ABSTRACT ALGEBRA

- A Quick Guide -

Huan Q. Bui

Colby College

PHYSICS & MATHEMATICS
Statistics

Class of 2021

September 25, 2019

Preface

Greetings,

Abstract Algebra: A Quick Guide to is compiled based on my MA333: Abstract Algebra notes with professor Tamar Friedmann. This guide is almost entirely based on *Contemporary Abstract Algebra, Fourth edition* by Gallian and my class notes with professor Friedmann.

Enjoy!

Contents

Preface 2

1 GROUPS **5**

1.1 Definition 5

1.2 Elementary Properties 5

1.2.1 Uniqueness of Identity 5

1.2.2 Cancellation 6

1.2.3 Uniqueness of Inverses 6

1.2.4 Socks-Shoes Property 6

2 FINITE GROUPS & SUBGROUPS **7**

Chapter 1

GROUPS

1.1 Definition

A group is always defined *under* some binary operation. What is a binary operation? Let a set G be given. A binary operation on G is a function that assigns to each ordered pair of elements of G an element of G.

A group, then is defined as follows. Let a (nonempty) set G be given with a binary operation that assigns to each ordered pair (a, b) where $a, b \in G$ an element $ab \in G$. G is a group under this operation if the following properties are satisfied:

1. *Associativity:* The operation is associative, i.e, $a(bc) = (ab)c$.

2. *Identity:* There exists an element e, called the identity, in G such that $ae = ea = a \forall a \in G$.

3. *Inverses:* $\forall a \in G, \exists b \in G$ s.t. $ab = ba = e$. We call b the inverse of a, denoted a^{-1}.

We note that the binary operation associated with each group is not necessarily commutative. A commutative group is called *Abelian*. A non-commutative group is called *non-Abelian*.

1.2 Elementary Properties

1.2.1 Uniqueness of Identity

In a group G, there is only one identity element. The proof of this is quite simple. Let a group G be given. Suppose $ae = a$ and $ae' = e'a = a$ for all $a \in G$. Then we have $ae = ea = a = ae' = ea'$. If $a = e$ then we immediately have $ee' = e = e'e = e'$. So $e = e'$. Thus, the identity is unique.

1.2.2 Cancellation

In a group G, the right and left cancellation laws hold, i.e, $ab = ac \implies b = c$, and $ba = ca \implies b = c$. The proof of this is also quite simple. We simply multiply both sides of each equation from the appropriate direction with a^{-1}. By associativity, the a vanishes from both sides, leaving $b = c$.

1.2.3 Uniqueness of Inverses

For each element a in a group G, there is a unique element b in G such that $ab = ba = e$. We once again prove by supposing there are two distinct inverses of a, say b and b'. Then we have $ab = ab' = e$. By cancellation, we have $b = b'$.

1.2.4 Socks-Shoes Property

$$(ab)^{-1} = b^{-1}a^{-1}. \tag{1.1}$$

Chapter 2

FINITE GROUPS & SUBGROUPS