# Lecture 1: Vector spaces

## Field

**Definition:** A field is a set $F$ along with two binary operations: $+$ (addition) and $\cdot$ (multiplication) such that:

- For $\forall\, x, y \in F$, $x+y = y+x$ and $x \cdot y = y \cdot x$
- For $\forall\, x, y, z \in F$, $(x+y)+z = x+(y+z)$ and $(x \cdot y) \cdot z = x \cdot (y \cdot z)$
- For $\forall\, x, y, z \in F$, $x \cdot (y+z) = x \cdot y + x \cdot z$
- $\exists!$ element $0 \in F \ni \forall\, x \in F$, $x + 0 = x$
- $\exists!$ element $1 \in F \ni \forall\, x \in F$, $x \cdot 1 = x$
- For $\forall\, x \in F$, $\exists$ an element $(-x) \in F \ni x + (-x) = 0$
- For $\forall\, x \in F$ (excluding $x = 0$), $\exists$ an element $x^{-1} \in F \ni x \cdot x^{-1} = 1$

**Remark:**
- We often write $xy$ for $x \cdot y$
- If $F$ is finite, we say it is a finite field

## Examples of field

1. $F = \mathbb{R}$
2. $F = \mathbb{C}$

} Most often considered in Math 2048.

3. $F = \{\text{Rational numbers}\} = \{ p/q : p, q \in \mathbb{Z} \}$
4. Finite field of order $p$ (where $p$ is a prime number)

Define $F_p = \{0, 1, 2, \ldots, p-1\}$ and $+ / \cdot$ are defined as:

$+$ : for $\forall x, y \in F_p$, $x + y$ are performed modulo $p$.

That is, $x+y$ is the remainder of $(x+y)/p$

$\cdot$ : for $\forall x, y, \in F_p$, $x \cdot y$ is the remainder of $x \cdot y / p$.

$F_2 = \{0, 1\}$ is the binary field (important for information theories)

# Vector Space

Goal: Build an abstract space (space of objects) simulating $\mathbb{R}^n$ or $\mathbb{C}^n$ (with addition and multiplication / scaled)

Definition: A vector space over $F$ is a set $V$ equipped w/ two operations:

(addition) $+ : V \times V \to V$ , $(\underset{V}{\vec{x}}, \underset{V}{\vec{y}}) \mapsto \vec{x} + \vec{y} \in V$

(scalar multiplication) $\cdot : F \times V \to V$ , $(\underset{F}{a}, \underset{V}{\vec{x}}) \mapsto a\vec{x} \in V$

satisfying 8 properties:

$+$

(VS1) : $\vec{x} + \vec{y} = \vec{y} + \vec{x} \quad \forall \vec{x}, \vec{y} \in V$

(VS2) : $(\vec{x} + \vec{y}) + \vec{z} = \vec{x} + (\vec{y} + \vec{z}) \quad \forall \vec{x}, \vec{y}, \vec{z} \in V$

(VS3) : $\exists\, \vec{0} \in V$ s.t. $\vec{x} + \vec{0} = \vec{x} \quad \forall \vec{x} \in V$

(VS4) : $\forall \vec{x} \in V, \ \exists\, \vec{y} \in V$ s.t. $\vec{x} + \vec{y} = \vec{0}$ (inverse)

$\cdot$

(VS5) : $\underset{\substack{\uparrow \\ F}}{1}\,\vec{x} = \vec{x} \quad \forall \vec{x} \in V$

(VS6) : $(\underset{\substack{\uparrow \\ F}}{a}\,\underset{\substack{\uparrow \\ F}}{b})\vec{x} = a(b\vec{x}) \quad \forall a, b \in F, \ \forall \vec{x} \in V$

$+/\cdot$

(VS7) : $\underset{\substack{\uparrow \\ F}}{a}\,(\underset{\substack{\uparrow \\ V}}{\vec{x}} + \underset{\substack{\uparrow \\ V}}{\vec{y}}) = a\vec{x} + a\vec{y} \quad \forall a \in F, \ \forall \vec{x}, \vec{y} \in V$

(VS8) : $(a + b)\vec{x} = a\vec{x} + b\vec{x} \quad \forall a, b \in F, \ \forall \vec{x} \in V$

Remark: an element in $F$ is called scalar.
an element in $V$ is called vector.

## Examples of vector spaces

- $F^n = \{(x_1, x_2, \ldots, x_n) : x_j \in F \text{ for } j = 1, 2, \ldots, n\}$ w/

$$(x_1, x_2, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n)$$

$$a(x_1, \ldots, x_n) = (ax_1, ax_2, \ldots, ax_n)$$

- $M_{m \times n}(F) = \{ m \times n$ matrices w/ entries in $F\}$
w/ matrix addition and scalar multiplication

- $P(F) = \{$polynomials w/ coefficients in $F\}$
w/ polynomial addition and scalar multiplication.

- $F^\infty = \{(x_1, x_2, \ldots) : x_j \in F, j = 1, 2, \ldots\}$
w/ component-wise addition and scalar multiplication.

- $\mathrm{Sym}_{n\times n}(F) = \{\, n \times n$ symmetric matrices $A$ w/ entries in $F$ : $A^T = A \,\}$

- Let $S$ be any non-empty set.

  Then: $\mathcal{F}(S, F) = \{$ functions $f : S \to F \}$

  is a vector space over $F$ under:

  $$(\underset{\mathcal{F}(S,F)}{f} + \underset{\mathcal{F}(S,F)}{g})(\overset{\in S}{s}) \overset{\text{def}}{=} f(s) + g(s)\,; \qquad (\underset{F}{a} f)(s) \overset{\text{def}}{=} a f(s).$$

- $\mathbb{C}$ is a vector space over $F = \mathbb{C}$

<u>Question</u>: Is $V = \mathbb{R}$ a vector space over $F = \mathbb{C}$ ??

- Consider the differential equation:

$$(*) \quad \frac{d^2y}{dx^2} + a\frac{dy}{dx} + by = 0 \qquad (a, b \in \mathbb{R})$$

Let $S$ be the set of twice differentiable functions on $\mathbb{R}$ satisfying $(*)$.

Then $S$ is a vector space under usual addition and scalar multiplication is a vector space.

**Proposition:** Let $V$ be a vector space over $F$. Then:

(a) The element $\vec{0}$ in (VS3) is unique, called <u>zero vector</u>

(b) $\forall \vec{x} \in V$, the element $\vec{y}$ in (VS4) is unique, called the <u>additive inverse</u> (Denoted as $-\vec{x}$)

(c) $\vec{x} + \vec{z} = \vec{y} + \vec{z} \Rightarrow \vec{x} = \vec{y}$ (Cancellation law)

(d) $\underset{\underset{F}{\uparrow}}{0}\vec{x} = \vec{0} \quad \forall \vec{x} \in V$

(e) $\underset{\underset{F}{\uparrow}}{(-a)}\vec{x} = -(a\vec{x}) = a(-\vec{x}), \quad \forall a \in F, \ \forall \vec{x} \in V$

(f) $\underset{\underset{F}{\uparrow}}{a}\vec{0} = \vec{0} \quad \forall a \in F$

## Subspace

**Definition:** A subset $W$ of a vector space $V$ over a field $F$ is called a subspace of $V$ if $W$ is a vector space over $F$ under the same addition and scalar multiplication inherited from $V$.

**Proposition:** Let $V$ be a vector space $V$ over $F$. A subset $W \subset V$ is a subspace iff the following 3 conditions hold:

(a) $\vec{0}_V \in W$

(b) $\vec{x} + \vec{y} \in W$, $\forall \vec{x}, \vec{y} \in W$ (closed under $+$)

(c) $a\vec{x} \in W$, $\forall a \in F$, $\forall \vec{x} \in W$ (closed under $\cdot$)

Examples:

- For any vector space $V / F$,

  $\{\vec{0}\} \subset V$ ; $V \subset V$ (trivial subspaces)

  "zero subspace"

- For $V = M_{n \times n}(F)$,

  $\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \in W_1 = \{\text{diagonal matrices}\} \subset V$ subspace

  $W_2 = \{A \in M_{n \times n}(F) : \det(A) = 0\} \subset V$

  is NOT subspace.

  $\left(\det(A+B) \neq \det(A) + \det(B)\right)$

  $+$

  $\begin{pmatrix} 1 & 2 \\ 2 & -1 \end{pmatrix} \in W_3 = \{A \in M_{n \times n}(F) : \mathrm{tr}(A) = 0\} \subset V$

  subspace

  $= \begin{pmatrix} 3 & 2 \\ 2 & 1 \end{pmatrix}$

- For $V = P(F)$

$P_n(F) \overset{\text{def}}{=} \{ f \in P(F) : \deg(f) \le n \}$ is a subspace

$W \overset{\text{def}}{=} \{ f \in P(F) : \deg(f) = n \}$ is NOT subspace.

- Consider $V = F^n = \{ \underset{\vec{x}^T}{\underset{\parallel}{(x_1, x_2, \dots, x_n)}} : x_j \in F \text{ for } j = 1, 2, \dots, n \}$

Consider linear system:

$$\left\{ \begin{array}{l} a_{11} x_1 + a_{12} x_2 + \cdots + a_{1n} x_n = b_1 \\ a_{21} x_1 + \cdots \quad\quad\quad + a_{2n} x_n = b_2 \\ \quad\quad\quad \vdots \quad\quad\quad\quad\quad\quad \vdots \\ a_{m1} x_1 + a_{m2} x_2 + \cdots + a_{mn} x_n = b_m \end{array} \right. \iff A\vec{x} = \vec{b}$$

gives a subset, the solution set $S \subset V$

Is $S$ a subspace?

Yes if $(b_1, b_2, \dots, b_m) = \vec{0}$ (Null space / kernel)

No if $(b_1, b_2, \dots, b_m) \neq \vec{0}$ $\left( \begin{array}{l} A\vec{x} = \vec{b} \\ A\vec{y} = \vec{b} \end{array} \Rightarrow A(\vec{x} + \vec{y}) = 2\vec{b} \right)$

**Theorem:** Any intersection of subspaces of a vector space $V$ is a subspace of $V$.

**Question:** $W_1$ = subspace ; $W_2$ = subspace

$$\Downarrow$$

$W_1 \cap W_2$ is subspace

Is $W_1 \cup W_2$ a subspace ?? No general.

$$W_1 = \{ 2\times 2 \text{ diagonal matrix} \} \subset M_{2\times 2}(\mathbb{R})$$

$$W_2 = \{ 2\times 2 \text{ matrices } A : tr(A) = 0 \} \subset M_{2\times 2}(\mathbb{R})$$

Is $W_1 \cup W_2$ a subspace of $M_{2\times 2}(\mathbb{R})$ ??

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in W_1 \cup W_2 \quad \checkmark$$

$$\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \in W_1 \cup W_2 \quad , \quad \begin{pmatrix} 1 & -2 \\ 2 & -1 \end{pmatrix} \in W_1 \cup W_2$$

$$\begin{pmatrix} 3 & -2 \\ 2 & 1 \end{pmatrix} \notin W_1 \cup W_2$$

# Linear combination and Span

**Definition:** Let $V$ be a vector space over $F$ and $S \subset V$ a non-empty subset.

- We say a vector $\vec{v} \in V$ is a <u>linear combination</u> of vectors of $S$ if $\exists\ \vec{u}_1, \vec{u}_2, \ldots, \vec{u}_n \in S$ and $a_1, a_2, \ldots, a_n \in F$ such that:

$$\vec{v} = a_1\vec{u}_1 + a_2\vec{u}_2 + \ldots + a_n\vec{u}_n.$$

**Remark:** $\vec{v}$ is usually called a linear combination of $\vec{u}_1, \ldots, \vec{u}_n$ and $a_1, \ldots, a_n$ are the coefficients of the linear combination.

- The <u>span</u> of $S$, denoted as $\mathrm{Span}(S)$, is the set of all linear combination of vectors of $S$.

$$\mathrm{Span}(S) \overset{\text{def}}{=} \{ a_1\vec{u}_1 + a_2\vec{u}_2 + \ldots + a_n\vec{u}_n : a_j \in F,\ \vec{u}_j \in S \text{ for } j = 1, 2, \ldots, n,\ n \in \mathbb{N} \}$$

**Remark:** • By convention, $\operatorname{span}(\underset{\substack{\shortparallel \\ \text{empty set}}}{\phi}) \overset{\text{def}}{=} \{\vec{0}\}$.

e.g. $1 \in \operatorname{Span}\left(\{1+x^2,\ 1-x^2\}\right)$

$\cancel{\checkmark}$

$\times$

Example:

- $F^n = \operatorname{Span}(\{\vec{e}_1, \vec{e}_2, \ldots, \vec{e}_n\})$ where $\vec{e}_j = (0, 0, \cdots, \underset{\substack{\uparrow \\ j^{th}}}{1}, 0, \ldots 0)$

- $P(F) = \operatorname{Span}(\{1, x, x^2, \ldots, x^n, \ldots\})$

- $M_{n\times n}(F) = \operatorname{Span}(S)$

$$S = \left\{ E_{ij} \stackrel{\text{def}}{=} \begin{array}{cl} \begin{matrix} \phantom{0} & \phantom{0} & & j^{th} & \phantom{0} \end{matrix} & \\ \begin{pmatrix} 0 & 0 & \cdots & \cdots & 0 \\ 0 & \cdots & \cdots & & 0 \\ 0 & \cdots & 1 & & 0 \\ & & & & \\ 0 & \cdots & & & 0 \end{pmatrix} & \begin{matrix} \\ \\ \leftarrow i^{th} \\ \\ \\ \end{matrix} \end{array} : 1 \le i, j \le n \right\}$$

- Given $\vec{u}_1 = \begin{pmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{n1} \end{pmatrix}$, $\vec{u}_2 = \begin{pmatrix} a_{12} \\ a_{22} \\ \vdots \\ a_{n2} \end{pmatrix}$, $\ldots$, $\vec{u}_n = \begin{pmatrix} a_{1n} \\ a_{2n} \\ \vdots \\ a_{nn} \end{pmatrix}$

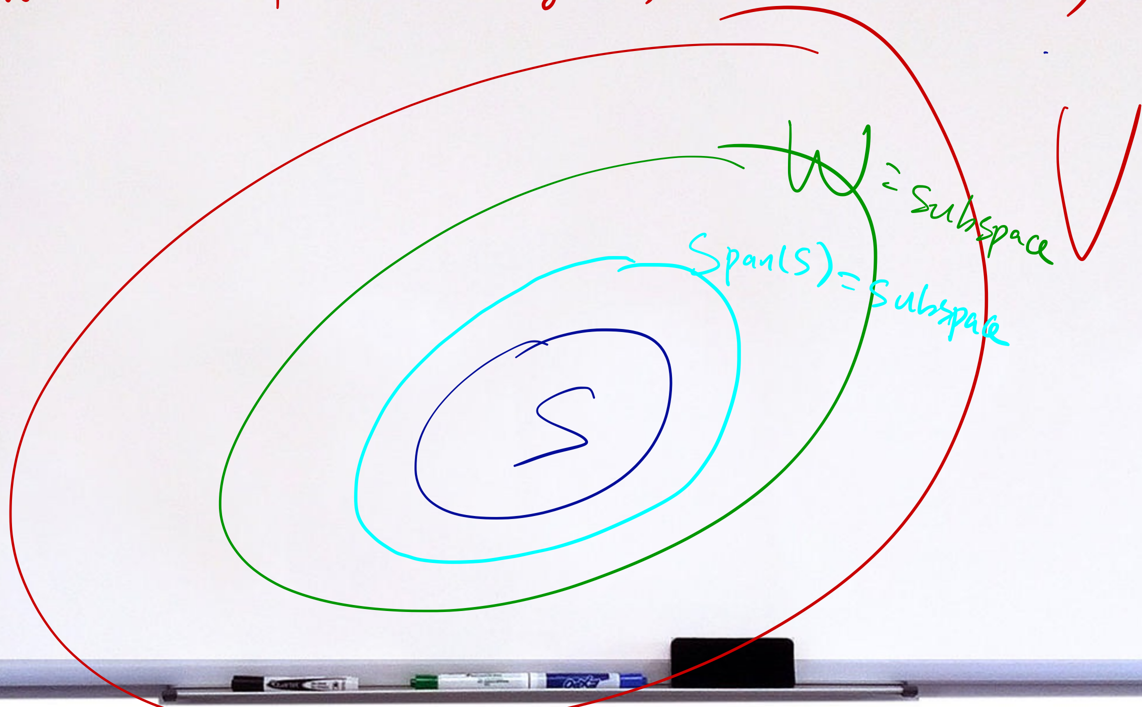
Then: $\underset{\begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix}}{\vec{v}} \in \operatorname{Span}(\{\vec{u}_1, \vec{u}_2, \ldots, \vec{u}_n\})$ iff

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = v_1 \\ a_{21}x_1 + \cdots + a_{2n}x_n = v_2 \\ \vdots \\ a_{n1}x_1 + \cdots + a_{nn}x_n = v_n \end{cases}$$

has a sol.

**Theorem:** Let $S \subset V$ be a subset of a vector space $V$ over $F$.
Then, span$(S)$ is the smallest[1] subspace[2] of $V$ consisting $S$.

( If $W$ is a subspace containing $S$, then $\text{span}(S) \subset W$ )



## Linear independence

**Definition:** Let $V$ be a vector space over $F$. A subset $S \subset V$ is said to be linearly dependent if $\exists$ distinct $\vec{u}_1, \vec{u}_2, \ldots, \vec{u}_n \in S$ and scalars $a_1, a_2, \ldots, a_n \in F$, not all zero, s.t.

$$a_1\vec{u}_1 + a_2\vec{u}_2 + \cdots + a_n\vec{u}_n = \vec{0}$$

Otherwise, it is said to be linearly independent.

e.g.

- The empty set $\phi \subset V$ is linearly independent.
- If $\vec{0} \in S$, the $S$ is linearly dependent $\left( \underset{\in S}{5\vec{0}} = \vec{0} \right)$
- If $S = \{\vec{u}\}$ and $\vec{u} \neq \vec{0}$, then $S$ is linearly independent. $\left( \begin{array}{c} \lambda \underset{\neq \vec{0}}{\vec{u}} = \vec{0} \\ \Rightarrow \lambda = 0 \end{array} \right)$

Proposition: Let $S \subset V$ be a subset of a vector space $V$. Then, the following are equivalent.

(1) $S$ is linearly independent

(2) Each $\vec{x} \in \text{span}(S)$ can be expressed in a unique way as a linear combination of vectors of $S$.

(3) The only representations of $\vec{0}$ as linear combinations of vectors of $S$ are trivial representations, i.e., if

$$\vec{0} = a_1 \vec{u}_1 + \dots + a_n \vec{u}_n \text{ for}$$

some $\vec{u}_1, \vec{u}_2, \dots, \vec{u}_n \in S$, $a_1, a_2, \dots, a_n \in F$, then we must have $a_1 = a_2 = \dots = a_n = 0$

**Example:** • For $k=0,1,2,\ldots,n$, let $f_k(x) = 1 + x + x^2 + \ldots + x^k$.

Then: $S = \{f_0(x), f_1(x), f_2(x), \ldots, f_n(x)\} \subset P_n(F)$ is a linearly independent subset.

$$0 = \vec{0} = a_0 f_0(x) + a_1 f_1(x) + \ldots + a_n f_n(x)$$

$$= a_0 + a_1(1+x) + a_2(1+x+x^2) + \ldots + a_n(1+x+\ldots+x^n)$$

$$= (a_0 + a_1 + \ldots + a_n)1 + (a_1 + a_2 + \ldots + a_n)x$$

$$+ (a_2 + a_3 + \ldots + a_n)x^2 + \ldots + a_n x^n$$

$$\left\{\begin{array}{l} a_0 + a_1 + \ldots + a_n = 0 \\ \quad a_1 + \ldots + a_n = 0 \\ \qquad a_2 + \ldots + a_n = 0 \\ \qquad\quad \vdots \\ \qquad\qquad a_n = 0 \end{array}\right. \Rightarrow a_1 = a_2 = \ldots = a_n = 0.$$

**Theorem:** Let $S$ be a linearly independent subset of a vector space $V$. Let $\vec{v} \in V \setminus S$. Then: $S \cup \{\vec{v}\}$ is linearly dependent iff $\vec{v} \in \operatorname{Span}(S)$.

**Definition:** A basis for a vector space $V$ is a subset $\beta \subset V$ such that:

- $\beta$ is linearly independent and
- $\beta$ spans $V$, i.e. $\mathrm{Span}(\beta) = V$.

e.g.

- $F^n$: $\{\vec{e}_1 = (1,0,\dots,0), \vec{e}_2 = (0,1,0,\dots,0), \dots, \vec{e}_i = (0,\dots,0,\overset{\overset{i\text{-th}}{\downarrow}}{1},0\dots0), \dots, \vec{e}_n = (0,0,\dots,1)\}$ is a basis for $F^n$. (Standard basis)
- $M_{2\times 2}(F)$: $\left\{ \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & -2 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 2 \end{pmatrix} \right\} \subset M_{2\times 2}(F)$ is a basis for $M_{2\times 2}(F)$
- $\{1, x, x^2, \dots, x^n\}$ is a basis for $P_n(F)$
- $\{1, x, x^2, \dots\}$ is a basis for $P(F)$.

<u>Theorem</u>: Let $V$ be a vector space and $\beta = \{\vec{u}_1, \vec{u}_2, \dots, \vec{u}_n\} \subset V$.

Then: $\beta$ is basis for $V$ if and only if: $\forall \vec{v} \in V$, $\exists!$ (unique)

(for all) (in) (there exist)

$a_1, a_2, \dots, a_n \in F$ such that:

$$\vec{v} = a_1 \vec{u}_1 + a_2 \vec{u}_2 + \dots + a_n \vec{u}_n.$$

---

$V$ with $\beta = \{$  ,  ,  $\}$

$\in V$

Pineapple is associated with a unique 2, 3, 4 such that

Pineapple = 2  + 3  + 4 

$$\text{Pineapple} \longleftrightarrow \begin{pmatrix} 2 \\ 3 \\ 4 \end{pmatrix} \in \mathbb{R}^3$$

**Lemma:** Let $S$ be a linearly dependent subset of a vector space $V$.

Then: $\exists \vec{v} \in S$ such that $\mathrm{span}(S \setminus \{\vec{v}\}) = \mathrm{span}(S)$.

**Theorem:** Suppose $S$ is a finite spanning set for a vector space $V$.

Then: $\exists \beta \subset S$ which is a basis for $V$.

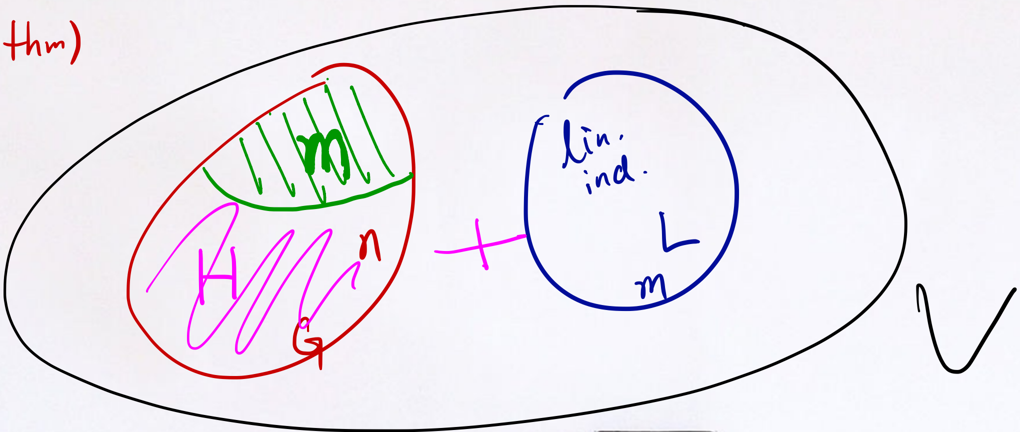
(A finite spanning set can be reduced to a basis)

**Theorem:** Let $V$ be a vector space.

Let $G \subset V$ be a spanning set for $V$ consisting of $n$ vectors.
and $L \subset V$ be a linearly independent subset consisting of $m$ vectors.

Then, $m \leq n$ and $\exists\, H \subset G$ consisting of exactly $n-m$ vectors
such that $L \cup H$ spans $V$.

(Replacement thm)



## Dimension

**Cor 1:** Let $V$ be a vector space having a finite basis. Then, every basis of $V$ contains the same number of vectors.

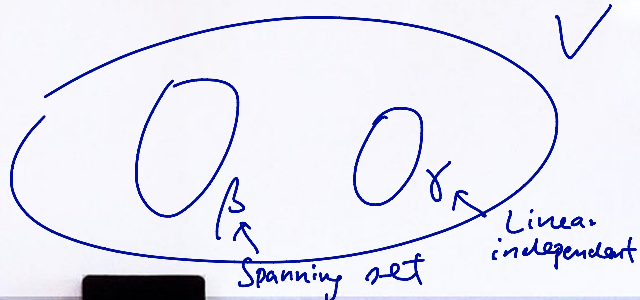
**Pf:** Let $\beta$ and $\gamma$ be two bases of $V$.

Since $\beta$ spans $V$ and $\gamma$ is lin. independent,

then $|\gamma| \le |\beta|$ (by replacement Thm)

Similarly, $|\beta| \le |\gamma|$

$\Rightarrow |\gamma| = |\beta|$.



**Definition:** A vector space $V$ is called <u>finite-dimensional</u> if it has a finite basis. The <u>dimension</u> of $V$, denoted as $\dim(V)$, is the number of vectors in a basis for $V$.

A vector space which is not finite-dimensional is called <u>infinite-dimensional</u>

**Example:**
- $F^n$ is $n$-dimensional
- $\mathcal{F}(\mathbb{R}, \mathbb{R})$ is infinite-dimensional