

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 | 7 |
| 1.1 | Set Notations | 7 |
| 1.2 | Properties | 7 |
| 1.3 | Set Equality | 7 |
| 1.4 | Set Operations | 7 |
| 1.5 | Boolean Algebra | 8 |
| 1.6 | Set Algebra | 9 |
| 2 | Functions | 11 |
| 2.1 | Function Basics | 11 |
| 2.2 | Composition of Injections | 12 |
| 2.3 | Composition of Surjection | 12 |
| 2.4 | Composition of Bijection | 12 |
| 2.5 | Cardinality of Sets | 13 |
| 3 | Permutations | 15 |
| 3.1 | Permutation Basics | 15 |
| 4 | Binary Relations | 17 |
| 4.1 | Equivalence Relations | 17 |
| 4.2 | Equivalence Classes | 17 |
| 4.3 | Quotient Groups | 18 |
| 5 | Groups | 21 |
| 5.1 | Group Basics | 21 |
| 5.2 | Multiplicative Group | 21 |
| 5.3 | Additive Group | 22 |
| 5.4 | Associativity of Sequential Composition of Functions | 23 |
| 5.5 | Subgroups | 23 |
| 5.6 | Lagrange's Theorem | 24 |
| 5.6.1 | Equivalence Classes | 26 |

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. $A \subseteq B \implies \forall x(x \in A \rightarrow x \in B)$
2. $B \subseteq A \implies \forall y(y \in B \rightarrow y \in A)$

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

1.4 Set Operations

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

1.5 Boolean Algebra

Definition 1.5.1 (De Morgan's Laws).

$$\neg(p \vee q) \equiv \neg p \wedge \neg q \quad (1.1)$$

$$\neg(p \wedge q) \equiv \neg p \vee \neg q \quad (1.2)$$

Definition 1.5.2 (Idempotent Laws).

$$p \vee p \equiv p \quad (1.3)$$

$$p \wedge p \equiv p \quad (1.4)$$

Definition 1.5.3 (Commutative Laws).

$$p \vee q \equiv q \vee p \quad (1.5)$$

$$p \wedge q \equiv q \wedge p \quad (1.6)$$

Definition 1.5.4 (Associative Laws).

$$p \vee (q \vee r) \equiv (p \vee q) \vee r \quad (1.7)$$

$$p \wedge (q \wedge r) \equiv (p \wedge q) \wedge r \quad (1.8)$$

Definition 1.5.5 (Distributive Laws).

$$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r) \quad (1.9)$$

$$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r) \quad (1.10)$$

Definition 1.5.6 (Identity Laws).

$$p \vee F \equiv p \quad (1.11)$$

$$p \vee T \equiv T \quad (1.12)$$

$$p \wedge T \equiv p \quad (1.13)$$

$$p \wedge F \equiv F \quad (1.14)$$

Definition 1.5.7 (Absorption Laws).

$$p \vee (p \wedge q) \equiv p \quad (1.15)$$

$$p \wedge (p \vee q) \equiv p \quad (1.16)$$

Definition 1.5.8 (Implication and Negation Laws).

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

- *Absorption:*
 $p \rightarrow T \equiv T$
 $p \rightarrow F \equiv \neg p$
 $T \rightarrow p \equiv p$
 $F \rightarrow p \equiv T$
- *Contrapositive:* $p \rightarrow q \equiv \neg q \rightarrow \neg p$
- *Law of Excluded Middle:*
 $p \vee \neg p \equiv T$
 $p \wedge \neg p \equiv F$
- *Double Negation:* $\neg\neg p \equiv p$
- *Reduction to Absurdity:* $\neg p \rightarrow F \equiv p$

1.6 Set Algebra

Definition 1.6.1 (De Morgan's Laws).

$$(A \cup B)^c \equiv A^c \cap B^c \quad (1.17)$$

$$(A \cap B)^c \equiv A^c \cup B^c \quad (1.18)$$

Definition 1.6.2 (Idempotent Laws).

$$A \cup A \equiv A \quad (1.19)$$

$$A \cap A \equiv A \quad (1.20)$$

Definition 1.6.3 (Commutative Laws).

$$A \cup B \equiv B \cup A \quad (1.21)$$

$$A \cap B \equiv B \cap A \quad (1.22)$$

Definition 1.6.4 (Associativity Laws).

$$A \cup (B \cup C) \equiv (A \cup B) \cup C \quad (1.23)$$

$$A \cap (B \cap C) \equiv (A \cap B) \cap C \quad (1.24)$$

Definition 1.6.5 (Distributive Laws).

$$A \cap (B \cup C) \equiv (A \cap B) \cup (A \cap C) \quad (1.25)$$

$$A \cup (B \cap C) \equiv (A \cup B) \cap (A \cup C) \quad (1.26)$$

Definition 1.6.6 (Identity Laws).

$$A \cup \emptyset \equiv A \quad (1.27)$$

$$A \cap \emptyset \equiv \emptyset \quad (1.28)$$

$$A \cap U \equiv A \quad (1.29)$$

$$A \cup U \equiv U \quad (1.30)$$

Definition 1.6.7 (Absorption Laws).

$$A \cup (A \cap B) \equiv A \quad (1.31)$$

$$A \cap (A \cup B) \equiv A \quad (1.32)$$

Definition 1.6.8 (Difference Identity Laws).

$$C \setminus (A \cup B) \equiv (C \setminus A) \cap (C \setminus B) \quad (1.33)$$

$$C \setminus (A \cap B) \equiv (C \setminus A) \cup (C \setminus B) \quad (1.34)$$

Definition 1.6.9 (Complement-Difference Identity Law).

$$C \setminus D \equiv C \cap D^c \quad (1.35)$$

Definition 1.6.10 (Double Complement Law).

$$(D^c)^c \equiv D \quad (1.36)$$

Definition 1.6.11 (Contraposition).

$$C \subseteq D \Leftrightarrow D^c \subseteq C^c \quad (1.37)$$

$$C = D \Leftrightarrow C^c = D^c \quad (1.38)$$

Definition 1.6.12 (Arbitrary Union).

Given sets A_1, A_2, \dots, A_n where $I = \{1, 2, \dots, n\}$

$$A_1 \cup A_2 \cup \dots \cup A_n := \bigcup_{i \in I} A_i \quad (1.39)$$

Then

$$x \in \bigcup_{i \in I} A_i \Leftrightarrow \exists i \in I: x \in A_i \quad (1.40)$$

Definition 1.6.13 (Arbitrary Intersection).

Given sets A_1, A_2, \dots, A_n where $I = \{1, 2, \dots, n\}$

$$A_1 \cap A_2 \cap \dots \cap A_n := \bigcap_{i \in I} A_i \quad (1.41)$$

Then

$$x \in \bigcap_{i \in I} A_i \Leftrightarrow \forall i \in I: x \in A_i \quad (1.42)$$

2 Functions

2.1 Function Basics

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

$$f: X \mapsto Y \quad (2.1)$$

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

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

$$\text{domain}(f) = X \quad (2.2)$$

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

$$\text{domain}(f) \subseteq X \quad (2.3)$$

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

$$f(X) = Y \Leftrightarrow \forall y \in Y: \exists x \in X: f(x) = y \quad (2.4)$$

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

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

$$\forall x_1, x_2 \in X: x_1 \neq x_2 \rightarrow f(x_1) \neq f(x_2) \quad (2.5)$$

$$\Leftrightarrow \forall x_1, x_2 \in X: f(x_1) = f(x_2) \rightarrow x_1 = x_2 \quad (2.6)$$

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

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

$$\text{Bijective}(f) := \text{Injective}(f) \wedge \text{Surjective}(f) \quad (2.7)$$

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

2.2 Composition of Injections

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

$$h(x) := g(f(x)) \quad (2.8)$$

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

$$f(x_1) \neq f(x_2) \quad (2.9)$$

as f is *injective*, and thus

$$h(x_1) = g(f(x_1)) \neq g(f(x_2)) = h(x_2) \quad (2.10)$$

h is *injective* consequently. ■

2.3 Composition of Surjection

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

$$h(x) := g(f(x)) \quad (2.11)$$

Then h is also a *surjective* function.

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

$$\forall z \in Z: \exists x \in X: h(x) = z \quad (2.12)$$

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

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

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

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

2.4 Composition of Bijection

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

$$h(x) := g(f(x)) \quad (2.13)$$

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

$$|X| = |Y| \quad (2.14)$$

Holds true if there exists a *bijection* $h: X \mapsto Y$ (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 $f: X \mapsto Y$

2. *injective* function $g: Y \mapsto X$

Then there exists a *bijection* function $h: X \mapsto Y$.

Equivalently,

$$(|X| \leq |Y|) \wedge (|Y| \leq |X|) \rightarrow (|X| = |Y|) \quad (2.15)$$

Remark. Examples include countable sets, enumerable sets

$$|\mathbb{Q}| = |\mathbb{Z}| = |\mathbb{N}| = \aleph_0 \quad (2.16)$$

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

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

$$|\mathbb{R}| > \aleph_0 \quad (2.17)$$

3 Permutations

3.1 Permutation Basics

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

$$\begin{array}{ccccccccc} 1 & 2 & 3 & \dots & n \\ \downarrow & \downarrow & \downarrow & \dots & \downarrow \\ \sigma(1) & \sigma(2) & \sigma(3) & \dots & \sigma(n) \end{array} \quad (3.1)$$

Is denoted as

$$\left(\begin{array}{ccccc} 1 & 2 & 3 & \dots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \dots & \sigma(n) \end{array} \right) \quad (3.2)$$

Where $\sigma: \{1, \dots, n\} \rightarrow \{1, \dots, n\}$ is the *permutation* bijection.

Definition 3.1.2 (Counting Permutations).

$$|S_n| := n! \quad (3.3)$$

Which is the number of different ways to permute n elements $\{1, 2, \dots, n\} \subset \mathbb{Z}$. 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

$$\begin{array}{ccc} \left(\begin{array}{ccc} 1 & 2 & 3 \\ 1 & 2 & 3 \end{array} \right) & \left(\begin{array}{ccc} 1 & 2 & 3 \\ 1 & 3 & 2 \end{array} \right) & \left(\begin{array}{ccc} 1 & 2 & 3 \\ 2 & 1 & 3 \end{array} \right) \\ \left(\begin{array}{ccc} 1 & 2 & 3 \\ 2 & 3 & 1 \end{array} \right) & \left(\begin{array}{ccc} 1 & 2 & 3 \\ 3 & 1 & 2 \end{array} \right) & \left(\begin{array}{ccc} 1 & 2 & 3 \\ 3 & 2 & 1 \end{array} \right) \end{array} \quad (3.4)$$

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

$$\sigma^k = \epsilon \quad (3.5)$$

Where ϵ is the *identity permutation*

$$\epsilon(x) = x \quad (3.6)$$

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

$$\text{sgn}(\sigma) = (-1)^k \quad (3.7)$$

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

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

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

Theorem 3.1.1 (Composition of Permutation).

$$\text{sgn}(\sigma_1 \sigma_2) := \text{sgn}(\sigma_1) \cdot \text{sgn}(\sigma_2) \quad (3.9)$$

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 $R: X \rightarrow Y$, $R \subseteq X \times Y$, $x \in X$ 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**

$$\forall x \in X: E(x, x)$$

2. **Symmetry**

$$\forall x, y \in X: E(x, y) \rightarrow E(y, x)$$

3. **Transitivity**

$$\forall x, y, z \in X: E(x, y) \wedge E(y, z) \rightarrow E(x, z)$$

4.2 Equivalence Classes

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

$$[a] := \{x \in X: E(x, a)\} \subseteq X \quad (4.1)$$

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

$$[a]_m := \{x \in \mathbb{Z}: x = a + km\} \quad (4.2)$$

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

$$\Leftrightarrow [a]_m := \{x \in \mathbb{Z}: x \equiv a \pmod{m}\} \quad (4.3)$$

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

$$r \bmod m \equiv k \bmod m \quad (4.4)$$

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

$$G_m := \{0, 1, 2, \dots, m-2, m-1\} \quad (4.5)$$

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 $a \bmod m$ is $[a] \subseteq \mathbb{Z}$

$$[a] := \{b \in \mathbb{Z} : b \equiv a \bmod m\} \quad (4.6)$$

$$\Leftrightarrow \{a + km : k \in \mathbb{Z}\} \quad (4.7)$$

$$\Leftrightarrow \{\dots, a - 2m, a - m, a, a + m, a + 2m, \dots\} \quad (4.8)$$

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

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

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

$$[1]_2 \oplus [1]_2 \Leftrightarrow [2]_2 \Leftrightarrow [0]_2 \quad (4.10)$$

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

$$\mathbb{Z}/E \equiv \{\text{EVEN}, \text{ODD}\} \quad (4.11)$$

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

$$[a]_m \oplus [b]_m \equiv [a + b]_m \quad (4.12)$$

$$[a]_m \otimes [b]_m \equiv [a \cdot b]_m \quad (4.13)$$

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

$$a_1 + b_1 \equiv a_2 + b_2 \bmod m \quad (4.14)$$

$$a_1 \cdot b_1 \equiv a_2 \cdot b_2 \bmod m \quad (4.15)$$

$$(4.16)$$

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

$$G_m := \{0, 1, 2, \dots, m - 2, m - 1\} \quad (4.17)$$

For example, given $m = 3$, then the multiplication and addition table of $+$ (mod 3) and $*$ (mod 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

5.1 Group Basics

A *group* is an abstract collection consisting of:

- A *nonempty set* G .
- A *binary operation* $\star: G \times G \rightarrow G$.

It has the following properties:

1. **Closure**

$$\forall x, y: x \in G \wedge y \in G \rightarrow x \star y \in G \quad (5.1)$$

2. **Associativity**

$$\forall x, y, z \in G: (x \star y) \star z \equiv x \star (y \star z) \quad (5.2)$$

3. **Neutral Element**

$$\exists \epsilon \in G: \forall x \in G: x \star \epsilon \equiv \epsilon \star x \equiv x \quad (5.3)$$

That there exists a unique *neutral* element $\epsilon \in G$.

4. **Invertibility**

$$\forall x \in G: \exists y \in G: x \star y \equiv y \star x \equiv \epsilon \quad (5.4)$$

That there exists a unique *inverse* element $y := x^{-1} \in G$ where x^{-1} denotes the *inverse* element of x .

Definition 5.1.1 (Commutative Group). An *commutative group* (or *abelian group*) is a *group* for which its operation $\star: G \times G \rightarrow G$ satisfies the additional *commutative* property:

- **Commutativity**

$$\forall x, y \in G: x \star y \equiv y \star x \quad (5.5)$$

5.2 Multiplicative Group

Proposition 5.2.1 (Multiplicative Group). A *multiplicative group* is a *group* $(G, *)$ which has the binary operation $\ast: G \times G \rightarrow G$:

- **Closure, Associativity.** The multiplication operation $\ast: G \times G \rightarrow G$ is closed and is left associative.
- **Neutral Element.** The neutral element ϵ is unique.
- **Invertibility.** The inverse element x^{-1} is unique.
- For all $a, b \in G$ the equation

$$a \ast x = b \quad (5.6)$$

Has the unique solution

$$x = a^{-1} \ast b \quad (5.7)$$

Since

$$a * x = b \Leftrightarrow a^{-1} * (a * x) = a^{-1} * b \quad (\text{Multiply by inverse element}) \quad (5.8)$$

$$\Leftrightarrow (a^{-1} * a) * x = a^{-1} * b \quad (\text{Associativity}) \quad (5.9)$$

$$\Leftrightarrow \epsilon * x = a^{-1} * b \quad (\text{Invertibility}) \quad (5.10)$$

$$\Leftrightarrow x = a^{-1} * b \quad (\text{Neutral Element}) \quad (5.11)$$

Remark. An example of a multiplicative group is permutations under composition, namely S_n is a group (G, \circ) where $\circ: G \times G \rightarrow G$.

For example, let G be the set of permutations

$$\epsilon = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \sigma_2 = \sigma_1^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \quad (5.12)$$

To verify that G does form a group with composition \circ , one may draw the multiplication table for the group. Note that

$$\sigma_2 \sigma_2 = \sigma_1^4 = \sigma_1^3 \sigma_1 = \epsilon \sigma_1 = \sigma_1 \quad (5.13)$$

| \circ | ϵ | σ_1 | σ_2 |
|------------|------------|------------|------------|
| ϵ | ϵ | σ_1 | σ_2 |
| σ_1 | σ_1 | σ_2 | ϵ |
| σ_2 | σ_2 | ϵ | σ_1 |

Table 5.1: Multiplication Table of Composition \circ over G

5.3 Additive Group

Definition 5.3.1 (Additive Group). An *additive group* is a group $(G, +)$ with the binary operation $+: G \times G \rightarrow G$. It has the same properties of a general group.

1. **Closure**

$$\forall x, y: x \in G \wedge y \in G \rightarrow x + y \in G \quad (5.14)$$

2. **Associativity**

$$\forall x, y, z \in G: (x + y) + z \equiv x + (y + z) \quad (5.15)$$

3. **Neutral Element**

$$\exists \epsilon \in G: \forall x \in G: x + \epsilon \equiv \epsilon + x \equiv x \quad (5.16)$$

That there exists an unique *neutral* element $0_G \in G$ (usually denoted simply as 0).

4. **Invertibility**

$$\forall x \in G: \exists y \in G: x + y \equiv y + x \equiv 0 \quad (5.17)$$

That there exists an unique *inverse* element $y := -x \in G$ where $-x$ denotes the *inverse* element of x .

Remark. An example of an additive group is $(\mathbb{Z}, +)$ (i.e. addition over the integers). Then for any of such *commutative group* $(G, +)$

- *Neutral element* 0 is unique.
- *Inverse element* $-x$ is unique.
- For any $a, b \in G$ the equation

$$a + x = b \quad (5.18)$$

Has a unique solution

$$x = b + (-a) = b - a \quad (5.19)$$

5.4 Associativity of Sequential Composition of Functions

Definition 5.4.1 (Sequential Composition of Functions). Let $f * g$ denote the sequential composition of functions $f * X \rightarrow Y$ and $g: Y \rightarrow Z$ such that $f * g: X \rightarrow Z$ where f is applied first then g , i.e. $\forall x \in X: (f * g)(x) := g(f(x))$.

Proposition 5.4.1 (Associativity of Sequential Composition of Functions). Given sets X, Y and Z and

- *Injection* $f: A \rightarrow B$
- *Injection* $g: B \rightarrow C$
- *Injection* $h: C \rightarrow D$

Then their composition is associative:

$$(f * g) * h \equiv f * (g * h) \quad (5.20)$$

Proof.

Let $s = (f * g)$ and $t = (s * h)$, then $t(x) = h(s(x)) = h(g(f(x)))$.

Let $u = (g * h)$ and $v = (f * u)$, then $v(x) = u(f(x)) = h(g(f(x)))$.

Together they yield the desired equality $t(x) = v(x)$. ■

5.5 Subgroups

Definition 5.5.1 (Subgroup). Given a *group* $(G, *)$, then the subset $H \subseteq G$ is a *subgroup* of G if it fulfills the properties:

1. **Closure**

$$\forall x, y: x \in H \wedge y \in H \rightarrow x * y \in H \quad (5.21)$$

2. **Neutral Element**

$$\epsilon \in H \quad (5.22)$$

That is, the *neutral* element ϵ from G is contained within the subset $H \subseteq G$.

3. **Invertibility**

$$\forall x \in H: x^{-1} \in H \quad (5.23)$$

5.6 Lagrange's Theorem

Theorem 5.6.1 (Lagrange's Theorem). Given a finite group of order n $(G, *)$ where

$$G := \{g_1, g_2, \dots, g_n\} \quad (5.24)$$

And its subgroup $(H, *)$ of order $k \leq n$

$$H := \{h_1, h_2, \dots, h_k\} \quad (5.25)$$

Then $k|n$ (k divides n).

G can be partitioned into ℓ disjoint subsets of the same size k such that

$$n = k\ell \quad (5.26)$$

Definition 5.6.1 (Left Coset). Given $(G, *)$ is a group, $(H, *)$ is a subgroup of $(G, *)$ and $g \in G$ then the left coset gH of H in G with respect to g is defined as

$$gH := \{g * h : h \in H\} \quad (5.27)$$

Remark. Visually,

$$G \equiv \left. \begin{array}{c} \boxed{g_1 H} \\ \boxed{g_2 H} \\ \vdots \\ \boxed{g_\ell H} \end{array} \right\} \ell \text{ disjoint subsets} \quad (5.28)$$

To verify that the left cosets together do in fact reconstruct G , check the multiplication table

| $*$ | h_1 | h_2 | \dots | h_k |
|------------|----------------|----------------|----------|----------------|
| $g_1 H$ | $g_1 * h_1$ | $g_1 * h_2$ | \dots | $g_1 * h_k$ |
| $g_2 H$ | $g_2 * h_1$ | $g_2 * h_2$ | \dots | $g_2 * h_k$ |
| \vdots | \vdots | \vdots | \ddots | \vdots |
| $g_\ell H$ | $g_\ell * h_1$ | $g_\ell * h_2$ | \dots | $g_\ell * h_k$ |

Table 5.2: Multiplication Table from ℓ Left Cosets, Each of Size $|H| = k$

Proposition 5.6.1. For any $a, b \in G$ from $(G, *)$

$$(a * b)^{-1} \equiv b^{-1} * a^{-1} \quad (5.29)$$

Proof.

$$(a * b)^{-1} \Leftrightarrow (a * b)^{-1} * \epsilon \quad (\text{Neutral element}) \quad (5.30)$$

$$\Leftrightarrow (a * b)^{-1} * (a * a^{-1}) \quad (\text{Invertibility}) \quad (5.31)$$

$$\Leftrightarrow (a * b)^{-1} * ((a * \epsilon) * a^{-1}) \quad (\text{Neutral element}) \quad (5.32)$$

$$\Leftrightarrow (a * b)^{-1} * [(a * (b * b^{-1})) * a^{-1}] \quad (\text{Invertibility}) \quad (5.33)$$

$$\Leftrightarrow (a * b)^{-1} * [(a * b) * (b^{-1} * a^{-1})] \quad (\text{Associativity}) \quad (5.34)$$

$$\Leftrightarrow [(a * b)^{-1} * (a * b)] * (b^{-1} * a^{-1}) \quad (\text{Associativity}) \quad (5.35)$$

$$\Leftrightarrow \epsilon * (b^{-1} * a^{-1}) \quad (\text{Invertibility}) \quad (5.36)$$

$$\Leftrightarrow b^{-1} * a^{-1} \quad (\text{Neutral Element}) \quad (5.37)$$

■

Proof. For a constructive proof of Lagrange's Theorem:

Let the binary relation $E(x, y)$ be defined on the group $(G, *)$, with its subgroup $(H, *)$

$$E(x, y) := x^{-1} * y \in H \quad (5.38)$$

For the equivalence

$$x = y \Leftrightarrow x^{-1} * y = 1 \quad (5.39)$$

Then for each of the required properties:

- **Neutral Element** from *Reflexivity* of $E(x, y)$

$$\forall x \in G: E(x, x) \quad (5.40)$$

Since

$$E(x, x) \equiv x^{-1} * x \in H \equiv \epsilon \in H \quad (5.41)$$

Then this satisfies the *reflexivity* requirement for *equivalence relations*, and proves the *neutral element* requirement for *subgroups*.

- **Invertibility** from *Symmetry* of $E(x, y)$

$$\forall x, y \in G: E(x, y) \rightarrow E(y, x) \quad (5.42)$$

Let for some $h \in H$, $x^{-1} * y = h$, then by proposition 5.6.1

$$y^{-1} * x \equiv (x^{-1} * y)^{-1} \equiv h^{-1} \in H \quad (5.43)$$

Which satisfies the *symmetry* requirement for *equivalence relations*, and proves the *invertibility* requirement for *subgroups*.

- **Closure** from *Transitivity* of $E(x, y)$

$$\forall x, y, z \in G: E(x, y) \wedge E(y, z) \rightarrow E(x, z) \quad (5.44)$$

Let for some $h_1, h_2 \in H$, $(x^{-1} * y = h_1) \wedge (y^{-1} * z = h_2)$, then

$$x^{-1} * z \Leftrightarrow x^{-1} * \epsilon * z \quad (5.45)$$

$$\Leftrightarrow (x^{-1} * y) * (y^{-1} * z) \quad (5.46)$$

$$\Leftrightarrow h_1 * h_2 \in H \quad (5.47)$$

Which satisfies the *transitivity* requirement for *equivalence relations*, and proves the *closure* requirement for *subgroups*. ■

Remark. To demonstrate Lagrange's Theorem, let the *group* be constructed from $x * y \pmod{10}$.

Let $(G, *)$ be a finite *group* of order $n = 4$ where

$$G = \{1, 3, 7, 9\} \quad (5.48)$$

And $(H, *)$ be its *subgroup* of order $k = 2$.

Constructing the multiplication table yields

| $* \pmod{10}$ | 1 | 9 |
|---------------|---|---|
| $1 * H$ | 1 | 9 |
| $3 * H$ | 3 | 7 |
| $7 * H$ | 7 | 3 |
| $9 * H$ | 9 | 1 |

Table 5.3: Multiplication Table for $(G, *)$

There are only $\ell = 2$ disjoint subsets (unique cosets) gH ; G can be partitioned into ℓ disjoint subsets, each of size $|H| = 2$ such that $4 = n = k\ell = 2 \cdot 2$.

Visually,

$$G = \left. \begin{array}{l} 1 * H = 9 * H = \{1, 9\} \\ 3 * H = 7 * H = \{3, 7\} \end{array} \right\} \ell = 2 \quad (5.49)$$

5.6.1 Equivalence Classes

Definition 5.6.2 (Equivalence Class). Given *group* $(G, *)$ and its *subgroup* $(H, *)$, then the *equivalence class* $[g]$ is defined as

$$[g] := \{y \in G \mid g^{-1} * y \in H\} \quad (5.50)$$

Then

$$\forall h \in H: g^{-1} * y = h \Leftrightarrow y = g * h \quad (5.51)$$

Which yields the equivalence

$$\{y \in G \mid g^{-1} * y \in H\} \equiv \{y \in G \mid y \in gH\} \quad (5.52)$$

Hence

$$[g] \equiv gH \quad (5.53)$$

That the *equivalence class* $[g]$ is exactly the *left coset* gH .

Let ℓ be the number of disjoint equivalence class $[g]$, then G can be partitioned into ℓ disjoint subsets where visually,

$$G = \left. \begin{array}{c} [g_1] \equiv g_1 H \\ [g_2] \equiv g_2 H \\ \vdots \\ [g_\ell] \equiv g_\ell H \end{array} \right\} \ell \text{ disjoint subsets} \quad (5.54)$$

Proposition 5.6.2.

$$\forall g \in G: |gH| \equiv |H| \equiv k \quad (5.55)$$

Proof. Let I be the set of indices $I := \{1, \dots, k\}$

$$\forall i, j \in I: (h_i = h_j) \Leftrightarrow (g * h_i = g * h_j) \quad (5.56)$$

$$\Leftrightarrow \forall i, j \in I: (h_i \neq h_j) \Leftrightarrow (g * h_i \neq g * h_j) \quad (5.57)$$

■

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.