Linear Algebra I

– Proof for Existence of Basis –

Ji, Yong-hyeon

July 8, 2025

Zorn's Lemma

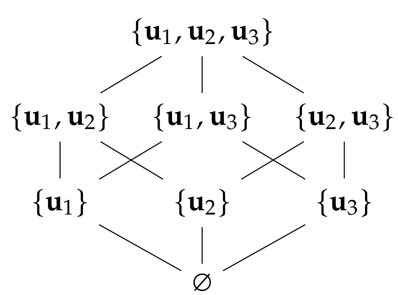
Axiom. Let $(P, \preceq)$ be a nonempty partially ordered set with property that every chain $C \subseteq P$ has an upper bound in P; that is, for every chain $C \subseteq P$,

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

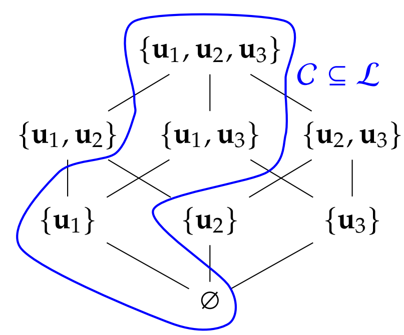
Then P contains at least one maximal element; that is,

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

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

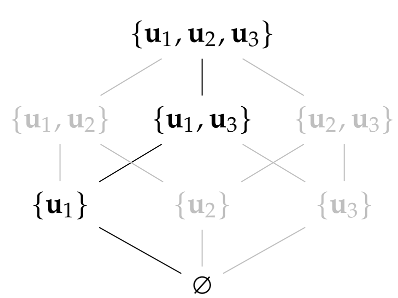


Hasse Diagram for a poset $(\mathcal{L}, \subseteq)$ in $\mathbb{R}^3$

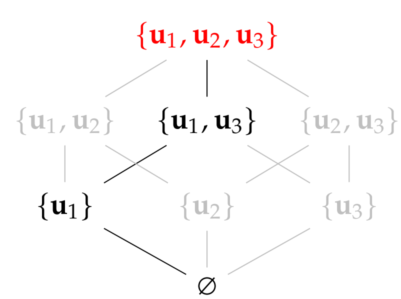


Any chain C

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



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."

Step 1 **Definition of Poset.** Define the set

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

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

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

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

Step 2 **Chains and Upper Bounds.** Let $\mathcal{C} \subseteq \mathcal{L}$ be any chain, i.e.,

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

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

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

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

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

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

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

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

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

Since S^* is an element of $\mathcal{C}$ (and $\mathcal{C} \subseteq \mathcal{L}$, 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

$$\forall S \in \mathcal{C},\ S \subseteq U,$$

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

Step 3 **Application of Zorn's Lemma.**

Since every chain $\mathcal{C}$ 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., $\operatorname{span} \mathcal{B} = V$. Assume, for contradiction, that

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

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 $a_0, a_1, \cdots, a_n \in F$ and distinct vectors $\mathbf{v}_0, \mathbf{b}_1, \mathbf{b}_2, \cdots, \mathbf{b}_n \in \mathcal{B}'$, 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 $i = 1, 2, \ldots, n$.

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

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

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

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 $\mathcal{B}$.

$\square$

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.