

group, tensor, spinor

Joey Yu Hsu, MD

since 2024/05

Contents

1	coloring	1
1.1	single coloring	1
1.2	recolor = coloring with regular expression (= RegEx = re)	2
I	group theory	2
2	basic definition	2
3	finite group	4
3.1	cyclic group	4
3.2	permutation group or symmetric group	5
3.3	dihedral group	10
4	subgroup	13
5	coset	19
5.1	left coset space	26
6	normal subgroup	30
6.1	quotient group	32
6.2	simple group	35
7	conjugate class	36
8	homomorphism	41
8.1	isomorphism	46
8.2	homomorphism kernel	46
II	tensor	46
9	tensor algebra	46
9.1	vector space	46
9.2	dual space	48
9.3	linear map transformation	51
9.4	metric tensor	52
9.5	bilinear form	52
10	tensor calculus	52
11	spinor	52
III	relativity	52
1	coloring	
1.1	single coloring	

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

also can be put into “preamble”

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

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

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

定理 2.2.

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

定理 2.3.

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

定理 2.4. rearrangement theorem

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

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

$$\begin{aligned}
 & \forall g \in G, \exists \bar{g} \in G \left[\bar{g}g = e = g\bar{g} \right] \\
 & \quad \Downarrow \\
 & \forall f \in G \left[f = ef \stackrel{e=\bar{g}g}{=} (g\bar{g})f \stackrel{(a)}{=} g(\bar{g}f) \right] \Rightarrow \forall f \in G [f = g(\bar{g}f)] \stackrel{(c)\bar{g}f \in G}{\Rightarrow} f \in \{g\bar{g}|\bar{g} \in G\} \\
 & \quad \Downarrow \\
 & \forall f \in G [f \in \{g\bar{g}|\bar{g} \in G\}] \\
 & \quad \Downarrow \\
 & G \subseteq \{g\bar{g}|\bar{g} \in G\} \\
 & \{g\bar{g}|\bar{g} \in G\} \subseteq G \because (e) \cdot_G \text{ closure} \\
 & \quad \Downarrow \\
 & G = \{g\bar{g}|\bar{g} \in G\}
 \end{aligned}$$

□

推論 2.5.

$$\begin{cases} \forall g \in G [g \in \{g\bar{g}|\bar{g} \in G\}] & (l) \text{ lossless} = \text{complete} \\ \forall g_1, g_2 \in G = \{g\bar{g}|\bar{g} \in G\} \Rightarrow_{g_1 \bar{g}_1 \neq g_2 \bar{g}_2} & (r) \text{ repeatless} = \text{rearrange} \\ g_1 \neq g_2 \end{cases}$$

定義 2.6. exponentiation or power

$$\begin{aligned}
 g^n &= \overbrace{g \cdot_G g \cdot_G \cdots_G g}^n = \overbrace{g \cdot g \cdots g}^n = \overbrace{g \cdots g}^n = \overbrace{g \cdots g}^n & n \in \mathbb{N} \\
 g^{-n} &= \bar{g}^n = \overbrace{\bar{g} \cdot_G \bar{g} \cdot_G \cdots_G \bar{g}}^n = \overbrace{\bar{g} \cdot \bar{g} \cdots \bar{g}}^n = \overbrace{\bar{g} \cdots \bar{g}}^n = \overbrace{\bar{g} \cdots \bar{g}}^n & n \in \mathbb{N} \\
 & \bar{g}g = e = g\bar{g} \\
 g^0 &= g^n \bar{g}^n = \bar{g}^n g^n = (\bar{g}^{n-1} \bar{g}) (g g^{n-1}) = \bar{g}^{n-1} (\bar{g}g) g^{n-1} = \bar{g}^{n-1} (e) g^{n-1} = \cdots = e \\
 g^0 &= e \\
 g^k &= \begin{cases} g^k & k > 0 \\ e & k = 0 \\ \bar{g}^{|k|} = g^{-|k|} & k < 0 \end{cases} & k \in \mathbb{Z}
 \end{aligned}$$

定義 2.7. infinite group vs. finite group

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

定義 2.8. discrete group vs. Lie group

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

定義 2.9. commutative group = Abelian group

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

定義 2.10. trivial group

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

3 finite group

3.1 cyclic group

定義 3.1. cyclic group

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

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

\mathbb{Z}_2

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

$$+_{\mathbb{Z}_2} \begin{array}{cc} 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{array}$$

\mathbb{Z}_3

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

$$+_{\mathbb{Z}_3} \begin{array}{ccc} 0 & 1 & 2 \\ 0 & (0 \bmod 3) & (1 \bmod 3) & (2 \bmod 3) \\ 1 & (1 \bmod 3) & (2 \bmod 3) & (3 \bmod 3) \\ 2 & (2 \bmod 3) & (3 \bmod 3) & (4 \bmod 3) \end{array} \rightarrow +_{\mathbb{Z}_3} \begin{array}{ccc} 0 & 1 & 2 \\ 0 & 0 & 1 & 2 \\ 1 & 1 & 2 & 0 \\ 2 & 2 & 0 & 1 \end{array}$$

定理 3.2.

$$\forall n \in \mathbb{N} \left[\begin{array}{l} +_{\mathbb{Z}_n} \text{ commutative} \Rightarrow \mathbb{Z}_n \text{ is an Abelian group} \\ \Updownarrow \\ \mathbb{Z}_n \text{ is a commutative group} \end{array} \right]$$

complex multiplication

定理 3.3.

$$e^{i \frac{2\pi}{n} k_1} e^{i \frac{2\pi}{n} k_2} = e^{i \frac{2\pi}{n} k_1} \cdot_{\mathbb{C}} e^{i \frac{2\pi}{n} k_2} = e^{i \frac{2\pi}{n} (k_1 + k_2)} \bmod n \quad \begin{array}{l} \forall k_1, k_2 \in \mathbb{Z} \\ |k_1|, |k_2| < n \in \mathbb{N} \end{array}$$

\mathbb{Z}_n

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

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

$$\begin{aligned}
\mathbb{Z}_3 & \\
\mathbb{Z}_3 &= (\mathbb{Z}_3, +) = (\mathbb{Z}_3, +_{\mathbb{Z}_3}) = \{0, 1, 3-1\} = \{0, 1, 2\} \\
\mathbb{Z}_3 &= (\mathbb{Z}_3, \cdot) = (\mathbb{Z}_3, \cdot_{\mathbb{C}}) = \left\{ e^{i\frac{2\pi}{3}0}, e^{i\frac{2\pi}{3}1}, e^{i\frac{2\pi}{3}(3-1)} \right\} = \left\{ e^{i0}, e^{i\frac{2\pi}{3}}, e^{i\frac{4\pi}{3}} \right\} = \left\{ 1, \frac{-1}{2} + i\frac{\sqrt{3}}{2}, \frac{-1}{2} - i\frac{\sqrt{3}}{2} \right\}
\end{aligned}$$

$$\begin{aligned}
\mathbb{Z}_4 & \\
\mathbb{Z}_4 &= (\mathbb{Z}_4, +) = (\mathbb{Z}_4, +_{\mathbb{Z}_4}) = \{0, 1, 2, 4-1\} = \{0, 1, 2, 3\} \\
\mathbb{Z}_4 &= (\mathbb{Z}_4, \cdot) = (\mathbb{Z}_4, \cdot_{\mathbb{C}}) = \left\{ e^{i\frac{2\pi}{4}0}, e^{i\frac{2\pi}{4}1}, e^{i\frac{2\pi}{4}2}, e^{i\frac{2\pi}{4}(4-1)} \right\} = \left\{ e^{i0}, e^{i\frac{\pi}{2}}, e^{i\pi}, e^{i\frac{3\pi}{2}} \right\} = \{1, i, -1, -i\}
\end{aligned}$$

3.2 permutation group or symmetric group

定義 3.4. permutation

$$\begin{aligned}
N &= \{1, 2, \dots, n\} = \{1, \dots, n\} = \left\{ \overbrace{1, \dots, n}^n \right\} & \text{finite set by } n \in \mathbb{N} \\
\sigma \in N^N &\Leftrightarrow \sigma : N \rightarrow N \Leftrightarrow N \xrightarrow{\sigma} N & \text{autofunction over } N = \mathbb{N}_{\leq n \in \mathbb{N}} = \mathbb{N}_{\leq n} \\
\sigma(N) &= N & \sigma(N) \text{ range equals codomain } N \Leftrightarrow \sigma \text{ is a permutation}
\end{aligned}$$

定義 3.5. permutation group = symmetric group

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

S_1

$$\begin{aligned}
\sigma(1) &= 1 \\
S_1 &= \{\sigma\} = \{e\} = \{e_{S_1}\} = \{\text{id}\} \\
\sigma\sigma(1) &= \sigma \cdot_{S_n} \sigma(1) = \sigma \circ \sigma(1) = \sigma(\sigma(1)) = \sigma(1) = 1 = \sigma(1) \\
\sigma\sigma(1) &= \sigma(1) \\
\sigma\sigma &= \sigma = \sigma \cdot_{S_n} \sigma = \sigma \circ \sigma \\
S_1 &= \left\{ \begin{array}{c} \sigma \\ 1 \rightarrow 1 = \sigma(1) \end{array} \right\} = \left\{ \begin{array}{c} \sigma_1 \\ 1 \rightarrow 1 = \sigma_1(1) \end{array} \right\} \\
&= \left\{ \begin{array}{c} 1 \\ \downarrow \\ 1 \end{array} \right\} = \left\{ \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\}
\end{aligned}$$

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

S_2

$$\begin{aligned} S_2 &= \left\{ \begin{array}{cc} \sigma_1 & \sigma_2 \\ 1 \rightarrow 1 = \sigma_1(1) & 1 \rightarrow 2 = \sigma_2(1) \\ 2 \rightarrow 2 = \sigma_1(2) & 2 \rightarrow 1 = \sigma_2(2) \end{array} \right\} = \left\{ \begin{array}{c} e \\ \parallel \\ e_{S_2} \end{array}, \sigma_2 \right\} \\ &= \left\{ \begin{array}{cc} \sigma_1 & \sigma_2 \\ \downarrow & \downarrow \\ 1 & 2 \end{array}, \begin{array}{cc} \downarrow & \downarrow \\ 2 & 1 \end{array} \right\} = \left\{ \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\} \end{aligned}$$

$$\begin{aligned} \sigma_1 \sigma_1(1) &= \sigma_1 \cdot_{S_n} \sigma_1(1) = \sigma_1 \circ \sigma_1(1) = \sigma_1(\sigma_1(1)) = \sigma_1(1) = 1 = \sigma_1(1) \\ \sigma_1 \sigma_1(2) &= \sigma_1 \cdot_{S_n} \sigma_1(2) = \sigma_1 \circ \sigma_1(2) = \sigma_1(\sigma_1(2)) = \sigma_1(2) = 2 = \sigma_1(2) \\ \sigma_1 \sigma_1 &= \sigma_1 \\ \sigma_2 \sigma_1(1) &= \sigma_2 \cdot_{S_n} \sigma_1(1) = \sigma_2 \circ \sigma_1(1) = \sigma_2(\sigma_1(1)) = \sigma_2(1) = 2 = \sigma_2(1) \\ \sigma_2 \sigma_1(2) &= \sigma_2 \cdot_{S_n} \sigma_1(2) = \sigma_2 \circ \sigma_1(2) = \sigma_2(\sigma_1(2)) = \sigma_2(2) = 1 = \sigma_2(2) \\ \sigma_2 \sigma_1 &= \sigma_2 \\ \sigma_1 \sigma_2(1) &= \sigma_1 \cdot_{S_n} \sigma_2(1) = \sigma_1 \circ \sigma_2(1) = \sigma_1(\sigma_2(1)) = \sigma_1(2) = 2 = \sigma_2(1) \\ \sigma_1 \sigma_2(2) &= \sigma_1 \cdot_{S_n} \sigma_2(2) = \sigma_1 \circ \sigma_2(2) = \sigma_1(\sigma_2(2)) = \sigma_1(1) = 1 = \sigma_2(2) \\ \sigma_1 \sigma_2 &= \sigma_2 \\ \sigma_2 \sigma_2(1) &= \sigma_2 \cdot_{S_n} \sigma_2(1) = \sigma_2 \circ \sigma_2(1) = \sigma_2(\sigma_2(1)) = \sigma_2(2) = 1 = \sigma_1(1) \\ \sigma_2 \sigma_2(2) &= \sigma_2 \cdot_{S_n} \sigma_2(2) = \sigma_2 \circ \sigma_2(2) = \sigma_2(\sigma_2(2)) = \sigma_2(1) = 2 = \sigma_1(2) \\ \sigma_2 \sigma_2 &= \sigma_1 \\ \sigma_1 \sigma_i &= \sigma_i \sigma_1 = \sigma_i \Rightarrow \sigma_1 = e = e_{S_2} = \bar{\sigma}_1 = \sigma_1^{-1} \\ \sigma_2 \sigma_2 &= \sigma_1 \Rightarrow \sigma_2 = \bar{\sigma}_2 = \sigma_2^{-1} \end{aligned}$$

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

$S_2 = \mathbb{Z}_2$

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

$|S_n| = n!$

$$|S_n| = P_n^n = n! = n \cdot (n-1) \cdot \dots \cdot 2 \cdot 1 = \overbrace{n(n-1) \cdots 1}^n = n(n-1) \cdots 1$$

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

two-line notation

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

定義 3.6. S_3

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

$$\begin{aligned}
&\sigma_6 \sigma_3 = \sigma_6 \circ \sigma_3 \\
&= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \\
&\quad \parallel \\
&= \begin{pmatrix} 3 & 1 & 2 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 3 & 1 & 2 \\ 1 & 3 & 2 \end{pmatrix} \\
&\quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \\
&= \begin{pmatrix} 3 & 1 & 2 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \sigma_5
\end{aligned}$$

$$\begin{array}{cccccc}
\cdot_{S_n} & [123] & [231] & [312] & [213] & [132] & [321] \\
[123] & [123] & [231] & [312] & [213] & [132] & [321] \\
[231] & [231] & & & & & \\
[312] & [312] & & & & & \\
[213] & [213] & & & & & \\
[132] & [132] & & & & & \\
[321] & [321] & & & & &
\end{array}
\leftrightarrow
\begin{array}{cc}
\circ & e \\
e & e \\
[231] & [231] \\
[312] & [312] \\
[213] & [213] \\
[132] & [132] \\
[321] & [321]
\end{array}$$

cycle notation= cyclic notation

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \nearrow & \nwarrow \\ 3 & 1 & 2 \end{pmatrix} = (1 \rightarrow 3 \rightarrow 2 \rightarrow 1) = (1321) = (132)$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ \downarrow \nearrow & \downarrow \nearrow & \downarrow \\ 2 & 3 & 1 \end{pmatrix} = (1 \rightarrow 2 \rightarrow 3 \rightarrow 1) = (1231) = (123)$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = (1 \rightarrow 1)(2 \rightarrow 2)(3 \rightarrow 3) = (11)(22)(33) = (1)(2)(3)$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1 \rightarrow 2 \rightarrow 3 \rightarrow 1) = (1231) = (123) = (231) = (312)$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1 \rightarrow 3 \rightarrow 2 \rightarrow 1) = (1321) = (132) = (321) = (213)$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (1 \rightarrow 2 \rightarrow 1)(3 \rightarrow 3) = (121)(33) = (12)(3) = (21)(3) = (3)(21) = (3)(12)$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (1 \rightarrow 1)(2 \rightarrow 3 \rightarrow 2) = (11)(232) = (1)(23) = (1)(32) = (32)(1) = (23)(1)$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1 \rightarrow 3 \rightarrow 1)(2 \rightarrow 2) = (131)(22) = (13)(2) = (31)(2) = (2)(31) = (2)(31)$$

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

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

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

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

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

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

Proof.

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

□

swap

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

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

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

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

定義 3.7. alternating group

$$A_n = \left\{ \sigma \mid \begin{array}{l} \sigma \in S_n \\ N_\sigma \in 2\mathbb{Z}_{\geq 0} \end{array} \right\}$$

3.3 dihedral group

D_3

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

$$\begin{aligned}
 (1) & = (1) (2) (3) : \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} \quad \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) & : \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} \quad \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) & : \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} \quad \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) & : \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} \quad \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) & : \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} \quad \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) & : \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} \quad \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}
 \end{aligned}$$

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

$$\cos \alpha \cos \beta = \frac{+\cos(\alpha + \beta) + \cos(\alpha - \beta)}{2}$$

$$\sin \alpha \sin \beta = \frac{-\cos(\alpha + \beta) + \cos(\alpha - \beta)}{2}$$

$$\sin \alpha \cos \beta = \frac{+\sin(\alpha + \beta) + \sin(\alpha - \beta)}{2}$$

$$\cos \alpha \sin \beta = \frac{+\sin(\alpha + \beta) - \sin(\alpha - \beta)}{2}$$

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

$$\rho_{k+3} = \rho_k$$

$$\pi_{k+3} = \pi_k$$

$$\rho_i \rho_j = \rho_{i+j}$$

$$\rho_i \pi_j = \pi_{i+j}$$

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

$$\pi_i \pi_j = \rho_{i-j}$$

$$D_3 = S_3$$

$$\rho_0 \leftrightarrow [123]$$

$$\rho_1 \leftrightarrow [231]$$

$$\rho_2 \leftrightarrow [312]$$

$$\pi_0 \leftrightarrow [213]$$

$$\pi_1 \leftrightarrow [132]$$

$$\pi_2 \leftrightarrow [321]$$

$$\begin{array}{c}
\begin{array}{c} \cdot_{D_3} \\ \rho_0 \\ \rho_1 \\ \rho_2 \\ \pi_0 \\ \pi_1 \\ \pi_2 \end{array} \quad \begin{array}{ccccccc} \rho_0 & \rho_1 & \rho_2 & \pi_0 & \pi_1 & \pi_2 \\ \rho_{0+0} & \rho_{0+1} & \rho_{0+2} & \pi_{0+0} & \pi_{0+1} & \pi_{0+2} \\ \rho_{1+0} & \rho_{1+1} & \rho_{1+2} & \pi_{1+0} & \pi_{1+1} & \pi_{1+2} \\ \rho_{2+0} & \rho_{2+1} & \rho_{2+2} & \pi_{2+0} & \pi_{2+1} & \pi_{2+2} \\ \pi_{0-0} & \pi_{0-1} & \pi_{0-2} & \rho_{0-0} & \rho_{0-1} & \rho_{0-2} \\ \pi_{1-0} & \pi_{1-1} & \pi_{1-2} & \rho_{1-0} & \rho_{1-1} & \rho_{1-2} \\ \pi_{2-0} & \pi_{2-1} & \pi_{2-2} & \rho_{2-0} & \rho_{2-1} & \rho_{2-2} \end{array} \\
\begin{array}{c} \cdot_{S_3} \\ [123] \\ [231] \\ [312] \\ [213] \\ [132] \\ [321] \end{array} \quad \begin{array}{ccccccc} [123] & [231] & [312] & [213] & [132] & [321] \\ [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] \end{array} \\
\begin{array}{c} +_{\mathbb{Z}_3} \\ 0_\rho \\ 1_\rho \\ 2_\rho \\ 0_\pi \\ 1_\pi \\ 2_\pi \end{array} \quad \begin{array}{ccccccc} 0_\rho & 1_\rho & 2_\rho & 0_\pi & 1_\pi & 2_\pi \\ 0_\rho & 0_\rho & 1_\rho & 2_\rho & 0_\pi & 1_\pi & 2_\pi \\ 1_\rho & 1_\rho & 2_\rho & 0_\rho & 1_\pi & 2_\pi & 0_\pi \\ 2_\rho & 2_\rho & 0_\rho & 1_\rho & 2_\pi & 0_\pi & 1_\pi \\ 0_\pi & 0_\pi & 2_\pi & 1_\pi & 0_\rho & 2_\rho & 1_\rho \\ 1_\pi & 1_\pi & 0_\pi & 2_\pi & 1_\rho & 0_\rho & 2_\rho \\ 2_\pi & 2_\pi & 1_\pi & 0_\pi & 2_\rho & 1_\rho & 0_\rho \end{array}
\end{array} \rightarrow \begin{array}{c}
\begin{array}{c} \cdot_{D_3} \\ \rho_0 \\ \rho_1 \\ \rho_2 \\ \pi_0 \\ \pi_1 \\ \pi_2 \end{array} \quad \begin{array}{ccccccc} \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_3 & \pi_1 & \pi_2 & \pi_3 \\ \rho_2 & \rho_2 & \rho_3 & \rho_4 & \pi_2 & \pi_3 & \pi_4 \\ \pi_0 & \pi_0 & \pi_{-1} & \pi_{-2} & \rho_0 & \rho_{-1} & \rho_{-2} \\ \pi_1 & \pi_1 & \pi_0 & \pi_{-1} & \rho_1 & \rho_0 & \rho_{-1} \\ \pi_2 & \pi_2 & \pi_1 & \pi_0 & \rho_2 & \rho_1 & \rho_0 \end{array} \\
\rho_{k+3} = \rho_k \downarrow \pi_{k+3} = \pi_k \\
\begin{array}{c} \cdot_{D_3} \\ \rho_0 \\ \rho_1 \\ \rho_2 \\ \pi_0 \\ \pi_1 \\ \pi_2 \end{array} \quad \begin{array}{ccccccc} \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} \\
\downarrow \\
\begin{array}{c} +_{\mathbb{Z}_3} \\ 0 \\ 1 \\ 2 \\ \pi_0 \\ \pi_1 \\ \pi_2 \end{array} \quad \begin{array}{ccccccc} 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 & \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}
\end{array}$$

$S_3 \xleftarrow{= D_3}$

\leftarrow

$$\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}\} \\
D_n &= \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}{l} \forall n \in \mathbb{N} \\ k \in \{0, \dots, n-1\} \end{array} \\
D_n &= \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}{l} \forall n \in \mathbb{N} \\ k \in \{0, \dots, 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\} \\
D_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\} \\
D_1 &= \left\{ \begin{bmatrix} \cos 0 & -\sin 0 \\ \sin 0 & \cos 0 \end{bmatrix}, \begin{bmatrix} \cos \pi & -\sin \pi \\ \sin \pi & \cos \pi \end{bmatrix}, \right. & = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \right. \\
& \quad \left. \begin{bmatrix} \cos 0 & \sin 0 \\ \sin 0 & -\cos 0 \end{bmatrix}, \begin{bmatrix} \cos \pi & \sin \pi \\ \sin \pi & -\cos \pi \end{bmatrix} \right\} & \left. \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \right\} \\
D_1 &= \{\rho_0, \rho_1, \pi_0, \pi_1\} & = \{\rho_0, \rho_1, \pi_0, \pi_1\} \\
D_1 &= \left\{ \begin{bmatrix} \cos 0 & -\sin 0 \\ \sin 0 & \cos 0 \end{bmatrix}, \begin{bmatrix} \cos 0 & \sin 0 \\ \sin 0 & -\cos 0 \end{bmatrix} \right\} & = \{\rho_{0,2}, \rho_{1,2}, \pi_{0,2}, \pi_{1,2}\} \\
& & = \{\rho_0, \pi_0\} \\
& & = \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

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

trivial subgroups

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

$$G = G \leq G$$

$$C_3 = \begin{array}{l} \mathbb{Z}_3 \leq D_3 = S_3 \\ \mathbb{Z}_2 \leq S_3 = D_3 \end{array} \quad \mathbb{Z}_2 \leq S_n \quad \forall n \in \mathbb{N}_{\geq 2}$$

$$\begin{array}{c}
\begin{array}{c} \cdot_{D_3} \\ \rho_0 \\ \rho_1 \\ \rho_2 \\ \pi_0 \\ \pi_1 \\ \pi_2 \end{array} \begin{array}{cccccc} \rho_0 & \rho_1 & \rho_2 & \pi_0 & \pi_1 & \pi_2 \end{array} \\
\begin{array}{cccccc} \rho_0 & \rho_{0+0} & \rho_{0+1} & \rho_{0+2} & \pi_{0+0} & \pi_{0+1} & \pi_{0+2} \\ \rho_1 & \rho_{1+0} & \rho_{1+1} & \rho_{1+2} & \pi_{1+0} & \pi_{1+1} & \pi_{1+2} \\ \rho_2 & \rho_{2+0} & \rho_{2+1} & \rho_{2+2} & \pi_{2+0} & \pi_{2+1} & \pi_{2+2} \\ \pi_0 & \pi_{0-0} & \pi_{0-1} & \pi_{0-2} & \rho_{0-0} & \rho_{0-1} & \rho_{0-2} \\ \pi_1 & \pi_{1-0} & \pi_{1-1} & \pi_{1-2} & \rho_{1-0} & \rho_{1-1} & \rho_{1-2} \\ \pi_2 & \pi_{2-0} & \pi_{2-1} & \pi_{2-2} & \rho_{2-0} & \rho_{2-1} & \rho_{2-2} \end{array} \\
\end{array} \rightarrow \begin{array}{c}
\begin{array}{c} \cdot_{D_3} \\ \rho_0 \\ \rho_1 \\ \rho_2 \\ \pi_0 \\ \pi_1 \\ \pi_2 \end{array} \begin{array}{cccccc} \rho_0 & \rho_1 & \rho_2 & \pi_0 & \pi_1 & \pi_2 \end{array} \\
\begin{array}{cccccc} \rho_0 & \rho_0 & \rho_1 & \rho_2 & \pi_0 & \pi_1 & \pi_2 \\ \rho_1 & \rho_1 & \rho_2 & \rho_3 & \pi_1 & \pi_2 & \pi_3 \\ \rho_2 & \rho_2 & \rho_3 & \rho_4 & \pi_2 & \pi_3 & \pi_4 \\ \pi_0 & \pi_0 & \pi_{-1} & \pi_{-2} & \rho_0 & \rho_{-1} & \rho_{-2} \\ \pi_1 & \pi_1 & \pi_0 & \pi_{-1} & \rho_1 & \rho_0 & \rho_{-1} \\ \pi_2 & \pi_2 & \pi_1 & \pi_0 & \rho_2 & \rho_1 & \rho_0 \end{array} \\
\rho_{k+3} = \rho_k \downarrow \pi_{k+3} = \pi_k \\
\begin{array}{c} \cdot_{D_3} \\ \rho_0 \\ \rho_1 \\ \rho_2 \\ \pi_0 \\ \pi_1 \\ \pi_2 \end{array} \begin{array}{cccccc} \rho_0 & \rho_1 & \rho_2 & \pi_0 & \pi_1 & \pi_2 \end{array} \\
\begin{array}{cccccc} \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} \\
\downarrow \\
\begin{array}{c} +_{\mathbb{Z}_3} \\ 0 \\ 1 \\ 2 \end{array} \begin{array}{cccccc} 0_\rho & 1_\rho & 2_\rho & 0_\pi & 1_\pi & 2_\pi \\ 0_\rho & 0_\rho & 1_\rho & 2_\rho & 0_\pi & 1_\pi & 2_\pi \\ 1_\rho & 1_\rho & 2_\rho & 0_\rho & 1_\pi & 2_\pi & 0_\pi \\ 2_\rho & 2_\rho & 0_\rho & 1_\rho & 2_\pi & 0_\pi & 1_\pi \\ 0_\pi & 0_\pi & 2_\pi & 1_\pi & 0_\rho & 2_\rho & 1_\rho \\ 1_\pi & 1_\pi & 0_\pi & 2_\pi & 1_\rho & 0_\rho & 2_\rho \\ 2_\pi & 2_\pi & 1_\pi & 0_\pi & 2_\rho & 1_\rho & 0_\rho \end{array} \\
\downarrow \\
\mathbb{Z}_3 = \{0, 1, 2\} \\
= \{0_\rho, 1_\rho, 2_\rho\} = \{[123], [231], [312]\} = \{(), (123), (132)\} \\
= \left\{e^{i\frac{2\pi}{3}0}, e^{i\frac{2\pi}{3}1}, e^{i\frac{2\pi}{3}2}, \dots, e^{i\frac{2\pi}{3}(n-1)}\right\} \stackrel{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, \dots, g^{n-1}\} = \{g^0, g^1, g^2\} = \{e, g, g^2\}, g^n = e
\end{array}$$

$$\begin{array}{c}
\begin{array}{c} \cdot_{S_3} \\ () \\ (123) \\ (132) \\ (12) \\ (23) \\ (31) \end{array} \begin{array}{cccccc} () & (123) & (132) & (12) & (23) & (31) \end{array} \\
\begin{array}{cccccc} () & () & (123) & (132) & (12) & (23) & (31) \\ (123) & (123) & (132) & () & (23) & (31) & (12) \\ (132) & (132) & () & (123) & (31) & (12) & (23) \\ (12) & (12) & (31) & (23) & () & (132) & (123) \\ (23) & (23) & (12) & (31) & (123) & () & (132) \\ (31) & (31) & (23) & (12) & (132) & (123) & () \end{array} \\
\downarrow \\
\mathbb{Z}_2 \leq S_3 = D_3 \\
\downarrow \\
\mathbb{Z}_2 \leq S_n \quad \forall n \in \mathbb{N}_{\geq 2}
\end{array}$$

$$\begin{array}{c}
\begin{array}{c} +_{\mathbb{Z}_2} \\ 0 \\ (123) \\ (132) \\ 1 \\ (23) \\ (31) \end{array} \begin{array}{cccccc} 0 & (123) & (132) & 1 & (23) & (31) \\ 0 & (123) & (132) & 1 & (23) & (31) \\ (123) & (123) & (132) & () & (23) & (31) & (12) \\ (132) & (132) & () & (123) & (31) & (12) & (23) \\ 1 & 1 & (31) & (23) & 0 & (132) & (123) \\ (23) & (23) & (12) & (31) & (123) & () & (132) \\ (31) & (31) & (23) & (12) & (132) & (123) & () \end{array} \\
\rightarrow \\
\begin{array}{c} +_{\mathbb{Z}_2} \\ 0 \\ (123) \\ (132) \\ 1 \\ (23) \\ (31) \end{array} \begin{array}{cccccc} 0 & (123) & (132) & (12) & 1 & (31) \\ 0 & (123) & (132) & (12) & 1 & (31) \\ (123) & (123) & (132) & () & (23) & (31) & (12) \\ (132) & (132) & () & (123) & (31) & (12) & (23) \\ (12) & (12) & (31) & (23) & () & (132) & (123) \\ 1 & 1 & (12) & (31) & (123) & 0 & (132) \\ (31) & (31) & (23) & (12) & (132) & (123) & () \end{array} \\
\leftarrow \\
\begin{array}{c} +_{\mathbb{Z}_2} \\ 0 \\ (123) \\ (132) \\ 1 \\ (23) \\ (31) \end{array} \begin{array}{cccccc} 0 & (123) & (132) & (12) & 1 & (31) \\ 0 & (123) & (132) & (12) & 1 & (31) \\ (123) & (123) & (132) & () & (23) & (31) & (12) \\ (132) & (132) & () & (123) & (31) & (12) & (23) \\ (12) & (12) & (31) & (23) & () & (132) & (123) \\ 1 & 1 & (12) & (31) & (123) & 0 & (132) \\ (31) & (31) & (23) & (12) & (132) & (123) & () \end{array} \\
\leftarrow \\
\begin{array}{c} +_{\mathbb{Z}_2} \\ 0 \\ (123) \\ (132) \\ 1 \\ (23) \\ (31) \end{array} \begin{array}{cccccc} 0 & (123) & (132) & (12) & 1 & (31) \\ 0 & (123) & (132) & (12) & 1 & (31) \\ (123) & (123) & (132) & () & (23) & (31) & (12) \\ (132) & (132) & () & (123) & (31) & (12) & (23) \\ (12) & (12) & (31) & (23) & () & (132) & (123) \\ 1 & 1 & (12) & (31) & (123) & 0 & (132) \\ (31) & (31) & (23) & (12) & (132) & (123) & () \end{array}
\end{array}$$

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

$$\begin{aligned}
\mathbb{Z}_2 = (\mathbb{Z}_2, +) &= (\mathbb{Z}_2, +_{\mathbb{Z}_2}) = \{0, 2-1\} = \{0, 1\} \\
= \mathbb{Z}_2 = (\mathbb{Z}_2, \cdot) &= (\mathbb{Z}_2, \cdot_{\mathbb{C}}) = \left\{e^{i\frac{2\pi}{2}0}, e^{i\frac{2\pi}{2}(2-1)}\right\} = \{e^{i0}, e^{i\pi}\} = \{1, -1\} \\
= S_2 = \mathbb{Z}_2 = (S_2, \cdot_{S_2}) &= (S_2, \circ) = \{\sigma_1, \sigma_2\} = \{e_{S_2}, \sigma_2\} = \{e, \sigma_2\} \\
= C_{2,1} &= (\mathbb{Z}_2, \cdot_{S_3}) = \{[123], [213]\} = \{(), (12)\} \\
= C_{2,2} &= (\mathbb{Z}_2, \cdot_{S_3}) = \{[123], [132]\} = \{(), (23)\} \\
= C_{2,3} &= (\mathbb{Z}_2, \cdot_{S_3}) = \{[123], [321]\} = \{(), (31)\} \\
E_3 &= (\mathbb{Z}_1, \cdot_{S_3}) = \{e\} = \{[123]\} = \{()\} \quad e = e_{S_3}
\end{aligned}$$

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

$$\mathbb{Z}_4 = \{e, a, a^2, a^3 \mid a^4 = e\}$$

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

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

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

$$\mathbb{Z}_{2n} = \{e, a, \dots, a^n, \dots, a^{2n-1} \mid a^{2n} = e\} \quad \forall n \in \mathbb{N}$$

$$\begin{array}{cccccc}
\cdot_{\mathbb{Z}_{2n}} & e & a & \dots & a^n & \dots & a^{2n-1} \\
e & e & a & \dots & a^n & \dots & a^{2n-1} \\
a & a & a^2 & \dots & a^{n+1} & \dots & a^{2n} \\
\vdots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\
a^n & a^n & a^{n+1} & \dots & a^{2n} & \dots & a^{3n-1} \\
\vdots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\
a^{2n-1} & a^{2n-1} & a^{2n} & \dots & a^{3n-1} & \dots & a^{4n-2}
\end{array}
\rightarrow
\begin{array}{cccccc}
\cdot_{\mathbb{Z}_{2n}} & e & a & \dots & a^n & \dots & a^{2n-1} \\
e & e & a & \dots & a^n & \dots & a^{2n-1} \\
a & a & a^2 & \dots & a^{n+1} & \dots & a^{2n} \\
\vdots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\
a^n & a^n & a^{n+1} & \dots & a^{2n} & \dots & a^{2n+(n-1)} \\
\vdots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\
a^{2n-1} & a^{2n-1} & a^{2n} & \dots & a^{2n+(n-1)} & \dots & a^{2(n-1)}
\end{array}
\downarrow$$

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

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

$$\mathbb{Z}_2 \not\leq \mathbb{Z}_{2n+1}$$

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

$$\mathbb{Z}_{2n+1} = \left\{ e, a, \dots, a^k, \dots, a^{2n} \mid \begin{array}{l} a^{2n+1} = e \quad (id) \\ k \in \mathbb{N}_{\leq 2n} \quad (xp) \end{array} \right\} \quad \forall n \in \mathbb{N}$$

$$\begin{aligned}
(xp) &\Rightarrow \{e, a^k \mid k \in \mathbb{N}_{\leq 2n}\} & \text{even } 2\mathbb{N} \ni 2k \neq 2n+1 \in 2\mathbb{N}+1 \text{ odd} \\
&\in \{\{e, a^k \mid 1 \leq k \leq 2n\}\} & \Rightarrow 2 \leq 2k \leq 2 \cdot 2n < 2(2n+1) \\
& & \downarrow \\
& & 2k \neq 2(2n+1) \Rightarrow 2n+1 \nmid 2k \\
& & \downarrow \\
& & a^{2k} = (a^k)^2 \neq (a^{2n+1})^m \stackrel{(id)}{=} (e)^m = e \quad m \in \mathbb{Z}_{\geq 0} \\
& & \Rightarrow \mathbb{Z}_2 \not\leq \mathbb{Z}_{2n+1}
\end{aligned}$$

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

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

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

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

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

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

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

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

$$D_n \leq S_n$$

$$D_n = \left\{ \begin{array}{c} \left| \begin{array}{l} \rho_{k,n} = \left[\begin{array}{cc} +\cos \frac{2\pi}{n}k & -\sin \frac{2\pi}{n}k \\ +\sin \frac{2\pi}{n}k & +\cos \frac{2\pi}{n}k \end{array} \right] \\ \pi_{k,n} = \left[\begin{array}{cc} +\cos \frac{2\pi}{n}k & +\sin \frac{2\pi}{n}k \\ +\sin \frac{2\pi}{n}k & -\cos \frac{2\pi}{n}k \end{array} \right] \end{array} \right\} \quad \begin{array}{l} \forall n \in \mathbb{N} \\ k \in \{0, \dots, n-1\} = \mathbb{Z}_{[0,n)} \end{array}$$

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

$$A_n \leq S_n$$

$$\begin{aligned}
A_n &= \left\{ \sigma \mid \begin{array}{l} \sigma \in S_n \\ N_\sigma \in 2\mathbb{Z}_{\geq 0} \end{array} \right\} \subseteq S_n \\
\sigma \tilde{\sigma} &= \underbrace{(s_{11}s_{12})}_{s_1} \cdots \underbrace{(s_{N_\sigma 1} s_{N_\sigma 2})}_{s_{N_\sigma}} \underbrace{(\tilde{s}_{11} \tilde{s}_{12})}_{\tilde{s}_1} \cdots \underbrace{(\tilde{s}_{\tilde{N}_\sigma 1} \tilde{s}_{\tilde{N}_\sigma 2})}_{\tilde{s}_{N_\sigma}} & \begin{array}{l} \forall \sigma \in A_n \Rightarrow N_\sigma \in 2\mathbb{Z}_{\geq 0} \\ \forall \tilde{\sigma} \in A_n \Rightarrow \tilde{N}_\sigma \in 2\mathbb{Z}_{\geq 0} \end{array} \\
&= \underbrace{(s_{11}s_{12})}_{s_1} \cdots \underbrace{(s_{N_\sigma 1} s_{N_\sigma 2})}_{s_{N_\sigma}} \underbrace{(\tilde{s}_{11} \tilde{s}_{12})}_{\tilde{s}_1} \cdots \underbrace{(\tilde{s}_{\tilde{N}_\sigma 1} \tilde{s}_{\tilde{N}_\sigma 2})}_{\tilde{s}_{N_\sigma}} & N_\sigma + \tilde{N}_\sigma \in 2\mathbb{Z}_{\geq 0} \\
&\in A_n \\
\sigma^{-1} = \bar{\sigma} &= \underbrace{(s_{11}s_{12})}_{s_1} \cdots \underbrace{(s_{N_\sigma 1} s_{N_\sigma 2})}_{s_{N_\sigma}} = \underbrace{(s_{N_\sigma 2} s_{N_\sigma 1})}_{\bar{s}_{N_\sigma}} \cdots \underbrace{(s_{12} s_{11})}_{\bar{s}_1} & \forall \sigma \in A_n \Rightarrow N_\sigma \in 2\mathbb{Z}_{\geq 0} \\
&\in A_n \\
&\Downarrow \\
A_n &\leq S_n
\end{aligned}$$

定理 4.2. *finite cyclic subgroup*

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

Proof. $g = e = e_G$,

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

$$g \neq e = e_G,$$

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

\Downarrow pigeonhole principle = Dirichlet drawer principle

$$\Leftarrow |\mathbb{N}| \not\leq \infty \wedge \begin{matrix} |G| < \infty \\ |\langle g \rangle| < \infty \end{matrix}$$

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

$$n_1, n_2 \in \mathbb{N}$$

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

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

$$\begin{aligned} g^{n_2} \overline{g^{n_1}} &= g^{n_1} \overline{g^{n_1}} = g^{n_1} g^{-n_1} = g^{n_1 - n_1} = g^0 = e = e_G & \forall G \text{ is a group, } \forall g^{n_2} \in G, \exists \overline{g^{n_2}} \in G \\ &= g^{n_2} g^{-n_1} = g^{n_2 - n_1} = g^{|n_2 - n_1|} & n_1 < n_2 \Rightarrow 0 < n_2 - n_1 = |n_2 - n_1| \\ g^{|n_2 - n_1|} &= e \end{aligned}$$

\downarrow

$$\text{ord } \langle g \rangle \stackrel{\text{def.}}{=} \min \{|n_2 - n_1|\} \in \mathbb{N} \quad \min \{|n_2 - n_1|\} \text{ is the order of } \langle g \rangle$$

$$\langle g \rangle = \{g^1, g^2, \dots, g^{\text{ord } \langle g \rangle}, \dots\} = \{g, g^2, \dots, e, \dots\} \quad g^{\text{ord } \langle g \rangle} = e$$

$$\langle g \rangle = \{g^1, g^2, \dots, g^{\text{ord } \langle g \rangle - 1}, g^{\text{ord } \langle g \rangle}, g^{\text{ord } \langle g \rangle + 1}, \dots\} = \{g, g^2, \dots, \bar{g}, e, g, \dots\}$$

$$= \{g^1, g^2, \dots, g^{\text{ord } \langle g \rangle - 1}, g^{\text{ord } \langle g \rangle}\} = \{g, g^2, \dots, \bar{g}, e\}$$

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

$$\langle g \rangle \subseteq G$$

$$g^{n_1} g^{n_2} = g^{n_1 + n_2} \in \langle g \rangle$$

$$\forall n_1, n_2 \in \mathbb{N} [n_1 + n_2 \in \mathbb{N}]$$

$$\exists \bar{g}^k = g^{\text{ord } \langle g \rangle - k} \left[\bar{g}^k g^k = g^{\text{ord } \langle g \rangle - k} g^k = g^{\text{ord } \langle g \rangle} = e \right] \quad \forall k \in \{1, \dots, \text{ord } \langle g \rangle\} = \mathbb{N}_{\leq \text{ord } \langle g \rangle}$$

\Downarrow

$$\langle g \rangle \leq G$$

□

定義 4.3. order of a group element

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

$$\langle g \rangle = \{g^1, g^2, \dots, g^{\text{ord } \langle g \rangle - 1}, g^{\text{ord } \langle g \rangle}, g^{\text{ord } \langle g \rangle + 1}, \dots\} = \{g, g^2, \dots, \bar{g}, e, g, \dots\}$$

$$= \{g^1, g^2, \dots, g^{\text{ord } \langle g \rangle - 1}, g^{\text{ord } \langle g \rangle}\} = \{g, g^2, \dots, \bar{g}, e\}$$

$$= \{g, g^2, \dots, e\} = \{g, g^2, \dots, g^{\min \{m\}}\} = \{g, g^2, \dots, g^{\text{ord } g}\}$$

$$|\langle g \rangle| = |\{g, g^2, \dots, g^{\text{ord } g}\}| = |\{g, g^2, \dots, g^{\text{ord } \langle g \rangle}\}|$$

$$= \text{ord } g = \text{ord } \langle g \rangle$$

$$\text{ord } \langle g \rangle = \text{ord } g = |\langle g \rangle| \in \mathbb{N}$$

$$\langle g \rangle \neq \emptyset = \{\}$$

$$|\langle g \rangle| \in \mathbb{N} \neq \mathbb{Z}_{\geq 0}$$

\mathbb{Z}_4

$$\mathbb{Z}_4 = \{0, 1, 2, 3\}$$

$$= \mathbb{Z}_{[0,4)} = (\mathbb{Z}_4, +_{\mathbb{Z}_n})$$

$$= \{e, g, g^2, g^3\}$$

$$= (\mathbb{Z}_4, \cdot) = (\mathbb{Z}_4, \cdot_G)$$

$$= \{g, g^2, g^3, e\}$$

$$= \{g^1, g^2, g^3, g^4\} = \langle g \rangle$$

$$g^4 = e$$

$$= \{a^1, a^2, a^3, a^4\}$$

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

$$a^4 = e$$

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

ord

$$\begin{array}{l}
g = e \quad g^1 = e^1 = e \quad \text{ord}g = \text{orde} = 1 \\
\prec \\
\begin{array}{l}
g \neq e \quad g^1 = g \neq e \quad g^2 \neq e \quad g^3 \neq e \quad g^4 = e \quad \text{ord}g = 4 \\
g^2 \neq e \quad (g^2)^1 = g^2 \neq e \quad (g^2)^2 = g^4 = e \quad \text{ord}g^2 = 2 \\
\quad \quad \quad (g^3)^2 = g^6 \quad (g^3)^3 = g^9 \\
g^3 \neq e \quad (g^3)^1 = g^3 \neq e \quad = g^4 g^2 \quad = (g^4)^2 g \quad (g^3)^4 = (g^4)^3 \quad \text{ord}g^3 = 4 \\
\quad \quad \quad = eg^2 \quad = e^2 g \quad = e^3 = e \\
\quad \quad \quad = g^2 \neq e \quad = eg \\
\quad \quad \quad \quad \quad = g \neq e
\end{array} \\
\prec \\
g^4 = e \quad (g^4)^1 = e^1 = e \quad \text{ord}g^4 = \text{orde} = 1
\end{array}$$

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

定理 4.4. subgroup intersection

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

定義 4.5. central subgroup

$$C(G) = \left\{ c \left| \begin{array}{l} c \in G \\ cg = gc \quad \forall g \in G \end{array} \right. \right\}$$

$$C(G) \leq G$$

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

$$c_1 c_2 g \stackrel{c_2 \in C(G)}{=} c_1 g c_2 \stackrel{c_1 \in C(G)}{=} g c_1 c_2 \quad \forall g \in G, \forall c_1, c_2 \in C(G)$$

$$c_1 c_2 g = g c_1 c_2$$

$$(c_1 c_2) g = g (c_1 c_2) \Rightarrow c_1 c_2 \in C(G)$$

$$\Downarrow$$

$$c_1 c_2 \in C(G)$$

$$\forall c_1, c_2 \in C(G)$$

$$\bar{c}c = e = e_G$$

$$\forall g \in G, \forall c \in C(G), \exists \bar{c} = c^{-1} \in G$$

$$\bar{c}g\bar{g}c = (\bar{c}g)(\bar{g}c) = \bar{c}(g\bar{g})c = \bar{c}ec = \bar{c}c = e \Rightarrow (g^{-1}c)^{-1} = \bar{g}\bar{c} = \overline{(\bar{g}c)} = \bar{c}g = c^{-1}g \quad (1)$$

$$g\bar{c}c\bar{g} = (g\bar{c})(c\bar{g}) = g(\bar{c}c)\bar{g} = ge\bar{g} = g\bar{g} = e \Rightarrow (cg^{-1})^{-1} = \overline{c\bar{g}} = \overline{(c\bar{g})} = g\bar{c} = gc^{-1} \quad (2)$$

$$\bar{c}g \stackrel{(1)}{=} \overline{g\bar{c}} \stackrel{\bar{g}c = c\bar{g}}{=} \overline{c\bar{g}} \stackrel{(2)}{=} g\bar{c}$$

$$\because c \in C(G), \bar{g} \in G \therefore \bar{g}c = c\bar{g}$$

$$\bar{c}g = g\bar{c}$$

$$\Rightarrow \bar{c} \in C(G)$$

$$\Downarrow$$

$$\bar{c} \in C(G)$$

$$\forall c \in C(G)$$

$$C(G) = \left\{ c \left| \begin{array}{l} c \in G \\ cg = gc \quad \forall g \in G \end{array} \right. \right\} \subseteq G \quad C(G) \leq G$$

$$c_1 c_2 \in C(G)$$

$$\forall c_1, c_2 \in C(G)$$

$$\bar{c} \in C(G)$$

$$\forall c \in C(G)$$

$$\Downarrow$$

$$C(G) \leq G$$

5 coset

定義 5.1. left coset

$$H \leq G$$

G is a group

$$\Downarrow$$

$$gH \stackrel{\text{def.}}{=} \{gh | h \in H\}$$

$$\forall g \in G$$

$$\Updownarrow$$

gH is a left coset of G

G is a group

$$gH = \{gh | h \in H \leq G\} \quad \forall g \in G$$

定義 5.2. right coset

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

G is a group

$$Hg = \{hg | h \in H \leq G\} \quad \forall g \in G$$

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

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

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

$$\begin{array}{ccc} \begin{array}{c} \cdot_{D_3} \\ \rho_0 \\ \rho_1 \\ \rho_2 \\ \pi_0 \\ \pi_1 \\ \pi_2 \end{array} & \begin{array}{ccccccc} \rho_0 & \rho_1 & \rho_2 & \pi_0 & \pi_1 & \pi_2 \\ \rho_0 & \rho_0 & \rho_1 & \rho_2 & \pi_0 & \pi_1 & \pi_2 \\ \rho_1 & \rho_1 & \rho_2 & \rho_0 & \pi_1 & \pi_2 & \pi_0 \\ \rho_2 & \rho_2 & \rho_0 & \rho_1 & \pi_2 & \pi_0 & \pi_1 \\ \pi_0 & \pi_0 & \pi_2 & \pi_1 & \rho_0 & \rho_2 & \rho_1 \\ \pi_1 & \pi_1 & \pi_0 & \pi_2 & \rho_1 & \rho_0 & \rho_2 \\ \pi_2 & \pi_2 & \pi_1 & \pi_0 & \rho_2 & \rho_1 & \rho_0 \end{array} & \xrightarrow{e=\rho_0} \\ \begin{array}{c} +_{\mathbb{Z}_3} \\ 0 \\ 1 \\ 2 \\ \pi_0 \\ \pi_1 \\ \pi_2 \end{array} & \begin{array}{ccccccc} 0 & 1 & 2 & \pi_0 & \pi_1 & \pi_2 \\ 0 & 0 & 1 & 2 & \pi_0 & \pi_1 & \pi_2 \\ 1 & 1 & 2 & 0 & \pi_1 & \pi_2 & \pi_0 \\ 2 & 2 & 0 & 1 & \pi_2 & \pi_0 & \pi_1 \\ \pi_0 & \pi_0 & \pi_2 & \pi_1 & e & \rho^2 & \rho \\ \pi_1 & \pi_1 & \pi_0 & \pi_2 & \rho & e & \rho^2 \\ \pi_2 & \pi_2 & \pi_1 & \pi_0 & \rho^2 & \rho & e \end{array} & \xleftarrow{\mathbb{Z}_3 \leq D_3} \\ \begin{array}{c} \cdot_{D_3} \\ e \\ \rho \\ \rho^2 \end{array} & \begin{array}{ccccccc} e & \rho_1 & \rho_2 & \pi_0 & \pi_1 & \pi_2 \\ e & e & \rho_1 & \rho_2 & \pi_0 & \pi_1 & \pi_2 \\ \rho_1 & \rho_1 & \rho_2 & e & \pi_1 & \pi_2 & \pi_0 \\ \rho_2 & \rho_2 & e & \rho_1 & \pi_2 & \pi_0 & \pi_1 \\ \pi_0 & \pi_0 & \pi_2 & \pi_1 & e & \rho_2 & \rho_1 \\ \pi_1 & \pi_1 & \pi_0 & \pi_2 & \rho_1 & e & \rho_2 \\ \pi_2 & \pi_2 & \pi_1 & \pi_0 & \rho_2 & \rho_1 & e \end{array} & \end{array}$$

$$\begin{aligned}
D_3 &= \left\{ \left. \begin{array}{l} \rho_{k,n} \\ \pi_{k,n} \end{array} \right| \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\} \quad \forall k \in \mathbb{Z}_{[0,3)} \quad n=3 \\
&= \{\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, \rho, \rho^2, \pi_0, \pi_1, \pi_2\} \supset \{e, \rho, \rho^2\} = \mathbb{Z}_3 &e \neq \rho = \rho^1 = \rho_1 \\
&\mathbb{Z}_3 \leq D_3 \Rightarrow \mathbb{Z}_3 = \{0, 1, 2\} &\rho^2 = (\rho_1)^2 = \rho_2 \\
&= \{e, g, g^2\} &= \mathbb{Z}_{[0,3)} = (\mathbb{Z}_3, +_{\mathbb{Z}_n}) \\
&= \{g, g^2, e\} &= (\mathbb{Z}_4, \cdot) = (\mathbb{Z}_4, \cdot_G) \\
&= \{g^1, g^2, g^3\} = \langle g \rangle &g^3 = e \\
&= \{a^1, a^2, a^3\} &a^3 = e \\
&= \{a^1, a^2, 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_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\rho_j = \pi_{i-j} \\
&\pi_i = \pi_{3+i} \\
&= \pi_0\mathbb{Z}_3 \\
&= \{\pi_0, \pi_{-1}, \pi_{-2}\} = \{\pi_0, \pi_2, \pi_1\} = \{\pi_0, \pi_1, \pi_2\} \\
\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_0\mathbb{Z}_3 \\
&= \{\pi_1, \pi_0, \pi_{-1}\} = \{\pi_1, \pi_0, \pi_2\} = \{\pi_0, \pi_1, \pi_2\} \\
\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_0\mathbb{Z}_3 \\
&= \{\pi_2, \pi_1, \pi_0\} = \{\pi_0, \pi_1, \pi_2\} \\
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)}
\end{aligned}$$

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

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

$$4\mathbb{Z} = \{\dots, -12, -8, -4, 0, +4, +8, +12, \dots\} = \{4k | k \in \mathbb{Z}\}$$

$$4\mathbb{Z} \subset \mathbb{Z}$$

$$4k_1 + 4k_2 = 4(k_1 + k_2) \in 4\mathbb{Z}$$

$$-4k = \overline{4k} = 4(-k) \in 4\mathbb{Z}$$

$$\Downarrow$$

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

$$\begin{aligned} 5 + 4\mathbb{Z} &= \{\dots, 5 + (-12), 5 + (-8), 5 + (-4), 5 + 0, 5 + 4, 5 + 8, 5 + 12, \dots\} \\ &= \{\dots, -7, -3, 1, 5, 9, 13, 17, \dots\} \end{aligned} \quad = 1 + 4\mathbb{Z}$$

$$\begin{aligned} 4 + 4\mathbb{Z} &= \{\dots, 4 + (-12), 4 + (-8), 4 + (-4), 4 + 0, 4 + 4, 4 + 8, 4 + 12, \dots\} \\ &= \{\dots, -8, -4, 0, 4, 8, 12, 16, \dots\} \end{aligned} \quad = 0 + 4\mathbb{Z}$$

$$\begin{aligned} 3 + 4\mathbb{Z} &= \{\dots, 3 + (-12), 3 + (-8), 3 + (-4), 3 + 0, 3 + 4, 3 + 8, 3 + 12, \dots\} \\ &= \{\dots, -9, -5, -1, 3, 7, 11, 15, \dots\} \end{aligned} \quad = -3 + 4\mathbb{Z}$$

$$\begin{aligned} 2 + 4\mathbb{Z} &= \{\dots, 2 + (-12), 2 + (-8), 2 + (-4), 2 + 0, 2 + 4, 2 + 8, 2 + 12, \dots\} \\ &= \{\dots, -10, -6, -2, 2, 6, 10, 14, \dots\} \end{aligned} \quad = -2 + 4\mathbb{Z}$$

$$\begin{aligned} 1 + 4\mathbb{Z} &= \{\dots, 1 + (-12), 1 + (-8), 1 + (-4), 1 + 0, 1 + 4, 1 + 8, 1 + 12, \dots\} \\ &= \{\dots, -11, -7, -3, 1, 5, 9, 13, \dots\} \end{aligned} \quad = -1 + 4\mathbb{Z}$$

$$\begin{aligned} 0 + 4\mathbb{Z} &= \{\dots, 0 + (-12), 0 + (-8), 0 + (-4), 0 + 0, 0 + 4, 0 + 8, 0 + 12, \dots\} \\ &= \{\dots, -12, -8, -4, 0, 4, 8, 12, \dots\} \end{aligned} \quad = 4\mathbb{Z}$$

$$\begin{aligned} -1 + 4\mathbb{Z} &= \{\dots, -1 + (-12), -1 + (-8), -1 + (-4), -1 + 0, -1 + 4, -1 + 8, -1 + 12, \dots\} \\ &= \{\dots, -13, -9, -5, -1, 3, 7, 11, \dots\} \end{aligned} \quad = 3 + 4\mathbb{Z}$$

$$\begin{aligned} -2 + 4\mathbb{Z} &= \{\dots, -2 + (-12), -2 + (-8), -2 + (-4), -2 + 0, -2 + 4, -2 + 8, -2 + 12, \dots\} \\ &= \{\dots, -14, -10, -6, -2, 2, 6, 10, \dots\} \end{aligned} \quad = 2 + 4\mathbb{Z}$$

$$\begin{aligned} -3 + 4\mathbb{Z} &= \{\dots, -3 + (-12), -3 + (-8), -3 + (-4), -3 + 0, -3 + 4, -3 + 8, -3 + 12, \dots\} \\ &= \{\dots, -15, -11, -7, -3, 1, 5, 9, \dots\} \end{aligned} \quad = 1 + 4\mathbb{Z}$$

$$\begin{aligned} -4 + 4\mathbb{Z} &= \{\dots, -4 + (-12), -4 + (-8), -4 + (-4), -4 + 0, -4 + 4, -4 + 8, -4 + 12, \dots\} \\ &= \{\dots, -16, -12, -8, -4, 0, 4, 8, \dots\} \end{aligned} \quad = 0 + 4\mathbb{Z}$$

$$\begin{aligned} -5 + 4\mathbb{Z} &= \{\dots, -5 + (-12), -5 + (-8), -5 + (-4), -5 + 0, -5 + 4, -5 + 8, -5 + 12, \dots\} \\ &= \{\dots, -17, -13, -9, -5, -1, 3, 7, \dots\} \end{aligned} \quad = -1 + 4\mathbb{Z}$$

\vdots

$$\begin{aligned} \{\dots, -8, -4, +0, +4, +8, \dots\} &+ 4\mathbb{Z} = \{4 + 4\mathbb{Z}\} = \{0 + 4\mathbb{Z}\} = \{4\mathbb{Z}\} \\ \cup & \cup \end{aligned}$$

$$\begin{aligned} \{\dots, -9, -5, -1, +3, +7, \dots\} &+ 4\mathbb{Z} = \{3 + 4\mathbb{Z}\} \\ \cup & \cup \end{aligned}$$

$$\begin{aligned} \{\dots, -10, -6, -2, +2, +6, \dots\} &+ 4\mathbb{Z} = \{2 + 4\mathbb{Z}\} \\ \cup & \cup \end{aligned}$$

$$\begin{aligned} \{\dots, -11, -7, -3, +1, +5, \dots\} &+ 4\mathbb{Z} = \{1 + 4\mathbb{Z}\} \\ \parallel & \parallel \end{aligned}$$

$$\begin{aligned} \mathbb{Z} &+ 4\mathbb{Z} = \{4\mathbb{Z}, \\ &1 + 4\mathbb{Z}, \\ &2 + 4\mathbb{Z}, \\ &3 + 4\mathbb{Z}\} \end{aligned}$$

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

$$= \{\dots, -3 + 4\mathbb{Z}, -2 + 4\mathbb{Z}, -1 + 4\mathbb{Z}, 0 + 4\mathbb{Z}, 1 + 4\mathbb{Z}, 2 + 4\mathbb{Z}, 3 + 4\mathbb{Z}, \dots\}$$

L_g : left shift

$$H \xrightarrow{L_g} gH$$

定理 5.3. according to the rearrangement theorem

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

定理 5.4.

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

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

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

$$\begin{array}{ccc} g \in H \Rightarrow gH = H & \Leftrightarrow & gH \neq H \Rightarrow g \notin H \\ & \text{let } H \leq G & \\ gH = H \Rightarrow g \in H & \Leftrightarrow & g \notin H \Rightarrow gH \neq H \\ g \cdot e = ge \in H & & \\ & H \leq G & \\ & \Downarrow & \\ & g \in H \Leftrightarrow gH = H & \\ & \Updownarrow & \\ & g \notin H \Leftrightarrow gH \neq H & \end{array}$$

定理 5.5.

$$\begin{array}{ccc} H \leq G & \wedge & g_1, g_2 \in G \\ & \Downarrow & \\ g_1H = g_2H & \Leftrightarrow & \bar{g}_2g_1 \in H \\ & \Updownarrow & \\ g_1H \neq g_2H & \Leftrightarrow & \bar{g}_2g_1 \notin H \end{array}$$

Proof.

$$\begin{array}{ll} g_1H = g_2H & \exists e = e_H = e_G \in H \subseteq G \\ g_1 = g_1 \cdot e = g_1e = g_2h & \exists h \in H \\ g_1 = g_2h & \\ \bar{g}_2g_1 = \bar{g}_2g_2h = eh = h & \\ \bar{g}_2g_1 = h \in H & \bar{g}_2g_1 \in H \end{array}$$

□

$$\bar{g}_2g_1 \in H \Rightarrow g_1H = g_2H$$

定理 5.6. coset mutually exclusive theorem

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

Proof.

$$\begin{array}{l} g_1H \cap g_2H \neq \emptyset \\ \Downarrow \\ \exists g_1h_1 = g_2h_2 \in g_1H \cap g_2H \\ \Downarrow \\ g_1h_1 = g_2h_2 \\ g_1 = g_1e = g_1h_1\bar{h}_1 = g_2h_2\bar{h}_1 \\ g_1 = g_2h_2\bar{h}_1 \\ \Downarrow \\ g_1H = \{g_1h | h \in H\} = \{g_2h_2\bar{h}_1h | h \in H\} \\ = \{g_2(h_2\bar{h}_1h) | h \in H\} \quad \tilde{h} = h_2\bar{h}_1h \in H \\ \stackrel{\text{rearrangement theorem}}{=} \{g_2\tilde{h} | \tilde{h} \in H\} = g_2H \Rightarrow g_1H \neq g_2H \end{array}$$

□

定理 5.7. coset partitioning group

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

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

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

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

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

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

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

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

$$= (D_3, \cdot) = (D_3, \cdot_G)$$

$$e = \rho_0$$

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

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

$$= \mathbb{Z}_{[0,3)} = (\mathbb{Z}_3, +_{\mathbb{Z}_n})$$

$$= (\mathbb{Z}_4, \cdot) = (\mathbb{Z}_4, \cdot_G)$$

$$\mathbb{Z}_3 \leq D_3 \Rightarrow \mathbb{Z}_3 = \{0, 1, 2\}$$

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

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

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

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

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

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

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

$$g^3 = e$$

$$a^3 = e$$

$$\rho^3 = e$$

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

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

$$= \mathbb{Z}_3$$

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

$$= \mathbb{Z}_3$$

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

$$= \mathbb{Z}_3$$

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

$$= \mathbb{Z}_3$$

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

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

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

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

$$= \{\pi_0, \pi_{-1}, \pi_{-2}\} = \{\pi_0, \pi_2, \pi_1\} = \{\pi_0, \pi_1, \pi_2\}$$

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

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

$$= \{\pi_1, \pi_0, \pi_{-1}\} = \{\pi_1, \pi_0, \pi_2\} = \{\pi_0, \pi_1, \pi_2\}$$

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

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

$$= \{\pi_2, \pi_1, \pi_0\} = \{\pi_0, \pi_1, \pi_2\}$$

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

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

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

$$= \{e\mathbb{Z}_3, \pi_i\mathbb{Z}_3\}$$

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

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

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

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

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

$$= \mathbb{Z}_3 \cup \pi_i\mathbb{Z}_3$$

$$= \dots$$

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

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

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

$$= \{\dots, -3 + 4\mathbb{Z}, -2 + 4\mathbb{Z}, -1 + 4\mathbb{Z}, 0 + 4\mathbb{Z}, 1 + 4\mathbb{Z}, 2 + 4\mathbb{Z}, 3 + 4\mathbb{Z}, \dots\}$$

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

定理 5.8.

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

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

$$\begin{aligned}
 H &\leq G \\
 |G| &< \infty \\
 &\Downarrow \\
 |gH| &= |H| \\
 G &= \bigcup_{g \in G} gH \\
 g_i H &\neq g_j H \Rightarrow g_i H \cap g_j H = \emptyset \\
 |G| / |H| &\in \mathbb{N} \Rightarrow |H| \mid |G| \Leftrightarrow |G| = n |H| \quad n \in \mathbb{N} \\
 G \text{ is a group} &\Rightarrow \{H | H \leq G\} = \{\{e\}, G\} \\
 |G| = p \in \mathbb{P} & \\
 G \text{ is a group} & \\
 |G| = p \in \mathbb{P} & \\
 g &\neq e = e_G \\
 \langle g \rangle &= \{g^n | n \in \mathbb{N}\} \\
 &\Downarrow \\
 \langle g \rangle &\leq G \\
 \langle g \rangle &\in \{H | H \leq G\} = \{\{e\}, G\} \\
 \langle g \rangle &\neq \{e\} \\
 &\Downarrow \\
 \langle g \rangle &= G \\
 \Downarrow \text{ord } \langle g \rangle &= |\langle g \rangle| \\
 \text{ord } \langle g \rangle &= \text{ord } G \\
 &= |\langle g \rangle| = |G| = p \in \mathbb{P} \\
 \text{ord } \langle g \rangle &= p \in \mathbb{P}
 \end{aligned}$$

5.1 left coset space

定義 5.10. indexed set

$$\begin{aligned}
 \{a_i\}_{i \in I} &= \{a_i | i \in I\} = \{\cdots, a_i, \cdots\} & i \in I \\
 &= \bigcup_{i \in I} \{a_i\} & i \in I \\
 &= \begin{cases} \bigcup_{i=1}^n \{a_i\} & |\{a_i\}_{i \in I}| = n \in \mathbb{N} \\ \bigcup_{i \in I} \{a_i\} & I \in \{\mathbb{N}, \mathbb{Z}, [0, 1], \mathbb{R}, \cdots\} \end{cases} \\
 \{a_i\}_{i \in \mathbb{N}} &= \{a_i | i \in \mathbb{N}\} = \{a_1, a_2, \cdots, a_i, \cdots\} = \{a_1, a_2, a_3, \cdots\} & i \in \mathbb{N} \\
 = \{a_n\}_{n \in \mathbb{N}} &= \{a_n | n \in \mathbb{N}\} = \{a_1, a_2, \cdots, a_n, \cdots\} = \{a_1, a_2, a_3, \cdots\} & n \in \mathbb{N} \\
 &= \bigcup_{i \in \mathbb{N}} \{a_i\} = \bigcup_{n \in \mathbb{N}} \{a_n\} = \begin{cases} \bigcup_{i=1}^n \{a_i\} & |\{a_i\}_{i \in \mathbb{N}}| = n \in \mathbb{N} \\ \bigcup_{n \in \mathbb{N}} \{a_n\} & |\{a_i\}_{i \in \mathbb{N}}| = |\mathbb{N}| \end{cases} \\
 \{a_i\}_{i=1}^n &= \bigcup_{i=1}^n \{a_i\} = \{a_1, a_2, \cdots, a_n\} = \{a_1, \cdots, a_n\} & \forall n \in \mathbb{N}
 \end{aligned}$$

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

定義 5.11. indexed sequence

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

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

定義 5.12. indexed tuple

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

$$\begin{aligned}
\mathbf{x} = x_i &= (x_i)_{i \in \mathbb{N}} = (x_i | i \in \mathbb{N}) = (x_1, x_2, \dots, x_i, \dots) = (x_1, x_2, x_3, \dots) & i \in \mathbb{N} \\
&= (x_n)_{n \in \mathbb{N}} = (x_n | n \in \mathbb{N}) = (x_1, x_2, \dots, x_n, \dots) = (x_1, x_2, x_3, \dots) & n \in \mathbb{N} \\
&= \left(\begin{matrix} , \\ i \in \mathbb{N} \end{matrix} , x_i \right) = \left(\begin{matrix} , \\ n \in \mathbb{N} \end{matrix} , x_n \right) \\
&= \langle x_i \rangle_{i \in \mathbb{N}} = (x_1 \quad x_2 \quad \dots \quad x_i \quad \dots)^\top = [x_1 \quad x_2 \quad \dots \quad x_i \quad \dots]^\top & i \in \mathbb{N} \\
&= \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_i \\ \vdots \end{pmatrix} = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_i \\ \vdots \end{bmatrix} & i \in \mathbb{N} \\
\langle x_i \rangle_{i=1}^n &= \left\langle \begin{matrix} n \\ i=1 \end{matrix} , x_i \right\rangle = \langle x_1, x_2, \dots, x_n \rangle = \langle x_1, \dots, x_n \rangle & \forall n \in \mathbb{N} \\
&= \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} & \forall n \in \mathbb{N}
\end{aligned}$$

$$\begin{aligned}
\mathbf{x} = x_\mu &= (x_i)_{i \in \mathbb{Z}_{\geq 0}} = (x_i | i \in \mathbb{Z}_{\geq 0}) = (x_0, x_1, x_2, \dots, x_i, \dots) = (x_0, x_1, x_2, x_3, \dots) & i \in \mathbb{Z}_{\geq 0} \\
&= (x_k)_{k \in \mathbb{Z}_{\geq 0}} = (x_k | k \in \mathbb{Z}_{\geq 0}) = (x_0, x_1, \dots, x_k, \dots) = (x_0, x_1, x_2, \dots) & k \in \mathbb{Z}_{\geq 0} \\
&= (x_\mu)_{\mu \in \mathbb{Z}_{\geq 0}} = (x_\mu | \mu \in \mathbb{Z}_{\geq 0}) = (x_0, x_1, \dots, x_\mu, \dots) = (x_0, x_1, x_2, \dots) & \mu \in \mathbb{Z}_{\geq 0} \\
&= \left(\begin{array}{c} x_i \\ i \in \mathbb{Z}_{\geq 0} \end{array} \right) = \left(\begin{array}{c} x_n \\ \mu \in \mathbb{Z}_{\geq 0} \end{array} \right) \\
&= \langle x_\mu \rangle_{\mu \in \mathbb{Z}_{\geq 0}} = (x_0 \ x_1 \ \dots \ x_\mu \ \dots)^\top = [x_0 \ x_1 \ \dots \ x_\mu \ \dots]^\top & \mu \in \mathbb{Z}_{\geq 0} \\
&= \begin{pmatrix} x_0 \\ x_1 \\ \vdots \\ x_\mu \\ \vdots \end{pmatrix} = \begin{bmatrix} x_0 \\ x_1 \\ \vdots \\ x_\mu \\ \vdots \end{bmatrix} & \mu \in \mathbb{Z}_{\geq 0} \\
\langle x_\mu \rangle_{\mu=0}^{n-1} &= \left\langle \begin{array}{c} x_\mu \\ \mu=0 \end{array} \right\rangle = \langle x_0, x_1, \dots, x_{n-1} \rangle = \langle x_0, \dots, x_{n-1} \rangle & \forall n \in \mathbb{N} \\
&= \begin{pmatrix} x_0 \\ x_1 \\ \vdots \\ x_{n-1} \end{pmatrix} = \begin{bmatrix} x_0 \\ x_1 \\ \vdots \\ x_{n-1} \end{bmatrix} = \begin{pmatrix} x_0 \\ \vdots \\ x_{n-1} \end{pmatrix} = \begin{bmatrix} x_0 \\ \vdots \\ x_{n-1} \end{bmatrix} & \forall n \in \mathbb{N}
\end{aligned}$$

定義 5.13. left coset space

G is a group

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

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

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

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

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

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

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

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

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

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

$$\mathbb{Z}_3 \leq D_3 \Rightarrow \mathbb{Z}_3 = \{0, 1, 2\}$$

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

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

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

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

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

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

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

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

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

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

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

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

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

$$= \{\pi_0, \pi_{-1}, \pi_{-2}\} = \{\pi_0, \pi_2, \pi_1\} = \{\pi_0, \pi_1, \pi_2\} \quad \pi_i = \pi_{3+i} = \pi_0\mathbb{Z}_3$$

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

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

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

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

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

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

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

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

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

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

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

$$\quad \quad \quad i \in \{0, 1, 2\} = \mathbb{Z}_{[0,3)}$$

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

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

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

$$\mathbb{Z}/4\mathbb{Z} = \mathbb{Z} + 4\mathbb{Z} = \{k + 4\mathbb{Z} | k \in \mathbb{Z}\} = \{4\mathbb{Z}, 1 + 4\mathbb{Z}, 2 + 4\mathbb{Z}, 3 + 4\mathbb{Z}\}$$

$$= \{\dots, -3 + 4\mathbb{Z}, -2 + 4\mathbb{Z}, -1 + 4\mathbb{Z}, 0 + 4\mathbb{Z}, 1 + 4\mathbb{Z}, 2 + 4\mathbb{Z}, 3 + 4\mathbb{Z}, \dots\}$$

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

6 normal subgroup

定義 6.1. normal subgroup

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

trivial subgroups are normal subgroups

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

central subgroup is a normal subgroup

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

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

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

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

$$\mathbb{Z}_2 \not\trianglelefteq S_3 = D_3$$

定義 6.2. set mulitplication and set inverse

$$\begin{aligned}
S^{-1} &= \overline{S} = \{\overline{s} | s \in S\} = \{s^{-1} | s \in S\} \\
gS &= \{gs | s \in S\} \quad \{sg | s \in S\} = Sg \\
S_1 S_2 &= \left\{ s_1 s_2 \left| \begin{array}{l} s_1 \in S_1 \\ s_2 \in S_2 \end{array} \right. \right\}
\end{aligned}$$

定理 6.3. subgroup or group multiplication closure and inverse closure

$$\begin{aligned}
H &\leq G \\
&\Downarrow \\
HH &= H \quad HH = \left\{ h_1 h_2 \left| \begin{array}{l} h_1 \in H \\ h_2 \in H \end{array} \right. \right\} \\
&\wedge \\
H^{-1} &= \overline{H} = H \quad H^{-1} = \overline{H} = \{\overline{h} | h \in H\} = \{h^{-1} | h \in H\} \\
H \leq G &\Rightarrow \begin{cases} HH = H & \text{group multiplication closure} \\ \overline{H} = H & \text{group inverse closure} \end{cases}
\end{aligned}$$

定理 6.4.

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

Proof.

$$\begin{aligned}
(g_1 N) (g_2 N) &= (g_1 N g_2) (N) & (g_1 n_1) (g_2 n_2) &= (g_1 n_1 g_2) n_2 \\
&= (g_1 g_2 N) (N) & & \stackrel{N \trianglelefteq G \Rightarrow gn = ng}{=} (g_1 g_2 n_1) n_2 \\
&= (g_1 g_2) (NN) & & = (g_1 g_2) (n_1 n_2) \\
&= (g_1 g_2) (N) \quad N \leq G \Rightarrow NN = N \Leftarrow HH = H \Leftarrow H \leq G \\
(g_1 N) (g_2 N) &= (g_1 g_2) N
\end{aligned}$$

□

定理 6.5.

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

Proof.

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

□

定理 6.6.

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

Proof.

$$\begin{aligned}
(N)(gN) &= (N)(Ng) & gN &= Ng \Leftarrow N \trianglelefteq G \\
&= (NN)g & (n_1)(n_2g) &= (n_1n_2)g \\
&= Ng & NN &= N \Leftarrow N \leq G \\
&= gN & gN &= Ng \Leftarrow N \trianglelefteq G
\end{aligned}$$

□

6.1 quotient group

 G is a group \Updownarrow

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

定義 6.7. quotient group

$$G/N = GN = (G/N, \cdot_{\text{group}}) = (GN, \cdot_{\text{set}})$$

$$= \left\{ gN \left| \begin{array}{ll} (g_1N)(g_2N) = (g_1g_2)N \in G/N & \forall g_1N, g_2N \in G/N \quad (c) \cdot_{\text{group}} \text{ closure} \\ g_1N(g_2Ng_3N) = (g_1Ng_2N)g_3N = g_1g_2g_3N & \forall g_1N, g_2N, g_3N \in G/N \quad (a) \cdot_{\text{group}} \text{ associativity} \\ (N)(gN) = NgN = gN = (gN)N = (gN)(N) & \exists N = e_{G/N} \in G/N, \forall gN \in G/N \quad (id) \text{ identity element} \\ \overline{(gN)}(gN) = \overline{gN}gN = N\bar{g}gN = NeN = NN = N & \forall gN \in G/N, \exists \overline{gN} \in G/N \quad (in) \text{ inverse element} \end{array} \right. \right\}$$

 \Downarrow

$$G/N = \{gN | g \in G\} \text{ is a group} \quad \forall N \trianglelefteq G$$

 \Updownarrow def. G/N is a quotient group

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

quotient group vs. left coset space

- quotient group

 G is a group

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

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

$$|G/N| = |G| / |N|$$

- left coset space

G is a group

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

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

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

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

$$|G/H| = |G| / |H|$$

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

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

$$\begin{aligned}
S_3 &= \{ \sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6 \} \\
&= \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\} \quad \text{two-line notation} \\
&= \{ [123], [231], [312], [213], [132], [321] \} \quad \text{one-line notation} \\
&= \{ 123, 231, 312, 213, 132, 321 \} \quad \text{one-line notation, simplified} \\
&= \{ (1)(2)(3), (123), (132), (12)(3), (1)(23), (31)(2) \} \quad \text{cycle notation} \\
&= \{ (), (123), (132), (12), (23), (31) \} \quad \text{cycle notation, simplified} \\
D_3 &= \{ \rho_0, \rho_1, \rho_2, \pi_0, \pi_1, \pi_2 \} \\
&= \{ e, \rho, \rho^2, \pi_0, \pi_1, \pi_2 \}
\end{aligned}$$

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

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

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

$$\begin{aligned}
D_3/C_3 = S_3/\mathbb{Z}_3 &= \{\sigma\mathbb{Z}_3 \mid \sigma \in S_3\} &&= S_3\mathbb{Z}_3 \\
&= \{[\textcolor{red}{123}]\mathbb{Z}_3, [\textcolor{violet}{213}]\mathbb{Z}_3\} &&= \{()\mathbb{Z}_3, (\textcolor{violet}{12})\mathbb{Z}_3\} \\
&= \{[\textcolor{red}{123}]\mathbb{Z}_3, [\textcolor{blue}{132}]\mathbb{Z}_3\} &&= \{()\mathbb{Z}_3, (\textcolor{blue}{23})\mathbb{Z}_3\} \\
&= \{[\textcolor{red}{123}]\mathbb{Z}_3, [\textcolor{brown}{321}]\mathbb{Z}_3\} &&= \{()\mathbb{Z}_3, (\textcolor{brown}{31})\mathbb{Z}_3\} \\
&= \{eC_3, \pi_i C_3\} &&= D_3C_3 \\
&= \{\rho_0 C_3, \pi_0 C_3\} \\
&= \{\rho_0 C_3, \pi_1 C_3\} \\
&= \{\rho_0 C_3, \pi_2 C_3\} \\
&= \{([\textcolor{red}{123}], [\textcolor{blue}{231}], [\textcolor{green}{312}]), ([\textcolor{violet}{213}], [\textcolor{blue}{132}], [\textcolor{brown}{321}])\} \\
&= \{([\textcolor{red}{123}], (\textcolor{blue}{123}), (\textcolor{green}{132})), ([\textcolor{violet}{213}], (\textcolor{blue}{23}), (\textcolor{brown}{31}))\} \\
&= \{(\rho_0, \rho_1, \rho_2), (\pi_0, \pi_1, \pi_2)\} \\
&= \{e, \rho, \rho^2\}, \{\pi_0, \pi_1, \pi_2\}
\end{aligned}$$

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

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

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

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

$$S_3 \triangleright C_3$$

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

$$|E_3| = 1$$

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

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

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

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

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

$$S_3 \triangleright C_3 \triangleright E_3$$

$$S_4 \triangleright A_4 \triangleright H_4 \triangleright C_2 \triangleright E_4$$

$$\begin{aligned}
S_4 &= \{ \begin{array}{cccccc} \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, \end{array} \} \\
&= \{ \begin{array}{cccccc} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, & \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \\ 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \\ 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}, & \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \\ 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \\ 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}, & \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \\ 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \\ 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}, & \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \\ 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \\ 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}, & \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \\ 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \\ 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} \} \\
&= \{ \begin{array}{cccccc} [123], & [231], & [312], & [213], & [132], & [321], \\ [123], & [231], & [312], & [213], & [132], & [321], \\ [123], & [231], & [312], & [213], & [132], & [321], \\ [123], & [231], & [312], & [213], & [132], & [321] \end{array} \} \\
&= \{ \begin{array}{cccccc} 123, & 231, & 312, & 213, & 132, & 321, \\ 123, & 231, & 312, & 213, & 132, & 321, \\ 123, & 231, & 312, & 213, & 132, & 321, \\ 123, & 231, & 312, & 213, & 132, & 321 \end{array} \} \\
&= \{ \begin{array}{cccccc} (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) \end{array} \} \\
&= \{ \begin{array}{cccccc} (), & (123), & (132), & (12), & (23), & (31), \\ (), & (123), & (132), & (12), & (23), & (31), \\ (), & (123), & (132), & (12), & (23), & (31), \\ (), & (123), & (132), & (12), & (23), & (31) \end{array} \}
\end{aligned}$$

6.2 simple group

定義 6.8. simple group

G is a group

G does not have no nontrivial normal groups $\forall N \trianglelefteq G [N \in \{\{e\}, G\}]$

\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 $\forall N \trianglelefteq G [N \in \{\{e\}, G\}]$

$|G| < \infty$

\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}_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 is a group

$$[g] = \{hg\bar{h} \mid h \in G\} \quad \forall g \in G$$

$$[g] \ni eg\bar{e} = ege = (eg)e = (g)e = ge = g$$

$$\Downarrow$$

$$g = eg\bar{e} \in [g]$$

$$\Downarrow$$

$$g \in [g]$$

G is a group

$$\tilde{g} \in [g] = \{hg\bar{h} \mid h \in G\} \quad \forall g \in G$$

$$\Downarrow$$

$$\tilde{g} = hg\bar{h}$$

$$\bar{h}\tilde{g}h = \bar{h}hg\bar{h}h = ege = g$$

G is a group

$$g = \bar{h}\tilde{g}h = \bar{h}\tilde{g}\bar{\bar{h}} \in \{\bar{h}\tilde{g}\bar{\bar{h}} \mid h \in G\} = \{h\tilde{g}\bar{h} \mid h \in G\} = [\tilde{g}] \quad \forall \tilde{g} \in G$$

$$\Downarrow$$

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

$$\bar{\bar{h}}h\tilde{h} = \bar{\bar{h}}h\tilde{h} = \bar{\bar{h}}(\bar{h}h)\tilde{h} = \bar{\bar{h}}(e)\tilde{h} = \bar{\bar{h}}\tilde{h} = e$$

$$\begin{cases} g \in [\tilde{g}] & \Rightarrow g = h\tilde{g}\bar{h} = h\tilde{h}\tilde{\bar{g}}\bar{\bar{h}} \stackrel{\bar{\bar{h}}h = \bar{\bar{h}}}{=} h\tilde{h}\tilde{\bar{g}}\bar{\bar{h}} \in \{h\tilde{h}\tilde{\bar{g}}\bar{\bar{h}} \mid h\tilde{h} \in G\} = [\tilde{\bar{g}}] \Rightarrow g \in [\tilde{\bar{g}}] \\ \tilde{g} \in [\tilde{\bar{g}}] & \Rightarrow \tilde{g} = \tilde{h}\tilde{\bar{g}}\bar{\bar{h}} \uparrow \end{cases}$$

G is a group

$$[e] = \{he\bar{h} \mid h \in G\} = \{h\bar{h} \mid h \in G\} = \{e \mid h \in G\} = \{e\} \quad e = e_G \in G$$

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

$$[c] = \{ch\bar{h} \mid h \in G\} = \{ch\bar{h} \mid ch = hc \quad \forall h \in G\} = \{ce \mid h \in G\} = \{c\} \quad \forall c \in C(G)$$

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

G is a group

$$g \in [\tilde{g}] = \{h\tilde{g}\bar{h} \mid h \in G\} \quad \tilde{g} \in G$$

$$\exists h \in G [g = h\tilde{g}\bar{h}]$$

$$g = h\tilde{g}\bar{h}$$

$$g^n = \overbrace{h\tilde{g}\bar{h}h\tilde{g}\bar{h} \cdots h\tilde{g}\bar{h}}^n = \overbrace{h\tilde{g}\bar{e}\bar{g}e \cdots e\bar{g}h}^n = \overbrace{h\tilde{g}\bar{g} \cdots \bar{g}h}^n = h\tilde{g}^n\bar{h} \in [\tilde{g}^n]$$

$$\forall n \in \mathbb{N}$$

$$g^n \in [\tilde{g}^n]$$

$$\forall n \in \mathbb{N}$$

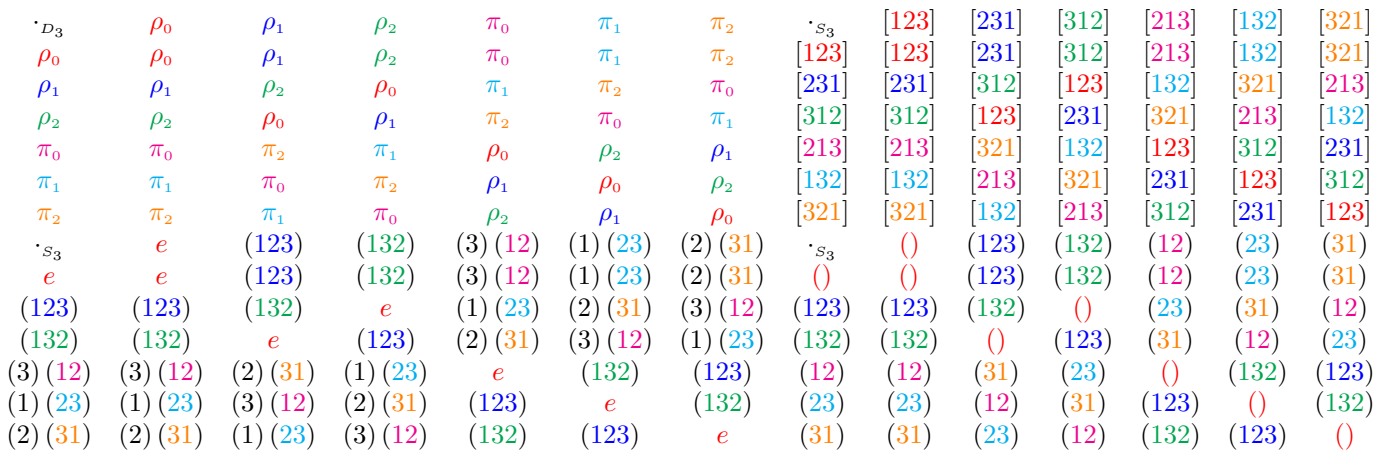
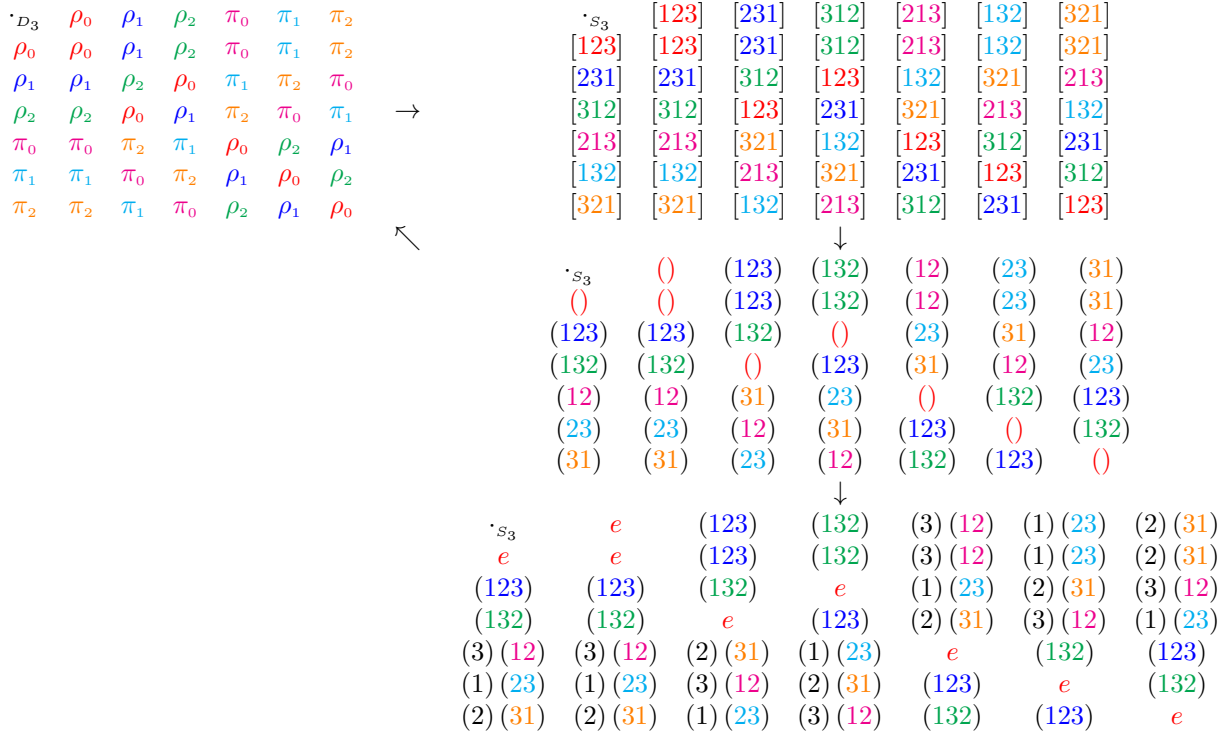
$$g^{-n} = \bar{g}^n = \overline{g^n} = \overline{h\tilde{g}^n\bar{h}} = \bar{\bar{h}}\bar{\tilde{g}^n}\bar{\bar{h}} = \bar{\bar{h}}\tilde{g}^n\bar{\bar{h}} = h\tilde{g}^{-n}\bar{h}$$

$$\forall n \in \mathbb{N}$$

$$g^m \in [\tilde{g}^m]$$

$$\forall m \in \mathbb{Z}$$

$$D_3 = S_3$$



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

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

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

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

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

$$= (D_3, \cdot) = (D_3, \cdot_G)$$

$$e = \rho_0$$

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

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

$$= \mathbb{Z}_{[0,3)} = (\mathbb{Z}_3, +_{\mathbb{Z}_n})$$

$$= (\mathbb{Z}_3, \cdot) = (\mathbb{Z}_3, \cdot_G)$$

$$g^3 = e$$

$$a^3 = e$$

$$\rho^3 = e$$

$$\mathbb{Z}_3 \leq D_3 \Rightarrow \mathbb{Z}_3 = \{0, 1, 2\}$$

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

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

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

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

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

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

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

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

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

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

$$= \{e\mathbb{Z}_3, \pi_i\mathbb{Z}_3\}$$

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

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

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

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

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

$$= \mathbb{Z}_3 \cup \pi_i\mathbb{Z}_3$$

$$= \dots$$

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

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

$$\rho_{k+3} = \rho_k$$

$$\pi_{k+3} = \pi_k$$

$$\rho_i \rho_j = \rho_{i+j}$$

$$\rho_i \pi_j = \pi_{i+j}$$

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

$$\pi_i \pi_j = \rho_{i-j}$$

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

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

$$\rho_0 = e = h e \bar{h} = h \bar{h} = e$$

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

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

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

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

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

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

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

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

\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)	$(12)(23)$	$(23)(31)$	$(31)(12)$
e	e	(123)	(132)	$(3)(12)$	$(1)(23)$	$(2)(31)$	$()$	$()$	(123)	(132)	$(12)(23)$	$(23)(31)$	$(31)(12)$
(123)	(123)	(132)	e	$(1)(23)$	$(2)(31)$	$(3)(12)$	(123)	(123)	(132)	$()$	$(23)(31)$	$(31)(12)$	$(12)(23)$
(132)	(132)	e	(123)	$(2)(31)$	$(3)(12)$	$(1)(23)$	(132)	(132)	$()$	(123)	$(31)(12)$	$(12)(23)$	$(23)(31)$
$(3)(12)$	$(3)(12)$	$(2)(31)$	$(1)(23)$	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)	$()$

$$D_3 = S_3$$

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

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

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

$$S_n$$

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

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

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

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

cycle type

$$n_i$$

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

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

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

Young diagram

$$S_4: [1^4] \times 1, [1^2 2] \times 6, [1^1 3^1] \times 8, [2^2] \times 3, [4^1] \times 6$$

D_n

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

$$N \trianglelefteq G$$

$$hN\overline{h}=h\overline{h}N=eN=N$$

$$N=hN\overline{h}=\left\{h\overline{h}\left|\begin{array}{l}n\in N\\h\in G\end{array}\right.\right\}=\bigcup_{n\in N}[n]$$

$$N=\bigcup_{n\in N}[n]$$

$$[n]\subseteq N\qquad\qquad\qquad\forall n\in N$$

$$\begin{aligned}
G &= (g_0N=eN=N) \cup (g_1N) \cup (g_2N) \cup \cdots \\
&\parallel \\
&[n_0]=[e] \\
&\cup \\
&[n_1] \\
&\cup \\
&[n_2] \\
&\cup \\
&\vdots
\end{aligned}$$

8 homomorphism

- homomorphism 同態 = 均態 = 均形
- endomorphism 內同態 = 內態 = 內形 = 內均形
- isomorphism 同構 = 同形
- automorphism 自同構 = 自構 = 同形 = 自同形

定義 8.1. homomorphism

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

preserving the corresponding identity element

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

preserving the corresponding inverse element

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

定義 8.2. endomorphism

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

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

$$\begin{array}{ll} \mathcal{V} \text{ is an additive Abelian group} & \Leftarrow \mathcal{V} = (\mathcal{V}, +_{\mathcal{V}}) = (\mathcal{V}, +_{\mathcal{V}}, \cdot_{\mathbb{F} \times \mathcal{V}, \mathbb{F}}) \\ \boldsymbol{v}, \tilde{\boldsymbol{v}} \in \mathcal{V} & \end{array}$$

$$\begin{array}{ll} \dot{\mathcal{V}} \text{ is an additive Abelian group} & \Leftarrow \dot{\mathcal{V}} = (\dot{\mathcal{V}}, +_{\dot{\mathcal{V}}}) = (\dot{\mathcal{V}}, +_{\dot{\mathcal{V}}}, \cdot_{\mathbb{F} \times \dot{\mathcal{V}}, \mathbb{F}}) \\ \dot{\boldsymbol{v}}, \tilde{\dot{\boldsymbol{v}}} \in \dot{\mathcal{V}} & \end{array}$$

$$L : \mathcal{V} \rightarrow \dot{\mathcal{V}} \quad \Leftrightarrow \mathcal{V} \xrightarrow{L} \dot{\mathcal{V}} \Leftrightarrow \varphi \in \dot{\mathcal{V}}^{\mathcal{V}}$$

$$\exists! \dot{\boldsymbol{v}} = L(\boldsymbol{v}), \exists! \tilde{\dot{\boldsymbol{v}}} = L(\tilde{\boldsymbol{v}})$$

$$\text{linear map } L : L(\lambda \boldsymbol{v} +_{\mathcal{V}} \tilde{\lambda} \tilde{\boldsymbol{v}}) = \lambda L(\boldsymbol{v}) +_{\dot{\mathcal{V}}} \tilde{\lambda} L(\tilde{\boldsymbol{v}})$$

\Downarrow

$$L(\boldsymbol{v} +_{\mathcal{V}} \tilde{\boldsymbol{v}}) = L(\boldsymbol{v}) +_{\dot{\mathcal{V}}} L(\tilde{\boldsymbol{v}})$$

$$= \dot{\boldsymbol{v}} \cdot_{\dot{\mathcal{V}}} \tilde{\dot{\boldsymbol{v}}}$$

$$L(\boldsymbol{v} +_{\mathcal{V}} \tilde{\boldsymbol{v}}) = L(\boldsymbol{v}) +_{\dot{\mathcal{V}}} L(\tilde{\boldsymbol{v}})$$

\Downarrow

$$\mathcal{V} \simeq \dot{\mathcal{V}}$$

homomorphism vs. isomorphism $\mathcal{V} \cong \dot{\mathcal{V}}$

\Updownarrow

$\mathcal{V}, \dot{\mathcal{V}}$ have homomorphism

homomorphism map L

preserving the corresponding identity element

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

preserving the corresponding inverse element

$$L(\boldsymbol{v}) = \dot{\boldsymbol{v}}$$

\Downarrow

$$L(\bar{\boldsymbol{v}}) = L(-\boldsymbol{v}) = -\dot{\boldsymbol{v}} = \bar{\dot{\boldsymbol{v}}}$$

定義 8.4. general linear group

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

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

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

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

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

範例 8.5. $GL_2(\mathbb{R}) \simeq \mathbb{R}_{\neq 0} \because \exists \det : GL(2, \mathbb{R}) = GL_2(\mathbb{R}) \rightarrow \mathbb{R}_{\neq 0} \subset \mathbb{R}$

$GL_2(\mathbb{R})$ is a multiplicative group

$$\Leftarrow GL_2(\mathbb{R}) = (GL_2(\mathbb{R}), \cdot_{\mathcal{M}})$$

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

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

$\mathbb{R}_{\neq 0}$ is a multiplicative group

$$\Rightarrow \mathbb{R}_{\neq 0} = (\mathbb{R}_{\neq 0}, \cdot_{\mathbb{R}})$$

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

$$\det : GL_2(\mathbb{R}) \rightarrow \mathbb{R}_{\neq 0} \subset \mathbb{R}$$

$$\Leftrightarrow GL_2(\mathbb{R}) \xrightarrow{\det} \mathbb{R} \Leftrightarrow \det \in \mathbb{R}^{GL_2(\mathbb{R})}$$

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

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

$$\Downarrow$$

$$GL_2(\mathbb{R}) \simeq \mathbb{R}_{\neq 0}$$

homomorphism not mentioned isomorphism here

$$\Updownarrow$$

$GL_2(\mathbb{R}), \mathbb{R}_{\neq 0}$ have homomorphism

homomorphism map \det

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

\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

$$\Leftarrow U(1) = (U(1), \cdot_{\mathbb{C}}) = \{|z| = 1 | \forall z \in \mathbb{C}\} = \{e^{i\theta} | \forall \theta \in \mathbb{R}\}$$

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

$$\exp i : \mathbb{R} \rightarrow U(1)$$

$$\Leftrightarrow \mathbb{R} \xrightarrow{\exp i} U(1) \Leftrightarrow \exp i \in U(1)^{\mathbb{R}}$$

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

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

$$\Downarrow$$

$$\mathbb{R} \simeq U(1)$$

homomorphism not mentioned isomorphism here

$$\Updownarrow$$

$\mathbb{R}, U(1)$ have homomorphism

homomorphism map $\exp i$

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

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

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

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

S_n is a group

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

\mathbb{Z}_2 is a group

$\sigma, \tilde{\sigma} \in \mathbb{Z}_2$

$\text{sgn} = \text{sgn} : S_n \rightarrow \mathbb{Z}_2$

$$\text{sgn}(\sigma \cdot_{S_n} \tilde{\sigma}) = \text{sgn}(\sigma \tilde{\sigma}) = \text{sgn}(\sigma) \text{sgn}(\tilde{\sigma}) = \text{sgn}(\sigma) \cdot_{\mathbb{Z}_2} \text{sgn}(\tilde{\sigma})$$

\Downarrow

$S_n \simeq \mathbb{Z}_2$

\Updownarrow

S_n, \mathbb{Z}_2 have homomorphism

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

$$\begin{aligned} \Leftarrow \mathbb{Z}_2 = (\mathbb{Z}_2, \cdot_{\mathbb{Z}_2}) &= \left\{ e^{i\frac{2\pi}{2} \cdot 0}, e^{i\frac{2\pi}{2} \cdot (2-1)} \right\} \\ &= \{e^{i0}, e^{i\pi}\} \\ &= \{-1, +1\} \end{aligned}$$

$$\begin{aligned} &\Leftrightarrow S_n \xrightarrow{\text{sgn}} \mathbb{Z}_2 \Leftrightarrow \text{sgn} \in \mathbb{Z}_2^{S_n} \\ \text{sgn}(\sigma) &= \begin{cases} +1 & \sigma \text{ even} \Leftrightarrow N_\sigma \in 2\mathbb{Z}_{\geq 0} \\ -1 & \sigma \text{ odd} \Leftrightarrow N_\sigma \in 2\mathbb{N} - 1 \end{cases} \end{aligned}$$

$$\exists! \sigma = \text{sgn}(\sigma), \exists! \tilde{\sigma} = \text{sgn}(\tilde{\sigma})$$

$$= \sigma \cdot_{\mathbb{Z}_2} \tilde{\sigma}$$

homomorphism not mentioned isomorphism here

homomorphism map sgn

8.1 isomorphism

8.2 homomorphism kernel

Part II

tensor

9 tensor algebra

9.1 vector space

$$\begin{aligned}
\mathbb{F}^n &\in \{\mathbb{R}^n, \mathbb{C}^n, \mathbb{R}^\infty, \dots\} & \tilde{\mathfrak{V}}, \mathfrak{V} \subseteq \mathcal{V} \subseteq \mathbb{F}^n &\in \{\mathbb{R}^n, \mathbb{C}^n, \dots\} \\
\mathcal{V} \ni \mathbf{v} = v^j \mathbf{v}_j &= \sum_j v^j \mathbf{v}_j & \mathbf{v}_j \in \mathfrak{V} = \{\mathbf{v}_j\} &= \{\mathbf{v}_j\}_j \\
&= \begin{cases} v^1 \mathbf{v}_1 + \dots + v^n \mathbf{v}_n &= \sum_{j=1}^n v^j \mathbf{v}_j \\ \dots + v^j \mathbf{v}_j + \dots &= \sum_{j \in J} v^j \mathbf{v}_j \end{cases} & &= \begin{cases} \{\mathbf{v}_j\}_{j=1}^n \\ \{\mathbf{v}_j\}_{j \in J} \end{cases} \quad J \in \{\mathbb{N}, \mathbb{Z}, \mathbb{R}, \dots\} \\
&= \begin{cases} v^1 \begin{bmatrix} | \\ \mathbf{v}_1 \\ | \end{bmatrix} + \dots + v^n \begin{bmatrix} | \\ \mathbf{v}_n \\ | \end{bmatrix} &= \begin{bmatrix} | & \dots & | \\ \mathbf{v}_1 & & \mathbf{v}_n \\ | & & | \end{bmatrix} \begin{bmatrix} v^1 \\ \vdots \\ v^n \end{bmatrix} \\ \dots + v^j \begin{bmatrix} | \\ \mathbf{v}_j \\ | \end{bmatrix} + \dots &= \begin{bmatrix} \dots & | & \dots \\ \dots & \mathbf{v}_j & \dots \\ \dots & | & \dots \end{bmatrix} \begin{bmatrix} \vdots \\ v^j \\ \vdots \end{bmatrix} \end{cases} = \begin{bmatrix} \vdots \\ \mathbf{v}_j \\ \vdots \end{bmatrix}^\top \begin{bmatrix} \vdots \\ v^j \\ \vdots \end{bmatrix} = V[\mathbf{v}]_V \quad [\mathbf{v}]_V \in \begin{cases} \mathbb{F}^n \\ \mathbb{F}^{|J|} \end{cases} \\
&= \tilde{v}^j \tilde{\mathbf{v}}_j = \sum_j \tilde{v}^j \tilde{\mathbf{v}}_j & \tilde{\mathbf{v}}_j \in \tilde{\mathfrak{V}} = \{\tilde{\mathbf{v}}_j\} &= \{\tilde{\mathbf{v}}_j\}_j \\
&= \begin{cases} \tilde{v}^1 \tilde{\mathbf{v}}_1 + \dots + \tilde{v}^n \tilde{\mathbf{v}}_n &= \sum_{j=1}^n \tilde{v}^j \tilde{\mathbf{v}}_j \\ \dots + \tilde{v}^j \tilde{\mathbf{v}}_j + \dots &= \sum_{j \in J} \tilde{v}^j \tilde{\mathbf{v}}_j \end{cases} & &= \begin{cases} \{\tilde{\mathbf{v}}_j\}_{j=1}^n \\ \{\tilde{\mathbf{v}}_j\}_{j \in J} \end{cases} \quad J \in \{\mathbb{N}, \mathbb{Z}, \mathbb{R}, \dots\} \\
&= \begin{cases} \tilde{v}^1 \begin{bmatrix} | \\ \tilde{\mathbf{v}}_1 \\ | \end{bmatrix} + \dots + \tilde{v}^n \begin{bmatrix} | \\ \tilde{\mathbf{v}}_n \\ | \end{bmatrix} &= \begin{bmatrix} | & \dots & | \\ \tilde{\mathbf{v}}_1 & & \tilde{\mathbf{v}}_n \\ | & & | \end{bmatrix} \begin{bmatrix} \tilde{v}^1 \\ \vdots \\ \tilde{v}^n \end{bmatrix} \\ \dots + \tilde{v}^j \begin{bmatrix} | \\ \tilde{\mathbf{v}}_j \\ | \end{bmatrix} + \dots &= \begin{bmatrix} \dots & | & \dots \\ \dots & \tilde{\mathbf{v}}_j & \dots \\ \dots & | & \dots \end{bmatrix} \begin{bmatrix} \vdots \\ \tilde{v}^j \\ \vdots \end{bmatrix} \end{cases} = \begin{bmatrix} \vdots \\ \tilde{\mathbf{v}}_j \\ \vdots \end{bmatrix}^\top \begin{bmatrix} \vdots \\ \tilde{v}^j \\ \vdots \end{bmatrix} = \tilde{V}[\mathbf{v}]_{\tilde{V}} \quad [\mathbf{v}]_{\tilde{V}} \in \begin{cases} \mathbb{F}^n \\ \mathbb{F}^{|J|} \end{cases}
\end{aligned}$$

$$\begin{aligned}
\mathbf{v} &= V[\mathbf{v}]_V = \tilde{V}[\mathbf{v}]_{\tilde{V}} \\
v^i &= V^i_j v^j = \tilde{V}^i_j \tilde{v}^j \\
v^k &= V^k_i v^i = \tilde{V}^k_j \tilde{v}^j \\
[\mathbf{v}]_V &= V^{-1} \tilde{V}[\mathbf{v}]_{\tilde{V}} = \bar{V} \tilde{V}[\mathbf{v}]_{\tilde{V}} = F[\mathbf{v}]_{\tilde{V}} \\
v^i &= (V^k_i)^{-1} \tilde{V}^k_j \tilde{v}^j = \bar{V}^k_i \tilde{V}^k_j \tilde{v}^j = F^i_j \tilde{v}^j \\
&= (V^{-1})^i_k \tilde{V}^k_j \tilde{v}^j = \bar{V}^i_k \tilde{V}^k_j \tilde{v}^j = F^i_j \tilde{v}^j \\
(V^{-1})^i_k \tilde{V}^k_j &= \bar{V}^i_k \tilde{V}^k_j = F^i_j \\
F^i_j &= (V^{-1})^i_k \tilde{V}^k_j \\
(V^{-1})^i_k &= (V^k_i)^{-1} \\
[\mathbf{v}]_{\tilde{V}} &= \tilde{V}^{-1} V[\mathbf{v}]_V = B[\mathbf{v}]_V \\
\tilde{v}^j &= \left(\tilde{V}^k_j \right)^{-1} V^k_i v^i = B^j_i v^i \\
&= \left(\tilde{V}^{-1} \right)^j_k V^k_i v^i = B^j_i v^i \\
&= \left(\tilde{V}^{-1} \right)^j_k V^k_i = B^j_i \\
B^j_i &= \left(\tilde{V}^{-1} \right)^j_k V^k_i \\
\left(\tilde{V}^{-1} \right)^j_k &= \left(\tilde{V}^k_j \right)^{-1}
\end{aligned}$$

$$\begin{aligned}
v^i v_i &= \tilde{v}^j \tilde{v}_j = \left(\tilde{V}^k_j \right)^{-1} V^k_i v^i \tilde{v}_j = B^j_i v^i \tilde{v}_j \quad \tilde{v}^j = \left(\tilde{V}^k_j \right)^{-1} V^k_i v^i = B^j_i v^i \\
v^i v_i &= \left(\tilde{V}^k_j \right)^{-1} V^k_i v^i \tilde{v}_j = B^j_i v^i \tilde{v}_j \quad \not\equiv \\
v_i &= \left(\tilde{V}^k_j \right)^{-1} V^k_i \tilde{v}_j = B^j_i \tilde{v}_j \\
\tilde{v}^j \tilde{v}_j &= v^i v_i = (V^k_i)^{-1} \tilde{V}^k_j \tilde{v}^j v_i = F^i_j \tilde{v}^j v_i \quad v^i = (V^k_i)^{-1} \tilde{V}^k_j \tilde{v}^j = F^i_j \tilde{v}^j \\
\tilde{v}^j \tilde{v}_j &= (V^k_i)^{-1} \tilde{V}^k_j \tilde{v}^j v_i = F^i_j \tilde{v}^j v_i \quad \not\equiv \\
\tilde{v}_j &= (V^k_i)^{-1} \tilde{V}^k_j v_i = F^i_j v_i
\end{aligned}$$

$$\left\{ \begin{array}{l} \left\{ \begin{array}{l} v^i = F^i_j \tilde{v}^j = (V^{-1})^i_k \tilde{V}^k_j \tilde{v}^j \\ \tilde{v}^j = B^j_i v^i = \left(\tilde{V}^{-1} \right)^j_k V^k_i v^i \end{array} \right. \quad \left\{ \begin{array}{l} [\mathbf{v}]_V = F[\mathbf{v}]_{\tilde{V}} = V^{-1} \tilde{V}[\mathbf{v}]_{\tilde{V}} \\ [\mathbf{v}]_{\tilde{V}} = B[\mathbf{v}]_V = \tilde{V}^{-1} V[\mathbf{v}]_V \end{array} \right. \quad \text{contravariant} \\ \left\{ \begin{array}{l} v_i = B^j_i \tilde{v}_j = \left(\tilde{V}^k_j \right)^{-1} V^k_i \tilde{v}_j \\ \tilde{v}_j = F^i_j v_i = (V^k_i)^{-1} \tilde{V}^k_j v_i \end{array} \right. \quad \left\{ \begin{array}{l} \begin{bmatrix} \mathbf{v}_1 \\ \vdots \\ \mathbf{v}_n \end{bmatrix}^T = \begin{bmatrix} \tilde{\mathbf{v}}_1 \\ \vdots \\ \tilde{\mathbf{v}}_n \end{bmatrix}^T B = \begin{bmatrix} \tilde{\mathbf{v}}_1 \\ \vdots \\ \tilde{\mathbf{v}}_n \end{bmatrix}^T \tilde{V}^{-1} V \\ \begin{bmatrix} \tilde{\mathbf{v}}_1 \\ \vdots \\ \tilde{\mathbf{v}}_n \end{bmatrix}^T = \begin{bmatrix} \mathbf{v}_1 \\ \vdots \\ \mathbf{v}_n \end{bmatrix}^T F = \begin{bmatrix} \mathbf{v}_1 \\ \vdots \\ \mathbf{v}_n \end{bmatrix}^T V^{-1} \tilde{V} \end{array} \right. \quad \text{covariant} \end{array} \right.$$

$$\left\{ \begin{array}{l} \left\{ \begin{array}{l} v^i = F^i_j \tilde{v}^j = (V^{-1})^i_k \tilde{V}^k_j \tilde{v}^j \\ \tilde{v}^j = B^j_i v^i = \left(\tilde{V}^{-1} \right)^j_k V^k_i v^i \end{array} \right. \quad \left\{ \begin{array}{l} \begin{bmatrix} v^1 \\ \vdots \\ v^n \end{bmatrix} = F \begin{bmatrix} \tilde{v}^1 \\ \vdots \\ \tilde{v}^n \end{bmatrix} = V^{-1} \tilde{V} \begin{bmatrix} \tilde{v}^1 \\ \vdots \\ \tilde{v}^n \end{bmatrix} \\ \begin{bmatrix} \tilde{v}^1 \\ \vdots \\ \tilde{v}^n \end{bmatrix} = B \begin{bmatrix} v^1 \\ \vdots \\ v^n \end{bmatrix} = \tilde{V}^{-1} V \begin{bmatrix} v^1 \\ \vdots \\ v^n \end{bmatrix} \end{array} \right. \quad \text{contravariant} \\ \left\{ \begin{array}{l} v_i = \tilde{v}_j B^j_i = \tilde{v}_j \left(\tilde{V}^k_j \right)^{-1} V^k_i \\ \tilde{v}_j = v_i F^i_j = v_i (V^k_i)^{-1} \tilde{V}^k_j \end{array} \right. \quad \left\{ \begin{array}{l} \begin{bmatrix} \mathbf{v}_1 \\ \vdots \\ \mathbf{v}_n \end{bmatrix}^T = \begin{bmatrix} \tilde{\mathbf{v}}_1 \\ \vdots \\ \tilde{\mathbf{v}}_n \end{bmatrix}^T B = \begin{bmatrix} \tilde{\mathbf{v}}_1 \\ \vdots \\ \tilde{\mathbf{v}}_n \end{bmatrix}^T \tilde{V}^{-1} V \\ \begin{bmatrix} \tilde{\mathbf{v}}_1 \\ \vdots \\ \tilde{\mathbf{v}}_n \end{bmatrix}^T = \begin{bmatrix} \mathbf{v}_1 \\ \vdots \\ \mathbf{v}_n \end{bmatrix}^T F = \begin{bmatrix} \mathbf{v}_1 \\ \vdots \\ \mathbf{v}_n \end{bmatrix}^T V^{-1} \tilde{V} \end{array} \right. \quad \text{covariant} \end{array} \right.$$

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

$$\left\{ \begin{array}{l} \left\{ \begin{array}{l} v^i = F^i{}_j \tilde{v}^j = (V^{-1})^i{}_k \tilde{V}^k{}_j \tilde{v}^j \\ \tilde{v}^j = B^j{}_i v^i = (\tilde{V}^{-1})^j{}_k V^k{}_i v^i \end{array} \right. \quad \begin{array}{l} \begin{bmatrix} v^1 \\ \vdots \\ v^n \end{bmatrix} = \begin{bmatrix} \cdots & F^i{}_j & \cdots \end{bmatrix} \begin{bmatrix} \tilde{v}^1 \\ \vdots \\ \tilde{v}^n \end{bmatrix} = V^{-1} \tilde{V} \begin{bmatrix} \tilde{v}^1 \\ \vdots \\ \tilde{v}^n \end{bmatrix} \\ \begin{bmatrix} \tilde{v}^1 \\ \vdots \\ \tilde{v}^n \end{bmatrix} = \begin{bmatrix} \cdots & B^j{}_i & \cdots \end{bmatrix} \begin{bmatrix} v^1 \\ \vdots \\ v^n \end{bmatrix} = \tilde{V}^{-1} V \begin{bmatrix} v^1 \\ \vdots \\ v^n \end{bmatrix} \end{array} \quad \text{contravariant} \\ \left\{ \begin{array}{l} v_i = \tilde{v}_j B^j{}_i = \tilde{v}_j (\tilde{V}^k{}_j)^{-1} V^k{}_i \\ \tilde{v}_j = v_i F^i{}_j = v_i (V^k{}_i)^{-1} \tilde{V}^k{}_j \end{array} \right. \quad \begin{array}{l} \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix}^\top = \begin{bmatrix} \tilde{v}_1 \\ \vdots \\ \tilde{v}_n \end{bmatrix}^\top \begin{bmatrix} \cdots & B^j{}_i & \cdots \end{bmatrix} = \begin{bmatrix} \tilde{v}_1 \\ \vdots \\ \tilde{v}_n \end{bmatrix}^\top \tilde{V}^{-1} V \\ \begin{bmatrix} \tilde{v}_1 \\ \vdots \\ \tilde{v}_n \end{bmatrix}^\top = \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix}^\top \begin{bmatrix} \cdots & F^i{}_j & \cdots \end{bmatrix} = \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix}^\top V^{-1} \tilde{V} \end{array} \quad \text{covariant} \end{array} \right.$$

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

9.2 dual space

$$\begin{aligned} \left\{ \begin{array}{l} v \in \mathcal{V} \subseteq \mathbb{F}^n \in \{\mathbb{R}^n, \mathbb{C}^n, \dots\} \\ \exists! \omega \in \mathbb{F} [\omega(v) = \omega] \end{array} \right\} & \Leftrightarrow \mathcal{V} \xrightarrow{\omega} \mathbb{F} \Leftrightarrow \omega : \mathcal{V} \rightarrow \mathbb{F} \\ & \Leftrightarrow \mathbb{F}^{\mathcal{V}} = \{\omega | \omega : \mathcal{V} \rightarrow \mathbb{F}\} \\ & \Downarrow \\ & |\mathbb{F}^{\mathcal{V}}| = |\mathbb{F}|^{|\mathcal{V}|} \end{aligned}$$

$$\begin{array}{ccccccc} v^1(v_1) = 1 & \cdots & v^1(v_j) & & \cdots & v^1(v_n) & \\ \vdots & & \vdots & & & \vdots & \\ v^i(v_1) & \cdots & v^i(v_j) \stackrel{\text{def.}}{=} \begin{cases} 1 & j=i \\ 0 & j \neq i \end{cases} = \delta_j^i & \cdots & v^i(v_n) & & \\ \vdots & & \vdots & & \vdots & & \\ v^n(v_1) & \cdots & v^n(v_j) & & \cdots & v^n(v_n) = 1 & \end{array}$$

$$v^i(v) = v^i(v^j v_j) = v^j v^i(v_j) \stackrel{\text{def.}}{=} v^j \delta_j^i = v^i$$

$$\begin{aligned}
& \begin{cases} \omega \in \mathcal{V}^* = (\mathcal{V}^*, \mathbb{F}, +, \cdot) = (\mathcal{V}^*, \mathbb{F}, +_{\mathcal{V}^*, \mathbb{F}}, \cdot_{\mathbb{F} \times \mathcal{V}^*, \mathbb{F}}) \\ \mathbf{v} \in \mathcal{V} = (\mathcal{V}, \mathbb{F}, +, \cdot) = (\mathcal{V}, \mathbb{F}, +_{\mathcal{V}, \mathbb{F}}, \cdot_{\mathbb{F} \times \mathcal{V}, \mathbb{F}}) \end{cases} \\
& \omega(\mathbf{v}) = \omega(v^j \mathbf{v}_j) = v^j \omega(\mathbf{v}_j) \\
& = \omega\left(\sum_j v^j \mathbf{v}_j\right) = \sum_j \omega(v^j \mathbf{v}_j) = \sum_j v^j \omega(\mathbf{v}_j) \\
& = \begin{cases} \omega(v^1 \mathbf{v}_1 + \cdots + v^n \mathbf{v}_n) = \omega\left(\sum_{j=1}^n v^j \mathbf{v}_j\right) \\ \omega(\cdots + v^j \mathbf{v}_j + \cdots) = \omega\left(\sum_{j \in J} v^j \mathbf{v}_j\right) \end{cases} \quad + = +_{\mathcal{V}, \mathbb{F}} \\
& = \begin{cases} v^1 \omega(\mathbf{v}_1) + \cdots + v^n \omega(\mathbf{v}_n) = \sum_{j=1}^n v^j \omega(\mathbf{v}_j) \\ \cdots + v^j \omega(\mathbf{v}_j) + \cdots = \sum_{j \in J} v^j \omega(\mathbf{v}_j) \end{cases} \quad + = +_{\mathcal{V}^*, \mathbb{F}} \\
& = v^j \omega(\mathbf{v}_j) = \mathbf{v}^j(\mathbf{v}) \omega(\mathbf{v}_j) \quad v^j = \mathbf{v}^j(\mathbf{v}) \Leftarrow \mathbf{v}^i(\mathbf{v}) = v^i \Leftarrow \mathbf{v}^i(\mathbf{v}_j) \stackrel{\text{def.}}{=} \delta_j^i \\
& = \mathbf{v}^j(\mathbf{v}) \omega_j^{\mathbf{v}} = \omega_j^{\mathbf{v}} \mathbf{v}^j(\mathbf{v}) = \omega_i^{\mathbf{v}} \mathbf{v}^i(\mathbf{v}) \quad \omega_j^{\mathbf{v}} \stackrel{\text{def.}}{=} \omega(\mathbf{v}_j) \\
& \omega(\mathbf{v}) = \omega_i^{\mathbf{v}} \mathbf{v}^i(\mathbf{v}) \\
& \omega = \omega_i^{\mathbf{v}} \mathbf{v}^i
\end{aligned}$$

$$\begin{aligned}
\mathcal{V}^* \ni \omega = \omega_i \omega^i &= \sum_i \omega_i \omega^i = \begin{cases} \omega_1 \omega^1 + \cdots + \omega_n \omega^n &= \sum_{i=1}^n \omega_i \omega^i \\ \cdots + \omega_i \omega^i + \cdots &= \sum_{i \in I} \omega_i \omega^i \end{cases} \\
&= \omega_i^{\mathbf{v}} \mathbf{v}^i = \sum_i \omega_i^{\mathbf{v}} \mathbf{v}^i = \begin{cases} \omega_1^{\mathbf{v}} \mathbf{v}^1 + \cdots + \omega_n^{\mathbf{v}} \mathbf{v}^n &= \sum_{i=1}^n \omega_i^{\mathbf{v}} \mathbf{v}^i \\ \cdots + \omega_i^{\mathbf{v}} \mathbf{v}^i + \cdots &= \sum_{i \in I} \omega_i^{\mathbf{v}} \mathbf{v}^i \end{cases} \\
&= \begin{pmatrix} \omega_1^{\mathbf{v}} \begin{bmatrix} | \\ \mathbf{v}^1 \\ | \end{bmatrix}^\top + \cdots + \omega_n^{\mathbf{v}} \begin{bmatrix} | \\ \mathbf{v}^n \\ | \end{bmatrix}^\top \\ \cdots + \omega_i^{\mathbf{v}} \begin{bmatrix} | \\ \mathbf{v}^i \\ | \end{bmatrix}^\top + \cdots \end{pmatrix} = \begin{bmatrix} \omega_1^{\mathbf{v}} \\ \vdots \\ \omega_n^{\mathbf{v}} \\ \vdots \\ \omega_i^{\mathbf{v}} \\ \vdots \end{bmatrix}^\top \begin{bmatrix} - & \mathbf{v}^1 & - \\ & \vdots & \\ - & \mathbf{v}^n & - \\ & \vdots & \\ - & \mathbf{v}^i & - \\ & \vdots & \end{bmatrix} = \begin{bmatrix} \vdots \\ \omega_i^{\mathbf{v}} \\ \vdots \end{bmatrix}^\top \begin{bmatrix} \vdots \\ \mathbf{v}^i \\ \vdots \end{bmatrix} = [\omega]^{\mathbf{V}} V^* \\
&= \omega_i^{\tilde{\mathbf{v}}} \tilde{\mathbf{v}}^i = \sum_i \omega_i^{\tilde{\mathbf{v}}} \tilde{\mathbf{v}}^i = \begin{cases} \omega_1^{\tilde{\mathbf{v}}} \tilde{\mathbf{v}}^1 + \cdots + \omega_n^{\tilde{\mathbf{v}}} \tilde{\mathbf{v}}^n &= \sum_{i=1}^n \omega_i^{\tilde{\mathbf{v}}} \tilde{\mathbf{v}}^i \\ \cdots + \omega_i^{\tilde{\mathbf{v}}} \tilde{\mathbf{v}}^i + \cdots &= \sum_{i \in I} \omega_i^{\tilde{\mathbf{v}}} \tilde{\mathbf{v}}^i \end{cases} \\
&= \begin{pmatrix} \omega_1^{\tilde{\mathbf{v}}} \begin{bmatrix} | \\ \tilde{\mathbf{v}}^1 \\ | \end{bmatrix}^\top + \cdots + \omega_n^{\tilde{\mathbf{v}}} \begin{bmatrix} | \\ \tilde{\mathbf{v}}^n \\ | \end{bmatrix}^\top \\ \cdots + \omega_i^{\tilde{\mathbf{v}}} \begin{bmatrix} | \\ \tilde{\mathbf{v}}^i \\ | \end{bmatrix}^\top + \cdots \end{pmatrix} = \begin{bmatrix} \omega_1^{\tilde{\mathbf{v}}} \\ \vdots \\ \omega_n^{\tilde{\mathbf{v}}} \\ \vdots \\ \omega_i^{\tilde{\mathbf{v}}} \\ \vdots \end{bmatrix}^\top \begin{bmatrix} - & \tilde{\mathbf{v}}^1 & - \\ & \vdots & \\ - & \tilde{\mathbf{v}}^n & - \\ & \vdots & \\ - & \tilde{\mathbf{v}}^i & - \\ & \vdots & \end{bmatrix} = \begin{bmatrix} \vdots \\ \omega_i^{\tilde{\mathbf{v}}} \\ \vdots \end{bmatrix}^\top \begin{bmatrix} \vdots \\ \tilde{\mathbf{v}}^i \\ \vdots \end{bmatrix} = [\omega]^{\tilde{\mathbf{V}}} \tilde{V}^*
\end{aligned}$$

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

$$\left\{ \begin{array}{l} \left\{ \begin{array}{l} \omega_j^v = \omega_k^{\tilde{v}} B^k{}_j \\ \omega_j^{\tilde{v}} = \omega_i^v F^i{}_j \end{array} \right. \begin{array}{l} \begin{bmatrix} \vdots \\ \omega_i^v \\ \vdots \end{bmatrix}^\top = \begin{bmatrix} \vdots \\ \omega_i^{\tilde{v}} \\ \vdots \end{bmatrix}^\top B \\ \begin{bmatrix} \vdots \\ \omega_i^{\tilde{v}} \\ \vdots \end{bmatrix}^\top = \begin{bmatrix} \vdots \\ \omega_i^v \\ \vdots \end{bmatrix}^\top F \end{array} \right. \text{covariant} \\ \\ \left\{ \begin{array}{l} v^j = F^j{}_i \tilde{v}^i \\ \tilde{v}^j = B^k{}_i v^i \end{array} \right. \begin{array}{l} \begin{bmatrix} \vdots \\ v^i \\ \vdots \end{bmatrix} = F \begin{bmatrix} \vdots \\ \tilde{v}^i \\ \vdots \end{bmatrix} \\ \begin{bmatrix} \vdots \\ \tilde{v}^i \\ \vdots \end{bmatrix} = B \begin{bmatrix} \vdots \\ v^i \\ \vdots \end{bmatrix} \end{array} \right. \text{contravariant} \end{array} \right.$$

$$\left\{ \begin{array}{l} \left\{ \begin{array}{l} v^j = F^j{}_i \tilde{v}^i \\ \tilde{v}^j = B^k{}_i v^i \end{array} \right. \begin{array}{l} \begin{bmatrix} \vdots \\ v^i \\ \vdots \end{bmatrix} = F \begin{bmatrix} \vdots \\ \tilde{v}^i \\ \vdots \end{bmatrix} \\ \begin{bmatrix} \vdots \\ \tilde{v}^i \\ \vdots \end{bmatrix} = B \begin{bmatrix} \vdots \\ v^i \\ \vdots \end{bmatrix} \end{array} \right. \text{contravariant} \\ \\ \left\{ \begin{array}{l} \omega_j^v = \omega_k^{\tilde{v}} B^k{}_j \\ \omega_j^{\tilde{v}} = \omega_i^v F^i{}_j \end{array} \right. \begin{array}{l} \begin{bmatrix} \vdots \\ \omega_i^v \\ \vdots \end{bmatrix}^\top = \begin{bmatrix} \vdots \\ \omega_i^{\tilde{v}} \\ \vdots \end{bmatrix}^\top B \\ \begin{bmatrix} \vdots \\ \omega_i^{\tilde{v}} \\ \vdots \end{bmatrix}^\top = \begin{bmatrix} \vdots \\ \omega_i^v \\ \vdots \end{bmatrix}^\top F \end{array} \right. \text{covariant} \end{array} \right.$$

$$\begin{array}{ccc}
\text{covariant} & & \text{contravariant} \\
\left. \begin{array}{l} \tilde{\mathfrak{V}} \\ \mathfrak{V} \end{array} \right\} \ni \left\{ \begin{array}{l} \tilde{v}_j = v_i F^i_j \\ v_j = \tilde{v}_i B^i_j \end{array} \right. & \mathbb{F} \ni \left\{ \begin{array}{l} \tilde{v}^i = B^i_j v^j \\ v^i = F^i_j \tilde{v}^j \end{array} \right. & \text{vector space } \mathcal{V} \ni v = v_j v^j \\
\mathbb{F} \ni \left\{ \begin{array}{l} \omega_j^{\tilde{v}} = \omega_i^v F^i_j \\ \omega_j^v = \omega_k^{\tilde{v}} B^k_j \end{array} \right. & \left. \begin{array}{l} \tilde{\mathfrak{V}}^* \\ \mathfrak{V}^* \end{array} \right\} \ni \left\{ \begin{array}{l} \tilde{v}^i = B^i_j v^j \\ v^i = F^i_j \tilde{v}^j \end{array} \right. & \text{dual space } \mathcal{V}^* \ni \omega = \omega_i^v v^i
\end{array}$$

$$\tilde{v}_j \tilde{v}^j = v_i F^i_j B^j_k v^k = v_i \delta^i_k v^k = \begin{cases} v_k v^k & v_k = v_i \delta^i_k \\ v_i v^i & \delta^i_k v^k = v^i \end{cases} = v^j v_j$$

9.3 linear map transformation

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

$$w = L(v) = L(v^j v_j) = v^j L(v_j)$$

$$\begin{aligned}
L(v_1) &= v_1 L^1_1 + \dots + v_n L^n_1 = \begin{bmatrix} | \\ v_1 \\ | \end{bmatrix} L^1_1 + \dots + \begin{bmatrix} | \\ v_n \\ | \end{bmatrix} L^n_1 = \begin{bmatrix} | & \dots & | \\ v_1 & \dots & v_n \\ | & & | \end{bmatrix} \begin{bmatrix} L^1_1 \\ \vdots \\ L^n_1 \end{bmatrix} \\
&\vdots \\
L(v_j) &= v_1 L^1_j + \dots + v_n L^n_j = \begin{bmatrix} | \\ v_1 \\ | \end{bmatrix} L^1_j + \dots + \begin{bmatrix} | \\ v_n \\ | \end{bmatrix} L^n_j = \begin{bmatrix} | & \dots & | \\ v_1 & \dots & v_n \\ | & & | \end{bmatrix} \begin{bmatrix} L^1_j \\ \vdots \\ L^n_j \end{bmatrix} \\
&\vdots \\
L(v_n) &= v_1 L^1_n + \dots + v_n L^n_n = \begin{bmatrix} | \\ v_1 \\ | \end{bmatrix} L^1_n + \dots + \begin{bmatrix} | \\ v_n \\ | \end{bmatrix} L^n_n = \begin{bmatrix} | & \dots & | \\ v_1 & \dots & v_n \\ | & & | \end{bmatrix} \begin{bmatrix} L^1_n \\ \vdots \\ L^n_n \end{bmatrix}
\end{aligned}$$

$$\begin{aligned}
\begin{bmatrix} | & & | \\ L(v_1) & \dots & L(v_n) \\ | & & | \end{bmatrix} &= \begin{bmatrix} | & & | \\ v_1 & \dots & v_n \\ | & & | \end{bmatrix} \begin{bmatrix} L^1_1 & & L^1_n \\ \vdots & \dots & \vdots \\ L^n_1 & & L^n_n \end{bmatrix} \\
w = L(v) = v^j L(v_j) &= \begin{bmatrix} | & & | \\ L(v_1) & \dots & L(v_n) \\ | & & | \end{bmatrix} \begin{bmatrix} v^1 \\ \vdots \\ v^n \end{bmatrix} = \begin{bmatrix} | & & | \\ v_1 & \dots & v_n \\ | & & | \end{bmatrix} \begin{bmatrix} L^1_1 & & L^1_n \\ \vdots & \dots & \vdots \\ L^n_1 & & L^n_n \end{bmatrix} \begin{bmatrix} v^1 \\ \vdots \\ v^n \end{bmatrix} \\
&= \begin{bmatrix} \dots & | & \dots \\ \dots & L(v_n) & \dots \\ \dots & | & \dots \end{bmatrix} \begin{bmatrix} \vdots \\ v^j \\ \vdots \end{bmatrix} = \begin{bmatrix} \dots & | & \dots \\ \dots & v_i & \dots \\ \dots & | & \dots \end{bmatrix} \begin{bmatrix} \vdots \\ L^i_j & \dots \\ \vdots \end{bmatrix} \begin{bmatrix} \vdots \\ v^j \\ \vdots \end{bmatrix} \\
&= v_i w^i_v = v_i L^i_j v^j & w^i_v = L^i_j v^j \\
&= \tilde{v}_i w^i_{\tilde{v}} = \tilde{v}_i \tilde{L}^i_j \tilde{v}^j & w^i_{\tilde{v}} = \tilde{L}^i_j \tilde{v}^j \\
\tilde{v}_h B^h_i L^i_j F^j_k \tilde{v}^k &= v_i L^i_j v^j = \tilde{v}_i \tilde{L}^i_j \tilde{v}^j = v_h F^h_i \tilde{L}^i_j B^j_k v^k \\
\tilde{v}_h B^h_i L^i_j F^j_k \tilde{v}^k &= \tilde{v}_h \tilde{L}^h_k \tilde{v}^k & \tilde{L}^h_k = B^h_i L^i_j F^j_k \\
v_h F^h_i \tilde{L}^i_j B^j_k v^k &= v_h L^h_k v^k & L^h_k = F^h_i \tilde{L}^i_j B^j_k
\end{aligned}$$

covariant (0,1)-tensor $\left. \begin{array}{l} \tilde{\mathfrak{V}} \\ \mathfrak{V} \end{array} \right\} \ni \left\{ \begin{array}{l} \tilde{v}_j = v_i F^i_j \\ v_j = \tilde{v}_i B^i_j \end{array} \right.$ $\mathbb{F} \ni \left\{ \begin{array}{l} \omega_j^{\tilde{v}} = \omega_i^v F^i_j \\ \omega_j^v = \omega_k^{\tilde{v}} B^k_j \end{array} \right.$	contravariant (1,0)-tensor $\mathbb{F} \ni \left\{ \begin{array}{l} \tilde{v}^i = B^i_j v^j \\ v^i = F^i_j \tilde{v}^j \end{array} \right.$ $\left. \begin{array}{l} \tilde{\mathfrak{V}}^* \\ \mathfrak{V}^* \end{array} \right\} \ni \left\{ \begin{array}{l} \tilde{v}^i = B^i_j v^j \\ v^i = F^i_j \tilde{v}^j \end{array} \right.$	vector space $\mathcal{V} \ni v = v_j v^j$ dual space $\mathcal{V}^* \ni \omega = \omega_i^v v^i$ $\mathcal{V} \xrightarrow{L} \mathcal{W}$ $\left\{ \begin{array}{l} \tilde{L}^h_k = B^h_i L^i_j F^j_k \\ L^h_k = F^h_i \tilde{L}^i_j B^j_k \end{array} \right.$ vector space $\mathcal{W} \ni v = v_j v^j$
$(1,1)$ -tensor		

9.4 metric tensor

$$\begin{aligned}
 \|v\|^2 &= v \cdot v = (v_i v^i) \cdot (v_j v^j) = (v_i \cdot v_j) v^i v^j = g_{ij} v^i v^j = v^i (v_i \cdot v_j) v^j = v^i g_{ij} v^j \\
 &= (\tilde{v}_i \tilde{v}^i) \cdot (\tilde{v}_j \tilde{v}^j) = (\tilde{v}_i \cdot \tilde{v}_j) \tilde{v}^i \tilde{v}^j = \tilde{g}_{ij} \tilde{v}^i \tilde{v}^j = \tilde{v}^i (\tilde{v}_i \cdot \tilde{v}_j) \tilde{v}^j = \tilde{v}^i \tilde{g}_{ij} \tilde{v}^j \\
 &= g_{ij} v^i v^j = \tilde{g}_{ij} \tilde{v}^i \tilde{v}^j = \tilde{g}_{hk} B^h_i v^i B^k_j v^j = \tilde{g}_{hk} B^h_i B^k_j v^i v^j & g_{ij} &= \tilde{g}_{hk} B^h_i B^k_j \\
 &= \tilde{g}_{ij} \tilde{v}^i \tilde{v}^j = g_{ij} v^i v^j = g_{hk} F^h_i \tilde{v}^i F^k_j \tilde{v}^j = g_{hk} F^h_i F^k_j \tilde{v}^i \tilde{v}^j & \tilde{g}_{ij} &= g_{hk} F^h_i F^k_j
 \end{aligned}$$

covariant (0,1)-tensor $\left. \begin{array}{l} \tilde{\mathfrak{V}} \\ \mathfrak{V} \end{array} \right\} \ni \left\{ \begin{array}{l} \tilde{v}_j = v_i F^i_j \\ v_j = \tilde{v}_i B^i_j \end{array} \right.$ $\mathbb{F} \ni \left\{ \begin{array}{l} \omega_j^{\tilde{v}} = \omega_i^v F^i_j \\ \omega_j^v = \omega_k^{\tilde{v}} B^k_j \end{array} \right.$	contravariant (1,0)-tensor $\mathbb{F} \ni \left\{ \begin{array}{l} \tilde{v}^i = B^i_j v^j \\ v^i = F^i_j \tilde{v}^j \end{array} \right.$ $\left. \begin{array}{l} \tilde{\mathfrak{V}}^* \\ \mathfrak{V}^* \end{array} \right\} \ni \left\{ \begin{array}{l} \tilde{v}^i = B^i_j v^j \\ v^i = F^i_j \tilde{v}^j \end{array} \right.$	vector space $\mathcal{V} \ni v = v_j v^j$ dual space $\mathcal{V}^* \ni \omega = \omega_i^v v^i$ $\mathcal{V} \xrightarrow{L} \mathcal{W}$ $\left\{ \begin{array}{l} \tilde{L}^h_k = B^h_i L^i_j F^j_k \\ L^h_k = F^h_i \tilde{L}^i_j B^j_k \end{array} \right.$ vector space $\mathcal{W} \ni v = v_j v^j$
$(1,1)$ -tensor		

$(0,2)$ -tensor $\mathbb{R}_{\geq 0}^{\mathcal{V}^2} \ni \left\{ \begin{array}{l} \tilde{g}_{ij} = g_{hk} F^h_i F^k_j \\ g_{ij} = \tilde{g}_{hk} B^h_i B^k_j \end{array} \right.$	$\mathcal{V}^2 \xrightarrow{g} \mathbb{R}_{\geq 0}$ metric space $\mathcal{V} \times \mathcal{V} \xrightarrow{g} \mathbb{F}$
--	---

$$\begin{aligned}
 u \cdot v &= (u_i u^i) \cdot (v_j v^j) = (u_i \cdot v_j) u^i v^j = g_{ij} u^i v^j = u^i (u_i \cdot v_j) v^j = u^i g_{ij} v^j \\
 &= (\tilde{u}_i \tilde{u}^i) \cdot (\tilde{v}_j \tilde{v}^j) = (\tilde{u}_i \cdot \tilde{v}_j) \tilde{u}^i \tilde{v}^j = \tilde{g}_{ij} \tilde{u}^i \tilde{v}^j = \tilde{u}^i (\tilde{u}_i \cdot \tilde{v}_j) \tilde{v}^j = \tilde{u}^i \tilde{g}_{ij} \tilde{v}^j
 \end{aligned}$$

9.5 bilinear form

10 tensor calculus

11 spinor

Part III

relativity