Linear Algebra Lecture Notes

Amane Fujimiya

November 2023

Chapter 1

Set, Relations and Functions

I Set

A set is a collections of objects, either algebraic structures, rigorous mathematics, or plain simple objects such as a collection of collected apples during harvest seasons.

A set X will have its collection of objects inside. If an object x is inside X, or x in X, we write it as

$$x \in X$$

with the notation $\in$ as the representation.

I.I Describing a set

To describe a set, we use some way of listing the set:

I.I.I 1. Listing elements of a set

Example includes:

$$\mathbb{N} = \{0, 1, 2, \cdots\}$$

of natural numbers set $\mathbb{N}$. For integer $\mathbb{Z}$, then

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \cdots\}$$

and for rational number:

$$\mathbb{Q} = \left\{ r = \frac{m}{n} : m, n \in \mathbb{Z}, n \neq 0 \right\}$$

I.I.II 2. Identification of set's properties

If a set E includes elements with some types of properties, we write

$$E = \{x : T(x)\}$$

For example, the set P of all even numbers is

$$E = \{x : x = 2k, k \in \mathbb{Z}\}$$

This is explained as for all even number, there is a properties that $x = 2k$ for all $k \in \mathbb{Z}$, that is, x must have an even factor of 2.

II Subset. Empty set

For any set X, given another set A. A is the subset of X if $x \in A$ then $x \in X$, denoted

$$A \subseteq X$$

or

$$X \supseteq A$$

The first notation is the subset notation, the second one establish a reverse relation, called superset, that is X is a superset of A. If $A \subseteq X$, and we have $y \in X$ but $y \notin A$, then A is a proper subset of X, denoted

$$A \subset X$$

An empty set is a set that contains no elements. It is denoted as $\varnothing$. Conventionally, $\varnothing \in X$ for all X. Two sets A and B is equal if $A \subseteq B$ and $B \subseteq A$, then $A = B$.

III Logic notations

A mathematical statements can be either right or wrong, no more. To simplify and generalize the wording (and to shorten the sentence), we use those notations:

1. $S \Rightarrow T$ means S is right then T is right.
2. $S \iff T$ means that S is right then T is right and the reverse is true.
3. $\forall x \in X : S$ means for all x in X there is a statement S.
4. $\exists x \in X : S'(\exists! \, x \in X : S)$ means that there exists one and only $x \in X$ so that S is right.

IV Logics operation

Given two sets A and B, some operations on them are

Definition IV..1. *Union of Sets.*
Union of A and B is

$$A \cup B = \{x : x \in A \, or \, x \in B\}$$

Definition IV..2. *Intersection of Sets*
Intersection of A and B is

$$A \cap B = \{x : x \in A \, and \, x \in B\}$$

Definition IV..3. *Difference between sets*
The difference between A and B is

$$A \setminus B = \{x : x \in A \, and \, x \notin B\}$$

If $A \cap B = \varnothing$, then A and B are disjoint. If $A \subseteq X$ then the notation $C_X A = X \setminus A$ is the complement of A in X.

The union of a family of sets is denoted as

$$\bigcup_{i \in I} A_i = \{x : \exists i \in I, x \in A_i\}$$

The intersection of a family of sets is denoted as

$$\bigcap_{i \in I} A_i = \{x : x \in A_i, \forall i \in I\}$$

IV.I Properties of set operation

Sets operations above have some interesting and elementary property:

1. Commutativity:

$$A \cup B = B \cup A \tag{1.1}$$

$$\tag{1.2}$$

$$A \cap B = B \cap A \tag{1.3}$$

2. Associativity:

$$\tag{1.4}$$

$$(A \cup B) \cup C = A \cup (B \cup C) \tag{1.5}$$

$$(A \cap B) \cap C = A \cap (B \cap C) \tag{1.6}$$

3. Distributivity:

$$\tag{1.7}$$

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \tag{1.8}$$

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \tag{1.9}$$

IV.II De Morgan Theorem

The De Morgan Theorem for Sets is given as

$$X \setminus \left(\bigcup_{i \in I} A_i \right) = \bigcap_{i \in I} (X \setminus A)$$

and

$$X \setminus \left(\bigcap_{i \in I} A_i \right) = \bigcup_{i \in I} (X \setminus A_i)$$

V Set Relations

V.I Descartes Product of Sets

Given two sets X and Y, then the Cartesian product (or Descartes product) $X \times Y$ is defined as

$$A \times B = \{(a, b) \mid a \in A \text{ and } b \in B\}$$

Generally, for a set of sets S_i with $i \in I$

$$S_i = \{S_1, S_2, S_3, \cdots\}$$

The Cartesian product of elements in S_i is

$$\prod_{i=1}^{n} S_i = \{x = (x_1, x_2, \cdots, x_n) : x_i \in S_i, i = 1, 2, \cdots, n\}$$

If $S_1 = S_2 = \cdots S_n$ then we have $S_1 \times S_2 \times \cdots \times S_n = S^n$. This is called n-nary Cartesian/Descartes product of S_i.

V.II Formal definition of Relations

We here will state the definition of relations between sets

Definition V.II.1. *Given a set X, then each $S \subset X \times X$ is an relation on X*

If the ordered pair $(x, y) \in S$ then we say that x is in relation S with y, denoted xSy. Then we have:

Theorem V.II.1. *Suppose S is an relation on X, then*

1. *S is called reflexive relation if $xSx, \forall x \in X$.*
2. *S is called symmetric if xSy then ySx.*
3. *S is called transitive if xSy and ySz then xSz.*
4. *S is called anti-symmetric if xSy and ySx then $x = y$.*

Relations have different types. One of the well-known and widely used relation is the equivalent relation

Definition V.II.2. *An equivalent relation is a relation that has reflective, symmetric and transitive properties*

Notation for equivalent relation is $\sim$, then $xSy \to x \sim y$ for equivalent relation.
For each x, we set

$$\bar{x} = \{x' \in X : x' \sim x\}$$

then $\bar{x}$ is called an equivalent class with x as it main. By reflective properties, we see that

$$x \in \bar{x}$$

then

$$\bar{x} \neq \varnothing, \bigcup_{x \in X} \bar{x} = X$$

The family of subsets $\{A_i\}_{i \in I}$ of X is called a **class separation** of X if $A_i \neq \varnothing$ for $\forall i \in I$. A property of this is that

$$A_i \cap A_j = \varnothing \ if \ \left(i \neq j, \bigcup_{i \in I} = X \right)$$

The set of all equivalence classes of X is denoted $X \backslash \sim$. Notationally,

$$X \backslash \sim = \{\bar{x} | x \in X\}$$

Next, we have the ordering relation.

Definition V.II.3. *Ordering relation*

An ordering relation on a set is a relation that is reflexive, transitive, and anti-symmetric. An ordering relation is often denoted $\leq$, and has these following properties:

1. $x \leq x, \forall x \in X$
2. $x \leq y, y \leq z \Rightarrow x \leq z$
3. $x \leq y, y \leq x \Rightarrow x = y$

If $x \leq y$ then we say that x stands before y, or the reverse. If $x \leq y$ and $x \neq y$ then we say that x is totally behind y and we write $x < y$.

A set X that has an ordering relation is called an ordered set and denoted $(X, \leq)$. If for all $x, y \in X$ we always have $x \leq y$ or $y \leq x$ then the set is a totally ordered set (totality of a set).

VI Functions and Mappings

We begin with the definition of functions

Definition VI..1. *A map f from X to Y, denoted $f : X \longrightarrow Y$ or $X \longrightarrow^f Y$ is a rule that bind each $x \in X$ with exactly one $y = f(x) \in Y$.*

VI.I Composition of mapping

Given two maps $f : X \longrightarrow Y$ and $g : Y \longrightarrow Z$, the product or composition of two maps f and g is $g \circ f : X \longrightarrow Z$ and is defined as

$$g \circ f = g(f(x)), \forall x \in X$$

The image of $A \subseteq X$ through the map f is the set

$$f(A) = \{f(x) : x \in A\}$$

Next, we also have the set denoted as $Imf = f(X)$, then Imf is called image of mapping f.

The inverse image of $D \subseteq Y$ is the set

$$f^{-1}(D) = \{x \in X : f(x) \in D\}$$

VI.II Types of Mapping

For a mapping, there are three types of mapping, which is injective, bijective and surjective, as well as some special cases. We will then go to define such mapping style.

VI.II.I Injection mapping

A map f is injective if

$$\forall x, x' \in X, x \neq x' \Rightarrow f(x) \neq f(x')$$

This can be written also as

$$\forall x, x' \in X, f(x) = f(x') \Rightarrow x = x'$$

VI.II.II Surjection mapping

A map f is surjective if

$$Imf = Y$$

In more detail, that is

$$\forall y \in Y, \exists x \in X \text{ such that } y = f(x).$$

VI.II.III Bijection mapping

A map f is bijective if f is both surjective and injective. Comprehensively,

$$\forall y \in Y, \exists! \, x \in X \text{ such that } y = f(x)$$

One note is that the composition of injective mappings is an injective mapping, so do surjective, thus we also have bijection mappings to have bijective compositions.

VI.II.IV Reverse Mapping and Identity

Suppose $f : X \longrightarrow Y$ is a bijective mapping from X to Y. Then for each $y \in Y$, there exists one and only $x \in X$ so that $f(x) = y$. Then we have a mapping $g : Y \longrightarrow X$ defined as

$$\forall y \in Y, x \in X : g(y) = x, f(x) = y \Longrightarrow g \circ f = i_X, f \circ g = i_Y$$

Then, the mapping g is called a reverse mapping of f and denoted f^{-1}

Here, we have the mapping called identity mapping. The **identity function** on any nonempty set A maps any element back to itself:

$$I_A = i_A : A \longrightarrow A, I_A(x) = x$$

VI.III Equivalence functions (same 'force' relation)

Definition VI.III.1. *Equivalent functions*

Two sets X and Y is called equivalent, that is $X \sim Y$ if there exists a bijective relation $f : X \longrightarrow Y$.

We will inspect some properties of equivalence function, by defining a mapping E_n, that is

$$f : E_n \to A, f(k) = a_k \forall k \in K = \{1, 2, \cdots, n\}$$

Chapter 2

Group, Ring, Field

I Binary operation

I.I Definition

Definition I.I.1. *Binary Relations Suppose X is a set. then a mapping $\theta : X \times X \longrightarrow X$ is a binary operation on X.*

From the definition, then $\theta(x, y)$ is the result of x and y, or the product of those two.

I.II Binary properties

Considering a binary operation θ on X, then θ is called:

Associative if

$$(x \cdot y) \cdot z = x \cdot (y \cdot z), \forall x, y, z \in X$$

Symmetric if

$$x \cdot y = y \cdot x, \forall x, y \in X$$

There exists an identity element e that

$$\forall e, x \in X, e \cdot x = x \cdot e = x$$

From the third conditional, we then have a proposition:

Theorem I.II.1. *Proposition For all binary operation and set X, there is only one identity element.*

The proof is easy because by definition, we suppose an element e' which is also an identity element. Then because of that $e \cdot e' = e'$ and this is equal to e. Thus e' and e are the same. QED.

Aside from those, we also have inverse elements

Definition I.II.1. *Inverse Elements*

An element $x \in X$ is called an inverse element if there exists $y \in X$ that

$$x \cdot y = y \cdot x = e$$

From the definition, we have the second proposition

Theorem I.II.2. *Proposition 2 If the binary operation θ has associative properties then for each $x \in X$, there exists only one inverse element denoted x^{-1}*

I.III Internal binary operation

Definition of internal binary operation can be as follow:

Definition I.III.1. *Definition A binary operation on a non-empty set S is any mapping*

$$f : S \times S \longrightarrow S$$

*such operation with $x, y \in S$ and the operation f result in $f(x, y) \in S$ is called an **internal binary operation**, denoted T*

Thus, the binary operation $f : x, y \mapsto x + y$ is an internal binary operation in $\mathbb{R}$.

I.IV External binary operation

In cases that we want the Cartesian product to contain another set, i.e., the mapping of of both set onto one other, we can define the inverse of an internal binary operation:

Definition I.IV.1. *Definition 2.3 A binary operation on $S \notin \varnothing$*

$$f : S \times F \longrightarrow S$$

*with F is another set. Comprehensively, this is similar as $x \in S$, $y \in F$ then $f(x, y) \in S$, then the binary operation is called an **external binary operation**, denoted $\perp$*

I.V Homomorphism and Isomorphism

A homomorphism is a map between two algebraic structure of the same type that preserve the operation of the structures.

Definition I.V.1. *Homomorphism A mapping $f : E \longrightarrow F$ with F as a set with an internal binary operation T, and a set E with binary operation T', and both have an external binary operation $\perp$ on a set $\Omega \not\subseteq F, E$. Then, f is a homomorphism if it satisfies:*

$$f(x\, T\, y) = f(x)\, T'\, f(y), \forall x, y \in E$$

and

$$f(\lambda \perp x) = \lambda \perp' f(x) \forall x \in E, \forall \lambda \in \Omega$$

For this, we can say that E and F have a homomorphism f with them. If a homomorphism is also bijective, that is, one-on-one correspondence, then the homomorphism g is called an isomorphism. For this, it means that for each $h : E \longrightarrow F$ there exists a mapping $h' : F \longrightarrow E$ that satisfies all the aforementioned properties.

After this, now we have the tools to appropriately describe three main types of algebraic structure: group, ring and field.

II Group, Ring and Fields

II.I Group

We begin by stating the definition of group.

Definition II.I.1. *Groups Let G be a non-empty set with binary operation T. Then (G, T) is called a group if the following holds:*

1. *(G1) Binary operation T is associative:*

$$xT(yTz) = (xTy)Tz$$

2. *(G2) G has an identity element with respect to T, that is $\exists e \in G, \forall x \in G, xTe = eTx = x$*

3. *(G3) $\forall x \in G, \exists h \in G$ such that $gTh = hTg = e$, meaning h is an inverse element of g and reverse.*

If a group is also commutative, that is

$$xTy = yTx \, \forall e \in G$$

then we call it an **Abelian group**.

II.I.I Subgroup

Definition II.I.2. *Subgroup definition Let G be a group. Then for $H \subseteq G$ we called $H \neq \varnothing$ a subgroup of G if, for H with binary operation*

1. *T, $x, y \in H$ then $xTy \in H$*

2. *$x \in H$ then $x^{-1} \in H$*

3. *$e \in G$ then $e \in H$*

*Further in, if $H \neq G$ then we say H is a **proper subgroup** of G.*

II.II Group Homomorphism, Group Isomorphism

We here will present and state the definition of homomorphism within groups.

Definition II.II.1. *Group Homomorphism Given E, F as groups. A homomorphism from E to F is a function mapping $f : E \longrightarrow F$ such that*

$$f(xTy) = f(x)T'f(y), \forall x, y \in G$$

with T as the binary operation on E and T' on F. This is called a ***group homomorphism***

Group homomorphism is often referred to as group map for short.

Continuing, we have the definition of isomorphism:

Definition II.II.2. *Group Isomorphism If a group homomorphism $f : E \longrightarrow F$ is also bijective, then f is called a group isomorphism, with two group $(E, *)$ and $(F, \odot)$ Two groups are isomorphic if there exists an isomorphism from one to the other, written as*

$$(E, *) \cong (F, \odot)$$

II.III Ring

Definition II.III.1. *Ring An algebraic structure $(R, +, \cdot)$ is called a ring if for $R \neq \varnothing$ and two binary operation $+$ and $\cdot$, such that*

1. *The group E with operation $(+)$, or $(R, +)$ is an Abelian group. that is:*
   - *(a)* $\forall a, b, c \in R, a + (b + c) = (a + b) + c$
   - *(b)* $\exists e \in R, \forall a \in R \to a + e = e + a = a$
   - *(c)* $\forall a \in R, \exists! -a \in R$ *such that* $a + (-a) = (-a) + a = 0$
   - *(d)* $\forall a, b \in R, a + b = b + a$
2. *Multiplication:* $\forall a, b, c \in R$, *we have* $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
3. *Addition and multiplication together:* $\forall a, b, c \in R$,
$$a \cdot (b + c) = a \cdot b + a \cdot c$$
and
$$(a + b) \cdot c = a \cdot b + b \cdot c$$

II.III.I Subring

Definition II.III.2. *Subring Let R be a ring and $S \subset R$ be a subset. We say $S \subset R$ is a subring if*

1. *S is closed under addition and multiplication:*
$$r, s \in S \implies r + s, r \cdot s \in S$$
2. *S is closed under additive inverses:*
$$r \in S \implies r^{-1} \in S$$
3. *S contains the identity $1_R \in S$*

Here, the word closed means that for all operation, the result is also in the set of the subring.

II.III.II Commutative Ring

Definition II.III.3. *Commutative Ring*
A commutative ring $(K, +, \cdot)$ is a ring that the multiplication binary operation is commutative:
$$x \cdot y = y \cdot x; \forall x, y \in K$$

II.III.III Ring Homomorphism

Given $(K, +, \cdot)$ and $(K', +, \cdot)$ are the given rings. We said that
$$f : K \longrightarrow K'$$
is a ring homomorphism if
$$f(x + y) = f(x) + f(y)$$
and
$$f(x \cdot y) = f(x) \cdot f(y)$$
As we see, each ring homomorphism is a mapping that conserves the mathematical operation of the structure.

If f is also bijective then we say that $f : K \longrightarrow K'$ is a **ring isomorphism**.

II.IV Field

Definition II.IV.1. *Definition of a field*
A structure $(R, +, \cdot)$ where $+$ and $\cdot$ are two binary operation on R is a field if

1. *$(R, +)$ is an Abelian group.*
2. *$(R \setminus \{0\}, \cdot)$ is an Abelian group.*
3. *The distributive laws hold.*

A more "easy definition" of a field is as followed.

Definition II.IV.2. *Field Definition 2*
*A field is a **commutative ring** $(K, +, \cdot)$ with unit $1 \neq 0$, and*

$$\forall x \neq 0, \exists x^{-1} \in K \text{ such that } x \cdot x^{-1} = 1$$

II.IV.I Subfield

Given that $(K, +, \cdot)$ is a field. Then the subfield of $(K, +, \cdot)$ is a ring $P \neq \{0\}$ that satisfy:

$$\forall x \in P, \text{ if } x \neq 0 \implies x^{-1} \in P$$

III Polynomial Ring

A polynomial ring is a ring of polynomials such as $P(n)$, and each element of the ring is defined as:

$$P(n) = a_n x^n + \cdots + a_1 x^1 + a_0 = \sum_{i=0}^{n} a_i x^i$$

For two polynomials $P(n)$ and $G(m)$ to be equal, then

$$a_n = b_m, \forall m, n \in I = \{1, \cdots, n\}$$

The degree of a polynomial is denoted $d^\circ P(n)$ and evaluated to n, or

$$d^\circ P(n) = n$$

III.I Polynomial Ring Operations

Given a polynomial ring $(K, +, \cdot)$, this ring has two operation $+$ and $\cdot$ defined as below

Definition III.I.1 (Polynomial Summation)**.** *Given two polynomial $P(n)$ and $G(m)$ such that*

$$P(n) = \sum_{k=0}^{n} a_k x^k$$

and

$$G(m) = \sum_{k=0}^{n} b_k x^k$$

with $k \in I = \{1, \cdots, n\}$, the operation $P(n) + G(n)$ is defined to be

$$P(n) + G(m) = \sum_{k=0}^{n} (a_k + b_k) x_k = \sum_{k=0}^{n} C_k x^k \ , \ \forall m \leq n, C_k = a_k + b_k$$

Definition III.I.2 (Polynomial Product)**.** *Given two polynomial $P(n)$ and $G(m)$ such that*

$$P(n) = \sum_{k=0}^{n} a_k x^k$$

and

$$G(m) = \sum_{k=0}^{n} b_k x^k$$

with $k \in I = \{1, \cdots, n\}$, the operation $P(n) \cdot G(n)$ is defined to be

$$P(n) \cdot G(n) = \sum_{s=0}^{n+m} \left[\sum_{R(k,l):k+l=s} (a_k b_l) x^s \right] = \sum_{s=0}^{n+m} D_s x^s \text{ with } \left(D_s = \sum_{R(k,l):k+l=s} a_k b_l \right)$$

III.II Polynomial Division and Euclidean Division Algorithm for Polynomial

Given $G(x)$ and $P(x)$ as two polynomial in ring $(S, +, \cdot)$, we have the division of them,

$$\frac{P(x)}{G(x)}$$

defined as

$$\frac{P(x)}{G(x)} = H(x), R(x) \text{ such that } P(x) = H(x)G(x) + R(x)$$

with $d^\circ R(x) < d^\circ G(x)$. Same for Euclidean division of normal number, $P(x)$ is the dividend (the one being divided), $G(x)$ is the divisor (the one that divides the dividend) and $H(x)$ is the quotient, while $R(x)$ is the remainder polynomial.

III.II.I Division Algorithm

All elementary school long division. Divide by the highest degree variable, then multiply back the divisor and take the dividend subtract the divisor, and repeat the process. This is called polynomial long division, albeit there is indeed another one called short division.

III.II.II Root of Polynomial

A element $\alpha \in K$ is called the root of a polynomial with degree $n > 0$ if we replace α for x, we have

$$f(x) = a_n \alpha^n + \cdots + a_1 \alpha + a_0 = 0$$

Then, we have a statement about this

Theorem III.II.1 (Theorem of root of polynomial)**.** *The element $\alpha \in K$ is the root of $f(x) \in K[x]$ with degree $n > 0$ if and only if*

$$f(x) | (x - \alpha)$$

Continuing, we see that for polynomial $f(x) \in K[x]$ with $n > 0$, the element $\alpha \in K$ is called a multiple root if

$$f(x) \mid (x - \alpha)^k$$

but not for $(x - \alpha)^{k+1}$

From all of this, we can say that a polynomial $f(x)$ with $n > 0$ be its degree **does not have more than n root, even with multiple root**

III.III GCD (Greatest Common Divisor) of Polynomial

The common divisor of two Polynomial $P(x)$ and $G(x)$ is $d(x)$ such that

$$d \vdots P(x) \quad \text{and} \quad d \vdots G(x)$$

Then $d(x)$ is called GCD of $P(x)$ and $G(x)$ if $D(x)$ is divisible to all common divisor of $P(x)$ and $G(x)$ A property of $d(x)$ is presented. Suppose that

$$d \vdots P(x) \quad \text{and} \quad d \vdots G(x)$$

then

$$d \vdots [P(x) \pm G(x)]$$

and

$$d \vdots F(x) \cdot G(x)$$

III.IV Properties of GCD of Polynomial

Here we will state some property of GCD of polynomial

Theorem III.IV.1. *Each GCD of a pair of polynomial $P(x), G(x) \neq 0$ is different by one zeroth order $(n = 0)$ factor.*

Theorem III.IV.2. *If $d(x)$ is the GCD of $P(x)$ and $G(x)$, then $a \cdot d(x)$ is also a GCD of $P(x), G(x)$ with $a \in K, a \neq 0$*

If $P(x)$ and $G(x)$ both has a GCD, then there exists only one norm form, or original form of the GCD. This is from the property 3 of which $a \cdot d(x)$ is also a GCD, thus $d(x)$ is the original GCD and exists only one.

The **norm form - original GCD** is denoted as

$$(f(x)\ ;\ g(x))$$

for every two polynomials $f(x), g(x)$

Apart from those, we will also have a general theorem for GCD of polynomials:

Theorem III.IV.3 (Existence of GCD)**.** *There is always GCD for every pair $P(x) \neq 0$, $G(x) \neq 0$*

III.IV.I Prime Polynomial

Two polynomials are called **prime polynomial** if for $f(x), g(x) \neq 0; f(x), g(x) \in K[x]$, then they have

$$(f(x)\ ;\ g(x)) = 1$$

From this, we have a theorem:

Theorem III.IV.4 (Theorem of Prime Polynomial)**.** *Two polynomials $f(x) \neq 0$ and $g(x) \neq 0$ are both prime polynomial if and only if there is two polynomial $u(x), v(x) \in K[x]$ such that*

$$f(x)u(x) + g(x)v(x) = 1$$

III.V Irreducible Polynomial

A polynomial $P(x) \neq 0$ of degree n is called **irreducible** if it cannot be factored into

$$P(x) = P_1(x) \cdot P_2(x)$$

of which

$$0 < d^\circ(P_1(x), P_2(x)) < n$$

From this, we also can say that all degree 1 polynomials are irreducible. And hence, all polynomial with degree $n \geq 2$ irreducible on $K[x]$ will have no root in $K[x]$, that is, undefined in such ring. Thus the irreducible property of polynomial depends on the property of ring K.

III.VI Polynomial on $\mathbb{C}$

We assume the following theorem as right, which can be used as axiom.

Theorem III.VI.1. *Every polynomial $p(x)$ with $d^\circ(P(x)) = n > 0$ on $\mathbb{C}$ has complex root.*

Consider $g(x)$ as a complex polynomial, with $d^\circ(g(x)) = n > 0$, then by axiom 1.6.1, we have that $g(x)$ has a complex root a_1. Then the polynomial can be written as:

$$g(x) = (x - a_1)q_1(x)$$

with $q_1(x)$ be a complex polynomial on $\mathbb{C}$. Then further assume that $q_1(x)$ is reducible, and has a complex root a_2, then $q_1(x)$ can be written as:

$$q_1(x) = (x - a_2)q_2(x)$$

Thus from here, we have that

$$g(x) = (x - a_2)(x - a_1)q_2(x)$$

Now, continuing this process assume that there is $q_n(x)$ to expand, then we will result in

$$g(x) = b(x - a_1)^{r_1} \cdots (x - a_m)^{r_m}$$

with b as the highest order coefficient, and

$$r_1 + \cdots r_m = n$$

additionally with

$$a_i \neq a_j \; \forall i \neq j$$

a_i is the rth complex root.

Chapter 3

Vector Spaces

I Definition of Vector Space

Given a set E, then E is called a K-vector spaces, or a linear spaces on field K if E is equipped with two inner and outer operations $(+, \cdot)$ respectively, addition scalar multiplication such that

$$\begin{cases} E(+) & \text{addition of } x_i \in E \\ E(\cdot) & \text{multiplication of } x_i \in E \text{ and } y_i \in K \end{cases}$$

Both operations must also satisfy

$$\begin{cases} (E, +) \text{ is an Abelian group} & \\ \lambda(x+y) = \lambda x + \lambda y, & \forall x, y \in E, \forall \lambda \in K \\ (\lambda + \beta)x = \lambda x + \beta x, & \forall \lambda, \beta \in K, \forall x \in E \\ \lambda(\beta x) = (\lambda\beta)x & \forall \lambda, \beta \in K, x \in E \\ 1 \cdot x = x & \forall x \in E \end{cases}$$

Each of the element of E is a vector. The zero vector of vector space E is denoted θ, and the counter/inverse vector is denoted $-\vec{x}$ of $\vec{x}$. Both of them exist only one, with θ being a single distinct element, and $-x + (x) = \theta, \forall x \in E$, that is, for every vector x there is only one inverse vector $-x$. We often use two types of notation for element vectors in vector spaces, either with arrows on top or not, and Greek symbols for special vectors.

We have some widely seen, and widely used vector spaces we will encounter in different forms. First one is the $\mathbb{R}^n$ vector space:

$$\mathbb{R}^n = \{(x_1, x_2, x_3, x_4, \ldots, x_n) | x_i \in \mathbb{R}, \forall i \in [1, n]\}$$

Secondly, is the polynomial vector spaces

$$P(x) = \{a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n | a_i \in \mathbb{R}\}$$

and the matrices vector spaces

$$M_n(x) = \{\text{matrices of the same order n}\}$$

I.I Property of Vector Space

In accordance, we present some properties of vector spaces E.

1. $\theta x = \theta, \forall x \in E$
2. $\alpha\theta = \theta, \forall \alpha \in K$
3. $\alpha \cdot x = \theta$ if and only if $\alpha = 0$ or $\theta = x$
4. $\alpha(-x) = -(\alpha)x, \forall \alpha \in K, x \in E$

I.II Vector Subspace

Just as same as fields and ring, we have the definition of vector subspace. A vector space $(E, +, \circ)$ on field K has a subspace with $V \subset E$ if

$$\forall x, y \in V, \forall k \in K, \begin{cases} x + y \in V \\ kx \in V \end{cases} \tag{3.1}$$

Loosely saying, V is a subspace in E if the operation contains itself, returning the value inside the space, of which the space is also a subset of the bigger space, E.

Formally, we would like to write it as a definition

Definition I.II.1. *A set $A \neq \varnothing$, of vector space E on K is called a vector subspace of E if it satisfies*

1. *$\forall \vec{x}, \vec{y} \in A$ then $\vec{x} + \vec{y} \in A$*
2. *$\forall \vec{x}, \forall \lambda \in K$ then $\lambda x \in A$*

II Linear Combination, Linear (In)dependent and System of Vectors

II.I Linear Combination

Let E be a vector spaces on K. Then, given a set A contains

$$A = \{\vec{V_1}, \vec{V_2}, \cdots, \vec{V_n}\}, n \in [1, n]$$

Then, the equation

$$L_n = \lambda_1\vec{V_1} + \lambda_2\vec{V_2} + \cdots + \lambda_n\vec{V_n} = \sum_{i=1}^{n} \lambda_i\vec{V_i} \ \forall \lambda_i \in K$$

is called the **linear combination** of A - a system of vectors.

A interesting property of linear combination is that - if you have a set of vectors $A = \{V_i\}$, $B = \{U_j\}$ and $C = \{W_k\}$, then if A can be represented by B, and B can be represented by C, the A can be represented by C. One tip to think of linear combination is the operation of combining vectors with additional steps - and a generalizing step.

II.II Linear Independent and Dependent

A system of vectors

$$A = \{\vec{V_1}, \vec{V_2}, \cdots, \vec{V_n}\}, n \in [1, n]$$

is called **linear dependent** if there exist scalars $\lambda_1, \cdots, \lambda_n$ not all *zero* such that

$$L_n = \lambda_1\vec{V_1} + \lambda_2\vec{V_2} + \cdots + \lambda_n\vec{V_n} = \sum_{i=1}^{n} \lambda_i\vec{V_i} = \mathbf{0}$$

with $\mathbf{0}$ the zero vector. This implies that at least one of the scalars is non-zero, that is $a_1 \neq 0$ and the equation is able to be written as

$$\vec{V_1} = \frac{-a_2}{a_1}\vec{V_2} + \cdots + \frac{-a_k}{a_1}\vec{V_k}, \ \forall k > 1$$

If $k = 1$, then $\vec{V_1} = \mathbf{0}$, and with $\lambda_i = a_i$

A sequence/system of vectors A is called linear independent if it is not dependent, that is,

$$\lambda_1\vec{V_1} + \lambda_2\vec{V_2} + \cdots + \lambda_n\vec{V_n} = \sum_{i=1}^{n} \lambda_i\vec{V_i} = \mathbf{0}$$

can only be satisfied by $\lambda_i = 0$ for $i = 1, \cdots, n$. This implies that no vector in the sequence can be represented as a linear combination of the remaining vectors in the sequence. If a sequence of vectors contains the same vector twice, it is necessarily dependent.

The definition can be expanded as

Definition II.II.1. *A vector set S in vector space V is linear independent if for all finite vector sets in S,*

$$\{\vec{V_1}, \vec{V_2}, \ldots, \vec{V_m}\} \subset S$$

for $\vec{v_i} \neq \vec{v_j}, \forall i \neq j$

II.III Properties

We then have a property of linear independent sequences.

Theorem II.III.1. *All subsets of a set of linear independent vectors are linear independent*

Theorem II.III.2. *If the subset A of a set S is linear dependent then the mother set S is also linear dependent.*

Theorem II.III.3. *$\{\vec{0}\}$ is a linear dependent vector system.*

Theorem II.III.4. *A system of vectors*

$$A = \{\vec{V_1}, \vec{V_2}, \cdots, \vec{V_n}\}$$

with $n \geq 2$ is linear dependent if and only if there is a vector $\vec{V_i}$ in A such that $\vec{V_i}$ can be represented by other vectors in the system.

III Generator, Basis, and Dimension of Vector Space

III.I Generator

Given a system of vectors V of E, if all vectors in vector space E can be represented by linear transformation from V, then V is the generator of E. Intuitively, if any vector inside a vector space can be constructed, or represented using a system of linear combination, that is, combining vectors, then that system of vector is the generator.

For example, the vector space $\mathbb{R}^3$ on $\mathbb{R}$ has the following system as generator:

$$V_{\mathbb{R}^3} = \{e_1 : (1,0,0); e_2 : (0,1,0); e_3 : (0,0,1)\}$$

since the combination

$$e_1\lambda_1 + e_2\lambda_2 + e_3\lambda_3 = \vec{x}, \vec{x} = (x_1, x_2, x_3)$$

is valid. Considerably, we can write the vector $\vec{x}$ in vector space as

$$\vec{x} = \begin{pmatrix}1\\0\\0\end{pmatrix} x_1 + \begin{pmatrix}0\\1\\0\end{pmatrix} x_2 + \begin{pmatrix}0\\0\\1\end{pmatrix} x_3$$

of which all the column matrices are e_1, e_2 and e_3 accordingly.

If L is the vector space generated from $\{V\}$, then we denoted

$$L = \mathcal{L}(\{\vec{V_i}\})$$

III.II Basis

A basis is like a base of a building - anything of the building will be constructed from that. In vector space, we can see that a basis works the same way: anything is constructed using the basis.

Hence, the definition of a basis is a system of vectors that is both a generator and linear independent. Formally, we will write them as

Definition III.II.1. *The vector system $S = \{\vec{V_i}\}, i = \bar{1,n}$ is a basis of E if and only if (iff) for all $\vec{Q} \in E$, we can construct them from S, that is*

$$\vec{Q} = \sum_{i=1}^{n} \lambda_i \vec{V_i}$$

For this definition, we will use necessity and sufficiency for better understanding.

Theorem III.II.1. *We say that* ***the statement A is a necessary and sufficient condition for the statement B when B is true if and only if A is also true****. That is, either A and B are both true, or they are both false. Note that if A is necessary and sufficient for B , then B is necessary and sufficient for A.*

III.II.I Span of Vector Spaces

The linear span of a set S of vector in vector space E is defined as the set of all linear combinations of the vectors in S. Given a vector space E over field F, The span of a set S of vectors (not necessary finite) is defined to be the intersection W of all subspaces of E containing S. Formulationally, we have

$$\text{span}(S) = \left\{ \sum_{i=1}^{k} \lambda_i \mathbf{v}_i \;\middle|\; k \in \mathbb{N}, \mathbf{v}_i \in S, \lambda_i \in K \right\}$$