

# HW #11. Solution.

§9.4 #42. Show:  $gHg^{-1} < G$ .

i) Since  $H < G$ ,  $1g \in H \Rightarrow 1g = g1g^{-1} \in gHg^{-1}$ .

ii) assume  $a, b \in gHg^{-1}$  i.e.  $\exists h_1, h_2 \in H \Rightarrow$

$$a = gh_1g^{-1}, \quad b = gh_2g^{-1}.$$

$$\text{then } ab = (gh_1g^{-1})(gh_2g^{-1}) = gh_1(g^{-1}g)h_2g^{-1} = gh_1h_2g^{-1}$$

$$= gh_1h_2g^{-1} \in gHg^{-1}$$

( $\because$  Since  $H < G$ ,  $h_1h_2 \in H$ .)

iii)  $a \in gHg^{-1}$  i.e.  $\exists h \in H \Rightarrow ghg^{-1} = a$ .

$$\text{then } a^{-1} = (ghg^{-1})^{-1} = gh^{-1}g^{-1} \in gHg^{-1}$$

( $\because$  Since  $H < G$ ,  $h^{-1} \in H$ )

by i), ii), iii),  $gHg^{-1} < G$ .

Show:  $H \cong gHg^{-1}$ .

Define  $\varphi: H \rightarrow gHg^{-1}$  given by  $\varphi(h) = ghg^{-1}$

$$\text{then } \varphi(h) = \varphi(h') \Rightarrow ghg^{-1} = gh'g^{-1}$$

$$\Rightarrow g^{-1}(ghg^{-1})g = g^{-1}(gh'g^{-1})g$$

$$\Rightarrow h = h' \quad \therefore \varphi \text{ is 1-1.}$$

$$\forall a \in gHg^{-1} \text{ i.e. } \exists h \in H \Rightarrow a = ghg^{-1}, \quad \varphi(ghg^{-1}) = a.$$

$\therefore \varphi$  is onto.

$$\varphi(h_1, h_2) = gh_1h_2g^{-1} = gh_1g^{-1}gh_2g^{-1} = \varphi(h_1)\varphi(h_2).$$

$\therefore \varphi$  is homo.

$$\therefore \exists \varphi: \text{iso.} \quad \therefore H \cong gHg^{-1}.$$

§9.6 #2.

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$$p_0 = \text{Id}$$

$$p_1 = (0 \ 1 \ 2)$$

$$p_2 = (0 \ 2 \ 1)$$

§10.1 #6.  $H = \langle (1 \ 2 \ 3) \rangle = \{(1 \ 2 \ 3), (1 \ 3 \ 2), (1)\}$   
 $(1 \ 2)H = \{(2 \ 3), (1 \ 3), (1 \ 2)\}$ .

$H$ : normal subgp.

$$G/H \cong \mathbb{Z}_2 \quad (\because |G/H| = 2 \text{ \& we know } \nexists! \text{ subgp } \mathbb{Z}_2 \text{ having order } 2)$$

§9.5 #8  $GF(2, x^2+x+1) = \{0, 1, \alpha, \alpha+1\}$ .

+	0	1	$\alpha$	$\alpha+1$
0	0	1	$\alpha$	$\alpha+1$
1	1	0	$\alpha+1$	$\alpha$
$\alpha$	$\alpha$	$\alpha+1$	0	1
$\alpha+1$	$\alpha+1$	$\alpha$	1	0

$\cong K$

$\uparrow$  every non identity elements of  $GF(2, (x^2+x+1), +)$  has order 2.

#25 ( $\Leftarrow$ )  $G \cong \mathbb{Z}_p$  for some prime  $p$ .

then  $|G| = |\mathbb{Z}_p| = p$

$\therefore$  by Lagrange,  $\forall H < G, |H| = 1$  or  $p$ .

i.e.  $H = \{id\}$  or  $H = G$ .

$\therefore \exists$  exactly 2 subgps of  $G$ .

( $\Rightarrow$ ) Suppose  $G$  has exactly 2 subgps but

$G \cong \mathbb{Z}_n$  where  $n$  is not prime.

i)  $n=1$ . by #24,  $G \cong \mathbb{Z}_1$   $G$  has only one subgp.

contradiction!

ii)  $n > 1$  Since  $n$  is not a prime,  $\exists a \in G \Rightarrow$

$m = |a| < n$

then  $\{1, a, \dots, a^{m-1}\} \subsetneq G$ .

$\therefore \exists$  at least 3 subgps of  $G$ .

contradiction!