}\widetilde{V}^k{}_j\widetilde{v}^j\boldsymbol{v}_i = F^i{}_j\widetilde{v}^j\boldsymbol{v}_i \qquad v^i = \left(V^k{}_i\right)^{-1}\widetilde{V}^k{}_j\widetilde{v}^j = F^i{}_j\widetilde{v}^j \\
\widetilde{v}^j\widetilde{\boldsymbol{v}}_j &= \left(V^k{}_i\right)^{-1}\widetilde{V}^k{}_j\widetilde{v}^j\boldsymbol{v}_i = F^i{}_j\widetilde{v}^j\boldsymbol{v}_i \qquad \cancel{\widetilde{v}^j} \\
\widetilde{\boldsymbol{v}}_j &= \left(V^k{}_i\right)^{-1}\widetilde{V}^k{}_j\boldsymbol{v}_i = F^i{}_j\boldsymbol{v}_i
\end{aligned}
$$

$$
\left\{
\begin{array}{l}
\left\{
\begin{array}{ll}
v^i = F^i{}_j\widetilde{v}^j = \left(V^{-1}\right)^i{}_k\widetilde{V}^k{}_j\widetilde{v}^j & \left[\boldsymbol{v}\right]_V = F\left[\boldsymbol{v}\right]_{\widetilde{V}} = V^{-1}\widetilde{V}\left[\boldsymbol{v}\right]_{\widetilde{V}} \\
\widetilde{v}^j = B^j{}_i v^i = \left(\widetilde{V}^{-1}\right)^j{}_k V^k{}_i v^i & \left[\boldsymbol{v}\right]_{\widetilde{V}} = B\left[\boldsymbol{v}\right]_V = \widetilde{V}^{-1}V\left[\boldsymbol{v}\right]_V
\end{array}
\right. \quad \text{contravariant} \\
\left\{
\begin{array}{ll}
\boldsymbol{v}_i = B^j{}_i\widetilde{\boldsymbol{v}}_j = \left(\widetilde{V}^k{}_j\right)^{-1}V^k{}_i\widetilde{\boldsymbol{v}}_j & \begin{bmatrix}\boldsymbol{v}_1\\ \vdots\\ \boldsymbol{v}_n\end{bmatrix}^{\intercal} = \begin{bmatrix}\widetilde{\boldsymbol{v}}_1\\ \vdots\\ \widetilde{\boldsymbol{v}}_n\end{bmatrix}^{\intercal} B = \begin{bmatrix}\widetilde{\boldsymbol{v}}_1\\ \vdots\\ \widetilde{\boldsymbol{v}}_n\end{bmatrix}^{\intercal}\widetilde{V}^{-1}V \\
\widetilde{\boldsymbol{v}}_j = F^i{}_j\boldsymbol{v}_i = \left(V^k{}_i\right)^{-1}\widetilde{V}^k{}_j\boldsymbol{v}_i & \begin{bmatrix}\widetilde{\boldsymbol{v}}_1\\ \vdots\\ \widetilde{\boldsymbol{v}}_n\end{bmatrix}^{\intercal} = \begin{bmatrix}\boldsymbol{v}_1\\ \vdots\\ \boldsymbol{v}_n\end{bmatrix}^{\intercal} F = \begin{bmatrix}\boldsymbol{v}_1\\ \vdots\\ \boldsymbol{v}_n\end{bmatrix}^{\intercal} V^{-1}\widetilde{V}
\end{array}
\right. \quad \text{covariant}
\end{array}
\right.
$$

$$
\left\{
\begin{array}{l}
\left\{
\begin{array}{ll}
v^i = F^i{}_j\widetilde{v}^j = \left(V^{-1}\right)^i{}_k\widetilde{V}^k{}_j\widetilde{v}^j & \begin{bmatrix}v^1\\ \vdots\\ v^n\end{bmatrix} = F\begin{bmatrix}\widetilde{v}^1\\ \vdots\\ \widetilde{v}^n\end{bmatrix} = V^{-1}\widetilde{V}\begin{bmatrix}\widetilde{v}^1\\ \vdots\\ \widetilde{v}^n\end{bmatrix} \\
\widetilde{v}^j = B^j{}_i v^i = \left(\widetilde{V}^{-1}\right)^j{}_k V^k{}_i v^i & \begin{bmatrix}\widetilde{v}^1\\ \vdots\\ \widetilde{v}^n\end{bmatrix} = B\begin{bmatrix}v^1\\ \vdots\\ v^n\end{bmatrix} = \widetilde{V}^{-1}V\begin{bmatrix}v^1\\ \vdots\\ v^n\end{bmatrix}
\end{array}
\right. \quad \text{contravariant} \\
\left\{
\begin{array}{ll}
\boldsymbol{v}_i = \widetilde{\boldsymbol{v}}_j B^j{}_i = \widetilde{\boldsymbol{v}}_j\left(\widetilde{V}^k{}_j\right)^{-1}V^k{}_i & \begin{bmatrix}\boldsymbol{v}_1\\ \vdots\\ \boldsymbol{v}_n\end{bmatrix}^{\intercal} = \begin{bmatrix}\widetilde{\boldsymbol{v}}_1\\ \vdots\\ \widetilde{\boldsymbol{v}}_n\end{bmatrix}^{\intercal} B = \begin{bmatrix}\widetilde{\boldsymbol{v}}_1\\ \vdots\\ \widetilde{\boldsymbol{v}}_n\end{bmatrix}^{\intercal}\widetilde{V}^{-1}V \\
\widetilde{\boldsymbol{v}}_j = \boldsymbol{v}_i F^i{}_j = \boldsymbol{v}_i\left(V^k{}_i\right)^{-1}\widetilde{V}^k{}_j & \begin{bmatrix}\widetilde{\boldsymbol{v}}_1\\ \vdots\\ \widetilde{\boldsymbol{v}}_n\end{bmatrix}^{\intercal} = \begin{bmatrix}\boldsymbol{v}_1\\ \vdots\\ \boldsymbol{v}_n\end{bmatrix}^{\intercal} F = \begin{bmatrix}\boldsymbol{v}_1\\ \vdots\\ \boldsymbol{v}_n\end{bmatrix}^{\intercal} V^{-1}\widetilde{V}
\end{array}
\right. \quad \text{covariant}
\end{array}
\right.
$$

$$\begin{cases} BF = \left(\widetilde{V}^{-1}V\right)\left(V^{-1}\widetilde{V}\right) = \widetilde{V}^{-1}\left(VV^{-1}\right)\widetilde{V} = \widetilde{V}^{-1}1\widetilde{V} = \widetilde{V}^{-1}\widetilde{V} = 1 & \Rightarrow B^k{}_iF^i{}_j = \delta^k{}_j \\ FB = \left(V^{-1}\widetilde{V}\right)\left(\widetilde{V}^{-1}V\right) = V^{-1}\left(\widetilde{V}\widetilde{V}^{-1}\right)V = V^{-1}1V = V^{-1}V = 1 & \Rightarrow F^i{}_jB^j{}_k = \delta^i{}_k \end{cases}$$

$$\begin{cases} \begin{cases} v^i = F^i{}_j\widetilde{v}^j = \left(V^{-1}\right)^i{}_k\widetilde{V}^k{}_j\widetilde{v}^j & \begin{bmatrix} v^1 \\ \vdots \\ v^n \end{bmatrix} = \begin{bmatrix} & \vdots & \\ \cdots & F^i{}_j & \cdots \\ & \vdots & \end{bmatrix}\begin{bmatrix} \widetilde{v}^1 \\ \vdots \\ \widetilde{v}^n \end{bmatrix} = V^{-1}\widetilde{V}\begin{bmatrix} \widetilde{v}^1 \\ \vdots \\ \widetilde{v}^n \end{bmatrix} \\ \widetilde{v}^j = B^j{}_iv^i = \left(\widetilde{V}^{-1}\right)^j{}_kV^k{}_iv^i & \begin{bmatrix} \widetilde{v}^1 \\ \vdots \\ \widetilde{v}^n \end{bmatrix} = \begin{bmatrix} & \vdots & \\ \cdots & B^j{}_i & \cdots \\ & \vdots & \end{bmatrix}\begin{bmatrix} v^1 \\ \vdots \\ v^n \end{bmatrix} = \widetilde{V}^{-1}V\begin{bmatrix} v^1 \\ \vdots \\ v^n \end{bmatrix} \end{cases} & \text{contravariant} \\ \begin{cases} \boldsymbol{v}_i = \widetilde{\boldsymbol{v}}_jB^j{}_i = \widetilde{\boldsymbol{v}}_j\left(\widetilde{V}^k{}_j\right)^{-1}V^k{}_i & \begin{bmatrix} \boldsymbol{v}_1 \\ \vdots \\ \boldsymbol{v}_n \end{bmatrix}^\intercal = \begin{bmatrix} \widetilde{\boldsymbol{v}}_1 \\ \vdots \\ \widetilde{\boldsymbol{v}}_n \end{bmatrix}^\intercal\begin{bmatrix} & \vdots & \\ \cdots & B^j{}_i & \cdots \\ & \vdots & \end{bmatrix} = \begin{bmatrix} \widetilde{\boldsymbol{v}}_1 \\ \vdots \\ \widetilde{\boldsymbol{v}}_n \end{bmatrix}^\intercal\widetilde{V}^{-1}V \\ \widetilde{\boldsymbol{v}}_j = \boldsymbol{v}_iF^i{}_j = \boldsymbol{v}_i\left(V^k{}_i\right)^{-1}\widetilde{V}^k{}_j & \begin{bmatrix} \widetilde{\boldsymbol{v}}_1 \\ \vdots \\ \widetilde{\boldsymbol{v}}_n \end{bmatrix}^\intercal = \begin{bmatrix} \boldsymbol{v}_1 \\ \vdots \\ \boldsymbol{v}_n \end{bmatrix}^\intercal\begin{bmatrix} & \vdots & \\ \cdots & F^i{}_j & \cdots \\ & \vdots & \end{bmatrix} = \begin{bmatrix} \boldsymbol{v}_1 \\ \vdots \\ \boldsymbol{v}_n \end{bmatrix}^\intercal V^{-1}\widetilde{V} \end{cases} & \text{covariant} \end{cases}$$

We do not denote $V\left[\boldsymbol{v}\right]_V = V\left[\boldsymbol{v}\right]_{\mathfrak{V}}$, because $\mathfrak{V}$ can have elements or bases in different orders whereas V cannot.

9.2 dual space

$$\begin{cases} \boldsymbol{v} \in \mathcal{V} \subseteq \mathbb{F}^n \in \left\{\mathbb{R}^n, \mathbb{C}^n, \cdots\right\} \\ \exists! \omega \in \mathbb{F}\left[\boldsymbol{\omega}\left(\boldsymbol{v}\right) = \omega\right] \end{cases} \Leftrightarrow \mathcal{V} \overset{\boldsymbol{\omega}}{\to} \mathbb{F} \Leftrightarrow \boldsymbol{\omega} : \mathcal{V} \to \mathbb{F}$$

$$\Leftrightarrow \mathbb{F}^{\mathcal{V}} = \left\{\boldsymbol{\omega} | \boldsymbol{\omega} : \mathcal{V} \to \mathbb{F}\right\}$$

$$\Downarrow$$

$$\left|\mathbb{F}^{\mathcal{V}}\right| = \left|\mathbb{F}\right|^{|\mathcal{V}|}$$

$$\begin{matrix} \boldsymbol{v}^1\left(\boldsymbol{v}_1\right) = 1 & \cdots & \boldsymbol{v}^1\left(\boldsymbol{v}_j\right) & \cdots & \boldsymbol{v}^1\left(\boldsymbol{v}_n\right) \\ \vdots & & \vdots & & \vdots \\ \boldsymbol{v}^i\left(\boldsymbol{v}_1\right) & \cdots & \boldsymbol{v}^i\left(\boldsymbol{v}_j\right) \overset{\text{def.}}{=} \begin{cases} 1 & j = i \\ 0 & j \neq i \end{cases} = \delta^i_j & \cdots & \boldsymbol{v}^i\left(\boldsymbol{v}_n\right) \\ \vdots & & \vdots & & \vdots \\ \boldsymbol{v}^n\left(\boldsymbol{v}_1\right) & \cdots & \boldsymbol{v}^n\left(\boldsymbol{v}_j\right) & \cdots & \boldsymbol{v}^n\left(\boldsymbol{v}_n\right) = 1 \end{matrix}$$

$$\boldsymbol{v}^i\left(\boldsymbol{v}\right) = \boldsymbol{v}^i\left(v^j\boldsymbol{v}_j\right) = v^j\boldsymbol{v}^i\left(\boldsymbol{v}_j\right) \overset{\text{def.}}{=} v^j\delta^i_j = v^i$$

$$
\begin{cases}
\boldsymbol{\omega} \in \mathcal{V}^* = (\mathcal{V}^*, \mathbb{F}, +, \cdot) = (\mathcal{V}^*, \mathbb{F}, +_{\mathcal{V}^*,\mathbb{F}}, \cdot_{\mathbb{F}\times\mathcal{V}^*,\mathbb{F}}) \\
\boldsymbol{v} \in \mathcal{V} = (\mathcal{V}, \mathbb{F}, +, \cdot) = (\mathcal{V}, \mathbb{F}, +_{\mathcal{V},\mathbb{F}}, \cdot_{\mathbb{F}\times\mathcal{V},\mathbb{F}})
\end{cases}
$$

$$
\begin{aligned}
\boldsymbol{\omega}(\boldsymbol{v}) =& \boldsymbol{\omega}(v^j \boldsymbol{v}_j) = v^j \boldsymbol{\omega}(\boldsymbol{v}_j) \\
=& \boldsymbol{\omega}\left(\sum_j v^j \boldsymbol{v}_j\right) = \sum_j \boldsymbol{\omega}(v^j \boldsymbol{v}_j) = \sum_j v^j \boldsymbol{\omega}(\boldsymbol{v}_j) \\
=& \begin{cases}
\boldsymbol{\omega}(v^1 \boldsymbol{v}_1 + \cdots + v^n \boldsymbol{v}_n) & = \boldsymbol{\omega}\left(\sum_{j=1}^n v^j \boldsymbol{v}_j\right) \\
\boldsymbol{\omega}(\cdots + v^j \boldsymbol{v}_j + \cdots) & = \boldsymbol{\omega}\left(\sum_{j\in J} v^j \boldsymbol{v}_j\right)
\end{cases} && + = +_{\mathcal{V},\mathbb{F}} \\
=& \begin{cases}
v^1 \boldsymbol{\omega}(\boldsymbol{v}_1) + \cdots + v^n \boldsymbol{\omega}(\boldsymbol{v}_n) & = \sum_{j=1}^n v^j \boldsymbol{\omega}(\boldsymbol{v}_j) \\
\cdots + v^j \boldsymbol{\omega}(\boldsymbol{v}_j) + \cdots & = \sum_{j\in J} v^j \boldsymbol{\omega}(\boldsymbol{v}_j)
\end{cases} && + = +_{\mathcal{V}^*,\mathbb{F}} \\
=& v^j \boldsymbol{\omega}(\boldsymbol{v}_j) = \boldsymbol{v}^j(\boldsymbol{v})\, \boldsymbol{\omega}(\boldsymbol{v}_j) && v^j = \boldsymbol{v}^j(\boldsymbol{v}) \Leftarrow \boldsymbol{v}^i(\boldsymbol{v}) = v^i \Leftarrow \boldsymbol{v}^i(\boldsymbol{v}_j) \overset{\text{def.}}{=} \delta^i_j \\
=& \boldsymbol{v}^j(\boldsymbol{v})\, \omega^{\boldsymbol{v}}_j = \omega^{\boldsymbol{v}}_j \boldsymbol{v}^j(\boldsymbol{v}) = \omega^{\boldsymbol{v}}_i \boldsymbol{v}^i(\boldsymbol{v}) && \omega^{\boldsymbol{v}}_j \overset{\text{def.}}{=} \boldsymbol{\omega}(\boldsymbol{v}_j) \\
\boldsymbol{\omega}(\boldsymbol{v}) =& \omega^{\boldsymbol{v}}_i \boldsymbol{v}^i(\boldsymbol{v}) \\
\boldsymbol{\omega} =& \omega^{\boldsymbol{v}}_i \boldsymbol{v}^i
\end{aligned}
$$

$$
\begin{aligned}
\mathcal{V}^* \ni \boldsymbol{\omega} =& \omega_i \boldsymbol{\omega}^i = \sum_i \omega_i \boldsymbol{\omega}^i = \begin{cases}
\omega_1 \boldsymbol{\omega}^1 + \cdots + \omega_n \boldsymbol{\omega}^n & = \sum_{i=1}^n \omega_i \boldsymbol{\omega}^i \\
\cdots + \omega_i \boldsymbol{\omega}^i + \cdots & = \sum_{i\in I} \omega_i \boldsymbol{\omega}^i
\end{cases} \\
=& \omega^{\boldsymbol{v}}_i \boldsymbol{v}^i = \sum_i \omega^{\boldsymbol{v}}_i \boldsymbol{v}^i = \begin{cases}
\omega^{\boldsymbol{v}}_1 \boldsymbol{v}^1 + \cdots + \omega^{\boldsymbol{v}}_n \boldsymbol{v}^n & = \sum_{i=1}^n \omega^{\boldsymbol{v}}_i \boldsymbol{v}^i \\
\cdots + \omega^{\boldsymbol{v}}_i \boldsymbol{v}^i + \cdots & = \sum_{i\in I} \omega^{\boldsymbol{v}}_i \boldsymbol{v}^i
\end{cases} \\
=& \begin{cases}
\omega^{\boldsymbol{v}}_1 \begin{bmatrix} | \\ \boldsymbol{v}^1 \\ | \end{bmatrix}^\intercal + \cdots + \omega^{\boldsymbol{v}}_n \begin{bmatrix} | \\ \boldsymbol{v}^n \\ | \end{bmatrix}^\intercal & = \begin{bmatrix} \omega^{\boldsymbol{v}}_1 \\ \vdots \\ \omega^{\boldsymbol{v}}_n \end{bmatrix}^\intercal \begin{bmatrix} — & \boldsymbol{v}^1 & — \\ & \vdots & \\ — & \boldsymbol{v}^n & — \end{bmatrix} \\
\cdots + \omega^{\boldsymbol{v}}_i \begin{bmatrix} | \\ \boldsymbol{v}^i \\ | \end{bmatrix}^\intercal + \cdots & = \begin{bmatrix} \vdots \\ \omega^{\boldsymbol{v}}_i \\ \vdots \end{bmatrix}^\intercal \begin{bmatrix} & \vdots & \\ — & \boldsymbol{v}^i & — \\ & \vdots & \end{bmatrix}
\end{cases} = \begin{bmatrix} \vdots \\ \omega^{\boldsymbol{v}}_i \\ \vdots \end{bmatrix}^\intercal \begin{bmatrix} \vdots \\ \boldsymbol{v}^i \\ \vdots \end{bmatrix} \quad = [\boldsymbol{\omega}]^V\, V^* \\
=& \omega^{\widetilde{\boldsymbol{v}}}_i \widetilde{\boldsymbol{v}}^i = \sum_i \omega^{\widetilde{\boldsymbol{v}}}_i \widetilde{\boldsymbol{v}}^i = \begin{cases}
\omega^{\widetilde{\boldsymbol{v}}}_1 \widetilde{\boldsymbol{v}}^1 + \cdots + \omega^{\widetilde{\boldsymbol{v}}}_n \widetilde{\boldsymbol{v}}^n & = \sum_{i=1}^n \omega^{\widetilde{\boldsymbol{v}}}_i \widetilde{\boldsymbol{v}}^i \\
\cdots + \omega^{\widetilde{\boldsymbol{v}}}_i \widetilde{\boldsymbol{v}}^i + \cdots & = \sum_{i\in I} \omega^{\widetilde{\boldsymbol{v}}}_i \widetilde{\boldsymbol{v}}^i
\end{cases} \\
=& \begin{cases}
\omega^{\widetilde{\boldsymbol{v}}}_1 \begin{bmatrix} | \\ \widetilde{\boldsymbol{v}}^1 \\ | \end{bmatrix}^\intercal + \cdots + \omega^{\widetilde{\boldsymbol{v}}}_n \begin{bmatrix} | \\ \widetilde{\boldsymbol{v}}^n \\ | \end{bmatrix}^\intercal & = \begin{bmatrix} \omega^{\widetilde{\boldsymbol{v}}}_1 \\ \vdots \\ \omega^{\widetilde{\boldsymbol{v}}}_n \end{bmatrix}^\intercal \begin{bmatrix} — & \widetilde{\boldsymbol{v}}^1 & — \\ & \vdots & \\ — & \widetilde{\boldsymbol{v}}^n & — \end{bmatrix} \\
\cdots + \omega^{\widetilde{\boldsymbol{v}}}_i \begin{bmatrix} | \\ \widetilde{\boldsymbol{v}}^i \\ | \end{bmatrix}^\intercal + \cdots & = \begin{bmatrix} \vdots \\ \omega^{\widetilde{\boldsymbol{v}}}_i \\ \vdots \end{bmatrix}^\intercal \begin{bmatrix} & \vdots & \\ — & \widetilde{\boldsymbol{v}}^i & — \\ & \vdots & \end{bmatrix}
\end{cases} = \begin{bmatrix} \vdots \\ \omega^{\widetilde{\boldsymbol{v}}}_i \\ \vdots \end{bmatrix}^\intercal \begin{bmatrix} \vdots \\ \widetilde{\boldsymbol{v}}^i \\ \vdots \end{bmatrix} \quad = [\boldsymbol{\omega}]^{\widetilde{V}}\, \widetilde{V}^*
\end{aligned}
$$

$$
\begin{aligned}
\boldsymbol{\omega} = [\boldsymbol{\omega}]^{V} V^* &= [\boldsymbol{\omega}]^{\widetilde{V}} \widetilde{V}^* \\
&= \omega_i^{\boldsymbol{v}} {V^*}^i{}_k = \omega_j^{\widetilde{\boldsymbol{v}}} {\widetilde{V}^*}{}^j{}_k \\
\omega_j^{\widetilde{\boldsymbol{v}}} {\widetilde{V}^*}{}^j{}_k &= \omega_i^{\boldsymbol{v}} {V^*}^i{}_k \\
\omega_j^{\widetilde{\boldsymbol{v}}} &= \omega_i^{\boldsymbol{v}} {V^*}^i{}_k \left({\widetilde{V}^*}{}^j{}_k\right)^{-1} = \omega_i^{\boldsymbol{v}} {V^*}^i{}_k \left(\widetilde{V}^{*-1}\right)^k{}_j = \omega_i^{\boldsymbol{v}} Q^i{}_j \\
\boldsymbol{\omega}\left(\widetilde{\boldsymbol{v}}_j\right) = \omega_j^{\widetilde{\boldsymbol{v}}} &= \omega_i^{\boldsymbol{v}} Q^i{}_j = \boldsymbol{\omega}\left(\boldsymbol{v}_i\right) Q^i{}_j = \boldsymbol{\omega}\left(\widetilde{\boldsymbol{v}}_k B^k{}_i\right) Q^i{}_j = \boldsymbol{\omega}\left(\widetilde{\boldsymbol{v}}_k\right) B^k{}_i Q^i{}_j \\
\boldsymbol{\omega}\left(\widetilde{\boldsymbol{v}}_j\right) &= \boldsymbol{\omega}\left(\widetilde{\boldsymbol{v}}_k\right) B^k{}_i Q^i{}_j \\
B^k{}_i Q^i{}_j &= \delta^k{}_j \Rightarrow Q^i{}_j = F^i{}_j \\
\omega_j^{\widetilde{\boldsymbol{v}}} &= \omega_i^{\boldsymbol{v}} Q^i{}_j = \omega_i^{\boldsymbol{v}} F^i{}_j \\
\omega_j^{\widetilde{\boldsymbol{v}}} &= \omega_i^{\boldsymbol{v}} F^i{}_j \Rightarrow \begin{bmatrix} \vdots \\ \omega_i^{\widetilde{\boldsymbol{v}}} \\ \vdots \end{bmatrix}^{\intercal} = \begin{bmatrix} \vdots \\ \omega_i^{\boldsymbol{v}} \\ \vdots \end{bmatrix}^{\intercal} F \\
\omega_k^{\widetilde{\boldsymbol{v}}} B^k{}_j &= \omega_i^{\boldsymbol{v}} F^i{}_k B^k{}_j = \omega_i^{\boldsymbol{v}} \delta^i{}_j = \omega_j^{\boldsymbol{v}} \\
\omega_j^{\boldsymbol{v}} &= \omega_k^{\widetilde{\boldsymbol{v}}} B^k{}_j \Rightarrow \begin{bmatrix} \vdots \\ \omega_i^{\boldsymbol{v}} \\ \vdots \end{bmatrix}^{\intercal} = \begin{bmatrix} \vdots \\ \omega_i^{\widetilde{\boldsymbol{v}}} \\ \vdots \end{bmatrix}^{\intercal} B
\end{aligned}
$$

$$
\begin{aligned}
\omega_j^{\widetilde{\boldsymbol{v}}} B^j{}_i \boldsymbol{v}^i = \omega_i^{\boldsymbol{v}} \boldsymbol{v}^i &= \omega_i^{\widetilde{\boldsymbol{v}}} \widetilde{\boldsymbol{v}}^i = \omega_j^{\boldsymbol{v}} F^j{}_i \widetilde{\boldsymbol{v}}^i \\
\omega_j^{\widetilde{\boldsymbol{v}}} B^j{}_i \boldsymbol{v}^i &= \omega_j^{\widetilde{\boldsymbol{v}}} \widetilde{\boldsymbol{v}}^j \Rightarrow B^j{}_i \boldsymbol{v}^i = \widetilde{\boldsymbol{v}}^j \Rightarrow \widetilde{\boldsymbol{v}}^j = B^k{}_i \boldsymbol{v}^i \\
\omega_j^{\boldsymbol{v}} F^j{}_i \widetilde{\boldsymbol{v}}^i &= \omega_j^{\boldsymbol{v}} \boldsymbol{v}^i \Rightarrow F^j{}_i \widetilde{\boldsymbol{v}}^i = \boldsymbol{v}^j \Rightarrow \boldsymbol{v}^j = F^j{}_i \widetilde{\boldsymbol{v}}^i
\end{aligned}
$$

$$
\left\{
\begin{array}{ll}
\left\{
\begin{array}{lll}
\omega_j^{\boldsymbol{v}} = \omega_k^{\widetilde{\boldsymbol{v}}} B^k{}_j & \begin{bmatrix} \vdots \\ \omega_i^{\boldsymbol{v}} \\ \vdots \end{bmatrix}^{\intercal} = \begin{bmatrix} \vdots \\ \omega_i^{\widetilde{\boldsymbol{v}}} \\ \vdots \end{bmatrix}^{\intercal} B \\
\omega_j^{\widetilde{\boldsymbol{v}}} = \omega_i^{\boldsymbol{v}} F^i{}_j & \begin{bmatrix} \vdots \\ \omega_i^{\widetilde{\boldsymbol{v}}} \\ \vdots \end{bmatrix}^{\intercal} = \begin{bmatrix} \vdots \\ \omega_i^{\boldsymbol{v}} \\ \vdots \end{bmatrix}^{\intercal} F
\end{array}
\right. & \text{covariant} \\
\left\{
\begin{array}{ll}
\boldsymbol{v}^j = F^j{}_i \widetilde{\boldsymbol{v}}^i & \begin{bmatrix} \vdots \\ \boldsymbol{v}^i \\ \vdots \end{bmatrix} = F \begin{bmatrix} \vdots \\ \widetilde{\boldsymbol{v}}^i \\ \vdots \end{bmatrix} \\
\widetilde{\boldsymbol{v}}^j = B^k{}_i \boldsymbol{v}^i & \begin{bmatrix} \vdots \\ \widetilde{\boldsymbol{v}}^i \\ \vdots \end{bmatrix} = B \begin{bmatrix} \vdots \\ \boldsymbol{v}^i \\ \vdots \end{bmatrix}
\end{array}
\right. & \text{contravariant}
\end{array}
\right.
$$

$$
\left\{
\begin{array}{ll}
\left\{
\begin{array}{ll}
\boldsymbol{v}^j = F^j{}_i \widetilde{\boldsymbol{v}}^i & \begin{bmatrix} \vdots \\ \boldsymbol{v}^i \\ \vdots \end{bmatrix} = F \begin{bmatrix} \vdots \\ \widetilde{\boldsymbol{v}}^i \\ \vdots \end{bmatrix} \\
\widetilde{\boldsymbol{v}}^j = B^k{}_i \boldsymbol{v}^i & \begin{bmatrix} \vdots \\ \widetilde{\boldsymbol{v}}^i \\ \vdots \end{bmatrix} = B \begin{bmatrix} \vdots \\ \boldsymbol{v}^i \\ \vdots \end{bmatrix}
\end{array}
\right. & \text{contravariant} \\
\left\{
\begin{array}{ll}
\omega_j^{\boldsymbol{v}} = \omega_k^{\widetilde{\boldsymbol{v}}} B^k{}_j & \begin{bmatrix} \vdots \\ \omega_i^{\boldsymbol{v}} \\ \vdots \end{bmatrix}^{\intercal} = \begin{bmatrix} \vdots \\ \omega_i^{\widetilde{\boldsymbol{v}}} \\ \vdots \end{bmatrix}^{\intercal} B \\
\omega_j^{\widetilde{\boldsymbol{v}}} = \omega_i^{\boldsymbol{v}} F^i{}_j & \begin{bmatrix} \vdots \\ \omega_i^{\widetilde{\boldsymbol{v}}} \\ \vdots \end{bmatrix}^{\intercal} = \begin{bmatrix} \vdots \\ \omega_i^{\boldsymbol{v}} \\ \vdots \end{bmatrix}^{\intercal} F
\end{array}
\right. & \text{covariant}
\end{array}
\right.
$$

$$\begin{array}{ccc} \text{covariant} & \text{contravariant} & \\ \left.\begin{matrix}\widetilde{\mathfrak{V}}\\ \mathfrak{V}\end{matrix}\right\} \ni \begin{cases}\widetilde{\boldsymbol{v}}_j = \boldsymbol{v}_i F^i{}_j \\ \boldsymbol{v}_j = \widetilde{\boldsymbol{v}}_i B^i{}_j\end{cases} & \mathbb{F} \ni \begin{cases}\widetilde{v}^i = B^i{}_j v^j \\ v^i = F^i{}_j \widetilde{v}^j\end{cases} & \text{vector space } \mathcal{V} \ni \boldsymbol{v} = \boldsymbol{v}_j v^j \\ \mathbb{F} \ni \begin{cases}\omega_j^{\widetilde{\boldsymbol{v}}} = \omega_i^{\boldsymbol{v}} F^i{}_j \\ \omega_j^{\boldsymbol{v}} = \omega_k^{\widetilde{\boldsymbol{v}}} B^k{}_j\end{cases} & \left.\begin{matrix}\widetilde{\mathfrak{V}}^*\\ \mathfrak{V}^*\end{matrix}\right\} \ni \begin{cases}\widetilde{\boldsymbol{v}}^i = B^i{}_j \boldsymbol{v}^j \\ \boldsymbol{v}^i = F^i{}_j \widetilde{\boldsymbol{v}}^j\end{cases} & \text{dual space } \mathcal{V}^* \ni \boldsymbol{\omega} = \omega_i^{\boldsymbol{v}} \boldsymbol{v}^i \end{array}$$

$$\widetilde{\boldsymbol{v}}_j \widetilde{v}^j = \boldsymbol{v}_i F^i{}_j B^j{}_k v^k = \boldsymbol{v}_i \delta^i{}_k v^k = \begin{cases}\boldsymbol{v}_k v^k & \boldsymbol{v}_k = \boldsymbol{v}_i \delta^i{}_k \\ \boldsymbol{v}_i v^i & \delta^i{}_k v^k = v^i\end{cases} = v^j \boldsymbol{v}_j$$

9.3 linear map transformation

$$\begin{cases}\boldsymbol{v} \in \mathcal{V} \subseteq \mathbb{F}^n \in \{\mathbb{R}^n, \mathbb{C}^n, \cdots\} \\ \exists! \boldsymbol{w} \in \mathcal{W}\left[L(\boldsymbol{v}) = \boldsymbol{w}\right]\end{cases} \begin{aligned} &\Leftrightarrow \mathcal{V} \xrightarrow{L} \mathcal{W} \Leftrightarrow L : \mathcal{V} \to \mathcal{W} \\ &\Leftrightarrow \mathcal{W}^{\mathcal{V}} = \{L | L : \mathcal{V} \to \mathcal{W}\} \\ &\Downarrow \\ &\left|\mathcal{W}^{\mathcal{V}}\right| = |\mathcal{W}|^{|\mathcal{V}|} \end{aligned}$$

$$\boldsymbol{w} = L(\boldsymbol{v}) = L(v^j \boldsymbol{v}_j) = v^j L(\boldsymbol{v}_j)$$

$$\begin{aligned} L(\boldsymbol{v}_1) =& \boldsymbol{v}_1 L^1{}_1 + \cdots + \boldsymbol{v}_n L^n{}_1 = \begin{bmatrix} | \\ \boldsymbol{v}_1 \\ | \end{bmatrix} L^1{}_1 + \cdots + \begin{bmatrix} | \\ \boldsymbol{v}_n \\ | \end{bmatrix} L^n{}_1 = \begin{bmatrix} | & & | \\ \boldsymbol{v}_1 & \cdots & \boldsymbol{v}_n \\ | & & | \end{bmatrix} \begin{bmatrix} L^1{}_1 \\ \vdots \\ L^n{}_1 \end{bmatrix} \\ \vdots & \\ L(\boldsymbol{v}_j) =& \boldsymbol{v}_1 L^1{}_j + \cdots + \boldsymbol{v}_n L^n{}_j = \begin{bmatrix} | \\ \boldsymbol{v}_1 \\ | \end{bmatrix} L^1{}_j + \cdots + \begin{bmatrix} | \\ \boldsymbol{v}_n \\ | \end{bmatrix} L^n{}_j = \begin{bmatrix} | & & | \\ \boldsymbol{v}_1 & \cdots & \boldsymbol{v}_n \\ | & & | \end{bmatrix} \begin{bmatrix} L^1{}_j \\ \vdots \\ L^n{}_j \end{bmatrix} \\ \vdots & \\ L(\boldsymbol{v}_n) =& \boldsymbol{v}_1 L^1{}_n + \cdots + \boldsymbol{v}_n L^n{}_n = \begin{bmatrix} | \\ \boldsymbol{v}_1 \\ | \end{bmatrix} L^1{}_n + \cdots + \begin{bmatrix} | \\ \boldsymbol{v}_n \\ | \end{bmatrix} L^n{}_n = \begin{bmatrix} | & & | \\ \boldsymbol{v}_1 & \cdots & \boldsymbol{v}_n \\ | & & | \end{bmatrix} \begin{bmatrix} L^1{}_n \\ \vdots \\ L^n{}_n \end{bmatrix} \end{aligned}$$

$$\begin{aligned} \begin{bmatrix} | & & | \\ L(\boldsymbol{v}_1) & \cdots & L(\boldsymbol{v}_n) \\ | & & | \end{bmatrix} &= \begin{bmatrix} | & & | \\ \boldsymbol{v}_1 & \cdots & \boldsymbol{v}_n \\ | & & | \end{bmatrix} \begin{bmatrix} L^1{}_1 & & L^1{}_n \\ \vdots & \dots & \vdots \\ L^n{}_1 & & L^n{}_n \end{bmatrix} \\ \boldsymbol{w} = L(\boldsymbol{v}) = v^j L(\boldsymbol{v}_j) = \begin{bmatrix} | & & | \\ L(\boldsymbol{v}_1) & \cdots & L(\boldsymbol{v}_n) \\ | & & | \end{bmatrix} \begin{bmatrix} v^1 \\ \vdots \\ v^n \end{bmatrix} &= \begin{bmatrix} | & & | \\ \boldsymbol{v}_1 & \cdots & \boldsymbol{v}_n \\ | & & | \end{bmatrix} \begin{bmatrix} L^1{}_1 & & L^1{}_n \\ \vdots & \dots & \vdots \\ L^n{}_1 & & L^n{}_n \end{bmatrix} \begin{bmatrix} v^1 \\ \vdots \\ v^n \end{bmatrix} \\ = \begin{bmatrix} & | & \\ \cdots & L(\boldsymbol{v}_n) & \cdots \\ & | & \end{bmatrix} \begin{bmatrix} \vdots \\ v^j \\ \vdots \end{bmatrix} &= \begin{bmatrix} & | & \\ \cdots & \boldsymbol{v}_i & \cdots \\ & | & \end{bmatrix} \begin{bmatrix} & \vdots & \\ \cdots & L^i{}_j & \cdots \\ & \vdots & \end{bmatrix} \begin{bmatrix} \vdots \\ v^j \\ \vdots \end{bmatrix} \\ = \boldsymbol{v}_i w_{\boldsymbol{v}}^i =& \boldsymbol{v}_i L^i{}_j v^j & w_{\boldsymbol{v}}^i = L^i{}_j v^j \\ = \widetilde{\boldsymbol{v}}_i w_{\widetilde{\boldsymbol{v}}}^i =& \widetilde{\boldsymbol{v}}_i \widetilde{L}^i{}_j \widetilde{v}^j & w_{\widetilde{\boldsymbol{v}}}^i = \widetilde{L}^i{}_j \widetilde{v}^j \\ \widetilde{\boldsymbol{v}}_h B^h{}_i L^i{}_j F^j{}_k \widetilde{v}^k = \boldsymbol{v}_i L^i{}_j v^j =& \widetilde{\boldsymbol{v}}_i \widetilde{L}^i{}_j \widetilde{v}^j = \boldsymbol{v}_h F^h{}_i \widetilde{L}^i{}_j B^j{}_k v^k \\ \widetilde{\boldsymbol{v}}_h B^h{}_i L^i{}_j F^j{}_k \widetilde{v}^k =& \widetilde{\boldsymbol{v}}_h \widetilde{L}^h{}_k \widetilde{v}^k & \widetilde{L}^h{}_k = B^h{}_i L^i{}_j F^j{}_k \\ \boldsymbol{v}_h F^h{}_i \widetilde{L}^i{}_j B^j{}_k v^k =& \boldsymbol{v}_h L^h{}_k v^k & L^h{}_k = F^h{}_i \widetilde{L}^i{}_j B^j{}_k \end{aligned}$$

covariant $(0,1)$-tensor contravariant $(1,0)$-tensor

$$\left.\begin{array}{c}\widetilde{\mathfrak{V}}\\ \mathfrak{V}\end{array}\right\} \ni \begin{cases}\widetilde{\boldsymbol{v}}_j = \boldsymbol{v}_i F^i{}_j\\ \boldsymbol{v}_j = \widetilde{\boldsymbol{v}}_i B^i{}_j\end{cases} \qquad \mathbb{F} \ni \begin{cases}\widetilde{v}^i = B^i{}_j v^j\\ v^i = F^i{}_j \widetilde{v}^j\end{cases} \qquad \text{vector space } \mathcal{V} \ni \boldsymbol{v} = \boldsymbol{v}_j v^j$$

$$\mathbb{F} \ni \begin{cases}\omega^{\widetilde{\boldsymbol{v}}}_j = \omega^{\boldsymbol{v}}_i F^i{}_j\\ \omega^{\boldsymbol{v}}_j = \omega^{\widetilde{\boldsymbol{v}}}_k B^k{}_j\end{cases} \qquad \left.\begin{array}{c}\widetilde{\mathfrak{V}}^*\\ \mathfrak{V}^*\end{array}\right\} \ni \begin{cases}\widetilde{\boldsymbol{v}}^i = B^i{}_j \boldsymbol{v}^j\\ \boldsymbol{v}^i = F^i{}_j \widetilde{\boldsymbol{v}}^j\end{cases} \qquad \text{dual space } \mathcal{V}^* \ni \boldsymbol{\omega} = \omega^{\boldsymbol{v}}_i \boldsymbol{v}^i$$

$(1,1)$-tensor $\qquad \mathcal{V} \xrightarrow{L} \mathcal{W}$

$$\begin{cases}\widetilde{L}^h{}_k = B^h{}_i L^i{}_j F^j{}_k\\ L^h{}_k = F^h{}_i \widetilde{L}^i{}_j B^j{}_k\end{cases} \qquad \text{vector space } \mathcal{W} \ni \boldsymbol{v} = \boldsymbol{v}_j v^j$$

9.4 metric tensor

$$\begin{aligned}\|\boldsymbol{v}\|^2 = \boldsymbol{v}\cdot\boldsymbol{v} &= (\boldsymbol{v}_i v^i)\cdot(\boldsymbol{v}_j v^j) = (\boldsymbol{v}_i\cdot\boldsymbol{v}_j)\, v^i v^j = g_{ij} v^i v^j = v^i\,(\boldsymbol{v}_i\cdot\boldsymbol{v}_j)\, v^j = v^i g_{ij} v^j\\ &= (\widetilde{\boldsymbol{v}}_i \widetilde{v}^i)\cdot(\widetilde{\boldsymbol{v}}_j \widetilde{v}^j) = (\widetilde{\boldsymbol{v}}_i\cdot\widetilde{\boldsymbol{v}}_j)\, \widetilde{v}^i \widetilde{v}^j = \widetilde{g}_{ij} \widetilde{v}^i \widetilde{v}^j = \widetilde{v}^i\,(\widetilde{\boldsymbol{v}}_i\cdot\widetilde{\boldsymbol{v}}_j)\, \widetilde{v}^j = \widetilde{v}^i \widetilde{g}_{ij} \widetilde{v}^j\\ &= g_{ij} v^i v^j = \widetilde{g}_{ij} \widetilde{v}^i \widetilde{v}^j = \widetilde{g}_{hk} B^h{}_i v^i B^k{}_j v^j = \widetilde{g}_{hk} B^h{}_i B^k{}_j v^i v^j \qquad g_{ij} = \widetilde{g}_{hk} B^h{}_i B^k{}_j\\ &= \widetilde{g}_{ij} \widetilde{v}^i \widetilde{v}^j = g_{ij} v^i v^j = g_{hk} F^h{}_i \widetilde{v}^i F^k{}_j \widetilde{v}^j = g_{hk} F^h{}_i F^k{}_j \widetilde{v}^i \widetilde{v}^j \qquad \widetilde{g}_{ij} = g_{hk} F^h{}_i F^k{}_j\end{aligned}$$

covariant $(0,1)$-tensor contravariant $(1,0)$-tensor

$$\left.\begin{array}{c}\widetilde{\mathfrak{V}}\\ \mathfrak{V}\end{array}\right\} \ni \begin{cases}\widetilde{\boldsymbol{v}}_j = \boldsymbol{v}_i F^i{}_j\\ \boldsymbol{v}_j = \widetilde{\boldsymbol{v}}_i B^i{}_j\end{cases} \qquad \mathbb{F} \ni \begin{cases}\widetilde{v}^i = B^i{}_j v^j\\ v^i = F^i{}_j \widetilde{v}^j\end{cases} \qquad \text{vector space } \mathcal{V} \ni \boldsymbol{v} = \boldsymbol{v}_j v^j$$

$$\mathbb{F} \ni \begin{cases}\omega^{\widetilde{\boldsymbol{v}}}_j = \omega^{\boldsymbol{v}}_i F^i{}_j\\ \omega^{\boldsymbol{v}}_j = \omega^{\widetilde{\boldsymbol{v}}}_k B^k{}_j\end{cases} \qquad \left.\begin{array}{c}\widetilde{\mathfrak{V}}^*\\ \mathfrak{V}^*\end{array}\right\} \ni \begin{cases}\widetilde{\boldsymbol{v}}^i = B^i{}_j \boldsymbol{v}^j\\ \boldsymbol{v}^i = F^i{}_j \widetilde{\boldsymbol{v}}^j\end{cases} \qquad \text{dual space } \mathcal{V}^* \ni \boldsymbol{\omega} = \omega^{\boldsymbol{v}}_i \boldsymbol{v}^i$$

$(1,1)$-tensor $\qquad \mathcal{V} \xrightarrow{L} \mathcal{W}$

$$\begin{cases}\widetilde{L}^h{}_k = B^h{}_i L^i{}_j F^j{}_k\\ L^h{}_k = F^h{}_i \widetilde{L}^i{}_j B^j{}_k\end{cases} \qquad \text{vector space } \mathcal{W} \ni \boldsymbol{v} = \boldsymbol{v}_j v^j$$

$(0,2)$-tensor $\qquad \mathcal{V}^2 \xrightarrow{g} \mathbb{R}_{\geq 0}$

$$\mathbb{R}^{\mathcal{V}^2}_{\geq 0} \ni \begin{cases}\widetilde{g}_{ij} = g_{hk} F^h{}_i F^k{}_j\\ g_{ij} = \widetilde{g}_{hk} B^h{}_i B^k{}_j\end{cases} \qquad \text{metric space } \mathcal{V}\times\mathcal{V} \xrightarrow{g} \mathbb{F}$$

$$\begin{aligned}\boldsymbol{u}\cdot\boldsymbol{v} &= (\boldsymbol{u}_i u^i)\cdot(\boldsymbol{v}_j v^j) = (\boldsymbol{u}_i\cdot\boldsymbol{v}_j)\, u^i v^j = g_{ij} u^i v^j = u^i\,(\boldsymbol{u}_i\cdot\boldsymbol{v}_j)\, v^j = u^i g_{ij} v^j\\ &= (\widetilde{\boldsymbol{u}}_i \widetilde{u}^i)\cdot(\widetilde{\boldsymbol{v}}_j \widetilde{v}^j) = (\widetilde{\boldsymbol{u}}_i\cdot\widetilde{\boldsymbol{v}}_j)\, \widetilde{u}^i \widetilde{v}^j = \widetilde{g}_{ij} \widetilde{u}^i \widetilde{v}^j = \widetilde{u}^i\,(\widetilde{\boldsymbol{u}}_i\cdot\widetilde{\boldsymbol{v}}_j)\, \widetilde{v}^j = \widetilde{u}^i \widetilde{g}_{ij} \widetilde{v}^j\end{aligned}$$

9.5 bilinear form

10 tensor calculus

11 spinor

Part III
relativity