A Reading Project on Algebraic Structures

Vikranth Pulamathi

January 20, 2021

Dept. of PG Physics
St. Joseph's College (Autonomous) Bangalore, India - 560027

Contents

Algebraic Structures

A Summary by Vikranth Pulamathi

Started: January 20, 2021
Completed: 2021

1 Introduction

A collection of family of things that share similar properties is simply called a *Set*, and the things in the set are called *elements* of that set. A Cartesian Product of two sets A and B is defined as

$$A \times B = \{(a, b) | a \in A, b \in B\} \tag{1.1}$$

The *cardinality* of a set A is the number of elements of A, denoted as $|A|$. The cardinality of the empty set ϕ is zero. The set of natural numbers $\mathbb{N}$ has inifinite cardinality.

For two sets A and B and their complements A' and B', the principle of Inclusion-Exclusion says

$$|A \cup B| = |A| + |B| - |A \cap B| \tag{1.2}$$

and De-Morgan's Laws state

$$(A \cup B)' = A' \cap B' \tag{1.3a}$$

$$(A \cap B)' = A' \cup B' \tag{1.3b}$$

Any subset R of the Cartesian Product $A \times B$ defines a relation from A to B. Then, for $(a, b) \in R$, the relation is denotes as aRb. There are several kinds of relations as follows:

1. **Empty Relation** is when $R = \phi$
2. **Universal Relation** is when every element of A is related to every element in B
3. **Identity Relation** is when every element of A is related to itself, $I = \{(a, a) | a \in A\}$
4. **Inverse Relation** is when if $R = \{(a, b)\} \in A \times B$ is a relation, then the inverse is $R^{-1} = \{(b, a) | a, b \in R\}$
5. **Reflexive Relation** iff every element of A maps to itself, i.e.,

$$\forall a \in A, \quad aRa \in R \tag{1.4}$$

6. **Symmetric Relation** iff

$$\forall a, b \in R, \quad aRb = bRa \tag{1.5}$$

7. **Transitive Relation** iff

$$\forall a, b, c \in R, \quad aRb \quad \& \quad bRc \Rightarrow aRc \tag{1.6}$$

8. **Equivalence Relation** when a given relation R is all Reflexive, Symmetric and Transitive.

A *function*, or a *mapping* is a relation between some input(called Domain) and output(called Range). Let $f : A \to B$ and $g : B \to C$. Then, the composition $\phi\psi$ is a mapping from A to C defined as

$$(f \circ g)(x) = f(g(x)), \quad \forall x \in A \tag{1.7}$$

Functions are of the following types:

1. **One to One** or **Injective Function**: A function $f : A \to B$ (or $f(a) = b$, $a \in A, b \in B$)is one-to-one if

$$f(a_1) = f(a_2) \Rightarrow a_1 = a_2, \quad \forall a_1, a_2 \in A \tag{1.8}$$

2. **Many to One Function**: when one or more elements of A maps to the same element in B

3. **Onto** or **Surjective Function**: A function in which every element of B has pre-image in A.

4. **One-One Correspondence** or **Bijective Function**: If a function is both injective and surjective, i.e., if every element in A has a unique element in B AND every element of B has a pre-image in A.

A *partition* of a set S is defined as a collection of non-empty and disjoint subsets of S, whose union is the whole set S. The equivalence classes of an equivalence relation on a set S constitute a partition of S. Conversely, for any partition P of S, there is an equivalence relation on S whose equivalence classes are the elements of P.

2 Group Like

2.1 Groups

Definition: A *Binary Operation* on a set G is a function that assigns each ordered pair of G an element of G.

So, if the memebers of the ordered pair of G undergo a binary operation to produce another element of the same set G, then the corresponding binary operation is said to be *closed*, and this is called the *closure property* of a binary operation.

Definition: Consider a set G with a binary operation *(usually multiplication). Then, the set G is called a *Group* if it satisfies the following:

1. **Associativity**: The binary operation must be associative, i.e.,

$$(a * b) * c = a * (b * c), \quad \forall a, b, c \in G \tag{2.1}$$

2. **Existence of Identities:**

$$\exists\, e \in G \ni a * e = e * a = a, \forall a \in G \tag{2.2}$$

3. **Existence of Inverse**

$$\forall a \in G, \exists\, b \in G \ni a * b = b * a = e \tag{2.3}$$

2.1.1 Properties of Groups

Theorem 2.1: In a group $(G, *)$, there is only one identity element
Proof: Suppose there are two identities e and e'. Then,
(a) $a * e = e * a = a, \quad \forall\, a \in G$
(b) $a * e' = e' * a = a, \quad \forall\, a \in G$
These two give us $e' * e = e * e' \Rightarrow \boxed{e' = e}$

NOTE: The notation of binary operation * will now be dropped, but it is always implied that

$$ab \equiv a * b \tag{2.4}$$

Theorem 2.2: In a group G, the Left and Right Cancellation Laws hold good.
Proof: Suppose $ba = ca$ and let a' be the inverse of a. Then on multiplying on the right side, we get

$$\begin{aligned} (ba)a' &= (ca)a' \\ b(aa') &= c(aa') \quad \text{(Associativity)} \\ b &= c \qquad\quad \text{(Since } aa' = e = 1\text{)} \end{aligned}$$

This leads to another theorem that tells that the inverse of each element of a group is *unique*.

Theorem 2.3: For each element $a \in G$, where G is a group, there exists a unique inverse b such that $ab = ba = e$
Proof:Suppose b and c are inverses of $a \in G$. Then,

$$\begin{aligned} ab = e, \quad ac &= e \\ ab &= ac \\ \Rightarrow b &= c \quad \text{(By Cancellation Laws)} \end{aligned}$$

A rather interesting result about the products and inverses of elements of a group is the **Socks-Shoes Property**:
Theorem 2.4: For group elements $a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$
Proof: Consider

$$\begin{aligned} (ab)(ab)^{-1} &= e \\ (ab)(b^{-1}a^{-1}) &= e \\ a(bb^{-1})a^{-1} &= e \\ aa^{-1} &= e \Rightarrow e = e \end{aligned}$$

This result can be generalized as

$$(abc \dots k)^{-1} = k^{-1} \dots c^{-1}b^{-1}a^{-1} \tag{2.5}$$

Definition: The *order* of a group G is the number of elements it has(finite or infinite), and is denoted as $|G|$
Definition: The *order of an element* g in a group G is the smallest integer n such that $g^n = e \in G$. If there is no such n, then the order of that element $|g|$ is said to be infinite.

2.1.2 Group Homomorphism

Definition: A *homomorphism* from a group $(G, \cdot)$ to another group $(G', *)$ is defined as

$$f(a \cdot b) = f(a) * f(b) \tag{2.6}$$

A homomorphism has several kinds:

1. **Monomorphism** is a group homomorphism that is injective(one-to-one)
2. **Epimorphism** is a group homomorphism that is surjective(onto)
3. **Isomorphism** is a group homomorphism that is bijective(both one-to-one and onto). If this condition is satisfied, then for a homomorphism $f : G \to G'$, G and G' are said to be *isomorphic groups.*
4. **Endomorphism** is a group homomorphism defined as $f : G \to G$, i.e., the same group G is both codomain and range.
5. **Automorphism** is an endomorphism that is bijective, and hence an isomorphism.

Definition: The *kernel* of a homomorphism $h : G \to G'$ is defined as the set of elements of G that map to the identity of G'

$$\ker(h) = \{k \in G \,|\, h(k) = e' \in G'\} \tag{2.7}$$

Definition: The *image* of the same homomorphism as above is defined as

$$\text{im}(h) = h(G) = \{h(k) \,|\, k \in G\} \tag{2.8}$$

Fundamental Theorem of Homomorphism
Given two groups G and G' and a group homomorphism defined as $f : G \to G'$, let K be a normal subgroup in G, and $\phi : G \to G/K$. If K is a subset of $\ker(f)$, then there exists a unique homomorphism $h : G/K \to G'$ such that $f = h\phi$.

2.1.3 Subgroup

Definition: If a subset H of a group G is itself a group under the same binary operation of G, then H is called a *subgroup* of G. The identity of a subgroup is the same as the identity of the group, i.e. $e_H = e_G$. The inverse of an element of a subgroup is the same inverse of that element in that group. i.e. if $ab = ba = e_H$, then $ab = ba = e_G$

Theorem 2.5 - The One-Step Subgroup Test: Let G be a group and H be a non-empty subset of G. Then, $\forall\, a, b \in H$, if $ab^{-1} \in H$, then H is a subgroup of G.
Proof: Let $a = x$, $b = x$ where $x \in H$. Then,

$$ab^{-1} = xx^{-1} = e \in H$$

And if we choose $a = e$ and $b = x$, then

$$ab^{-1} \in H \Rightarrow ex^{-1} \in H \Rightarrow x^{-1} \in H$$

If some arbitrary $x, y \in H$, then $xy \in H$ since it is a subset of G. So, there is an identity element, inverse exists and since it is a subset of a group, associativity is satisfied. Therefore, H is a subgroup of G.

Theorem 2.6 - Two-Step Subgroup Test: Let G be a group and H be a non-empty subset of G. We say H is a subgroup of G if

$$1.\ ab \in H, \forall\, a, b \in H \qquad\qquad 2.\ a^{-1} \in H, \forall a \in H \tag{2.9}$$

The proof to Theorem 2.6 is left as an exercise to the reader. Note that if H is closed under the same binary operation of G, even then, H can be called a subgroup, since by default, $e \in H \Rightarrow a^{-1} \in H$. This is the Finite Subgroup Test.

Definition: The *center* $Z(G)$ of a group G is a set of those elements that commutes with every other element of the group

$$Z(G) = \{a \in G |\, ax = xa, \forall\, x \in G\} \tag{2.10}$$

Theorem 2.7: The center $Z(G)$ of a group G is a subgroup.
Proof: Clearly, $e \in Z(G) \Rightarrow Z(G) \neq \phi$. Take two elements $a, b \in Z(G)$. Then,

$$(ab)x = a(bx) = a(xb) = (ax)b = (xa)b = x(ab) \Rightarrow ab \in Z(G) \quad \ldots (1)$$

Now consider,

$$\begin{aligned} ax &= xa \\ a^{-1}(ax)a^{-1} &= a^{-1}(xa)a^{-1} \\ (a^{-1}a)xa^{-1} &= a^{-1}x(aa^{-1}) \\ xa^{-1} &= a^{-1}x \Rightarrow a^{-1} \in Z(G) \quad \ldots (2) \end{aligned}$$

From (1) and (2) and Theorem 2.6, we can conclude that $Z(G)$ is a subgroup of G. From the definition of a center, the set of all such x for a fixed $a \in G$ is called the *centralizer* of a in G

$$C(a) = \{x \in G \,|\, ga = ag, \forall a \in G\} \tag{2.11}$$

It can be proven similar to Theorem 2.7, that $C(a)$ is also a subgroup of G.

The intersection of any two subgroups A and B of a group G is again a subgroup of G. The union of A and B is a subgroup iff either A or B contains the other.

2.1.4 Cosets

Let H be a subgroup of a group G. Given $a \in G$, the **Left** and **Right** Cosets are obtained by multiplying each element of H with a fixed element a where a is the left and the right factor respectively, i.e.,

$$\text{Left Coset: } aH = \{ah \,|\, a \in G, h \in H\} \tag{2.12a}$$

$$\text{Right Coset: } Ha = \{ha \,|\, h \in H, a \in G\} \tag{2.12b}$$

If the group G is Abelian, then the notation changes to $g + H$ and $H + g$ respectively. Properties of Cosets are as follows:

1. $a \in aH$
   Proof: $a = ae \in aH$

2. $aH = H$ iff $a \in H$
   Proof: Assume $a \in H$ and let $h \in H$. Then, since $a \in G$ and $h \in H$, we know $a^{-1}h \in H$. Then, $h = eh = (aa^{-1})h = a(a^{-1}h) \in H$ and therefore $H \subset aH$ By direct observation, $aH \subset H$. Hence, $aH = H$ iff $a \in H$

3. $aH = bH$ iff $a \in bH$
   Proof: If $aH = bH$, then $a = ae \in aH = bH$. Conversely, if $a \in bH \Rightarrow a = bh$, $h \in H$ and therefore $aH = b(hH) = bH$.

4. $aH = bH$ or $aH \cap bH = \phi$
   Proof: It follows from the previous property that if $\exists c \in (aH \cap bH)$, then $cH = aH$ and $cH = bH$

5. $aH = bH$ iff $a^{-1}b \in H$
   Proof: Notice that $aH = bH$ if and only if $H = a^{-1}bH$. From the second property, this property is fairly obvious.

6. $|aH| = |bH|$
   Proof: The correspondence $ah \to bh$ maps $aH \to bH$, and hence by cancellation laws, the one-to-one property follows.

7. $aH = Ha$ iff $H = aHa^{-1}$
   Proof: Notice that $aH = Ha$ iff $(aH)a^{-1} = (Ha)a^{-1} \Rightarrow H = aHa^{-1}$

8. aH is subgroup of G iff $a \in H$
   Proof: If aH is a subgroup, then $e \in aH \Rightarrow aH \neq \phi$ and we have $aH = eH = H$. Thus from property 2, we have $a \in H$ and from its converse, we have that if $a \in H$, then again $aH = H$.

Lagrange's Theorem
If G is a finite group and H is a subgroup of G, then $|H|$ divides $|G|$ and the number of disctinct left(or right) cosets of H in G is $\frac{|G|}{|H|}$
Proof: Let $a_1H, a_2H, \ldots, a_rH$ be distinct left cosets of a subgroup H in a group G. Then, $a \in G$, we have $aH = a_iH$ for some i. Then, the group is given as

$$G = a_1H \cup a_2H \cup \ldots \cup a_rH$$

and the order can then be written as

$$|a_iH| = |H| \Rightarrow \boxed{|G| = r|H|}$$

Some Corollaries:

1. $|G : H| = |G|/|H|$
2. $|a|$ divides $|G|$
3. Groups whose order is a prime number are *cyclic*
4. $a^{|G|} = e \in G$
5. **Fermat's Little Theorem**

$$a^p \, mod \, p = a \, mod \, p, \quad a \in \mathbb{Z}, \quad p = \text{prime number}$$

2.1.5 Normal Subgroups

Definition: $\lhd$

2.1.6 Quotient Groups

2.2 Semigroups and Monoids

2.3 Quasigroup and Loops

2.4 Abelian Group

2.5 Magma

2.6 Lie Group

2.7 Group Theory

3 Ring Like

3.1 Ring

3.2 Semiring

3.3 Commutative Ring

3.4 Integral Domain

3.5 Fields

3.6 Ring Theory

4 Lattice Like

4.1 Lattices

4.2 Semilattice

4.3 Boolean Algebra

4.4 Lattice Theory

5 Module Like

5.1 Modules

5.2 Vector Space

5.3 Linear Algebra

6 Algebra Like

6.1 Algebra

6.2 Associative and Non-Associative

6.3 Composition Algebra

6.4 Lie Algebra

6.5 Bialgebra