Solution - Abstract Algebra Assignments © BinaryPhi

Name: ________ **Assignment:** Number 3

Score: ________ **Last Edit:** May 31, 2022 PDT

Problem 1: Definitions

(a) Assuming H is a non-empty subset of group G while H is also a group with respect to the operation of G, we call H a **Subgroup** of G.

(b) H is a subgroup of a group G. If $H = \{e\}$ or $H = G$, H is called a **Trivial Subgroup**. Other subgroups are called the **Non-trivial Subgroup**.

(c) Prove that the following statements are equivalent if H is a non-empty subset of G.

1. $H < G$.
2. $a, b \in H \Longrightarrow a \circ b \in H, a^{-1} \in H$.
3. $a, b \in H \Longrightarrow a \circ b^{-1} \in H$.

$1 \Rightarrow 2$:
Since H is a group, according to the closure property, we have $a \circ b \in H$. Any element a must have an inverse element a^{-1} in H. Because $H < G$, which means the operations in both groups are the same, indicating that the inverse of a in H is exactly the inverse of a in G. Therefore, $a^{-1} \in H$.

$2 \Rightarrow 3$:
We have $b \in H \Longrightarrow b^{-1} \in H$, and $a, b^{-1} \in H$. Thus, $a \circ b^{-1} \in H$.

$3 \Rightarrow 1$:
We have $a, a \in H \Longrightarrow a \circ a^{-1} \in H$, which means $e \in H \Longrightarrow H$ has identity element in it. Then, we have $e, b \in H \Longrightarrow e \circ b^{-1} \in H$, which means $b^{-1} \in H \Longrightarrow$ every element in H has its corresponding inverse element. Because $a, b^{-1} \in H \Longrightarrow a \circ (b^{-1})^{-1} \in H$, which means $a \circ b \in H$, indicating the closure property of the operation of H. Additionally, the operation of the elements in H satisfies the associative law because H is a subset of a group G. Therefore, H is a group respect to the operation of G.

(d) Assume H is a subgroup of group G, $a \in G$, then:

$$a \circ H = \{a \circ h \mid h \in H\}, H \circ a = \{h \circ a \mid h \in H\}$$

(Or often written as: $aH = \{ah \mid h \in H\}, Ha = \{ha \mid h \in H\}$) are called the **left coset** and **right coset** of H with the representative el ement a, respectively.

(e) Assuming H is a subgroup of group G and $aRb \iff a^{-1}b \in H$,
i) prove that the relation R in G is an equivalent relation and
ii) the equivalent class of a, $\overline{a}$, is exactly the left coset of H represented by a: aH;
iii) thus the set of all left cosets of $H : \{aH\}$ is a partition of G.

For $a, b \in G$, we could determine that $a^{-1}b \in H$, thus R is a relation in G.
1) Reflexive Property: $\forall a \in G, a^{-1}a \in H \implies e \in H$, thus aRa.
2) Symmetric Property: If aRb, then $a^{-1}b \in H$, thus $(a^{-1}b)^{-1} \in H$ because H is a group. Therefore, $b^{-1}a \in H \implies bRa$.
3) Transitive Property: If aRb, bRc; then $a^{-1}b \in H$ and $b^{-1}c \in H$. Since H is a group, we have $a^{-1}bb^{-1}c \in H \implies a^{-1}c \in H$, $aRb, bRc \Rightarrow aRc$. Therefore, R is an equivalent relation in G.

$\forall b \in \overline{a}$ ($b \in H$), we have aRb, thus $a^{-1}b \in H$. Assuming $h \in H$ that satisfies $a^{-1}b = h$, which is $b = ah \in aH$, we have $\overline{a} \subseteq aH$ since $\forall b \in \overline{a}$. Additionally, we have $\forall b \in aH$, then assuming $h \in H \implies b = ah$. Thus, $a^{-1}b = h \in H \implies b \in \overline{a}$. In conclusion, $\overline{a} \subseteq aH, aH \subseteq \overline{a} \implies \overline{a} = aH$.

An equivalent relation R determines a partition of a set, each class is the equivalent class $\overline{a}$ with respect to this equivalent relation R. Since $\overline{a} = aH, \{aH\}$ is a partition of G.

(f) The quotient set G/R of group G with respect to the equivalent relation $aRb \iff a^{-1}b \in H, H < G$ is called the **Quotient Set of G by left congruence modulo H** or **Left Coset Space**, denoted by $G/H^{\mathbb{L}}$.

(g) The **Index** of a subgroup H in a group G is the number of left cosets or right cosets of H in G, which is denoted by $[G : H]$ or $|G : H|$.

(h) Assuming a group G has a subgroup $H < G$, we define H to be a **Normal Subgroup** of G (denoted by $H \lhd G$), if:

$$ghg^{-1} \in H, \forall g \in G, \forall h \in H.$$

(i) Prove the following statements are equivalent assuming G is a group and $H < G$:

1) $H \lhd G$;
2) $gH = Hg, \forall g \in G$;
3) $g_1H \cdot g_2H = g_1g_2H = \{g_1h_1g_2h_2 \mid h_1, h_2 \in H\}$.

1) $\Longrightarrow$ 2) : Since $H \lhd G$, $\forall g \in G$ and $\forall h \in H$, we have:

$$gh = ghg^{-1}g \in Hg;$$
$$hg = gg^{-1}hg \in gH;$$
$$\text{Since } gh \in gH \text{ and } hg \in Hg$$
$$\therefore\ gH = Hg.$$

2) $\Longrightarrow$ 3) : $\forall g_1, g_2 \in G$, there is an element $g_1h_1g_2h_2$ in $g_1H \cdot g_2H$ where $h_1, h_2 \in H$. We have $h_1g_2 \in Hg_2 = g_2H$, and considering $h_3 \in H$ which satisfies $h_1g_2 = g_2h_3$. Thus,

$$g_1h_1g_2h_2 = g_1g_2h_3h_2 \in g_1g_2H;$$
$$g_1H \cdot g_2H \subseteq g_1g_2H.$$

Then, any element g_1g_2h from g_1g_2H has:

$$g_1g_2h = g_1eg_2h \in g_1H \cdot g_2H;$$
$$g_1g_2H \subseteq g_1H \cdot g_2H.$$
$$\therefore g_1g_2H = g_1H \cdot g_2H.$$

3) $\Longrightarrow$ 1) : $\forall g \in G, \forall h \in H$, we have:

$$ghg^{-1} = ghg^{-1}e \in gH \cdot g^{-1}H = gg^{-1}H = eH = H$$

Therefore, $H \lhd G$.

(j) Assuming G is a group and $H < G$, R is a relation defined by $aRb \iff a^{-1}b \in H$, then:

$$R \text{ is a congruence relation in } G \iff H \lhd G.$$

$\Longleftarrow$: Assuming a_1Rb_1, a_2Rb_2, we have $a_1^{-1}\ b_1 \in H, a_2^{-1}\ b_2 \in H$. Since we have:

$$\begin{aligned}
(a_1\ a_2)^{-1}\ (b_1\ b_2) &= a_2^{-1}\ (a_1^{-1}\ b_1)\ a_2\ a_2^{-1}\ b_2;\\
\because H \lhd G, a_2^{-1}\ (a_1^{-1}\ b_1)\ a_2 \in H &\Longrightarrow a_2^{-1}\ (a_1^{-1}\ b_1)\ a_2\ a_2^{-1}\ b_2;\\
&\Longrightarrow (a_1\ a_2)^{-1}\ (b_1\ b_2) \in H
\end{aligned}$$

Therefore, $(a_1\ a_2)^{-1}R(b_1\ b_2)$, which means R is a congruence relation with respect to the operation in G.

$\Longrightarrow$: $\forall g \in G, \forall h \in H$, in order to prove $ghg^{-1} \in H$, we have:

$$\begin{aligned}
g^{-1}gh = h \in H &\Longrightarrow gR(gh),\\
gg^{-1}R(gh)g^{-1} &\Longrightarrow\ eRghg^{-1} \text{ because } g^{-1}Rg^{-1},\\
\therefore e^{-1}ghg^{-1} &= ghg^{-1} \in H.
\end{aligned}$$

More importantly, the quotient set G/R and the operation with respect to the congruence relation R is, a group, which is also called the **Quotient Group** or **Factor Group** of G by H, denoted by G/H.

Problem 2: Prove:

(a) Assuming H is a non-empty and finite subset of group G, we have

$$H < G \iff H \text{ is closed under the operation of } G$$

"$\Longrightarrow$":

Since G is a group, the operation in G must have associative property, left and right cancellative properties. Thus, the elements in the subset H with respect to the operation in G also have associative and cancellative properties. Because H is closed under the operation of G, H is a finite semigroup which also has the cancellative property. *Thus H is a group with respect to the operation of G.

$\therefore H < G$

*: Why? Recall the 2nd lecture.

(b) If H_1 and H_2 are both subgroup of group G, then $H_1 \cap H_2 < G$.

$e \in H_1 \cap H_2, \forall a, b \in H_1 \cap H_2$,we have $a, b \in H_1$ and $a, b \in H_2 \Longrightarrow a \circ b^{-1} \in H_1$ and $a \circ b^{-1} \in H_2$ because H_1 and H_2 are two subgroups of G.

Thus, $a \circ b^{-1} \in H_1 \cap H_2 \Longrightarrow H_1 \cap H_2 < G$.

(c) $[\mathbb{Z} : m \circ \mathbb{Z}] = m$, where $m \in \mathbb{N}$

Considering the left coset space of $\mathbb{Z}$ modulo $m \circ \mathbb{Z}$, we have:

$$\begin{aligned}\mathbb{Z} &= (0 + m \circ \mathbb{Z}) \cup (1 + m \circ \mathbb{Z}) \cup \cdots \cup ((m-1) + m \circ \mathbb{Z}) \\ &= \overline{0} \cup \overline{1} \cup \cdots \cup \overline{(m-1)}.\end{aligned}$$

$\therefore \quad [\mathbb{Z} : m \circ \mathbb{Z}] = m$

Problem 3: **Lagrange Theorem:**

For a finite group G, $H < G$, then we have:

$$|G| = [G : H] \cdot |H|,$$

which means the order of the subgroup H is a factor of the order of G.

First of all, the number of elements in any left coset aH of H is equal to the number of elements in H (which is denoted by $|H|$). It will be easier to think the map $h \to ah, \forall h \in H$.

Then, G can be described by the union of all non-intersecting left cosets of H, which is $[G : H]$ of them.

Therefore, there are $[G : H] \cdot |H|$ elements in $G \Longrightarrow |G| = [G : H] \cdot |H|$.

Problem 4: **Corollary** of Lagrange Theorem:

If G is a finite group and $K < G, H < K$, we have:

$$[G : H] = [G : K] \cdot [K : H].$$

According to Lagrange Theorem, we have

$$\begin{aligned} |G| &= [G : K] \cdot |K| = [G : K] \cdot [K : H] \cdot |H|, \\ |G| &= [G : H] \cdot |H|. \\ [G : H] \cdot |H| &= [G : K] \cdot [K : H] \cdot |H|, \\ \therefore [G : H] &= [G : K] \cdot [K : H]. \end{aligned}$$

Therefore, the corollary is proved.

Problem 5: Which of the following are true?

(a) False There exists a group in which the cancellation law fails.

(b) False Every group has exactly two improper subgroups.

(c) True Every group is a subgroup of itself.

(d) False A subgroup can be defined as the subset of a group.

(e) False Every set of numbers that is a group under addition is also a group under multiplication.

Problem 6: Prove that

if G is an abelian group, written multiplicatively, with identity element e, then all elements x of G satisfying the equation $x^2 = e$ form a subgroup H of G.

Closure:

$\forall a, b \in H$, since G is abelian, we have $(ab)^2 = a^2b^2 = ee = e$, so $ab \in H \Longrightarrow H$ is closed.

Identity:

$\because\ ee = e$, we have $e \in H$.

Inverses:

$\because\ \forall a \in H, aa = e$, which means the element of H and its inverse is the same.

(Ref: John B. Fraleigh, Victor J. Katz. A first course in abstract algebra, 2003.)

Problem 7: Assume H, K are two normal subgroups of group G and $H \cap K = \{1\}$. Prove the following

$$hk = kh, \forall h \in H, \forall k \in K.$$

Because H, K are normal subgroups, we have:

$$\begin{aligned} hkh^{-1} \in K; \quad & kh^{-1}k^{-1} \in H; \\ hkh^{-1}k^{-1} = \ & (hkh^{-1})k^{-1} \in K \\ = \ & h(kh^{-1}k^{-1}) \in H \\ \in \ & K \cap H = \{1\} \end{aligned}$$

Therefore, $hkh^{-1}k^{-1} = 1 \Longrightarrow hk = kh$.

Problem 8: Assume H is a normal subgroup of group G. Prove that the sufficient prerequisite for G/H to be an abelian group is the following:

$$gkg^{-1}k^{-1} \in H, \forall g, k \in G.$$

The quotient group $G/H = \{gH \mid g \in G\}$ has $gHkH = gkH, (gH)^{-1} = g^{-1}H$. Then,

$$\begin{aligned} gHkH = kHgH &\text{ if and only if } gHkH(gH)^{-1}(kH)^{-1} = H \\ &\text{ if and only if } gkg^{-1}k^{-1}H = H \\ &\text{ if and only if } gkg^{-1}k^{-1} \in H \end{aligned}$$