20181288 윤성호 추상대수학 3차 과제

7.3.26 (a) Let $a_1, a_2 \in H$ and $b_1, b_2 \in K$. Then $a_1b_1, a_2b_2 \in HK$, which means $HK \neq \phi$.

(i) $a_1b_1 \cdot a_2b_2 = a_1a_2b_1b_2 \in HK$ since $a_1a_2 \in H$ and $b_1b_2 \in K$.

($\because$ G is an abelian group)

(ii) $(a_1b_1)^{-1} = b_1^{-1}a_1^{-1} = a_1^{-1}b_1^{-1}$ ($\because$ G is an abelian group).

This means that every element in HK has its inverse.

By (i) and (ii), HK is a subgroup of G ∎

(b) Suppose $G = S_3$. and $H = \langle a \rangle$ and $K = \langle b \rangle$ where

$$a = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad b = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$ Then,

$HK = \{1, a, b, ab\}$ does not contain $(ab)^{-1}$, thus HK is not a subgroup ∎

$$(ab)^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

7.3.38 (a) We know that $U(\mathbb{Z}_p) = \{1, 2, \cdots p-1\}$ thus $|U(\mathbb{Z}_p)| = p-1$.

Since $U(\mathbb{Z}_p)$ is a multiplicative group of nonzeros of $\mathbb{Z}_p$, $U(\mathbb{Z}_p)$ is a cyclic group. This means that for some $g \in U(\mathbb{Z}_p)$, g is a generator of $U(\mathbb{Z}_p)$ of order $p-1$.

Let $b = g^k$ ($k \in \mathbb{Z}$) then $b^{p-1} = (g^k)^{p-1} = (g^{p-1})^k = 1$ ∎

(b) If $(a, p) = 1$ then $[a]^{p-1} = 1$ by (i). This means that $a^{p-1} \equiv 1 \pmod p$ thus $a^p \equiv a \pmod p$.

If $(a, p) > 1$ then $p | a$. and $a \equiv 0 \pmod p$, which means that $a^p \equiv a \pmod p$ ∎

7.3.50. Let $G = \langle a \rangle$ be a cyclic group of infinite order.
Using additive notation, $2x = a$ has no solution in G.

But $\mathbb{Q}$ always has a solution of such equation as $x = \frac{a}{2}$,

which is a contradiction.

Thus $\mathbb{Q}$ is not a cyclic group ∎.

7.4.39 Let $f: \mathbb{Z} \to \mathbb{Q}$ be an isomorphism.

Then for some $b \in \mathbb{Q}$, $f(1) = b$. Thus we can say that

$f(u) = ub$ $(u \in \mathbb{Z})$.

Then $\frac{1}{2}b \in \mathbb{Q}$, but there is no $a \in \mathbb{Z}$ s.t $f(a) = \frac{1}{2}b$.

which is a contradiction.

Thus additive groups $\mathbb{Z}$ and $\mathbb{Q}$ are not isomorphic ∎

7.4.40 $\mathbb{Z}_6$ is commutative but S_3 is not.

Let $a, b \in S_3$ s.t $a \circ b \neq b \circ a$.

Suppose $f: \mathbb{Z}_6 \to S_3$ be an isomorphism.

Then, $\exists$ n, m s.t $f(n) = a$ and $f(m) = b$.

$f(n+m) = a \circ b \neq b \circ a = f(m+n)$ which is a contradiction ∎

7.4.42 All elements of $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ have order 2. However,

$(1,1) \in \mathbb{Z}_4 \times \mathbb{Z}_2$ has order 4. We know that if

$f: A \to B$ is an isomorphism, then order of $a \in A$ and

the order of $f(a) \in B$ should be the same ∎

7.4.61. Let $[g]$ be a generator of $\mathbb{Z}_n$ then let $\alpha_g : \mathbb{Z}_n \to \mathbb{Z}_n$

$\alpha_g(x) = gx \pmod{n}$

(i) Let $x, y \in \mathbb{Z}_n$ then suppose $\alpha_g(x) = \alpha_g(y)$ then

$gx = gy$ then $x = y$. Thus injective.

(ii) Let $p \in \mathbb{Z}_n$, $p = gg^{-1}x = g(g^{-1}x) = \alpha_g(g^{-1}x)$.

Thus surjective.

(iii) $\alpha_g(x+y) = g(x+y) = gx + gy = \alpha_g(x) + \alpha_g(y)$.

By (i), (ii), (iii), α_g is an automorphism of $\mathbb{Z}_n$.

Thus, $\alpha_g \in \operatorname{Aut} \mathbb{Z}_n$. Let $f : \operatorname{Aut}\mathbb{Z}_n \to U_n$ s.t $f(\alpha_g) = g \pmod{n}$

(i) Let $\alpha_{g_1}, \alpha_{g_2} \in \operatorname{Aut}\mathbb{Z}_n$ and let $f(\alpha_{g_1}) = f(\alpha_{g_2})$

then $g_1 = g_2$ $\to \alpha_{g_1}(1) = \alpha_{g_2}(1)$.

Since $\alpha_{g_1}, \alpha_{g_2}$ is automorphism, $\alpha_{g_1}(x) = \alpha_{g_2}(x)$

for $x \in \mathbb{N}$, $1 \le x < n$. $\longrightarrow$ Thus injective.

(ii) For any $g \in U_n$, it is a generator of $\mathbb{Z}_n$. Thus there exists $\alpha_g \in \mathrm{Aut}\,\mathbb{Z}_n$ s.t $f(\alpha_g) = g$ $\longrightarrow$ Thus surjective.

(iii) $(\alpha_{g_1} \circ \alpha_{g_2})(x) = \alpha_{g_1}([g_2 x]) = [g_1 g_2 x] = \alpha_{g_1 g_2} x$

By above, $\alpha_{g_1 g_2} = \alpha_{g_1} \circ \alpha_{g_2}$.

$f(\alpha_{g_1} \circ \alpha_{g_2}) = f(\alpha_{g_1 g_2}) = g_1 g_2 = f(g_1) \cdot f(g_2)$

$\rightarrow$ Thus, homomorphism.

By (i), (ii), (iii), $\mathrm{Aut}\,\mathbb{Z}_n$ and U_n are isomorphic $\blacksquare$