

The Incomplete Codex of Basic Mathematics  
for Computer Scientists  
From Programmers to Hackers: Mathematical Basis to Computer  
Science

None (@n0n3x1573n7)

December 19, 2018

# Chapter 1

## Introduction

Do you read me, Overleaf?

# Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
<b>I</b>	<b>Mathematical Preliminaries</b>	<b>3</b>
<b>2</b>	<b>Algebraic Structures</b>	<b>4</b>
2.1	Algebraic Structures . . . . .	4
2.1.1	Sets . . . . .	4
2.1.2	Group . . . . .	5
2.1.3	Ring . . . . .	6
2.1.4	Field . . . . .	6
2.1.5	Polynomial Ring . . . . .	7
2.2	From $\mathbb{N}$ to $\mathbb{R}$ . . . . .	7
<b>3</b>	<b>Number Theory</b>	<b>8</b>
3.1	Arithmetic . . . . .	8
3.1.1	Integer Arithmetic . . . . .	8
3.1.2	Modular Arithmetic . . . . .	8
<b>4</b>	<b>Analysis</b>	<b>9</b>
<b>5</b>	<b>Linear Algebra</b>	<b>10</b>
<b>6</b>	<b>Calculus</b>	<b>11</b>
<b>7</b>	<b>Statistics</b>	<b>12</b>
<b>8</b>	<b>Logic</b>	<b>13</b>
<b>II</b>	<b>Applications to Computer Science</b>	<b>14</b>
<b>9</b>	<b>Relational algebra</b>	<b>15</b>
<b>10</b>	<b>Automata</b>	<b>16</b>
<b>11</b>	<b>Complexity Theory</b>	<b>17</b>
11.1	test . . . . .	17
11.1.1	subtest . . . . .	17
<b>12</b>	<b>Cryptosystem</b>	<b>18</b>
12.1	Basic Terminology . . . . .	18
12.2	Symmetric-key Cryptosystems . . . . .	18
12.3	Asymmetric-key Cryptosystems . . . . .	18

## **Part I**

# **Mathematical Preliminaries**

## Chapter 2

# Algebraic Structures

### 2.1 Algebraic Structures

#### 2.1.1 Sets

**Definition 1** (Set)

A set is a collection of distinct objects.

**Definition 2** (Order)

Let  $S$  be a set. An order on  $S$  is a relation, denoted by  $<$ , with the following properties:

- If  $x \in S$  and  $y \in S$  then one and only one of the following statements is true:

$$x < y, x = y, y < x$$

- For  $x, y, z \in S$ , if  $x < y$  and  $y < z$ , then  $x < z$ .

**Remark**

- It is possible to write  $x > y$  in place of  $y < x$
- The notation  $x \leq y$  indicates that  $x < y$  or  $x = y$ .

**Definition 3** (Ordered Set)

An ordered set is a set in which an order is defined.

**Definition 4** (Bound)

Suppose  $S$  is an ordered set, and  $E \subset S$ .

If there exists  $\beta \in S$  such that  $x \leq \beta$  for every  $x \in E$ , we say that  $E$  is bounded above, and call  $\beta$  an upper bound of  $E$ . If there exists  $\alpha \in S$  such that  $x \geq \alpha$  for every  $x \in E$ , we say that  $E$  is bounded below, and call  $\alpha$  a lower bound of  $E$ .

**Definition 5** (Least Upper Bound)

Suppose that  $S$  is an ordered set, and  $E \subset S$ . If there exists a  $\beta \in S$  with the following properties:

- $\beta$  is an upper bound of  $E$
- If  $\gamma < \beta$ , then  $\gamma$  is not an upper bound of  $E$

Then  $\beta$  is called the Least Upper Bound of  $E$  or the supremum of  $E$ , denoted

$$\beta = \sup(E)$$

**Definition 6** (Greatest Lower Bound)

Suppose that  $S$  is an ordered set, and  $E \subset S$ . If there exists a  $\alpha \in S$  with the following properties:

- $\alpha$  is a lower bound of  $E$
- If  $\gamma < \alpha$ , then  $\gamma$  is not a lower bound of  $E$

Then  $\alpha$  is called the Greatest Lower Bound of  $E$  or the infimum of  $E$ , denoted

$$\beta = \inf(E)$$

**Definition 7** (least-upper-bound property)

An ordered set  $S$  is said to have the least-upper-bound property if the following is true:

if  $E \subset S$ ,  $E$  is not empty, and  $E$  is bounded above, then  $\sup(E)$  exists in  $S$ .

**Definition 8** (greatest-lower-bound property)

An ordered set  $S$  is said to have the greatest-lower-bound property if the following is true:

if  $E \subset S$ ,  $E$  is not empty, and  $E$  is bounded below, then  $\inf(E)$  exists in  $S$ .

**Theorem 1**

Suppose  $S$  is an ordered set with the least-upper-bound property,  $B \subset S$ ,  $B$  is not empty, and  $B$  is bounded below.

Let  $L$  be the set of all lower bounds of  $B$ . Then

$$\alpha = \sup(L)$$

exists in  $S$ , and  $\alpha = \inf(B)$ .

*Proof.* Note that  $\forall x \in L, y \in B, x \leq y$ .

$L$  is nonempty as  $B$  is bounded below.

$L$  is bounded above since  $\forall x \in S \setminus L, \forall y \in L, x > y$ .

Since  $S$  has the least-upper-bound property and  $L \subset S$ ,  $\exists \alpha = \sup(L)$ .

The followings hold:

- $\alpha$  is a lower bound of  $B$ .  
( $\because$ )  $\forall \gamma \in B, \gamma > \alpha$
- $\beta$  with  $\beta > \alpha$  is not a lower bound of  $B$   
( $\because$ ) Since  $\alpha$  is an upper bound of  $L$ ,  $\beta \notin L$ .

Hence  $\alpha = \inf(B)$ . □

**Corollary**

For all ordered sets, the Least Upper Bound property and the Greatest Lower Bound Property are equivalent.

**2.1.2 Group****Definition 9** (Group)

A group is a set  $G$  with a binary operation  $\cdot$ , denoted  $(G, \cdot)$ , which satisfies the following conditions:

- **Closure:**  $\forall a, b \in G, a \cdot b \in G$
- **Associativity:**  $\forall a, b, c \in G, (a \cdot b) \cdot c = a \cdot (b \cdot c)$
- **Identity:**  $\exists e \in G, \forall a \in G, a \cdot e = e \cdot a = a$

- **Inverse:**  $\forall a \in G, \exists a^{-1} \in G, a \cdot a^{-1} = a^{-1} \cdot a = e$

**Definition 10** (Semigroup)

A semigroup is  $(G, \cdot)$ , which satisfies Closure and Associativity.

**Definition 11** (Monoid)

A monoid is a semigroup  $(G, \cdot)$  which also has identity.

**Definition 12** (Abelian Group)

An Abelian Group or Commutative Group is a group  $(G, \cdot)$  with the following property:

- **Commutativity:**  $\forall a, b \in G, a \cdot b = b \cdot a$

### 2.1.3 Ring

**Definition 13** (Ring)

A Ring is a set  $R$  with two binary operations  $+$  and  $\cdot$ , often called the addition and multiplication of the ring, denoted  $(R, +, \cdot)$ , which satisfies the following conditions:

- $(R, +)$  is an abelian group
- $(R, \cdot)$  is a semigroup
- **Distribution:**  $\cdot$  is distributive with respect to  $+$ , that is,  $\forall a, b, c \in R$ :
  - $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$
  - $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$

The identity element of  $+$  is often noted 0.

**Definition 14** (Ring with identity(1))

A Ring with identity is a ring  $(R, +, \cdot)$  of which  $(R, \cdot)$  is a monoid. The identity element of  $\cdot$  is often noted 1.

**Definition 15** (Commutative Ring)

A commutative ring is a ring  $(R, +, \cdot)$  of which  $\cdot$  is commutative.

**Definition 16** (Zero Divisor)

For a ring  $(R, +, \cdot)$ , let 0 be the identity of  $+$ .

$a, b \in R$ ,  $a \neq 0$  and  $b \neq 0$ , if  $a \cdot b = 0$ ,  $a, b$  are called the zero divisors of the ring.

**Definition 17** (Integral Domain)

An integral domain is a commutative ring  $(R, +, \cdot)$  with 1 which does not have zero divisors.

### 2.1.4 Field

**Definition 18** (Field)

A Field is a set  $F$  with two binary operations  $+$  and  $\cdot$ , often called the addition and multiplication of the field, denoted  $(F, +, \cdot)$ , which satisfies the following conditions:

- $(F, +, \cdot)$  is a ring
- $(F \setminus \{0\}, \cdot)$  is a group

Alternatively, a Field may be defined with a set of Field Axioms listed below:

(A) **Axioms for Addition**

- (A1) **Closed under Addition**  
 $\forall a, b \in F, a + b \in F$
- (A2) **Addition is Commutative**  
 $\forall a, b \in F, a + b = b + a$
- (A3) **Addition is Associative**  
 $\forall a, b, c \in F, (a + b) + c = a + (b + c)$
- (A4) **Identity of Addition**  
 $\exists 0 \in F, \forall a \in F, 0 + a = a$
- (A5) **Inverse of Addition**  
 $\forall a \in F, \exists -a \in F, a + (-a) = 0$

(M) **Axioms for Multiplication**

- (M1) **Closed under Multiplication**  
 $\forall a, b \in F, a \cdot b \in F$
- (M2) **Multiplication is Commutative**  
 $\forall a, b \in F, a \cdot b = b \cdot a$
- (M3) **Multiplication is Associative**  
 $\forall a, b, c \in F, (a \cdot b) \cdot c = a \cdot (b \cdot c)$
- (M4) **Identity of Multiplication**  
 $\exists 1 \in F, \forall a \in F, 1 \cdot a = a$
- (M5) **Inverse of Multiplication**  
 $\forall a \in F \setminus \{0\}, \exists a^{-1} \in F, a \cdot a^{-1} = 1$

(D) **Distributive Law**

$\forall a, b, c \in F, (a + b) \cdot c = a \cdot c + b \cdot c$   
where  $\cdot$  takes precedence over  $+$ .

**Definition 19** (Ordered Field)

An ordered field is a field  $F$  which is an ordered set, such that

- $x + y < x + z$  if  $x, y, z \in F$  and  $y < z$
- $xy > 0$  if  $x, y \in F, x > 0$  and  $y > 0$

**Theorem 2** (Existence of  $\mathbb{R}$ )

There exists an ordered field  $\mathbb{R}$  containing  $\mathbb{Q}$  as a subfield which has the least-upper-bound property.

**Definition 20** (Extended Real Number System)

The extended real number system, denoted  $\overline{\mathbb{R}}, [-\infty, \infty]$ , or  $\mathbb{R} \cup \{-\infty, \infty\}$ , consists of the real field  $\mathbb{R}$  and two symbols,  $+\infty$  and  $-\infty$ . We preserve the original order in  $\mathbb{R}$ , and define  $\forall x \in \mathbb{R}$ ,

$$-\infty < x < \infty$$

**Remark**

The extended real number system does not form a field.

### 2.1.5 Polynomial Ring

## 2.2 From $\mathbb{N}$ to $\mathbb{R}$



## Chapter 3

# Number Theory

### 3.1 Arithmetic

#### 3.1.1 Integer Arithmetic

**Theorem 3** (Division Algorithm)

**Definition 21** (Divisibility)

**Theorem 4** (Euclidean Algorithm)

**Theorem 5** (Extended Euclidean Algorithm)

**Definition 22** (Linear Diophantine Equation)

**Theorem 6** (Solutions for Linear Diophantine Equation)

#### 3.1.2 Modular Arithmetic

**Definition 23** (Modulus)

## **Chapter 4**

# **Analysis**

## Chapter 5

# Linear Algebra

## Chapter 6

# Calculus

## **Chapter 7**

# **Statistics**

## Chapter 8

# Logic

## Part II

# Applications to Computer Science

## Chapter 9

# Relational algebra



## Chapter 10

# Automata

## Chapter 11

# Complexity Theory

### 11.1 test

#### 11.1.1 subtest

**Definition 24** (This)  
This is Sparta.

## Chapter 12

# Cryptosystem

12.1 Basic Terminology

12.2 Symmetric-key Cryptosystems

12.3 Asymmetric-key Cryptosystems