FUNDAMENTAL ALGEBRA & ANALYSIS

Contents

Chapter 1

Basic Logic

1.1 Statement

Definition 1.1.1 We call statement a declarative sentence that is either true or false, but not both(it can be potential).

Example 1.1.1 ”$2 > 1$”(True) ”$1 < 0$”(False)

If we specify the value of x ,then ”$x > 2$”becomes a statement, otherwise it is not a statement.

Definition 1.1.2 In a mathematical theory,
axiom refer to statements that accepted to be true without justification.
theorem refer to statements that are proved by assuming axioms.
proposition refer to the statements that are either easy or not used many times.
corollary refer to direct consequence of a theorem.

1.2 Negation

Definition 1.2.1 Let p be a statement, then the negation of p is denoted by $\neg p$, which is a statement that is true if and only if p is false. In other words, p and $\neg p$ has opposite truth values.

Proposition 1.2.1 For any statement p, $\neg\neg p$and p have the same value.

p	q	$p \wedge q$	$p \vee q$
T	T	T	T
T	F	F	T
F	T	F	T
F	F	F	F

Table 1.1: Truth table for conjunction and disjunction

1.3 Conjunction and Disjunction

Definition 1.3.1 Let p and q be statements,
we denote by $p \wedge q$the statement "p and q"
we denote by $p \vee q$the statement "p or q"

Proposition 1.3.1 Let $P$and Qbe statements $(\neg P) \vee (\neg Q) and \neg (P \wedge Q)$have the same truth value.

1.4 Conditional statements

Definition 1.4.1 Let P and Q be statements,we denote by $P \Rightarrow Q$ the statement(if P then Q)

Remark 1.4.1 It has the same truth value as that of $(\neg P \vee Q)$,only when P s true and $Q$is false,otherwise it's true .
If one can prove Q is assuming that $P$is true ,then $P \Rightarrow Q$ is true .

Proposition 1.4.1 Let $P$and Q be statements.If $P$and $P \Rightarrow Q$ are true,then Q is also true.

Proposition 1.4.2 Let P, Q, R be statements.If $P \Rightarrow Q$and $Q \Rightarrow R$ are true,then $P \Rightarrow R$ is also true .

Theorem 1.4.1 Let $P$and Q be statements.$P \Rightarrow Q$ and $(\neg Q) \Rightarrow (\neg P)$ have the same truth value.

$(\neg Q) \Rightarrow (\neg P)$ is called the contraposition of $P \Rightarrow Q$,if we prove $(\neg Q) \Rightarrow (\neg P)$,then $P \Rightarrow Q$ is also true .

Example 1.4.1 Prove that ,let $n$be an integer,if n^2 is even ,then n is even .

Proof Since $n$is an integer,there exists$k \in \mathbb{Z}$ such that $n = 2k + 1$.Hence $n^2 = 4k^2 + 4k + 1$is not even. □

1.5 Biconditional statement

Definition 1.5.1 Let $P$and Q be statements.We denote by $P \Leftrightarrow Q$ the statement

$$"P \text{ if and only if } Q"$$

its true when$P$and Qhave the same truth value,it's false when they have the opposite truth value.

Proposition 1.5.1 Let P and Q be statements.$P \Leftrightarrow Q$ has the same truth value as

$$(P \Rightarrow Q) \wedge (Q \Rightarrow P)$$

Example 1.5.1 Let n be an integer.
n is even if and only if n^2 is even

Definition 1.5.2 Let P and Q be statements.
$Q \Rightarrow P$ is called the converse of$P \Rightarrow Q$
$\neg P \Rightarrow \neg Q$is called the inverse of $P \Rightarrow Q$

Remark 1.5.1 If one proves $P \Rightarrow Q$and $\neg P \Rightarrow \neg Q$,then $P \Leftrightarrow Q$ is true.

1.6 Proof by Contradiction

Definition 1.6.1 Let P be a statement.If we assume $\neg P$is true and deduce that a certain statement is both true and false, then we say that a contradiction happens and the assumption $\neg P$ is false. Thus the statement P is true. Such a reasoning is called proof by contradiction.

Example 1.6.1 Prove that the equation $x^2 = 2$ does not have solution in $\mathbb{Q}$

Proof By contradiction,we assume that $x := \frac{p}{q}$ is a solution,where p and q are integers ,which do not have common prime divisor.
By $x^2 = 2$ we obtain $p^2 = 2q^2$ So p^2 is even,p is even.Let $p_1 \in \mathbb{Z}$ such that $p = 2p_1$ Then $p^2 = 4p_1^2 = 2q^2$,hence q is even.
Therefore 2 is a common prime divisor of p and q,which leads to a contradiction. □

1.7 Exercises

1. Let P and Q be statements. Use truth tables to determine the truth values of the following statements according to the truth values of P and Q:

$$P \wedge \neg P,\ P \vee \neg P,\ (P \vee Q) \Rightarrow (P \wedge Q),\ (P \Rightarrow Q) \Rightarrow (Q \Rightarrow P)$$

2. Let P and Q be statements.

   (a) Show that $P \Rightarrow (Q \wedge \neg Q)$ has the same truth value as $\neg P$.

   (b) Show that $(P \wedge \neg Q) \Rightarrow Q$ has the same truth value as $P \Rightarrow Q$.

3. Consider the following statements:

$$P := \text{“Little Bear is happy”},$$

$$Q := \text{“Little Bear has done her math homework”},$$

$$R := \text{“Little Rabbit is happy”}.$$

   Express the following statements using P, Q, and R, along with logical connectives:

   (a) If Little Bear is happy and has done her math homework, then Little Rabbit is happy.

   (b) If Little Bear has done her math homework, then she is happy.

   (c) Little Bear is happy only if she has done her math homework.

4. Does the following reasoning hold? Justify your answer.

   - It is known that Little Bear is both smart and lazy, or Little Bear is not smart.
   - It is also known that Little Bear is smart.
   - Therefore, Little Bear is lazy.

5. Does the following reasoning hold? Justify your answer.

   - It is known that at least one of the lion or the tiger is guilty.
   - It is also known that either the lion is lying or the tiger is innocent.
   - Therefore, the lion is either lying or guilty.

6. An explorer arrives at a cave with three closed doors, numbered 1, 2, and 3. Exactly one door hides treasure, while the other two conceal deadly traps.

   - Door 1 states: "*The treasure is not here*";
   - Door 2 states: "*The treasure is not here*";
   - Door 3 states: "*The treasure is behind Door 2*".

   Only one of these statements is true. Which door should the explorer open to find the treasure?

7. The Kingdom of Truth sent an envoy to the capital of the Kingdom of Lies. Upon entering the border, the envoy encountered a fork with three paths: dirt, stone, and concrete. Each path had a signpost:

   - The concrete path's sign: "*This path leads to the capital, and if the dirt path leads to the capital, then the stone path also does.*"
   - The stone path's sign: "*Neither the concrete nor the dirt path leads to the capital.*"
   - The dirt path's sign: "*The concrete path leads to the capital, but the stone path does not.*"

   All signposts lie. Which path should the envoy take?

8. Let a and b be real numbers. Prove that, if $a \neq -1$ and $b \neq -1$, then $ab + a + b \neq -1$.

9. Let a, b, and c be positive real numbers such that $abc > 1$ and

$$a + b + c < \frac{1}{a} + \frac{1}{b} + \frac{1}{c}.$$

   Prove the following:

   (a) None of a, b, or c equals 1.

   (b) At least one of a, b, or c is greater than 1.

   (c) At least one of a, b, or c is less than 1.

10. Let $a \neq 0$ and b be real numbers. For real numbers x and y, prove that if $x \neq y$, then $ax + b \neq ay + b$.

11. Let $n \geq 2$ be an integer. Prove that if n is composite, then there exists a prime number p dividing n such that $p \leq \sqrt{n}$.

12. Let n be an integer. Prove that either 4 divides n^2 or 4 divides $n^2 - 1$.

13. Let n be an integer. Prove that 12 divides $n^2(n^2 - 1)$.

14. Prove that any integer divisible by 4 can be written as the difference of two perfect squares.

15. Let x and y be non-zero integers. Prove that $x^2 - y^2 \neq 1$.

16. A plane has 300 seats and is fully booked. The first passenger ignores their assigned seat and chooses randomly. Subsequent passengers take their assigned seat if available; otherwise, they choose randomly. What is the probability that the last passenger sits in their assigned seat?

17. Little Bear, Little Goat, and Little Rabbit are all wearing hats. A parrot prepared four red feathers and four blue feathers to decorate their hats. The parrot selected two feathers for each hat-wearing animal to place on their hats. Each animal cannot see the feathers on their own hat but can see the feathers on the other animals' hats. Here is their conversation:

    - Little Bear: *I don't know what color the feathers on my hat are, but I know the other animals also don't know what color the feathers on their hats are.*
    - Little Goat: *Haha, now even without looking at Little Bear's hat, I know what color the feathers on my hat are.*
    - Little Rabbit: *Now I know what color the feathers on my hat are.*
    - Little Bear: *Hmm, now I also know what color the feathers on my hat are.*

    Question: What color are the feathers on Little Goat's hat?

18. The Sphinx tells the truth on one fixed weekday and lies on the other six. Cleopatra visits The Sphinx for three consecutive days:

    - Day 1: The Sphinx declared, "*I lie on Monday and Tuesday.*"
    - Day 2: The Sphinx declared, "*Today is either Thursday, or Saturday, or Sunday.*"
    - Day 3: The Sphinx declared, "*I lie on Wednesday and Friday.*"

    On which day does the Sphinx tell the truth? On which days of the week did Cleopatra visit the Sphinx?

Chapter 2

Set Theory

2.1 Roster Notation

Definition 2.1.1 We call a set a certain collection of distinct objects.
An object in a collection considered as a set is called element of it .
Two sets A and B are said to be equal if they have the same elements.We denoted by $A = B$ the statement "A and B are equal"
If A is a set and x is an object,$x \in A$ denotes x is an element of A (reads x belongs to A),$x \notin A$ denotes "x is NOT an element of A"

Notation Roster method:to be continue. . .

Example 2.1.1 {1,2,3}={3,2,1}={1,1,2,3}

More generally ,if I is a set ,and for any $i \in I$,we fix an x_i,then the set of all x_i is noted as

$$\{x_i | i \in I\}$$

Example 2.1.2

$$\{2k + 1 | k \in \mathbb{Z}\}$$

2.2 Set-builder Notation

Definition 2.2.1 Let A be a set .If for any $x \in A$ we fix a statement $P(x)$,then we say that $P(\cdot)$ is a condition on A

Example 2.2.1 "n is even" is a condition on $\mathbb{N}$, "x>2" is a condition on $\mathbb{R}$.

Definition 2.2.2 Let A be a set and $P(\cdot)$ be a condition on A .If $x \in A$ is such that $P(x)$ is true, then we say that x satisfies the condition $P(\cdot)$.We noted by

$$\{x \in A | P(x)\}$$

the set of $x \in A$ that satisfies the condition $P(\cdot)$

Example 2.2.2 $\{x \in \mathbb{R} | x > 2\}$ denotes the set of real numbers that are $x > 2$.

sometimes we combine the two methods of representation.

2.3 Subsets and Set Difference

Definition 2.3.1 Let A and B be sets. If any element of A is an element of B, we say that A is a subset of B,denoted as $A \subseteq B$ or $B \supseteq A$.

Example 2.3.1

- We denote by $\varnothing$ the set that does not have any element.We consider it as a subset of any set.
- Let A be a set ,then $A \subseteq A$

Definition 2.3.2 Let A be a set ,we denote by $\wp(A)$ the set of all subset of A ,called the power set of A.

Example 2.3.2 $\wp(\varnothing) = \{\varnothing\}$, $\wp(\wp(\varnothing)) = \{\varnothing, \{\varnothing\}\}$

Definition 2.3.3 Let A and B be sets. We denote by $B \backslash A$ the set $\{x \in B | x \notin A\}$. This is a subset of B called the set difference of B and A.
If in condition $A \subseteq B$, we say that $B \backslash A$ is the complement of A inside B

Example 2.3.3 If A is a set ,$P(\cdot)$ is a condition on A, then

$$\{x \in A | \neg P(x)\} = A \backslash \{x \in A | P(x)\}$$

Proposition 2.3.1 Let A and B be sets.Then

$$B\backslash A = \varnothing \Leftrightarrow B \subseteq A$$

If in condition A is the subset of B, then

$$B\backslash A = \varnothing \Leftrightarrow A = B$$

2.4 Quantifiers

Definition 2.4.1 Let A be a set and $P(\cdot)$ be a condition on A .We denote by "$\forall x \in A, P(x)$" the statement $\{x \in A | P(x)\} = A$
"$\exists x \in A, P(x)$"denotes$\{x \in A | P(x)\} \neq \varnothing$.

Example 2.4.1 $\forall x \in \varnothing, P(x)$ is true ;$\exists x \in \varnothing, P(x)$ is false.

Theorem 2.4.1 Let A be a set and $P(\cdot)$ be a condition on A
(1)$\exists x \in A, \neg P(x)$ and $\forall x \in A, P(x)$ have opposite truth values.
(2)$\forall x \in A, \neg P(x)$ and $\exists x \in A, P(x)$ have opposite truth value.

2.5 Sufficient and Necessary Condition

Definition 2.5.1 Let A be a set and $P(\cdot)$ and $Q(\cdot)$ be conditions on A. If

$$\{x \in A | P(x)\} \subseteq \{x \in A | Q(x)\}$$

we say that $P(\cdot)$ is a sufficient condition of $Q(\cdot)$.$Q(\cdot)$ is a necessary condition of $P(\cdot)$
If $\{x \in A | P(x)\} = \{x \in A | Q(x)\}$,we say that $p(\cdot)$ and $Q(\cdot)$ are equivalent.

Proposition 2.5.1 Let A be a set ,$P(\cdot)$ and $Q(\cdot)$ be conditions on A.
(1)$P(\cdot)$ is a sufficient condition of $Q(\cdot)$ iff.$\forall x \in A, P(x) \Rightarrow Q(x)$
(2)$P(\cdot)$ is a necessary condition of $Q(\cdot)$ iff.$\forall x \in A, Q(x) \Rightarrow P(x)$
(3)$P(\cdot)$ and $Q(\cdot)$ are equivalent iff. $\forall x \in A, P(x) \Leftrightarrow Q(x)$

Proof

$$\begin{aligned}\varnothing &= \{x \in A | P(x)\} - \{x \in A | Q(x)\} \\ &= \{x \in A | P(x) \wedge (\neg Q(x))\} \\ &= A \backslash \{x \in A | (\neg P(x)) \vee Q(x)\} \\ &= A \backslash \{x \in A | P(x) \Rightarrow Q(x)\}\end{aligned}$$

□

Russell's paradox: $P(A) := A \notin A$,The collection of all sets should not be considered as a set.

2.6 Union

Definition 2.6.1 Let I be a set ,and for any $i \in I$, let A_i be a set ,we say that $(A_i)_{i \in I}$ is a family of sets parametrized by I.We denote by $\cup_{i \in I} A_i$ the set of all elements of all A_i.It is also called the **union** of the sets $A_i, i \in I$. By definition,a mathematical object x belongs to $\cup_{i \in I} A_i$ if and only if

$$\exists i \in I, x \in A_i$$

Proposition 2.6.1 $\bigcup_{i \in I} A_i \subseteq B$ if and only if

$$\forall i \in I, A_i \subseteq B$$

Corollary 2.6.1 Let $P_i(\cdot)$be a condition on B,then

$$\{x \in B | \exists i \in I, P_i(x)\} = \bigcup_{i \in I} \{x \in B | P_i(x)\}$$

Proposition 2.6.2

$$\left(\bigcup_{i \in I} A_i\right) \backslash B = \bigcup_{i \in I} (A_i \backslash B)$$

2.7 Intersection

Definition 2.7.1 Let I be a **non-empty** set and $(A_i)_{i\in I}$ be a family os sets parametrized by I. We denote by $\bigcap\limits_{i\in I} A_i$ the set of all common elements of $A_i, i \in I$.This set is called the **intersection** of $A_i, i \in I$.Note that ,if i_0 is an arbitrary element of I ,the set-builder notation ensure that

$$\{x \in A_{i_0} | \forall i \in I, x \in A_i\}$$

is a set. This set id the intersection of $(A_i)_{i\in I}$.
By definition, an mathematical object x belongs to $\cap_{i\in I} A_i$ if and only if

$$\forall i \in I, x \in A_i$$

Remark 2.7.1 In set theory, it does not make sense to consider the intersection of an empty family of sets .In fact, if such an intersection exists as a sets ,for any mathematical object x, since the statement

$$\forall i \in \varnothing, x \in A_i$$

is true, we obtain that x belongs to $\cap_{i\in\varnothing} A_i$.By Russell's paradox, this is impossible.

Proposition 2.7.1 Let I be a non-empty set and $(A_i)_{i\in I}$ be a set parametrised by I. Let B be a set. Then $B \subseteq \cap_{i\in I} A_i$ if and only if

$$\forall\, i \in I,\ B \subseteq A_i.$$

Proof Let $A = \cap_{i\in I} A_i$.
Suppose that $B \subseteq A$. For any $x \in B$, one has $x \in A$, and hence

$$\forall\, i \in I,\ x \in A_i.$$

Therefore, for any $i \in I$, B is contained in A_i.
Suppose that, for any $i \in I$, $B \subseteq A_i$. Then, for any $x \in B$ and any $i \in I$, one has $x \in A_i$. Hence, for any $x \in B$, one has $x \in A$. Therefore, $B \subseteq A$. □

Corollary 2.7.1 Let B be a set, I be a non-empty set. For any $i \in I$, let $P_i(\cdot)$ be a condition on B. Then

$$\{x \in B \mid \forall\, i \in I,\ P_i(x)\} = \bigcap_{i\in I} \{x \in B \mid P_i(x)\}.$$

Proof Let

$$A := \{x \in B \mid \forall\, i \in I,\ P_i(x)\}.$$

For any $i \in I$, let

$$A_i := \{x \in B \mid P_i(x)\}.$$

For any $x \in A$ and any $i \in I$, $P_i(x)$ is true. Hence $A \subseteq A_i$. By Proposition 2.7.1 we obtain

$$A \subseteq \bigcap_{i \in I} A_i.$$

Conversely, if $x \in \bigcap_{i \in I} A_i$, then for any $i \in I$, one has $x \in A_i$. Hence $x \in B$, and for any $i \in I$, $P_i(x)$ is true. Thus $x \in A$. □

Proposition 2.7.2 Let B be a set, $(A_i)_{i \in I}$ be a family of sets. The following equality holds

$$\left(\bigcap_{i \in I} A_i\right) \setminus B = \bigcap_{i \in I} (A_i \setminus B).$$

Proof Let $A := \bigcap_{i \in I} A_i$. For any $i \in I$, one has $A \subseteq A_i$. Hence

$$A \setminus B = \{x \in A \mid x \notin B\} \subseteq \{x \in A_i \mid x \notin B\}.$$

By Proposition 2.7.1 we get

$$A \setminus B \subseteq \bigcap_{i \in I} (A_i \setminus B).$$

Conversely, if $x \in \bigcap_{i \in I} (A_i \setminus B)$, then, for any $i \in I$, one has $x \in A_i \setminus B$, namely $x \in A_i$ and $x \notin B$. Thus $x \in \bigcap_{i \in I} A_i$ and $x \notin B$. Therefore $x \in A \setminus B$. □

Proposition 2.7.3 Let I be a set and $(A_i)_{i \in I}$ be a family of sets parametrised by I. For any set B, the following statements hold.

1. $B \cap (\bigcup_{i \in I} A_i) = \bigcup_{i \in I} (B \cap A_i)$.
2. If $I \neq \varnothing$, $B \cup (\bigcap_{i \in I} A_i) = \bigcap_{i \in I} (B \cup A_i)$,
3. If $I \neq \varnothing$, $B \setminus \bigcup_{i \in I} A_i = \bigcap_{i \in I} (B \setminus A_i)$,
4. If $I \neq \varnothing$, $B \setminus \bigcap_{i \in I} A_i = \bigcup_{i \in I} (B \setminus A_i)$.

Proof 1. By Corollary 2.7.1 we obtain

$$\begin{aligned} B \cap \left(\bigcup_{i \in I} A_i \right) &= \{x \in B \mid \exists\, i \in I,\ x \in A_i\} \\ &= \bigcup_{i \in I} \{x \in B \mid x \in A_i\} = \bigcup_{i \in I} (B \cap A_i). \end{aligned}$$

2. Let $A := \bigcap_{i \in I} A_i$. By definition, for any $i \in I$, one has $A \subseteq A_i$ and hence $B \cup A \subseteq B \cup A_i$. Thus, by Proposition 2.7.1 we obtain

$$B \cup \left(\bigcap_{i \in I} A_i \right) \subseteq \bigcap_{i \in I} (B \cup A_i).$$

Conversely, let $x \in \bigcap_{i \in I} (B \cup A_i)$. For any $i \in I$, one has $x \in B \cup A_i$. If $x \in B$, then $x \in B \cup (\bigcap_{i \in I} A_i)$; otherwise one has

$$\forall\, i \in I,\ x \in A_i,$$

and we still get $x \in B \cup (\bigcap_{i \in I} A_i)$.

3. By Theorem2.4.1

$$\begin{aligned} B \setminus \bigcup_{i \in I} A_i &= \{x \in B \mid \neg(\exists\, i \in I,\ x \in A_i)\} \\ &= \{x \in B \mid \forall\, i \in I,\ x \notin A_i\}. \end{aligned}$$

By Corollary 2.7.1 this is equal to

$$\bigcap_{i \in I} \{x \in B \mid x \notin A_i\} = \bigcap_{i \in I} (B \setminus A_i).$$

4. By Theorem2.4.1

$$\begin{aligned} B \setminus \bigcap_{i \in I} A_i &= \{x \in B \mid \neg(\forall\, i \in I,\ x \in A_i)\} \\ &= \{x \in B \mid \exists\, i \in I,\ x \notin A_i\}. \end{aligned}$$

By Corollary 2.6.1 this is equal to

$$\bigcup_{i \in I} \{x \in B \mid x \notin A_i\} = \bigcup_{i \in I} (B \setminus A_i).$$

□

2.8 Cartesian Product

Definition 2.8.1 Let A and B be sets. We denote by $A \times B$ the following set of ordered pairs

$$\{(x, y) \mid x \in A,\ y \in B\},$$

and call it the **Cartesian product** of sets A and B.
More generally, if n is a positive integer and $A_1, \ldots, A_n$ be sets, we denote by

$$A_1 \times \cdots \times A_n$$

the set of all n-tuples $(x_1, \ldots, x_n)$, where $x_1 \in A_1, \ldots, x_n \in A_n$.

The following proposition shows that ordered pairs can be realized through set-theoretic constructions.

Proposition 2.8.1 Let x, y, x', and y' be mathematical objects. Then

$$\{\{x\}, \{x, y\}\} = \{\{x'\}, \{x', y'\}\}$$

if and only if $x = x'$ and $y = y'$.

Proof If $x = x'$ and $y = y'$, then the equality

$$\{\{x\}, \{x, y\}\} = \{\{x'\}, \{x', y'\}\}$$

certainly holds.
Conversely, suppose the equality

$$\{\{x\}, \{x, y\}\} = \{\{x'\}, \{x', y'\}\}$$

holds. If $x \neq x'$, then $\{x\} \neq \{x'\}$, so $\{x\} = \{x', y'\}$. This still implies $x = x'$, leading to a contradiction. Therefore, $x = x'$ must hold.
Now, assume $y \neq y'$. Then $\{x, y\} \neq \{x', y'\}$, unless $y = x'$ and $x = y'$. Since $x = x'$, this would imply $y = y'$, which is a contradiction. Thus, $\{x, y\} = \{x'\}$ and $\{x', y'\} = \{x\}$. This again leads to $y = x'$ and $x = y'$, resulting in a contradiction. Hence, $y = y'$ must hold. □

Chapter 3

Correspondence

3.1 Correspondence and its Inverse

Definition 3.1.1 We call a **correspondence** any triplet of the form

$$f = (\mathscr{D}_f, \mathscr{A}_f, \Gamma_f)$$

where $\mathscr{D}_f, \mathscr{A}_f$ are two sets, called respectively the **departure set** and the **arrival set** of f and Γ_f is a subset of $\mathscr{D}_f \times \mathscr{A}_f$, called the **graph** of f.
If X, Y are two sets and f is a correspondence of the form (X, Y, Γ_f),we say that f is a correspondence from X to Y.

Definition 3.1.2 Let f be a correspondence.We denote by f^{-1} the correspondence defined as follows:

$$\mathscr{D}_f^{-1} := \mathscr{A}_f, \mathscr{A}^{-1} := \mathscr{D}_f,$$

$$\Gamma_{f^{-1}} := \{(y, x) \in \mathscr{D}_f \times \mathscr{A}_f | (x, y) \in \Gamma_f\}$$

The correspondence f^{-1} is called the **inverse correspondence** of f. Clearly one has

$$(f^{-1})^{-1} = f$$

namely f is the inverse correspondence of f^{-1}

3.2 Illustration of a Correspondence

3.3 Image and Preimage

Definition 3.3.1 Let X, Y be sets ,and f be a correspondence from X to Y. If (x, y) is an element of Γ_f, we say that x is a **preimage** of y under f, and y is an **image** of x under f.
If A is a set , we denote by $f(A)$ the set :

$$\{y \in \mathscr{A}_f | \exists x \in A, (x, y) \in \Gamma_f\}$$

called the image of A by the correspondence f
If B is a set ,the set $f^{-1}(B)$ is called the preimage of B by the correspondence f.
Note that it is by definition the image of B by the inverse correspondence f^{-1}.

Definition 3.3.2 Let f be correspondence. The set $f(\mathscr{D}_f)$ is called the **range** of f, denoted as $\mathrm{Im}(f)$. The set $f^{-1}(\mathscr{A}_f)$ is called the **domain of definition** of f, denoted as $\mathrm{Dom}(f)$. Note that the domain of definition of a correspondence f is the projection of the graph Γ_f to the arrival set $\mathscr{A}_f$.

For any sets A and B,

$$f(A) \subseteq \mathrm{Im}(f), f^{-1}(B) \subseteq \mathrm{Dom}(f),$$

$$\mathrm{Dom}(f) = \mathrm{Im}(f^{-1}), \mathrm{Im}(f) = \mathrm{Dom}(f^{-1})$$

Proposition 3.3.1 Let f be a correspondence.
(1) If A and A' are two sets such that $A' \subseteq A$,then one has $f(A') \subseteq f(A)$.
(2) If B and B' are two sets such that $B' \subseteq B$,then one has $f^{-1}(B') \subseteq f^{-1}(B)$

Proof

$$\begin{aligned} f(B') &= \{y \in \mathrm{Im}(f) | \exists x \in B', (x, y) \in \Gamma_f\} \\ &\subseteq \{y \in \mathrm{Im}(f) | \exists x \in B', (x, y) \in \Gamma_f\} \\ &= f(B) \end{aligned}$$

□

Proposition 3.3.2 Let f be a correspondence. The following equalities hold:

$$\mathrm{Im}(f) = f(\mathrm{Dom}(f)), \mathrm{Dom}(f) = f^{-1}(\mathrm{Im}(f))$$

Proof Since $\mathrm{Dom}(f) \subseteq \mathscr{D}_f$, by proposition 3.3.1,one has

$$f(\mathrm{Dom}(f)) \subseteq f(\mathscr{D}_f) = \mathrm{Im}(f)$$

Let y be an element of $\mathrm{Im}(f)$, there exist $x \in \mathscr{D}_f$ such that $(x, y) \in \Gamma_f$. By definition, one has $x \in \mathrm{Dom}(f)$ and hence $y \in f(\mathrm{Dom}(f)), \mathrm{Im}(f) \subseteq f(\mathrm{Dom}(f))$.Therefore the equality $\mathrm{Im}(f) = f(\mathrm{Dom}(f))$ is true .Applying this equality to f^{-1} , we obtain the second equality. □

Proposition 3.3.3 Let f be a correspondence,A be a set and y be an mathematical object. Then y belongs to $f(A)$ if and only if $A \cap f^{-1}(\{y\}) \neq \varnothing$

Proposition 3.3.4 Let f be a correspondence, I be a set and $(A_i)_{i\in I}$ be a family of sets parametrised by I. Then the equality

$$f\left(\bigcup_{i\in I} A_i\right) = \bigcup_{i\in I} f(A_i)$$

Moreover,if I is not empty, then

$$f\left(\bigcap_{i\in I} A_i\right) \subseteq \bigcap_{i\in I} f(A_i)$$

Proof

$$\begin{aligned} f\left(\bigcup_{i\in I} A_i\right) &= \left\{y \in Y | \left(\bigcup_{i\in I} A_i\right) \cap f^{-1}(\{y\}) \neq \varnothing\right\} \\ &= \left\{y \in Y | \bigcup_{i\in I} \left(A_i \cap f^{-1}(\{y\})\right) \neq \varnothing\right\} \\ &= \left\{y \in Y | \exists i \in I, A_i \cap f^{-1}(\{y\}) \neq \varnothing\right\} = \bigcup_{i\in I} f(A_i) \end{aligned}$$

$$\begin{aligned} f\left(\bigcap_{i\in I} A_i\right) &= \left\{y \in Y | \left(\bigcap_{i\in I} A_i\right) \cap f^{-1}(\{y\}) \neq \varnothing\right\} \\ &= \left\{y \in Y | \bigcap_{i\in I} \left(A_i \cap f^{-1}(\{y\})\right) \neq \varnothing\right\} \\ &\subseteq \left\{y \in Y | \forall i \in I, A_i \cap f^{-1}(\{y\}) \neq \varnothing\right\} \\ &= \bigcap_{i\in I} f(A_i) \end{aligned}$$

□

3.4 Composition

Definition 3.4.1 Let f and g be correspondences. We define the **composite** of g and f as the correspondence $g \circ f$ from $\mathscr{D}_f$ to $\mathscr{A}_g$ whose graph $\Gamma_{g\circ f}$ is composed of the element (x, z) of $\mathscr{D}_f \times \mathscr{A}_g$ such that there exists some objet y satisfying $(x, y) \in \Gamma_f$ and $(y, z) \in \Gamma_g$. In other words,

$$\Gamma_{g\circ f} = \{(x, z) \in \mathscr{D}_f \times \mathscr{A}_g | \exists y \in \mathscr{A}_f \cap \mathscr{D}_g, (x, y) \in \Gamma_f \wedge (y, z) \in \Gamma_g\}$$

Proposition 3.4.1 Let f and g be correspondences. The following equality holds:

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1} \tag{3.4.1}$$

Proposition 3.4.2 Let f and g be correspondences.The following equality holds:

$$h \circ (g \circ f) = (h \circ g) \circ f \tag{3.4.2}$$

Proposition 3.4.3 Let X and Y be sets ,f be a correspondence from X to Y.Then the following equalities hold:

$$f \circ \mathrm{Id}_X = f = \mathrm{Id}_Y \circ f$$

Propositions above can be proved by definition.

Proposition 3.4.4 Let f and g be correspondences.For any set A ,one has

$$(g \circ f)(A) = g(f(A))$$

In particular,

$$\mathrm{Im}(g \circ f) = g(\mathrm{Im}(f)) \subseteq \mathrm{Im}(g)$$

If in addition $\mathrm{Dom}(g) \subseteq \mathrm{Im}(f)$, then the equality $\mathrm{Im}(g \circ f) = \mathrm{Im}(g)$ holds.

Proof By definition,

$$\begin{aligned}(g \circ f)(A) &= \{z \in \mathscr{A}_g | \exists x \in A, (x, z) \in \Gamma_{g \circ f}\} \\ &= \{z \in \mathscr{A}_g | \exists x \in A, \exists y \in \mathscr{A}_f, (x, y) \in \Gamma_f, (y, z) \in \Gamma_g\} \\ &= \{z \in \mathscr{A}_g | \exists y \in f(A), (y, z) \in \Gamma_g\} = g(f(A))\end{aligned}$$

Applying this equality to the case where $A = \mathscr{D}_f$, we obtain

$$\mathrm{Im}(g \circ f) = (g \circ f)(\mathscr{D}_f) = g(f(\mathscr{D}_f)) = g(\mathrm{Im}(f)) \subseteq \mathrm{Im}(g)$$

In the case where $\mathrm{Dom}(g) \subseteq \mathrm{Im}(f)$, by proposition 3.3.1 and 3.3.2 we obtain

$$\mathrm{Im}(g) = g(\mathrm{Dom}(g)) \subseteq g(\mathrm{Im}(f)) = \mathrm{Im}(g \circ f)$$

□

3.5 Surjectivity

Definition 3.5.1 Let f be a correspondence. If $\mathscr{A}_f = \mathrm{Im}(f)$, we say that f is **surjective**. If f^{-1} is surjective , or equivalently $\mathrm{Dom}(f) = \mathscr{D}_f$, we say that f is a **multivalued mapping**.

Remark 3.5.1 multivalued mapping is not always a mapping

Proposition 3.5.1 Let f be a correspondence.Assume that f is surjective. Then ,for any subset B of $\mathscr{A}_f$, one has $B \subseteq f(f^{-1}(B))$.

Proof Let y be an element of B. Since f is surjective there exists $x \in \mathscr{D}_f$ such that $(x, y) \in \Gamma_f$ .Therefore, $x \in f^{-1}(B)$ and hence $y \in f(f^{-1}(B))$ □

Proposition 3.5.2 Let f and g be correspondences.
(1) If $g \circ f$ is surjective, so is g.
(2) If $g \circ f$ is multivalued mapping, so is f.

Proof One has

$$\mathrm{Im}(g \circ f) \subseteq \mathrm{Im}(g) \subseteq \mathscr{A}_g = \mathscr{A}_{g\circ f}$$

If $g \circ f$ is surjective, namely $\mathrm{Im}(g \circ f) = \mathscr{A}_{g\circ f}$, then we deduce $\mathrm{Im}(g) = \mathscr{A}_g$, namely g is surjective. □

Proposition 3.5.3 Let f and g be correspondences.
(1) If g is surjective and $\mathrm{Dom}(g) \subseteq \mathrm{Im}(f)$,then $g \circ f$ is also surjective.
(2) If f is a multivalued mapping and $\mathrm{Im}(f) \subseteq \mathrm{Dom}(g)$, then $g\circ f$ is a multivalued mapping.

Proof (1) Since $\mathrm{Dom}(g) \subseteq \mathrm{Im}(f)$,by proposition3.4.4,we obtain

$$\mathrm{Im}(g \circ f) = \mathrm{g}$$

Since g is surjective,

$$\mathrm{Im}(g) = \mathscr{A}_g = \mathscr{A}_{g\circ f}$$

Hence $g \circ f$ is also surjective.
Applying (1) to g^{-1} and f^{-1} ,we obtain (2). □

3.6 injectivity

Definition 3.6.1 Let f be a correspondence. If each element of $\mathscr{D}_f$ has at most one image under f , we say that f is a **function**.If f^{-1} is a function, we say that f is **injective** .

Notation 3.6.1 Functions form a special case of correspondences.The definition feature of functions is that corresponding to each element in the domain of definition, is a unique element in the arrival set of function.
Let f be a function,and let $x \in \mathrm{Dom}(f)$. We denote the unique image of x under f as $f(x)$,and we say that f sends $x \in \mathrm{Dom}(f)$ to $f(x)$ or $f(x)$ is the **value** of f at x .we can also use the notation:

$$x \mapsto f(x)$$

to indicate the correspondence of x to its image under f.

Proposition 3.6.1 Let f be a correspondence.
(1) Assume that f is injective.For any set A one has $f^{-1}(f(A)) \subseteq A$.
(2) Assume that f is a function. For any set B on has $f(f^{-1}(B)) \subseteq B$.

Proof Let x be an element of $f^{-1}(f(A))$,By definition,there exists $y \in f(A)$ such that $(x, y) \in \Gamma_f$. Since $y \in f(A)$ there exist $x' \in A$ such that $(x', y) \in \Gamma_f$.Since y admits at most one preimage, we obtain $x' = x$. Hence $x \in A$
Applying (1) to f^{-1} we obtain(2). □

Proposition 3.6.2 Let f and g be correspondences.
(1) If f and g are functions, so is $g \circ f$. Moreover, for any $x \in \mathrm{Dom}(g \circ f)$, one has $(g \circ f)(x) = g(f(x))$.
(2) If f and g are injective, so is $g \circ f$.

Proof Let x be an element of $\mathrm{Dom}(g \circ f)$. Assume that z and z' are images of x under $g \circ f$. Let y and y' be such that

$$(x, y) \in \Gamma_f, \quad (y, z) \in \Gamma_g, \quad (x, y') \in \Gamma_f, \quad (y', z') \in \Gamma_g.$$

Since f is a function, one has $y = y' = f(x)$. Since g is a function, we deduce that $z = z' = g(f(x))$. Therefore $g \circ f$ is a function, and the equality $(g \circ f)(x) = g(f(x))$ holds for any $x \in \mathrm{Dom}(g \circ f)$.
Applying (1) to g^{-1} and f^{-1}, we obtain (2). □

Proposition 3.6.3 Let f and g be correspondences.
(1) If $g \circ f$ is injective and $\mathrm{Im}(f) \subseteq \mathrm{Dom}(g)$, then f is also injective.
(2) If $g \circ f$ is a function and $\mathrm{Dom}(g) \subseteq \mathrm{Im}(f)$, then g is also a function.

Proof (1) Let y be an element of the image of f. Let x and x' be preimages of y under f. Since $\mathrm{Im}(f) \subseteq \mathrm{Dom}(g)$, one has $y \in \mathrm{Dom}(g)$.
Hence there exists $z \in \mathscr{A}_g$ such that $(y, z) \in \Gamma_g$.
We then deduce that (x, z) and (x', z) are elements of $\Gamma_{g \circ f}$. Since $g \circ f$ is injective, we obtain $x = x'$. Therefore, f is injective.
Applying (1) to g^{-1} and f^{-1}, we obtain (2). □

Proposition 3.6.4 Let f be a correspondence, and I be a non-empty set.
(1) Suppose that f is a function. For any family $(B_i)_{i \in I}$ of sets parametrised by

I, one has

$$f^{-1}\left(\bigcap_{i\in I} B_i\right) = \bigcap_{i\in I} f^{-1}(B_i).$$

(2) Suppose that f is injective. For any family $(A_i)_{i\in I}$ of sets parametrised by I, one has

$$f\left(\bigcap_{i\in I} A_i\right) = \bigcap_{i\in I} f(A_i).$$

Proof

(1) Let x be an element of $\cap_{i\in I} f^{-1}(B_i)$. For any $i \in I$, one has $f(x) \in B_i$. Hence $x \in f^{-1}(\cap_{i\in I} B_i)$. Therefore we obtain

$$f^{-1}\left(\bigcap_{i\in I} B_i\right) \supseteq \bigcap_{i\in I} f^{-1}(B_i).$$

Combining with (2) of proposition3.3.4 , we obtain the equality

$$f^{-1}\left(\bigcap_{i\in I} B_i\right) = \bigcap_{i\in I} f^{-1}(B_i).$$

Applying (1) to f^{-1}, we obtain (2). □

3.7 Mapping

Definition 3.7.1 A correspondence f is said to be a **mapping** if any element of $\mathscr{D}_f$ has a unique image, or equivalently, f is a function and $\mathscr{D}_f = \mathrm{Dom}(f)$. Note that f is a mapping if and only if f^{-1} is both injective and surjective.

Notation 3.7.1 Let X and Y be sets. We denote by Y^X the set of all mappings from X to Y. An element $u \in Y^X$ is often written in the form of a family of elements of Y parametrised by X as follows

$$(u(x))_{x\in X}.$$

In the case where $X = \{1, \ldots, n\}$, where n is a positive integer, the set $Y^{\{1,\ldots,n\}}$ is also denoted as Y^n. An element u of Y^n is often written as

$$(u(1), \ldots, u(n)).$$

Example 3.7.1

1. Let X be a set. The identity correspondence Id_X is a mapping. It is also called the **identity mapping** of X.
2. Let X and Y be sets and y be an element of Y. The mapping from X to Y sending any $x \in X$ to y is called the **constant mapping with value** y.
3. Let X be a set and $A \subseteq X$, we define $\mathbb{1}_A : X \to \mathbb{R}$

$$\mathbb{1}_A(x) := \begin{cases} 1, \text{if} x \in A \\ 0, \text{if} x \notin A \end{cases}$$

It is called **indicator function**

Remark 3.7.1 Let $f : X \to Y$ be a mapping, I be a set.

1. By (1) of Proposition3.3.4, for any family of sets $(A_i)_{i\in I}$, one has

$$f\left(\bigcup_{i\in I} A_i\right) = \bigcup_{i\in I} f(A_i).$$

By (2) of Proposition 3.3.4, for any family of sets $(B_i)_{i\in I}$, one has

$$f^{-1}\left(\bigcup_{i\in I} B_i\right) = \bigcup_{i\in I} f^{-1}(B_i).$$

2. Assume that I is not empty. By (1) of Proposition 3.3.4, for any family of sets $(A_i)_{i\in I}$, one has

$$f\left(\bigcap_{i\in I} A_i\right) \subseteq \bigcap_{i\in I} f(A_i).$$

By (1) of Proposition 3.6.4, for any family of sets $(B_i)_{i\in I}$, one has

$$f^{-1}\left(\bigcap_{i\in I} B_i\right) = \bigcap_{i\in I} f^{-1}(B_i).$$

3. By (2) of Proposition 3.6.1, for any set B, one has $f(f^{-1}(B)) \subseteq B$. Since f is a function and f^{-1} is injective, by (1) of Proposition 3.6.1 and (2) of Proposition 3.5.1, for any subset A of X one has $f^{-1}(f(A)) = A$.

Proposition 3.7.1 Let f and g be mappings. Suppose that $\mathrm{Im}(f) \subseteq \mathscr{D}_g$. Then $g \circ f$ is also a mapping. Moreover, for any $x \in \mathscr{D}_f = \mathscr{D}_{g\circ f}$ one has

$$(g \circ f)(x) = g(f(x)).$$

Proof Note that $\mathscr{D}_g = \mathrm{Dom}(g)$ since g is a mapping. Hence the statement is a direct consequence of Propositions 3.6.2 and 3.5.3

□

Remark 3.7.2 Let $f : X \to Y$ and $g : Y \to Z$ be mappings.

1. By Proposition 3.5.3, if f and g are both surjective, so is $g \circ f$. By Proposition 3.5.2, if $g \circ f$ is surjective, so is g.
2. By Proposition 3.6.2, if f and g are both injective, so is $g \circ f$. By Proposition 3.6.3, if $g \circ f$ is injective, so is f.

3.8 Bijection

Definition 3.8.1 Let f be a mapping, that is, a correspondence such that f^{-1} is injective and surjective. If f is injective and surjective, we say that f is a **bijection**, or a **one-to-one correspondence**. Note that a correspondence is a bijection if and only if its inverse is a bijection.

Proposition 3.8.1 Let X and Y be sets, f be a correspondence from X to Y. If f is a bijection, then $f^{-1} \circ f = \mathrm{Id}_X$ and $f \circ f^{-1} = \mathrm{Id}_Y$. Conversely, if there exists a correspondence g such that $g \circ f = \mathrm{Id}_X$ and $f \circ g = \mathrm{Id}_Y$, then f is a bijection and $g = f^{-1}$.

Proof If f is a bijection, then f and f^{-1} are both mappings. By Proposition 3.7.1, one has

$$\forall x \in X, \quad (f^{-1} \circ f)(x) = f^{-1}(f(x)) = x,$$

$$\forall y \in Y, \quad (f \circ f^{-1})(y) = f(f^{-1}(y)) = y.$$

Hence $f^{-1} \circ f = \mathrm{Id}_X$ and $f \circ f^{-1} = \mathrm{Id}_Y$.
Assume that g is a correspondence such that $g \circ f = \mathrm{Id}_X$ and $f \circ g = \mathrm{Id}_Y$. Since identity correspondences are surjective mappings, by Proposition 3.5.2, we deduce from the equality $g \circ f = \mathrm{Id}_X$ that g is surjective and $\mathrm{Dom}(f) = X =$

$\mathrm{Im}(g)$. Similarly, we deduce from the equality $f \circ g = \mathrm{Id}_Y$ that f is surjective and $\mathrm{Dom}(g) = Y = \mathrm{Im}(f)$.
Since identity correspondences are injective, by Proposition 3.6.5, we deduce from $g \circ f = \mathrm{Id}_X$ that f is injective. Similarly, we deduce from $f \circ g = \mathrm{Id}_Y$ that f is a function. Therefore, f is a mapping which is injective and surjective, namely a bijection.
Finally, by Propositions 3.4.3 and 3.4.2, we obtain

$$g = g \circ \mathrm{Id}_Y = g \circ (f \circ f^{-1}) = (g \circ f) \circ f^{-1} = \mathrm{Id}_X \circ f^{-1} = f^{-1}.$$

□

Proposition 3.8.2 Let $f : X \to Y$ and $g : Y \to Z$ be bijections. Then the composite correspondence $g \circ f$ is also a bijection.

Proof This is a direct consequence of Propositions 3.7.1, 3.6.2 and 3.5.3

□

Proposition 3.8.3 Let X and Y be sets, f be a correspondence from X to Y, and g be a correspondence from Y to X. If $f \circ g$ and $g \circ f$ are bijections, then f and g are both bijections.

Proof By Proposition 3.5.2, f and g are surjective and are multivalued mappings. In particular,

$$\mathrm{Dom}(f) = X, \quad \mathrm{Im}(f) = Y, \quad \mathrm{Dom}(g) = Y, \quad \mathrm{Im}(g) = X.$$

Therefore, by Proposition 3.6.3, we deduce that f and g are injective and are functions. Hence f and g are both bijections.

□

3.9 Direct product

Definition 3.9.1 Let I be a set and $(A_i)_{i \in I}$ be a family of sets parametrised by I. We denote by

$$\prod_{i \in I} A_i$$

the set of all mappings from I to $\bigcup_{i \in I} A_i$ which send any $i \in I$ to an element

of A_i. This set is called the **direct product** of $(A_i)_{i\in I}$. Using Notation 3.7.1 we often write an element of the direct product in the form of a family $x := (x_i)_{i\in I}$ parametrised by I, where each x_i is an element of A_i, called the i-th *coordinate* of x. In the case where I is the empty set, the union $\bigcup_{i\in I} A_i$ is empty. Therefore, the direct product contains a unique element (identity mapping of $\varnothing$).
For each $j \in I$, we denote by

$$\mathrm{pr}_j : \prod_{i\in I} A_i \longrightarrow A_j$$

the mapping which sends each element $(a_i)_{i\in I}$ of the direct product to its j-th coordinate a_j. This mapping is called the *projection to the j-th coordinate*.

Notation 3.9.1 Let n be a non-zero natural number. If $(A_i)_{i\in\{1,\dots,n\}}$ is a family of sets parametrised by $\{1,\dots,n\}$, then the set

$$\prod_{i\in\{1,\dots,n\}} A_i$$

is often denoted as

$$A_1 \times \cdots \times A_n.$$

Axiom 1 (Axiom of choice) In this book, we adopt the following axiom. If I is a non-empty set and if $(A_i)_{i\in I}$ is a family of non-empty sets, then the direct product $\prod_{i\in I} A_i$ is not empty.

Proposition 3.9.1 Let I be a set and $(A_i)_{i\in I}$ be a family of sets parametrised by I. For any set X, the mapping

$$\left(\prod_{i\in I} A_i\right)^X \longrightarrow \prod_{i\in I} A_i^X,$$

which sends f to $(\mathrm{pr}_i \circ f)_{i\in I}$, is a bijection.

$$\begin{array}{ccc} X & \xrightarrow{f} & \displaystyle\prod_{i\in I} A_i \\ & \searrow^{f_j} & \downarrow{\scriptstyle \mathrm{pr}_j} \\ & & A_j \end{array}$$

Proof Let $(f_i)_{i\in I}$ be an element of

$$\prod_{i\in I} A_i^X,$$

where each f_i is a mapping from X to A_i. Let $f : X \to \prod_{i\in I} A_i$ be the mapping which sends $x \in X$ to $(f_i(x))_{i\in I}$. By definition, for any $i \in I$ one has

$$\forall x \in X, \quad \mathrm{pr}_i(f(x)) = f_i(x).$$

Therefore the mapping is surjective.
If f and g are two mappings from X to $\prod_{i\in I} A_i$ such that $\mathrm{pr}_i \circ f = \mathrm{pr}_i \circ g$ for any $i \in I$, then, for any $x \in X$ one has

$$\forall i \in I, \quad \mathrm{pr}_i(f(x)) = \mathrm{pr}_i(g(x)).$$

Hence $f(x) = g(x)$ for any $x \in X$, namely $f = g$. Therefore the mapping is injective. □

Notation 3.9.2 Let I be a set, $(A_i)_{i\in I}$ be a family of sets parametrised by I. Let X be a set. For any $i \in I$, let $f_i : X \to A_i$ be a mapping from X to A_i. By Proposition 3.9.1 there exists a unique mapping $f : X \to \prod_{i\in I} A_i$ such that $\mathrm{pr}_i \circ f = f_i$ for any $i \in I$. By abuse of notation, we denote by $(f_i)_{i\in I}$ this mapping.
Let $(B_i)_{i\in I}$ be a family of sets parametrised by I. For any $i \in I$, let $g_i : B_i \to A_i$ be a mapping from B_i to A_i. We denote by

$$\prod_{i\in I} g_i : \prod_{i\in I} B_i \longrightarrow \prod_{i\in I} A_i$$

the mapping which sends $(b_i)_{i\in I}$ to $(g_i(b_i))_{i\in I}$. In the case where $I = \{1, \ldots, n\}$, where n is a non-zero natural number, the mapping $\prod_{i\in\{1,\ldots,n\}} g_i$ is also denoted as

$$g_1 \times \cdots \times g_n.$$

Proposition 3.9.2 Let $f : X \to Y$ be a mapping.

(1) If f is surjective, then there exists an injective mapping $g : Y \to X$ such that $f \circ g = \mathrm{Id}_Y$.

(2) If f is injective and X is not empty, then there exists a surjective mapping $h : Y \to X$ such that $h \circ f = \mathrm{Id}_X$.

Proof (1) The case where $Y = \varnothing$ is trivial since in this case $X = \varnothing$ and f is the identity mapping of $\varnothing$. In the following, we assume that Y is not empty. Since f is surjective, for any $y \in Y$, the set $f^{-1}(\{y\})$ is not empty. Hence the direct product

$$\prod_{y \in Y} f^{-1}(\{y\})$$

is not empty. In other words, there exists a mapping g from Y to X such that $f(g(y)) = y$ for any $y \in Y$, that is $f \circ g = \mathrm{Id}_Y$. By (2) of Remark 3.7.2 g is injective.
(2) Let x_0 be an element of X. We define a mapping $h : Y \to X$ as follows:

$$h(y) := \begin{cases} f^{-1}(y), & \text{if } y \in \mathrm{Im}(f), \\ x_0, & \text{else.} \end{cases}$$

Then, by construction one has $h \circ f = \mathrm{Id}_X$.
By (1) of Remark 3.7.2 h is surjective. □

3.10 Restriction and Extension

Definition 3.10.1 Let f and g be correspondence. If $\Gamma_f \subseteq \Gamma_g$, we say that f is a **restriction** of g and that g is an **extension** of f
Let X anf Y be sets, h be a correspondence from X to Y ,and A be a subset of X.Denote by $h|_A$ the correspondence from A to Y such that

$$\Gamma_{h|_A} = \Gamma_h \bigcap (A \times Y)$$

We call it the **restriction of** h **to** A

Chapter 4

Binary Relations

†This chapter was written in pre-course at first,then added some sections in make-up session,which titled ”Ordering”.Some notations haven't been changed yet and some sections have the same knowledge.It's a bit mess.

4.1 Generalities

Definition 4.1.1 Let X be a set ,we call **binary relation** on X any correspondence from X to X .If R is a binary relation on X ,for any $(x, y) \in X \times X$ we denote by xRy the statement $(x, y) \in \Gamma_R$

Example 4.1.1 We denote by” $=$” the correspondence Id_X

Definition 4.1.2 If R is a binary relation on X, we denote by $\not{R}$ the binary relation such that

$$x\not{R}y \Leftrightarrow (x, y) \notin \Gamma_R$$

4.2 Equivalent Relation

Definition 4.2.1 Let X be a set and R a binary relation on X.
(1) If $\forall x \in X, xRx$, we say that R is **reflexive**
(2) If $\forall (x, y) \in X \times X, xRy \Rightarrow yRx$,we say that R is **symmetric**.
(3) If for all x, y, z of X, $xRy \wedge yRz \Rightarrow xRz$,we say that R is **transitive**.
(4) If R is reflexive,symmetric and transitive, we say that R is an **equivalent relation**

Definition 4.2.2 Let $\sim$ be an equivalent relation on X.For any $x \in X$, the set

$$[x] := \{y \in X | y \sim x\}$$

We call it the equivalent class of x under $\sim$,we denote by $X/\sim$ the set $\{[x]|x \in X\}$ of all equivalent class.It is a subset of $\wp(X)$.Moreover, since $\forall x \in X, x \in [x]$,one has

$$X = \bigcup_{A \in X/\sim} A$$

Proposition 4.2.1 $\forall (x, y) \in X \times X$,either $[x] = [y]$ or $[x] \cap [y] = \varnothing$

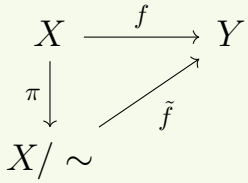
Definition 4.2.3 The mapping $\pi : X \to X/\sim$ is called the **projection mapping** of $\sim$

Proposition 4.2.2 $f : X \to Y$ be a mapping,if $\forall (x, y) \in X \times X, x \sim y \Rightarrow f(x) = f(y)$,then there exists a unique mapping

$$\tilde{f} : X/\sim \to Y, [x] \mapsto f(x)$$

such that

$$\tilde{f} \circ \pi = f$$



4.3 Partial Order

Definition 4.3.1 If
(1) R is reflexive.
(2) R is antisymmetric $\forall (x, y) \in X^2, xRy$ and yRx then $x = y$.
(3) R is transitive.
then we say that R is a **partial order** on X and (X, R) is a **partially ordered set**.If in addition ,$\forall (x, y) \in X, xRy$ or yRx, we say that R is a **total order** and (X, R) is totally ordered set.

Example 4.3.1 $(\mathbb{R}, \leq)$ is a totally ordered set.$(\mathbb{N}, |)$ is a partially ordered set.

Definition 4.3.2 Let $(X, \underline{R})$ be a partially ordered set. We denote by R the binary relation on X defined as:

$$xRy \Leftrightarrow x\underline{R}y \wedge x \neq y$$

we call R the **strict partial order**(not a partial order) associated with $\underline{R}$.

Example 4.3.2
(1)$<$ on $\mathbb{R}$
(2)$\subset$on$\wp(X)$

Proposition 4.3.1 R is the strict partial order associated with some partial order iff.the following condition are satisfied:
(1)Irreflexivity $\forall x \in X, x\not{R}x$
(2)Asymmetry.$\forall (x, y) \in X^2, xRy \Rightarrow y\not{R}x$
(3)Transitivity.

Proof "$\Rightarrow$" :easy
"$\Leftarrow$":Suppose that R is a binary relation satisfying $(1) \sim (3)$.Define another binary relation $\underline{R}$ on X as:

$$x\underline{R}y \Leftrightarrow xRy \vee x = y$$

We claim that $xRy \Leftrightarrow x\underline{R}y \wedge x \neq y$:
Suppose that xRy, then by definition,$x\underline{R}y$.By the irreflexivity ,$x \neq y$
Conversely,if $x\underline{R}y \wedge x \neq y$,then xRy should be true. □

4.4 Monotonic Functions

Definition 4.4.1 Let$(I, \leq)$ and $(X, \leq)$ be partially ordered sets,and f be a function from I to X.
(1) If $\forall (x, y) \in \mathrm{Dom}(f)^2, x < y \Rightarrow f(x) \leq f(y)$ we say that f is increasing
(2) If $\forall (x, y) \in \mathrm{Dom}(f)^2, x < y \Rightarrow f(x) < f(y)$, we say that f is strictly increasing.
(3) If $\forall (x, y) \in \mathrm{Dom}(f)^2, x < y \Rightarrow f(x) \geq f(y)$, we say that f is decreasing.

(4) If $\forall(x,y) \in \mathrm{Dom}(f)^2, x < y \Rightarrow f(x)\ f(y)$, we say that f is strictly decreasing.
increasing and decreasing functions are called **monotonic function**,strictly increasing and decreasing functions are called **strictly monotonic function**

Proposition 4.4.1 Let f, g be functions between partially ordered sets.
(1) If both f and g are increasing or both f and g are decreasing,then $g \circ f$ is increasing
(2) If one function between f and g is increasing while the order is decreasing,then $g \circ f$ is decreasing.

Proposition 4.4.2 Let f be a function between partially ordered set. If f is monotonic and injective,then f is strictly monotonic.

Proposition 4.4.3 Let I be a totally ordered set,X be a partially ordered set ,and f be a function from I to X .I f f is strictly monotonic ,then f is injective.

Proof Let $(x,y) \in \mathrm{Dom}(f)^2$,such that $f(x) = f(y)$.Since I is totally ordered, then $x < y$ or $x > y$ or $x = y$.Suppose that f is strictly increasing.If $x < y$,then $f(x) < f(y)$,contradiction. If $x > y$,then $f(x) > f(y)$,contradiction. □

Proposition 4.4.4 Let X be a totally ordered set ,Y be an partially ordered set ,f be an injective function from X to Y. If f is monotonic, then f^{-1} is also monotonic,and they have the same monotonic direction.

Proof We may suppose that f is increasing. Let $(a,b) \in \mathrm{Dom}(f^{-1})^2 = \mathrm{Im}(f)^2, a < b$.Since f^{-1} is a injective function,$f^{-1}(a) \neq f^{-1}(b)$,so either $f^{-1}(a) < f^{-1}(b)$ or $f^{-1}(a) > f^{-1}(b)$.If

$$f^{-1}(a) > f^{-1}(b), a = f(f^{-1}(a)) > f^{-1}(b) = b$$

Contradiction.Therefore,$f^{-1}(a) < f^{-1}(b)$.Hence f^{-1} is strictly increasing □

4.5 Bounds

Definition 4.5.1 Let $(X, \leq)$ be a partially ordered set ,let A be a subset of X.
(1) Let $M \in X$. If $\forall a \in A, a \leq M$, we say that M is an upper bound of A.
(2) Let $m \in X$. If $\forall a \in A, m \leq a$, we say that m is an lower bound of A.
Denote by A^u the set of upper bounds of A in $(X, \leq)$
Denote by A^l the set of lower bounds of A in $(X, \leq)$

Example 4.5.1 $\Omega = \{1, 2, 3\}, X = \wp(\Omega).(X, \subseteq)$ forms a partially ordered set.Let $A = \{\{1\}, \{2\}, \{1, 2\}\}, A^u = \{\{1, 2\}, \{1, 2, 3\}\}, A^l = \{\varnothing\}$

Definition 4.5.2 Let $(X, \leq)$ be a partially ordered set ,let A be a subset of X.
(1)If $M \in A$ is an upper bound of A, we say that M is the **greatest element** of A ,denote as $\max_{\leq} A$
(2)If $m \in A$ is an lower bound of A, we say that m is the **least element** of A ,denote as $\min_{\leq} A$
If there is not ambiguity on $\leq$,we can also write as $\max A, \min A$

Definition 4.5.3 $A \subseteq Y \subseteq X$,let $A_Y^{\mathrm{u}} := \{y \in Y | \forall a \in A, a \leq y\}$ be the set of upper bounds of A in Y.If A_Y^{u} has a least element ,we call it the **supremum** of A in Y ,denoted as $\sup_{(Y,\leq)} A$,if there's no ambiguity on $\leq$ we can also write as $\sup_Y A$.So as **infimum**

Notation 4.5.1 Let $(X, \leq)$ be a partially ordered set ,$f : I \to X$ be a function.

$$\max f(I), \min f(I), \sup f(I), \inf f(I)$$

are written as

$$\max f, \min f, \sup f, \inf f$$

Let $(X, \leq)$ be a partially ordered set ,and $(x_i)_{i \in I} \in X^I$,

$$\max\{x_i | i \in I\}, \min\{x_i | i \in I\}, \sup\{x_i | i \in I\}, \inf\{x_i | i \in I\}$$

are denoted as

$$\max_{i \in I} x_i, \min_{i \in I} x_i, \sup_{i \in I} x_i, \inf_{i \in I} x_i$$

Proposition 4.5.1 Let $(X, \leq)$ be a partially ordered set $(A, Z, Y) \in \wp(X)^3, A \subseteq Z \subseteq Y$
(1) If $\max A$ exists,then it is also the supremum of A in $(Y, \leq)$.So as infimum
(2) If $\sup_{(Y,\leq)} A$ exists and belongs to Z ,then it is also the supremum of A in $(Z, \leq)$. So as infimum

Proof
(1) By definition,$\max A$ is an upper bound of A. Since $A \subseteq Y, \max A \in Y$,Hence $\max A \in A^{\mathrm{u}}_Y$.Let $M \in A^{\mathrm{u}}_Y$.Since M is upper bound of A and $\max A \in A, \max A \leq M$ .Then $\max A = \min A^{\mathrm{u}}_Y$
(2) Since $Z \subseteq Y, A^{\mathrm{u}}_Z \subseteq A^{\mathrm{u}}_Y$.For any $M \in A^{\mathrm{u}}_Z$,one has $\sup_{Y,\leq} A \leq M$.If $\sup_{(Y,\leq)} A \in Z$,then $\sup_{(Y,\leq)} A \in A^{\mathrm{u}}_Z$.Hence $\sup_{(Y,\leq)} A = \min A^{\mathrm{u}}_Z$ □

Proposition 4.5.2 Let $(X, \leq)$ be a partially ordered set ,$(A, B, Y) \in \wp(X)^3, A \subseteq B \subseteq Y$
(1) If $\sup_{(Y,\leq)} A$ and $\sup_{(Y,\leq)} B$ exist, then

$$\sup_{(Y,\leq)} A \leq \sup_{(Y,\leq)} B$$

(2)If $\inf_{(Y,\leq)} A$ and $\inf_{(Y,\leq)} B$ exist, then

$$\inf_{(Y,\leq)} B \leq \inf_{(Y,\leq)} A$$

Proof
(1) $\forall x \in A$,since $A \subseteq B, x \in B \leq \sup B$,by definition, $\sup B$ is an upper bound of A,$\sup B \in A^{\mathrm{u}}_Y$.$\sup A$ is the least in A^{u}_Y.Hence,$\sup_{(Y,\leq)} A \leq \sup_{(Y,\leq)} B$ □

Proposition 4.5.3 Let $(X, \leq)$ be a partially ordered set ,f, g be elements of X^I where I is a set .Suppose that ,$\forall i \in I, f(i) \leq g(i)$
(1)If $\sup f, \sup g$ exist ,then $\sup f \leq \sup g$
(2)So as infimum.

Proof $\forall t \in I, f(t) \leq g(t) \leq \sup g$,hence $\sup g$ is an upper bound of f.Since $\sup f$ is a the least upper bound of $f(i)$,$\sup f \leq \sup g$. □

Proposition 4.5.4 Let I be a totally ordered set $J \subseteq I$,and $f : I \to X$ be a mapping. Assume that J does not have any upper bound in I.
(1) If f is increasing, then $f(I)^{\mathrm{u}} = f(J)^{\mathrm{u}}$
(2) If f is decreasing, then $f(I)^{\mathrm{l}} = f(J)^{\mathrm{l}}$

Proof
(1) $f(J) \subseteq f(I)$ Any upper bound of $f(I)$ is also an upper bound of $f(J)$,hence $f(I)^{\mathrm{u}} \subseteq f(J)^{\mathrm{u}}$.Let $M \in f(J)^{\mathrm{u}}$,for any $i \in I, \exists j \in J, i < j$. Hence $f(i) \leq f(j) \leq M$ .So $M \in f(I)^{\mathrm{u}}$,$f(J)^{\mathrm{u}} \subseteq f(I)^{\mathrm{u}}$.Therefore,$f(I)^{\mathrm{u}} = f(J)^{\mathrm{u}}$. □

Proposition 4.5.5 Let $(X, \leq)$ be a partially ordered set ,$Y \subseteq X, I$ be a set, and $(A_i)_{i\in I} \in \wp(Y)^I$ .Let $A = \cup_{i\in I} A_i$
(1) Suppose that ,$\forall i \in I, A_i$ has a supremum y_i in $(Y, \leq)$ and $\{y_i | i \in I\}$ has a supremum in $(Y, \leq)$. Then A has a supremum in $(Y, \leq)$ and

$$\sup_{(Y,\leq)} A = \sup_{(Y,\leq)} \{y_i | i \in I\}$$

(2)So as inf

Proof Let $y = \sup_{(Y,\leq)}\{y_i | i \in I\}, \forall a \in A, \exists i \in I, a \in A_i$. Hence $a \leq y_i \leq y$. Thus y is an upper bound of A in Y.Let $M \in A_Y^{\mathrm{u}}, \forall i \in I, M \in (A_i)_Y^{\mathrm{u}}$, So $y_i \leq M$We then deduce that $y \leq M$ □

Proposition 4.5.6 Let $(X, \leq)$ be a partially ordered set ,$Y \subseteq X$.

$$\varnothing_Y^{\mathrm{u}} = \varnothing_Y^{\mathrm{l}} = Y$$

4.6 Intervals

Definition 4.6.1 Let $(X, \leq)$ be a partially ordered set.$\forall (a, b) \in X^2$, let

$$[a, b] := \{x \in X | a \leq x \leq b\}$$

$$[a, b[:= \{x \in X | a \leq x < b\}$$

We say that a subset is a **interval** if $\forall (a, b) \in I^2, [a, b] \subseteq I$

Proposition 4.6.1 Let $(X, \leq)$ be a partially ordered set ,let Λ be a non-empty set and $(I_\lambda)_{\lambda\in\Lambda}$ be a family of interval in X, then
(1) $I := \bigcap\limits_{\lambda\in\Lambda} I_\lambda$ is an intervals
(2) If $\bigcap\limits_{\lambda\in\Lambda} I_\lambda \neq \varnothing$,then $J := \bigcup\limits_{\lambda\in\Lambda} I_\lambda$ is an interval.

Proof (2):Let $x \in I = \cap_{\lambda\in\Lambda} I_\lambda$,let $(a, b) \in J^2, \exists(\alpha, \beta) \in \Lambda^2, \alpha \in I_\alpha, \beta \in I_\beta$.We will show that $[a, b] \subseteq I_\alpha \cup I_\beta$. If $a \not\leq b$, then $[a, b] \neq \varnothing \subseteq I_\alpha \cup I_\beta$. We may assume $a \leq b$
If $b \leq x$, then $[a, b] \subseteq [a, x] \subseteq I_\alpha$, if $x \leq a$, then $[a, b] \subseteq [x, b] \subseteq I_\beta$.Suppose that $a < x < b$,one has $[a, b] = [a, x] \cup [x, b]$ and so on , $[a, b] = [a, x] \cup [x, b] \subseteq I_\alpha \cup I_\beta \subseteq J$

□

Definition 4.6.2 Let $(X, \leq)$ be a partially ordered set and I be a non-empty interval in X.
If $\sup I$ exists ,we call it the right endpoint of I.
If $\inf I$ exists ,we call it the left endpoint of I.

Proposition 4.6.2 Let $(X, \leq)$ be a totally ordered set and I be a interval in X
(1) Suppose that I has a supremum b in $X, \forall x \in I, [x, b[\subseteq I$
(2) Suppose that I has a infimum b in $X, \forall x \in I,]b, x] \subseteq I$

Remark 4.6.1 totally ordered set condition is used to prove (2)

Proposition 4.6.3 Let $(X, \leq)$ be a totally ordered set and I be a non-empty interval in X .Assume that I has an infimum a and a supremum b in X. Then I is one of the following sets:$[a, b], [a, b[,]a, b],]a, b[$

Proof $\forall x \in I, a \leq x \leq b$,hence $I \subseteq [a, b]$
(i) if $\{a, b\} \in I$, then $I = [a, b]$
(ii) if $a \in I, b \notin I, I \subseteq [a, b[= [a, b]\backslash\{b\}$. Let $x \in [a, b[$, since $x < b$, x is not an upper bound of I. Hence $\exists y \in I, x < y$. Note that $[a, y] \subseteq I$, hence $x \in I$, therefore $[a, b[\subseteq I$. Similarly , is $b \in I, a \notin I$, then $]a, b] = I$
(iii) if $\{a, b\} \cap I = \varnothing$, then $I \subseteq]a, b[.\forall x \in]a, b[, \exists s, t \in I, s < x < t$ Hence $x \in [s, t] \subseteq I$. Therefore $]a, b[= I$

□

Definition 4.6.3 (Dense) Let $(X, \leq)$ be a totally ordered set, if $\forall (x, z) \in X^2, x < z \Rightarrow]x, z[\neq \varnothing$ then we say that $(X, \leq)$ is **dense**.

Proposition 4.6.4 Let $(X, \leq)$ be a totally ordered set that is dense, $(a, b) \in X^2, a < b$. If I is one of the intervals $[a, b], [a, b[\ldots$, then $a = \inf I, b = \sup I$

Proof By definition, b is an upper bound of I, since $(X, \leq)$ is a totally ordered set,if b is not the supremum of I , $\exists M \in I^{\mathrm{u}}$ such that $M < b$. Let $x \in I$,one has $x \leq M < b$.Since $[x, b[\subseteq I, M \in I$, hence $M = \max I$. Since X is dense ,pick $M' \in]M, b[$.Since $M \in I, b = \sup I, [M, b[\subseteq I$. Hence $M' \in I, M' \leq M$.This contradicts $M < M'$. □

4.7 Well-ordered Set

Definition 4.7.1 Let $(X, \leq)$ be a partially ordered set.If $\forall A \in \wp(X), A \neq \varnothing \Rightarrow A$ has a least element,we say that $(X, \leq)$ is a **well-ordered set**.

Axiom 2 $(\mathbb{N}, \leq)$ is a well-ordered set

Proposition 4.7.1 If $(X, \leq)$ is a well-ordered set, then it is a totally ordered set.

Proposition 4.7.2 $(X, \leq)$ is a well-ordered set,$Y \subseteq X$, then $(Y, \leq)$ is a well-ordered set.

Theorem 4.7.1 Let $(X, \leq)$ be a well-ordered ste .Let $P(\cdot)$ be a condition on X. If

$$\forall x \in X, (\forall y \in X_{<x}, P(y)) \Rightarrow P(x)$$

then $\forall x \in X, P(x)$

Remark 4.7.1 Suppose that $X \neq \varnothing$,There is a least element m of X.The statement

$$\forall x \in X, (\forall y \in X_{<m}, P(m)) \Rightarrow P(x) \text{and} P(m) \text{have the same truth value}$$

Proof Let $A = \{x \in X | \neg P(x)\}$.If $A \neq \varnothing, \exists x \in A$ which is the least element of A.By definition,$(\forall y \in X_{<x}, P(y))$ is true.It contradicts to . □

Remark 4.7.2 We add a formal element $+\infty$ to $\mathbb{N}$ and require $\forall n \in \mathbb{N}, n < +\infty$

Fact:$\mathbb{N}\cup\{+\infty\}$ is a well-ordered set.Let $P(\cdot)$ be a condition on $\mathbb{N}\cup\{+\infty\}$,We need to check:

1. $P(0)$
2. $\forall n\in\mathbb{N}_{\leq 1}, P(0)\wedge\cdots\wedge P(n-1)\Rightarrow P(n)$
3. $(\forall n\in\mathbb{N}, P(n))\Rightarrow P(+\infty)$

4.8 Order-completeness

Definition 4.8.1 Let $(X,\leq)$ be a partially ordered set .If any subset of X has a supremum in X, we say that $(X,\leq)$ is **order-complete**. Note that an order-complete partially ordered set is never empty.

Axiom 3 Let $\overline{\mathbb{R}}:=\mathbb{R}\cup\{-\infty,+\infty\}$, where $-\infty,+\infty$ are distinct formal elements that do not belongs to $\mathbb{R}$.If we equip $\overline{\mathbb{R}}$ with the total order extending that of $\mathbb{R}$ such that

$$\forall x\in\mathbb{R}, -\infty<x<+\infty$$

, then $(\overline{\mathbb{R}},\leq)$ is order complete.

Example 4.8.1 Let Ω be a set ,$X=\wp(\Omega)$.Then $(X,\subseteq)$ is order complete.

Proof Let $Y\subseteq X$.Then

$$Y^{\mathrm{u}}=\{B\in\wp(\Omega)|\forall A\in Y, A\subseteq B\}$$

$\bigcup_{A\in Y} A$ is the least upper bound of Y in X. So $\sup(Y)=\cup_{A\in Y}A$ □

Proposition 4.8.1 Let $(X,\leq)$ be an order complete partially ordered set. Any subset of X has an infimum in X.

Proof Let $A\subseteq X, m:=\sup A^{\mathrm{l}}$. We prove that $m\in A^{\mathrm{l}}$
Let $x\in A, \forall y\in A^{\mathrm{l}}, y\leq x$,so $x\in(A^{\mathrm{l}})^{\mathrm{u}}$.Hence $m\leq x$ □

Here Huayi gave a notation which have been given in Notation4.5.1,then came to Proposition4.5.1 and the following.

Definition 4.8.2 Let X be a set and $f : X \to X$ be a mapping. If $x \in X$ is such that $f(x) = x$, then we say that x is a fixed point of f.

Theorem 4.8.1 (Knaster-Tarski fixed point)
Let $(X, \leq)$ be an order complete partially ordered set ,$f : X \to X$ be an increasing mapping.Let

$$F = \{x \in X | f(x) = x\}$$

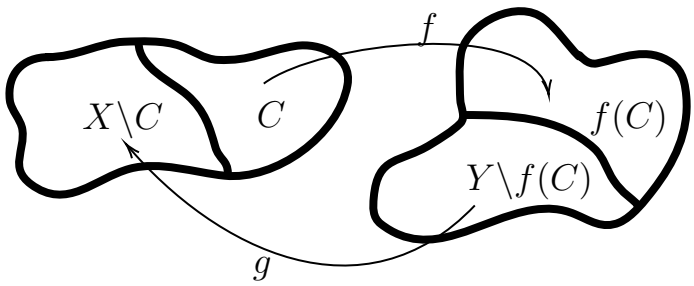
Then $(F, \leq)$ is order complete.In particular $F \neq \varnothing$

Proof Let A be a subset of F.We consider

$$S_A := \{y \in A^{\mathrm{u}} | f(y) \leq y\}$$

Let $m := \inf S_A, \forall a \in A, a$ is a lower bound of S_A.So $a \leq m$.So $m \in A^{\mathrm{u}}, \sup A \leq m$.For any $y \in S_A$,one has $m \leq y$.Since f is increasing, $f(m) \leq f(y) \leq y$ .So $f(m)$ is a lower bound of S_A, which leads to $f(m) \leq m$ .That means $m \in S_A$.Hence $m = \min S_A$.For any $x \in A, x = f(x) \leq f(m)$.So $f(m) \in A^{\mathrm{u}}$.Moreover ,since $f(m) \leq m, f(f(m)) \leq f(m)$.So $f(m)$ is an element of S_A, which leads to $m \leq f(m)$.Hence $m \in F$.Therefore, $m = \sup_{(F,\leq)} A$ □

Definition 4.8.3 Let X, Y be sets.If there exists a bijection from X to Y, we say that X and Y are **equipotent**.



Theorem 4.8.2 (Cantor-Bernstein) Let X and Y be sets .Assume that there exists injective mappings $f : X \to Y$ and $g : Y \to X$.Then X and Y are equipotent.

Proof Consider $\Phi : \wp(X) \to \wp(X), A \mapsto X\backslash g(Y\backslash f(A))$.If $(A,B) \in \wp(X)^2$ such that $A \subseteq B$, then $f(A) \subseteq f(B), Y\backslash f(A) \supseteq Y\backslash f(B), g(Y\backslash f(A)) \supseteq g(Y\backslash f(A)), \Phi(A) \subseteq \Phi(B)$.So Φ is increasing.By Knaster-Tarski theorem,$\exists C \in \wp(X), C = \Phi(C)$.Then $h : X \to Y, h(x) := \begin{cases} f(x), x \in C \\ g^{-1}(x), x \in X\backslash C \end{cases}$ is a bijection. □

Lemma 4.8.3 Let $(X, \leq)$ is a partially ordered set.
(1) Let $(A,B) \in \wp(X)^2$, if $A \subseteq B$, then $B^{\mathrm{u}} \subseteq A^{\mathrm{u}}, B^{\mathrm{l}} \subseteq A^{\mathrm{l}}$
(2) $\forall A \in \wp(X), A \subseteq (A^{\mathrm{u}})^{\mathrm{l}} \cap (A^{\mathrm{l}})^{\mathrm{u}}$

Theorem 4.8.4 (Dedekind-MacNeille)
Let $(X, \leq)$ be a partially ordered set.Let $\hat{X} := \{A \in \wp(X) | (A^{\mathrm{u}})^{\mathrm{l}} = A\}$
(1) $(\hat{X}, \subseteq)$ is order complete.
(2) $\forall A \in \wp(X), A^{\mathrm{l}} \in \hat{X}$
(3) $X \to \hat{X}, x \mapsto \{x\}^{\mathrm{l}}$ is strictly increasing.
(4) $\forall A \in \hat{X}$ one has $A = \cup_{x \in A} \{x\}^{\mathrm{l}} = \cup_{x \in A} \hat{x}$.In particular,

$$A = \sup_{(\hat{X}, \subseteq)} \{\hat{x} | x \in A\}$$

(5) Let $A \in \hat{X}$.If $A\mathrm{u} = \varnothing$,then $A = X$.If $A^{\mathrm{u}} \neq \varnothing$,then

$$A = \bigcap_{x \in A^{\mathrm{u}}} \hat{x} = \inf_{(\hat{X}, \subseteq)} \{\hat{x} | x \in A^{\mathrm{u}}\}$$

$$A = \bigcup_{x \in A} \hat{x} = \sup_{(\wp(X), \subseteq)} \{\hat{x} | x \in A\} = \sup_{(\hat{X}, \subseteq)} \{\hat{x} | x \in A\}$$

Proof
(1) Consider $\Phi : \wp(X) \to \wp(X), A \mapsto (A^{\mathrm{u}})^{\mathrm{l}}$.By the lemma, Φ is increasing.Since $\wp(X)$ is complete,and $\hat{X}$ is the set of fixed point of Φ. By Knaster-Tarski fixed point theorem,$(\hat{X}, \subseteq)$ is order complete.
(2) Let $A \in \wp(X)$, we prove that $A^{\mathrm{l}} = ((A^{\mathrm{l}})^{\mathrm{u}})^{\mathrm{l}}$.Since $A \subseteq (A^{\mathrm{l}})^{\mathrm{u}}$(by the lemma),$((A^{\mathrm{l}})^{\mathrm{u}})^{\mathrm{l}} \subseteq A^{\mathrm{l}}$,by (2) of the lemma applied to A^{l}.Hence $A^{\mathrm{l}} = ((A^{\mathrm{l}})^{\mathrm{u}})^{\mathrm{l}}$
(3) Let x and y be element of X such that $x < y$ then $\{x\}^{\mathrm{l}} \subseteq \{y\}^{\mathrm{l}}$.In fact , if $z \in \{x\}^{\mathrm{l}}, z \leq x$ .Since $x < y, z < y$.Moreover,$y \in \{y\}^{\mathrm{l}}$,but $y \notin \{x\}^{\mathrm{l}}$
(4) $\forall x \in A, x \in \{x\}^{\mathrm{l}} = \hat{x}$. So $A \subseteq \cup_{x \in A} \hat{x}$. Conversely,$\forall x \in A, x = \min(\{x\}^{\mathrm{u}})$.Hence $\{x\}^{\mathrm{l}} = (\{x\}^{\mathrm{u}})^{\mathrm{l}} \subseteq (A^{\mathrm{u}})^{\mathrm{l}} = A$.Therefore $\cup_{x \in A} \{x\}^{\mathrm{l}} \subseteq$

A.Finally we get $\bigcup_{x\in A}\hat{x}=A\in\hat{X}$
(5) If $A^{\mathrm{u}}=\varnothing$ then $A=(A^{\mathrm{u}})^{\mathrm{l}}=\varnothing^{\mathrm{l}}=X$.We assume that $A^{\mathrm{u}}\neq\varnothing$.

$$\inf_{(\wp(X),\subseteq)}\{\hat{x}|x\in A^{\mathrm{u}}\}=\bigcap_{x\in A^{\mathrm{u}}}\hat{x}=\bigcap_{x\in A^{\mathrm{u}}}\{x\}^{\mathrm{l}}=(A^{\mathrm{u}})^{\mathrm{l}}=A$$

So it is equal to $\inf_{(\hat{X},\subseteq)}\{\hat{x}|x\in A^{\mathrm{u}}\}$ □

Remark 4.8.1 $\forall A\in\hat{X},A=\{x\in X|\hat{x}\subseteq A\},A^{\mathrm{u}}=\{x\in X|A\subseteq\hat{x}\}$

Definition 4.8.4 $\hat{X}$ is called the Dedekind-MacNeille order completion of $(X,\leq)$

4.9 Recursive Construction

Definition 4.9.1 Let $(X,\leq)$ be a partially ordered set.Let $I\subseteq X$. If $\forall a\in I,X_{<a}\subseteq I$, we say that I is an initial segment of X.

Proposition 4.9.1 Let $(X,\leq)$ be a totally ordered set, I,J be initial segments of X. Either $I\subseteq J$ or $J\subseteq I$.

Proof Assume that $I\backslash J\neq\varnothing$.take $x\in I\backslash J,\forall y\in J$, if $y\not\leq x$,then $x<y$ and hence $x\in X_{<y}\subseteq J$,contradiction.Therefore $y\leq x$.Then $y=x\in I$ or $y\in X_{<x}\subseteq I$. □

Proposition 4.9.2 Let $(X,\leq)$ be a well-ordered set. I be an initial segment of X, such that $I\neq X$.There is a unique $a\in X$ such that $I=X_{<a}$.

Proof $X\backslash I\neq\varnothing$ Let $a=\min(X\backslash I)$.By definition,$I\subseteq X_{<a}$.In fact ,$\forall y\in I$ if $y\not<a$, then $a\leq y$. Since I is an initial segment $a\in I$,contradiction.
Conversely,if $x\in X_{<a}$, then $x\notin X\backslash I$.Since otherwise $a\leq x$.Therefore $x\in I$ .Uniqueness,$\forall a\in X,a=\min(X\backslash X_{<a})=\min(X_{\leq}a)$.Hence $X_{<a}=X_{<b}\Rightarrow a=b$ □

Chapter 5

Groups

5.1 Composition Law

Definition 5.1.1 Let X be a set.

(i) A **compositon law** on X is a mapping

$$* : X \times X \to X, (x, y) \mapsto x * y$$

(ii) Let $Y \subseteq X$ be a set , Y is **close under** $*$ if $\forall x, y \in Y, x * y \in Y$

(iii) $*$ is **communitative** if $\forall (x, y) \in X^2, x * y = y * x$

(iv) $*$ is **associative** if $\forall (x, y, z) \in X^3, (x*y)*z = x*(y*z)$. If $*$ is associative, then we can define

$$x_1 * x_2 * \cdots * x_n = (x_1 * x_2 * \cdots * x_{n-1}) * x_n$$

(v) Let G be a set , $*$ is a composition law on G. If $*$ is associative,then we say $(G, *)$ is a **semigroup**

Example 5.1.1
(1) Let $(X, *)$ be a composition law .We define $(X, \hat{*})$ satisfies:

$$\hat{*} : X \times X \to X, (x, y) \mapsto y * x$$

By definition,$x = \hat{x} \Leftrightarrow *$ is communitative.If $*$ is associative, then so does $\hat{*}$.
Let $\mathfrak{M}_X$ the set of all mapping from X to X.On $\mathfrak{M}_X$,the composition of mapping

defines a composition law:

$$\begin{aligned}\mathfrak{M}_X \times \mathfrak{M}_X &\to \mathfrak{M}_X \\ (f, g) &\mapsto f \circ g\end{aligned}$$

It is associative but not communitative:
Let $f_a : x \mapsto a, f_b : x \mapsto b, \forall x \in X$ Then,$f_a \circ f_b = f_a, f_b \circ f_a = f_b$

Proposition 5.1.1 Let $(X, *)$ be an associative composition law on a set X.If $n \in \mathbb{N}_{>}0, x_1, \ldots, x_n \in X$, then , $\forall 1 \leq i \leq n-1$, we have

$$x_1 * \cdots * x_n = x_1 * \cdots * (x_i * x_{i+1}) * \cdots * x_n$$

Proof
$i = 1$: By definition,$x_1 * \cdots * x_n = (x_1 * x_2) * \cdots * x_n$.We suppose $i \geq 2$, by the associativity of $*$, we have

$$x_1 * \cdots * x_{i+1} = (x_1 * \cdots * x_{i-1}) * x_i * x_{i+1} = x_1 * \cdots * x_{i-1} * (x_i * x_{i+1})$$

□

Definition 5.1.2 Let $(G, *)$ be a set equipped with a composition law , $g \in G$
If $\forall (x, y) \in G^2, g * x = g * y \Rightarrow x = y$,we say that g is **left cancellative**.
If $\forall (x, y) \in G^2, x * g = y * g \Rightarrow x = y$,we say that g is **right cancellative**.
If $*$ is communitative, left cancellative $\Leftrightarrow$ right cancellative.

Example 5.1.2
In $(\mathbb{N}, +)$, any element is cancellative.
In $(\mathbb{N}, *)$, any positive natural number is cancellative.

5.2 Neutral Element & Invertible Element

Definition 5.2.1 $(X, *), e \in X$ is called a **neutral element** if

$$e * x = x = x * e$$

Proposition 5.2.1 Assume $(X, *)$ admits a neutral element, then its neutral element is unique.

Proof Let $e, e' \in X$ be neutral elements.Then

$$e = e * e' = e'$$

□

Definition 5.2.2 Let $(G, *)$ be a semigroup. If $(G, *)$ has a neutral element , then we say $(G, *)$ is **monoid**.

Example 5.2.1
(1) X is a set, $(\mathfrak{M}_x, \circ)$ is a monoid with hte neutral element Id_X
(2) $d \in \mathbb{N}_{>}0$,$(d\mathbb{N}, +)$ with neutral 0,$(\mathbb{N}, \times)$ with neutral 1

Definition 5.2.3 Let $(G, *)$ be a monoid with the neutral element e. $\forall (x, y) \in G^2$, if $x * y = e$ then we say x is a **left inverse** of y,and y is the **right inverse** of x.

Remark 5.2.1 We say x is **left invertible** if x has a left inverse.(resp. right invertible)

Remark 5.2.2 x is left invertible in $(G, *) \Leftrightarrow x$ is right invertible in $(G, \hat{*})$

Proposition 5.2.2 Let $(G, *)$ be a monoid, $g \in G$ .If g is both left invertible and right invertible, then g has a unique left inverse and a unique right inverse,which actually coincide.

Proof Let x (resp. y) be a left (resp. right) inverse of g.Then , by the associativity law , we have

$$x = x * e = x * (g * y) = (x * g) * y = y$$

Hence any left inverse is equal to y, hence it is unique.Similarly for the right. □

Definition 5.2.4 Let $(G, *)$ be a monoid. If $g \in G$ is both left invertible and right invertible, then we say g is **invertible**. If g is invertible, the left inverse is equal to right inverse, hence we called it the inverse of g, denote by $\iota(g)$

Proposition 5.2.3 Let $(G, *)$ be a monoid, $g \in G$.If g is right (resp. left) invertible, then it is right (resp. left) cancellative.

Proof Let h be the right inverse of g.If $x * g = y * g$, then

$$x = x * e = x * (g * h) = (x * g) * h = (y * g) * h = y * (g * h) = y * e = y$$

□

Notation 5.2.1 For a monoid $(G, *)$.
If $*$ is written multiplicatively,we usually denote $x * y$ as $x \cdot y$ or xy.If no ambiguity,neutral element as 1,inverse of x as x^{-1}.
If $*$ is written additively, $x * y$ as $x + y$,neutral element as 0, inverse of x as $-x$

Proposition 5.2.4 Let $(G, *)$ be a monoid.
(1) If $x \in G$ is an invertible element , then $\iota(x)$ is also invertible, and $\iota(\iota(x)) = x$.
(2) If $x, y \in G$ are invertible, so does $x * y$ and $\iota(x * y) = \iota(y) * \iota(x)$

Proof
(1)

$$x * \iota(x) = \iota(x) * x = e$$

(2)

$$(xy)(\iota(y)\iota(x)) = xy\iota(y)\iota(x) = xe\iota(x) = x = \iota(x) = e$$

$$(\iota(y)\iota(x))(xy) = \iota(y)\iota(x)xy = \iota(y)ey = \iota(y)y = e$$

□

Definition 5.2.5 Let $(G, *)$ be a monoid.If any element of G is invertible, then we say G with the composition law is a **group**.A communitative group is also called **abelian group**.

Now we have :
(binary operations on X)$\supseteq$(semigroup)$\supseteq$(monoids)$\supseteq$(group)$\supseteq$(abelian group)

Example 5.2.2
(1) $(\mathbb{Z}, +)$ is an abelian group.
(2) Let X be a set $\mathfrak{S}_X$ the set of bijections from X to X.$(\mathfrak{S}_X, \circ)$ is a monoid with the neutral element Id_X.Since $f \in \mathfrak{S}_X$ is bijective, hence there exists a unique inverse $f^{-1} \in \mathfrak{S}_X$.So $(\mathfrak{S}_x, \circ)$ is a group (but not abelian in general),called the symmetric group of X.

Let $\mathfrak{S}_n$ be the symmetric group of the set $\mathbb{N}_{\leq n}$, its element f can be denoted as a table:

$$\begin{pmatrix} 1 & 2 & \dots & n \\ f(1) & f(2) & \dots & f(n) \end{pmatrix}$$

5.3 Substructure

Definition 5.3.1 Let $(G, *)$ be a semigroup, H be a subset of G.If H is close under $*$,then we say H is a **subsemigroup** of $(G, *)$.Note that H equipped with the restriction of $*$ forms a semigroup. Let $(G, *)$ be a monoid.If a sub-semigroup H of $(G, *)$ contains the neutral element of $(G, *)$, then we say H is a submonoid of $(G, *)$.

Example 5.3.1
(1) Let $d \in \mathbb{N}^*$, then $d\mathbb{N}$ forms a submonoid of $(\mathbb{N}, +)$.
$d\mathbb{N}$ is a subsemigroup of $(\mathbb{N}, \cdot)$
(2) $\mathfrak{S}_X$ is submonoid of $(\mathfrak{M}_X, \circ)$

Proposition 5.3.1 Let $(M, *)$ be a monoid, $H \subseteq M$ be a non-empty subset. Suppose that any element of H is invertible in M , and $(\forall x, y \in H, (x, y) \mapsto x * \iota(y))$,if $\forall x, y \in H, x * \iota(y) \in H$, then H is a submonoid of M,Moreover, H equipped with the restriction of $*$ forms a group.

Proof Let e be the neutral element of $(M, *)$.Let $a \in H$, then $e = a \circ \iota(a) \in H$.For any $y \in H$, one has $\iota(y) = e * \iota(y) \in H$.For any $(x, y) \in H^2$,$x * y = x * \iota(\iota(y)) \in H$ Hence H is closed under $*$ and it contains the neutral element .Also, $\forall y \in H, \iota(y) \in H$, hence H is group. □