Set, Group, Field and Ring Theory

Contents

Part I

Introduction

Chapter 1

History

Part II

Method

Chapter 2

Basics

2.1 Simple Sets

A collection of objects is defined as a Set. The objects have to be distinct and a set is an object itself.

Notation

We demonstrate a set with the following notation called Roster Notation:

$$S = \{1, 2, 3\} \tag{2.1}$$

This is useful for small finite sets, but many descriptions will use Set-builder Notation:

$$S = \{n | n \mod 2 = 0, 0 < n < 21\} \tag{2.2}$$

Which describes all the even numbers between 0 and 21.

Membership

If we have an element of a set we describe it as a member and use the following notation:

$$x \in B \tag{2.3}$$

We can also describe exclusion from a set:

$$x \notin B \tag{2.4}$$

Subset

Further to membership we can compare two sets and determine whether one set is contained within another. Meaning each individual element of set B is at least in the set A. A 'Proper Subset' is described where a subset is not equal to the other set.

$$\{1, 2, 3\} \subset \{1, 2, 3, 4\} \tag{2.5}$$

$$\{1, 2\} \subseteq \{1, 2\} \tag{2.6}$$

Power Set

A power set is the set of all subsets of a set.

$$S = \{1, 2, 3\}$$

$$P(S) = \{\{\varnothing\}, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\} \tag{2.7}$$

Cardinality

For a set S, the cardinality is the number of members of S.

$$|S| = 3$$

$$|P(S)| = 8$$

2.2 Special Sets

$\mathbb{P}$ the set of all primes
$\mathbb{N}$ the set of all natural numbers
$\mathbb{Z}$ the set of all integers
$\mathbb{Q}$ the set of all rational numbers
$\mathbb{R}$ the set of all real numbers
$\mathbb{C}$ the set of all complex numbers
$\mathbb{H}$ the set of all quaternions

2.3 Basic Operations

Unions

A union of sets is the set formed by all elements in each set.
Denoted by A $\cup$ B

Intersections

The intersection of sets is the set formed by the common elements in all sets.
Denoted by A $\cap$ B

Complements

A complement is the subtraction of all elements in one set from another.
Denoted by A $\setminus$ B

Cartesian

The Cartesian is the set formed by associating every element in one set with every element of the other set.
Denoted by A $\times$ B

Chapter 3

Group Theory

3.1 Groups

A Group is a Set equipped with a single operation that combines two elements to form a third that fulfills a series of axioms.

Notation

We demonstrate a group with the following notation:

$$G = (S, +) \tag{3.1}$$

Which a Set S with the addition operation to form Group G.

3.1.1 Axioms

To qualify as a group it needs to fulfill the following series of axioms.

Closure

For any two elements in G, the result of the operation is also in G.

$$a \cdot b \in G \ \forall \ a, b \in G \tag{3.2}$$

Associativity

$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \ \forall \ a, b, c \in G \tag{3.3}$$

Identity element

There exists an element in the group such that applying the operation with it against other elements equals that element.

$$\exists \ i \in G \ s.t. a \cdot i = a \tag{3.4}$$

Inverse element

For each element in the group there is another element that when acted together with the operation equals the identity element.

$$\forall\ a \in G\ \exists\ a^{-1} \in\ Gs.t. a \cdot a^{-1} = i \tag{3.5}$$

3.1.2 Abelian Group

A group is considered abelian if the operation is commutative

$$\forall\ a, b \in G\ a \cdot b = b \cdot a \tag{3.6}$$

3.1.3 Theorems

3.1.4 Homomorphism

Given two groups (G, $*$) and (H, $\cdot$) a group homomorphism is a function defined as h : G $\rightarrow$ H such that:

$$\forall\ u, v \in G,\ h(u * v) = h(u) \cdot h(v) \tag{3.7}$$

Kernel

The kernel of a homomorphism is the set of elements in G that are mapped to the identity in H

Chapter 4

Ring Theory

4.1 Rings

4.1.1 Axioms

The following ring axioms must be satisfied to qualify as a ring

Abelian group under addition

$$\forall\ a, b, c \in R\ (a + b) + c = a + (b + c) \tag{4.1}$$

$$a + b = b + a \tag{4.2}$$

$$\exists\ 0\ \in R\ s.t.\ a + 0 = a \tag{4.3}$$

$$\exists - a\ \in R\ s.t.\ a + (-a) = 0 \tag{4.4}$$

Monoid under addition

$$\forall\ a, b, c \in R\ a \cdot (b \cdot c) = (a \cdot b) \cdot c \tag{4.5}$$

$$\exists\ 1 \in R\ s.t.\ a \cdot 1 = 1 \cdot a = a \tag{4.6}$$

Existence of a unity element for multiplication is sometimes optional for definitions of a ring

Distributivity of multiplication with respect to addition

$$a \cdot (b + c) = a \cdot b + a \cdot c \tag{4.7}$$

$$(b + c) \cdot a = b \cdot a + c \cdot a \tag{4.8}$$

4.1.2 Commutative Ring

When the $\cdot$ operation is commutative then R is said to be a *Commutative Ring* or *Abelian Ring*

4.1.3 Examples

Infinite set of integers $\mathbb{Z}$

4.1.4 Subring

Let (R,+,x) be a ring and S a non-empty subset of R. If S still fulfills the ring axioms it is a sub-ring of R. R is also said to be a ring extension of S.

The trivial subring of R is S = {0}. If a subring is different to R it is called a proper sub-ring of R.

4.1.5 Ideal

Let R be a commutative ring, an Ideal is a non empty subset I.

(I , +) is a sub-group of (R , +)

I is stable if

$$\forall\ i \in I, r \in R, i * r \in I \tag{4.9}$$

I is a Proper Ideal if I $\neq$ R

Maximal Ideal

For an ideal I of ring R

$$s.t \nexists\ I' \subseteq I \tag{4.10}$$

where I' is a distinct ideal of R

Principal Ideal

$$I = aR = \{a * x \mid x \in R\} \tag{4.11}$$

4.1.6 Homomorphism

https://www.youtube.com/watch?v=neQm8x0iJZk

4.1.7 Quotient Ring

Let I be a proper Ideal of R. The quotient group R/I is formed of elements of the cosets (r + I) of R with respect to I

$$(r + I) \in I\ \{r + i \mid i \in I\} \tag{4.12}$$

Which can also form a quotient ring

$$(r + I) \oplus (s + I) = (r + s + I) \tag{4.13}$$

$$(r + I) \otimes (s + I) = (r * s + I) \tag{4.14}$$

(r $\in$ R, s $\in$ R) denoted by (R/I, $\oplus$, $\otimes$) or R/I

Chapter 5

Field Theory

5.1 Fields

A field is a set on which addition, subtraction, multiplication and division are defined and behave as the corresponding operations on rational and real numbers do

5.1.1 Axioms

The following field axioms must be satisfied to qualify as a field

Associativity of addition and multiplication

$$(a+b)+c = a+(b+c) \ \forall \ a,b,c \in F \tag{5.1}$$

$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \ \forall \ a,b,c \in F \tag{5.2}$$

Commutativity of addition and multiplication

$$a+b = b+a \ \forall \ a,b \in F \tag{5.3}$$

$$a \cdot b = b \cdot a \ \forall \ a,b \in F \tag{5.4}$$

Additive and multiplicative identity

$$\exists \ c,d \in F, \ c \ / \ d \ s.t. \ a+c = a \ , \ b \cdot d = b \tag{5.5}$$

Additive inverse

$$\exists \ a, a^{-1} \in F \ s.t. \ a + a^{-1} = 0 \tag{5.6}$$

Multiplicative inverse

$$\exists \ a, a^{-1} \in F \ s.t. \ a \cdot a^{-1} = 1 \tag{5.7}$$

Distributivity of multiplication over addition

$$\forall \ a,b,c \in F \ a \cdot (b+c) = a \cdot b + a \cdot c \tag{5.8}$$