Reading Questions 6

page 43: Definition 2.23

page 43: Theorem 2.24 and its proof

1. If a and b are elements of a semigroup and $ab = e$ where e is the identity element of the semigroup then a is a left inverse of b.
2. All semigroups are groups.
3. Do you have any concerns about the proof? Is the proof complete?

Section 2.2 Cancellation Properties (Part 1)

Properties of a Group

Definition

or

F a set S, a map $b : S \times S \to S$ is called a binary operation on S.

} monday reading

Definition

$(a \circ b) \circ c = a \circ (b \circ c)$

Assume that $\circ$ is an associative binary operation on a set G. Then $(G, \circ)$ is called a semigroup. In this case, we say G is a semigroup.

Theorem

Let G be an non-empty semigroup. Assume that G has a left identity and that every element of G has a left inverse. That is, there exists an element $e \in G$ such that, for every $a \in G$, $ea = a$, and, for every $a \in G$, there exists an element, denoted by a^{-1}, such that $a^{-1}a = e$. Then G is a group.

wed reading

P 1. Let G be a group such that $a, b, c \in G$. Prove if $ba = ca$ then $b = c$.

P 2. Prove: Let G be a group. For all $a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$. ← shoes - sock

More Properties of a Group

$\{1,3\}$ ||

P 3. Show that $((Z_4)^\times, \cdot)$ is ~~not~~ a group.

$$\begin{array}{c|cc} & 1 & 3 \\ \hline 1 & 1 & 3 \\ 3 & 3 & 1 \end{array}$$

P 4. Prove: The group G is abelian if and only if $(ab)^{-1} = a^{-1}b^{-1}$ for all $a, b \in G$.

$ba = ab$

$(Z_4, \cdot)$ is not a group.

	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

identity e DNE

$b = aba^{-1}$

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

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

Theorem

Let G be an non-empty semigroup. Assume that G has a left identity and that every element of G has a left inverse. That is, there exists an element $e \in G$ such that, for every $a \in G$, $ea = a$, and, for every $a \in G$, there exists an element, denoted by a^{-1}, such that $a^{-1}a = e$. Then G is a group.

WTS $\exists x \in G$ s.t. $ax = xa = a$ $\forall a \in G$

(identity) Consider e. We know

$\forall a \in G$ $ea = a$. Suppose $ae = b$.

Then $a^{-1}ae = a^{-1}b$

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

$c :=$ left inverse of a^{-1}

$\Rightarrow ca^{-1} = e$

(left inverse)

$\Rightarrow$ $\underbrace{ca^{-1}}_{e}a = ca^{-1}b$ $\Rightarrow$ $ea = eb$

(cancl prop.)

$\Rightarrow$ $\underline{a = b}$

$\Rightarrow$ $ae = a$.

(inverse) Suppose $ab = e$. Then $a^{-1}ab = a^{-1}e$

$= a^{-1}$.

Hence $eb = a^{-1} \Rightarrow b = a^{-1}$. $\Rightarrow aa^{-1} = a^{-1}a = e$

<u>lem:</u> Let G be a group such that $a, b, c \in G$.

Then $ab = ac \Rightarrow b = c$ and $ba = ca \Rightarrow b = c$.

<u>pf:</u> S $ab = ac$. Then $a^{-1}ab = a^{-1}ac$

$\Rightarrow$ $(a^{-1}a)b = (a^{-1}a)c$ (assoc.)

$\Rightarrow$ $eb = ec$ (inverse)

$\Rightarrow$ $b = c$. (id)

lem: let G be a group.

(1) e (identity) is unique.

pf: $\exists$ $xa = ax = a$ $\forall a \in G$. Then

$xe = e$. By def of e, $xe = x$

Hence $e = x$.

(2) a^{-1} is unique $\forall a \in G$

(pf) $\exists$ $ab = ba = e$. Then

$a^{-1}ab = a^{-1}e$

$\Rightarrow$ $eb = a^{-1}e$

$\Rightarrow$ $b = a^{-1}$ $\therefore$

(3) the inverse of a^{-1} is a $\forall a \in G$.

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

$a^{-1} \Rightarrow aa^{-1} = a^{-1}a = e$

by def of a^{-1}