COMP0147 Discrete Mathematics for Computer Scientists Notes

Joe

April 16, 2019

Notes adapted from:

- Lecture notes by Max Kanovich and Robin Hirsch [1].
- *A First Course in Abstract Algebra* by Joseph J. Rotman [2].

Contents

1 Set Theory

1.1 Set Notations

- Set definition: $A = \{a, b, c\}$
- Set membership (element-of): $a \in A$
- Set builder notation: $\{x \mid x \in \mathbb{R} \wedge x^2 = x\}$
- Empty set: $\emptyset$

1.2 Properties

- No structure
- No order
- No copies

For example, a, b, c are references to actual objects in

$$\{a, b, c\} \Leftrightarrow \{c, a, b\} \Leftrightarrow \{a, b, c, b\}$$

1.3 Set Equality

Definition 1.3.1 (Set Equality)**.** Set $A = B$ iff:

1. $A \subseteq B \implies \forall\, x(x \in A \to x \in B)$
2. $B \subseteq A \implies \forall\, y(y \in B \to y \in A)$

Remark. $A = B \Leftrightarrow A \subseteq B \wedge B \subseteq A$

1.4 Set Operations

- *Union*: $A \cup B \coloneqq \{x \mid x \in A \vee x \in B\}$
- *Intersection*: $A \cap B \coloneqq \{x \mid x \in A \wedge x \in B\}$
- *Relative Complement*: $A \setminus B \coloneqq \{x \mid x \in A \wedge x \notin B\}$
- *Absolute Complement*: $A^c \coloneqq U \setminus A \coloneqq \{x \mid x \in U \wedge x \notin A\}$
- *Symmetric Difference*: $A \Delta B \coloneqq (A \setminus B) \cup (B \setminus A) \coloneqq (A \cup B) \setminus (A \cap B)$
- *Cartesian Product*: $A \times B \coloneqq \{(x, y) \mid x \in A \wedge y \in B\}$

1.5 Boolean Algebra

Definition 1.5.1 (De Morgan's Laws).

$$\neg(p \vee q) := \neg p \wedge \neg q \tag{1.1}$$
$$\neg(p \wedge q) := \neg p \vee \neg q \tag{1.2}$$

Definition 1.5.2 (Idempotent Laws).

$$p \vee p := p \tag{1.3}$$
$$p \wedge p := p \tag{1.4}$$

Definition 1.5.3 (Commutative Laws).

$$p \vee q := q \vee p \tag{1.5}$$
$$p \wedge q := q \wedge p \tag{1.6}$$

Definition 1.5.4 (Associative Laws).

$$p \vee (q \vee r) := (p \vee q) \vee r \tag{1.7}$$
$$p \wedge (q \wedge r) := (p \wedge q) \wedge r \tag{1.8}$$

Definition 1.5.5 (Distributive Laws).

$$p \wedge (q \vee r) := (p \wedge q) \vee (p \wedge r) \tag{1.9}$$
$$p \vee (q \wedge r) := (p \vee q) \wedge (p \vee r) \tag{1.10}$$

Definition 1.5.6 (Identity Laws).

$$p \vee \mathrm{F} := p \tag{1.11}$$
$$p \vee \mathrm{T} := \mathrm{T} \tag{1.12}$$
$$p \wedge \mathrm{T} := p \tag{1.13}$$
$$p \wedge \mathrm{F} := \mathrm{F} \tag{1.14}$$

Definition 1.5.7 (Absorption Laws).

$$p \vee (p \wedge q) := p \tag{1.15}$$
$$p \wedge (p \vee q) := p \tag{1.16}$$

Definition 1.5.8 (Implication and Negation Laws).

- *Identity*: $p \to q := \neg p \vee q$
- *Counter-example*: $\neg(p \to q) := p \wedge \neg q$
- *Equivalences*: $p \to q \to r := (p \wedge q) \to r := q\ to(p \to r)$

- *Absorption*:
  $p \to \mathrm{T} := T$
  $p \to \mathrm{F} := \neg p$
  $\mathrm{T} \to p := p$
  $\mathrm{F} \to p := T$
- *Contrapositive*: $p \to q := \neg q \to \neg p$
- *Law of Excluded Middle*:
  $p \vee \neg p := \mathrm{T}$
  $p \wedge \neg p := \mathrm{F}$
- *Double Negation*: $\neg\neg p := p$
- *Reduction to Absurdity*: $\neg p \to \mathrm{F} := p$

1.6 Set Algebra

Definition 1.6.1 (De Morgan's Laws).

$$(A \cup B)^c := A^c \cap B^c \tag{1.17}$$
$$(A \cap B)^c := A^c \cup B^c \tag{1.18}$$

Definition 1.6.2 (Idempotent Laws).

$$A \cup A := A \tag{1.19}$$
$$A \cap A := A \tag{1.20}$$

Definition 1.6.3 (Commutative Laws).

$$A \cup B := B \cup A \tag{1.21}$$
$$A \cap B := B \cap A \tag{1.22}$$

Definition 1.6.4 (Associativity Laws).

$$A \cup (B \cup C) := (A \cup B) \cup C \tag{1.23}$$
$$A \cap (B \cap C) := (A \cap B) \cap C \tag{1.24}$$

Definition 1.6.5 (Distributive Laws).

$$A \cap (B \cup C) := (A \cap B) \cup (B \cap C) \tag{1.25}$$
$$A \cup (B \cap C) := (A \cup B) \cap (B \cup C) \tag{1.26}$$

Definition 1.6.6 (Identity Laws).

$$A \cup \emptyset := A \tag{1.27}$$
$$A \cap \emptyset := \emptyset \tag{1.28}$$
$$A \cap U := A \tag{1.29}$$
$$A \cup U := U \tag{1.30}$$

Definition 1.6.7 (Absorption Laws).

$$A \cup (A \cap B) \coloneqq A \tag{1.31}$$
$$A \cap (A \cup B) \coloneqq A \tag{1.32}$$

Definition 1.6.8 (Difference Identity Laws).

$$C \setminus (A \cup B) \coloneqq (C \setminus A) \cap (C \setminus B) \tag{1.33}$$
$$C \setminus (A \cap B) \coloneqq (C \setminus A) \cup (C \setminus B) \tag{1.34}$$

Definition 1.6.9 (Complement-Difference Identity Law).

$$C \setminus D \coloneqq C \cap D^c \tag{1.35}$$

Definition 1.6.10 (Double Complement Law).

$$(D^c)^c \coloneqq D \tag{1.36}$$

Definition 1.6.11 (Contraposition).

$$C \subseteq D \Leftrightarrow D^c \subseteq C^c \tag{1.37}$$
$$C = D \Leftrightarrow C^c = D^c \tag{1.38}$$

Definition 1.6.12 (Arbitrary Union).
Given sets $A_1, A_2, \ldots, A_n$ where $I = \{1, 2, \ldots, n\}$

$$A_1 \cup A_2 \cup \cdots \cup A_n \coloneqq \bigcup_{i \in I} A_i \tag{1.39}$$

Then

$$x \in \bigcup_{i \in I} A_i \Leftrightarrow \exists\, i \in I : x \in A_i \tag{1.40}$$

Definition 1.6.13 (Arbitrary Intersection).
Given sets $A_1, A_2, \ldots, A_n$ where $I = \{1, 2, \ldots, n\}$

$$A_1 \cap A_2 \cap \cdots \cap A_n \coloneqq \bigcap_{i \in I} A_i \tag{1.41}$$

Then

$$x \in \bigcap_{i \in I} A_i \Leftrightarrow \forall\, i \in I : x \in A_i \tag{1.42}$$

2 Functions

2.1 Function Basics

Definition 2.1.1 (Function). A function f is a mapping from X to Y

$$f\colon X \mapsto Y \tag{2.1}$$

- $\mathrm{domain}(f) = X$
- $\mathrm{image}(f) = f(X)$

Definition 2.1.2 (Total Function). A function is *total* if

$$\mathrm{domain}(f) = X \tag{2.2}$$

Definition 2.1.3 (Partial Function). A function is *partial* if

$$\mathrm{domain}(f) \subseteq X \tag{2.3}$$

Definition 2.1.4 (Surjection). A function $f\colon X \mapsto Y$ is *surjective* iff

$$f(X) = Y \Leftrightarrow \forall\, y \in Y\colon\ \exists\, x \in X\colon\ f(x) = y \tag{2.4}$$

Namely each $y \in Y$ has a corresponding $x \in X$.

Definition 2.1.5 (Injection (Encodings, One-to-one)). A function $f\colon X \mapsto Y$ is *injective* iff

$$\forall\, x_1, x_2 \in X\colon\ x_1 \neq x_2 \rightarrow f(x_1) \neq f(x_2) \tag{2.5}$$

$$\Leftrightarrow \forall\, x_1, x_2 \in X\colon\ f(x_1) = f(x_2) \rightarrow x_1 = x_2 \tag{2.6}$$

Namely each distinct element $x \in X$ maps to a different element in Y.

Definition 2.1.6 (Bijection). A function $f\colon X \mapsto Y$ is *bijective* iff f is both *injective* and *surjective*.

$$\mathrm{Bijective}(f) := \mathrm{Injective}(f) \wedge \mathrm{Surjective}(f) \tag{2.7}$$

The *inverse bijection* $f^{-1}\colon Y \mapsto X$ does exist.

2.2 Composition of Injections

Proposition 2.2.1 (Composition of Injection)**.** Given *injections* $f\colon X \mapsto Y$ and $g\colon Y \mapsto Z$, then their *composition* $h\colon X \mapsto Z$ is given by

$$h(x) = g(f(x)) \tag{2.8}$$

Then h is also an *injective* function. Namely $h = g \circ f$ where h is composed from g and f with f applied first.

Proof. Given any $x_1, x_2 \in X$ where $x_1 \neq x_2$, then

$$f(x_1) \neq f(x_2) \tag{2.9}$$

as f is *injective*, and thus

$$h(x_1) = g(f(x_1)) \neq g(f(x_2)) = h(x_2) \tag{2.10}$$

h is *injective* consequently. ■

2.3 Composition of Surjection

Proposition 2.3.1 (Composition of Surjection)**.** Given *surjections* $f\colon X \mapsto Y$ and $g\colon Y \mapsto Z$, then their *composition* $h\colon X \mapsto Z$ is given by

$$h(x) = g(f(x)) \tag{2.11}$$

Then h is also a *surjective* function.

Proof. To prove $h\colon X \mapsto Z$ is *injective*, it is required to prove that

$$\forall\, z \in Z\colon\ \exists\, x \in X\colon h(x) = z \tag{2.12}$$

Where $h(x) \Leftrightarrow (g \circ f)(x) \Leftrightarrow g(f(x))$.

Given any element $z \in Z$ ($\forall\, z \in Z$):

1. That $g\colon Y \mapsto Z$ is *surjective* by definition, then $\exists\, y \in Y\colon g(y) = z$.
2. That $f\colon X \mapsto Y$ is *surjective* by definition, then $\exists\, x \in X\colon f(x) = y$.

Then $\forall\, z \in Z\colon\ \exists\, x \in X\colon h(x) = (g \circ f)(x) = g(f(x)) = g(y) = z$ holds true. ■

2.4 Composition of Bijection

Proposition 2.4.1 (Composition of Bijection)**.** Given *bijections* $f\colon X \mapsto Y$ and $g\colon Y \mapsto Z$, then their composition $h\colon X \mapsto Z$ is given by

$$h(x) = g(f(x)) \tag{2.13}$$

Then h is also a *bijective* function; an *inverse bijection* $h^{-1}\colon Z \mapsto X$ also exists.

2.5 Cardinality of Sets

Definition 2.5.1 (Cardinality)**.** The number of elements in a set X is denoted $|X|$.

Definition 2.5.2 (Equal Cardinality and Bijection)**.**

$$|X| = |Y| \tag{2.14}$$

Holds true if there exists a *bijection* $h\colon X \mapsto Y$ (one-to-one correspondence between X and Y).

Namely, X and Y have the same number of distinct elements, and each distinct element $x \in X$ corresponds to exactly one distinct element $y \in Y$.

Theorem 2.5.1 (Cantor-Bernstein)**.** Given

1. *injective* function $f\colon X \mapsto Y$
2. *injective* function $g\colon Y \mapsto X$

Then there exists a *bijective* function $h\colon X \mapsto Y$.

Equivalently,

$$(|X| \leq |Y|) \wedge (|Y| \leq |X|) \rightarrow (|X| = |Y|) \tag{2.15}$$

Remark. Examples include countable sets, enumerable sets

$$|\mathbb{Q}| = |\mathbb{Z}| = |\mathbb{N}| = \aleph_0 \tag{2.16}$$

Where the cardinality of countable sets such as the *rational numbers*, *integers* and the *natural numbers* is denoted as "alpeh-zero" ($\aleph_0$).

On the other hand, continuum such as the *real numbers* are not countable and as such

$$|\mathbb{R}| > \aleph_0 \tag{2.17}$$

3 Permutations

3.1 Permutation Basics

Definition 3.1.1 (Permutation)**.** The bijection – *permutation* – of

$$\begin{array}{ccccc} 1 & 2 & 3 & \cdots & n \\ \downarrow & \downarrow & \downarrow & \cdots & \downarrow \\ 1 & 2 & 3 & \cdots & n \end{array} \tag{3.1}$$

Is denoted as

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 1 & 2 & 3 & \cdots & n \end{pmatrix} \tag{3.2}$$

Where $\sigma\colon \{1, \ldots, n\} \to \{1, \ldots, n\}$ is the *permutation* bijection.

Definition 3.1.2 (Counting Permutations)**.**

$$|S_n| := n! \tag{3.3}$$

Which is the number of different ways to permutate n elements $\{1, 2, \ldots, n\} \subset \mathbb{Z}$. Together, the different permutations for n distinct elements is the *symmetric group* S_n.

Remark. For example, with $S_3 = \{1, 2, 3\}$, there are $3! = 6$ different ways to arrange the three distinct elements

$$\begin{matrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} & \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} & \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \\ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} & \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} & \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \end{matrix} \tag{3.4}$$

Definition 3.1.3 (Order of Permutation)**.** The *order* of a permutation σ is the smallest $k \in \mathbb{Z}^+$ such that

$$\sigma^k = \epsilon \tag{3.5}$$

Where ϵ is the *identity permutation*

$$\epsilon(x) = x \tag{3.6}$$

Definition 3.1.4 (Sign of Permutation)**.** The *sign* of a permutation $\operatorname{sgn}\sigma\colon \sigma \to \{-1, +1\}$ where $\sigma \in S_n$ is defined as

$$\operatorname{sgn}(\sigma) = (-1)^k \tag{3.7}$$

Where k is the number of *disorders* within σ, the number of pairs (x, y) such that $x > y \to \sigma(x) < \sigma(y)$ or the converse $x < y \to \sigma(x) > \sigma(y)$. Additionally,

$$\operatorname{sgn}(\sigma) = \begin{cases} +1 & \text{if k is even} \\ -1 & \text{if k is odd} \end{cases} \tag{3.8}$$

Remark. For example, in

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$1 < 2$ but $\sigma(1) = 2 > \sigma(2) = 1$, hence a disorder.

For each $i \in \{1, \ldots, n\}$, starting from $i = 1$, compare $\sigma(i)$ with $\sigma(i+1), \ldots, \sigma(n)$ and add the number of disordered pairs, then move on to $i + 1$ and compare $\sigma(i + 1)$ with $\sigma(i + 2), \ldots, \sigma(n)$ and so on.

Theorem 3.1.1 (Composition of Permutation)**.**

$$\operatorname{sgn}(\sigma_1 \sigma_2) := \operatorname{sgn}(\sigma_1) \cdot \operatorname{sgn}(\sigma_2) \tag{3.9}$$

Where

$\circ$	even	odd
even	even	odd
odd	odd	even

Table 3.1: Sign Changes on Composition

4 Binary Relations

Definition 4.0.1 (Binary Relation)**.** A binary relation $R(x, y)$ describes some relationship between x and y where $R\colon X \to Y$, $R \subseteq X \times Y$, $x \in X$ and $y \in Y$. This relation can be expressed in infix notation as xRy.

4.1 Equivalence Relations

Definition 4.1.1 (Equivalence Relation)**.** A binary relation $E(x, y)$ is an *equivalence relation* on X iff it satisfies all three conditions:

1. **Reflexivity**
   $\forall\, x \in X\colon E(x, x)$
2. **Symmetry**
   $\forall\, x, y \in X\colon E(x, y) \to E(y, x)$
3. **Transitivity**
   $\forall\, x, y, z \in X\colon E(x, y) \land E(y, z) \to E(x, z)$

4.2 Equivalence Classes

Definition 4.2.1 (Equivalence Class)**.** If $a \in X$, the *equivalence class* $[a]$ is

$$[a] \coloneqq \{x \in X\colon E(x, a)\} \subseteq X \tag{4.1}$$

Definition 4.2.2 (Congruence and Equivalence Class of mod m on $\mathbb{Z}$)**.** For *congruence mod* m on $\mathbb{Z}$, if $a \in \mathbb{Z}$ then the *congruence class* of a is

$$[a]_m \coloneqq \{x \in \mathbb{Z}\colon x = a + km\} \tag{4.2}$$

Where $k \in \mathbb{Z}$. Since $x = a + km \Leftrightarrow x \equiv a \bmod m$, then the *equivalence class* of a is also the *congruence class*.

$$\Leftrightarrow [a]_m \coloneqq \{x \in \mathbb{Z}\colon x \equiv a \bmod m\} \tag{4.3}$$

Definition 4.2.3 (Set of Remainders)**.** Over $\mathbb{Z}$, the *remainder* r from the integer division $k \div m$ is

$$r \bmod m \equiv k \bmod m \tag{4.4}$$

Then the set of remainders G_m from the integer division $k \div m$ is defined by

$$G_m \coloneqq \{0, 1, 2, \dots, m-2, m-1\} \tag{4.5}$$

4.3 Quotient Groups

Definition 4.3.1 (Quotient Group). A *quotient group* is a group constructed via congruence mod m.

Definition 4.3.2 (Congruence Class). If $m \leq 2$ and $a \in \mathbb{Z}$ then the *congruence class* of a mod m is $[a] \subseteq \mathbb{Z}$

$$[a] := \{b \in \mathbb{Z} \colon b \equiv a \bmod m\} \tag{4.6}$$
$$\Leftrightarrow \{a + km \colon k \in \mathbb{Z}\} \tag{4.7}$$
$$\Leftrightarrow \{\dots, a - 2m, a - m, a, a + m, a + 2m, \dots\} \tag{4.8}$$

Remark. Let $E(x, y) :=$ "$x - y \equiv 0 \bmod 2$", that is, $x - y$ is divisible by 2. Then,

$$[k]_2 := \{y \colon E(k, y)\} \tag{4.9}$$

Where $[k]_2$ is the congruence class of integers modulo 2.
Computing $[0]_2$ and $[1]_2$ yields

- $[0]_2 = \{0, 2, -2, 4, -4, \dots, 2n, -2n, \dots\}$
- $[1]_2 = \{1, -1, 3, -3, \dots, 2n + 1, \dots\}$

Observe that

$$[1]_2 \oplus [1]_2 \Leftrightarrow [2]_2 \Leftrightarrow [0]_2 \tag{4.10}$$

It can be deduced that $[0]_2$ and $[1]_2$ are two congruence (and equivalence) classes which partition the integers $\mathbb{Z}$ into two disjoint subsets – integers which are odd, and integers which are even. This may be denoted as

$$\mathbb{Z}/E \equiv \{\text{EVEN}, \text{ODD}\} \tag{4.11}$$

Definition 4.3.3 (Congruence Modular Arithmetic $\pmod m$ on $\mathbb{Z}$).

$$[a]_m \oplus [b]_m \equiv [a + b]_m \tag{4.12}$$
$$[a]_m \otimes [b]_m \equiv [a \cdot b]_m \tag{4.13}$$

If $a_1 \equiv a_2 \bmod m$ and $b_1 \equiv b_2 \bmod m$ then

$$a_1 + b_1 \equiv a_2 + b_2 \bmod m \tag{4.14}$$
$$a_1 \cdot b_1 \equiv a_2 \cdot b_2 \bmod m \tag{4.15}$$
$$\tag{4.16}$$

Remark. We may introduce addition $(+)$ and multiplication $(*)$ over the remainders G_m previously defined as

$$G_m := \{0, 1, 2, \dots, m - 2, m - 1\} \tag{4.17}$$

For example, given $m = 3$, then the multiplication and addition table of $+ \pmod 3$ and $* \pmod 3$ over G_3 can be computed:

+ (mod 3)	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$*$ (mod 3)	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Table 4.1: Multiplication and Addition Table of G_3

5 Groups

Bibliography

[1] Max Kanovich and Robin Hirsch.
"Lecture Notes on Discrete Mathematics for Computer Scientists".
URL: http://www.cs.ucl.ac.uk/1819/a4u/t2/comp0147_discrete_mathematics_for_computer_scientists/.

[2] Joseph J. Rotman. *A First Course in Abstract Algebra*. 3rd ed.
University of Illinois at Urbana-Champaign: Pearson. ISBN: 978-0131862678.