

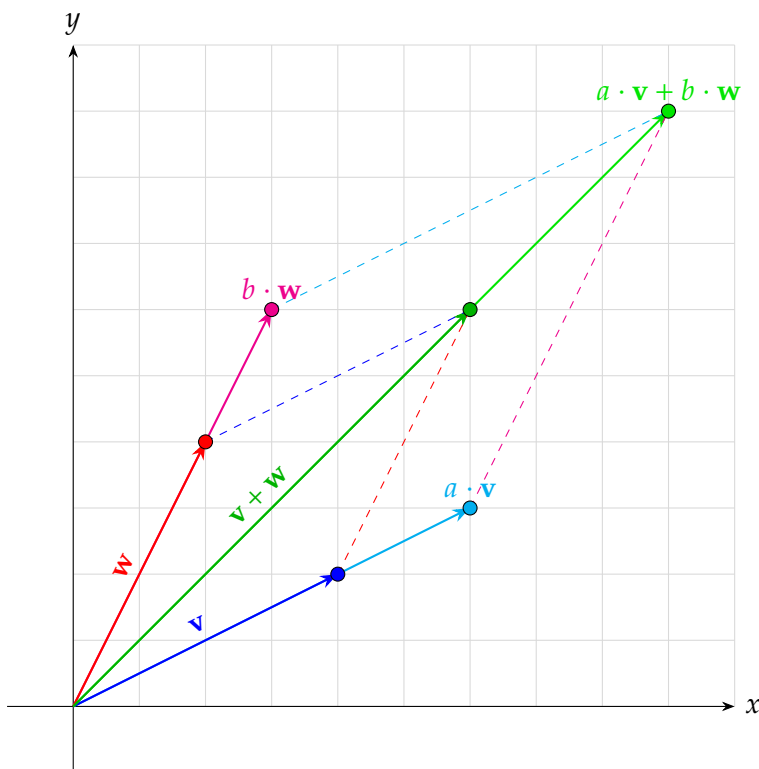
Linear Algebra I

Ji, Yong-hyeon

February 25, 2025

We cover the following topics in this note.

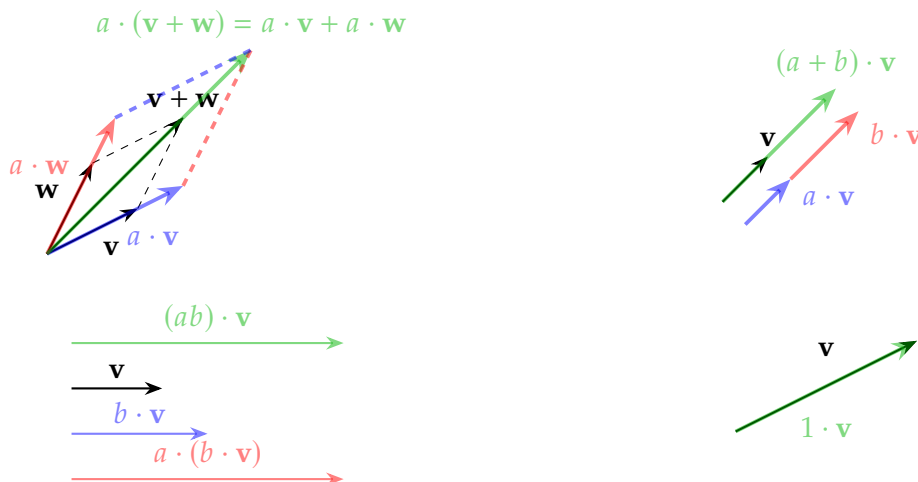
- Linear Combination, Spanning Set
 - Linearly Independent and Dependent
 - (Hamel) Basis
 - Partial Order; POSET
 - Total Order (Linear Order); TOSET
 - Maximal, Minimal, Hasse Diagram
 - Chain, Zorn's Lemma
 - Hamel Basis Theorem (Existence of Basis)
 - Invariance of Basis Cardinality; Dimension of 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 $\cdot : F \times V \rightarrow V, (a, \mathbf{v}) \mapsto a \cdot \mathbf{v}$.
- (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

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

Then

$$0_F \cdot \mathbf{v} + (-0_F \cdot \mathbf{v}) = 0_F \cdot \mathbf{v} + 0_F \cdot \mathbf{v} + (-0_F \cdot \mathbf{v}),$$

$$\mathbf{0} = 0_F \cdot \mathbf{v} + \mathbf{0},$$

$$\mathbf{0} = 0_F \cdot \mathbf{v}.$$

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 $\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_n \in S$ and scalars $a_1, a_2, \dots, a_n \in F$ such that

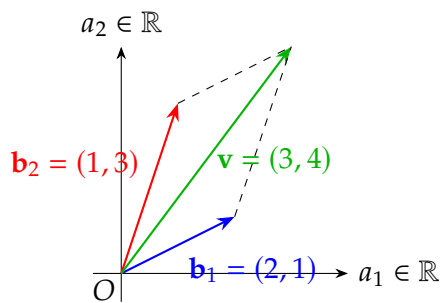
$$\mathbf{v} = a_1 \mathbf{b}_1 + a_2 \mathbf{b}_2 + \dots + a_n \mathbf{b}_n = \sum_{i=1}^n a_i \mathbf{b}_i.$$

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

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

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 linearly 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

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

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 $\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_n \in S$ and any scalars $a_1, a_2, \dots, a_n \in F$,

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

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

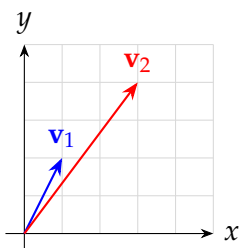
$$a_1\mathbf{b}_1 + a_2\mathbf{b}_2 + \dots + a_n\mathbf{b}_n = \mathbf{0}.$$

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

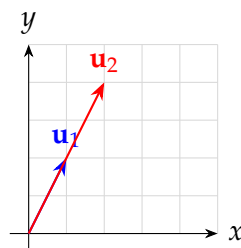
$$a_1\mathbf{b}_1 = -a_2\mathbf{b}_2 - \dots - a_n\mathbf{b}_n \iff \mathbf{b}_1 = -a_1^{-1}(a_2\mathbf{b}_2 + \dots + a_n\mathbf{b}_n).$$

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

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

For instance, taking $S = V$ gives $\text{span}(S) = V$. 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 $\text{span}(S) = V$.

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 \emptyset 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 $\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_n \in \mathcal{B}$ and scalars $a_1, a_2, \dots, a_n \in F$,

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

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

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

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 exists a unique sequence of scalars $\{a_n\}_{n=1}^{\infty} \subseteq F$ such that

$$x = \sum_{i=1}^{\infty} (a_i \cdot x_i),$$

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

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 set. A binary relation \leq on S (i.e., $\leq \subseteq S \times S$) is called a **partial order** if it satisfies the following three axioms for all $a, b, c \in X$,

- (i) (Reflexivity) $a \leq a$;
- (ii) (Anti-symmetry) $a \leq b$ and $b \leq a \implies a = b$;
- (iii) (Transitivity) $a \leq b$ and $b \leq c \implies a \leq c$.

Note. A **partially ordered set (POSET)** is an (S, \leq) , where S is a set and \leq 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 :

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

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

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

Note. A **totally ordered set (TOSET)** is a poset (S, \leq) in which the relation \leq is a total order. In other words, (S, \leq) 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, \leq) be a poset.

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

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

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

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

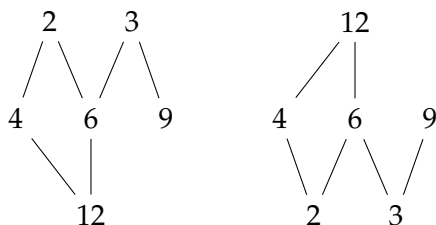
$$\forall a \in P, \quad (a \leq m) \implies (a = m).$$

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., $x \leq y \iff x \mid y$). See the Hasse diagram:

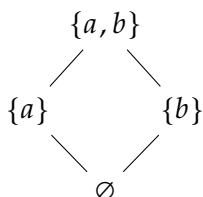


In this example, the minimal elements here are: $\{2, 3\}$.

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

$$\{\emptyset, \{a\}, \{b\}, \{a, b\}\},$$

partially ordered by “is a subset of.”



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

Chain

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

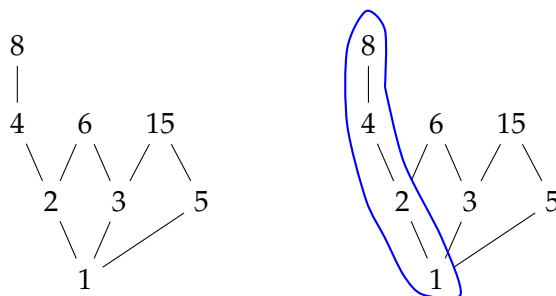
$$\forall a, b \in C, \quad \text{either } a \leq b \text{ or } b \leq a.$$

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:



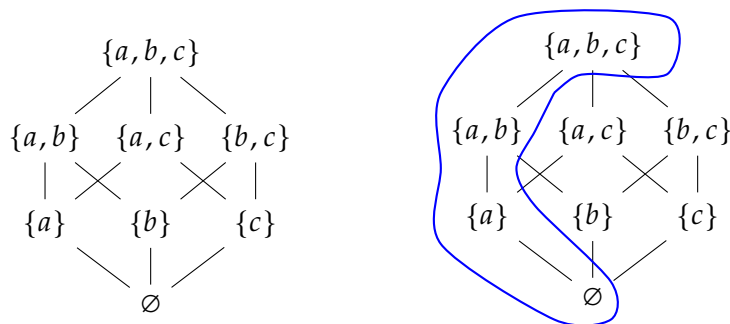
Here, $C = \{1, 2, 4, 8, 16\}$ is a *chain* under divisibility.

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

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

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

$$A \leq B \iff A \subseteq B.$$



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

Zorn's Lemma

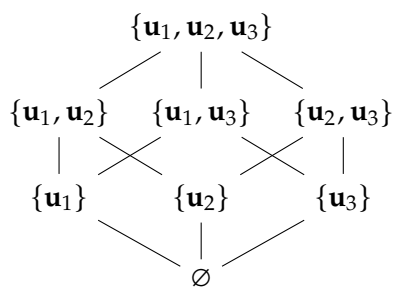
Axiom. Let (P, \leq) be a partially ordered set (poset) with property that every chain $C \subseteq P$ has an upper bound in P ; that is, for every chain $C \subseteq P$,

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

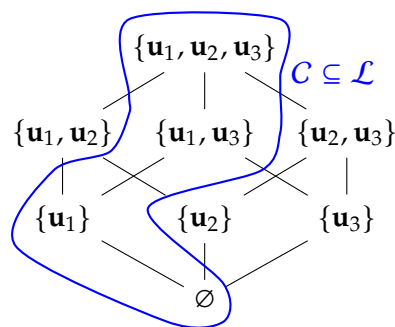
Then P contains at least one maximal element; that is,

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

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

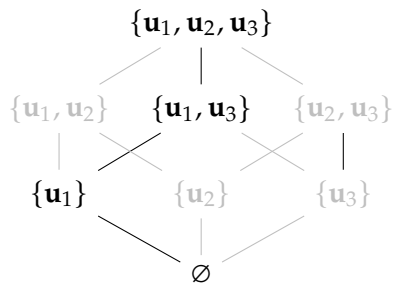


Hasse Diagram for a poset (\mathcal{L}, \subseteq) in \mathbb{R}^3

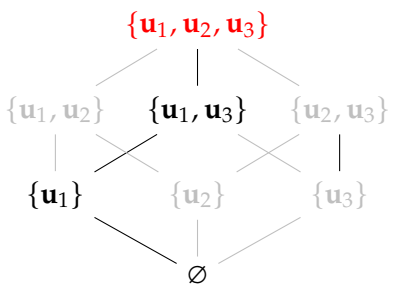


Any chain C

$$U = \emptyset \cup \{u_1\} \cup \{u_1, u_3\} \cup \{u_1, u_2, u_3\}$$



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



Maximal element $\mathcal{B} = \{u_1, u_2, u_3\}$

★ Hamel 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.”

Step 1 Definition of Poset.

Define the set

$$\mathcal{L} := \{S \subseteq V : S \text{ is linearly independent}\}.$$

with the partial order \leq on \mathcal{L} by set inclusion:

$$\forall S, T \in \mathcal{L}, \quad S \leq T \iff S \subseteq T.$$

Since $\emptyset \in \mathcal{L}$, we have $\mathcal{L} \neq \emptyset$. Thus, (\mathcal{L}, \subseteq) forms a poset.

Step 2 Chains and Upper Bounds.

Let $C \subseteq \mathcal{L}$ be any chain, i.e.,

$$\forall S, T \in C, \quad S \subseteq T \text{ or } T \subseteq S.$$

Now, we need to find an upper bound $U \in \mathcal{L}$ of C . Define

$$U := \bigcup_{S \in C} S.$$

Clearly, $U \subseteq V$. We claim that U is linearly independent, i.e., $U \in \mathcal{L}$:

(Proof of $U \in \mathcal{L}$) Let $n \in \mathbb{N}$ and suppose

$$a_1 \mathbf{u}_1 + a_2 \mathbf{u}_2 + \cdots + a_n \mathbf{u}_n = 0 \quad \text{with } a_i \in F, \mathbf{u}_i \in U \text{ for } i = 1, 2, \dots, n.$$

Since $U = \bigcup_{S \in C} S$,

$$\mathbf{u}_i \in U \iff \exists S_i \in C \text{ such that } \mathbf{u}_i \in S_i.$$

for each $i \in \{1, 2, \dots, n\}$. Since C is a chain (totally ordered by inclusion), the sets S_1, S_2, \dots, S_n are comparable. Therefore, there exists at least one set $S^* \in C$ such that

$$(\forall i \in \{1, 2, \dots, n\}, \mathbf{u}_i \in S^*) \quad \text{i.e.,} \quad \{\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_n\} \subseteq S^*.$$

Since S^* is an element of C (and $C \subseteq \mathcal{L}$, where every element is linearly independent), the linear independence of S^* implies that

$$a_1 = a_2 = \cdots = a_n = 0.$$

Thus, U is linearly independent, i.e., $U \in \mathcal{L}$.

By definition of U , we know

$$\forall S \in C, S \subseteq U,$$

and so $U \in \mathcal{L}$ be an upper bound of C .

Step 3 Application of Zorn's Lemma.

Since every chain C in \mathcal{L} has an upper bound $U \in \mathcal{L}$, Zorn's Lemma guarantees the existence of a maximal element $\mathcal{B} \in \mathcal{L}$ such that

$$\forall S \in \mathcal{L}, (\mathcal{B} \subseteq S) \implies (\mathcal{B} = S), \quad \text{i.e.,} \quad \nexists S \in \mathcal{L} \text{ with } \mathcal{B} \subsetneq S.$$

Step 4 \mathcal{B} is a Basis of V .

We now show that \mathcal{B} spans V , i.e., $\text{span } \mathcal{B} = V$. Assume, for contradiction, that

$$\text{span } \mathcal{B} \neq V, \quad \text{i.e.,} \quad \exists \mathbf{v}_0 \in V \setminus \text{span } \mathcal{B}.$$

Consider

$$\mathcal{B}' = \mathcal{B} \cup \{\mathbf{v}_0\}.$$

We NTS that \mathcal{B}' is linearly independent. Suppose that for $n \in \mathbb{N}$, scalars $a_0, a_1, \dots, a_n \in F$ and distinct vectors $\mathbf{v}_0, \mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_n \in \mathcal{B}'$, the followings holds:

$$a_0 \mathbf{v}_0 + (a_1 \mathbf{b}_1 + a_2 \mathbf{b}_2 + \cdots + a_n \mathbf{b}_n) = 0.$$

(Case I) If $a_0 = 0$, then

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

and since \mathcal{B} is linearly independent, $a_i = 0$ for $i = 1, 2, \dots, n$.

(Case II) If $a_0 \neq 0$, then

$$\mathbf{v}_0 = -\frac{1}{a_0}(a_1 \mathbf{b}_1 + a_2 \mathbf{b}_2 + \cdots + a_n \mathbf{b}_n) \in \text{span } \mathcal{B},$$

which contradicts the assumption that $\mathbf{v}_0 \notin \text{span } \mathcal{B}$.

Thus, in all cases,

$$a_0 = a_1 = \cdots = a_n = 0.$$

Hence, \mathcal{B}' is linearly independent, i.e., $\mathcal{B}' \in \mathcal{L}$, and $\mathcal{B} \subseteq \mathcal{B}'$, contradicting the maximality of \mathcal{B} .

□

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

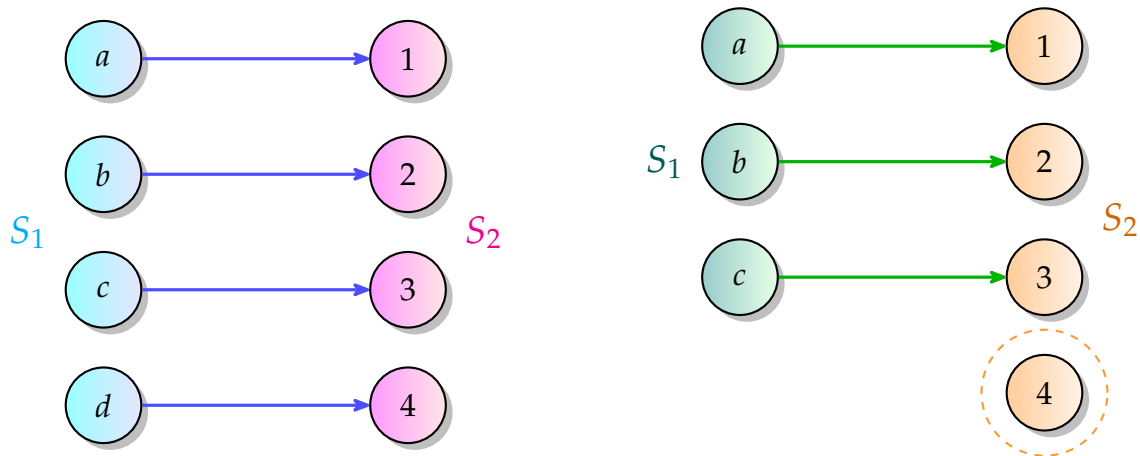
$$|S_1| = |S_2|$$

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

(2) (Strict Inequality of Cardinalities) We write

$$|S_1| < |S_2|$$

if and only if there exists an injective (one-to-one) function $f : S_1 \rightarrow S_2$ 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) $\mathcal{X} = \{\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_m\} \subseteq V$ is a linearly independent set, and
- (ii) $\mathcal{Y} = \{\mathbf{y}_1, \mathbf{y}_2, \dots, \mathbf{y}_n\} \subseteq V$ is a spanning set of V , i.e., $\text{span } \mathcal{Y} = V$.

Then

$$|\mathcal{X}| \leq |\mathcal{Y}|,$$

that is, there exists an injective function $f : \mathcal{X} \rightarrow \mathcal{Y}$.

Proof. TBA

□

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

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

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

□

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.

References

- [1] 수학의 즐거움, Enjoying Math. “수학 공부, 기초부터 대학원 수학까지, 14. 선형대수학 (a) 벡터공간의 정의와 초론의 보조정리” YouTube Video, 27:20. Published October 8, 2019. URL: <https://www.youtube.com/watch?v=esLn0FeedyQ>.
- [2] 수학의 즐거움, Enjoying Math. “수학 공부, 기초부터 대학원 수학까지, 15. 선형대수학 (b) 벡터공간의 기저의 존재성과 차원” YouTube Video, 24:41. Published October 10, 2019. URL: https://www.youtube.com/watch?v=oGC_BU5Erkk&t=875s.
- [3] Wikipedia, The Free Encyclopedia. “Steinitz exchange lemma.” Wikipedia Article. Accessed February 25, 2025. URL: https://en.wikipedia.org/wiki/Steinitz_exchange_lemma.