Homework 1

Due date: 2019. 3.13.

1. Give two reasons why the set of odd integers under addition is not a group.

2. Show that the set $\{5,15,25,35\}$ is a group under multiplication modulo 40. What is the identity element of this group?

3. Let G be a group with the following property: Whenever a,b and c belong to G and $ab=ca$, then $b=c$. Prove G is Abelian.

4. Let a and b be elements of an Abelian group and let n be any integer. Show that $(ab)^n = a^n b^n$.

5. Solve the problem 25 on exercise 2.

6. Let G be a finite group. Show that the number of elements x of G such that $x^3 = e$ is odd.

7. Prove that if G is a group with the property that the square of every element is the identity, G is Abelian.

8. Prove that the set $\{1,2,\cdots,n-1\}$ is a grop under multiplication modulo n if and only if n is prime.

9. Show that if $(ab)^2 = a^2b^2$ for a and b in a group G, then G is Abelian.

10. Let G be a group and let $a,b \in G$. Show that $(ab)^{-1} = a^{-1}b^{-1}$ if and only if G is Abelian.

현대대수 I. HW1

파이낸스경영학과
2017004093
양 정 우

1. $S = \{2, 4, 6, 8, \cdots\}$

$\{0\} \notin S$; not exist addition identity

not exist inverse

2. $S = \{5, 15, 25, 35\}$

	5	15	25	35
5	25	35	5	5
15	35	25	15	5
25	5	15	25	35
35	5	5	35	25

$\cap$
S

i) operation multiplication modulo 40 is binary operation

ii) $\forall a, b, c \in S$, $(ab)c = a(bc)$

iii) $\forall a \in S$, $a \cdot 25 = a$ → identity

iv) $\forall a \in S$ has inverse as itself a

$\therefore$ S is group.

3. G is group. $a, b, c \in G$

$ab = ca \rightarrow b = c$

각변 c에 b를 대입 $\Rightarrow ab = bc$

$\therefore$ G is Abelian Group

4. Prove $ab = ba \rightarrow (ab)^n = a^n b^n$

i) $n = 1$, $(ab)^1 = ab$ (trivial)

ii) $n = k$, Assume $(ab)^k = a^k b^k$

iii) $n = k+1$

$(ab)^{k+1} = (ab)^k ab = a^k b^k ab$ (by ii)

$= a^k b^k ba = a^k b^{k+1} a = a^k a b^{k+1} = a^{k+1} b^{k+1}$

iv) $n < 0$ $n = -m$ $(m \in \mathbb{N})$

$a^n b^n = a^{-m} b^{-m} = (a^m b^m)^{-1} = ((ab)^m)^{-1} = (ab)^{-m} = (ab)^n$

$\therefore \forall n \in \mathbb{Z}$, $ab = ba \rightarrow (ab)^n = a^n b^n$

5. G : group. Prove that

G is Abelian : $ab = ba \Leftrightarrow (ab)^{-1} = a^{-1}b^{-1} \quad \forall a, b \in G$

($\Rightarrow$) $ba \cdot a^{-1}b^{-1} = beb^{-1} = bb^{-1} = e$

$a^{-1}b^{-1} \cdot ba = a^{-1}ea = a^{-1}a = e$ (*)

$\therefore a^{-1}b^{-1}$ is inverse of ba

$\Rightarrow (ba)^{-1} = a^{-1}b^{-1}$

$(ab)^{-1} = (ba)^{-1} \quad (\because ab = ba)$

$\therefore (ab)^{-1} = a^{-1}b^{-1}$

($\Leftarrow$) $(ab)^{-1} = a^{-1}b^{-1}$

$\Rightarrow ab \cdot a^{-1}b^{-1} = a^{-1}b^{-1} \cdot ab = e$

$a^{-1}b^{-1} = (ba)^{-1} \quad (\because (*))$

$\Rightarrow ba \cdot a^{-1}b^{-1} = a^{-1}b^{-1} \cdot ba = e$

$\Rightarrow (ab)^{-1} = (ba)^{-1}$

$\therefore ab = ba$

6. G : finite group

Prove number of $x \in G$ s.t $x^3 = e$ is odd.

Put $S = \{x \mid x^3 = e\} \subset G$

i) $x = e$

$e^3 = e \quad \therefore e \in S$

ii) $x \neq e$, suppose $x^3 = e$

$x \cdot x^2 = x^2 \cdot x = e \quad \therefore x^{-1} = x^2$

$(x^2)^3 = x^2 \cdot x^2 \cdot x^2 = x^6 = x^3 \cdot x^3 = e \cdot e = e \quad \therefore x^2 \in S$

WTS $x^2 \neq e$, If $x^2 = e$, $x = x \cdot e = x \cdot x^2 = x^3 = e$ ($\Rightarrow\Leftarrow$)

$\therefore x^2 \neq e$.

$\Rightarrow \forall x$ s.t $x^3 = e$, x^2 is also included in S

by i), ii) $S = \{e, x_1, x_1^2, x_2, x_2^2, \cdots x_k, x_k^2\}$

$\therefore n(S)$ is odd number.

7. Prove $\forall a \in G,\ a^2 = e \Rightarrow G$ is Abelian group.

$a, b \in G,\quad a^2 = e,\ b^2 = e$

$(ab)^2 = abab = e$

$aababb = aeb$

$a^2 ba b^2 = ab$

$ebae = ab$

$\Rightarrow ba = ab \quad \therefore G$ is Abelian group.

8. $S = \{1, 2, 3, \cdots, n-1\}$

Prove S is group under multiplication modulo n

$\Leftrightarrow n$ is prime

($\Rightarrow$) Suppose n is not prime

Then $n = pq$ where $1 < p, q < n \ (p, q \in S)$

$pq = 0 \pmod n$ but $0 \notin S$

$\therefore S$ is not group multiplication modulo n

This implies if S is group under multiplication modulo n, n is prime

($\Leftarrow$) (1) associativity $a(bc) = (ab)c$

(2) $\exists e \in S$ s.t $ae = ea = a \quad e = 1$

(3) choose $a \in S$

Note that n is prime. $n \geq 2$

$\Rightarrow a^{n-1} = 1 \pmod n$ by 페르마 소정리

$a \cdot a^{n-2} = a^{n-1} = 1$

a^{n-2} is inverse of a

$\therefore S$ is group

9. Prove $(ab)^2 = a^2b^2$ $\forall a, b \in G \longrightarrow G$ is Abelian group

$a^{-1}, b^{-1} \in G$ ($\because G$ is group)

$(ab)^2 = abab = aabb = a^2b^2$

$(a^{-1}a)ba(bb^{-1}) = (a^{-1}a)ab(bb^{-1})$

$\Rightarrow ebae = eabe$

$\Rightarrow ba = ab$ $\therefore G$ is Abelian group.

10. $(ab)^{-1} = a^{-1}b^{-1} \Leftrightarrow ab = ba$

($\Rightarrow$) $ab \cdot b^{-1}a^{-1} = aea^{-1} = aa^{-1} = e$

$b^{-1}a^{-1} \cdot ab = b^{-1}eb = b^{-1}b = e$

(*) $(ab)^{-1} = b^{-1}a^{-1}$

$(ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1}$

$(b^{-1})^{-1}(a^{-1})^{-1} = (a^{-1})^{-1}(b^{-1})^{-1}$

$\Rightarrow ba = ab$

($\Leftarrow$) $ab = ba \Rightarrow (ab)^{-1} = (ba)^{-1}$

$b^{-1}a^{-1} = (ab)^{-1} = (ba)^{-1} = a^{-1}b^{-1}$

$\therefore (ab)^{-1} = a^{-1}b^{-1}$