Solution - Abstract Algebra Assignments © BinaryPhi

Name: __________ **Assignment:** Number 4

Score: __________ **Last Edit:** June 8, 2022 PDT

Problem 1: Definitions

(a) Assuming $\{G_1; \circ\}$ and $\{G_2; *\}$ are two groups and f is a map from G_1 to G_2, if:

$$f(a \circ b) = f(a) * f(b), \quad \forall a, b \in G_1,$$

the map f is called a **Group Homomorphism**.

If G_1 and G_2 are two same groups,

f is called an **Endomorphism**.

If a Group Homomorphism f is an injection (one-to-one),

f is called a **Monomorphism**.

If a Group Homomorphism f is a surjection (onto),

f is called an **Epimorphism**.

If a Group Homomorphism f is a bijection (one-to-one correspondence, invertible),

f is called an **Isomorphism**, and G_1 and G_2 are **Isomorphic**, which is denoted by $G_1 \cong G_2$.

(b) Supplement:

Injection | One to One:

$$f : A \to B, \forall\, a, b \in A, \text{ such that } f(a) = f(b) \Longrightarrow a = b.$$

Surjection | Onto:

$$f : A \to B, \forall\, b \in B, \exists\, a \in A \text{ s.t. } f(a) = b.$$

Bijection | One to One Correspondence:

$$f : A \to B, \forall\, b \in B, \text{exists a unique } a \in A \text{ s.t. } f(a) = b.$$

(c) Assuming f is a group homomorphism from group G_1 to group G_2, then the set of all elements from G_1 which map to element e in G_2 is called the **Kernel** of group homomorphism f, which is denoted by $\ker f$. Mathematically written as:

$$\ker f := \{g_1 \in G_1 \mid f(g_1) = e\}.$$

(d) Assuming f is a group homomorphism from group G_1 to group G_2, e_1, e_2 are the identity elements in G_1, G_2 respectively, $\circ, *$ are the operations in G_1, G_2 respectively, prove that $f(e_1) = e_2$ and $\forall a \in G_1, f(a^{-1}) = f(a)^{-1}$.

$f(e_1) = e_2$:

$$\begin{aligned} f(e_1) &= f(e_1 \circ e_1) = f(e_1) * f(e_1) \\ f(e_1)^{-1} * f(e_1) &= f(e_1)^{-1} * f(e_1) * f(e_1) \\ e_2 &= f(e_1) \end{aligned}$$

$\forall a \in G_1, f(a^{-1}) = f(a)^{-1}$:

$$\forall a \in G_1, f(a^{-1}) * f(a) = f(a^{-1} \circ a) = f(e_1) = e_2 \Longrightarrow f(a^{-1}) = f(a)^{-1}.$$

(e) Assuming f is a group homomorphism from group G_1 to group G_2, $H < G_1$, prove that the image set of H, $f(H)$ is a subgroup of G_2.

Assuming $\forall a_2 \in f(H), \exists\, a_1 \in H$ s.t. $f(a_1) = a_2$, and $\forall b_2 \in f(H), \exists\, b_1 \in H$ s.t. $f(b_1) = b_2$. Because H is a group, $e_2 = f(e_1) \in f(H) \Longrightarrow f(H)$ is non-empty. We know that

$$\forall a, b \in S \Longrightarrow ab^{-1} \in S \iff S \text{ is a subgroup of ...}$$

Thus, $a_2 b_2^{-1} = f(a_1) f(b_1)^{-1} = f(a_1) f(b_1^{-1}) = f(a_1 b_1^{-1}) \in f(H)$.

$f(H)$ is a subgroup of G_2

(f) Assuming G is a group, $H \lhd G$, ι is a map from G to G/H:

$$\iota(a) = aH,\ \forall a \in G.$$

Then, ι is an epimorphism, and is called the **Canonical Homomorphism** from group G to quotient group G/H.

(g) **Group Isomorphism Theorem I | Fundamental Theorem on Group Homomorphisms**

Prove that if f is an epimorphism from group G_1 to group G_2, $G_1/\ker f \cong G_2$.

Let a map $\phi : G_1/\ker f \longrightarrow G_2$, and assume $F = \ker f$, which means

$$\phi : G_1/F \longrightarrow G_2;\quad gF \longmapsto f(g).$$

If

$$\begin{aligned} g_1F = g_2F,\ &\text{where } g_1, g_2 \in G_1 \\ &\Longrightarrow g_1 R g_2 \Longrightarrow g_1^{-1}g_2 \in F \Longrightarrow f(g_1^{-1}g_2) = e_2 \\ &\Longrightarrow f(g_1)^{-1}f(g_2) = e_2 \\ &\Longrightarrow f(g_1) = f(g_2), \end{aligned}$$

which means it is well-defined to say that ϕ is a map

Similarly, ϕ is an injection because if

$$f(g_1) = f(g_2) \Longrightarrow g_1F = g_2F,\ \text{where } g_1, g_2 \in G_1,$$

We know that f is an epimorphism, so ϕ is a surjection map $\Longrightarrow$ ϕ is a bijection. Then, to prove ϕ is a group homomorphism from G_1/F with operation "$\circ$" to G_2 with operation "$*$", we have:

$$\begin{aligned} \forall aF, bF \in G_1/F,\ \phi(aF \circ bF) &= \phi(abF) \\ &= f(ab) \\ &= f(a)f(b) \\ &= \phi(aF) * \phi(bF) \end{aligned}$$

Therfore, ϕ is an isomorphism, denoted by $G_1/\ker f \cong G_2$.

(h) **Group Isomorphism Theorem II**

Let G be a group, $N \lhd G$, and H is a subgroup of G. Then:

1. HN is a subgroup of G which contains N.

2. $(H \cap N) \lhd H$.

3. $HN/N \cong H/(H \cap N)$.

(i) **Group Isomorphism Theorem III**

Let G be a group, $N \lhd G, N \lhd G, N \subseteq H$. Then:

1. $H/N \lhd G/N$

2. $(G/N)/(H/N) \cong G/H$

(j) **Group Isomorphism Theorem IV | Correspondence Theorem**

Assume f is an epimorphism from group G_1 to G_2, and the kernel of group homomorphism f is $F = \ker f$. We have:

1. The map from a subgroup of G_1 that contains N to a subgroup of G_2 is bijective.

2. The bijection from the subgroup of G_1 that contains N to the subgroup of G_2 is also a map from a normal subgroup onto a normal subgroup.

3. For a normal subgroup $H \lhd G_1$ such that H contains N, $G_1/H \cong G_2/f(H)$.

Problem 2: Prove:

(a) Assuming f is a group homomorphism from group G_1 to G_2, we have $\ker f \lhd G_1$.

First prove $\ker f < G_1$:

Assume e_1, e_2 are the identities of group G_1 and G_2 respectively. For a non-empty subset $\ker f$ of G_1 because $e_1 \in \ker f, \forall a, b \in \ker f$, we have:

$$\begin{aligned} f(ab^{-1}) = f(a)f(b^{-1}) = f(a)f(b)^{-1} = e_2 e_2^{-1} = e_2 \\ \Longrightarrow ab^{-1} \in \ker f. \end{aligned}$$

Thus, $\ker f < G_1$.

Then, prove $\ker f \lhd G_1$:

$\forall g \in G_1, a \in \ker f$, we have:

$$\begin{aligned} f(gag^{-1}) = f(g)f(a)f(g^{-1}) = f(g)e_2 f(g)^{-1} = e_2 \\ \Longrightarrow gag^{-1} \in \ker f. \end{aligned}$$

Therefore, $\ker f \lhd G_1$.

(Group Isomorphism Theorem I)

(b) Assuming f is a group homomorphism from group G_1 to group G_2, then

$$f \text{ is monomorphism } \iff \ker f = \{e_1\}, \text{ where } e_1 \text{ is the identity of } G_1.$$

"$\Longrightarrow$: "

$\because f(e_1) = e_2, \ \therefore \{e_1\} \subseteq \ker f$.

$\forall a \in \ker f, f(a) = e_2 = f(e_1)$. $\because f$ is injective, $\therefore a = e_1$.

Thus, $\ker f = \{e_1\}$.

"$\Longleftarrow$: "

If $f(a) = f(b), a, b \in G_1$, then

$$f(ab^{-1}) = f(a)f(b)^{-1} = e_2 \Longrightarrow ab^{-1} \in \ker f.$$

$\because \ker f = \{e_1\}, \ \therefore ab^{-1} = e \Longrightarrow a = b$.

Thus, f is a monomorphism.

Problem 3: Define a binary operation $\circ$ in the integer set $\mathbb{Z}$ such that:

$$a \circ b = a + b - a \times b, \quad \forall a, b \in \mathbb{Z}.$$

Prove that $\{\mathbb{Z}, \circ\}$ is a monoid, and is isomorphic to a monoid of $\mathbb{Z}$ with respect to the operation multiplication "$\times$".

$\{\mathbb{Z}, \circ\}$ is a monoid:

Let $a, b, c \in \mathbb{Z}$, we have:

$$\begin{aligned}
a \circ b &= a + b - a \times b = b \circ a \\
e \circ a &= 0 \circ a = 0 + a - 0 \times a = a \\
(a \circ b) \circ c &= (a + b - a \times b) + c - (a + b - a \times b)c \\
&= a + b + c - a \times b - a \times c - b \times c + a \times b \times c \\
&= a \circ (b \circ c).
\end{aligned}$$

Thus, $\{\mathbb{Z}, \circ\}$ is a commutative monoid.

$\{\mathbb{Z}, \circ\}$ and a monoid of $\mathbb{Z}$ with the operation multiplication are isomorphic.

We need to find a map f that satisfies $f(m) \circ f(n) = f(m \times n)$. For a map $f(a) = 1 - a$, we have:

$$\begin{aligned}
f(m) \circ f(n) &= f(m) + f(n) - f(m) \times f(n) \\
&= 1 - m + 1 - n - (1 - m) \times (1 - n) \\
&= 1 - m \times n \\
&= f(m) \times f(n).
\end{aligned}$$

Thus, $\{\mathbb{Z}, \circ\}$ and a monoid $\{\mathbb{Z}, \times\}$ are isomorphic.

Problem 4: Let G be a group, prove the following statements:

$$m \longrightarrow m^{-1} \text{ is an automorphism of } G \text{ if and only if } G \text{ is an Abelian Group.}$$

Suppose the map $m \longrightarrow m^{-1}$ is ϕ. Since G is a group, ϕ is a surjection (one-to-one correspondence). If ϕ is an automorphism, we have:

$$\begin{aligned}\phi(a)\phi(b) &= \phi(ab) = (ab)^{-1} = b^{-1}a^{-1} \\ &= \phi(b)\phi(a), \forall a, b \in G.\end{aligned}$$

Thus, G is a commutative group.

If G is a commutative group, we have:

$$\begin{aligned}\phi(ab) &= (ab)^{-1} = b^{-1}a^{-1} \\ &= \phi(b)\phi(a) = \phi(a)\phi(b)\end{aligned}$$

Thus, f is an automorphism.

Problem 5: Assume G is an abelian group, prove that

$$\forall n \in \mathbb{Z}, m \longrightarrow m^n \text{ is an endomorphism of } G$$

What we are going to prove is $\forall n \in \mathbb{Z}, \forall a, b \in G, (ab)^n = a^n b^n$.
By using Mathematical induction, we have for $n = 1$ the equation holds, and assuming the equation holds for $n - 1$, which means:

$$\begin{aligned}(ab)^n &= (ab)(ab)^{n-1} \\ &= aba^{n-1}b^{n-1} \\ &= a^n b^n\end{aligned}$$

Thus, $\forall n \in \mathbb{Z}, a \longrightarrow a^n$ is an endomorphism of G.

Problem 6: Let $\phi : G \longrightarrow H$ be a group homomorphism.

Prove that $\phi(G)$ is abelian if and only if $\forall a, b \in G, aba^{-1}b^{-1} \in \ker\, \phi$.

Assume

$$\phi(a) = \alpha \in \phi(G)$$
$$\phi(b) = \beta \in \phi(G)$$
$$\forall a, b \in G.$$

$\forall \alpha, \beta \in \phi(G), \phi(G)$ is abelian

$$\begin{aligned}
&\text{if and only if} \;\; \alpha\beta = \beta\alpha \\
&\text{if and only if} \;\; (\beta\alpha)^{-1}(\alpha\beta) = (\beta\alpha)^{-1}(\beta\alpha) = e|_{\phi(G)} \\
&\text{if and only if} \;\; \alpha^{-1}\beta^{-1}\alpha\beta = e|_{\phi(G)} \\
&\text{if and only if} \;\; \phi(a)^{-1}\phi(b)^{-1}\phi(a)\phi(b) = e|_{\phi(G)} \\
&\text{if and only if} \;\; \phi(a^{-1}b^{-1}ab) = e|_{\phi(G)} \\
&\text{if and only if} \;\; a^{-1}b^{-1}ab \in \ker\, \phi \\
&\text{if and only if} \;\; aba^{-1}b^{-1} \in \ker\, \phi, \text{WLOG.}
\end{aligned}$$

Therefore, $\phi(G)$ is abelian if and only if $\forall a, b \in G, aba^{-1}b^{-1} \in \ker\, \phi$

Problem 7: The map $\phi : \mathbb{Z} \longrightarrow \mathbb{Z}$ defined by $\phi(n) = n - 1$ for $n \in \mathbb{Z}$ is bijective. Give the expression of the binary operation "*" on $\mathbb{Z}$ such that ϕ is isomorphic.

$$\{\mathbb{Z}, \times\} \longrightarrow \{\mathbb{Z}, *\}$$

If the map ϕ is isomorphic, we have:

$$\begin{aligned}
\phi(m \times n) &= \phi(m) * \phi(n) = (m-1) * (n-1) \\
\text{WLOG}, m * n &= \phi(m+1) * \phi(n+1) \\
&= \phi((m+1) \times (n+1)) \\
&= \phi(m \times n + m + n + 1) \\
&= m \times n + m + n
\end{aligned}$$

Therefore, we have $\forall m, n \in \mathbb{Z}, m * n = m \times n + m + n$.

Problem 8: The map $\phi : \mathbb{Q} \longrightarrow \mathbb{Q}$ defined by $\phi(n) = 2n + 1$ for $n \in \mathbb{Q}$ is bijective. Give the expression of the binary operation "*" on $\mathbb{Q}$ such that ϕ is isomorphic.

$$\{\mathbb{Q}, *\} \longrightarrow \{\mathbb{Q}, +\}$$

The map ϕ^{-1} is isomorphic because ϕ is isomorphic, we have:

$$\begin{aligned}
\phi(m + n) &= \phi(m) * \phi(n) = (2m+1) * (2n+1) \\
m * n &= \phi^{-1}(2m+1) * \phi^{-1}(2n+1) = \phi^{-1}((2m+1) + (2n+1)) \\
&= \phi^{-1}(2m + 2n + 2) \\
&= m + n + \frac{1}{2}
\end{aligned}$$

Therefore, we have $\forall m, n \in \mathbb{Z}, m * n = m + n + \frac{1}{2}$.