Linear Algebra I

Ji, Yong-hyeon

June 30, 2025

We cover the following topics in this note.

Part I

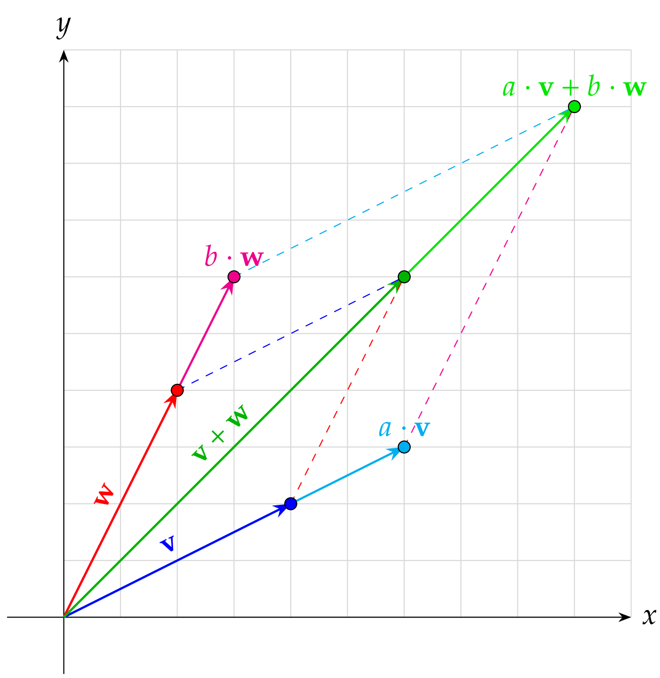
- Linear Combination, Spanning Set
- Linearly Independent and Dependent
- Basis

Part II

- Partial Order; POSET
- Total Order (Linear Order); TOSET
- Maximal, Minimal, Hasse Diagram

Part III

- Chain, Zorn's Lemma
- Basis Theorem (Existence of Basis)
- Invariance of Basis Cardinality; Dimension of Vector Space



Vector Space

Definition. Let F be a field. A **vector space** over F (or a F-vector space) is a structure $(V, +, \cdot)$ satisfying the following axioms:

(i) $(V, +)$ is an abelian group with additive identity $\mathbf{0} \in V$.

(ii) Define *scalar multiplication* as the function $\cdot : F \times V \to V, \quad (a, \mathbf{v}) \mapsto a \cdot \mathbf{v}$.

(iii) (Compatibility) For all $a, b \in F$ and $\mathbf{v}, \mathbf{w} \in V$,

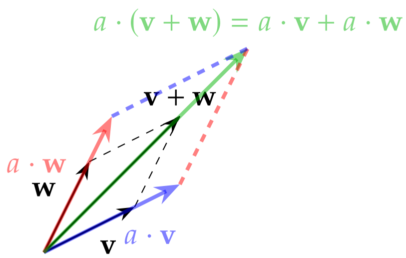
(a) $a \cdot (\mathbf{v} + \mathbf{w}) = a \cdot \mathbf{v} + a \cdot \mathbf{w}$. (Distributivity over vector addition)

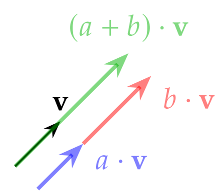
(b) $(a + b) \cdot \mathbf{v} = a \cdot \mathbf{v} + b \cdot \mathbf{v}$. (Distributivity over field addition)

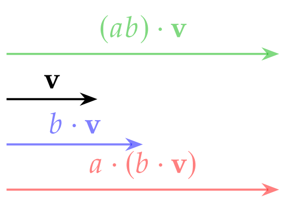
(c) $a \cdot (b \cdot \mathbf{v}) = (ab) \cdot \mathbf{v}$. (Associativity of scalar multiplication)

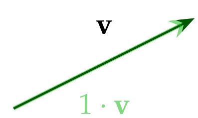
(d) $1_F \cdot \mathbf{v} = \mathbf{v}$. (Identity of scalar multiplication)

(e) $0_F \cdot \mathbf{v} = \mathbf{0}$.









Remark. Consider a vector space V over a field F. Let $\mathbf{v} \in V$. Since $0_F = 0_F + 0_F$ (over F), we have

$$0_F \cdot \mathbf{v} = (0_F + 0_F) \cdot \mathbf{v} \overset{\text{(iii)-(b)}}{=} 0_F \cdot \mathbf{v} + 0_F \cdot \mathbf{v}.$$

Then

$$\begin{aligned} 0_F \cdot \mathbf{v} + (-0_F \cdot \mathbf{v}) &= 0_F \cdot \mathbf{v} + 0_F \cdot \mathbf{v} + (-0_F \cdot \mathbf{v}), \\ \mathbf{0} &= 0_F \cdot \mathbf{v} + \mathbf{0}, \\ \mathbf{0} &= 0_F \cdot \mathbf{v}. \end{aligned}$$

Linear Combination and Spanning Set

Definition. Let V be a vector space over a field F, and let S be a subset of V

(1) A vector $\mathbf{v} \in V$ is called a **linear combination** of elements of S if there exists finite number of vectors $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n \in S$ and scalars $a_1, a_2, \ldots, a_n \in F$ such that

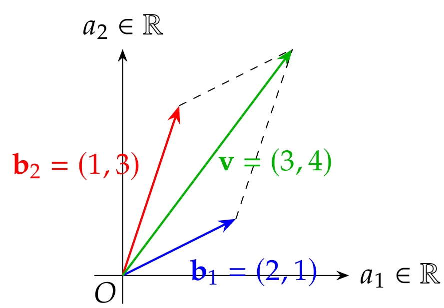
$$\mathbf{v} = a_1\mathbf{b}_1 + a_2\mathbf{b}_2 + \cdots + a_n\mathbf{b}_n = \sum_{i=1}^{n} a_i\mathbf{b}_i.$$

(2) The **subspace spanned by** S (or **spanning set** S), denoted by $\operatorname{span}(S)$, is the set of all finite linear combinations of elements of S:

$$\begin{aligned}\operatorname{span}(S) &= \left\{a_1\mathbf{b}_1 + a_2\mathbf{b}_2 + \cdots + a_n\mathbf{b}_n \mid a_i \in F, \mathbf{b}_i \in S \text{ for all } i = 1, 2, \ldots, n\right\} \\ &= \left\{\sum_{i=1}^{n} a_i\mathbf{b}_i \,\middle|\, a_i \in F, \mathbf{b}_i \in S \text{ for all } i = 1, 2, \ldots, n\right\}\end{aligned}$$

Example. Consider the vector space $\mathbb{R}^2$ and the subset

$$S = \{\mathbf{b}_1, \mathbf{b}_2\} \quad \text{with} \quad \mathbf{b}_1 = (2, 1) \text{ and } \mathbf{b}_2 = (1, 3).$$



- A vector $\mathbf{v} = (3, 4) \in \mathbb{R}^2$ is a linear combination of $\mathbf{b}_1$ and $\mathbf{b}_2$ since

$$\mathbf{v} = (3, 4) = (2 \cdot 1 + 1, 1 + 3 \cdot 1) = 1 \cdot (2, 1) + 1 \cdot (1, 3), \quad \text{i.e.,} \quad \mathbf{v} = \begin{bmatrix} 3 \\ 4 \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 3 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \end{bmatrix}.$$

- Since $\mathbf{b}_1$ and $\mathbf{b}_2$ are not colinear (they are lineary independent), every vector in $\mathbb{R}^2$ can be expressed in the form $(2a_1 + a_2, a_1 + 3a_2)$ for some $a_1, a_2 \in \mathbb{R}$. Hence

$$\operatorname{span}(S) = \mathbb{R}^2.$$

Linearly Independent and Dependent

Definition. Let V be a vector space over a field F and let $S \subseteq V$.

(1) The set S said to be **linearly independent** if, for any finite collection of distinct vectors $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n \in S$ and any scalars $a_1, a_2, \ldots, a_n \in F$,

$$a_1\mathbf{b}_1 + a_2\mathbf{b}_2 + \cdots + a_n\mathbf{b}_n = \mathbf{0} \implies a_1 = a_2 = \cdots = a_n = 0.$$

(2) The set S is said to be **linearly dependent** (i.e., not linearly independent) if there exists finitely many distinct vectors $\mathbf{b}_1, \mathbf{b}_2, \cdots, \mathbf{b}_n \in S$ and scalars $a_1, a_2, \ldots, a_n \in F$, not all zeros, such that

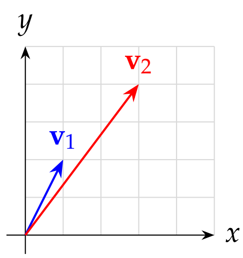
$$a_1\mathbf{b}_1 + a_2\mathbf{b}_2 + \cdots + a_n\mathbf{b}_n = \mathbf{0}.$$

Remark. In (2), suppose that $a_1 \neq 0$, Then

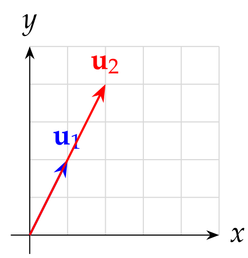
$$a_1\mathbf{b}_1 = -a_2\mathbf{b}_2 - \cdots - a_n\mathbf{b}_n \iff \mathbf{b}_1 = -a_1^{-1}(a_2\mathbf{b}_2 + \cdots + a_n\mathbf{b}_n).$$

That is, a set S is linearly dependent if at least one vector in S can be expressed as a linear combination of the others.

Example.



Linearly Independent Vectors



Linearly Dependent Vectors (Collinear)

- The vectors $\mathbf{v}_1 = (1, 2)$ and $\mathbf{v}_2 = (3, 4)$ are linearly independent because the only solution to

$$a\mathbf{v}_1 + b\mathbf{v}_2 = \mathbf{0}$$

  is $a = 0$ and $b = 0$.

- The vectors $\mathbf{u}_1 = (1, 2)$ and $\mathbf{u}_2 = (2, 4)$ are linearly dependent because $\mathbf{u}_2$ is a multiple of $\mathbf{u}_1$; nontrivial solutions exist for

$$a\mathbf{u}_1 + b\mathbf{u}_2 = \mathbf{0}.$$

Remark. In any vector space V, we can always find a subset of S such that

$$\operatorname{span}(S) = V.$$

For instance, taking $S = V$ gives $\operatorname{span}(S) = V$. Since $S = V$, each vector $\mathbf{v} \in V$ can be expressed as a trivial linear combination $\mathbf{v} = 1 \cdot \mathbf{v}$. Thus, there exists a subset $S \subseteq V$ such that $\operatorname{span}(S) = V$.

Remark.

- A singleton set $\mathcal{B} = \{\mathbf{b}\}$ is linearly independent since $k\mathbf{b} = 0 \implies k = 0$ for any $k \in F$.
- The empty set $\varnothing$ is linearly independent; this holds vacuously.

⋆ ~~(Hamel)~~ Basis ⋆

Definition. Let V be a vector space over a field F. A subset $\mathcal{B} \subseteq V$ is called a ~~**(Hamel)**~~ **basis** for V if it satisfies the following two conditions:

(i) (*Linearly Independent*) The set $\mathcal{B}$ is linearly independent; that is, for any *finite* collection of distinct elements $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n \in \mathcal{B}$ and scalars $a_1, a_2, \ldots, a_n \in F$,

$$a_1\mathbf{b}_1 + a_2\mathbf{b}_2 + \cdots + a_n\mathbf{b}_n = 0 \implies a_1 = a_2 = \cdots = a_n = 0.$$

(ii) (*Spanning Property*) The set $\mathcal{B}$ spans V ($\operatorname{span}\mathcal{B} = V$); that is, every vector $\mathbf{v} \in V$, there exist a positive integer $n \in \mathbb{Z}^+$, scalars $a_1, a_2, \ldots, a_n \in F$, and distinct elements $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n \in \mathcal{B}$ such that

$$\mathbf{v} = a_1\mathbf{b}_1 + a_2\mathbf{b}_2 + \cdots + a_n\mathbf{b}_n,$$

Remark (Schauder Basis)**.** Let X be a Banach space (or more generally, a complete normed vector space) over the field F. A sequence $\{x_n\}_{n=1}^{\infty} \subseteq X$ is called a **Schauder basis** for X if it satisfies the following condition:

For every vector $x \in X$, there exits a unique sequence of scalars $\{a_n\}_{n=1}^{\infty} \subseteq F$ such that

$$x = \sum_{i=1}^{\infty} (a_n \cdot x_n),$$

where the series converges in the norm topology of X, i.e., $\lim_{N\to\infty} \left\| x - \sum_{n=1}^{N} (a_n \cdot x_n) \right\| = 0.$

Remark. A Hamel basis is unique in the sense that every vector in V has a unique representation as a finite linear combination of the elements of $\mathcal{B}$.

Partial Order

Definition. Let S be a nonempty set. A binary relation $\preceq$ on S is called a **partial order** if it satisfies the following three axioms for all $a, b, c \in X$,

(i) (Reflexivity) $a \preceq a$;

(ii) (Anti-symmetry) $a \preceq b$ and $b \preceq a \implies a = b$;

(iii) (Transitivity) $a \preceq b$ and $b \preceq c \implies a \preceq c$.

Note. A **partially ordered set (POSET)** is an $(S, \preceq)$, where S is a set and $\preceq$ is a partial order on S.

Example (Poset of the Power Set with Set Inclusion)**.** Let S be any set. Consider the power set of S:

$$2^S = \{A : A \subseteq S\} \quad \text{with} \quad \text{binary relation} \subseteq \text{on } 2^S.$$

We claim that $(2^S, \subseteq)$ is partially ordered set: for any $A, B, C \in 2^S$,

(i) Reflexivity: $A \subseteq A$;

(ii) Anti-symmetry: $A \subseteq B$ and $B \subseteq A \implies A = B$;

(iii) Transitivity: $A \subseteq B$ and $B \subseteq C \implies A \subseteq C$.

Hence, $(2^S, \subseteq)$ forms a poset.

Total Order (Linear Order)

Definition. Let $(S, \preceq)$ be a poset; that is, $\preceq$ is a partial order on S. We say that $\preceq$ is a **total order** (or **linear order**) on S if it satisfies the *comparability condition*: for each $a, b \in S$, either

$$a \preceq b \quad \text{or} \quad b \preceq a.$$

Note. A **totally ordered set (TOSET)** is a poset $(S, \preceq)$ in which the relation $\preceq$ is a total order. In other words, $(S, \preceq)$ is totally ordered if every pair of elements in S is comparable.

Example. Consider all binary string of length 3:

$$\{000, 001, 010, 011, 100, 101, 110, 111\}.$$

They are ordered as follows:

$$000 \longrightarrow 001 \longrightarrow 010 \longrightarrow 011 \longrightarrow 100 \longrightarrow 101 \longrightarrow 110 \longrightarrow 111$$

Maximal and Minimal

Definition. Let $(P, \preceq)$ be a poset.

(1) An element $m \in P$ is said to be **maximal** in P if

$$\forall a \in P, \quad (m \preceq a) \implies (m = a).$$

In other words, there exits no element in P that is strictly greater than m.

(2) An element $m \in P$ is said to be **minimal** in P if

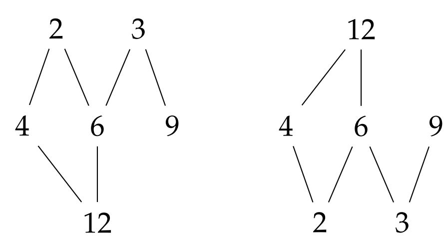
$$\forall a \in P, \quad (a \preceq m) \implies (a = m).$$

That is, there is no element in P that is strictly less than m.

Example. Consider the set

$$S = \{2, 3, 4, 6, 9, 12\} \subseteq \mathbb{N}$$

with the partial order defined by *divisibility* (i.e., $x \preceq y \iff x \mid y$). See the Hasse diagram:

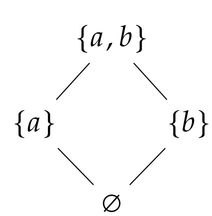


In this example, the minimal elements here are: $\{2, 3\}$.

Example. Consider the power set of $\{a, b\}$ with the usual subset relation $\subseteq$. The poset is

$$\left\{\varnothing, \{a\}, \{b\}, \{a, b\}\right\},$$

partially ordered by "is a subset of."



- The *minimal element* here is $\varnothing$ (there's nothing strictly smaller).
- The *maximal element* here is $\{a, b\}$ (there's nothing strictly bigger).

Chain

Definition. Let $(P, \preceq)$ be a poset. A subset $C \subseteq P$ is called a **chain** if

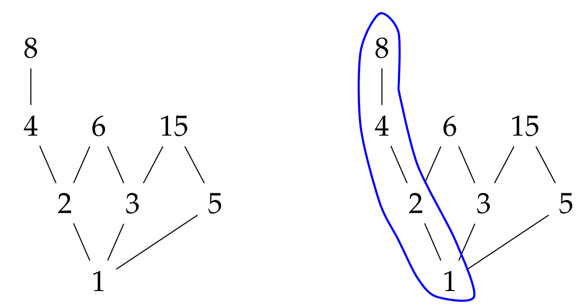
$$\forall a, b \in C, \quad \text{either } a \preceq b \text{ or } b \preceq a.$$

In other words, a chain in a poset is a subset in which every two elements are comparable (i.e.the subset is totally ordered).

Example. Consider a poset

$$P = \{1, 2, 3, 4, 5, 6, 8, 15\} \subseteq \mathbb{N}$$

with the partial order defined by divisibility. See the Hasse diagram:



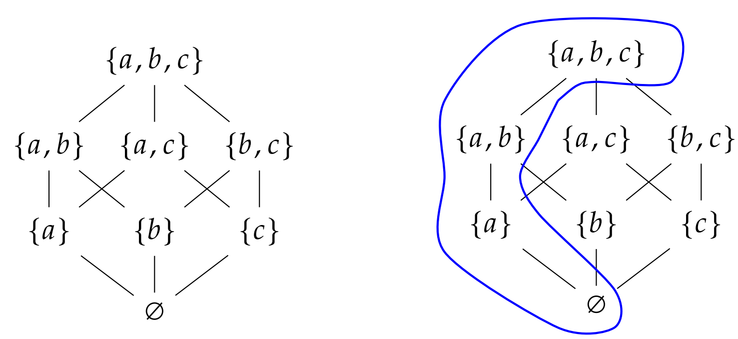
Here, $C = \{1, 2, 4, 8\}$ is a *chain* under divisibility.

Example. Let $S = \{a, b, c\}$. Consider all the subsets of S under the subset relation $\subseteq$. The entire power set of S is

$$2^S = \{\varnothing, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}.$$

This set 2^S (the power set) is partially ordered by $\subseteq$: for any $A, B \in 2^S$,

$$A \preceq B \iff A \subseteq B.$$



Here, $C = \{\varnothing, \{a\}, \{a, b\}, \{a, b, c\}\}$ is a *chain* in 2^S.

Zorn's Lemma

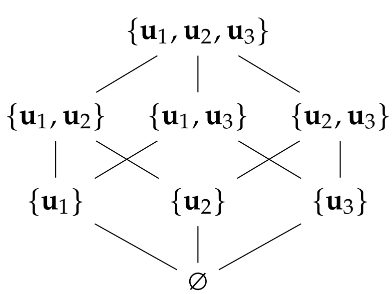
Axiom. Let $(P, \preceq)$ be a nonempty partially ordered set with property that every chain $C \subseteq P$ has an upper bound in P; that is, for every chain $C \subseteq P$,

$$\exists u \in P \quad \text{such that} \quad \forall c \in C, \quad c \preceq u.$$

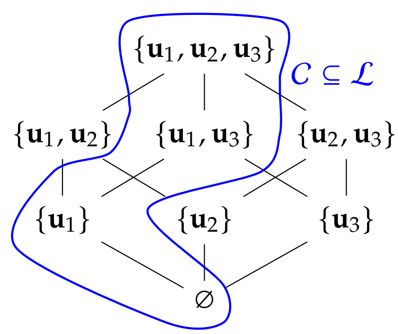
Then P contains at least one maximal element; that is,

$$\exists m \in P \quad \text{such that} \quad \forall a \in P, \quad (m \preceq a) \implies (m = a).$$

Observation (Existence of Basis). Let $\mathcal{L} := \left\{ S \subseteq \mathbb{R}^3 : S \text{ is linearly independent} \right\}$.

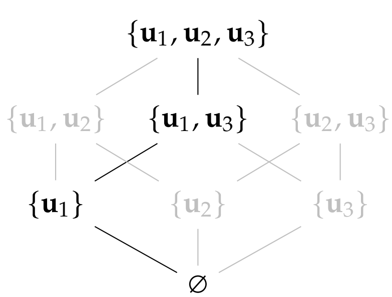


Hasse Diagram for a poset $(\mathcal{L}, \subseteq)$ in $\mathbb{R}^3$

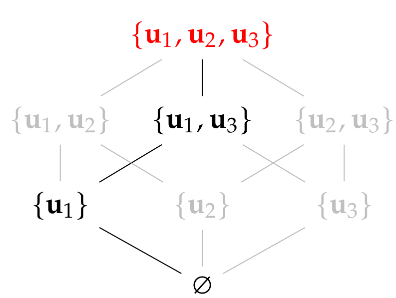


Any chain C

$U = \varnothing \cup \{\mathbf{u}_1\} \cup \{\mathbf{u}_1, \mathbf{u}_3\} \cup \{\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3\}$



Upper Bound $U = \bigcup_{S \in C} S$



Maximal element $\mathcal{B} = \{\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3\}$

⋆ Basis Theorem ⋆

Theorem. *Every vector space V over a field F has a basis.*

Proof.

Key Idea: "By considering all linearly independent subsets of V and partially ordering them by inclusion, we use Zorn's Lemma to guarantee a maximal linearly independent set exists."

□

Remark. This theorem and its proof is a classic demonstration of how abstract set-theoretic principles can yield concrete and essential results in linear algebra.

Definition. Consider any two sets S_1 and S_2.

(1) (Equal Cardinalities) We write

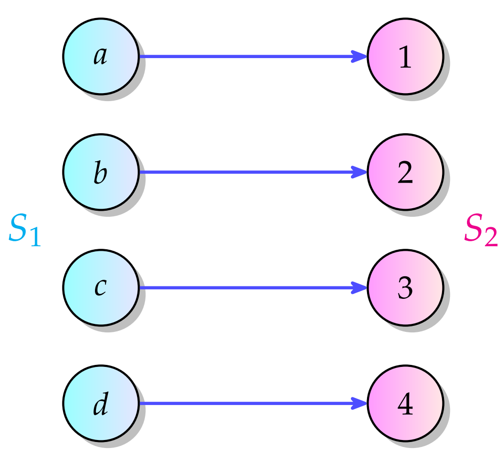
$$|S_1| = |S_2|$$

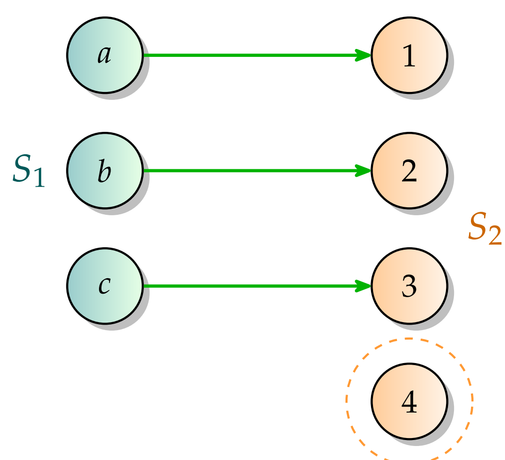
if and only if there exists a bijective (one-to-one and onto) function $f : S_1 \longrightarrow S_2$.

(2) (Strict Inequality of Cardinalities) We write

$$|S_1| < |S_2|$$

if and only if there exists an injective (one-to-one) function $f : S_1 \longrightarrow S_2$ but no bijective function from S_1 onto S_2 exists.





Steinitz's Exchange Lemma

Lemma. *Let V be a vector space over a field F. Suppose that*

(i) $\mathcal{X} = \{\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_m\} \subseteq V$ *is a linearly independent set, and*

(ii) $\mathcal{Y} = \{\mathbf{y}_1, \mathbf{y}_2, \ldots, \mathbf{y}_n\} \subseteq V$ *is a spanning set of V*, i.e., $\operatorname{span} \mathcal{Y} = V$.

Then $|\mathcal{X}| \leq |\mathcal{Y}|$, *that is, there exists an injective function* $f : \mathcal{X} \rightarrowtail \mathcal{Y}$.

Proof. TBA $\square$

Invariance of Basis Cardinality

Theorem. *Let V be a vector space over a field F, and let $\mathcal{B}_1$ and $\mathcal{B}_2$ be two bases of V. Then*

$$|\mathcal{B}_1| = |\mathcal{B}_2| .$$

Proof. Suppose, for the contradiction, that

$$|\mathcal{B}_1| < |\mathcal{B}_2| .$$

Since $\mathcal{B}_1$ is a basis, it spans V. Also since $\mathcal{B}_2$ is a basis, it is linearly independent. Applying the Steinitz's Exchange Lemma, we obtain

$$|\mathcal{B}_2| \leq |\mathcal{B}_1| \quad \lightning .$$

Thus, it is not possible to have bases $\mathcal{B}_1$ and $\mathcal{B}_2$ of V with different cardinalities. $\square$

Dimension of Vector Space

Definition. Let V be a vector space over a field F. The **dimension** of V, denoted by $\dim V$, is defined as the cardinality of any basis $\mathcal{B}$ of V:

$$\dim V := |\mathcal{B}| .$$

Remark. By the Invariance of Basis Cardinality, this definition does not depend on the choice of the basis.