Notes on Charles Pinter's 'A Book Of Abstract Algebra'

Unathi Skosana

July 18, 2021

Personal notes taken while studying Charles Pinter's 'A Book Of Abstract Algebra'

Contents

Operations

Question 1. *What is an **operation** on a set A?*

Definitions 2 (Informal definition)**.** An operation is any rule which assigns to each ordered pair of elements of A a unique element in A.

Definitions 3 (Formal definition)**.** Let A be any set:
An operation $*$ on A is a rule which assigns to each ordered pairs (a, b) of elements of A exactly one $a * b$ in A, such that:

- $a * b$ is defined for *every* ordered pair (a, b) of elements of A. [1]
- $a * b$ must be *uniquely* defined. [2]
- If $a, b \in A$, then $a * b \in A$. [3]

Definitions 4 (Commutativity)**.** An operation $*$ is said to be *commutative* if it satisfies

$$a * b = b * a \tag{1}$$

for any two elements a and b in A.

Definitions 5 (Associativity)**.** An operation $*$ is said to be *associative* if it satisfies

$$(a * b) * c = a * (b * c) \tag{2}$$

for any three elements a, b and c in A.

Definitions 6 (Identity element)**.** The *identity* element e with respect to the operation $*$ has the property that:

$$e * a = a \quad \text{and} \quad a * e = a \tag{3}$$

is true for every element a in A.

Definitions 7 (Inverses)**.** The inverse of any element a, item denoted by a^{-1} has the property that:

$$a * a^{-1} = e \quad \text{and} \quad a^{-1} * a = e \tag{4}$$

[1] In $\mathbb{R}$, division does not qualify as operation since it does not satisfy this condition. i.e. the ordered pair $(a, 0)$ has undefined quotient $a/0$.

[2] If $\diamond$ is defined on (a, b) to be the number whose square is ab. In $\mathbb{R}$, $\diamond$ does not qualify as an operation since $2 \diamond 2$ could be either 2, or +2.

[3] A is closed under the operation $*$

The Definitions of Groups

Question 8. *What is a **group**?*

Definitions 9 (Informal definition)**.** A group is defined to be a set with an operation ($*$) which is associative, has an identity element, and each element in the set has an inverse.

Definitions 10 (Formal definition)**.** A group is a set G, together with an operation $*$ which satisfies:

- $*$ is associative.
- There exists an element e in G such that $a * e = a$ and $e * a = a$ for every element a in G.
- For every element in a in G, there is an element a^{-1} in G such that $a * a^{-1} = e$ and $a^{-1} * a = e$.

A group as defined above is usually denoted by the pair symbol $(G, *)$, which denotes that a group is a set G together with the operation $*$. [4]

[4] If there is no chance of ambiguity, the group is usually denoted with just the letter G.

Remark 11. The set of integers $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ is a group with the operation of addition, denoted by $(\mathbb{Z}, +)$. Similarly,the set of rationals numbers and addition $(\mathbb{Q}, +)$, and the set of real numbers $(\mathbb{R}, +)$.

Remark 12. Many a times, algebraic structures apparent in the study of natural phenomena (that is to say in physics) are groups, *i.e.* quantum spin, angular momentum

Example 13 (Finite groups: Groups of integers modulo n)**.** The group of integers modulo $n > 1$ consists of the set

$$\{0, 1, 2, \dots, n - 1\} \tag{5}$$

together with the operation of addition modulo n; The addition of two numbers a and b modulo n, can be described by imaging a set of equidistant points on an arc of a unit circle. To add a and b, we start at a and hop b points on the arc each at an angle of $2\pi/n$ from the next, where we end up will be the sum $a + b$, see Figure 1. This operation is associative (instead of starting at a, we can start at b and hop a times, we'll end up at $a + b$ again). The identity element for this group is 0, and the $n - a$ is the inverse of a ($a + n - a = n = 0$). [5] Such a group is denoted by the symbol $\mathbb{Z}_n$.

[5] The element $-a$ would seem to quality as inverse of a, $a + (-a) = 0$. However $-a$ does not belong to the group.

Cayley table shows the operation of a finite group, by arranging all possible group operations of all the elements in the group in a square table, and from the Cayley table, many properties of the group can be easily discerned. Consider the Cayley table for the group $\mathbb{Z}_3$ below:

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

a quick glance at the table, we can see that $\mathbb{Z}_3$ is a commutative or Abelian group and 1 and 2 are inverses of one another. Any finite group $(G, *)$ has a Cayley table of the form

$*$	$\cdots$	y	$\cdots$
$\vdots$			
x		$x * y$	
$\vdots$			

each element in G has one designated row and similarly a column, then the entry in the row of x and the column of y is $x * y$.

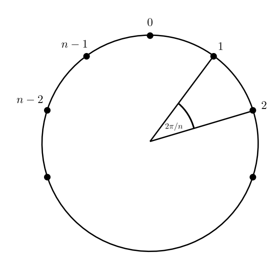

Figure 1: Addition modulo n can be visualized by hoping around equidistant points on an arc of a unit circle.