FUNDAMENTAL ALGEBRA & ANALYSIS

Compiled by **Huayi Chen**[I],

&

Edited by **Jiete Xue**[II],

TAs:Postdoc **Jiedong Jiang, Yijun Yuan, Chunhui Liu**[III, IV, V], and

Substitute Professor[1]: **Yigeng Zhao**[VI]

[I]*Department of Mathematics (ITS), School of Science, Westlake University*
[II]*Undegraduate β Collage, Westlake University*
[I]chenhuayi@westlake.edu.cn
[II]xuejiete@westlake.edu.cn

[1] Chapter 5: Group, Section1-4

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 1.1.2 “$2 > 1$”(True) “$1 < 0$”(False)
If we specify the value of x , then “$x > 2$”becomes a statement, otherwise it is not a statement.

Definition 1.1.3 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 1.2.2 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 1.3.2 Let $P$and Q be 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 1.4.2 It has the same truth value as that of $(\neg P \vee Q)$, only when P is 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 1.4.3 Let P and Q be statements. If P and $P \Rightarrow Q$ are true, then Q is also true.

Proposition 1.4.4 Let P, Q, R be statements. If $P \Rightarrow Q$ and $Q \Rightarrow R$ are true, then $P \Rightarrow R$ is also true.

Theorem 1.4.5 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 1.4.6 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 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 1.5.2 Let P and Q be statements.$P \Leftrightarrow Q$ has the same truth value as

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

Example 1.5.3 Let n be an integer.n is even if and only if n^2 is even.

Definition 1.5.4 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 1.5.5 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 1.6.2 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
(1) We call a **set** a certain collection of distinct objects.
(2) An object in a collection considered as a set is called **element** of it .
(3) 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”.
(4) 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 2.1.2 {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 2.1.3

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

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 2.2.2 “n is even” is a condition on $\mathbb{N}$, “$x > 2$” is a condition on $\mathbb{R}$.

Definition 2.2.3 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 2.2.4 $\{x \in \mathbb{R}|x > 2\}$ 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 2.3.2

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

Example 2.3.4 $\wp(\varnothing) = \{\varnothing\}$, $\wp(\wp(\varnothing)) = \{\varnothing, \{\varnothing\}\}$.

Definition 2.3.5 Let A and B be sets. We denote by $B\backslash A$ the set

$$\{x \in B \mid x \notin A\}.$$

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

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

Proposition 2.3.7 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 $\{x \in A \mid P(x)\} = A$
"$\exists x \in A, P(x)$"denotes$\{x \in A \mid P(x)\} \neq \varnothing$.

Example 2.4.2 $\forall x \in \varnothing, P(x)$ is true ; $\exists x \in \varnothing, P(x)$ is false.

Theorem 2.4.3 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

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

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

Proposition 2.5.2 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

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

□

Russell's paradox leads to: $P(A) := A \notin A$. 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 2.6.2 $\bigcup\limits_{i \in I} A_i \subseteq B$ if and only if

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

Corollary 2.6.3 Let $P_i(\cdot)$ be a condition on B, then

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

Proposition 2.6.4

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

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

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

is a set. This set is 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 2.7.2 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 2.7.3 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 $B \subseteq \bigcap_{i\in I} A_i$ if and only if

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

Proof Let $A = \bigcap_{i\in I} A_i$.
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 2.7.4 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 2.7.3 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 2.7.5 Let B be a set, $(A_i)_{i\in I}$ be a family of sets. The following equality holds

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

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 2.7.3 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 2.7.6 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 $I \neq \varnothing$, $B \cup (\bigcap_{i\in I} A_i) \subseteq \bigcap_{i\in I}(B \cup A_i)$,

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 2.7.4 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 2.7.3 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 Theorem2.4.3

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

By Corollary 2.7.4 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 Theorem2.4.3

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

By Corollary 2.6.3 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 ordered pairs can be realized through set-theoretic constructions.

Proposition 2.8.2 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 3.3.3 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 3.3.4 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 3.3.3, 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 3.3.5 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 3.3.6 Let f be a correspondence, I be a set and $(A_i)_{i\in I}$ be a family of sets parametrised by I. Then

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

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

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

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

□

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

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

Proposition 3.4.3 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 3.4.4 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 3.4.5 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 3.3.3 and 3.3.4 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 3.5.2 multivalued mapping is not always a mapping

Proposition 3.5.3 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 3.5.4 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

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

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

Proposition 3.5.5 Let f and g be correspondences.
(1) If g is surjective and $\operatorname{Dom}(g) \subseteq \operatorname{Im}(f)$, then $g \circ f$ is also surjective.
(2) If f is a multivalued mapping and $\operatorname{Im}(f) \subseteq \operatorname{Dom}(g)$, then $g \circ f$ is a multivalued mapping.

Proof (1) Since $\operatorname{Dom}(g) \subseteq \operatorname{Im}(f)$, by proposition3.4.5, we obtain

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

Since g is surjective,

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

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 3.6.2 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 $x \in \operatorname{Dom}(f)$. We denote the unique image of x under f as $f(x)$, and we say that f sends $x \in \operatorname{Dom}(f)$ 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 3.6.3 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 3.6.4 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 3.6.5 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 3.6.6 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 $\bigcap_{i\in I} f^{-1}(B_i)$. For any $i \in I$, one has $f(x) \in B_i$. Hence $x \in f^{-1}(\bigcap_{i\in I} B_i)$. 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 proposition3.3.6 , 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 3.7.2 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 3.7.3

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

1. By (1) of Proposition3.3.6, 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 3.3.6, 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 3.3.6, 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 3.6.6, 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 3.6.3, 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 3.6.3 and (2) of Proposition 3.5.3, for any subset A of X one has $f^{-1}(f(A)) = A$.

Proposition 3.7.5 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 3.6.4 and 3.5.5

□

Remark 3.7.6 Let $f : X \to Y$ and $g : Y \to Z$ be mappings.

1. By Proposition 3.5.5, if f and g are both surjective, so is $g \circ f$. By Proposition 3.5.4, if $g \circ f$ is surjective, so is g.

2. By Proposition 3.6.4, if f and g are both injective, so is $g \circ f$. By Proposition 3.6.5, 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 3.8.2 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 3.7.5, 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 3.5.4, 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 3.4.4 and 3.4.3, 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 3.8.3 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 3.7.5, 3.6.4 and 3.5.5

□

Proposition 3.8.4 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 3.5.4, 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 3.6.5, 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 3.7.2 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 3.9.2 Let n be a non-zero natural number. If $(A_i)_{i\in\{1,\ldots,n\}}$ is a family of sets parametrised by $\{1,\ldots,n\}$, then the set

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

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 3.9.3 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

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

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

$$\begin{tikzcd}
X \arrow[r, "f"] \arrow[dr, "f_j"'] & \prod_{i\in I} A_i \arrow[d, "\mathrm{pr}_j"] \\
 & A_j
\end{tikzcd}$$

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 3.9.4 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 3.9.3 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 3.9.5 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 3.7.6 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 3.7.6 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 first written in pre-course, then added some sections in make-up session, which titled “Ordering”.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 4.1.2 We denote by“ $=$” the correspondence Id_X.

Definition 4.1.3 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

Section 5.5:Quotient, will use this concept.

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 $x \in X$, we call the set

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

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 4.2.3 $\forall (x, y) \in X \times X$, either $[x] = [y]$ or $[x] \cap [y] = \varnothing$.

Definition 4.2.4 The mapping $\pi : X \to X/\sim$ is called the **projection mapping** of $\sim$.

Proposition 4.2.5 (Theorem 5.5.5) $f : X \to Y$ 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

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

$$\begin{tikzcd}
X \arrow[r, "f"] \arrow[d, "\pi"'] & Y \\
X/\sim \arrow[ru, "\tilde{f}"'] &
\end{tikzcd}$$

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 4.3.2 $(\mathbb{R}, \leq)$ is a totally ordered set.$(\mathbb{N}, |)$ is a partially ordered set.

Definition 4.3.3 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 4.3.4
(1) $<$ on $\mathbb{R}$.
(2) $\subset$on$\wp(X)$.

Proposition 4.3.5 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 4.4.2 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 4.4.3 Let f be a function between partially ordered set. If f is monotonic and injective, then f is strictly monotonic.

Proposition 4.4.4 Let I be a totally ordered set, X be a partially ordered set , and f be a function from I to X. If 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 4.4.5 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 4.5.2 $\Omega = \{1,2,3\}, X = \wp(\Omega).(X, \subseteq)$ forms a partially ordered set.Let $A = \{\{1\},\{2\},\{1,2\}\}, A^{\mathrm{u}} = \{\{1,2\},\{1,2,3\}\}, A^{\mathrm{l}} = \{\varnothing\}$.

Definition 4.5.3 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 4.5.4 $A \subseteq Y \subseteq X$, let $A^{\mathrm{u}}_Y := \{y \in Y | \forall a \in A, a \leq y\}$ be the set of upper bounds of A in Y.If A^{u}_Y 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 $\sup_Y A$. Resp. **infimum**.

Notation 4.5.5 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 4.5.6
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 $(Z, \leq)$. Resp. 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 4.5.7
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 4.5.8 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) Resp. 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 4.5.9 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 4.5.10 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) Resp. 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 $M \in A^{\mathrm{u}}_Y, \forall i \in I, M \in (A_i)^{\mathrm{u}}_Y$, So $y_i \leq M$ We then deduce that $y \leq M$. □

Proposition 4.5.11 Let $(X, \leq)$ be a partially ordered set , $Y \subseteq X$.

$$\varnothing^{\mathrm{u}}_Y = \varnothing^{\mathrm{l}}_Y = Y.$$

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 4.6.2 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 $a \nleq b$, 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 4.6.3 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 4.6.4 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 4.6.5 totally ordered set condition is used to prove (2)

Proposition 4.6.6 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 4.6.7 (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 4.6.8 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 4.7.2 If $(X,\leq)$ is a well-ordered set, then it is a totally ordered set.

Proposition 4.7.3 $(X,\leq)$ is a well-ordered set, $Y\subseteq X$, then $(Y,\leq)$ is a well-ordered set.

Theorem 4.7.4 Let $(X,\leq)$ be a well-ordered set .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 4.7.5 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 4.7.6 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 4.8.2 Let Ω be a set, $X = \wp(\Omega)$. Then $(X, \subseteq)$ is order complete.

Proof Let $Y \subseteq X$.Then

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

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

Proposition 4.8.3 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 Notation4.5.5, then came to Proposition4.5.6 and the following.

Definition 4.8.4 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 4.8.5 (Knaster-Tarski fixed point)
Let $(X, \leq)$ be an order complete partially ordered set , $f : X \to X$ be an increasing mapping. Let

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

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

Proof Let A be a subset of F. We consider

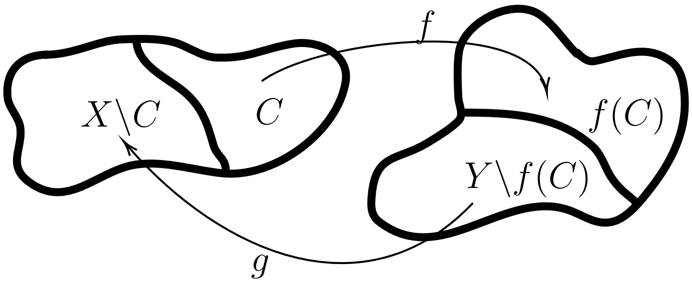
$$S_A := \{y \in A^{\mathrm{u}} \mid f(y) \leq y\}.$$

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

Theorem 4.8.7 (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 4.8.8 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 4.8.9 (Dedekind-MacNeille)
Let $(X, \leq)$ be a partially ordered set. Let $\hat{X} := \{A \in \wp(X) \mid (A^{\mathrm{u}})^{\mathrm{l}} = A\}$
(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,

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

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

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

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

Remark 4.8.10 We've know that $(\wp(X), \subseteq)$ is order complete. So for the sets not order complete, we can build a relation between them to make it become order complete. And this theorem tell us how to do.

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 $A \subseteq \bigcup_{x \in A} \hat{x}$. 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 $\bigcup_{x \in A} \{x\}^{\mathrm{l}} \subseteq A$. 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 4.8.11 $\forall A \in \hat{X}, A = \{x \in X | \hat{x} \subseteq A\}, A^{\mathrm{u}} = \{x \in X | A \subseteq \hat{x}\}$.

Definition 4.8.12 $\hat{X}$ 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 4.9.2 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 4.9.3 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 $X_{<a} = X_{<b} \Rightarrow a = b$. □

Proposition 4.9.4 Let $(X, \leq)$ be a partially ordered set, Λ be a non-empty set, and $(I_\lambda)_{\lambda \in \Lambda}$ be a family of initial segments of X. Then

$$I := \bigcap_{\lambda \in \Lambda} I_\lambda, J := \bigcup_{\lambda \in \Lambda} I_\lambda$$

are initial segments of X.

Proof
Let $a \in I . \forall \lambda \in \Lambda, a \in I_\lambda$ and hence $X_{<a} \subseteq I_\lambda$. Therefore, $X_{<a} \subseteq \bigcap_{\lambda \in \Lambda} I_\lambda = I$.
Let $b \in J$.Then $\exists \lambda_0 \in \Lambda$ such that $b \in I_{\lambda_0}$. So $X_{<b} \subseteq I_{\lambda_0} \subseteq \bigcup_{\lambda \in \Lambda} I_\lambda = J$. □

Theorem 4.9.5 (Recursive construction) Let $(X, \leq)$ be a well ordered set, and Y be a set. For any $x \in X$ and any mapping $h : X_{<x} \to Y$, we fix an element $\Phi(h) \in Y$. Then, there exists a unique mapping $f : X \to Y$ such that

$$\forall x \in X, f(x) = \Phi(f\mid_{X_{<x}}).$$

Example 4.9.6 For any $(a_0, \ldots, a_{n-1}) \in \mathbb{R}^n$, we fix an element $a_{n-1} + \varepsilon \in \mathbb{R}$, where ε is a real number. There exists a unique mapping $(n \in \mathbb{N}) \mapsto f(n)$ such that $f(n) = f(n-1) + \varepsilon .(f(n) := n\varepsilon)$.

Proof
"Uniqueness":
Let f, g be mappings from X to Y such that

$$\forall x \in X, f(x) = \Phi(f\mid_{X_{<x}}), g(x) = \Phi(g\mid_{X_{<x}}).$$

Then: $\forall x \in X$, we have

$$(\forall y \in X_{<x}, f(y) = g(y)) \Rightarrow f(x) = g(x).$$

So by inclusion $\forall x \in X, f(x) = g(x)$, namely, $f = g$.
"Existence":
Let $\mathscr{S}$ be the set of initial segments S of X such that $\exists f_S : S \to Y$ satisfying

$$\forall x \in S, f_S(x) = \Phi(f_S |_{X_{<x}}). \tag{$*$}$$

Let $X_0 = \bigcup_{S \in \mathscr{S}} S$. It is also an initial segment of X. For any $x \in X_0$ there exists S such that $x \in S$. If S_1 and S_2 are two elements of $\mathscr{S}$, then $S_1 \cap S_2$ is also an initial segment. Moreover $f_{S_1} |_{S_1 \cap S_2}$ and $f_{S_2} |_{S_1 \cap S_2}$ satisfy $(*)$ So $f_{S_1} |_{S_1 \cap S_2} = f_{S_2} |_{S_1 \cap S_2}$. Thus $f_S(x)$ does not depend on the choice of $S \in \mathscr{S}$ containing x. We denote it as $f(x)$. $f : X_0 \to Y$ satisfying $(*)$. So $X_0 \in \mathscr{S}$. If $X_0 \neq X . \exists a \in X$ such that $X_0 = X_{<a}$. We extend f to $X_0 \cup \{a\}$ by letting $f(a) = \Phi(f)$. Then we get $X_0 \cup \{a\} \in \mathscr{S}$.Contradiction.Therefore $X_0 = X$ and we get the existence of f. □

Definition 4.9.7 Let A be a set. If there exists an injective mapping $A \to \mathbb{N}$, then we say that A is **countable**. If there exists an injective mapping $f : A \to \mathbb{N}$ such that $f(A)$ is bounded from above (having an upper bound in $\mathbb{N}$), then we say that A is **finite**.

Lemma 4.9.8
(1) Let $n \in \mathbb{N}$ and $x_0, \ldots, x_n$ be elements of $\mathbb{N}$ such that $x_0 < \cdots < x_n$, then $\forall i \in \mathbb{N}_{\leq n}, i \leq x_i$.
(2) Let $(x_n)_{n \in \mathbb{N}}$ be a family of elements in $\mathbb{N}$ such that $\forall n \in \mathbb{N}, x_n < x_{n+1}$, then $\forall i \in \mathbb{N}, i \leq x_i$.

Proof If $j \leq x_j$ for $j \in \{0, \ldots, i-1\}$. Then, in the case where $i = 0, 0 \leq x_0$ holds since $0 = \min_{\leq} \mathbb{N}$. In the case where $i > 0$, one has $i - 1 \leq x_{i-1} < x_i$. So $x_i \geq x_{i-1} + 1 \geq i - 1 + 1 = i$. □

Proposition 4.9.9 Let $f : A \to B$ be a mapping.
(1) If f is injective and if B is finite, then A is finite.(resp. countable)
(2) If f is surjective and A is finite, then B is finite.(resp countable)

Proof
(1) Let $g : B \to \mathbb{N}$ injective and bounded from above. Then $g \circ f$ is injective and $\operatorname{Im}(g \circ f) \subseteq \operatorname{Im}(g)$.
(2) $\exists$ injective mapping $B \to A$ by the axiom of choice. $f : A \to B$ For any

$b \in B$, pick $h(b) \in f^{-1}(\{b\}) \subseteq A$, $h : B \to A$. If $h(b) = h(b')$, then $f(h(b)) = f(h(b')) = b'$. □

Proposition 4.9.10 Let X, Y be sets.
(1) If X and Y are finite, then $X \cup Y$ is finite.(resp. countable)
(2) If X is infinite and Y is finite, then $X \backslash Y$ is infinite.(resp. uncountable)

Proof
(1) Let $f : X \to \mathbb{N}$ and $g : Y \to \mathbb{N}$ be injective mappings. We construct $h : X \cup Y \to \mathbb{N}$ such that

$$h(x) = \begin{cases} 2f(x) & x \in X \\ 2g(x) + 1 & x \in Y \backslash X \end{cases}$$

h is then injective, and h is bounded if f and g are bounded.
In fact, if $(x, y) \in (X \cup Y)^2$,
either $(x, y) \in X^2$ and $h(x) = 2f(x) = h(y) = 2f(y)$ if and only if $x = y$.
or $(x, y) \in (Y \backslash X)^2$ and $h(x) = h(y) \Rightarrow x = y$.
or $x \in X, y \in Y \backslash X. h(x) \neq h(y)$ (So $h(x) = h(y) \Rightarrow x = y$).
or $y \in X, x \in Y \backslash X, h(x) \neq h(y)$.
(2) Assume that $X \backslash Y$ is finite, then $X = (X \backslash Y) \cup Y$ is also finite. □

Notation 4.9.11 If $f : X \to X$ is a mapping. Then f^0 denotes Id_X. For $n \in \mathbb{N}_{\geq 1}$, f^n denotes $\underbrace{f \circ f \circ \cdots \circ f}_{n}$.

Theorem 4.9.12 $\mathbb{N} \times \mathbb{N}$ and $\mathbb{N}$ are equipotent.

Proof Let $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}, (a, b) \mapsto 2^a(2b+1)$. It is an injective mapping since $2^a(2b+1) = 2^{a'}(2b'+1)$.So $a = a', b = b'$.Moreover $x \mapsto (0, x)$ is injective. □

Corollary 4.9.13 $\forall n \in \mathbb{N}, n \geq 1, \mathbb{N}^n$ and $\mathbb{N}$ are equipotent.

Proof Induction on n.
For $n = 1$, easy. We assume that $\mathbb{N}^n$ is equipotent to $\mathbb{N}$ and $f : \mathbb{N}^n \to \mathbb{N}$ be a bijection. Then the mapping

$$f' : \mathbb{N}^n \times \mathbb{N} \to \mathbb{N} \times \mathbb{N},\ (x_1, \ldots, x_n; x_{n+1}) \mapsto (f(x_1, \ldots, x_n), x_{n+1})$$

is a bijection. By Theorem 4.9.12, there exists a bijection $g : \mathbb{N}^2 \to \mathbb{N}$.Therefore,

$$g \circ f' : \mathbb{N}^{n+1} \to \mathbb{N}$$

is a bijection, which leads to $\mathbb{N}^{n+1}$ and $\mathbb{N}$ are equipotent. □

Motivation: Let X be a set. A sequence in X is by definition a family $(x_i)_{i\in I}$, where I is an infinite subset of $\mathbb{N}$, and each x_i is an element of X.

Example 4.9.14 $(a + bn)_{n\in\mathbb{N}}$; $\left(\frac{1}{n}\right)_{n\in\mathbb{N}_{\geq 1}}$.

Proposition 4.9.15 Let $I \subseteq \mathbb{N}$.
(1) $\mathrm{Id}_I : I \to I$ is the only increasing mapping bijection from I to I.
(2) If I is bounded from above, then Id_I is the only strictly increasing mapping from I to I.

Proof
(1) Let $f : I \to I$ be an increasing bijection. We want to prove:

$$A := \{x \in I \mid f(x) \neq x\} = \varnothing.$$

If this set is non-empty, it has a least element n_0. By definition, $f(n_0) \neq n_0$. So either $n_0 < f(n_0)$ or $n_0 > f(n_0)$.
If $f(n_0) < n_0$, then $f(n_0) \notin A$, and hence $f(n_0) = f(f(n_0)) < f(n_0)$, contradiction. So $n_0 < f(n_0)$. For any $n \in I$, if $n_0 \leq n$ then $f(n_0) \leq f(n)$. If $n_0 > n$, then $n \notin A$ and $f(n) = n < n_0$.$(*)$Hence $f(n) \neq n_0$ for any $n \in I$. This contradicts the assumption that f is bijective.
(2) Suppose that I is bounded from above, and $f : I \to I$ is strictly increasing. We follow the same reasoning until $(*)$. $n_0 < f(n_0)$ implies that $\forall k \in \mathbb{N}$, $f^k(n_0) < f^{k+1}(n_0)$, that means

$$n_0 < f(n_0) < \cdots < f^{k+1}(n_0).$$

So by the lemma 4.9.8, $k \leq f^k(n_0)$, this contradicts the assumption that I is bounded from above. □

Corollary 4.9.16 Let $I \subseteq \mathbb{N}$ bounded from above, and $J \subseteq I$.If $J \neq I$, there does not exist a strictly increasing mapping from I to J.

Proof Suppose that $f : I \to J$ is a strictly increasing mapping. Let $g : J \to I, x \mapsto x$ be a inclusion mapping. So $g \circ f : I \to I$ is strictly increasing and hence $g \circ f = \mathrm{Id}_I$. However $\mathrm{Im}(g \circ f) \subseteq \mathrm{Im}(g) = J \neq I$. Contradiction. □

Proposition 4.9.17 Let $I \subseteq \mathbb{N}$ non-empty.
(1) If I is bounded from above, then there exists a unique pair (N, f), where $N \in \mathbb{N}$ and $f : \{0, 1, \ldots, N\} \to I$ is an increasing bijection. (We say that the cardinality of I is $N + 1$.)
(2) If I is NOT bounded from above, there exists an increasing bijection from $\mathbb{N}$ to I. (We say that the cardinality of I is $\aleph_0$)

Proof
We construct in a recursive way a family of elements in I. Let $x_0 = \min(I)$. If $x_0, \ldots, x_n$ are chosen (with $x_0 < \cdots < x_n$) we pick $x_{n+1} = \min(I \backslash \{x_0, \ldots, x_n\})$. We slop at N if $\{x_0, \ldots, x_N\} = I$. Thus we obtain the increasing bijection needed by the proposition.
"Uniqueness" for (2): If $f : \mathbb{N} \to I, g : \mathbb{N} \to I$ are increasing bijections, then $f^{-1} \circ g : \mathbb{N} \to \mathbb{N}$ and $g^{-1} \circ f : \mathbb{N} \to \mathbb{N}$ are increasing bijections. So $f^{-1} \circ g = \mathrm{Id}_{\mathbb{N}}$. Hence $f = g$.
"Uniqueness" for (1): Let $f : \{0, 1, \ldots, N\} \to I$ and $g : \{0, 1, \ldots, M\} \to I$ be increasing bijections. $g^{-1} \circ f : \{0, 1, \ldots, N\} \to \{0, 1, \ldots, M\}$ and $g : \{0, 1, \ldots, M\} \to I$ be increasing bijections. $f^{-1} \circ g : \{0, 1, \ldots, M\} \to \{0, 1, \ldots, N\}$ are increasing bijection. So $N \leq M$ and $M \leq N$, which leads to $N = M, g = f$. □

Corollary 4.9.18 A non-empty set X is finite if and only if it can be written as $\{x_0, \ldots, x_N\}$ where $N \in \mathbb{N}$, and $x_0, \ldots, x_N$ are distinct elements of X.

Proof Let $f : X \to \mathbb{N}$ be an injective mapping with $f(x)$ bounded from above. Then there exists (N, g) where $N \in \mathbb{N}$ and $g : \{0, \ldots, N\} \to f(x)$ is an increasing bijection. Then $f^{-1} \circ g : \{0, \ldots, N\} \to X$ is a bijection. We take x_i to be $(f^{-1} \circ g)(i)$ (Note that N is unique $N + 1$ is called the cardinality of X). □

Proposition 4.9.19 Let X be a set. The following condition are equipotent:
(1) X is infinite.
(2) $\exists \mathbb{N} \to X$ injective.
(3) $\exists$ injective mapping $f : X \to X$ such that $f(X) \neq X$.

Proof

(1)⇒(2) We construct a sequence $(x_n)_{n\in\mathbb{N}}$ in X as follows. $X \neq \varnothing$. We pick arbitrary $x_0 \in X$. Suppose that distinct elements $x_0, \dots, x_n$ of X are chosen. The set $X \backslash \{x_0, \dots, x_n\} \neq \varnothing$ since otherwise $X = \{x_0, \dots, x_n\}$ is finite. We pick $x_{n+1} \in X \backslash \{x_0, \dots, x_n\}$, $x_0, \dots, x_{n+1}$ are distinct. The mapping $\mathbb{N} \to X, n \mapsto x_n$ is injective.

(2)⇒(3) Let $f : \mathbb{N} \to X$ be injective. We define $g : X \to X$.

$$g(x) := \begin{cases} f(n+1) & , \quad x = f(n) \\ \quad x & , \quad x \notin f(\mathbb{N}). \end{cases}$$

$g(X) \neq X$ since $f(0) \notin g(X)$ If $x \notin f(\mathbb{N}), g(x) = x \notin f(\mathbb{N})$, so $g(x) \neq f(0)$. If $x = f(n), g(x) = f(n+1) \neq f(0)$ since f is injective.

(3)⇒(2) Let $g : X \to X$ be injective with $g(X) \neq X$. We pick $x_0 \in X \backslash g(X)$. We define a sequence $(x_n)_{n\in\mathbb{N}}$ by letting $x_{n+1} := g(x_n)$. Since g is injective, $x_n \in g^n(X) \backslash g^{n+1}(X)$. otherwise $\exists y \in X$, such that $x_n = g^n(x_0) = g^{n+1}(y)$. Hence $x_0 = g(y) \in g(x)$ contradiction. Then $x_0, x_1, \dots,$ are distinct, which defines an injective mapping $\mathbb{N} \to X, n \mapsto x_n$.

(2)⇒(1) If X is finite, $\exists g : X \to \mathbb{N}$ injective with $g(x)$ bounded. Then $\mathbb{N} \to X \xrightarrow{g} \mathbb{N}$ is injective with $h(\mathbb{N})$ bounded from above. □

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 5.1.2
(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 5.1.3 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 5.1.4 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 5.1.5
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

$$\forall x \in X,\ e * x = x = x * e.$$

Proposition 5.2.2 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 5.2.3 Let $(G, *)$ be a semigroup. If $(G, *)$ has a neutral element , then we say $(G, *)$ is **monoid**.

Example 5.2.4
(1) X is a set, $(\mathfrak{M}_x, \circ)$ is a monoid with the neutral element Id_X.
(2) $d \in \mathbb{N}_{>0}$, $(d\mathbb{N}, +)$ with neutral 0, $(\mathbb{N}, \times)$ with neutral 1.

Definition 5.2.5 Let $(G, *)$ be a monoid with the neutral element e. For any $(x, y) \in G^2$, if $x * y = e$ then we say x is a **left inverse** of y, and y is the **right inverse** of x.

Remark 5.2.6 We say x is **left invertible** if x has a left inverse.(resp. right invertible)

Remark 5.2.7 x is left invertible in $(G, *)$ ⇔ x is right invertible in $(G, \hat{*})$.

Proposition 5.2.8 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 5.2.9 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 5.2.10 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 5.2.11 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 5.2.12 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 5.2.13 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 5.2.14
(1) $(\mathbb{Z}, +)$ is an abelian group.
(2) Let X be a set and $\mathfrak{S}_X$ be 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 5.3.2
(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 5.3.3 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 $(H, *|_H)$.

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. □

Corollary 5.3.4 Let $(M, *)$ be a monoid, G be the set of all invertible element in M. Then G is a submonoid. Moreover, G equipped with the restriction of $*$ forms a group.

Proof By definition, any element in G is invertible in M. By Proposition 5.2.12, $\forall x, y \in G, x * \iota(y) \in G$. Therefore, Proposition 5.3.3 implies the claim. □

Notation 5.3.5 Let M be a monoid, we often use $M^\times$ to denote the submonoid of M consisting of all invertible element if the composition law on M is not written additively.

Example 5.3.6 Let X be a set, $\mathfrak{M}_X^\times = \mathfrak{S}_X$.

Definition 5.3.7 Let $(G, *)$ be a group, $H \subseteq G$ be a submonoid. If $\forall x \in H$, one has $\iota(x) \in H$, then we say H is **subgroup** of G.

Proposition 5.3.8 Let $(M, *)$ be a monoid, $\varnothing \neq H \subseteq M^\times$ be a subset such that $\forall x, y \in H$,

$$x * \iota(y) \in H.$$

Then H is a subgroup of $M^\times$.

Proof Let e be the neutral element of $(M, *)$.By Proposition5.3.3, we obtain that H forms a submonoid of $M^\times$.Moreover, $\forall x \in H$, one has $\iota(x) = e*\iota(x) \in H$.So H is a subgroup of $M^\times$. □

Proposition 5.3.9 Let $(G, *)$ be a semigroup (resp. monoid, group), $(H_i)_{i\in I}$ be a family of subsemigroups (resp. submonoids, subgroups), where I is a non-empty set. Then

$$H := \bigcap_{i\in I} H_i$$

is a subsemigroup (resp.submonoid, subgroup) of G.

Proof

For semigroup case, let $x, y \in H$ then $x, y \in H_i, \forall i \in I$.Then $x * y \in H_i, \forall i \in I$, thus

$$x * y \in \cap_{i\in I} H_i = H.$$

For monoid case, the neutral element e of G satisfies

$$e \in H_i, \forall i \in I \Rightarrow e \in \bigcap_{i\in I} H_i = H.$$

For group case, to check $x * \iota(y) \in H$ like above. □

5.4 Homomorphism

Definition 5.4.1 Let $(M, *)$ and $(N, \star)$ be semigroups, $f : M \to N$ be a mapping of sets.
(1) f is called a **semigroup homomorphism** from $(M, *)$ to $(N, \star)$ if

$$f(a * b) = f(a) \star f(b), \forall a, b \in M.$$

(2) If moreover, $(M, *)$ and $(N, \star)$ are both monoids with neutral elements e_M, e_N, f is called a **monoid homomorphism** if

$$f(a * b) = f(a) \star f(b), \forall a, b \in M,$$

$$f(e_M) = e_N.$$

(3) If moreover, $(M, *)$ and $(N, \star)$ are both groups, f is called a **group homomorphism** if

$$f(a * b) = f(a) \star f(b), \forall a, b \in M,$$

$$f(e_M) = e_N,$$

$$f(\iota(a)) = \iota(f(a)), \forall a \in M.$$

(They are not independent.)

Remark 5.4.2 Let $(M, *), (N, \star)$ be groups, we claim that if $\forall a, b \in M, f(a * b) = f(a) \star f(b)$, then $f(e_M) = e_N$ and $f(\iota(a)) = \iota(f(a))$. Let $b = e_M$, then

$$f(e_M) = (\iota(f(a)) \star f(a)) \star f(e_M) = \iota(f(a)) \star (f(a) \star f(e_M)) = \iota(f(a)) \star f(a) = e_N.$$

$$\iota(f(a)) = \iota(f(a)) \star e_N = \iota(f(a)) \star (f(a) \star f(\iota(a))) = \iota(f(a)) \star f(a) \star f(\iota(a)) = f(\iota(a)).$$

But for monoid, we need $f(e_M) = e_N$.

Proposition 5.4.3
Let $f : (M, *) \to (N, \star)$ be a semigroup (resp. monoid, group) homomorphism. If M_1 is a subsemigroup (resp. submonoid, subgroup) of M, then the image $f(M_1)$ is a subsemigroup (resp. submonoid, subgroup).

Proof The semigroup case.Let $x, y \in f(M_1)$, we may write $x = f(a), y =$

$f(b), a, b \in M_1$

$$x \star y = f(a) \star f(b) = f(a * b) \in f(M_1).$$

The monoid case.We denote e_M, e_N be the neutral elements of M, N

$$e_M \in M_1, e_N = f(e_M) \in f(M_1).$$

The group case.We have to check that $x, y \in f(M_1), x \star \iota(y) \in f(M_1)$

$$\forall a \in M, f(a) \star f(\iota(a)) = f(a * \iota(a)) = f(e_M) = e_N.$$

We may write $x = f(a), y = f(b), a, b \in M_1$

$$x \star \iota(y) = f(a) \star \iota(f(b)) = f(a) \star f(\iota(b)) = f(a * \iota(b)) \in f(M_1).$$

□

Remark 5.4.4
(1) The semigroup homomorphism

$$f : (\mathbb{N}, \times) \to (\mathbb{N}, \times), n \mapsto 0$$

of two monoids, but is not a monoid homomorphism, and its image is $\{0\}$, which is not a submonoid of $(\mathbb{N}, \times)$.
(2) Let M be a semigroup (resp. monoid, group) and let N be a subsemigroup (resp. submonoid, subgroup).Then the inclusion mapping $\jmath : N \to M$ is a semigroup (resp. monoid, group) homomorphism.

Proposition 5.4.5 Let $(X, *) \xrightarrow{f} (Y, \star) \xrightarrow{g} (Z, \diamond)$ be semigroup (resp. monoid, group) homomorphisms.Then so does the composite mapping $g \circ f$.

Proof The semigroup case.

$$\begin{aligned}(g \circ f)(x_1 * x_2) &= g(f(x_1 * x_2)) = g(f(x_1) \star f(x_2)) \\ &= g(f(x_1)) \diamond g(f(x_2)), \forall x_1, x_2 \in X.\end{aligned}$$

The monoid case :

$$(g \circ f)(e_X) = g(f(e_X)) = g(e_Y) = e_Z.$$

The group case:

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

□

Proposition 5.4.6 Let $f : (X, *) \to (Y, \star)$ be a semigroup (resp.monoid, group) homomorphism between semigroups (resp.monoids groups).If f is bijective, then its inverse mapping $f^{-1} : Y \to X$ is also a semigroup homomorphism (resp.monoid, group)

Proof The semigroup case: Let $y_1, y_2 \in Y$ and let $x_i = f^{-1}(y_i)$, $i = 1, 2$. Then

$$y_1 \star y_2 = f(x_1) \star f(x_2) = f(x_1 * x_2),$$

$$f^{-1}(y_1 \star y_2) = x_1 * x_2 = f^{-1}(y_1) * f^{-1}(y_2).$$

The monoid case:

$$f(e_X) = e_Y \Rightarrow f^{-1}(e_Y) = e_X.$$

The group case:

$$f^{-1}(\iota(y)) \overset{y=f(x)}{=} f^{-1}(\iota(f(x))) = (f^{-1} \circ f)(\iota(x)) = \iota(f^{-1}(y)).$$

□

Definition 5.4.7 A semigroup (resp. monoid, group) homomorphism $f : X \to Y$ is called a **semigroup (resp.monoid, group) isomorphism** if there exists a semigroup (resp.monoid, group) homomorphism $g : Y \to X$, such that

$$g \circ f = \mathrm{Id}_X, f \circ g = \mathrm{Id}_Y.$$

By Proposition 5.4.5, a semigroup (resp.monoid group) homomorphism is a semigroup (resp.monoid , group) isomorphism if and only if f is a bijection.

Proposition 5.4.8 Let $(G, *)$ be a group.The inversion mapping $\imath : (G, *) \to (G, \hat{*})$ is a group isomorphism.

5.5 Quotient

Definition 5.5.1 Let X be a set and $\sim$ be a binary relation on X. (We write $x \sim y$ the condition $(x, y) \in \Gamma_\sim$)
(1) If $\forall x \in X, x \sim x$.
(2) $\forall (x, y) \in X^2, x \sim y \Rightarrow y \sim x$.
(3) $\forall (x, y, z) \in X^3, (x \sim y$ and $y \sim z) \Rightarrow x \sim z$.
We say that $\sim$ is a **equivalence relation**.

Check Section 4.2:Equivalent Relation, to get more information about it.

Proposition 5.5.2 Let $(X_i)_{i\in i}$ be a family of sets. For any $i \in I$, let $\sim_i$ be an equivalence relation on X_i. Let $X = \prod_{i\in I} X_i$. We define a binary relation $\sim$ on X as follows:

$$(x_i)_{i\in I} \sim (y_i)_{i\in I} \Leftrightarrow \forall i \in I, x_i \sim_i y_i.$$

Then, $\sim$ is an equivalence relation, and the mapping

$$X/\sim \xrightarrow{\Phi} \prod_{i\in I} X_i/\sim_i,$$

$$[(x_i)_{i\in I}] \longmapsto ([x_i])_{i\in I}$$

is a bijection.

Proof
(1) Let $(x_i)_{i\in I} \in X. \forall i \in I, x_i \sim x_i$, so $(x_i)_{i\in I} \sim (x_i)_{i\in I}$.
(2) Let $x = (x_i)_{i\in I}, y = (y_i)_{i\in I}, x_i \sim_i y_i$, so $y_i \sim x_i$. Therefore, $y \sim x$.
(3) Let $x = (x_i)_{i\in I}, y = (y_i)_{i\in I}, z = (z_i)_{i\in I}$ in X. If $x \sim y$ and $y \sim z$, then $\forall i \in I, x_i \sim_i y_i$ and $y_i \sim_i z_i$. Hence $\forall i \in I, x_i \sim_i z_i$. So $x \sim z$.
We check that Φ is well defined. Let $x = (x_i)_{i\in I}$ and $y = (y_i)_{i\in I}$ be elements of X. If $[x] = [y]$, then $x \sim y$ and hence $\forall i \in I, x_i \sim_i y_i$, that means

$$([x_i])_{i\in I} = ([y_i])_{i\in I}.$$

By definition, Φ is surjective. If $\Phi([(x_i)_{i\in I}]) = \Phi([(y_i)_{i\in I}])$, then $\forall i \in I, [x_i] = [y_i]$, namely $x_i \sim_i y_i$. Therefore, $([(x_i)_{i\in I}]) = ([(y_i)_{i\in I}])$. □

Notation 5.5.3 Let X be a set , $\sim$ be an equivalence relation on X. Then $X/\sim$

is called the **quotient** of X by $\sim$. The mapping

$$\pi : X \longrightarrow X/\sim,$$

$$x \longmapsto [x]$$

is called the **quotient mapping**.

Definition 5.5.4 Let X be a set, $f : X \to Y$ be a mapping and $\sim$ an equivalence relation on X. If $\forall (x, y) \in X^2, x \sim y \Rightarrow f(x) = f(y)$ we say that $\sim$ is **compatible** with f.

Theorem 5.5.5 (Proposition4.2.5) Let $f : X \to Y$ be a mapping and $\sim$ be an equivalence relation on X which is compatible with f. Then there exists a unique mapping

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

such that

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

$$\begin{tikzcd}
X \arrow[r, "f"] \arrow[d, "\pi"'] & Y \\
X/\sim \arrow[ur, "\tilde{f}"'] &
\end{tikzcd}$$

Proof If such $\tilde{f}$ exists. For an $x \in X$.

$$\tilde{f}([x]) = \tilde{f}(\pi(x)) = f(x)$$

So $\tilde{f}$ is unique. To prove the existence, it suffices to check that $\tilde{f} : X/\sim \longrightarrow Y$ is well defined. If $[x] = [y]$, then $[x] \mapsto f(x), x \sim y$ and hence $f(x) = f(y)$. So $\tilde{f}$ is well defined. □

Definition 5.5.6 We call $\tilde{f}$ the **mapping induced by f by passing to quotient**.

Example 5.5.7 Let X be a set and $*$ a composition law on X. We say that an equivalence relation $\sim$ on X is compatible to $*$ if $\forall (x_1, y_1), (x_2, y_2) \in X^2$

$$(x_1 \sim x_2 \text{ and } y_1 \sim y_2) \Leftrightarrow x_1 * y_1 \sim x_2 * y_2$$

Or equivalently, the equivalence relation R on $X \times X$ defined by

$$(x_1, y_1)R(x_2, y_2) \Leftrightarrow x_1 \sim x_2 \text{ and } y_1 \sim y_2$$

is compatible with the mapping:

$$X \times X \longrightarrow X/\sim$$

$$(x, y) \longmapsto [x * y]$$

By the theorem, $*$ induces by passing to quotient a mapping

$$(X/\sim) \times (X/\sim) \longrightarrow (X \times X)/R \longrightarrow X/\sim$$

$$([x], [y]) \longmapsto [(x, y)] \longmapsto [x * y]$$

The compatible mapping

$$(X/\sim) \times (X/\sim) \longrightarrow X/\sim$$

$$([x], [y]) \longmapsto [x * y]$$

defines a composition law on $X/\sim$, which is often denoted as $*$ by abuse of notation, called the composition law on $X/\sim$ induced by the composition law $*$ on X by passing to quotient.

Example 5.5.8 N_n on $\mathbb{Z}$.
If $n \mid (x_1 - x_2)$ $n \mid (y_1 - y_2)$, then $n \mid (x_1 + y_1) - (x_2 + y_2)$.
Since $x_1y_1 - x_2y_2 = x_1(y_1 - y_2) + (x_1 - x_2)y_2$, $n \mid x_1y_1 - x_2y_2$.
Hence $+$ and $\cdot$ on $\mathbb{Z}$ induces by passing to equivalent composition law on $\mathbb{Z}/\sim_n$.

Proposition 5.5.9
(1) If $* : X \times X \to X$ is associative (resp.communitative) then so is

$$* : (X/\sim) \times (X/\sim) \to X/\sim$$

(2) If e is a neutral element of $(X, *)$, then $[e]$ is a neutral element of $(X/\sim, *)$.
(3) If $(X, *)$ is a semigroup (resp. monoid), then the projection

$$\pi : X \to X/\sim, x \mapsto [x]$$

is a homomorphism of semigroup (resp.monoid).
(4) If $(X, *)$ is a monoid, $x \in X$ is invertible, then $[x]$ is invertible in $(X/\sim, *)$.

Proof
(1)associative: $[x] * ([y] * [z]) = [x] * [y * z] = [x * (y * z)] = [(x * y) * z] = [x * y] * [z] = ([x] * [y]) * [z]$.
communitative: $[x] * [y] = [x * y] = [y * x] = [y] * [x]$
(2) $[e] * [x] = [e * x] = [x], [x] * [e] = [x * e] = [x]$.
(3)

$$\pi(x * y) = [x * y] = [x] * [y] = \pi(x) * \pi(y)$$

$\pi(e) = [e]$ is the neutral element of $(X/\sim, *)$.
(4) By (3), π is a homomorphism of monoid, $\forall x \in X^\times, \pi(x) = [x] \in (X/\sim)^\times$ and $\iota([x]) = [\iota(x)]$. □

Remark 5.5.10 If $(X, *)$ is a group, so is $(X/\sim, *)$.

Definition 5.5.11
If $(X, *)$ is a semigroup (resp. monoid, group), then $(X/\sim, *)$ is called the **quotient semigroup** (resp. quotient monoid, quotient group) of $(X, *)$ by $\sim$.

Definition 5.5.12 Let $(X, *), (Y, \star)$ be groups and $f : X \to Y$ be a homomorphism of groups. We define the **kernel** of f as

$$\ker(f) := \{x \in X \mid f(x) = e_Y\}$$

where e_Y is the neutral element of Y.

Proposition 5.5.13 Let $(X, *)$ be a monoid, $(Y, \star)$ be a semigroup, $f : X \to Y$ be a homomorphism of semigroups. If f is surjective, then $(Y, \star)$ is a monoid, and f is a homomorphism of monoid.

Proof We check that $f(e_X)$ is the neutral element of Y. $\forall y \in Y, \exists x \in X, f(x) = y$. So $f(e_X) \star y = f(e_X) \star f(x) = f(e_X * x) = f(x) = y$. Also $y \star f(e_X) = f(x) \star f(e_X) = f(x * e_X) = f(x) = y$. □

Proposition 5.5.14 Let $(X, *)$ be a monoid and $(Y, \star)$ be a group. If $f : X \to Y$ is a homomorphism of semigroups, then it is homomorphism of monoids.

Proof Let e_X and e_Y be neutral elements of X and Y. One has $e_X = e_X * e_X$, so $f(e_X) = f(e_X) \star f(e_X)$, so $e_Y = f(e_X)$. □

Proposition 5.5.15
(1) $\ker(f)$ is a subgroup of X.
(2) $\forall(a,x)\in X\times\ker(f)$, there exists $y\in\ker(f)$ such that $a*x=y*a$.

Proof
(1) The neutral element e_x of $(X,*)$ belongs to $\ker(f)$. If x,y are elements of $\ker(f)$, then

$$f(x*\iota(y))=f(x)\star f(\iota(y))=f(x)\star\iota(f(y))=e_Y\star\iota(e_Y)=e_Y,$$

so, $x*\iota(y)\in\ker(f)$.
(2) We should take $y:=(a*x)*\iota(a)$. It remains to check that $y\in\ker(f)$. One has $f(y)=f(a*x*\iota(a))=f(a)\star f(x)\star\iota(f(a))=f(a)\star\iota(f(a))=e_Y$. □

Definition 5.5.16 Let $(G,*)$ be a group and H be a subgroup of G. If $\forall(a,x)\in G\times H$, $a*x*a^{-1}\in H$, we say that H is a **normal subgroup**.

Proposition 5.5.17 Let $(G,*)$ be a group and H be a normal subgroup of G.
(1) The binary relation $\sim_H$ on G defined as

$$x\sim_H y\Leftrightarrow x*\iota(y)\in H$$

is an equivalence relation on G. Moreover,

$$\forall x\in G,[x]=H*x:=\{y*x\mid y\in H\}.$$

(2) If H is normal, then

$$\forall x\in G,x*H=H*x.$$

Moreover, $\sim_H$ is compatible with $*$.
(3) The kernel of $\pi:G\to G/\sim_H$ is equal to H.

Proof
(1) If $x\sim_H y$, then $x*\iota(y)\in H$, so $y*\iota(x)=\iota(x*\iota(y))\in H$, so $y\sim_H x$. If $x\sim_H y$ and $y\sim_H z$, then $x*\iota(y)\in H, y*\iota(z)\in H$, so $x*\iota(z)=x*\iota(y)*y*\iota(z)\in H$. Hence $x\sim_H z$. By definition, $[x]:=\{y\in G\mid x*\iota(y)\in H\}$. If $y\in[x]$, then $y*\iota(x)\in H$. Hence $y=(y*\iota(x))*x\in H*x$. Conversely, if $y=h*x\in H*x\quad(h\in H)$, then $y*\iota(x)=h*x*\iota(x)\in H$. So $y\in[x]$,

$[x] = H * x$.
We denote by G/H the set

$$G/H := \{x * H \mid x \in G\}.$$

We denote by $H\backslash G$ the set

$$H\backslash G := \{H * x \mid x \in G\}.$$

(2) Suppose that H is normal.$\forall (x, y) \in G \times H$, one has $x * y * \iota(x) \in H$. So $\forall y \in H, \exists z (= x * y * \iota(x)) \in H$ such that $x * y = z * x$. So $x * H \subseteq H * x$. Conversely, $H * x \subseteq x * H$. Let x_1, x_2, y_1, y_2 be elements of G, such that $x_1 \sim_H x_2, y_1 \sim_H y_2$.

$$\begin{aligned}
&(x_1 * y_1) * \iota(x_2 * y_2)\\
=&x_1 * y_1 * \iota(y_2) * \iota(x_2)\\
=&x_1 * (y_1 * \iota(y_2)) * \iota(x_1) * x_1 * \iota(x_2) \in H.
\end{aligned}$$

(3)

$$\ker(\pi) = [e_G] = H * e_G = H.$$

□

Notation 5.5.18 If H is a normal subgroup of G, we denote by G/H the quotient group $G/\sim_H$.

Theorem 5.5.19 Let $f : (X, *) \to (Y, \star)$ be a homomorphism of groups, and $K = \ker(f)$. Then $\sim_K$ is compatible with f, and f induces by passing to quotient a mapping

$$\tilde{f} : X/K \longrightarrow Y,$$

which is actually an injective homomorphism of groups, with $\tilde{f}(X/K) = f(X)$. In particular, X/K is isomorphism to $f(X)$.

$$\begin{tikzcd}
X \arrow[r, "f"] \arrow[d, "\pi"'] & f(X) \subseteq Y \\
X/\ker(f) \arrow[ur, "\tilde{f}"'] &
\end{tikzcd}$$

Proof Let x and y be elements of X. $x \sim_K y \Leftrightarrow x * \iota(y) \in K$. Hence $f(x) \star \iota(f(y)) = f(x * \iota(y)) = e_Y$. So $f(x) = f(y)$. $\tilde{f}([x] * [y]) = \tilde{f}([x * y]) = f(x * y) = f(x) \star f(y) = \tilde{f}([x]) \star \tilde{f}([y])$. □

5.6 Universal Homomorphisms

Proposition 5.6.1 Let $(M, *)$ be a monoid, $x \in M$. Then there exists a unique homomorphism of monoid $f : (\mathbb{N}, +) \to (M, *)$ such that $f(1) = x$.

Proof We construct a mapping $f : \mathbb{N} \to M$ in a recursive way as follows: $f(0) = e_M$. For any $n \in \mathbb{N}$, we let $f(n+1) = f(n) * x$. We will prove that f is a homomorphism of monoids, that is

$$\forall (n, m) \in \mathbb{N} \times \mathbb{N}, f(n + m) = f(n) * f(m).$$

We reason by induction on m. If $m = 0$, $f(n) = f(n) * e_M$. Suppose that $f(n + m) = f(n) * f(m)$. One has

$$f(n + m + 1) = f(n + 1) * f(m) = f(n) * f(1) * f(m) = f(n) * f(m + 1).$$

If $g : \mathbb{N} \to M$ is a homomorphism of monoid, such that $g(1) = x$. Since $g(n + 1) = g(n) * g(1) = g(n) * x$, we have $g(n) = f(n)$. By induction, $\forall n \in \mathbb{N}, g(n) = f(n)$. So f is unique. □

Notation 5.6.2 Let $(M, *)$ be a monoid, $x \in M$, $f : (\mathbb{N}, +) \to (M, *)$ be the unique homomorphism of monoid, such that $f(1) = x$. For any $n \in \mathbb{N}$, we denote by x^{*n} the element $f(n) \in M$, $x^{*0} = e_M$, $x^{*(n+m)} = x^{*n} * x^{*m}$.
Two exceptions: If $* = \cdot$ is written multiplicatively, x^{*n} is written as x^n. If $* = +$, then x^{*n} is written as nx.

Proposition 5.6.3 Let $(M, *)$ be a monoid, $x \in M$. There exists a unique homomorphism of monoids $f : (\mathbb{Z}, +) \to (M, *)$ such that $f(1) = x$. Note that $f(\mathbb{Z}) \subseteq M^\times$. So f defines a homomorphism of groups $f : (\mathbb{Z}^\times, +) \to (M^\times, *)$.

Proof We define f as

$$f(n) := \begin{cases} x^{*n}, & n \geq 0 \\ \iota(x^{*(-n)}), & n < 0 \end{cases}.$$

Let n, m be two elements of $\mathbb{Z}$.
(1) If $n, m > 0$. Then $f(n+m) = x^{*n} * x^{*m} = f(n+m)$.
(2) If $n, m < 0$. Then $f(n+m) = \iota(x^{*(-n-m)}) = \iota(x^{*(-m)} * x^{*(-n)}) = \iota(x^{*(-n)}) * \iota(x^{*(-m)}) = f(n) * f(m)$.
(3) If $n > 0, m < 0$ and $n + m > 0$. Then

$$f(n+m) = x^{*(n-(-m))} = x^{*n} * \iota(x^{*(-m)}) = f(n) * f(m).$$

(4) If $n > 0, m < 0$ and $n + m < 0$. Then

$$f(n+m) = \iota(x^{*(-n-m)}) = \iota(\iota(x^{*n}) * x^{*(-m)}) = \iota(x^{*(-m)}) * x^{*n} = f(m) * f(n).$$

□

Notation 5.6.4 If $x \in M^{\times}$, for any $n \in \mathbb{Z}$, let x^{*n} be the image of n by this unique homomorphism of monoids $(\mathbb{Z}, +) \to (M, *)$, $1 \mapsto x$. $x^{\cdot n}$ is denoted as x^n, x^{+n} is denoted as nx.

Proposition 5.6.5 Let $(M, *)$ be a monoid, $x, y \in M$.
(1) If $x * y = y * x$, then for any $(n, m) \in \mathbb{N}^2$,

$$x^{*n} * y^{*m} = y^{*m} * x^{*n}.$$

$$(x * y)^{*n} = x^{*n} * y^{*n}.$$

(2) If $x \in M$, $\iota(x^{*n}) = \iota(x)^{*n}$ and for any $(n, m) \in \mathbb{N}^2$, with $n \geq m$,

$$x^{*(n-m)} = x^{*n} * \iota(x)^{*m},$$

$$\iota(x^{*(n-m)}) = \iota(x)^{*n} * x^{*m}.$$

Proof
(1) We prove by induction on n such that $x^{*n} * y = y * x^{*n}$. If $n = 0$, $x^{*n} = e_M$, so $y * e_M = y = e_M * y$. If $x^{*n} * y = y * x^{*n}$, we have $x^{*n+1} * y = x^{*n} * y * x = y * x^{*n} * x = y * x^{*(n+1)}$. We apply this statement in replacing n by m, x by y, and y by x^{*n}. From $x^{*n} * y = y * x^{*n}$, we deduce that $y^{*m} * x^{*n} = x^{*n} * y^{*m}$. We prove $(x * y)^{*n} = x^{*n} * y^{*n}$ by induction on n. If $n = 0, e_M = e_M * e_M$. If $n = 1, x * y = x * y$. If $(x * y)^{*n} = x^{*n} * y^{*n}$, then

$$(x*y)^{*(n+1)} = (x*y)^{*n}*x*y = x^{*n}*y^{*n}*x*y = x^{*n}*x*y^{*n}*y = x^{*(n+1)}*y^{*(n+1)}.$$

(2) $x^{*n} * \iota(x)^{*n} = (x * \iota(x))^{*n} = e_M^{*n} = e_M$, since $(\mathbb{N}, +) \to (M, *), n \mapsto e_M$ is a homomorphism of monoids. $\iota(x)^n * x^{*n} = (\iota(x) * x)^{*n} = e_M$. If $n \geq m$

$$x^{*n} * \iota(x)^{*m} = x^{*(n-m)} * x^{*m} * \iota(x)^{*m} = x^{*(n-m)}.$$

$$\iota(x)^{*n} * x^{*m} = \iota(x)^{*(n-m)} * \iota(x)^{*m} * x^{*m} = \iota(x)^{*(n-m)} = \iota(x^{*(n-m)}).$$

□

Definition 5.6.6 Let I be a set. For any $i \in I$, let $(M_i, *_i)$ be a set equipped with a composition law. Let

$$M = \prod_{i\in I} M_i = \{(x_i)_{i\in I} \mid \forall i \in I, x_i \in M_i\}.$$

We define a composition law on M such that

$$(x_i)_{i\in I} * (y_i)_{i\in I} = (x_i * y_i)_{i\in I}.$$

For any $j \in I$, let $\pi_j : M \to M_j,\ (x_i)_{i\in I} \mapsto x_j$.

Proposition 5.6.7
(1) If $\forall i \in I, *_i$ is commutative, then $*$ is communitative.
(2) If $\forall i \in I, *_i$ is associative, then $*$ is associative. Moreover, $\pi_j : (M, *) \to (M_j, *_j)$ is a homomorphism of semigroups.
(3) If $\forall i \in I$, e_i is a neutral element of $(M_i, *_i)$, then $e := (e_i)_{i\in I}$ is a neutral element of $(M, *)$. Moreover, if each $(M_i, *_i)$ is a monoid, then $\pi_j : (M, *) \to (M_j, *_j)$ is a homomorphism of monoids.
(4) Assume that each $(M_i, *_i)$ is a monoid. Then $M^\times = \prod_{i\in I} M_i^\times$. In particular, if each $(M_i, *_i)$ is a group, then $M^\times = \prod_{i\in I} M_i^\times$ is also a group.

Proof If $(x_i)_{i\in I}, (y_i)_{i\in I} \in M$, then $\pi_j(x * y) = \pi_j((x_i * y_i)_{i\in I}) = x_j *_j y_j = \pi_j(x) * \pi_j(y)$.
proof of (4): Assume that $x = (x_i)_{i\in I} \in M^\times$. Then $\exists y = (y_i)_{i\in I} \in M^\times$ such that $x * y = e := (e_i)_{i\in I}$, where e_i is the neutral element of $(M_i, *_i)$. $x * y = (x_i * y_i)_{i\in I} = (e_i)_{i\in I} =$. So $x_i *_i y_i = e_i$ for all $i \in I$. Therefore, $x_i \in M_i^\times$ for all $i \in I$. Hence $M^\times \subseteq \prod_{i\in I} M_i^\times$. Now let $x = (x_i)_{i\in I} \in \prod_{i\in I} M_i^\times$. We claim that $(\iota(x_i))_{i\in I}$ is the inverse of x. In fact $(x_i)_{i\in I} * (\iota(x_i))_{i\in I} = e$. So $x \in M^\times$. □

Theorem 5.6.8 Suppose that each $(M_i, *_i)$ is a semigroup. Let $(N, \star)$ be a semigroup (resp. monoid, group). For any $i \in I$, let $f_i : N \to M_i$ be a homomorphism of semigroups (resp. monoid, group). Then there is a unique homomorphism of semigroups (resp. monoid, group) $f : M \to N$ such that $\forall i \in I, \pi_i \circ f = f_i$. $(M, *)$ is called the **product** of $(M_i, *_i)$.

Proof By Proposition 3.9.5, there exists a unique mapping $f : N \to M$ such that $\forall i \in I, \pi_i \circ f = f_i$. We check that f is a homomorphism.
Recall that $\forall y \in N, f(y) = (f_i(y))_{i\in I}$. If $(y, z) \in N \times N$, then $f(y * z) = (f_i(y) * f_i(z))_{i\in I} = (f_i(y))_{i\in I} * (f_i(z))_{i\in I} = f(y) * f(z)$. If each $(M_i, *_i)$ is a monoid with neutral element e_i, and e_N is the neutral element of N, in the case where each f_i is a homomorphism of monoids $(f_i(e_N) = e_i)$. One has $f(e_n) = (f_i(e_N))_{i\in I} = (e_i)_{i\in I}$ is the neutral element of M. □

Notation 5.6.9 Let M be a communitative monoid, $(x_i)_{i\in I}$ be a family of elements in M. We suppose that $I_0 = \{i \in I \mid x_i \neq e\}$ is finite. We pick a natural number n and a bijection $\sigma : \{1, 2, \dots, n\} \to I_0$. If the composition law of M is written as $+$, then

$$\sum_{i\in I} x_i \text{ denotes } (x_{\sigma(1)} + x_{\sigma(2)} + \cdots + x_{\sigma(n)}),$$

it denotes the neutral element 0 of M when $I_0 = \varnothing$. If the composition law of M is written as $\cdot$, then

$$\prod_{i\in I} x_i \text{ denotes } (x_{\sigma(1)} \cdot x_{\sigma(2)} \cdots x_{\sigma(n)}),$$

it denotes the neutral element 1 of M when $I_0 = \varnothing$.
Let $(M_i)_{i\in I}$ be a family of communitative monoids. (The composition law of M_i is written additively, the neutral element of M_i is written 0)

Notation 5.6.10 Let $(M_i)_{i\in I}$ be a family of communitative monoids. For any $i \in I$, let e_i be a neutral element of M_i. We denote by

$$\bigoplus_{i\in I} M_i$$

the set of $(x_i)_{i\in I} \in \prod_{i\in I} M_i$ such that $\{i \in I \mid x_i \neq e_i\}$ is finite.

Proposition 5.6.11 $\bigoplus\limits_{i\in I} M_i$ is a submonoid of $\prod\limits_{i\in I} M_i$.

Proof First, $e := (e_i)_{i\in I} \in \bigoplus_{i\in I} M_i$. Let $*_i$ be the composition law of M_i, $*$ be the direct product of $(*_i)_{i\in I}$. If $x = (x_i)_{i\in I}$ and $y = (y_i)_{i\in I}$ are in $\bigoplus_{i\in I} M_i$, then $x * y = (x_i * y_i)_{i\in I}$. If $I_x = \{i \in I \mid x_i \neq e_i\}$ and $I_y = \{i \in I \mid y_i \neq e_i\}$ are finite, then $\{i \in I \mid x_i * y_i \neq e\} \subseteq I_x \cup I_y$. So $x \in \bigoplus_{i\in I} M_i$ and $y \in \bigoplus_{i\in I} M_i$ imply that $x * y \in \bigoplus_{i\in I} M_i$. □

Definition 5.6.12 (Direct sum) $\bigoplus_{i\in I} M_i$ is called the **direct sum** of $(M_i)_{i\in I}$. For any $j \in I$, the homomorphisms

$$\begin{aligned} M_j &\xrightarrow{\mathrm{Id}_{M_j}} M_j \\ M_j &\longrightarrow M_i, \quad (i \neq j) \\ x_j &\longmapsto e_i \end{aligned}$$

induce:

$$\begin{aligned} M_j &\longrightarrow \textstyle\prod_{i\in I} M_i \\ x_j &\longmapsto (y_i)_{i\in I} \end{aligned}$$

with

$$y_i = \begin{cases} x_j, & j = i \\ e_i, & i \neq j \end{cases}.$$

Claim: This homomorphism takes value in $\bigoplus_{i\in I} M_i$. We denote by

$$\lambda_j : M_j \longrightarrow \bigoplus_{i\in I} M_i$$

this homomorphism.

$$\lambda_j(x_j)_i = \begin{cases} x_j, & i = j \\ e_i, & i \neq j \end{cases},$$

$$\lambda_j(x_j)_i = (\lambda_j(x_j)_i)_{i\in I}.$$

Theorem 5.6.13 Let $(N, \star)$ be a communitative monoid. Then for any $i \in I$, let $\psi_i : M_i \to N$ be a homomorphism of monoids. Then there is a unique homomorphism of monoids $\psi : \bigoplus\limits_{i\in I} M_i \to N$ such that for any $j \in I, \psi \circ \lambda_j = \psi_j$.

$$\begin{tikzcd}
\bigoplus_{i\in I} M_i \arrow[r, "\psi"] & N \\
M_j \arrow[u, "\lambda_j"] \arrow[ru, "\psi_j"'] &
\end{tikzcd}$$

Proof For simplicity, we write all composition laws as $+$, and all neutral element as 0. We should define $\psi : \bigoplus_{i\in I} M_i \to N,\ (x_i)_{i\in I} \mapsto \sum_{i\in I} \psi_i(x_i)$. $\psi\left((0)_{i\in I}\right) = \sum_{i\in I} 0 = 0$. $\psi\left((x_i)_{i\in I} + (y_i)_{i\in I}\right) = \psi\left((x_i + y_i)_{i\in I}\right) = \sum_{i\in I} \psi_i(x_i + y_i) = \sum_{i\in I} [\psi_i(x_i) + \psi_i(y_i)] = \sum_{i\in I} \psi_i(x_i) + \sum_{i\in I} \psi_i(y_i)$. (The last equality holds because the composition law of N is commutative.) □

Chapter 6

Rings and Modules

6.1 Unitary Rings

Definition 6.1.1 Let A be a set, and $+$ and $*$ be composition laws. If
(1) $(A, +)$ forms a communitative group.
(2) $(A, *)$ forms a monoid.
(3) For any $(a, b, c) \in A^3$, $a*(b+c) = (a*b)+(a*c)$ and $(b+c)*a = (b*a)+(c*a)$.
(4)† If in addition, $*$ is communitative, then we say that the unitary ring $(A, +, *)$ is communitative.

Example 6.1.2 $(\mathbb{Z}, +, \cdot)$ is a unitary ring.

Note that, if we denote by $\hat{*}$ the composition law

$$A \times A \longrightarrow A,$$

$$(a, b) \longmapsto b * a.$$

Then $(A, +, \hat{*})$ forms a unitary ring. We call it the opposite unitary ring of $(A, +, *)$.

Notation 6.1.3 Usually, we denote by $+$ the first composition law, of a unitary ring A and call it the **addition**. We denote by 0 the neutral element of $+$, and call it the **zero element** of A. Usually we denote by $\cdot$ the second composition law of A and call it the **multiplication**. We denote by 1 the neutral element with respect to $\cdot$, and call it the **unity element** of A.

Definition 6.1.4 Let A be a unitary ring and B be a subset of A. If B is a subgroup of $(A, +)$ and a submonoid of $(A, \cdot)$, then we call B a **unitary subring** of A.

Example 6.1.5 Let $\{0\}$ be the set of 1 element. Let $+$ and $\cdot$ be both the composition law $\{0\} \times \{0\} \to \{0\}, (0, 0) \mapsto 0$. Then $(\{0\}, +, *)$ is a unitary ring. We call it the **zero ring**.

Definition 6.1.6 Let A and B be unitary rings and $f : A \to B$ be a mapping. If f is a group homomorphism from $(A, +)$ to $(B, +)$, and is a monoid homomorphism from $(A, \cdot)$ to $(B, \cdot)$, then we call f a **unitary ring homomorphism**.

Proposition 6.1.7 For any unitary ring A, there exists a unitary ring homomorphism $A \to \{0\}$.

Lemma 6.1.8 Let A be a unitary ring.
(1) $\forall a \in A, 0a = a0 = 0$.
(2) $\forall a, b \in A, -(ab) = (-a)b = a(-b)$.

Proof
(1) $0 + 0 = 0$, so $0 + 0a = 0a = (0 + 0)a = 0a + 0a$. Hence $0a = 0$.
(2) $ab + (-a)b = (a + (-a))b = 0b = 0, ab + a(-b) = a(b + (-b)) = a0 = 0$.
□

Proposition 6.1.9 For any unitary ring A, there exists a unitary ring homomorphism from $\mathbb{Z}$ to A.

Proof If $f : \mathbb{Z} \to A$ is a unitary ring homomorphism, then $f(1) = 1_A$. So f is identifies with the unitary group homomorphism.

$$(\mathbb{Z}, +) \longrightarrow (A, +),$$

$$n \longmapsto n1_A.$$

It remains to check that for any $(n, m) \in \mathbb{Z}^2$, $f(nm) = f(n)f(m)$. Note that , if $(n, m) \in \mathbb{N} \times \mathbb{N}$, then

$$f(n) = \underbrace{1_A + \cdots + 1_A}_{n \text{ copies}},\ f(m) = \underbrace{1_A + \cdots + 1_A}_{m \text{ copies}}.$$

So $f(n)f(m) = nm1_A1_A = nm1_A = f(nm)$. $f(-n)f(m) = (-f(n))f(m) = -f(n)f(m) = -f(nm) = f(-nm)$. $f(-n)f(-m) = \ldots$ □

Definition 6.1.10 Let K be a unitary ring. We denote by $K^\times$ the invertible elements of $(K, \cdot)$. If $K^\times = K\backslash\{0\}$ then we say that K is a division ring. If in addition, K is commutative, then we say that K is a **field**.

Example 6.1.11 $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields.

6.2 Action of Monoids

Definition 6.2.1 Let $(G, *)$ be a monoid, the neutral element of which is denoted as e. Let X be a set. We call **left action** of G on X any mapping

$$\phi : G \times X \to X,$$

such that
(1) $\phi(e, x) = x$, for any $x \in X$.
(2) $\forall(a, b) \in G \times G, \forall x \in X$,

$$\phi(a * b, x) = \phi(a, \phi(b, x)).$$

(Resp. right action)

Remark 6.2.2 A left action of $(G, *)$ on X is a right action of $(G, \hat{*})$ on X.

Notation 6.2.3 If $* = \cdot$, a left action is usually denoted as

$$G \times X \longrightarrow X,$$

$$(a, x) \longmapsto ax.$$

Condition (1) becomes $ex = x$, (2) becomes $(ab)x = a(bx)$.

Example 6.2.4 Let G be a group, H be a subgroup of G. Then

$$H \times G \longrightarrow G,$$

$$(h, g) \longmapsto hg.$$

is a left action of H on G. (Resp. right action.)

Proposition 6.2.5 Let G be a monoid, X be a set and $\phi : G \times X \longrightarrow X$ be a left action of G on X. We define a binary relation $\sim_\phi$ on X as follows:

$$x \sim_\phi y \Leftrightarrow \exists g \in G, \phi(g, x) = y.$$

Then $\sim_\phi$ is reflexive and transitive. It is an equivalence relation if G is a group.

Proof
Reflexivity: Let e be the neutral element of G, then $x = ex$, so $x \sim_\phi x$.
Transitivity: If $y = ax$ and $z = by$, then $z = b(ax) = (ba)x$, so $x \sim_\phi y \wedge y \sim_\phi z \Rightarrow x \sim_\phi z$.
Assume that G is a group. If $y = ax$, then $\iota(a)y = \iota(a)(ax) = (\iota(a)a)x = ex = x$, so $x \sim_\phi y$ implies $y \sim_\phi x$. □

Definition 6.2.6 Let G be a group, X be a set and $\phi : G \times X \longrightarrow X$ be a left action. For any $x \in X$, the equivalence class of x under the equivalence relation $\sim_\phi$ is called the **orbit** of x under the action ϕ, denoted as $\mathrm{orb}_\phi(x)$. We denote by $G\backslash X$ the set of all orbits of X under the action ϕ. (Resp. right action and X/G.)

Remark 6.2.7 If X is finite, then

$$\mathrm{card}(X) = \sum_{A \in G\backslash X} \mathrm{card}(A).$$

In particular, if $(G, *)$ is a finite group, and H is a subgroup of G, then $\mathrm{card}(G) = \mathrm{card}(H)\mathrm{card}(H\backslash G)$. In fact, $H\backslash G = \{H{*}x \mid x \in G\}$, $H{*}x := \{h{*}x \mid h \in H\}$.

6.3 Vector Space

Definition 6.3.1 Let K be a unitary ring. Let $(V, +)$ be an abelian group. (Neutral element of $(V, +)$ is denote as 0.) We call a **left K-module structure** any left action of $(K, \cdot)$ on V.

$$\phi : K \times V \longrightarrow V$$

(1) $\forall (a, b) \in K \times K, \forall x \in V$,

$$\phi(a + b, x) = \phi(a, x) + \phi(b, x).$$

(2) $\forall a \in K, \forall (x,y) \in V \times V$,

$$\phi(a, x+y) = \phi(a,x) + \phi(a,y).$$

The abelian group $(V,+)$ equipped with a left K-module structure is called a **left K-module**. If K is communitative, left and right K-modules structures have the same axioms. So we just call them K-module structures. Left and right K-modules structures are called K-modules. If K is a field, a K-module is called a **vector space** over K.

Example 6.3.2 $(\{0\},+)$ is a left K-module. Action

$$\phi : K \times \{0\} \longrightarrow \{0\},$$

$$\phi(a,0) = 0.$$

It is called the zero K-module.

Example 6.3.3 Consider the action

$$\phi : K \times K \longrightarrow K,$$

$$\phi(a,x) = ax.$$

ϕ defines a left K-module structure on K.

Definition 6.3.4 Let I be a set and $(V_i)_{i\in I}$ be a family of left K-modules.

$$V = \prod_{i\in I} V_i.$$

The action

$$\phi : (K \times V) \longrightarrow V,$$

$$(a, (x_i)_{i\in I}) \longmapsto (a * x_i)_{i\in I}$$

defines a left K-module structure on V.

6.4 Submodules

Definition 6.4.1 Let V be a left K-module, we call **left sub-K-module** of V any subgroup W of $(V, +)$ such that for any $(a, x) \in K \times W, ax \in W$. (resp. right.)

Example 6.4.2 $\{0\}$ and V itself is a left sub-K-modules of V.

Definition 6.4.3 Let E and F be left-K-modules. We call **homomorphism of left K-modules from** E **to** F any mapping $f : E \to F$, such that
(1) f is a homomorphism of groups from $(E, +)$ to $(F, +)$.
(2) For any $(a, x) \in K \times E, f(ax) = af(x)$.
If K is communitative, a homomorphism of K-module is also called a K**-linear mapping**.

Lemma 6.4.4 Let V be a left K-module.
(1) $\forall a \in K, a0_V = 0_V$.
(2) $\forall x \in V, 0x = 0_V$.

Proof
(1) $a0_V = a(0_V + 0_V) = a0_V + a0_V \Rightarrow 0_V = a0_V$.
(2) $0x = (0 + 0)x = 0x + 0x \Rightarrow 0x = 0_V$. □

Theorem 6.4.5 Let $f : E \to F$ be a homomorphism of left-K-modules.
(1) $\ker(f)$ is a left sub-K-module of E.
(2) $\mathrm{Im}(f)$ is a left sub-K-module of F.

Proof First, $\ker(f)$ is a subgroup of E, $\mathrm{Im}(f)$ is a subgroup of F.
(1) Let $a \in K, x \in \ker(f), f(ax) = af(x) = a0_V = 0_V$. So $ax \in \ker(f)$.
(2) Let $y \in \mathrm{Im}(f)$, there exists $x \in E$ such that $f(x) = y$. For any $a \in K, ay = af(x) = f(ax) \in \mathrm{Im}(f)$ □

Proposition 6.4.6 Let V be a left K-module. For any $x \in V, -x = (-1)x$.

Proof

$$(-1)x + x = (-1 + 1)x = 0x = 0_V.$$

□

Example 6.4.7 Let $(V_i)_{i\in I}$ be a family of left K-modules. We denote by

$$\bigoplus_{i\in I} V_i \text{ the set of } (x_i)_{i\in I} \in \prod_{i\in I} V_i,$$

such that $\{i \in I \mid x_i \neq 0_{V_i}\}$. This is a subgroup of $\prod_{i\in I} V_i$. For any $a \in K$, and $(x_i)_{i\in I} \in \bigoplus_{i\in I} V_i$,

$$\{i \in I \mid ax_i \neq 0_{V_i}\} \subseteq \{i \in I \mid x_i \neq 0_{V_i}\}.$$

So $a(x_i)_{i\in I} = (ax_i)_{i\in I} \in \bigoplus\limits_{i\in i} V_i$, which means that $\bigoplus\limits_{i\in I} V_i$ is a left sub-K-module of $\prod\limits_{i\in I} V_i$. $\bigoplus\limits_{i\in I} V_i$ is called the direct sum of $(V_i)_{i\in I}$. We denote by

$$K^{\oplus I}$$

the left sub-K-module of K^I.

Proposition 6.4.8 Let E and F be left K-modules, $f : E \to F$ be a mapping.
(1) If f is a homomorphism of left K-modules, for any $n \in \mathbb{N}_{\geq 1}$, any $(a_1, a_2, \ldots, a_n) \in K$, and $(x_1, x_2, \ldots, x_n) \in E^n$,

$$f(a_1x_1 + \cdots + a_nx_n) = a_1f(x_1) + \cdots + a_nf(x_n).$$

(2) Suppose that for any $a \in K$, $(x, y) \in E^2$,

$$f(x + ay) = f(x) + af(y).$$

Then f is a homomorphism of left K-modules.

Proof (1) Induction on n.
(2) Take $a = 1$, for any $(x, y) \in E$, $f(x + y) = f(x) + f(y)$.
Take $x = 0_E$, $f(ay) = 0_F + af(y) = af(y)$. □

Definition 6.4.9 If a left K-module homomorphism is a bijection we say that it is a **left K-module isomorphism**.

6.5 Universal Property

Proposition 6.5.1 Let $(V,+)$ be a communitative group. Then

$$\begin{aligned} \mathbb{Z}\times V &\longrightarrow V\\ (n,x) &\longmapsto nx \end{aligned}$$

defines a $\mathbb{Z}$-module substructure on V.

Proof First, nx is the image of n by the unique homomorphism of groups $\phi_x : \mathbb{Z}\to V, 1\mapsto x$.

$$(n+m)x = \phi_x(n+m) = \phi_x(n)+\phi_x(m) = nx+mx.$$

Let $(x,y)\in V^2$,

$$\begin{aligned} \phi_x+\phi_y :&\mathbb{Z}\longrightarrow V,\\ &n\longmapsto \phi_x(n)+\phi_y(n) = nx+ny \end{aligned}$$

is a homomorphism of groups, since for any $(n,m)\in\mathbb{Z}^2$

$$\begin{aligned} &(\phi_x+\phi_y)(n+m)\\ =&\phi_x(n+m)+\phi_y(n+m) = \phi_x(n)+\phi_x(m)+\phi_y(n)+\phi_y(m)\\ =&(\phi_x(n)+\phi_y(n))+(\phi_x(m)+\phi_y(m)). \end{aligned}$$

Since $(\phi_x+\phi_y)(1) = x+y = \phi_{x+y}$, $\phi_{x+y} = \phi_x+\phi_y$. So $n(x+y) = nx+ny, \forall n\in\mathbb{Z}$. $1x = \phi_x(1) = x$. If $n\in\mathbb{N}$,

$$(nm)x = \phi_x(nm) = \phi_x(\underbrace{m+\cdots+m}_{n\text{ copies}}) = n\phi_x(m) = n(mx).$$

If $-n\in\mathbb{N}$,

$$\phi_x(nm) = -\phi_x((-n)m) = -(-n)\phi(m) = n\phi_x(m).$$

□

Proposition 6.5.2 Let V be a left K-module, $x\in V$. There exists a unique homomorphism of left K-modules $\phi_x : K\longrightarrow V$, such that $\phi_x(1) = x$.

Proof If ϕ_x exists, then it should satisfy

$$\forall a \in K, \phi_x(a) = a\phi_x(1) = ax.$$

It suffices to check that $\phi_x : K \to V, a \mapsto ax$ is a homomorphism.

$$\phi_x(a+b) = (a+b)x = ax + bx = \phi_x(a) + \phi_x(b),$$

$$\phi_x(\lambda a) = (\lambda a)x = \lambda(ax) = \lambda\phi_x(a).$$

□

Proposition 6.5.3 Let $(V_i)_{i\in I}$ be a family of left K-modules.
(1) Let W be a left K-module. For any $i \in I$, let $f_i : W \to V_i$ be aa homomorphism. Then there exists a unique homomorphism

$$f : W \longrightarrow \prod_{i\in I} V_i,$$

such that

$$\forall i \in I, \pi_i \circ f = f_i,$$

where π_i sends $(x_j)_{j\in I} \in \prod_{j\in I} V_j$ to x_i.
(2) Let W be a left K-module, for any $i \in I$, let $g_i : V_i \to W$ be a homomorphism of left K-modules. There exists a unique homomorphism

$$g : \bigoplus_{i\in I} V_i \longrightarrow W$$

such that

$$\forall i \in I, g \circ \lambda_i = g_i,$$

where

$$\lambda_j : V_j \longrightarrow \bigoplus_{i\in I} V_i,$$

$$x_j \longrightarrow (y_i)_{i\in I} \text{ with } y_i = \begin{cases} x_j, i = j \\ 0, i \neq j \end{cases}.$$

Proof
(1) There exists a unique mapping $f : W \to \prod_{i\in I} V_i$, such that

$$\forall i \in I, \pi_i \circ f = f_i,$$

$$\forall z \in W, f(z) = (f_i(z))_{i\in I}.$$

We have proved that f is a homomorphism of groups.

$$\forall a \in K, z \in W. f(az) = (f_i(az))_{i\in I} = (af_i(z))_{i\in I} = af(z).$$

(2) We have prove that there exists a unique $g : \bigoplus_{i\in I} V_i \to W$ homomorphism of group such that $\forall i \in I, g \circ \lambda_i = g_i$. $g((x_i)_{i\in I}) = \sum_{i\in I} g_i(x_i)$.

$$\begin{aligned}\forall a \in K, g\left(a(x_i)_{i\in I}\right) =& g\left((ax_i)_{i\in I}\right)\\ =& \sum_{i\in I} g_i(ax_i) = \sum_{i\in I} ag_i(x_i) = a\sum_{i\in I} g_i(x_i) = ag(x).\end{aligned}$$

□

Application 6.5.4 Let V be a left K-module. Let I be a set and $(x_i)_{i\in I} \in V^I$. For any $i \in I$, let

$$\phi_{x_i} : K \longrightarrow V, a \mapsto ax_i.$$

So the family $(\phi_{x_i})_{i\in I}$ determines a homomorphism of left K-modules

$$\Phi : K^{\oplus I} \longrightarrow V,$$

$$(a_i)_{i\in I} \longmapsto \sum_{i\in I} \phi_{x_i}(a_i) = \sum_{i\in I} a_i x_i.$$

6.6 Matrices

Definition 6.6.1 Let $n \in \mathbb{N}$. Let V be a **left** K-module. For any $(x_1, \ldots, x_n) \in V^n$, we denote by

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} : K^n \longrightarrow V,$$

$$(a_1, \ldots, a_n) \longmapsto a_1x_1 + \cdots + a_nx_n.$$

This is a homomorphism of left K-modules.

Example 6.6.2 Consider the case where $V = K^p$ with $p \in \mathbb{N}$. Each x_i is of the form $(b_{i,1},\ldots,b_{i,p})$.

$$\text{So} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \text{ becomes} \begin{pmatrix} b_{1,1} & \ldots & b_{1,p} \\ \vdots & \ddots & \vdots \\ b_{n,1} & \ldots & b_{n,p} \end{pmatrix}.$$

Definition 6.6.3 We call n by p matrix with coefficients in K any homomorphism of left K-module from K^n to K^p.

Definition 6.6.4 Let n and p be natural numbers,and V be a left K-module. Let $A : K^n \to K^p$, and $\varphi : K^p \to V$ be homomorphism of left K-modules. We denote by

$$A\varphi : K^n \longrightarrow V$$

be the mapping $\varphi \circ A$.

Proposition 6.6.5 Let E, F and G be left K-modules. Let $\varphi : E \to F$ and $\psi : F \to G$ be homomorphism of left K-modules. Then $(\varphi \circ \psi) : E \to G$ is a homomorphism of left K-modules.

Proof Let $(x,y) \in E^2, a \in K.(\psi \circ \phi)(x+ay) = \psi(\varphi(x+ay)) = \psi(\varphi(x) + a\varphi(y)) = \psi(\varphi(x)) + a\psi(\varphi(y))$. □

Computation Suppose that

$$A = \begin{pmatrix} a_{1,1} & \cdots & a_{1,p} \\ \vdots & \ddots & \vdots \\ a_{n,1} & \cdots & a_{n,p} \end{pmatrix}, \ \varphi = \begin{pmatrix} x_1 \\ \vdots \\ x_p \end{pmatrix}.$$

For $t = (t_1,\ldots,t_n) \in K^n$,

$$t \xmapsto{A} \left(\sum_{i=1}^{n} t_i a_{i,1}, \ldots, \sum_{i=1}^{n} t_i a_{i,p} \right) \xmapsto{\varphi} \sum_{j=1}^{p} \sum_{i=1}^{n} t_i a_{i,j} x_j.$$

So,

$$A\varphi = \begin{pmatrix} a_{1,1}x_1 + \cdots + a_{1,p}x_p \\ \vdots \\ a_{n,1}x_1 + \cdots + a_{n,p}x_p. \end{pmatrix}$$

Question Let

$$A = \begin{pmatrix} a_{1,1} & \cdots & a_{1,p} \\ \vdots & \ddots & \vdots \\ a_{n,1} & \cdots & a_{n,p} \end{pmatrix}, B = \begin{pmatrix} b_{1,1} & \cdots & b_{1,q} \\ \vdots & \ddots & \vdots \\ b_{p,1} & \cdots & b_{p,q} \end{pmatrix}. AB = ?$$

We have

$$AB = \begin{pmatrix} a_{1,1}b_{1,1} + \cdots + a_{1,p}b_{p,1} & \cdots & a_{1,1}b_{p,1} + \cdots + a_{1,p}b_{p,q} \\ \vdots & \ddots & \vdots \\ a_{n,1}b_{1,1} + \cdots + a_{n,p}b_{p,1} & \cdots & a_{n,1}b_{p,1} + \cdots + a_{n,p}b_{p,q} \end{pmatrix}.$$

Example 6.6.6 Let $(a_1, a_2, \ldots, a_n) \in K^n$, we denote by

$$\begin{aligned} \mathrm{diag}(a_1, \ldots, a_n) : K^n &\longrightarrow K^n \\ (t_1, \ldots, t_n) &\longmapsto (t_1a_1, \ldots, t_na_n). \end{aligned}$$

$\mathrm{diag}(a_1, \ldots, a_n)$ is called a **diagonal matrix**.

Example 6.6.7 $\mathrm{Id}_{K^n} : K^n \longrightarrow K^n,\ t \mapsto t$ is also written as $I_n = \begin{pmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{pmatrix}$

Let V be a left K-module, $(x_1, \ldots, x_n) \in V^n$, $(a_1, \ldots, a_n) \in K^n$.

$$\mathrm{diag}(a_1, \ldots, a_n) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} a_1x_1 \\ \vdots \\ a_nx_n \end{pmatrix}.$$

$$\mathrm{diag}(a_1, \ldots, a_n)\mathrm{diag}(b_1, \ldots, b_n) = \mathrm{diag}(a_1b_1, \ldots, a_nb_n).$$

6.7 Linear Equations

We fix a unitary ring.

Definition 6.7.1 Let $p \in \mathbb{N}$. For $(a_1, \ldots, a_p) \in K^p$, let $j(a_1, \ldots, a_p)$ be the least index $i \in \{1, \ldots, p\}$ such that $a_i \neq 0$. By convention,

$$j(0, \ldots, 0) = p + 1.$$

Let V be a left K-module, $A \in M_{n,p}(K)$. Let $(b_1, \dots, b_n) \in V^n$. We consider

$$A \begin{pmatrix} x_1 \\ \vdots \\ x_p \end{pmatrix} = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \tag{$*$}$$

We write A into the form

$$\begin{pmatrix} \vec{a}^{(1)} \\ \vdots \\ \vec{a}^{(n)} \end{pmatrix}, \vec{a}^{(i)} = (a_{i,1}, \dots, a_{i,p}).$$

Definition 6.7.2 We say that the matrix is of row echelon form if

$$j\left(\vec{a}^{(1)}\right) \leq j\left(\vec{a}^{(2)}\right) \leq \cdots \leq j\left(\vec{a}^{(n)}\right),$$

and the strict inequality holds once

$$j\left(\vec{a}^{(i)}\right) \leq p.$$

If in addition $a_{i,j\left(\vec{a}^{(i)}\right)} = 1$, and $a_{k,j\left(\vec{a}^{(i)}\right)} = 0$ for any $k \neq i$ once $\vec{a}^{(i)} \neq (0, \dots, 0)$. We say that A is of **reduced row echelon form**.

Example 6.7.3

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 0 & 0 & 2 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

are of row echelon form.

Theorem 6.7.4 Suppose that A is of reduced echelon form. Let

$$I(A) = \{i \in \{1, \dots, n\} \mid \vec{a}^{(i)} \neq (0, \dots, 0)\},$$

$$J_0(A) = \{1, \dots, p\} \backslash \{j\left(\vec{a}^{(i)}\right) \mid i \in I(A)\}.$$

(1) If there exists $i \in \{1, \dots, n\} \backslash I(A), b_i \neq 0$ the equation $A \begin{pmatrix} x_1 \\ \vdots \\ x_p \end{pmatrix} = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$ has no solution.

(2) If $\forall i \in \{1,\ldots,n\}\backslash I(A), b_i = 0$. The solution set of the equation is the image of the following mapping:

$$\Phi : V^{I(A)} \longrightarrow V^p \text{ with}$$

$$(z_l)_{l\in J_0(A)} \longmapsto (x_1,\ldots,x_p),$$

$$x_k = \begin{cases} z_k & \text{, if } k \in J_0(A) \\ b_i - \sum_{l\in J_0(A)} a_{i,l} z_l & \text{, if } k = j\left(\vec{a}^{(i)}\right). \end{cases}$$

Proposition 6.7.5 Let m, n, p be natural numbers. $S \in M_{m,n}(K), A \in M_{n,p}$. If $(x_1,\ldots,x_p)$ is a solution of the equation

$$A\begin{pmatrix} x_1 \\ \vdots \\ x_p \end{pmatrix} = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}. \qquad (*)$$

Then it is also a solution of the equation

$$(SA)\begin{pmatrix} x_1 \\ \vdots \\ x_p \end{pmatrix} = S\begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}. \qquad (*_S)$$

Moreover, if S is left invertible (namely there exists $T \in M_{n,m}(K)$ such that $TS = I_n$), then $(*)$ and $(*_S)$ have the same solution set.

Proof

$$(SA)\begin{pmatrix} x_1 \\ \vdots \\ x_p \end{pmatrix} = S\begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}.$$

So

$$TSA\begin{pmatrix} x_1 \\ \vdots \\ x_p \end{pmatrix} = TS\begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \Rightarrow A\begin{pmatrix} x_1 \\ \vdots \\ x_p \end{pmatrix} = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}.$$

□

Definition 6.7.6 Let $n \in \mathbb{N}$ and $\sigma : \{1,\ldots,n\} \to \{1,\ldots,n\}$ be a bijection.

Denote by

$$P_\sigma : K^n \longrightarrow K^n,$$

$$P(t_1, \dots, t_n) := \left(t_{\sigma^{-1}(1)}, \dots, t_{\sigma^{-1}(n)}\right).$$

P_σ is a homomorphism of left K-modules.

$$P_\sigma P_{\sigma^{-1}} = P_{\sigma^{-1}} P_\sigma = I_n.$$

Let V be a left K-module, $(x_1, \dots, x_n) \in V$,

$$P_\sigma \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} : K^n \longrightarrow V,$$

$$(t_1, \dots, t_n) \overset{P_\sigma}{\longmapsto} (t_{\sigma^{-1}(1)}, \dots, t_{\sigma^{-1}(n)}) \overset{\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}}{\longmapsto} \sum_{i=1}^{n} t_{\sigma^{-1}(i)} x_i = \sum_{j=1}^{n} t_j x_{\sigma(j)}.$$

$$P_\sigma \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} x_{\sigma(1)} \\ \vdots \\ x_{\sigma(n)} \end{pmatrix}, \; P_\sigma \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix} = \begin{pmatrix} e_{\sigma(1)} \\ \vdots \\ e_{\sigma(n)} \end{pmatrix}$$

Definition 6.7.7 If $\underline{r} = (r_1, r_2, \dots, r_n) \in K^n$, we denote by $D_{\underline{r}}$ the matrix $\operatorname{diag}(r_1, \dots, r_n)$. If for any $i \in \{1, \dots, n\}$, r_i is left invertible and is a inverse of s_i, then

$$D_{\underline{s}} D_{\underline{r}} = I_n.$$

Definition 6.7.8 Let $n \in \mathbb{N}, i \in \{1, \dots, n\}, c = (c_1, \dots, c_n) \in K^n, c_i = 0$. Denote by

$$S_{i,c} : K^n \longrightarrow K^n,$$

$$S_{i,c}(t_1, \dots, t_n) := \left(t_1, \dots, t_{i-1}, t_i + \sum_{j=1}^{n} t_j c_j, t_{i+1}, \dots, t_n\right)$$

$$S_{i,c}S_{i,-c} = S_{i,-c}S_{i,c} = I_n$$

$$S_{i,c}\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} : (t_1, \dots, t_n) \longmapsto \sum_{j=1}^{n} t_j x_j + \sum_{j=1}^{n} t_j c_j x_i$$

$$S_{i,c}\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} x_1 + c_1 x_i \\ \vdots \\ x_i \\ \vdots \\ x_n + c_n x_i \end{pmatrix}$$

Definition 6.7.9 Let $G_n(K)$ be the subset of $M_{n,n}(K)$ consisting of matrices S, that can be written as $U_1, \dots, U_N$, where $N \in \mathbb{N}$ (if $N = 0$, by convention, $S = I_n$) and each U_i is of the following forms:
(1) P_σ, with $\sigma : \{1, \dots, n\} \to \{1, \dots, n\}$ being a bijection.
(2) $D_{\underline{r}}$ with each r_i being left invertible.
(3) $S_{i,c}$ with $i \in \{1, \dots, n\}, c = (c_1, \dots, c_n) \in K^n, c_i = 0$.
Let $p \in \mathbb{N}$. We say that $A \in M_{n,p}(K)$ is **reducible by Gaussian elimination** if there exists $S \in G_n(K)$ such that SA is of reduced row echelon form.

Lemma 6.7.10 If $A \in M_{n,p}(K)$ is such that SA is reducible by Gaussian elimination, for some $S \in G_n(K)$, then A is also reducible by Gaussian elimination.

Theorem 6.7.11 Suppose that K is a division ring. For any $(n, p) \in \mathbb{N}^2$, any matrix $A \in M_{n,p}(K)$ is reducible by Gaussian elimination.

Proof We reason by induction on p.
$p = 0$. A is already of reduced row echelon form.
Suppose that the statement is true for matrices of at most $p - 1$ columns. $(p \geq 1)$
We write A as $\begin{pmatrix} \lambda_1 & \\ \vdots & B \\ \lambda_n & \end{pmatrix}$ where $B \in M_{n,p-1}(K)$. If $\lambda_1 = \cdots = \lambda_n = 0$. By induction hypothesis, there exists $S \in G_n(K)$ such that SB is of reduced row

echelon form.

$$SA = \begin{pmatrix} 0 & \\ \vdots & SB \\ 0 & \end{pmatrix}$$

is of reduced row echelon form. If $(\lambda_1, \dots, \lambda_n) \neq (0, \dots, 0)$, by the lemma, we may suppose that $\lambda_1 \neq 0$ (By permuting rows). By multiplying A by $\mathrm{diag}(\lambda_1^{-1}, 1, \dots, 1)$ we may assume (by the lemma) that $\lambda_1 = 1$. So

$$A = \begin{pmatrix} 1 & \\ \lambda_2 & \\ \vdots & B \\ \lambda_n & \end{pmatrix}.$$

By multiplying $S_{1,(0,-\lambda_2,\dots,-\lambda_n)}$ and A, we may assume (by the lemma) that A is of the form

$$\begin{pmatrix} 1 & \mu_2 & \dots & \mu_n \\ 0 & & & \\ \vdots & & C & \\ 0 & & & \end{pmatrix}.$$

Applying the induction hypothesis to C. (For any $T \in G_{n-1}(K), T : K^{n-1} \to K^{n-1}, S : K^n \to K^n$, $S(t_1, \dots, t_n) = (t_1, T(t_2, \dots, t_n))$ belongs to $G_n(K)$.) We write C as $\begin{pmatrix} c_2 \\ \vdots \\ c_n \end{pmatrix}$ where $c_2, \dots, c_k$ belong to $k^{p-1} \backslash \{(0, \dots, 0)\}, c_{k+1} = \dots = c_n = (0, \dots, 0), j(c_2) < \dots < j(c_k)$. For any $i \in \{2, \dots, k\}$, we multiply $-\mu_{j(c_i)}$ times the i^{th} row of A to the first row. The result is a matrix of reduced row echelon form. □

6.8 Quotient Modules

Let K be a unitary ring.

Proposition 6.8.1 Let E be a left K-module, F be a left sub-K-module of E. The mapping

$$K \times E/F \longrightarrow E/F,$$

$$(a, [x]) \longmapsto [ax]$$

(Resp. right,$[xa]$) is well defined, and determines a structure of left K-module on

E/F. Moreover, the projection mapping

$$\pi : E \longrightarrow E/F$$

$$x \longmapsto [x]$$

is a homomorphism.

Proof Recall that F is a subgroup of $(E, +)$ such that

$$\forall a \in K, \forall y \in F, ay \in F,$$

$$[x] = \{y \in E \mid y - x \in F\}.$$

If $[x] = [y]$, then $y - x \in F$, so $ay - ax = a(y - x) \in F$, which means $[ay] = [ax]$.
(1) $[1x] = [x]$.
(2) $(ab)[x] = [(ab)x] = [a(bx)] = a[bx] = a(b[x])$.
(3)

$$(a + b)[x] = [(a + b)x] = [ax + bx] = [ax] + [bx] = a[x] + b[x].$$

$$a[x + y] = [a(x + y)] = [ax + ay] = [ax] + [ay] = a[x] + a[y].$$

Finally,

$$\pi(x + ay) = [x + ay] = [x] + [ay] = [x] + a[y] = \pi(x) + a\pi(y).$$

□

Theorem 6.8.2 Let $f : V \to W$ be a homomorphism of left K-modules.
(1) $\mathrm{Im}(f)$ is a sub-K-module of W.
(2) $\ker(f)$ is a sub-K-module of V.
(3) $\tilde{f} : V/\ker(f) \longrightarrow W, [x] \longmapsto f(x)$ is a homomorphism of left K-modules. Moreover, as a mapping, $\tilde{f}$ is injective and has $\mathrm{Im}(f)$ as its range. Hence it defines an isomorphism between $V/\ker(f)$ and $\mathrm{Im}(f)$.

Proof
(1) We have proved that $\mathrm{Im}(f)$ is a subgroup of W. If $y = f(x) \in \mathrm{Im}(f), \forall a \in K, ay = af(x) = f(ax) \in \mathrm{Im}(f)$. So $\mathrm{Im}(f)$ is a left sub-K-module of W.
(2) We have proved that $\ker(f)$ is a subgroup of V. If $x \in \ker(f), \forall a \in K, f(ax) = af(x) = a0 = 0$. So $\ker(f)$ is a left sub-K-module of V.

(3) We have proved that $\tilde{f}$ is an injective homomorphism of groups, with $\mathrm{Im}(\tilde{f}) = \mathrm{Im}(f)$. So $\tilde{f}$ defines an isomorphism of group $V/\ker(f) \longrightarrow \mathrm{Im}(f)$. Moreover, $\tilde{f}(a[x]) = \tilde{f}([ax]) = f(ax) = af(x) = a\tilde{f}([x])$. So $\tilde{f}$ is a homomorphism of left K-modules. □

6.9 Quotient Ring

Proposition 6.9.1 Let A be a unitary ring. Let $\sim$ be an equivalence relation on A that is compatible with the addition and with the multiplication. Then $A/\sim$ equipped with the quotient composition law of $+$ and $\cdot$ forms a unitary ring, and the projection mapping $\pi : A \longrightarrow A/\sim$ is a homomorphism of unitary ring.

Proof We have seen that $(A/\sim, +)$ forms an abelian group and $(A, \cdot)$ forms a monoid, and $\pi : A \longrightarrow A/\sim$ is a homomorphism of additive groups and multiplicative monoids. It remains to check the distributivity.

$$[a]([b]+[c]) = [a][b+c] = [a(b+c)] = [ab+ac] = [ab]+[ac] = [a][b]+[a][c].$$

$$([b]+[c])[a] = [(b+c)a] = [ba+ca] = [b][a]+[c][a].$$

□

Definition 6.9.2 $A/\sim$ is called the **quotient ring of** A .

Remark 6.9.3 There exists a subgroup I of A such that

$$a \sim b \Leftrightarrow b - a \in I.$$

$\forall x \in I, [x] = 0$, so for any $a \in A$,

$$[ax] = [a][x] = 0,\ [xa] = [x][a] = 0.$$

So I is a left sub-A-module of A and a right sub-A-module of A.

Definition 6.9.4 Let A be a unitary ring. If a subset I of A is a left sub-A-module of A and a right sub-A-module of A, then we call I a **ideal** of A. If I is an ideal of A, then the composition laws of A define by passing to quotient a structure of unitary ring on the quotient mapping A/I. So that A/I becomes a quotient ring of A.

Theorem 6.9.5 Let $f : A \to B$ be a homomorphism of unitary rings. Let $I = \ker(f)$.
(1) I is an ideal of A.
(2) $f(A)$ is a unitary subring of B.
(3) f induces $\tilde{f} : A/I \longrightarrow f(A)$ an isomorphism of unitary rings.

Proof
(1)

$$\forall a \in A, \forall x \in I, f(ax) = f(a)f(x) = f(a)0 = 0 = 0f(a) = f(x)f(a) = f(xa).$$

So $\{ax, xa\} \subseteq I$. Since I is a subgroup of A, it is actually an ideal.
(2) Since f is a homomorphism of groups $(A, +) \longrightarrow (B, +)$ and a homomorphism of monoids $(A, \cdot) \longrightarrow (B, \cdot)$, $f(A)$ is a subgroup of $(B, +)$ and a submonoid of $(B, \cdot)$.
(3) $\tilde{f}$ is a homomorphism of unitary rings. $\tilde{f}([x]) := f(x)$. In the same time $\tilde{f} : A/I \longrightarrow f(A)$ is a bijection. So it is a homomorphism of rings. □

Example 6.9.6 Consider $\mathbb{Z}$. Let I be an ideal of $\mathbb{Z}$. If $I \neq \{0\}$, then $I \cap \mathbb{N}_{\geq 1} \neq \varnothing$. Let $d \in I \cap \mathbb{N}_{\geq 1}$ be the least element. For any $n \in I$, we can write n as

$$n = dm + r, \text{ where } m \in \mathbb{Z}, r \in \{0, \ldots, d-1\}.$$

So $r = n - dm \in I$, which means $r = 0$. Therefore, $I = d\mathbb{Z}$.

Definition 6.9.7 Let A be a communitative unitary ring. If an ideal of A is of the form

$$Ax : \{ax \mid a \in A\} \text{ with } x \in A.$$

We say that it is a **principal ideal**. If all ideals of A are principal, we say that A is a **principal ideal ring**.

Example 6.9.8 $\mathbb{Z}$ is a principal ideal ring.

Remark 6.9.9 If A is a unitary ring, $\mathbb{Z} \longrightarrow A$, $n \longmapsto n1_A$ is the unique homomorphism of unitary rings. $\ker(\mathbb{Z} \longrightarrow A)$ is an ideal of $\mathbb{Z}$. It is of the form

$d\mathbb{Z}, d \in \mathbb{N}$. This natural number d is called the **characteristic** of A, denoted as $\mathrm{char}(A)$.

Definition 6.9.10 Let A be a communitative unitary ring. Let $a \in A$. If $\exists b \in A\backslash\{0\}$ such that $ab = 0$, we say that a is a zero divisor. If $0 \in A$ is the ONLY zero divisor, we say that A is an **(integral) domain**.

A is an integral domain if and only if $0 \neq 1$, and $\forall (a,b) \in (A\backslash\{0\})^2,\ ab \neq 0$.

Example 6.9.11
$\mathbb{Z}$ is an integral domain.
All field are integral domains.
$\mathbb{Z}/6\mathbb{Z}$ is NOT a integral domain.$[2][3] = [6] = [0]$.

Proposition 6.9.12 All unitary subrings of an integral domain are integral domains.

Proposition 6.9.13 Let A be a unitary ring. E be a left A-module and I be an ideal of A. Suppose that

$$\forall (a,x) \in I \times E,\ ax = 0.\ (I \text{ annihilates } E)$$

Then the mapping

$$(A/I) \times E \longrightarrow E,$$
$$([a],x) \longmapsto ax$$

is well defined and defines a left A-module structure on E.

Proof If $[a] = [b]$, then $b - a \in I$. So $\forall x \in E, (b-a)x = bx = ax = 0$. Hence $ax = bx$. $\forall (a,b) \in A \times A, \forall (x,y) \in E \times E$:
(1) $[1]x = 1x = x$. $([a][b])\,x = [ab]x = (ab)x = a(bx) = [a](bx) = [a]([b]x)$.
(2) $([a]+[b])\,x = [a+b]x = (a+b)x = ax+bx = [a]x+[b]x$. $[a](x+y) = a(x+y) = ax+ay = [a]x+[a]y$. □

6.10 Free Modules

We fix a unitary ring K.

Definition 6.10.1 Let V be a left K-module. For any family $\underline{x} := (x_i)_{i\in I} \in V^I$, we denote by

$$\varphi_{\underline{x}} : K^{\oplus I} \longrightarrow V$$

the homomorphism sending $(a_i)_{i\in I}$ to $\sum_{i\in I} a_i x_i$.
(1) $\mathrm{Im}\,(\varphi_{\underline{x}})$ is a left K-submodule of V, called the **left sub-K-module generated by** $\underline{x}$, denote as $\mathrm{Span}_K\left((x_i)_{i\in I}\right)$. If φ_x is surjective, we say that $(x_i)_{i\in I}$ is a system of generators of V. $(\forall y \in V, \exists (a_i)_{i\in I} \in K^{\oplus I}, y = \sum_{i\in I} a_i x_i)$ Elements of $\mathrm{Span}_K\left((x_i)_{i\in I}\right)$ are called **K-linear combinations** of $(x_i)_{i\in I}$.
(2) If φ_x is injective, we say that $(x_i)_{i\in I}$ is **K-linearly independent**. $(\forall (a_i)_{i\in I} \in K^{\oplus I}, \sum_{i\in I} a_i x_i = 0 \to a_i = 0, \forall i \in I)$
(3) If $\varphi_{\underline{x}}$ is an isomorphism, we say $(x_i)_{i\in I}$ is a **basis** of V. If V has at least a basis, we say that V is a **free left K-module**. If V has a system of generators $(x_i)_{i\in I}$ such that I is finite, we say that V is **finitely generated**, or is **finite types**.

Example 6.10.2 $K^{\oplus I}$ is a free left K-module.

Remark 6.10.3 Any left K-module is isomorphic to a free quotient module of a free left K-module.

Theorem 6.10.4 Let K be a division ring and V be a left K-module of finite type. Let $(x_i)_{i=1}^n$ be a system of generators of V. There exists $I \subseteq \{1, \ldots, n\}$ such that $(x_i)_{i\in I}$ forms a basis of V.

Proof By induction on n.
Case $n = 0$, $V = \{0\}.(x_i)_{i\notin\varnothing}$ is a basis of V. Suppose that $n \geq 1$. If $(x_i)_{i=1}^n$ is K-linearly independent, it is already a basis. Otherwise there exists $0 \neq (b_1, \ldots, b_n) \in K^n$ such that $b_1x_1 + \cdots + b_nx_n = 0$. By permuting $x_1, \ldots, x_n$, we may assume that $b_n \neq 0$. $x_n = -b_n^{-1}(b_1x_1 + \cdots + b_{n-1}x_{n-1})$. For any $y \in V$, there exists $(a_1, \ldots, a_n) \in K^n$, such that

$$y = \sum_{i=1}^{n} a_i x_i = \sum_{i=1}^{n-1} a_i x_i - a_n b_n^{-1}\left(b_1 x_1 + \cdots + b_{n-1} x_{n-1}\right).$$

□

Theorem 6.10.5 Let K be a unitary ring. V be a left K-module and W bw a left sub-K-module of V. Let $(x_i)_{i=1}^n \in W^n$ and $(\alpha_j)_{j=1}^l \in (V/W)^l$, with $(n, l) \in \mathbb{N}^2$.

For any $j \in \{1, \ldots, l\}$. Let x_{n+j} be an element of the equivalence class of α_j. $([x_{n+j}] = \alpha_j)$
(1) If $(x_i)_{i=1}^n$ and $(\alpha_j)_{j=1}^l$ are K-linearly independent, then $(x_i)_{i=1}^{n+l}$ is K-linearly independent.
(2) If $(x_i)_{i=1}^n$ and $(\alpha_j)_{j=1}^l$ are system of generators, then $(x_i)_{i=1}^{n+l}$ is a system of generators.

Proof
(1) Let $(a_i)_{i=1}^l \in K^{n+l}$ such that

$$\sum_{i=1}^{n+l} a_i x_i = 0.$$

Taking the equivalence class of both sides in V/W, we get $\sum\limits_{j=1}^{l} a_{n+j}\alpha_j = [0]$. So $a_{n+1} = \cdots = a_{n+l} = 0$. Hence $a_1x_1 + \cdots + a_nx_n = 0$. So $a_1 = \cdots = a_n = 0$.
(2)Let $y \in V$. There exists $(c_{n+1}, \ldots, c_{n+l}) \in K^l$, such that

$$[y] = c_{n+1}\alpha_1 + \cdots + c_{n+l}\alpha_l = [c_{n+1}x_{n+1} + \cdots + c_{n+l}x_{n+l}].$$

So, $y-(c_{n+1}x_{n+1} + \cdots + c_{n+l}x_{n+l}) \in W$. Hence, there exists $(c_1, \ldots, c_n) \in K^n$,

$$y - (c_{n+1}x_{n+1} + \cdots + c_{n+l}x_{n+l}) = c_1x_1 + \cdots + c_nx_n.$$

So $y = \sum\limits_{i=1}^{n+l} c_i x_i$. □

Proposition 6.10.6
(1) If A is injective and $(x_i)_{i\in I}$ is a K-linearly independent, then $(y_j)_{j\in I}$ is K-linearly independent.
(2) If A is surjective, then $(x_i)_{i\in I}, (y_j)_{j\in J}$ generate the same left sub-K-module of V.

$$\mathrm{Im}(\varphi_y) = \mathrm{Im}(\varphi_{\underline{x}} \circ A) = \mathrm{Im}(\varphi_{\underline{x}}).$$

In particular, if $f(x_i)_{i\in I}$ is a system of generators, and A is surjective, then $(y_j)_{j\in J}$ is a system of generators.
(3) If $(x_i)_{i\in I}$ is a basis and A is a bijection, then $(y_j)_{j\in J}$ is a basis.

Application Let $n \in \mathbb{N}$, $(x_1, \ldots, x_n) \in V^n$. Let $(y_1, \ldots, y_n) \in V^n$ such that

$$\begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = S \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \text{ with } S \text{ invertible.}$$

$(x_i)_{i \in I}^n$ is K-linearly independent if and only if $(y_j)_{j \in J}^n$ is K-linearly independent.
$(x_i)_{i \in I}^n$ is a system of generators if and only if $(y_j)_{j \in J}^n$ is a system of generators.
$(x_i)_{i \in I}^n$ is a basis if and only if $(y_j)_{j \in J}^n$ is a basis.

Theorem 6.10.7 Let $(n, p) \in \mathbb{N}^2$ and $A \in M_{n,p}(K)$. We write A into the form

$$A = \begin{pmatrix} \underline{a}^{(1)} \\ \ldots \\ \underline{a}^{(n)} \end{pmatrix} \text{ where } \underline{a}^{(i)} = (a_{i,1}, \ldots, a_{i,p}) \in K^p.$$

Assume that A is of reduced row echelon form.
(1) $\left(\underline{a}^{(i)}\right)_{i=1}^n$ is K-linearly independent if and only if $\forall i \in \{1, \ldots, n\}, a^{(i)} \neq (0, \ldots, 0)$.
(2) $\left(\underline{a}^{(i)}\right)_{i=1}^n$ is a system of generators if and only if there are exactly p non-zero elements among $\underline{a}^{(1)}, \ldots, \underline{a}^{(n)}$.

Proof
(1) It suffice to check, if $\forall i \in \{1, 2, \ldots, n\}, \underline{a}^{(i)} \neq (0, \ldots, 0)$, then $\left(\underline{a}^{(i)}\right)_{i=1}^n$ is K-linearly independent. Since A is of reduced row echelon form

$$1 \leq j(\underline{a}^{(1)}) < j(\underline{a}^{(2)}) < \cdots < j(\underline{a}^{(n)}) \leq p.$$

Suppose that $(\lambda_1, \ldots, \lambda_n) \in K^n$ such that

$$\lambda_1 \underline{a}^{(1)} + \cdots + \lambda_n \underline{a}^{(n)} = (0, \ldots, 0).$$

Note that the coordinate of index $j(\underline{a}^{(i)})$ of $\lambda_1 \underline{a}^{(1)} + \cdots + \lambda_n \underline{a}^{(n)}$ is λ_i, so

$$\lambda_1 = \cdots = \lambda_n = 0.$$

(2) "$\Leftarrow$": Suppose that $\underline{a}^{(i)} \neq (0, \ldots, 0)$ for $i \in \{1, \ldots, p\}$. Since $1 \leq j(\underline{a}^{(1)}) < \cdots < j(\underline{a}^{(p)}) \leq p$, one has $j(\underline{a}^{(i)}) = i, \forall i \in \{1, \ldots, p\}$. Hence

$$\lambda_1 \underline{a}^{(1)} + \cdots + \lambda_p \underline{a}^{(p)} = (\lambda_1, \ldots, \lambda_p).$$

"⇒": suppose that $(a_i)_{i=1}^n$ is a system of generators. There could not be more than p non-zero elements among $\underline{a}^{(1)}, \dots, \underline{a}^{(n)}$. If $\underline{a}^{(1)}, \dots, \underline{a}^{(k)}$ are non-zero and

$$\underline{a}^{(k+1)} = \cdots = \underline{a}^{(n)} = 0,$$

let $(b_1, \dots, b_p) \in K^p \backslash \{(0, \dots, 0)\}$, $\forall i \in \{1, \dots, k\}, b_{j(\underline{a}^{(1)})} = 0$. If $(b_1, \dots, b_p)$ is a linear combination of $\underline{a}^{(1)}, \dots, \underline{a}^{(n)}$, there exists $(\lambda_1, \dots, \lambda_k)$ such that

$$\lambda_1 \underline{a}^{(1)} + \cdots + \lambda_k \underline{a}^{(k)} = (b_1, \dots, b_p).$$

So $\lambda_1 = \cdots = \lambda_k = 0$. □

Definition 6.10.8 Let K be a division ring and V is a left K-module of finite type. We denote by $\mathrm{rk}_K(V)$ or $\mathrm{rk}(V)$ the least cardinality of the bases V, called the **rank** of V. If K is a field, then $\mathrm{rk}(V)$ is also denoted as $\dim(V)$, called the **dimension** of V. If $f : W \longrightarrow V$ is a homomorphism of left K-modules, the rank of f is defined as the rank of $\mathrm{Im}(f)$, denoted as $\mathrm{rk}(f)$.

Theorem 6.10.9 (rank-nullity theorem) Let K be a division ring and V be a left K-module of finite type, and W be a left sub-K-module of V.
(1) W and V/W are of finite type, and $\mathrm{rk}(W) + \mathrm{rk}(V/W) = \mathrm{rk}(V)$.
(2) Any basis of V has $\mathrm{rk}(V)$ as its cardinality.

Proof
(1) Let $(x_i)_{i=1}^n$ be a basis of V. Then $([x_i])_{i=1}^n$ also form a system opf generators of V/W. By theorem 6.10.4, one can extract a subset $I \subseteq \{1, 2 \dots, n\}$ such that $([x_i]_{i \in I})$ forms a basis of V/W. By permuting the elements $x_1, x_2, \dots, x_n$, we may assume, without loss of generality, that $I = \{1, 2, \dots, l\}$, $l \le n$. For any $j \in \{l+1, \dots, n\}$ there exists $(b_{j,1}, \dots, b_{j,l})$ such that

$$[x_j] = \sum_{i=1}^{l} b_{j,i} [x_i].$$

$$y_j := x_j - \sum_{i=1}^{l} b_{j,i} x_i.$$

For any $x \in W$, there exists $(a_i)_{i=1}^n \in K^n$ such that

$$x = \sum_{i=1}^{l} a_i x_i + \sum_{j=l+1}^{n} a_j \left(y_j + \sum_{i=1}^{l} b_{j,i} x_i \right) = \sum_{i=1}^{l} \left(a_i + \sum_{j=l+1}^{n} a_j b_{j,i} \right) x_i + \sum_{j=l+1}^{n} a_j y_j.$$

Taking the equivalence class of $x \in V/W$ (i.e.[0]) we obtain.

$$\forall i \in \{1, \dots, l\},\ a_i + \sum_{j=l+1}^{n} a_j b_{i,j} = 0.$$

Hence,

$$x = \sum_{j=l+1}^{n} a_j y_j.$$

Therefore, W is of finite type, and $\mathrm{rk}(W) + \mathrm{rk}(V/W) \leq \mathrm{rk}(V)$. Moreover, by theorem 6.10.5,

$$\mathrm{rk}(V) \leq \mathrm{rk}(W) + \mathrm{rk}(V/W).$$

Hence,

$$\mathrm{rk}(W) + \mathrm{rk}(V/W) = \mathrm{rk}(V).$$

(2) We reason by induction on $\mathrm{rk}(V)$. If $\mathrm{rk}(V) = 0$, then $\{\varnothing\}$ is the only basis. If $\mathrm{rk}(V) = 1$, then V is of the form Ke, where e is a non-zero element of V. Suppose $\mathrm{rk}(V) = n \geq 1$, and the statement has been proven for modules of $\mathrm{rk} < n$. Let $(e_i)_{i=1}^m$ be a basis of V. Let $W = K \cdot e_1$. Then, $([e_i])_{i=2}^m$ forms a system of generators of V/W. Moreover, $(a_i)_{i=2}^m \in K^{m-1}$ such that

$$\sum_{i=2}^{m} a_i [e_i] = 0,$$

then,

$$\sum_{i=2}^{m} a_i e_i \in W,$$

and hence, there exists $a_1 \in K$,

$$\sum_{i=1}^{m} a_i e_i = 0.$$

We conduct that, in particular

$$a_2 = \cdots = a_n = 0.$$

Hence $([e_i])_{i=2}^m$ is a basis of V/W, $\mathrm{rk}(V/W) = n-1$, so $n-1 = m-1 \Leftrightarrow n = m$.
□

6.11 Algebra

In this section, we fix a communicative unitary ring K.

Definition 6.11.1 Let K be a communicative unitary ring. If A is a K-module equipped with a composition law

$$A \times A \longrightarrow A,$$

$$(a, b) \longmapsto ab.$$

such that $(A, +, \cdot)$ forms a unitary ring, such that

$$\forall \lambda \in K, \forall (a, b) \in A \times A,\ \lambda\,(ab) = (\lambda a)\,b = a\,(\lambda b)\,.$$

Then we say that A is a **K-Algebra**.

Remark 6.11.2

$$K \longrightarrow A,$$

$$\lambda \longmapsto \lambda 1_A.$$

is a homomorphism of unitary rings.
(1) $(\lambda + \mu)1_A = \lambda 1_A + \mu 1_A$.
(2) $(\lambda 1_A)\,(\mu 1_A) = \lambda\,(1_A(\mu 1_A)) = \lambda\,(\mu(1_A 1_A)) = \lambda(\mu 1_A) = (\lambda\mu)1_A$.
(3) $1_K 1_A = 1_A$.

Remark 6.11.3 Suppose that A is a unitary ring and $f : K \longrightarrow A$ be a homomorphism of unitary rings such that $\forall \lambda \in K,\ \forall a \in A\ af(\lambda) = f(\lambda)a$. Then

$$K \times A \longrightarrow A,$$

$$(\lambda, a) \longmapsto f(\lambda)a$$

defines a structure of K-modules on A.

$$f(\lambda\mu)a = f(\lambda)f(\mu)a = f(\lambda)\,(f(\mu)a)\,,$$

$$f(1_K)a = 1_A a = a,$$

$$f(\lambda + \mu)a = (f(\lambda) + f(\mu))\,a = f(\lambda)a + f(\mu)a,$$

$$f(\lambda)(a + b) = f(\lambda)a + f(\lambda)b.$$

Moreover,

$$f(\lambda)(ab) = (f(\lambda)a)\,b = a\,(f(\lambda)b)\,.$$

Therefore,A equipped with a structure of K-algebra.

Example 6.11.4 (1) $\{0\}$, (2) K.

Example 6.11.5 Let $(S, \cdot)$ be a monoid. We denote by $k[\![S]\!]$ the K-module K^S. If $(a_s)_{s\in S}$ belongs to K^S, while coordinating $(a_s)_{s\in S}$ as an element of $K[\![S]\!]$, we write it formally as

$$\sum_{s\in S} a_s s.$$

Assume that, for any $s \in S$, the preimage of s by the mapping

$$S \times S \longrightarrow S,$$

$$(\alpha, \beta) \longmapsto \alpha\beta$$

is finite.

$$(\{(\alpha, \beta) \in S \times S \mid \alpha\beta = s\} \text{ is finite.})$$

For example,

$$\mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N},$$

$$(m, n) \longmapsto m + n.$$

$$\forall k \in \mathbb{N}, \{(m, n) \in \mathbb{N} \times \mathbb{N} \mid m + n = k\} \text{ is finite.}$$

We define a composition law on $K[\![S]\!]$ by

$$K[\![S]\!] \times K[\![S]\!] \longrightarrow K[\![S]\!]$$

$$\left(\sum_{s\in S} a_s s, \sum_{s\in S} b_s s\right) \longmapsto \sum_{s\in S} \left(\sum_{(u,v)\in S^2, uv=s} a_u b_v\right) s.$$

We write $(\mathbb{N}, +)$ formally as

$$(\{T^n \mid n \in \mathbb{N}\}, \cdot)$$

such that $T^n \cdot T^m := T^{n+m}$. In this particular case, we write $K[\![N]\!]$ as $k[\![T]\!]$. The element of $K[\![T]\!]$ is of the form

$$\sum_{n\in\mathbb{N}} a_n T^n.$$

It is called a **formal power series (of variable T) with coefficients in K**.

Proposition 6.11.6 $K[\![S]\!]$ is a K-algebra.

Proof

$$\begin{aligned}
&\sum_{s\in S} a_s s \left(\left(\sum_{s\in S} b_s s\right)\left(\sum_{s\in S} c_s s\right)\right)\\
=&\left(\sum_{s\in S} a_s s\right)\left(\sum_{s\in S}\left(\sum_{vw=s} b_v c_w\right) s\right)\\
=&\sum_{s\in S}\left(\sum_{uvw=s} a_u b_v c_w\right) s\\
=&\left(\sum_{s\in S} a_s s\right)\left(\sum_{s\in S} b_s s\right)\left(\sum_{s\in S} c_s s\right)
\end{aligned}$$

□

Definition 6.11.7 Let A be a K-algebra. If B is a subset of A which is a sub-K-module and a unitary subring of A, we say that B is a **sub-K-algebra** of A.

Example 6.11.8 Let S be a monoid. We write $K^{\oplus S}$ as $k[S]$ and define

$$K[S]\times K[S]\longrightarrow K[S],$$

$$\left(\left(\sum_{s\in S} a_s s\right),\left(\sum_{s\in S} b_s s\right)\right)\longmapsto\sum_{s\in S}\left(\sum_{uv=s} a_u b_v\right) s.$$

Then $K[S]$ forms a K-algebra. If $K[\![S]\!]$ is well defined, then $K[S]$ ia a sub-K-algebra of $K[\![S]\!]$.

Appendix A

Axioms

A.1 Axiom of Foundation (Regularity)

Axiom 4 (Axiom of foundation)

$$\forall A(A \neq \varnothing \to \exists x \in A(x \cap A = \varnothing)).$$

Regularity means that :If A is a non-empty set, then there exists at least one element x of A satisfies: Either x is not a set or does not intersect with A.

Based on axiom of foundation, we have the following propositions.

Proposition A.1.1 There does not exists a set S, such that $S \in S$.

Proof If $S = \varnothing, \varnothing \notin \varnothing$; If $S \neq \varnothing$, consider the set $\{S\}$, it has a single element S. Since $S \in S, S \in (S \cap \{S\}) \neq \varnothing$. □

Proposition A.1.2 Let $(X, <)$ be a strictly ordered set, $(A_i)_{i \in X}$ be a family of sets.If $\forall (i, j) \in X^2, i < j \Rightarrow (\exists k \in X, i < k \leq j \wedge A_i \in A_k)$, then $(X, \leq)$ is a well ordered set.

Proof Let I be a subset of X, $S := \{A_i | i \in I\}$.If $(i, j) \in S^2, i < j$, then $\exists A_k \in S, A_i \in A_k$.Since $A_i \in S$ at the same time, $A_k \cap S \subseteq \{A_i\} \neq \varnothing$.By axiom of regularity, $\exists A_i \in S, A_i \cap S = \varnothing$.Hence, $\forall A_j \in S, A_j \notin A_i$.Thus, $j \not> i$, which leads to $\forall j \in I, j > i$.i is the least element of I. □

Proposition A.1.3 Let $(X, <)$ be a strictly ordered set, $(A_i)_{i \in X}$ be a family of sets.If $\forall (i,j) \in X^2, i < j \Rightarrow (\exists k \in X, A_i \in A_k)$, then $\forall (i,j) \in X^2, i < j \Rightarrow A_j \notin A_i$.

Proof If $\exists i < j \in X, A_j \in A_i$ and $i < k \leq j, A_i \in A_k$, we consider the set $S = \{A_k | i \leq k \leq j\}, \forall A_k \in S, \exists A_m \in S, A_k \in A_m$.Therefore $A_k \cap S \neq \varnothing$.That contradicts to the axiom. □

Corollary A.1.4 Let X, Y be two sets, if $X \in Y$, then $Y \notin X$.

Appendix B

Inequalities

Definition B.0.1 (Convex functions on intervals) Let $X \subseteq \mathbb{R}$ bbe an interval. A function $f : X \to \mathbb{R}$ is called **convex** for all $x_1, x_2 \in X, t \in [0, 1]$

$$f(tx_1 + (1-t)x_2) \leq tf(x_1) + (1-t)f(x_2)$$

A function $f : X \to \mathbb{R}$ is called **concave** for all $x_1, x_2 \in X, t \in [0, 1]$

$$f(tx_1 + (1-t)x_2) \geq tf(x_1) + (1-t)f(x_2)$$

Theorem B.0.2 (Jensen's Inequality) Let f be a convex function $0 \leq \alpha_i \leq 1$ for $i = 1, 2, \ldots, n$, such that

$$\sum_{i=1}^{n} \alpha_1 = 1.\text{show that } \forall x_i \in X$$

$$f\left(\sum_{i=1}^{n} a_i x_i\right) \leq \sum_{i=1}^{n} \alpha_i f(x_i)$$

Equality holds if and only if $x_1 = x_2 = \cdots = x_n$ or f is linear on some interval containing $x_1, x_2, \ldots, x_n$.

Remark B.0.3 Consider $f(x) = x^2$, we obtain Cauchy-Schwartz inequality, $f(x) = \ln(x)$, we obtain AM-GM-HM inequality.

Theorem B.0.4 (Young's Inequality)

Fix $pq > 1$ such that $\frac{1}{p} + \frac{1}{q} = 1$, then

$$xy \le \frac{1}{p}x^p + \frac{1}{q}y^q$$

Theorem B.0.5 (Hölder's Inequality)
Fix $pq > 1$ such that $\frac{1}{p} + \frac{1}{q} = 1 . x_1, x_2, \ldots, x_n; y_1, y_2, \ldots, y_n \ge 0$, then

$$\sum_{i=1}^{n} x_i y_i \le \left(\sum_{i=1}^{n} x_i^p \right)^{\frac{1}{p}} \cdot \left(\sum_{j=1}^{n} y_j^q \right)^{\frac{1}{q}}$$

In particular, when $p = q = 2$, this is Cauchy-Schwartz inequality.