The Incomplete Codex of Basic Mathematics for Computer Scientists

From Programmers to Hackers: Mathematical Basis to Computer Science

None(@n0n3x1573n7), jh05013(@jhznktrkstlhknm)

December 21, 2018

Chapter 1

Introduction

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.

To see some traits on sets, we literally start from nothing:

Axiom 2 (Empty Set Axiom)
There is a set containing no members, that is:

$$\exists B \text{ such that } \forall x, (x \notin B)$$

We call this set the empty set, and denote it by the symbol $\emptyset$.

We now have $\emptyset$; we now write down a few rules for how to manipulate sets.

Axiom 3 (Axiom of Extensionality)
Two sets are equal if and only if they share the same elements, that is:

$$\forall A, B[\forall z, ((z \in A) \Leftrightarrow (z \in B)) \Rightarrow (A = B)]$$

Axiom 4 (Axiom of Pairing)
Given any two sets A and B, there is a set which have the members just A and B, that is:

$$\forall A, B \exists C \forall x [x \in C \Leftrightarrow ((x = A) \vee (x = B))]$$

If A and B are distinct sets, we write this set C as $\{A, B\}$; if $A = B$, we write it as $\{A\}$.

Axiom 5 (Axiom of Union, simple version)
Given any two sets A and B, there is a set whose members are those sets belonging to either A or B, that is:

$$\forall A, B \exists C \forall x [x \in C \Leftrightarrow ((x \in A) \vee (x \in B))]$$

We write this set C as $A \cup B$.

In the simplified version of Axiom of Union, we take union of only two things, but we sometimes we want to take unions of more than two things or even more than finitely many things. This is given by the full version of the axiom:

Axiom 6 (Axiom of Union, full version)
Given any set A, there is a set C whose elements are exactly the members of the members of A, that is:

$$\forall A \exists C[x \in C \Leftrightarrow (\exists A'(A' \in A) \wedge (x \in A'))]$$

We denote this set C as

$$\bigcup_{A' \in A} A'$$

Axiom 7 (Axiom of Intersection, simple version)
Given any two sets A and B, there is a set whose members are member of both A and B, that is:

$$\forall A, B \exists C \forall x[(x \in C) \Leftrightarrow ((x \in A) \wedge (x \in B))]$$

Sometimes as union, we would want to take intersection of more than finitely many things. This is given by the full version of the axiom:

Axiom 8 (Axiom of Intersection, full version)
Given any set A, there is a set C whose elements are exactly the members of all members of A, that is:

$$\forall A \exists C \forall x[(x \in C) \Leftrightarrow (\forall A'((A' \in A) \Rightarrow (x \in A')))]$$

We denote this set C as

$$\bigcap_{A' \in A} A'$$

Axiom 9 (Axiom of Subset)
For any two sets A and B, we say that $B \subset A$ if and only if every member of B is a member of A, that is:

$$(B \subseteq A) \Leftrightarrow (\forall x(x \in B) \Rightarrow (x \in A))$$

By the Axiom of Subset we can define the power set of an any given set:

Definition 10 (Power Set)
For any set A, the <u>power set</u> of the set A, denoted $P(A)$, whose members are precisely the collection of all possible subsets of A, that is:

$$\forall A \exists P(A) \forall B((B \subseteq A) \Leftrightarrow (B \in P(A)))$$

Definition 11 (Equivalence Relation)
Let S be a set. An <u>Equivalence Relation</u> on S is a relation, denoted by ~, with the following properties, $\forall a, b, c \in S$:

- **Reflexivity** $a \sim a$
- **Symmetry** $a \sim b \Leftrightarrow b \sim a$
- **Transitivity** $(a \sim b) \wedge (b \sim c) \Rightarrow (a \sim c)$

Definition 12 (Setoid)
A <u>setoid</u> is a set in which an equivalence relation is defined, denoted $(S, \sim)$.

Definition 13 (Equivalence Class)
The equivalence class of $a \in S$ under ~, denoted $[a]$, is defined as $[a] = \{b \in S | a \sim b\}$.

Definition 14 (Order)
Let S be a set. An <u>order</u> 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 15 (Ordered Set)
An ordered set is a set in which an order is defined, denoted $(S, <)$.

Definition 16 (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 17 (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 18 (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 19 (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 20 (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 21
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 22
For all ordered sets, the Least Upper Bound property and the Greatest Lower Bound Porperty are equivalent.

3.1.2 Group

Definition 23 (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 24 (Semigroup)
A semigroup is $(G, \cdot)$, which satisfies Closure and Associativity.

Definition 25 (Monoid)
A monoid is a semigroup $(G, \cdot)$ which also has identity.

Definition 26 (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 27 (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 28 (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 29 (Commutative Ring)
A commutative ring is a ring $(R,+,\cdot)$ of which $\cdot$ is commutative.

Definition 30 (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 31 (Integral Domain)
An integral domain is a commutative ring $(R,+,\cdot)$ with 1 which does not have zero divisors.

3.1.4 Field

Definition 32 (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 33 (Ordered Field)
An ordered field is a field F which is an ordered set, such that the order is compatible with the field operations, that is:

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

3.1.5 Polynomial Ring

Definition 34 (Polynomial over a Ring)
A polynomial $f(x)$ over the ring $(R, +, \cdot)$ is defined as

$$f(x) = \sum_{i=0}^{\infty} a_i x^i = a_0 + a_1 x^1 + \cdots, a_i \in R$$

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

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

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

Definition 36 (Polynomial Ring)
The set of polynomials over the ring $(R, +, \cdot)$, $R[x] = \{f(x) | f(x) \text{ is a polynomial over } R\}$ is called the Polynomial Ring(or Polynomials) over R.

Theorem 37 (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 38 (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 39 (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. $\square$

Chapter 4

Number Theory

4.1 Arithmetic

4.1.1 Integer Arithmetic

Theorem 40 (Division Algorithm)

Definition 41 (Divisibility)

Theorem 42 (Euclidean Algorithm)

Theorem 43 (Extended Euclidean Algorithm)

Definition 44 (Linear Diophantine Equation)

Theorem 45 (Solutions for Linear Diophantine Equation)

4.1.2 Modular Arithmetic

Definition 46 (Modulus)

Chapter 5

Analysis

Chapter 6

Linear Algebra

Chapter 7

Calculus

Chapter 8

Statistics

Chapter 9

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

9.1 $\mathbb{N}$: The set of Natural Numbers

9.1.1 Construction of $\mathbb{N}$

We start from the Axioms of Set and the following definitions:

Definition 47 (Successor)
For any set x, the successor of x, denoted $\sigma(x)$, is defined as the following set:

$$\sigma(x) = x \cup \{x\}$$

Let us define $0 = \emptyset$, $1 = \sigma(\emptyset) = \sigma(0)$. Using the definition of successors, and following the pattern, $2 = \sigma(1)$, $3 = \sigma(2)$, and so on. Basically we can make any finite number using the definition of successor and the Axioms of Set, but actually getting all of the natural numbers at once(or any infinitely large set, since only the empty set is guaranteed to exist by the axioms) is not possible with our axioms. We define the concept of Inductive Sets and make another Axiom for this purpose:

Definition 48 (Inductive Set)
A set A is called inductive if it satisfies the following two properties:

- $\emptyset \in A$
- $(x \in A) \Rightarrow (\sigma(x) \in A)$

Axiom 49 (Axiom of Infinity)
There is an inductive set, that is:

$$\exists A(\emptyset \in A) \wedge (\forall x \in A, \sigma(x) \in A)$$

Theorem 50
Take any two inductive sets, S and T. Then, $S \cap T$ is also an inductive set.

Proof. Let $U = S \cap T$.

1. $\emptyset \in U$

   $\emptyset \in S$ and $\emptyset \in T$ since S and T are both inductive.

2. $(x \in U) \Rightarrow (\sigma(x) \in U)$

   $\forall x \in U, (x \in S) \wedge (x \in T)$.
   Since S and T are both inductive, $(\sigma(x) \in S) \wedge (\sigma(x) \in T)$
   Therefore $\sigma(x) \in U$.

Therefore U is inductive. $\square$

Corollary 51
An intersection of any number of inductive sets is inductive.

Theorem 52
For any inductive set S, define N_S as follows:

$$N_S = \bigcap_{\substack{A \subseteq S \\ A \text{ is inductive}}} A$$

Take any two inductive sets, S and T. Then $N_S = N_T$.

Proof. Suppose not; WLOG, $\exists x$ such that $x \in N_S$ and $x \notin N_T$.
Let $X = N_S \cap N_T$. Then X is inductive, $X \subset N_S$, and $x \notin X$.
Since by the definition of N_S, $N_S = X \cap N_S$, but $x \notin X \cap N_S$ hence the RHS and the LHS are different.
Therefore the assumption is wrong; therefore $N_S = N_T$. $\square$

Using this theorem, we can finally define the set of natural numbers:

Definition 53 (The Set (N) of natural numbers)
Take any inductive set S, and let

$$N = \bigcap_{\substack{A \subseteq S \\ A \text{ is inductive}}} A$$

This set is the natural numbers, which we denote as $\mathbb{N}$.

9.1.2 Operations on $\mathbb{N}$

We now define two operations on $mathbbN$, addition$(+)$ and multiplication$(\cdot)$.

Definition 54 (Addition and Multiplication on $\mathbb{N}$)
The operation of addition, denoted by $+$, is defined by following two recursive rules:

1. $\forall n \in \mathbb{N}, n + 0 = n$
2. $\forall n, m \in \mathbb{N}, n + \sigma(m) = \sigma(n + m)$

Similarly the operation of multiplication, denoted by $\cdot$, is defined by following two recursive rules:

1. $\forall n \in \mathbb{N}, n \cdot 0 = 0$
2. $\forall n, m \in \mathbb{N}, n \cdot \sigma(m) = n \cdot m + n$

Lemma 55 (Operations on 0)
$\forall x \in \mathbb{N}$

- $x + 0 = 0 + x$
- $x \cdot 0 = 0 \cdot x$

Proposition 56 (Properties of $+$ and $\cdot$)
$\forall x, y, z \in \mathbb{N}$,

- **Associativity of Addition** $x + (y + z) = (x + y) + z$
- **Commutativity of Addition** $x + y = y + x$

- **Associativity of Multiplication** $x \cdot (y \cdot z) = (x \cdot y) \cdot z$
- **Commutativity of Multiplication** $x \cdot y = y \cdot x$
- **Distributive Law** $x \cdot (y + z) = x \cdot y + x \cdot z$
- **Cancellation Law for Addition** $x + z = y + z \Rightarrow x = y$

9.1.3 Ordering on $\mathbb{N}$

Definition 57 (Ordering on $\mathbb{N}$)
For $n, m \in \mathbb{N}$, we say that n is less than m, written $n \geq m$, if there exists a $k \in \mathbb{N}$ such that $m = n + k$. We also write $n < m$ if $k \neq 0$.

Theorem 58
$(N, <)$ is an ordered set[15].

Proposition 59
The followings are true:

- If $n \neq 0$, then $0 < n$.
- Let $x, y, z \in \mathbb{N}$. Then the followings are true:
  - $(x \leq y) \wedge (y < z) \Rightarrow (x < z)$
  - $(x < y) \wedge (y \leq z) \Rightarrow (x < z)$
  - $(x \leq y) \wedge (y \leq z) \Rightarrow (x \leq z)$
  - $(x < y) \Rightarrow (x + z < y + z)$
  - $(x < y) \Rightarrow (xz < yz)$
- $\forall n \in \mathbb{N}, n \neq n + 1$
- $\forall n, k \in \mathbb{N}, k \neq 0, n \neq n + k$

Definition 60 (Least Element)
Let $S \subset \mathbb{N}$. An element $n \in S$ is called a least element if $\forall m \in S, n \leq m$

Proposition 61 (Uniqueness of the Least Element)
Let $S \subset \mathbb{N}$. Then if S has a least element, then it is unique.

Theorem 62 (Well-Ordering Property)
Let S be a nonempty subset of $\mathbb{N}$. Then S has a least element.

Note
The well-ordering property states that the set of natural numbers $\mathbb{N}$ has the greatest lower bound property[20] and thereby theorem 21, has the least upper bound property[19].

9.1.4 Properties of $\mathbb{N}$

Many of the mathematics book defines the set of Natural Numbers as the set satisfying the Peano Axioms.

Proposition 63 (Peano Axioms)

1. 0, which we defined as the empty set $\emptyset$, is a natural number.
2. There exist a distinguished set map $\sigma : \mathbb{N} \to \mathbb{N}$
3. σ is injective

4. There does not exist an element $n \in \mathbb{N}$ such that $\sigma(n) = 0$
5. (Principle of Induction) If $S \in N$ is inductive, then $S = N$.

Proposition 64
Suppose that a is a natural number, and that $b \in a$. Then $b \subseteq a$, $a \nsubseteq b$.

Proposition 65
For any two natural numbers $a, b \in \mathbb{N}$, if $\sigma(a) = \sigma(b)$, then $a = b$.

Lemma 66
If $n \in \mathbb{N}$ and $n \neq 0$, then there exists $m \in \mathbb{N}$ such that $\sigma(m) = n$.

9.2 $\mathbb{Z}$: The set of Integers

9.2.1 Construction of $\mathbb{Z}$

We now have the set of natural numbers, and starting there, we construct the set of integers.

Proposition 67
Define a relation $\equiv$ on $\mathbb{N} \times \mathbb{N}$ by $(a, b) \equiv (c, d)$ iff $a + d = b + c$. This relation is an equivalence relation on $\mathbb{N} \times \mathbb{N}$.

Let $\mathbb{Z}$ be the set of equivalence classes under this relation, and the equivalence class containing (a, b) be denoted by $[a, b]$.

9.2.2 Operations on $\mathbb{Z}$

Definition 68 (Addition and Multiplication on $\mathbb{Z}$)
Addition and multiplication on $\mathbb{Z}$ are defined by:

- $[a, b] + [c, d] = [a + c, b + d]$
- $[a, b] \cdot [c, d] = [ac + bd, ad + bc]$

Definition 69 (Subtraction on $\mathbb{Z}$)
Subtraction on $\mathbb{Z}$ is defined by:

$$[a, b] - [c, d] = [a, b] + [d, c]$$

9.2.3 Ordering on $\mathbb{Z}$

Definition 70 (Ordering on $\mathbb{Z}$)
Let $[a, b], [c, d] \in \mathbb{Z}$. $[a, b] < [c, d]$ iff $a + d < b + c$.

9.2.4 Property of $\mathbb{Z}$

Theorem 71 (Arithmetic Properties of $\mathbb{Z}$)

1. Addition and multiplication are well-defined.
2. Addition and multiplication have identity elements $[n, n]$ and $[n, n + 1]$, respectively.
3. Addition and multiplication are commutative and associative.
4. The distributive law holds.
5. Each element $[a, b]$ has an additive inverse $[b, a]$.

We can treat $\mathbb{N}$ to be a subset of $\mathbb{Z}$ by identifying the number n with the class $[0,n]$. Since $[0,a]+[0,b]=[0,a+b]$ and $[0,a]\cdot[0,b]=[0,ab]$, these operations mirror the corresponding operation in $\mathbb{N}$.

Given $n \in \mathbb{N}$, we write $-n$ for $[n,0]$, 0 for $[n,n]$, and 1 for $[n,n+1]$. By the fifth arithmetic property of $\mathbb{Z}$[71], this defines $-n$ to be the additive inverse of n. We also use the minus sign for subtraction; it is therefore natural to write $[a,b]$ as $b-a$.

Proposition 72
For $a,b \in \mathbb{N}$, let $-b$, a, and b be defined in $\mathbb{Z}$ as above. Then

$$a-b=a+(-b) \text{ and } -(-b)=b$$

9.3 $\mathbb{Q}$: The set of Rational Numbers

We construct the set of rational numbers from the set of integers as follows:

9.3.1 Construction of $\mathbb{Q}$

Proposition 73
Define a relation $\equiv$ on $\mathbb{Z}\times(\mathbb{Z}\backslash\{0\})$ by $(a,b)\equiv(c,d)$ iff $ad=bc$. This relation is an equivalence relation on $\mathbb{Z}\times(\mathbb{Z}\backslash\{0\})$.

Let $\mathbb{Q}$ be the set of equivalence classes under this relation, and the equivalence class containing (a,b) is denoted by a/b or $\frac{a}{b}$, and $\frac{a}{b}=\frac{c}{d}$ mean that (a,b) and (c,d) belong to the same equivalence class. Especially we write 0 and 1 to denote $\frac{0}{1}$ and $\frac{1}{1}$, respectively.

9.3.2 Operations on $\mathbb{Q}$

Definition 74 (Addition and Multiplication on $\mathbb{Q}$)
The <u>sum</u> and <u>product</u> of $\frac{a}{b},\frac{c}{d}\in\mathbb{Q}$ are defined by

$$\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd} \text{ and } \frac{a}{b}\frac{c}{d}=\frac{ac}{bd}$$

Definition 75 (Subtraction on $\mathbb{Q}$)
Subtraction on $\mathbb{Z}$ is defined by:

$$\frac{a}{b}-\frac{c}{d}=\frac{ad-bc}{bd}$$

Definition 76 (Division on $\mathbb{Q}$)
Division on $\mathbb{Z}$ is defined by:

$$\frac{a}{b}\div\frac{c}{d}=\frac{ad}{bc}$$

9.3.3 Ordering on $\mathbb{Q}$

Definition 77 (Ordering on $\mathbb{Q}$)
Let $\frac{a}{b},\frac{c}{d}\in\mathbb{Q}$. $\frac{a}{b}<\frac{c}{d}$ iff $(bd>0\wedge ad<bc)\vee(bd<0\wedge ad>bc)$.

9.3.4 Property of $\mathbb{Q}$

Theorem 78 (Arithmetic Properties of $\mathbb{Z}$)

1. Addition and multiplication are well-defined.

2. Addition and multiplication have identity elements 0 and 1, respectively.
3. Addition and multiplication are commutative and associative.
4. The distributive law holds.
5. Each element $\frac{a}{b}$ has an additive inverse $\frac{b}{a}$.

Theorem 79
$(\mathbb{Q}, +, \cdot)$ forms an ordered field.

9.4 $\mathbb{R}$: The set of Real Numbers

9.4.1 Construction of $\mathbb{R}$

Theorem 80 (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 81 (Extended Real Number System)
The extended real number system, denoted $\mathbb{R}^+$, $[-\infty, \infty]$, 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.

9.4.2 Operations on $\mathbb{R}$

9.4.3 Ordering on $\mathbb{R}$

9.4.4 Property of $\mathbb{R}$

9.5 $\mathbb{I}$: The set of Complex Numbers

9.5.1 Construction of $\mathbb{I}$

9.5.2 Operations on $\mathbb{I}$

9.5.3 Ordering on $\mathbb{I}$

9.5.4 Property of $\mathbb{I}$

Part II

Applications to Computer Science

Chapter 10

Relational algebra

Chapter 11

Automata

Chapter 12

Complexity Theory

12.1 Turing Machine and Complexity

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

Definition 82 (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 83 (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 $g = o(f)$.

12.2 Complexity Classes

Definition 84 (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)

12.3 Reduction

Is there a polynomial-time algorithm for a given decision problem? Computer scientists are interested in this question because if there is one, it is usually a small-degree polynomial like $O(n^2)$ or $O(n^5)$. Some problems have a special property that if the problem has a polynomial-time algorithm, then several other problems do.

Definition 85 (Polynomial-time Karp reduction)
A problem $A \subseteq \{0,1\}^*$ is <u>polynomial-time Karp reducible</u> to $B \subseteq \{0,1\}^*$, denoted $A \leq_p B$, if there is a polynomial-time computable function $f : \{0,1\}^* \to \{0,1\}^*$ such that for every $x \in \{0,1\}^*$, $x \in A$ iff $f(x) \in B$.

The intuitive meaning is that a problem of A can be "reduced" to a problem of B, and if we can solve B in polynomial-time, then we can solve A in polynomial-time too.

Definition 86 (NP-complete)
A problem A is <u>NP-hard</u> if every problem in **NP** is polynomial-time reducible to A, and <u>NP-complete</u> if A is NP-hard and NP.

Theorem 87 1. If $A \leq_p B$ and $B \leq_p C$, then $A \leq_p C$.

2. An NP-complete problem A is in **P** iff **P** $=$ **NP**.

3. If $A \leq_p B$ and A is NP-hard, then B is NP-hard.

Proof. (1) Let f be a reduction from A to B with polynomial time $p(n)$, and g from B to C with $q(n)$. Then $g \circ f$ is a reduction from A to C with polynomial time $q(p(n))$.

(2) Suppose A is NP-complete and in **P**. Then any problem B in **NP** can be polynomial-time reduced to A, so transitivity implies that B is polynomial-time computable. The converse is trivial.

(3) Any problem C in **NP** can be polynomial-time reduced to A. Transitivity implies that C can be polynomial-time reduced to B. □

Now the obvious question is, does such a strong problem actually exist? The answer is yes, and a lot of important problems are NP-complete.

(TODO: SAT)

Having proven that SAT is NP-hard, more problems can be proven NP-hard if we can reduce SAT to those problems in polynomial-time.

(TODO: NP-Complete problems)

Chapter 13

Graph Theory

Chapter 14

Cryptosystem