The Incomplete Codex of Basic Mathematics for Computer Scientists

From Programmers to Hackers: Mathematical Basis to Computer Science

None(@n0n3x1573n7)

December 20, 2018

Chapter 1

Introduction

Do you read me, Overleaf?

Contents

Part I

Mathematical Preliminaries

Chapter 2

Logic

Chapter 3

Algebraic Structures

3.1 Algebraic Structures

3.1.1 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 β 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 α 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:

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

Then β 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:

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

Then α 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 $\forall x \in S \backslash L, \forall y \in L, x > y$.
Since S has the least-upper-bound property and $L \subset S$, $\exists \alpha = sup(L)$.
The followings hold:

- α is a lower bound of B.
  ($\because$) $\forall \gamma \in B, \gamma > \alpha$
- β with $\beta > \alpha$ is not a lower bound of B
  ($\because$) Since α 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 Porperty are equivalent.

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

3.1.3 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.

3.1.4 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 $(R, +, \cdot)$, which satisfies the following conditions:

- $(F, +, \cdot)$ is a ring
- $(F \backslash \{0\}, \cdot)$ 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**
$\forall a \in F \backslash \{0\}, \exists a^{-1} \in F, a \cdot a^{-1} = 1$

(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.

3.1.5 Polynomial Ring

Definition 21 (Polynomial over a Ring)
A polynomial $f(x)$ over the ring $(R,+,\cdot)$ is defined as

$$f(x)=\sum_{i=0}^{\infty}a_ix^i=a_0+a_1x^1+\cdots,a_i\in R$$

where $a_i=0$ for all but finitely many values of i.
The degree of the polynomial $\deg(f)$ is defined as $\deg(f)=\max\{n|n\in\mathbb{N},a_n\neq 0\}$.
The leading coefficient of the polynomial is defined as $a_{\deg(f)}$.

Definition 22 (Addition and Multiplication of Polynomials)
Let $f(x)=\sum_{i=0}^{\infty}a_ix^i$, $g(x)=\sum_{i=0}^{\infty}b_ix^i$, $a_i,b_i\in R$ be a polynomial over the ring $(R,+,\cdot)$. Define:

$$f(x)+g(x)=\sum_{i=0}^{\infty}(a_i+b_i)x^i$$

$$f(x)g(x)=\sum_{k=0}^{\infty}(c_k)x^k \text{ where } c_k=\sum_{i+j=k}a_ib_j$$

Definition 23 (Polynomial Ring)
The set of polynomials over the ring $(R,+,\cdot)$, $R[x]=\{f(x)|f(x)$ is a polynomial over $R\}$ is called the Polynomial Ring(or Polynomials) over R.

Theorem 3 (Degree of Polynomial on Addition and Multiplication)
Let $f(x),g(x)\in R[x]$ with $\deg(f)=n$, $\deg(g)=m$.

- $0\leq\deg(f+g)\leq\max(\deg(f),\deg(g))$
- $\deg(fg)\leq\deg(f)+\deg(g)$.
  If $(R,+,\cdot)$ is an integral domain, $\deg(fg)=\deg(f)+\deg(g)$

Theorem 4 (Relationship between a Ring and its Polynomial Ring)
Let $(R,+,\cdot)$ be a ring and $R[x]$ the polynomials over R.

1. If $(R,+,\cdot)$ is a commutative ring with 1, then $(R[x],+,\cdot)$ is a commutative ring with 1.
2. If $(R,+,\cdot)$ is a integral domain, then $(R[x],+,\cdot)$ is a integral domain.

Theorem 5 (Division Algorithm for Polynomials over a Ring)
Let $(R,+,\cdot)$ be a commutative ring with 1.
Let $f(x),g(x)\in R[x]$, $g(x)\neq 0$ with the leading coefficient of $g(x)$ being invertible.
Then, $\exists!q(x),r(x)\in R[x]$ such that

$$f(x)=q(x)g(x)+r(x)$$

where either $r(x)=0$ or $\deg(r)<\deg(g)$.

Proof. Use induction on $\deg(f)$.
1. $f(x)=0$ or $\deg(f)<\deg(g)$: $q(x)=0,r(x)=f(x)$
2. $\deg(f)=\deg(g)=0$: $q(x)=f(x)\cdot g(x)^{-1},r(x)=0$
3. $\deg(f)\geq\deg(g)$:

1) Existence
Let $\deg(f)=n$, $\deg(g)=m$, $n>m$.

Suppose the theorem holds for $\deg(f) < n$.
Let $f(x) = a_0 + a_1x^1 + \cdots + a_nx^n$, $g(x) = b_0 + b_1x^1 + \cdots + b_mx^m$.
Choose $f_1(x) = f(x) - (a_nb_m^{-1})x^{n-m}g(x) \in R[x]$.
Since $\deg(f_1) < n$, $\exists q(x), r(x) \in R[x]$ so that $f_1(x) = g(x)q(x) + r(x)$, where $r(x) = 0$ or $\deg(r) < \deg(g)$.
$f_1(x) = f(x) - (a_nb_m^{-1})x^{n-m}g(x) = g(x)q(x) + r(x)$
$f(x) = g(x)((a_nb_m^{-1})x^{n-m} + q(x)) + r(x)$
Hence such pair exists.

2) Uniqueness
Suppose $f(x) = g(x)q_1(x) + r_1(x) = g(x)q_2(x) + r_2(x)$.
$g(x)(q_1(x) - q_2(x)) = r_2(x) - r_1(x)$
If $r_1 \neq r_2$, $\deg(g) > \deg(r_2 - r_1) = \deg(g(q_1 - q_2))$.
Since $\deg(g(q_1 - q_2)) \geq \deg(g)$ if $q_1 - q_2 \neq 0$, $q_1 = q_2$, but if so, $r_1 = r_2$.
If $r_1 = r_2$, trivially $q_1 = q_2$.
Hence they exist uniquely. □

3.2 From $\mathbb{N}$ to $\mathbb{R}$

Chapter 4

Number Theory

4.1 Arithmetic

4.1.1 Integer Arithmetic

Theorem 6 (Division Algorithm)

Definition 24 (Divisibility)

Theorem 7 (Euclidean Algorithm)

Theorem 8 (Extended Euclidean Algorithm)

Definition 25 (Linear Diophantine Equation)

Theorem 9 (Solutions for Linear Diophantine Equation)

4.1.2 Modular Arithmetic

Definition 26 (Modulus)

Chapter 5

Analysis

Chapter 6

Linear Algebra

Chapter 7

Calculus

Chapter 8

Statistics

Part II

Applications to Computer Science

Chapter 9

Relational algebra

Chapter 10

Automata

Chapter 11

Complexity Theory

11.1 Turing Machine and Complexity

(TODO: Before giving the definition of Turing Machine, I have to give some intuition here.)

Definition 27 (Turing machine)
A Turing machine is a tuple $M = (\Gamma, Q, \delta)$, where:

- Q is the set of states, which contains the starting state q_0 and the halting state q_F.
- Γ is the set of symbols, which contains the blank symbol $square$, and two numbers 0 and 1. Γ is called the alphabet of M.
- $\delta : Q \times \Gamma \to Q \times \Gamma \times \{L, R\}$ is the decision function.

The definition of a Turing Machine is not unique. Some definitions use multiple tapes, using one of them as the input tape that can't be modified and another as the output tape. Some has more than one halting states. Some include the "starting symbol" in the alphabet. But in general, a Turing machine starts from one state, follows the decision function every step, and halts at the halting state.

In fact, the different definitions of a Turing machine turns out to be the same, in the sense that a function $f : \{0,1\}^* \to \{0,1\}$ is computable using one definition of a Turing machine iff it is computable using another definition of a Turing Machine.

(TODO: Write something about asymptotic notation here)

Definition 28 (Asymptotic notation)
Let f and g be two functions from $\mathbb{N}$ to $\mathbb{N}$. Then we say:

- $f = O(g)$ if there is a constant c such that $f(n) \leq c \cdot g(n)$ for every sufficiently large n. That is, $n > N$ for some N.
- $f = \Omega(g)$ if $g = O(f)$.
- $f = \Theta(g)$ if $f = O(g)$ and $g = O(f)$.
- $f = o(g)$ if for every constant $c > 0$, $f(n) < c \cdot g(n)$ for every sufficiently large n.
- $f = \omega(g)$ if $g = o(f)$.

11.2 Complexity Classes

Definition 29 (P)
P is the set of boolean function computable in time $O(n^c)$ for some constant $c > 0$.

(TODO: Non-deterministic Turing Machine)
(TODO: NP)
(TODO: EXP)

11.3 Reduction

(TODO: Polynomial-time reduction)
(TODO: NP-Hard, NP-Complete)
(TODO: SAT)
(TODO: NP-Complete problems)

Chapter 12

Cryptosystem