Section 4 Groups, p45 #8,19,23,25,31,35

8. We can also consider multiplication $\cdot_n$ modulo n in $\mathbb{Z}_n$. For example, $5 \cdot_7 6 = 2$. The set $\{1, 3, 5, 7\}$ with multiplication $\cdot_8$ modulo 8 is a group. Give the table for this group.

Cayley Table:

$\cdot_8$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

In Exercise 11 through 18, determine whether the given set of matrices under the specified operation or multiplication, is a group.

19. Let S be the set of all real numbers except -1. Define $*$ on S by

$$a * b = a + b + ab$$

Complete the following:

a. Show that $*$ give a binary operation on S.

A binary operation is closed and uniquely defined.

Proof. i. Closed: Consider if $a * b = -1$.

$$\begin{aligned} a * b &= -1 \\ a + b + ab &= -1 \\ b(1 + a) &= -(1 + a) \\ b(1 + a) + (1 + a) &= 0 \\ (b + 1)(a + 1) &= 0 \\ b &= -1 \text{ or } a = -1 \end{aligned}$$

Since we are only considering $a, b \in S$.

ii. Uniquely defined:

$$a * b = a + b + ab$$

Since addition $+$ and multiplication $\cdot$ are uniquely defined, the result of $a + b + ab$, which consists of addition and multiplication, will always yield with a single result. Thus $*$ is uniquely defined.

Since $*$ is uniquely defined and closed, thus it is a binary operation on S. □

b. Show that $\langle S, * \rangle$ is a group

A group is closed, associative, has an identity, and has an inverse for every element.

Proof. i. Associative: Consider $a, b \in S$.

$$\begin{aligned} a * (b * c) &= a * (b + c + bc) \\ &= a + (b + c + bc) + a(b + c + bc) \\ &= a + b + c + bc + ab + ac + abc \end{aligned}$$

$$\begin{aligned} (a * b) * c &= (a + b + ab) * c \\ &= (a + b + ab) + c + (a + b + ab)c \\ &= a + b + c + ab + ac + bc + abc \end{aligned}$$

Thus $*$ is associative for S.

ii. Identity: Consider $e = 0$

$$\begin{aligned} a * e &= a + 0 + a0 = a \\ e * a &= 0 + a + 0a = a \end{aligned}$$

Thus S has an identity element under $*$.

iii. Inverse: Consider $a * a' = e$.

$$\begin{aligned} a * a' &= e \\ a + a' + aa' &= 0 \\ a' + aa' &= -a \\ a'(1 + a) &= -a \\ a' &= \frac{-a}{1 + a} \end{aligned}$$

Since S does not include -1, this will always be a defined value, thus every element has an inverse.

Since $\langle S, * \rangle$ is closed, associative, has an identity, and has an inverse for every element, it is a group. □

---

c. Find the solution of the equation $2 * x * 3 = 7$ in S

We can use the properties of the group to help us solve this.

$$\begin{aligned} 2 * x * 3 &= 7 \\ 2 + x + 3 + 2x + 6 + 3x + 6x &= 7 \\ 11 + 12x &= 7 \\ 12x &= -4 \\ x &= -\frac{1}{3} \end{aligned}$$

Concepts

23. The following ”definitions” of a group are taken verbatim, including spelling and punctuation, from papers of students who write a bit too quickly and carelessly.

Critizie them.

a. [Refer to book]

answer

b. [Refer to book]

answer

c. [Refer to book]

answer

d. [Refer to book]

answer

25. Mark each of the following.

True or False:

a. A group may have more than one identity element.

false

b. Any two groups of three elements are ismorphic.

true, because there is only one kind of group with three elements.

c. In a group, each linear equation has a solution.

true, since a group is closed.

d. The proper attitude toward a definition is to memorize it so that you can reproduce it word for word as in the text.

neither, whatever works best for the indivdual.

e. Any definition a person gives for a group is correct provided that everything that is a group by that person’s definition is also a group by the definition in the text.

false, it could be that something from the text is a group but not by the person’s definition.

f. Any definition a person gives for a group is correct provided he or she can show that everything that satifies the definition satifies the one in the text and conversely.

true

g. Every finite group of at most three elements is abelian.

true, since the corresponding single, dual, and triple element groups are all commutative.

h. An equation of the form $a * x = c$ always has a unique solution in a group.

true.

i. The empty set can be considered a group

false, there is no identity element

j. Every group is a binary algebraic structure

true, because a group requires a binary operation on a closed set.

Theory

31. If $*$ is a binary operation on a set S, an element x of S is an **idempotent for** $*$ if $x * x = x$. Prove that a group has exactly one idempotent element. (You may use any theorems proved so far in the text.)

Claim: The only idempotent element for a group is the identity element.

Proof. Consider $e * e$:

$$e * e = e$$

Thus e is idempotent. Consider if any other element were idempotent, meaning $a * a = a$ for some $a \neq e$.

$$\begin{aligned} a * a &= a & & \\ a * a &= a * e & & \mathfrak{G}_2 \\ a &= e & & \text{left cancellation law} \end{aligned}$$

However, thus contradicts our assertion that $a \neq e$. Thus the only idempotent element in any group is the identity element. $\square$

35. Show that if $(a * b)^2 = a^2 * b^2$ for a and b in a group G, then $a * b = b * a$. See Exercise 33 for the meaning of a^2.

$a^n = \underbrace{a * a * \cdots * a}_{n}$

Proof. Let $(a * b)^2 = a^2 * b^2$ for group G.

$$\begin{aligned} (a * b)^2 &= a^2 * b^2 && \\ (a * b) * (a * b) &= (a * a) * (b * b) && \text{by definition} \\ a * (b * a) * b &= a * (a * b) * b && \mathfrak{G}_1 \\ b * a &= a * b && \text{left, right cancellation laws} \end{aligned}$$

Thus $b * a = a * b$. $\square$