§6 Groups of low order and Klein's Four-Group

- $|G| = 1$. $G = \{e\}$.

- $|G| = 2$, $G = \{e, a\}$, $a \neq e$. $a^2 = e$.
  $= \langle a \rangle$
  $G = \mathbb{Z}_2$.

- $|G| = 3$, $G = \mathbb{Z}_3$.

- $|G| = 4$. $G = \{e, a, b, c\}$

  - If $o(a) = 4$, $\langle a \rangle = \{e, a, a^2, a^3\} \leq G \Rightarrow G = \langle a \rangle$.
    $\mathbb{Z}_4$.

  - $a^2 = b^2 = c^2 = e$.

    $\boxed{ab = a} \Rightarrow b = e$. ✗

    $ab = b \Rightarrow a = e$ ✗

    $ab = c$

    $ac = b$

    $bc = a$

    $\{e, a, b, ab\}$, $a^2 = b^2 = e$. $ab = ba$.

Klein four-group V_4 or K_4

(Vierergruppe)

Thm 6.1. Every group of order 4 is either $\mathbb{Z}_4$, or the V_4.

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

$V_4 = \{e, a, b, ab\}$

$a^2 = b^2 = e, \; ab = ba$

- V_4 is abelian.
- V_4 is smallest (order) non-cyclic group.
- all elements different from e have order 2.

※ • V_4 can be seen as a subgroup of S_4

$$\left\{ e, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \right\}.$$

$= \{e, (12), (34), (12)(34)\} \leq S_4$

Example 6.1

$e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ $a = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, $b = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$

$c = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$

Exercise

Example 6.2 $V_4 = \{e, a, b, ab\}$.

$H = \{e, a\}$. $Ha = \{e, a\} = H$

$Hb = \{b, ab\}$, $Hab = \{b, ab\}$

§7. Direct product

$A \times B = \{(a,b) : a \in A, b \in B\}$

Def 7.1 Let G_1 and G_2 be two groups. Then $G = G_1 \times G_2$ is a group, with the multiplication law

$$(g_1, g_2)(g_1', g_2') = (g_1 g_1', g_2 g_2').$$

$G_1 \times G_2$ is called the direct product of G_1 and G_2.

$$G_1 \times \{e_2\} \leq G_1 \times G_2$$

Exercise: prove: $G_1 \times \{e_2\} \cong G_1$

- G_1 and G_2 are abelian, then $G_1 \times G_2$ is abelian.

$$\begin{aligned}(g_1, g_2)(g_1', g_2') &= (g_1 g_1', g_2 g_2') \\ &= (g_1' g_1, g_2' g_2) \\ &= (g_1', g_2')(g_1, g_2).\end{aligned}$$

- $|G_1 \times G_2| = |G_1||G_2|$

$\mathbb{Z}_2 = \{e, a\}$.

$G_1 = G_2 = \mathbb{Z}_2$.

$$\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(e,e), (e,a), (a,e), (a,a)\}.$$

$$(e,a)^2 = (e,a)(e,a) = (e, a^2) = (e,e).$$

$\mathbb{Z}_2 \times \mathbb{Z}_2 \cong V_4$.

$G_1 \times G_2$

Lem 7.1. All groups of even order contain at least one-identity element whose order is two.

Pf. $|G| = 2n$, but has no element whose order is two.

$G = \{e, g_1, g_2, \cdots, g_{2n-1}\}$.

g_1, g_k .

Thm 7.1. A group of order 6 is either $\mathbb{Z}_6$ or S_3.

Pf. $|G| = 6$. $1, 2, 3, 6$.

$\exists\, a,\ o(a) = 6. \Rightarrow G = \langle a \rangle. \Rightarrow G = \mathbb{Z}_6$.

$\exists\, a \in G,\ o(a) = 2. \quad o(b) = 2$.

$ab = (ab)^{-1} = b^{-1}a^{-1} = ba \Rightarrow V_4 \leq G$. $\times$

$o(a) = 3, \quad o(b) = 2$.

$\{e, a, a^2, b \ldots\}$.

$(a, b) \in G_1 \times G_2$

$(a, b)^n$

$ab = ba^2$ $\quad ab = ba$ $\quad (ab)^n = a^n b^n = e$

$n = 6$

$a^3 = e, \quad b^2 = e, \quad ab = ba^2 \Rightarrow S_3$

$a = (123)$ $\quad b = (12)$

- $|G| = 1, 2, 3, 4, 5, 6, 7, 8, 9, \ldots$

4: $\mathbb{Z}_4 \quad V_4$ $\quad 6$: $\mathbb{Z}_6 \quad S_3$ $\quad 8$: $\mathbb{Z}_8$

- $\mathbb{Z}_2 \times \mathbb{Z}_2 \cong V_4$. $\quad \not\cong \mathbb{Z}_4$

- $\mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$

Thm 7.2. $\mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}$ if and only if $(p, q) = 1$.

Pf $\quad \Leftarrow$

$\mathbb{Z}_p = \langle a \rangle, \quad \mathbb{Z}_q = \langle b \rangle, \quad a^p = e, \quad b^q = e.$

$(a, b) \in \mathbb{Z}_p \times \mathbb{Z}_q$

$(a,b)^n = (e,e)$.

(a,b)

$\Rightarrow \quad (a^n, b^n) = (e, e)$

$\Rightarrow \quad a^n = e, \quad b^n = e$

$\Rightarrow \quad n = kp, \quad n = lq \quad \Rightarrow \quad kp = lq \quad \Rightarrow \quad k = q, \quad l = p.$

$\Rightarrow \quad n = pq$

$o((a,b)) = pq$

$\mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}$.

" $\Rightarrow$ " $\quad p, q$ are not relatively prime, $\mathbb{Z}_p \times \mathbb{Z}_q \ncong \mathbb{Z}_{pq}$.

$(u, v) \in \mathbb{Z}_p \times \mathbb{Z}_q$

$(u,v)^n = (e,e)$

$\Rightarrow \quad n = kp = lq \quad \Rightarrow \quad \frac{k}{l} = \frac{q}{p} = \frac{q'}{p'} \qquad p = sp', \quad q = sq'$

$\Rightarrow \quad k = q', \quad l = p' \qquad \frac{q'p < pq}{p'q}$

$\mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}$

Exercise. If G is abelian, $o(a)=m$, $o(b)=n$. prove

$$o(ab) = \frac{mn}{(m,n)}.$$