Homework 5

Due date: 2019. 4. 24.

1. Prove that $Aut(\mathbb{Z}_6) \approx Aut(\mathbb{Z})$.

2. The group $\left\{ \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \middle| a \in \mathbb{Z} \right\}$ is isomorphic to what familiar group?

3. Let $M = \left\{ \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \middle| a,b \in \mathbb{R} \right\}$. Prove that $\mathbb{C}$ and M are isomorphic under addition.

4. Prove that $\mathbb{Z} \not\approx \mathbb{Q}$.

5. Show that if H is a subgroup of index 2 in a finite group G, that every left coset of H is also every right coset of H.

6. Find all left cosets of the subgroup $< 4 >$ of $\mathbb{Z}_{12}$.

7. Let G be a group with $|G| = pq$, where p and q are prime. Prove that every proper subgroup of G is cyclic.

8. Compute 5^{2019} mod 7.

9. Let H and K be subgroups of a finite group G with $H \subseteq K \subseteq G$. Prove that $|G:H| = |G:K||K:H|$.

10. Show that $\mathbb{Q}$ has no proper subgroup of finite index.

현대대수 I – HW5

파이낸스경영학과
2017004093
양 준 우

1. $Aut(\mathbb{Z}_6) \approx Aut(\mathbb{Z})$.

i) $Aut(\mathbb{Z}_6) \approx \mathbb{Z}_2$

$\alpha : \mathbb{Z}_6 \to \mathbb{Z}_6$.

$\alpha(k) = \alpha(1+1+\cdots+k) = k\alpha(1)$

Since $|1| = 6$, $|\alpha(1)| = 6$.

$U(6) = 1, 5$. $\therefore \alpha(1) = 1$ or 5.

$\alpha_1(k) = k$, $\alpha_2(k) = 5k$.

$\alpha_1 \cdot \alpha_2(k) = \alpha_1(5k) = 5k = \alpha_2(k)$

$\alpha_2 \cdot \alpha_2(k) = \alpha_2(5k) = k \pmod 6 = \alpha_1(k)$.

$\alpha_2^3(k) = \alpha_2(k)$.

$\therefore \langle \alpha_2 \rangle = Aut(\mathbb{Z}_6)$: cyclic $\therefore Aut(\mathbb{Z}_6) \approx \mathbb{Z}_2$.

ii) $Aut(\mathbb{Z}) \approx \mathbb{Z}_2$.

$\phi : \mathbb{Z} \to \mathbb{Z}$

$\phi(k) = \phi(1+1+\cdots+1) = k \cdot \phi(1)$.

$\phi(1) = \pm 1 \to$ automorphism. trivial.

$\phi(1) \neq \pm 1 \to \phi(k) = mk$ $(m \neq \pm 1)$.

for some $z \in \mathbb{Z}$, $\phi(k) = mk = z$.

then $k = \frac{z}{m}$.

There exist k s.t $\frac{k}{m} \notin \mathbb{Z}$ $\therefore$ not onto.

$\therefore Aut(\mathbb{Z}) = \{\phi_1(k) = k, \phi_2(k) = -k \mid k \in \mathbb{Z}\}$.

$\phi_1 \circ \phi_2 = \phi_2$, $\phi_2 \cdot \phi_2 = \phi_1$, $\phi_2^3 = \phi_2$

$\langle \phi_2 \rangle = Aut(\mathbb{Z})$: cyclic $\therefore Aut(\mathbb{Z}) \approx \mathbb{Z}_2$

$\therefore Aut(\mathbb{Z}_6) \approx A(\mathbb{Z})$.

2. $\phi\left(\begin{bmatrix}1 & a\\ 0 & 1\end{bmatrix}\right) = \begin{bmatrix}1 & a\\ 0 & 1\end{bmatrix}\begin{bmatrix}1-a^2 & -a\\ a & 1\end{bmatrix} = \begin{bmatrix}1 & 0\\ a & 1\end{bmatrix}$

$M = \left\{\begin{bmatrix}1 & 0\\ a & 1\end{bmatrix} \mid a \in \mathbb{Z}\right\}$

homo) $\phi\left(\begin{bmatrix}1 & x\\ 0 & 1\end{bmatrix}\begin{bmatrix}1 & y\\ 0 & 1\end{bmatrix}\right) = \phi\left(\begin{bmatrix}1 & x+y\\ 0 & 1\end{bmatrix}\right) = \begin{bmatrix}1 & 0\\ x+y & 1\end{bmatrix}$
$= \begin{bmatrix}1 & 0\\ x & 1\end{bmatrix}\begin{bmatrix}1 & 0\\ y & 1\end{bmatrix} = \phi\left(\begin{bmatrix}1 & x\\ 0 & 1\end{bmatrix}\right)\cdot\phi\left(\begin{bmatrix}1 & y\\ 0 & 1\end{bmatrix}\right)$

1-1) $\phi\left(\begin{bmatrix}1 & x\\ 0 & 1\end{bmatrix}\right) = \phi\left(\begin{bmatrix}1 & y\\ 0 & 1\end{bmatrix}\right) \Rightarrow \begin{bmatrix}1 & 0\\ x & 1\end{bmatrix} = \begin{bmatrix}1 & 0\\ y & 1\end{bmatrix}$
$\Rightarrow x = y$

onto) $\begin{bmatrix}1 & 0\\ r & 1\end{bmatrix} \in M$, $\phi\left(\begin{bmatrix}1 & r\\ 0 & 1\end{bmatrix}\right) = \begin{bmatrix}1 & 0\\ r & 1\end{bmatrix}$

$\therefore \left\{\begin{bmatrix}1 & a\\ 0 & 1\end{bmatrix} \mid a \in \mathbb{Z}\right\} \approx \left\{\begin{bmatrix}1 & 0\\ a & 1\end{bmatrix} \mid a \in \mathbb{Z}\right\}$

3. $M = \left\{\begin{bmatrix}a & -b\\ b & a\end{bmatrix} \mid a, b \in \mathbb{R}\right\} \approx \mathbb{C} = a+bi$
$\phi : \mathbb{C} \to M \quad (a+bi) \mapsto \begin{bmatrix}a & -b\\ b & a\end{bmatrix}$

i) homo
$a, b, c, d \in \mathbb{R}$, $a+bi, c+di \in \mathbb{C}$
$\phi((a+bi)+(c+di)) = \phi((a+c)+(b+d)i)$
$= \begin{bmatrix}a+c & -(b+d)\\ b+d & a+c\end{bmatrix} = \begin{bmatrix}a & -b\\ b & a\end{bmatrix} + \begin{bmatrix}c & -d\\ d & c\end{bmatrix}$

$= \phi(a+bi) + \phi(c+di)$ $\therefore$ homomorphism.

ii) 1-1
$\phi(a+bi) = \phi(c+di) \Rightarrow \begin{bmatrix}a & -b\\ b & a\end{bmatrix} = \begin{bmatrix}c & -d\\ d & c\end{bmatrix}$
$\Rightarrow a = c, b = d$ $\therefore (a+bi) = (c+di)$

iii) onto
$\forall \begin{bmatrix}x & -y\\ y & x\end{bmatrix} \in M$, $\phi(x+yi) = \begin{bmatrix}x & -y\\ y & x\end{bmatrix}$ $\therefore$ onto.

$\therefore$ $\mathbb{C}$ and M are isomorphic under addition.

4. $\mathbb{Z} \ncong \mathbb{Q}$.

$\phi : \mathbb{Q} \to \mathbb{Z}$ isomorphic. $\phi(1) = n$.

$\phi(1) = \phi\left(\frac{1}{n+1} + \frac{1}{n+1} + \cdots + \frac{1}{n+1}\right) = (n+1)\cdot\phi\left(\frac{1}{n+1}\right) = n$

$\phi\left(\frac{1}{n+1}\right) = \frac{n}{n+1} \in \mathbb{Z}$.

$\therefore$ candidates for n : $0, -2$.

(if $n \neq 0, -2$, $\frac{n}{n+1} \notin \mathbb{Z} \Rightarrow \nexists \phi$)

i) $n = 0$. $\phi(1) = 0$.

$\phi(2) = \phi(1+1) = \phi(1) + \phi(1) = 0$. $\therefore$ not 1-1 ($\lightning$).

ii) $n = -2$ $\phi(1) = -2$

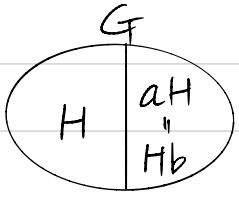
$\phi(1) = \phi\left(\frac{1}{4}+\frac{1}{4}+\frac{1}{4}+\frac{1}{4}\right) = 4\cdot\phi\left(\frac{1}{4}\right) = -2$

$\therefore \phi\left(\frac{1}{4}\right) = -\frac{1}{2} \in \mathbb{Z}$ ($\lightning$).

$\therefore$ There no exist a map ϕ which is isomorphism of a group $\mathbb{Q}$ into $\mathbb{Z}$

5. G : group of order $2n$.

H : subgroup of order n. ($|G:H| = 2$).



$\forall a, b \in G$, $h \in H$,

Every left (right) coset are same or disjoint.

($aH = bH$ or $aH \cap bH = \phi$).

Also $\bigcup aH = G$ for $\forall a \in G$, $|H| = |aH|$.

$|G:H| = |G| / |H|$.

In this case, $|G:H| = 2$, $H \cup aH = G$.

If $a, b \in H$, $aH = H = Hb$. (satisfies). ($\because H < G$).

If $a, b \notin H$, $\forall ah \in aH \cap H = \phi$ & $aH \cup H = G$.

$\therefore aH = Ha = bH = Hb$.

6. $\mathbb{Z}_{12} = \{0, 1, 2, \cdots, 11\}$. $\langle 4 \rangle = \{0, 4, 8\}$.

$0\langle 4 \rangle = \{0, 4, 8\} = 4\cdot\langle 4 \rangle = 8\langle 4 \rangle$

$1\cdot\langle 4 \rangle = \{1, 5, 9\} = 5\cdot\langle 4 \rangle = 9\langle 4 \rangle$

$2\cdot\langle 4 \rangle = \{2, 6, 10\} = 6\cdot\langle 4 \rangle = 10\langle 4 \rangle$

$3\cdot\langle 4 \rangle = \{3, 7, 11\} = 7\cdot\langle 4 \rangle = 11\langle 4 \rangle$

$\{0, 4, 8\} \cup \{1, 5, 9\} \cup \{2, 6, 10\} \cup \{3, 7, 11\} = \mathbb{Z}_{12}$

7. $|G| = pq$ p, q : prime. $H \leq G$.

By Lagrange's thm, $|H| \mid |G|$

$\therefore$ candidates for $|H|$: $1, p, q, pq$.

Every proper subgroup has order 1 or p or q

i) $|H| = 1 \Rightarrow H = \{e\}$: cyclic

ii) $|H| = p$ or q. H has order of prime.

$\forall h \in H \setminus \{e\}$, $|h| = |\langle h \rangle| = |H|$

$\therefore H$ is cyclic group.

$\therefore$ Every proper subgroup of G is cyclic.

8. $5^{2019} \mod 7$.

$5^{2019} = 5^{6\times 336 + 3}$

By Fermat's little thm, $a^p \equiv a \pmod p$.

and $a^{p-1} \equiv 1 \pmod p$ (a : integer, p : prime).

$\therefore 5^6 = 1 \pmod 7$.

$5^{6\times 336+3} = (5^6)^{336} \times 5^3 \equiv 5^3 = 125 \equiv 6 \pmod 7$.

9. $H \le G$, $K \le G$, $H \subseteq K \subseteq G$. $\Rightarrow H \le K \le G$.

$|G:H| = |G:K||K:H|$.

$|H| \mid |G|$, $|K| \mid |G|$.

$|G:H| = \frac{|G|}{|H|}$, $|G:K| = \frac{|G|}{|K|}$, $|K:H| = \frac{|K|}{|H|}$

$\therefore |G:K||K:H| = \frac{|G|}{|K|} \cdot \frac{|K|}{|H|} = \frac{|G|}{|H|} = |G:H|$

10. If there is a finite index $|\mathbb{Q}:H| = n$.

$\mathbb{Q} = (q_1+H) \cup (q_2+H) \cup \cdots \cup (q_n+H)$.

Claim $\forall q \in \mathbb{Q}$, $\exists m \in \{1, 2, \cdots, n\}$ s.t. $mq \in H$.

pf claim) consider $q, 2q, 3q, \cdots, (n+1)q$.

There are at least two aq, bq in same coset.

$aq, bq \in q_k + H$ $(a > b,\ 1 \le k \le n)$

$aq = q_k + h_1$ $\quad aq - bq = \underbrace{(a-b)}_{m} q = h_1 - h_2 \in H$.

$bq = q_k + h_2$

$\therefore \forall q \in \mathbb{Q}$, $mq \in H$ for some m.

$\Rightarrow \forall q \in \mathbb{Q}$, $n!\, q \in H$

$\forall q \in \mathbb{Q}$, $n!\left(\frac{q}{n!}\right) \in H$

Thus $\mathbb{Q} \subseteq H$,

$\therefore \mathbb{Q}$ has no proper subgroup of finite index.