

# A light introduction to Advance Mathematics: an Abstract Algebra Approach

Fares AlHarbi <sup>†</sup>

August 2021 <sup>‡§</sup>

## Abstract

This booklet written to be used in 60x60 event, to provide the big picture of advance mathematics and how mathematician's really work. No deep technical nor tough subjects, It's written with intuition and simplicity in mind.

---

<sup>†</sup>Mathematics student, with interest in Computer Science. Website: <https://faares.com>,  
E-Mail: [Faares@acm.org](mailto:Faares@acm.org).

<sup>‡</sup>This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike  
4.0 International License.

<sup>§</sup>Booklet source repository: [Github.com/Faares/60x60booklet](https://github.com/Faares/60x60booklet)

# Contents

<b>I</b>	<b>Introduction</b>	<b>4</b>
<b>1</b>	<b>About Mathematics</b>	<b>4</b>
<b>2</b>	<b>About Proof</b>	<b>4</b>
2.1	Mathematics and Proof . . . . .	5
<b>3</b>	<b>How Mathematician's really work?</b>	<b>5</b>
<b>II</b>	<b>Digging Technical</b>	<b>6</b>
<b>4</b>	<b>Understanding Mathematics</b>	<b>6</b>
<b>5</b>	<b>Sets, Relations, Mapping, Operations</b>	<b>7</b>
5.1	Sets . . . . .	7
5.1.1	Basic Concepts . . . . .	7
5.1.2	Special Sets . . . . .	8
5.2	Relations . . . . .	8
5.2.1	Ordered Pair . . . . .	8
5.2.2	Define Relationship . . . . .	8
5.2.3	Properties of Relationships . . . . .	9
5.3	Mapping . . . . .	10
5.3.1	Mapping, What is that? . . . . .	10
5.3.2	Types of Mapping . . . . .	10
5.3.3	The Inverse Map . . . . .	11
5.4	Operations . . . . .	12
5.4.1	Abstract and Generalize . . . . .	12
5.4.2	Operation as Algebraic System . . . . .	12
<b>III</b>	<b>Algebraic Structures</b>	<b>14</b>
<b>6</b>	<b>Algebraic Structure</b>	<b>14</b>
6.1	What is The Algebraic Structure? . . . . .	14
6.2	The Benefit of Studying Algebraic Structure . . . . .	14
<b>7</b>	<b>Groups</b>	<b>15</b>
7.1	Prologue . . . . .	15
7.1.1	Symmetry, The Shape of Nature . . . . .	15
7.2	Group, Formally . . . . .	15

<b>8</b>	<b>Rings</b>	<b>16</b>
8.1	Prologue . . . . .	16
8.2	Rings, Formally . . . . .	16
<b>9</b>	<b>Fields</b>	<b>17</b>
9.1	Prologue . . . . .	17
9.2	Fields, Formally . . . . .	18
	<b>References</b>	<b>19</b>

## Part I

# Introduction

## 1 About Mathematics

Mathematics, is the art of abstracted beauty. That art which everybody in this world can understand it in a different way and they struggling in explain it to other people. When we talk mathematically, we are trying to express our self's, reaching others, and touching souls. Meanwhile, we deeply care about truth and being formal after all of that.

Learning Mathematics is the learning of how to manage our ideas and beliefs about the world, how to understands things and put them into systems gives us the ability to predict the consequences of each step we can do. Our world is rich, rich of beauty which makes us wondering how it consist, how every part interact with and affect the whole. From here, Mathematics can be helpful to describe that beauty and make it measurable, usable, with accuracy.

## 2 About Proof

I mentioned that when we talk mathematically we are trying to express our self's, reaching others and we struggling in doing that. In the early history the humanity developed languages to jump over this problem and going forward, and we succeeded! But, later we faced *the problem of correctness and trust: How can we know if what we say correct or not? And how can we know Alice is not lying to us?* So, we needed a tool to investigate and make sure everything is as what we expected, that tool was what we call now *Proof*.

In every proof you will see in your life, it will starts with a common knowledge between two sides - I will call them *Prover* and *Learner* - and they already agreed on its correctness, no doubt's or arguing about that. After, the *Prover* begin to use that knowledge to derive a new information wasn't obvious to the *Learner*, by logical steps none of them can be false. As a result, the *Learner* should be convinced and have no doubt's about the new knowledge. Necessary to say, the last step comes with soul depth and believe.

Generally speaking, there are two way to proof something: Deduction or Induction. The first takes top-down approach while the second takes the opposite. Each one of them has several and various techniques, and its depends on the subject field and area to determine its usefulness. However, we will not go that far here and it's enough for the reader to know this. For more check *How to solve it* by George Pólya [7].

## 2.1 Mathematics and Proof

What if we mix beauty with truth? the result will be **Mathematics**. Grasp the whole world, and let it down in proofed system, and enjoy with the diamond. Euclid in his Elements[4] was the first known person who's done that, since then mathematics dressed her new form.

Mathematicians had basic units and wanted to build a skyscraper. The *Proof* was -and still- what deny it from falling apart. Since that, the story begins.

## 3 How Mathematician's really work?

Mathematics is an art. The art of discovery, invent, abstract, generalize ideas, and finally solve problems. What really mathematicians do is playing with their flight thoughts to answer a question. Like artists, Mathematicians are differ in their working style, depending on their personalities, approaches, cognitive functions. Some people prefer to work on a specific problem and solve it, other people enjoy developing theories and getting things formal in a general framework, while others stays in between: anatomizing the theories for the solver's so they can solve harder problems. A mathematician becomes professional when he started to create his tools and develop his theorems and proofs, You can figure out his power and abilities when you reading his papers.

They -Mathematician- started with a well definitions, building a floor over floor, to hit a goal. Seeking for clarity or to develop a tool to be used in solving a problem: Basically they *Implement a Strategy*. Imagination and intuition, are the energy of Mathematician's, learning is the foot, writing is the hand, and finally: a proof or solution is the product.

## Part II

# Digging Technical

## 4 Understanding Mathematics

Mathematician built a skyscraper over centuries, and in order to reach the wanted floor you have to pass through at least the requisite floors first. The learning process in mathematics is hierarchical, whenever you are well and good in the basics, you will get O-Ah! moment faster. In order to treat complicated things, we need to have tools process it accurately like surgical instrument in surgery.

Over the history, Mathematics developed from vocabulary in Al-Khawarizmi era, tell quantitize in Scientific Revolution era in 16-17th century, and finally symbolism in 18-19th century by Cantor, Whitehead, Russell and others - From them, we begin.<sup>1</sup>

Before going towards, I assume the reader is already grasp the essential rule of Logic in Mathematics, since I will not explain it here because in my opinion Logic is intuitive and people don't need to learn it.

---

<sup>1</sup>To know more about the history of Mathematics, see [6].

## 5 Sets, Relations, Mapping, Operations

Mathematics developed so fast, and grow in way opened the doors for more generalization and invent or discover different treatments. *Set Theory* was the first room to enter.

### 5.1 Sets

What is *set*? Generally speaking, its a collection of things. I would rather say a *Container* for objects, we put things in and work on it. Symbolically:

$$S = \{ x \mid P(x) \}$$

where  $P(x)$  the characterization property i.e. what decide does the element can be in the set or not.

#### 5.1.1 Basic Concepts

**Membership.** Let's say we have an object  $y$ , if the object belongs to the set -i.e. satisfying the  $P(x)$ - we write  $y \in S$  if not  $y \notin S$ .

**Union.** If we have  $A, B, C$  as sets, and we wanted to group all of their elements in one set  $S$ . How to do that? We use the *Union* operation, symbolically:

$$\begin{aligned} A &= \{ a \}, & B &= \{ b \}, & C &= \{ c \} \\ A \cup B &= \{ a, b \} & A \cup C &= \{ a, c \} & B \cup C &= \{ c \} \\ A \cup B \cup C &= \{ a, b, c \} \end{aligned}$$

**Intersection.** Same as *Union* except we want to group all of the common elements between sets:

$$\begin{aligned} A &= \{ a, b \}, & B &= \{ b, c \}, & C &= \{ c \} \\ A \cap B &= \{ b \} & A \cap C &= \{ \} = \phi & B \cap C &= \{ b \} \\ A \cap B \cap C &= \{ \} = \phi \end{aligned}$$

**Subset.** TODO.

### 5.1.2 Special Sets

There are special sets in Mathematics, we talk about and use them on a daily basis. Here are some:

Symbol	Name	Definition
$\mathbb{N}$	Natural Numbers	$\{1, 2, 3, 4, 5, 6, \dots\}$
$\mathbb{Z}$	Integers	$\{\dots, -2, -1, 0, 1, 2, \dots\}$
$\mathbb{Q}$	Rational Numbers	$\{\frac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0\}$
$\mathbb{I}$	Irrational Numbers	$\{x \mid x \notin \mathbb{Q}\}$
$\mathbb{R}$	Real Numbers	$\mathbb{Q} \cup \mathbb{I}$
$\mathbb{C}$	Complex Numbers	$\{a + ib \mid a, b \in \mathbb{R}, i = \sqrt{-1}\}$
$\phi$	Empty set	The nothing set! e.g. $A \cap C$

Its enough for the reader to know this, Set Theory is a huge topic I can't cover it all here.

## 5.2 Relations

### 5.2.1 Ordered Pair

We already defined sets and learned the basic concepts. But until now we didn't study how they interact with each other and what's the nature of it. To accomplish that, we need to introduce a new concept associate an element from set  $A$  with an element from  $B$  set or from and into the set of it self e.g. from  $A$  to  $A$ . This new concept called *Ordered Pair*, symbolically:

$$(a, b) \mid a \in A, b \in B$$

Whenever we write it, we mean there exist an association between  $a$  and  $b$ . A marked note to remember: *The order of the element is important:*

$$(a, b) \neq (b, a)$$

The reason behind is because the left hand side (LHS) associate  $a$  with  $b$ , while the right hand side (RHS) associate  $b$  with  $a$  and the meaning is broadly different! as we will see later <sup>2</sup>. Needless to say, we didn't specify the nature of that association yet.

### 5.2.2 Define Relationship

The *Ordered Pair* associate one element from a set with a one from another. What about sets? how can we associate a set with another? the answer is by *Cartesian Product*: the set of all possible ordered pairs combined from the two sets. Symbolically:

$$A \times B = \{(a, b) \mid a \in A \text{ and } b \in B\}$$

A relationship  $R$  is *the set of ordered pairs  $(a, b)$  satisfying  $aRb$ , which is a subset of  $A \times B$ .*

---

<sup>2</sup>in 5.2.2 Examples, you can see it clearly with order relationships.



**Examples.**

$$A = \{1, 2\}, \quad B = \{2, 3\}, \quad C = \{4, 5\}$$

$$A \times B = \{(1, 2), (1, 3), (2, 2), (2, 3)\}$$

$$B \times A = \{(2, 1), (3, 1), (2, 2), (3, 2)\}$$

- Equality relationship (=):
  - on  $A \times B$ :  $\{(2, 2)\}$ .
  - on  $B \times A$ :  $\{(2, 2)\}$ .
- Less than relationship (<):
  - on  $A \times B$ :  $\{(1, 2), (1, 3), (2, 3)\}$ .
  - on  $B \times A$ :  $\phi$ .
- Less than or equal relation (>):
  - on  $A \times B$ :  $\phi$ .
  - on  $B \times A$ :  $\{(2, 1), (3, 1), (3, 2)\}$ .
- Less than or equal relation ( $\leq$ ):
  - on  $A \times B$ :  $\{(1, 2), (1, 3), (2, 2), (2, 3)\}$ .
  - on  $B \times A$ :  $\{(2, 2)\}$ .

### 5.2.3 Properties of Relationships

When we define a relation on a set, we create a vague patterns. Figuring it out help us to know *how the elements of the set are behaves under that relationship*, which gives a rich and clear understanding of the set objects. Moreover, it will expands our knowledge and maybe knock closed doors in research.

For technical reasons, we will assume there exist a set  $S$  for the following definition.

**Reflexivity** A relation  $R$  is **Reflexive** relation if and only if for every element in the set  $S$  is associated with it self. Formally  $aRa$  for all  $a \in S$ .

**Symmetry** A relation  $R$  is **Symmetric** relation if and only if  $a$  associated with  $b$  then  $b$  is also associated with  $a$ , Formally if  $aRb$  then  $bRa$ .

**Transitivity** A relation  $R$  is **Transitive** relation if and only if  $a$  associated with  $b$  and  $b$  associated with  $c$ , then  $a$  also associated with  $c$ . Formally if  $aRb$  and  $bRc$  then  $aRc$

**Order Relations** Some relations rearrange the elements to a specific order. For example, take less than or equal  $\leq$  relation on  $\mathbb{Z}$ , you can easily figure out that for any  $z_1, z_2 \in \mathbb{Z}$  either  $z_1 \leq z_2$  or  $z_2 \leq z_1$ , these relations are very useful when working on something like Lattice Theory [10] and others [9]! We will not going forward, it's enough to know these relations for now.

## 5.3 Mapping

I assume by now, you noticed that we started by a collection of things - the set elements -, putted them into a bag - the set -, and lastly associate its elements with each other - by relationship -. All of that's gave us a vague pattern we can determine it by the relations properties we learned! Eventually all of what we have done so far are an internal study, we didn't do any external movements on the elements, like: transfer, shifting, or even combined two elements to produce one. Mapping and Operation are the two mathematical concepts did that.

### 5.3.1 Mapping, What is that?

I like the term *Mapping*, because its so fruitful semantically. When we lost in the desert, we can use a *Map* to decide which direction have to take, the same map takes a piece of Earth surface and *associate* each point of it with a point on a piece of paper. That's mapping!

Mapping is all about *doing association on a certain condition or rule*. Something like: Take a point from the Earth surface, scale it down by a specific ratio, then draw it again on the same position in the paper.

Some people call it *Function* other *Mapping*, but still it's the same concept. Formally, you must have two sets -not necessarily different- the *Origin* set and *Destination* set, with a formula or algorithm to map the elements from the *Origin* to the *Destination*. Mathematician differs in naming them, but the concepts are the same again.

**Mapping.** Given two sets  $O, D$  we say  $f(x)$  is a map from  $O$  to  $D$  if:  
for every element  $o \in O$  there exist a one and only one destination element  $d \in D$ , such that  $f(o) = d$ .

### 5.3.2 Types of Mapping

There are several types of mapping <sup>3</sup>, here are the important one's:

- A map  $f(x)$  called **Injective** if every associated element in the *Destination* set associated with only one element in the *Original* set. Formally, if  $f(o_1) = f(o_2)$  then  $o_1 = o_2$ .

---

<sup>3</sup>Actually, mathematicians admire define new types and create their own tools, see section 3 to know more.

- A map  $f(x)$  called **Surjective** if every element in the *Destination* set associated with an element in the *Original* set. Formally, for every  $d \in D$  there exist  $o \in O$  such that  $f(o) = d$  or  $f(O) = D$ .
- A map  $f(x)$  called **Bijjective** if it both injective and surjective.<sup>4</sup>

### 5.3.3 The Inverse Map

You can think and ask your self: Ok, I mapped an element  $o \in \textit{Original}$  to another  $f(o) = d \in \textit{Destination}$ , how can I get  $o$  If I know  $d = f(o)$ ?

You have  $d$ , and  $f$  only. To answer this question, the first thing you have to do is to check the map  $f$  it self. To decide does it **Injective** or not. Why? assume  $f$  not injective, that means  $d$  could be associated with two different element in the *Original* set, so you cannot determine which one is the correct one! Another reason, is because if we associate two elements with  $d$  that deny us from defining a mapping from the *Destination* set to the *Original* set, since it violate the the only and only one rule.

Secondly, you have to check does the map  $f$  **Surjective** or not. Why? Again you have  $d \in \textit{Destination}$  and  $f$  only. If  $f$  not surjective, that means  $d$  may not associated with any element at all! You will waste your time and get nothing, because nothing was there at all! Another reason, is because that also will deny us from defining a map from the *Destination* set to the *Original* set, since it violate the every element in *Original* must associate with another rule.

If the map  $f$  passed the previous two tests, that means it's **Bijjective** and now you can define what we call the **Inverse Map** denoted by  $f^{-1}$ . The main goal of this map is to reverse the original map operation. For example let say we have a map  $f(x) = 2x$  from  $\mathbb{Z}$  to  $\mathbb{Z}$ , the inverse map will be  $f^{-1}(x) = \frac{x}{2}$ , in other word if we composite the two maps we will get the base element:  $f(1) = 2(1) = 2$  and  $f^{-1}(2) = \frac{2}{2} = 1$ , so  $f^{-1}(f(1)) = \frac{2(1)}{2} = \frac{2}{2} = 1$ .

Clearly not all maps have an inverse map. But of course, if the map bijective then it have one. The idea behind finding the inverse map if it passed the tests above is very basic, *by reversing all the operations in the original map with the reverse order*. For example if you see addition reverse it by subtraction, multiplication by division, multiplication then addition by subtraction then division<sup>5</sup>.

An interesting to say, there are bunch of branches in mathematics specialized in Mapping and their types. It's a fundamental concept in modern mathematics, almost any branch in mathematics have his own functions, their types and applications.

---

<sup>4</sup>Other books maybe call the three as *one to one*, *onto*, and *one to one and onto* respectively.

<sup>5</sup>The reverse concept is very importation especially in Algebra and any algebraic system overall. We will study it widely later, so make sure you understands this section well.

## 5.4 Operations

We saw that mapping is the way to *do something*, takes one -or more than one from the same set- input and produce an output. *Operation* is similar to map, but with no restriction on the original set. Generally, an *Operation* is a map could takes different inputs from different sets – i.e. by their cross product –, and produce one output.

### 5.4.1 Abstract and Generalize

A good example for operation is the basic arithmetic operations *Addition* and *Subtraction*, you can add or subtract numbers from different sets, for example define addition operation as  $+_1 : \mathbb{Z} \times \mathbb{Q} \longrightarrow \mathbb{Q}$  or  $+_2 : V^6 \times V \longrightarrow V$ , they do the same thing, but on different sets which eventually leads to distinct results. In *Operation* we generalize our naive concept about addition and subtraction..etc to new area: It's not bounded by anything except the nature of sets elements: numbers, sets, vectors..etc. In other word, we abstract the nature of the operation and apply it to different objects.

To state the obvious,  $+_1$  will takes two numbers, one from integers the other from rational, and produce of course a rational number. But  $+_2$  even it's an addition, but on vectors instead of numbers, taking two vectors and return a new vector.

One can think of something like: *Can we takes two elements from the same set, and produce a completely different object?*. Actually, that's one of the powerful properties operation gave us. Take for example what we call in Vector Calculus the *Scalar Product* defined as  $\cdot : V \times V \longrightarrow \mathbb{R}$  which takes two vectors and return a scalar quantity can be used to answer: does they perpendicular or not?<sup>7</sup>

### 5.4.2 Operation as Algebraic System

When we equip a set  $S$  with an operation  $\cdot$  like this  $(S, \cdot)$  we create what we call a *System*. A number of elements with specific operation let us manipulate them under.

There is an interesting property if it occurs in the system, that leads to be mathematically impressive. They call it *Closure property*, and we say *the system is algebraically closed* or *the system is closed* if the operation defined takes elements from the equipped set and output an element in the same set, symbolically  $\cdot : S \times S \longrightarrow S$ <sup>8</sup>.

Whenever the system satisfying the closure property, nothing strange will appears – No solutions, results, or even proof will leads to undefined object. To

---

<sup>6</sup> $V$  refers to Vector Space.

<sup>7</sup>A famous result in Vector Calculus, states that two vectors  $a, b \in \mathbb{V}$  are perpendicular if their scalar product equal zero.

<sup>8</sup>Nice to mention that The Fundamental Theorem of Algebra states that the Complex Numbers  $\mathbb{C}$  are algebraically closed, see [8].

illustrate this, imagine you are a mathematician in the middle ages and wanted to solve the quadratic equation:

$$(1)x^2 + (0)x + (1) = 0 \implies x^2 + 1 = 0 \implies x^2 = -1$$

at that time, the Complex Numbers  $\mathbb{C}$  wasn't invented<sup>9</sup> yet. So, all solutions must be in  $\mathbb{R}$ , but there is no  $x \in \mathbb{R}$  such that  $x^2 = -1$ . The Closure property emphasize this will not happen if the system satisfy it. Moreover, if the system  $(S, \cdot)$  wasn't closed under that operation we cannot procedure for more than one operation. Since the output element of the firsts step *is not in*  $S$ <sup>10</sup>.

The closure property is not the only property for operations. There are various and several properties, like *Associativity*, *Commutativity* Its helpful when it becomes to prove something and plan a strategy.

---

<sup>9</sup>Or discovered, I don't like that byzantine discussion; Does the math invented or discovered?

<sup>10</sup>Take  $+$  :  $V \times V \longrightarrow \mathbb{R}$  as example.

## Part III

# Algebraic Structures

## 6 Algebraic Structure

We discussed the closure property, and saw what does it emphasized. Backing to the history, algebra especially, and lets start thinking again of equations in more general way. Like what if we use the concept of *Operations* instead of the elementary and naive concepts? I mean, what if we deal with *Addition* as an *Original Operation* and *Subtraction* as *Inverse Operation*? by this, we clear the vague pattern into what we call *Algebraic Structure*.

### 6.1 What is The Algebraic Structure?

The *Algebraic Structure* is an algebraic system with more generalization for the operation, and restriction conditions to hold that structure. Maybe we have an algebraic system, with algebraic structure maybe not. Moreover, the system could have only a subset holds that structure, and maybe it contains more than one structure.

In simple words: its a clear pattern frequently appears, can be defined formally using axioms, and digging into by Theorems and Lemmas. Symbolically:

**Algebraic Structure.** Let  $(S, \cdot)$  be an algebraic system, and  $\{P_1(x), P_2(x), \dots\}$  be the set of axioms define a structure. We say  $(S, \cdot)$  is an *Algebraic Structure or Structure* if and only if the system satisfy the set of axioms – i.e None of them have *False* as truth value.

### 6.2 The Benefit of Studying Algebraic Structure

The main idea behind structures is to develop a deep understanding of a general system rather than a special one. Every structure has a huge Theory contains its proved theorems and properties, so if the algebraic system satisfies the structure definition, we directly apply it and know the system properties. Only by checking the definition!

After learning one or two structures, it will become clear why we care so much about, and how it can expand our research to new areas sometimes we couldn't expect it. Let's dive into it!

## 7 Groups

### 7.1 Prologue

Look at the integer set  $\mathbb{Z}$ , look into it again with the addition. Again, look and think about the behavior of 0 with them. In school, we learned the natural numbers  $\mathbb{N}$  then the integers  $\mathbb{Z}$ , the Group structure is the evolution to the next stage. It takes the properties of the system  $(\mathbb{Z}, +)$  to the next level. Abstracted it, with elegancy.

#### 7.1.1 Symmetry, The Shape of Nature

Newton in his third law states a beautiful way for looking over the nature, he extended the quantity with reversing the direction. The same thing, but in the opposite direction and if they combined together we have the nothing: Zero. This is symmetry. This is what Group Structure orchestrate<sup>11</sup>.

### 7.2 Group, Formally

$(G, \cdot)$  is Group if and only if:

- $(G, \cdot)$  is closed system.
- The operation  $\cdot$  Associative:  $a \cdot (b \cdot c) = (a \cdot b) \cdot c$  for all  $a, b, c \in G$ . In simple words: The order of applying the operation doesn't matter.
- There exist an element  $e \in G$  such that  $g \cdot e = e \cdot g = g$  for all  $g \in G$ . In simple words:  $e$  doesn't affect or effect under the operation. We call  $e$  the *Identity* element.
- For all  $g \in G$ , there exist another  $g_1 \in G$  such that  $g \cdot g_1 = g_1 \cdot g = e$ , In simple words: They reverse each other under the operation, to produce the nothing: Identity. We call  $g_1$  the *Inverse* of  $g$  and denote it by  $g^{-1}$ .

A clear and perfect example for Group is  $(\mathbb{Z}, +)$ :  $e = 0$ , pick any  $z \in \mathbb{Z}$ , for example  $z = 2$ , then  $z^{-1} = -2 \in \mathbb{Z}$ , calculate  $z + z^{-1} = 2 + -2 = (e = 0) = -2 + 2 = z^{-1} + z = e$ <sup>12</sup>.

Simply, Group is the mathematical formalization of symmetry, by this formalization we can obtain important results about Counting, Substructures, Existence and Uniqueness, and so on.<sup>13</sup>

---

<sup>11</sup>Well, The Standard Model also [11].

<sup>12</sup>I will not prove anything in this booklet, the reader can go to [5], and [2] for advance.

<sup>13</sup>I will not go further, If the reader has a potential interest in Group Theory, I recommend reading [5] it's a well written introduction for it.

## 8 Rings

### 8.1 Prologue

Until now, we worked on a system with one operation. Rings, unlike Group it has two equipped operations. Essentially, it developed to generalize two main ideas: number of operations, and Addition with Multiplication idea, especially the second, its the abstraction of them. As in [3] they name it "Ring" because of that closure property, with circulation. Rings is important in studying Polynomials<sup>14</sup>, Algebraic Geometry, and a variant of subjects.

Since Rings as mentioned has two operation, we have to be careful about their relationship. We will see how it should be.

### 8.2 Rings, Formally

The axioms of Rings can be divided into three parts: axioms for Addition, Multiplications, and their relationship.

We say  $(R, +, \cdot)$  is a Ring, if it satisfy:

- $+$  axioms:
  - $(R, +)$  is Group.
  - And for all  $a, b \in R$ :  $a + b = b + a$ <sup>15</sup>.
- $\cdot$  axioms:
  - For any  $a, b, c \in R$ :  $a \cdot (b \cdot c) = (a \cdot b) \cdot c$  – Associativity of  $\cdot$ , the order doesn't matter.
- $+, \cdot$  relationship axioms:
  - For any  $a, b, c \in R$ :  $a \cdot (b + c) = a \cdot b + a \cdot c$  – Right Distributivity.
  - For any  $a, b, c \in R$ :  $(a + b) \cdot c = a \cdot c + b \cdot c$  – Left Distributivity.

In simple words: A structure, you can add, subtract, multiply in it, and the multiplication can be distributed on the addition. A good example for it is  $(\mathbb{Z}, +, \cdot)$  with the arithmetic addition and multiplication, you can try and prove it.

I can see Rings as an abstraction of Real Line, you can go far away either left or right, slowly by addition, quickly by multiplication, hurry by distributivity, and reverse the direction using subtraction. But wait, why we don't see division? the answer, is because of "Gaps" caused by Undefined Division, like  $\frac{1}{0}$ . Fortunately, There is a special type of Rings, called *Division Ring* which the division operation is possible, since for every  $a \in R$ , there exist multiplicative inverse  $a^{-1} \neq 0$  such that  $aa^{-1} = a^{-1}a = 1$  where 1 is the multiplicative identity.

---

<sup>14</sup>Recall Polynomial formula:  $a_n x^n + a_{n-1} x^{n-1} + \dots + a_0 x^0$

<sup>15</sup>If any Group satisfy this property, we call it *Commutative Group* or *Abelian Group*.



Using this formalization, we can derive special types or Rings like *Division Ring*, lets illustrate it:

1. First we have *Rings*.
  - (a) If it has a Multiplicative Identity not equal to zero, we call it *Ring with Identity*.
    - i. If it Ring with Identity, and every nonzero element has a multiplicative inverse, we call it *Division Ring*.
  - (b) If for every two element in the Ring,  $ab = ba$ , we call it *Commutative Ring*.
  - (c) If it (a.i)– Ring with Identity and (b)– Commutative Ring, we call it *Integral Domain*<sup>16</sup>.
2. Lastly, we have *Fields*, the next structure we will introduce. A Ring is Field, if and only if it's *Integral Domain* and *Division Ring*.

This derivation could be ambiguous right now, but we will light it up later. Looking clearly to the beauty of mathematics.

## 9 Fields

### 9.1 Prologue

The end of the last section was tricky, and it was intended for a purpose. Fields are very related to Rings, it developed over Rings, unlike the relationship between Rings and Groups. Every Field is a Ring with certain restriction conditions.

Mainly, Fields developed to solve polynomials equations, side by side with Galois Theory, and other theories developed to solve polynomials equations with degrees 4,5, and more. But, I would rather -and prefer- to introduce it as a geometric concept instead of an algebraic. Why? I think its properties have geometric richness over algebraic. Even if we introduced the *extension* idea, it's clear that "Bigger"<sup>17</sup> is what you have to pass through, needless to mention the relationship between the degree of the extension field and Vector Space.

Fields, as far as I can see, is the new form of the connected line between Numbers and Geometry, Discrete and Continues, a new and more abstracted form of  $xy$ -plane. Usually, we use  $\mathbb{R}$  with simple  $xy$ -plane, now we use Field  $\mathbb{F}$  with a set of vectors  $V$  to define a Vector Space  $\mathbb{V} = (V, \mathbb{F})$  – The generalization of  $xy$ -plane.

---

<sup>16</sup>To understands the meaning behind *Integral Domain*, I refer the reader to this glamorous explanation [1].

<sup>17</sup>For example,  $\mathbb{C}$  is the extension field of  $\mathbb{R}$ , which can be represented by  $0i + x, x \in \mathbb{R}$  which is a line in the Complex Plane, the same for  $\mathbb{Q}$  with respect to  $\mathbb{R}$ , it's a line with "gap points – irrationals",  $\mathbb{R}$  is the extension field of  $\mathbb{Q}$ .

## 9.2 Fields, Formally

We already defined Fields using Rings. However, in mathematics we can always do the same job with a different approach. Here, we will define Fields by axioms instead of Rings with restricted conditions<sup>18</sup>.

Lets say we have a system  $(F, +, \cdot)$ , we call it *Field* if and only if:

- Axioms for  $(F, +)$ :
  1.  $(F, +)$  form Abelian Group.
- Axioms for  $(F, \cdot)$ :
  1.  $\cdot$  is Associative.
  2.  $\cdot$  is Commutative.
  3. There exist  $0 \neq 1 \in F$  such that  $1a = a1 = a$  for any  $a \in F$ .
  4. There exist  $a^{-1} \in F$  such that  $a^{-1}a = aa^{-1} = 1$  for any  $0 \neq a \in F$ .
- Axioms for the relation between  $+$  and  $\cdot$ :
  1.  $1 \neq 0$  – The addition and multiplication identities are distinct.
  2. The multiplication is distributed over addition.

That's it! It's a system, where you can add, subtract, multiply, and divide.

---

<sup>18</sup>Ring, satisfying Integral Domain and Division Ring conditions.

## References

- [1] Dan Bach. *Where does the term Integral Domain come from?* Mathematics Stack Exchange. eprint: <https://math.stackexchange.com/q/46944>. URL: <https://math.stackexchange.com/q/46944>.
- [2] Alan Beardon. *Algebra and geometry*. Cambridge, UK New York: Cambridge University Press, 2005. ISBN: 0521890497.
- [3] Bill Dubuque. *Why are rings called rings?* Mathematics Stack Exchange. eprint: <https://math.stackexchange.com/q/61505>. URL: <https://math.stackexchange.com/q/61505>.
- [4] Euclid. *The Elements of Euclid*. Ed. by Sir Thomas L. Heath. 2nd. New York: Dover Publications Inc., 1956. URL: [https://archive.org/details/euclid\\_heath\\_2nd\\_ed](https://archive.org/details/euclid_heath_2nd_ed).
- [5] John Fraleigh. *A first course in abstract algebra*. Boston: Addison-Wesley, 2003. ISBN: 0201763907.
- [6] Steven Krantz. *An episodic history of mathematics : mathematical culture through problem solving*. Washington, DC: Mathematical Association of America, 2010. ISBN: 978-0883857663.
- [7] G. Polya. *How to Solve It*. Princeton University Press, Nov. 1971. ISBN: 0691023565. URL: <http://www.amazon.com/exec/obidos/redirect?tag=citeulike07-20%5C&path=ASIN/0691023565>.
- [8] Wikipedia contributors. *Fundamental theorem of algebra* — *Wikipedia, The Free Encyclopedia*. [https://en.wikipedia.org/w/index.php?title=Fundamental\\_theorem\\_of\\_algebra&oldid=1023272575](https://en.wikipedia.org/w/index.php?title=Fundamental_theorem_of_algebra&oldid=1023272575). [Online; accessed 17-August-2021]. 2021.
- [9] Wikipedia contributors. *Lattice (order)* — *Wikipedia, The Free Encyclopedia*. [https://en.wikipedia.org/w/index.php?title=Lattice\\_\(order\)&oldid=1038741711](https://en.wikipedia.org/w/index.php?title=Lattice_(order)&oldid=1038741711). [Online; accessed 14-August-2021]. 2021.
- [10] Wikipedia contributors. *List of order theory topics* — *Wikipedia, The Free Encyclopedia*. [https://en.wikipedia.org/w/index.php?title=List\\_of\\_order\\_theory\\_topics&oldid=945896905](https://en.wikipedia.org/w/index.php?title=List_of_order_theory_topics&oldid=945896905). [Online; accessed 14-August-2021]. 2020.
- [11] Wikipedia contributors. *Mathematical formulation of the Standard Model* — *Wikipedia, The Free Encyclopedia*. [https://en.wikipedia.org/w/index.php?title=Mathematical\\_formulation\\_of\\_the\\_Standard\\_Model&oldid=1038581383](https://en.wikipedia.org/w/index.php?title=Mathematical_formulation_of_the_Standard_Model&oldid=1038581383). [Online; accessed 19-August-2021]. 2021.