Linear independence

Definition: A set of vectors X is *linearly independent*, if the zero vector *cannot* be expressed as a nontrivial linear combination of vectors from X; otherwise it is *linearly dependent*.

Formally: vectors $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ are linearly independent if and only if $\sum_{i=1}^{n} a_i \boldsymbol{v}_i = \mathbf{0}$ has only trivial solution $a_1 = \cdots = a_n = 0$

Observation: If $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ are linearly dependent, then $\sum_{i=1}^{n} a_i \boldsymbol{v}_i = \mathbf{0}$, where some $a_i \neq 0$. Hence the corresponding $\boldsymbol{v}_i$ can be expressed as a linear combination of the remaining vectors: $\boldsymbol{v}_i = \sum_{j \neq i} -\frac{a_j}{a_i} \boldsymbol{v}_j$.

Examples

- When $\mathbf{0} \in X$ then X is linearly dependent as $1 \cdot \mathbf{0} = \mathbf{0}$ is a nontrivial linear combination.
- Rows or columns of $\boldsymbol{I}_n$ are linearly independent.
- Rows of a matrix in row echelon form are linearly independent.
- In $\mathbb{R}^2$: $X = \{\boldsymbol{v}\}$ is linearly independent iff $\boldsymbol{v} \neq \mathbf{0}$;
  The set $Y = \{\boldsymbol{u}, \boldsymbol{v}\}$ is linearly independent iff
  the line determined by $\boldsymbol{u}$ and $\boldsymbol{v}$ does not contain the origin.
  Any Z of size at least three is linearly dependent.
- In the vector space of real polynomials, the infinite set $\{x^0, x^1, x^2, \dots\}$ is linearly independent.
- The empty set is linearly independent.

Two distinct tests of linear independence in $\mathbb{K}^n$

Is the following set X linearly independent in $\mathbb{Z}_5^4$?
$X = \{(2,1,0,3)^T, (4,3,1,4)^T, (0,2,2,1)^T, (3,4,1,0)^T, (0,2,2,2)^T\}$

a) By using the fact that elementary operations do not modify the *row space*:

$$\begin{pmatrix} 2 & 1 & 0 & 3 \\ 4 & 3 & 1 & 4 \\ 0 & 2 & 2 & 1 \\ 3 & 4 & 1 & 0 \\ 0 & 2 & 2 & 2 \end{pmatrix} \sim \cdots \sim \begin{pmatrix} 2 & 1 & 0 & 3 \\ 0 & 1 & 1 & 3 \\ 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

We have obtained the zero row. In other words,
the zero vector can be obtained as a nontrivial linear combination,
hence X is linearly dependent.

b) By finding a nontrivial solution of $a_1\boldsymbol{v}_1 + \cdots + a_n\boldsymbol{v}_n = \mathbf{0}$.

We obtain a homogeneous system with the matrix:

$$\begin{pmatrix} 2 & 4 & 0 & 3 & 0 \\ 1 & 3 & 2 & 4 & 2 \\ 0 & 1 & 2 & 1 & 2 \\ 3 & 4 & 1 & 0 & 2 \end{pmatrix} \sim \cdots \sim \begin{pmatrix} 2 & 4 & 0 & 3 & 0 \\ 0 & 1 & 2 & 0 & 2 \\ 0 & 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

The resulting matrix *contains at least one free variable*: a_3.
Hence the system has also a nontrivial solution, e.g.:

$$4(2,1,0,3)^T + 3(4,3,1,4)^T + (0,2,2,1)^T = \mathbf{0}$$

Consequently, X is linearly dependent.

Properties

Observation: If X is linearly independent and $Y \subseteq X$ then Y is linearly independent.

Observation: If Y is linearly dependent and $Y \subseteq X$ then X is linearly dependent.

Observation: A set X is linearly independent if and only if $\forall \boldsymbol{v} \in X : \boldsymbol{v} \notin \mathcal{L}(X \setminus \boldsymbol{v})$.

Proof: $\boldsymbol{v} \in \mathcal{L}(X \setminus \boldsymbol{v}) \Leftrightarrow \boldsymbol{v} = \sum_{i=1}^{n} a_i \boldsymbol{v}_i$ where $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n \in X \setminus \boldsymbol{v}$.

Proposition: If Y is finite generating set of a space V and X is linearly independent in V, then $|X| \leq |Y|$.

Proof: By contradiction. Assume that $Y = \{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\}$. Choose distinct $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_{n+1} \in X$. Express each $\boldsymbol{u}_i$ as $\boldsymbol{u}_i = \sum_{j=1}^{n} a_{i,j} \boldsymbol{v}_j$.

The corresponding matrix $\boldsymbol{A}$ has $n+1$ rows and n columns, hence some row is a linear combination of the others. This combination yields also linear dependence of $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_{n+1}$.

Properties

Observation: If X is linearly independent and $Y \subseteq X$ then Y is linearly independent.

Observation: If Y is linearly dependent and $Y \subseteq X$ then X is linearly dependent.

Observation: A set X is linearly independent if and only if $\forall \boldsymbol{v} \in X : \boldsymbol{v} \notin \mathcal{L}(X \setminus \boldsymbol{v})$.

Proof: $\boldsymbol{v} \in \mathcal{L}(X \setminus \boldsymbol{v}) \Leftrightarrow \boldsymbol{v} = \sum_{i=1}^{n} a_i \boldsymbol{v}_i$ where $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n \in X \setminus \boldsymbol{v}$.

Proposition: If Y is finite generating set of a space V and X is linearly independent in V, then $|X| \leq |Y|$.

Proof: By contradiction. Assume that $Y = \{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\}$. Choose distinct $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_{n+1} \in X$. Express each $\boldsymbol{u}_i$ as $\boldsymbol{u}_i = \sum_{j=1}^{n} a_{i,j} \boldsymbol{v}_j$.

Formally: $\exists \boldsymbol{b} = (b_1, \ldots, b_{n+1})^T \in \mathbb{K}^{n+1}$: $\boldsymbol{b}^T \boldsymbol{A} = \boldsymbol{0}^T \Rightarrow$

$$\sum_{i=1}^{n+1} b_i \boldsymbol{u}_i = \sum_{i=1}^{n+1} b_i \sum_{j=1}^{n} a_{i,j} \boldsymbol{v}_j = \sum_{j=1}^{n} \left(\sum_{i=1}^{n+1} b_i a_{i,j} \right) \boldsymbol{v}_j = \sum_{j=1}^{n} 0 \boldsymbol{v}_j = \boldsymbol{0}$$

Basis

Definition: A *basis* of a vector space V is
a linearly independent set X that generates V.

Why is the concept of a basis so important?

- $\mathcal{L}(X) = V$ imply that every vector of V
  is a linear combination of vectors of the basis X
- X is linearly independent, hence the above linear combination
  is *unique* for each vector of V.

Proof: If X is linearly independent and $\boldsymbol{u} = \sum_{i=1}^{n} a_i \boldsymbol{v}_i = \sum_{i=1}^{n} b_i \boldsymbol{v}_i$ then
$\boldsymbol{0} = \boldsymbol{u} - \boldsymbol{u} = \sum_{i=1}^{n} (a_i - b_i)\boldsymbol{v}_i \Rightarrow \forall i : a_i = b_i$.

Definition: Let $X = (\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n)$ be an ordered basis of a vector space V over $\mathbb{K}$. The *coordinate vector* of $\boldsymbol{u} \in V$ with respect to the basis X is $[\boldsymbol{u}]_X = (a_1, \ldots, a_n)^T \in \mathbb{K}^n$ where $\boldsymbol{u} = \sum_{i=1}^{n} a_i \boldsymbol{v}_i$.

Examples

- In the arithmetic vector space $\mathbb{K}^n$ the columns $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n$ of $\boldsymbol{I}_n$ form the so called *standard basis* K (aka canonical or natural).
- In $\mathbb{R}^2$, a set $X = \{\boldsymbol{v}_1, \boldsymbol{v}_2\}$ is a basis iff the line determined by $\boldsymbol{v}_1$ and $\boldsymbol{v}_2$ does not contain the origin.
- In the vector space of real polynomials, the infinite set $\{x^0, x^1, x^2, \ldots\}$ is an infinite basis.
- In the vector space $V = \mathcal{P}(X)$ over $\mathbb{Z}_2$ the single-element sets form a basis.

Distinct ways to describe a vector space

Let $V = \{(0,0,0,0)^T, (0,1,2,1)^T, (0,2,1,2)^T, (1,0,1,0)^T, (1,1,0,1)^T, (1,2,2,2)^T, (2,0,2,0)^T, (2,1,1,1)^T, (2,2,0,2)^T, \}$ be a space of arithmetic vectors over $\mathbb{Z}_3$.

(These vectors viewed as 4-letter words over a 3-letter alphabet have the property that any two words differ in at least two symbols.

Similar sets could be used to design error-correcting codes.)

Could V be described more efficiently than by the list of 9 values?

We may observe that these vectors are dependent, e.g. $(0,0,0,0)^T$, $(2,1,1,1)^T = (2,0,2,0)^T + (0,2,1,2)^T$ or $(2,0,2,0)^T = 2 \cdot (1,0,1,0)^T$.

Repetitive removal of dependent vectors leads to a subset which is independent but still generates the entire V.

Namely, V could be generated just by two vectors, e.g. $(0,1,2,1)^T$, and $(1,0,1,0)^T$.

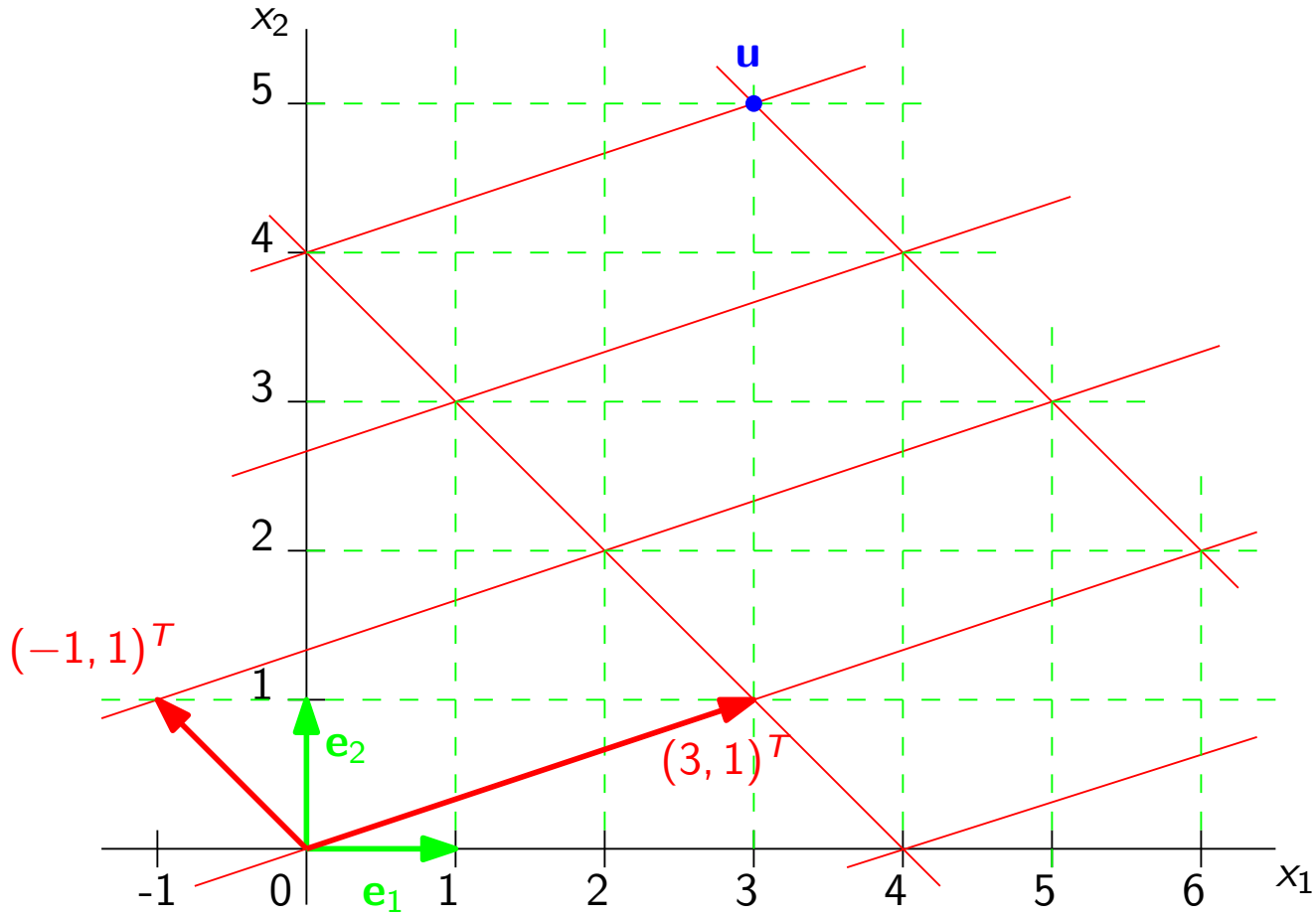
0000	0121	0212
1010	1101	1222
2020	2111	2202

Also, each vector of V is a *unique* linear combination of these two!

Coordinates of a vector with respect to different bases

The coordinates of u with respect to the standard basis $K = \{\boldsymbol{e}_1, \boldsymbol{e}_2\} = \{(1,0)^T, (0,1)^T\}$ are: $\boldsymbol{u} = [\boldsymbol{u}]_K = (3,5)^T$.

With respect to another basis $X = \{(3,1)^T, (-1,1)^T\}$, *the same* vector has the coordinates: $[\boldsymbol{u}]_X = (2,3)^T$.



Existence of a basis

Observation: If $\mathcal{L}(X) = V$ and $\forall \boldsymbol{v} \in X : \boldsymbol{v} \notin \mathcal{L}(X \setminus \boldsymbol{v})$ then X is a basis of V.

Corollary: Every finite generating set Y of a vector space V contains a basis X as a subset.

Proof: First set $X = Y$. Then iteratively test all $\boldsymbol{v} \in X$ whether $\boldsymbol{v} \in \mathcal{L}(X \setminus \boldsymbol{v})$. If so then remove $\boldsymbol{v}$ from X.

Theorem: Every vector space has a basis.

. . . for finitely generated it is proven above, for infinitely generated we omit a proof — it is equivalent with the axiom of choice.

Exchange lemma

Lemma: Let Y generate a vector space V over $\mathbb{K}$. If for a vector $\boldsymbol{u} \in V$ exist $\boldsymbol{v}_1 \ldots, \boldsymbol{v}_n \in Y$ and $a_1, \ldots, a_n \in \mathbb{K}$ such that $\boldsymbol{u} = \sum_{i=1}^{n} a_i \boldsymbol{v}_i$, where $a_i \neq 0$ for some i, then $\mathcal{L}((Y \setminus \boldsymbol{v}_i) \cup \boldsymbol{u}) = V$

Proof: $\boldsymbol{u} = a_1 \boldsymbol{v}_1 + \cdots + a_i \boldsymbol{v}_i + \cdots + a_n \boldsymbol{v}_n \Rightarrow \boldsymbol{v}_i = \frac{1}{a_i}\left(\boldsymbol{u} - \sum_{j \neq i} a_j \boldsymbol{v}_j\right)$.

We can write any $\boldsymbol{w} \in V$ as a linear combination of elements from Y and if $\boldsymbol{v}_i$ occurs in this combination, we substitute the above expression for $\boldsymbol{v}_i$. This way we get $\boldsymbol{w}$ as a linear combination of elements from $(Y \setminus \boldsymbol{v}_i) \cup \boldsymbol{u}$.

In the finite case, if $Y = \{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\}$ and $\boldsymbol{w} = \sum_{j=1}^{n} b_j \boldsymbol{v}_j$

we get $\boldsymbol{w} = \frac{b_i}{a_i} \boldsymbol{u} + \sum_{j \neq i} \left(b_j - \frac{a_j b_i}{a_i}\right) \boldsymbol{v}_j$

Example in $\mathbb{R}^3$

Given a system of generators
$X = \{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_4\} = \{(1,0,0)^T, (0,1,0)^T, (0,0,1)^T, (1,1,0)^T\}$
and vectors $\boldsymbol{u} = (1,1,1)^T$, $\boldsymbol{u}' = (2,1,0)^T$.

If we express: $(1,1,1)^T = (1,0,0)^T + (0,1,0)^T + (0,0,1)^T$,
we see that $\boldsymbol{u}$ could be exchanged with any of $\boldsymbol{v}_1$, $\boldsymbol{v}_2$ or $\boldsymbol{v}_3$.

Similarly, if we express: $(1,1,1)^T = (1,1,0)^T + (0,0,1)^T$,
we see that $\boldsymbol{u}$ could also be exchanged with $\boldsymbol{v}_4$.

On the other hand, any combination
$a_1\boldsymbol{v}_1 + \cdots + a_4\boldsymbol{v}_4 = (a_1 + a_4, a_2 + a_4, a_3)^T$ has the third component zero if and only if $a_3 = 0$.

Evidently, $\boldsymbol{u}'$ cannot be expressed as a linear combination, where a_3 is nonzero. Hence $\boldsymbol{u}'$ cannot be exchanged with $\boldsymbol{v}_3$ to obtain a system of generators.

Steinitz exchange theorem

Lemma: Let Y generate a vector space V over $\mathbb{K}$. If for a vector $\boldsymbol{u} \in V$ exist $\boldsymbol{v}_1 \ldots, \boldsymbol{v}_n \in Y$ and $a_1, \ldots, a_n \in \mathbb{K}$ such that $\boldsymbol{u} = \sum_{i=1}^{n} a_i \boldsymbol{v}_i$, where $a_i \neq 0$ for some i, then $\mathcal{L}((Y \setminus \boldsymbol{v}_i) \cup \boldsymbol{u}) = V$

Theorem: Let Y be a *finite* generating set of a vector space V and X be linearly independent in V. Then there exists Z such that:

- $\mathcal{L}(Z) = V$
- $X \subseteq Z$
- $|Z| = |Y|$
- $Z \setminus X \subseteq Y$

Proof: Denote $X \setminus Y = \{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots\}$ and set $Z_0 = Y$.
By induction we construct sets $Z_1, Z_2, \ldots$ that each generates V, $X \cap Y \subseteq Z_j$, $|Z_j| = |Z_{j-1}|$, $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_j \in Z_j$ and $Z_j \setminus \boldsymbol{u}_j \subset Z_{j-1}$.
For $j > 0$ apply the lemma for $\boldsymbol{u}_j$ and Z_{j-1} to obtain Z_j.
Since X is linearly independent, $a_i \neq 0$ for some $\boldsymbol{v}_i \in Z_{j-1} \setminus X$.
The process may have at most $|Y \setminus X|$ steps, hence is finite.
The last obtained Z satisfies all four properties.
Note: Since $|X \setminus Y| \leq |Y \setminus X|$ we have also $|X| \leq |Y|$.

The exchange theorem — an example in $V = \mathbb{Z}_2^4$

Given a linearly independent set $X = \{(1,1,0,0)^T, (1,1,0,1)^T\}$ and a system of generators $Y = Z_0 = \{(1,0,0,0)^T, (0,1,0,0)^T, (0,0,1,0)^T, (0,0,0,1)^T, (1,1,1,1)^T\}$.

1. We express e.g.: $(1,1,0,0)^T = (1,0,0,0)^T + (0,1,0,0)^T$ and exchange $(1,0,0,0)^T$ with $(1,1,0,0)^T$.

We have $Z_1 = \{(1,1,0,0)^T, (0,1,0,0)^T, (0,0,1,0)^T, (0,0,0,1)^T, (1,1,1,1)^T\}$.

2. We express e.g.: $(1,1,0,1)^T = (1,1,0,0)^T + (0,0,0,1)^T$ and exchange $(0,0,0,1)^T$ with $(1,1,0,1)^T$.

We have obtained the desired set of generators $Z_2 = Z = \{(1,1,0,0)^T, (0,1,0,0)^T, (0,0,1,0)^T, (1,1,0,1)^T, (1,1,1,1)^T\}$.

A bit stronger Steinitz exchange theorem

Theorem: Let X be a finite linearly independent set in a vector space V and Y be a generating set of V. Then there exists Z s.t.:

- $\mathcal{L}(Z) = V$
- $X \subseteq Z$
- $|Z| = |Y|$
- $Z \setminus X \subseteq Y$

Proof: By induction on $|X \setminus Y|$. If $X \setminus Y = \emptyset$, then $Z = Y$.

Choose any $\boldsymbol{u} \in X \setminus Y$ and set $X' = X \setminus \boldsymbol{u}$.

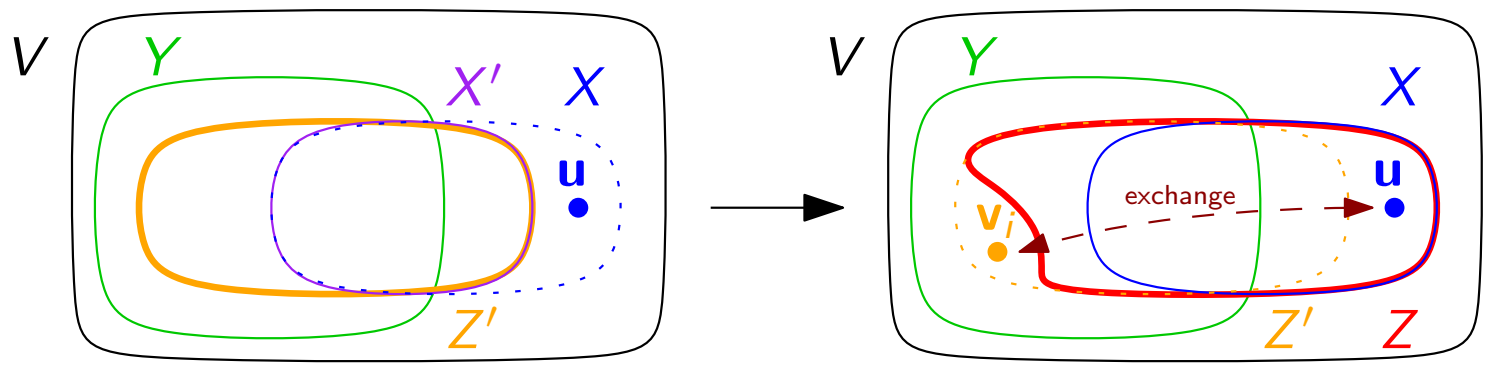
As the set X' is linearly independent and $|X' \setminus Y| < |X \setminus Y|$, by induction hypothesis there exists Z' for X' and Y such that:

- $\mathcal{L}(Z') = V$
- $X' \subseteq Z'$
- $|Z'| = |Y|$
- $Z' \setminus X' \subseteq Y$

Apply exchange lemma for $\boldsymbol{u}$ and $Z' = \{\boldsymbol{v}_1 \ldots, \boldsymbol{v}_n\}$.

Since X is linearly independent, $a_i \neq 0$ for some $\boldsymbol{v}_i \in Z' \setminus X$.

Then $Z = Z' \cup \boldsymbol{u} \setminus \boldsymbol{v}_i$ satisfies all four properties.



Consequences

Theorem: Let Y be a *finite* generating set of a vector space V and X be linearly independent in V. Then there exists Z such that:

- $\mathcal{L}(Z) = V$
- $X \subseteq Z$
- $|Z| = |Y|$
- $Z \setminus X \subseteq Y$

Corollary: If a vector space is finitely generated then any linearly independent set can be extended to a basis.

Corollary: If a vector space is finitely generated then all its bases have the same cardinality.

Proof: Consider bases X, Y of V then:

$$\left.\begin{array}{l} X \text{ independent, } Y \text{ generates } V \Rightarrow |X| \leq |Y| \\ Y \text{ independent, } X \text{ generates } V \Rightarrow |Y| \leq |X| \end{array}\right\} \Rightarrow |Y| = |X|$$

Dimension

Definition: If a vector space V is finitely generated, then its *dimension* $\dim(V)$ is the cardinality of any of its bases.

Examples:

- $\dim(\mathbb{K}^n) = n$
- $\dim(\mathcal{R}(\boldsymbol{A})) = \text{rank}(\boldsymbol{A})$
- The vector space of real polynomials of degree at most n has dimension $n + 1$.

Observation: If V is a subspace of a finitely generated space W then $\dim(V) \leq \dim(W)$

Proof: A basis of V is linearly independent in W and can be extended to a basis of W.

Dimension

Definition: If a vector space V is finitely generated, then its *dimension* $\dim(V)$ is the cardinality of any of its bases.

Examples:

- $\dim(\mathbb{K}^n) = n$
- $\dim(\mathcal{R}(\boldsymbol{A})) = \text{rank}(\boldsymbol{A})$
- The vector space of real polynomials of degree at most n has dimension $n + 1$.

Observation: If V is a subspace of a finitely generated space W then $\dim(V) \leq \dim(W)$

Observation: If U, V are subspaces of a finitely generated W then $\dim(U) + \dim(V) = \dim(U \cap V) + \dim(\mathcal{L}(U \cup V))$