1. (1) $(ab)c = a(bc)$.

(2) $\exists e$, s.t. $ea = a$, $\forall a \in G$.

(3) $\forall x \in G$, $\exists y \in G$, s.t. $yx = e$.

$\Rightarrow$ G is a group.

pf. (3). $\forall x \in G$, $\exists y \in G$, s.t. $yx = e$.

($\Rightarrow$ $xy = e$)

By (3), we know that $\exists z \in G$, $zy = e$. Then

$$xy = e(xy) = (zy)(xy) = z(yx)y = zey = zy = e.$$

(2). $\forall x \in G$, $ex = x$

($\Rightarrow$ $xe = x$)

$\exists y \in G$, $xy = yx = e$.

$$xe = x(yx) = (xy)x = ex = x.$$ ✓

2. ($xy = xz \Rightarrow y = z$)

$G = \{g_1, \cdots, g_n\}$.

$\forall a \in G$, we define

$$aG = \{ag_1, \cdots, ag_n\} = G, \quad Ga = \{g_1 a, \cdots, g_n a\} = G.$$

$\exists g_k \in G$, s.t. $g_k a = a$. $\Rightarrow g_k = e$

$\forall g \in G$, $\exists g_l \in G$ s.t. $g = ag_l$.

$$g_k g = g_k (a g_l) = (g_k a) g_l = a g_l = g.$$

$\Rightarrow$ g_k is left identity. $g_k = e$.

$\boxed{\forall g \in G, \exists h \text{ s.t. } hg = e.}$

$\forall g \in G$, $Gg \overset{d}{=} G \Rightarrow \exists h \in G$, s.t.

$hg = e$.

$\Rightarrow$ G is a group.

§5 Cosets and Lagrange's Theorem

- $a \sim b \Leftrightarrow ab^{-1} \in H$, where $H \leq G$.

  equivalence relation.

  $a \sim a$. $a \cdot a^{-1} = e \in H$. (Reflexive).

  $a \sim b \Rightarrow b \sim a$. $\boxed{ab^{-1} \in H \Rightarrow ba^{-1} \in H}$

  $\exists\, h \in H$, s.t. $ab^{-1} = h \Rightarrow a = hb \Rightarrow e = hba^{-1}$

  $ba^{-1} = h^{-1} \in H$. $\Rightarrow b \sim a$. (Symmetric)

  $a \sim b$, $b \sim c \Rightarrow a \sim c$

  $ab^{-1} \in H$, $bc^{-1} \in H$ $(\Rightarrow ac^{-1} \in H)$.

  $ab^{-1}bc^{-1} = ac^{-1} \in H$.

  equivalence class $\boxed{[a] = \{b \in G : a \sim b\}}$.

  $a \sim b \Rightarrow [a] = [b]$.

  $c \sim a$, $c \sim b \Rightarrow [a] = [c] = [b]$.

Define. $Ha = \{ha : \forall h \in H\}$.

Thm. $[a] = Ha$.

Pf. $[a] \subseteq Ha$, $Ha \subseteq [a]$

$\forall\, c \in [a]$, $a \sim c$.

$\Rightarrow ac^{-1} \in H \Rightarrow \exists\, h \in H$, s.t. $ac^{-1} = h$.

$\Rightarrow c = h^{-1}a \in Ha \Rightarrow [a] \subseteq Ha$.

$\forall\, c \in Ha$, $\exists\, h \in H$, s.t. $c = ha \Rightarrow ca^{-1} = h \in H$

$\Rightarrow c \sim a \Rightarrow a \sim c \Rightarrow c \in [a] \Rightarrow Ha \subseteq [a]$

$\Rightarrow Ha = [a]$.

Def 5.1 The set of equivalence class $\{Ha : a \in G\}$ is the set of right cosets of G with respect to H, $H \leq G$.

- left coset $aH = [a]$, $a \sim b \Leftrightarrow a^{-1}b \in H$

exercise

Def 5.2 left cosets

Thm 5.1 Two right cosets of G with respect to H are either disjoint or identical.

pf. Let $a, b \in G$, $Ha \cap Hb = \emptyset$. ∨.

$Ha \cap Hb \neq \emptyset \Rightarrow Ha = Hb$.

$\exists\, c \in Ha \cap Hb \Rightarrow c \in [a] \cap [b]$

$\Rightarrow c \sim a,\ c \sim b \Rightarrow a \sim b. \Rightarrow [a] = [b].$

$\Rightarrow Ha = Hb.$

Thm 5.2 All rights cosets of G with respect to H have the same number of elements.

pf. $|H| = |Ha|$, $\forall a \in G$.

$M: H \to Ha$

$h \mapsto ha$

injective: $M(h_1) = M(h_2) \Rightarrow h_1 = h_2$

$h_1 a = h_2 a \Rightarrow h_1 = h_2$.

surjective: $\forall\, y \in Ha,\ \exists\, h$ s.t. $M(h) = y$.

$y = Hha$

Def 5.3 The number of cosets of G with respect to H is called index of H into G. $i(H, G)$ or $[G : H]$

Thm 5.3 (Lagrange's thm) Let H be subgroup of G. The order of H divides the order of G. i.e. $|G| = |H| \, i(H, G)$.

pf. $G = \bigcup_{a \in G} Ha = \bigcup_{i=1}^{i(H,G)} Ha_i$, a_i

$\Rightarrow |G| = i(H, G) |H|$.

$Ha = \{ha : h \in H\} \subseteq G$.

Def 5.4 A proper subgroup of a group G is a subgroup $H \leq G$ that is different from $\{e\}$ and from itself, G.

Cor 5.0.1 If $|G|$ is prime, then the group G has no proper subgroup.

$\mathbb{Z}_2$, $\mathbb{Z}_3$ $\mathbb{Z}_5$

Cor 5.0.2 Let $a \in G$, and let $k = o(a)$. The $k \mid |G|$.

pf. $|\langle a\rangle| = k$.

$\langle a\rangle \le G$

Lagrange's $\Rightarrow$ $k \mid |G|$.

Cor 5.1.3 If $|G|$ is prime, then G is a cyclic group.

pf. $\forall\, a \neq e$, $\langle a\rangle \le G$.

$\langle a\rangle = G$. ✓

$\mathbb{Z}_p$, p is prime C_p

$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$

Example 1.

$S_3 = \{e, (123), (132), (12), (13), (23)\}$.

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

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

$He = H$, $Ha = H$, $Ha^2 = H$

$Hb = \{b, ab, a^2b\}$ $Hab = \{ab, a^2b, b\}$.

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

- $H = \{e, b\}$.

$ba = a^2b \Rightarrow ba^2 = ab$.

$He = H$, $Ha = \{a, a^2b\}$, $Ha^2 = \{a^2, ab\}$

$Hb = H$, $Hab = \{ab, a^2\}$, $Ha^2b = \{a^2b, a\}$

$bab = a^2$ $ba^2b = a$

$ba = a^2b$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 5 & 2 & 6 & 3 \end{pmatrix}$$

$= (24)(356)$

习题.

1. $G = S_3 = \{e, a, a^2, b, ab, a^2b\}$.

① $H = \{e, a, a^2\}$ ② $H = \{e, b\}$.

left cosets.

2. 初始时 Z_6 中 [0], [1], [2], [3], [4], [5] 的阶分别是 1, 6, 3, 2, 3, 6.