

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 $\mathbf{v}_1, \dots, \mathbf{v}_n$ are linearly independent if and only if $\sum_{i=1}^n a_i \mathbf{v}_i = \mathbf{0}$ has only trivial solution $a_1 = \dots = a_n = 0$.

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

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 I_n are linearly independent.
- ▶ Rows of a matrix in row echelon form are linearly independent. ... a pivot is independent on the zeros below.
- ▶ In \mathbb{R}^2 : $X = \{\mathbf{v}\}$ is linearly independent iff $\mathbf{v} \neq \mathbf{0}$;
The set $Y = \{\mathbf{u}, \mathbf{v}\}$ is linearly independent iff the line determined by \mathbf{u} and \mathbf{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 $X = \{(2, 1, 0, 3)^T, (4, 3, 1, 4)^T, (0, 2, 2, 1)^T, (3, 4, 1, 0)^T, (0, 2, 2, 2)^T\}$ linearly dependent or independent set in \mathbb{Z}_5^4 ?

a) As elementary operations do not modify the *row space*:

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

We get the zero row. I.e., the zero vector can be written as a nontrivial linear combination, hence X is linearly dependent.

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

The equation corresponds to a homogeneous system with matrix:

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

The resulting matrix *contains at least one free variable*: a_3 .

A nontrivial solution of the system, e.g. $(4, 3, 1, 0, 0)^T$, yields $4(2, 1, 0, 3)^T + 3(4, 3, 1, 4)^T + (0, 2, 2, 1)^T = \mathbf{0}$, thus X is dependent.

Properties of linear independence

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

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

Observation: X is independent iff $\forall \mathbf{v} \in X : \mathbf{v} \notin \mathcal{L}(X \setminus \mathbf{v})$.

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

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

Proof: By contrapositive assume that $Y = \{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ and there are distinct $\mathbf{u}_1, \dots, \mathbf{u}_{n+1} \in X$. Express each \mathbf{u}_i as $\mathbf{u}_i = \sum_{j=1}^n a_{i,j} \mathbf{v}_j$.

The corresponding matrix \mathbf{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 $\mathbf{u}_1, \dots, \mathbf{u}_{n+1}$.

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

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

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!

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 $\mathbf{u} = \sum_{i=1}^n a_i \mathbf{v}_i = \sum_{i=1}^n b_i \mathbf{v}_i$

then $\mathbf{0} = \mathbf{u} - \mathbf{u} = \sum_{i=1}^n (a_i - b_i) \mathbf{v}_i \Rightarrow \forall i : a_i = b_i$.

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

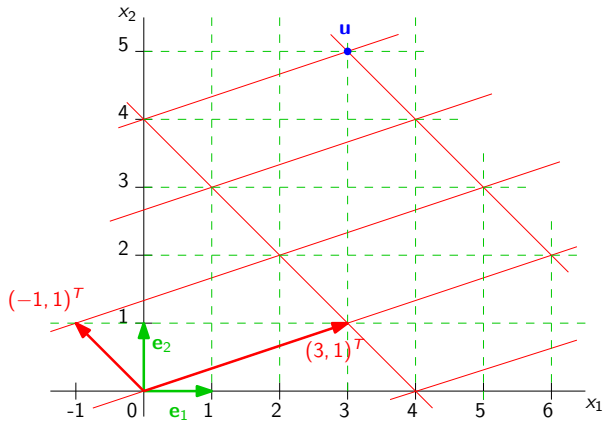
Examples

- ▶ In the arithmetic vector space \mathbb{K}^n the columns $\mathbf{e}_1, \dots, \mathbf{e}_n$ of I_n form the so called *standard basis* K (aka *canonical* or *natural*).
- ▶ In \mathbb{R}^2 , a set $X = \{\mathbf{v}_1, \mathbf{v}_2\}$ is a basis if and only if the line determined by \mathbf{v}_1 and \mathbf{v}_2 does not contain the origin.
- ▶ In the vector space of real polynomials, the infinite set $\{x^0, x^1, x^2, \dots\}$ is an example of infinite basis.
- ▶ In the space of polynomials of degree at most 4 we have e.g.:
 $[x^3 + 2x - 1]_{(x^0, x^1, \dots, x^4)} = (-1, 2, 0, 1, 0)^T$, but also
 $[x^3 + 2x - 1]_{(x^0+x^1, x^1-2x^2, x^2, x^3, x^4)} = (-1, 3, 6, 1, 0)^T$, as
 $x^3 + 2x - 1 = -1(x^0 + x^1) + 3(x^1 - 2x^2) + 6x^2 + 1x^3$
- ▶ In the vector space $V = \mathcal{P}(X)$ over \mathbb{Z}_2 we have e.g. a basis from the single-element sets: $[\{a, c\}]_{(\{a\}, \{b\}, \{c\})} = (1, 0, 1)^T$.

Coordinates of a vector with respect to different bases

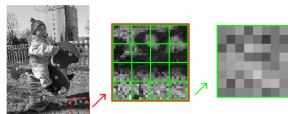
The coordinates of \mathbf{u} with respect to the standard basis $\mathcal{K} = \{\mathbf{e}_1, \mathbf{e}_2\} = \{(1, 0)^T, (0, 1)^T\}$ are: $\mathbf{u} = [\mathbf{u}]_{\mathcal{K}} = (3, 5)^T$.

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

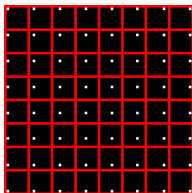


Distinct bases — Jpeg

A vector \mathbf{u} is an 8×8 cut from a single color plane and is normalized to $(-128, 127)$:



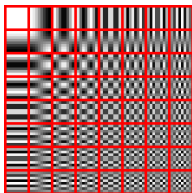
Standard basis K :



$$[\mathbf{u}]_K =$$

$$\begin{pmatrix} 0 & 7 & 30 & -35 & 29 & 1 & -10 & 20 \\ -6 & -54 & -15 & 0 & -18 & -69 & -10 & -32 \\ -38 & 18 & -36 & 58 & 37 & 18 & -7 & -4 \\ 17 & 38 & 27 & -19 & -26 & -43 & -2 & 44 \\ 26 & 33 & 44 & 48 & 42 & 7 & -8 & 20 \\ 11 & 30 & -2 & 32 & 70 & 25 & 25 & 17 \\ 22 & -44 & 30 & -19 & 14 & 48 & 55 & 6 \\ -11 & -16 & 8 & 6 & 22 & -28 & -10 & 17 \end{pmatrix}$$

Basis X from harmonic functions:



$$[\mathbf{u}]_X \doteq$$

$$\begin{pmatrix} 11 & -59 & 16 & 4 & -14 & 4 & -9 & -10 \\ -6 & 110 & -8 & -30 & -30 & 46 & -19 & -13 \\ 16 & -84 & 23 & 5 & -20 & 6 & -12 & -14 \\ -20 & -83 & -29 & -2 & 18 & -4 & 16 & 27 \\ 2 & 91 & 3 & -1 & 29 & -14 & -13 & 21 \\ 27 & 21 & 38 & 41 & -52 & -2 & -40 & 22 \\ -20 & 40 & -28 & 41 & 16 & -46 & -12 & 27 \\ -9 & 59 & -13 & -46 & 11 & 15 & -58 & -39 \end{pmatrix}$$

These are 64-dimensional vectors, only depicted as matrices.

Lossy compression and decompression (simplified)

$$\begin{pmatrix} 11 & -59 & 16 & 4 & -14 & 4 & -9 & -10 \\ -6 & 110 & -8 & -30 & -30 & 46 & -19 & -13 \\ 16 & -84 & 23 & 5 & -20 & 6 & -12 & -14 \\ -20 & -83 & -29 & -2 & 18 & -4 & 16 & 27 \\ 2 & 91 & 3 & -1 & 29 & -14 & -13 & 21 \\ 27 & 21 & 38 & 41 & -52 & -2 & -40 & 22 \\ -20 & 40 & -28 & 41 & 16 & -46 & -12 & 27 \\ -9 & 59 & -13 & -46 & 11 & 15 & -58 & -39 \end{pmatrix}$$

divide component-wise by the so-called *quantization matrix*

$$\begin{pmatrix} 16 & 11 & 10 & 16 & 24 & 40 & 51 & 61 \\ 12 & 12 & 14 & 19 & 26 & 58 & 60 & 55 \\ 14 & 13 & 16 & 24 & 40 & 57 & 69 & 56 \\ 14 & 17 & 22 & 29 & 51 & 87 & 80 & 62 \\ 18 & 22 & 37 & 56 & 68 & 109 & 103 & 77 \\ 24 & 35 & 55 & 64 & 81 & 104 & 113 & 92 \\ 49 & 64 & 78 & 87 & 103 & 121 & 120 & 101 \\ 72 & 92 & 95 & 98 & 112 & 100 & 103 & 99 \end{pmatrix}$$

and round

$$\begin{pmatrix} 3 & -1 & -2 & -1 & 1 & 0 & 0 & 1 \\ -5 & 2 & 0 & -1 & 0 & 0 & 0 & 0 \\ -4 & -2 & 0 & 1 & 0 & 0 & 0 & 1 \\ 5 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 2 & 1 & -1 & 0 & 0 & 0 & 0 \\ 1 & -1 & 1 & 0 & -1 & 0 & 0 & 0 \\ 1 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

multiply by the quant. matrix

$$\begin{pmatrix} 48 & -11 & -20 & -16 & 24 & 0 & 0 & 61 \\ -60 & 24 & 0 & -19 & 0 & 0 & 0 & 0 \\ -56 & -26 & 0 & 24 & 0 & 0 & 0 & 56 \\ 70 & 0 & 0 & 29 & 0 & 0 & 0 & 0 \\ 18 & 44 & 37 & -56 & 0 & 0 & 0 & 0 \\ 24 & -35 & 55 & 0 & -81 & 0 & 0 & 0 \\ 49 & 0 & -78 & 0 & 0 & 0 & 0 & 0 \\ 72 & 0 & -95 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

convert from the basis X to K

$$\begin{pmatrix} 1 & 0 & 39 & -16 & 23 & -13 & 23 & 0 \\ 1 & -53 & -40 & -38 & -3 & -61 & -36 & -14 \\ -41 & -15 & 32 & 47 & 55 & 20 & -2 & -24 \\ 15 & 33 & 12 & -38 & -71 & -36 & 12 & 43 \\ 31 & 27 & 48 & 82 & 56 & 5 & -11 & 18 \\ 22 & -1 & 6 & 23 & 53 & 35 & 25 & 13 \\ 1 & -5 & 7 & -33 & 25 & 38 & 62 & 21 \\ -2 & -29 & 17 & -3 & 34 & -38 & -4 & 5 \end{pmatrix}$$

Data: 27 ints. $\in \{-5, \dots, 5\} \setminus 0$

Average hue deviation $< 6\%$

Original:



Restored:



Existence of a basis

Observation: If $\mathcal{L}(X) = V$ and $\forall \mathbf{v} \in X : \mathbf{v} \notin \mathcal{L}(X \setminus \mathbf{v})$
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 $\mathbf{v} \in X$
whether $\mathbf{v} \in \mathcal{L}(X \setminus \mathbf{v})$. If so then remove \mathbf{v} from X .

Theorem: Every vector space has a basis.

... for finitely generated it is proven above;
for infinitely generated we omit a proof.

(This part of the theorem is equivalent to the axiom of choice.)

Exchange lemma

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

Example: For the space $V = \mathbb{R}^3$, a system of generators $Y = \{\mathbf{v}_1, \dots, \mathbf{v}_4\} = \{(1, 0, 0)^T, (0, 1, 0)^T, (0, 0, 1)^T, (1, 1, 0)^T\}$ and vectors $\mathbf{u} = (1, 1, 1)^T$, $\mathbf{u}' = (2, 1, 0)^T$.

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

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

Any combination $a_1 \mathbf{v}_1 + \dots + a_4 \mathbf{v}_4 = (a_1 + a_4, a_2 + a_4, a_3)^T$ has the third component zero if and only if $a_3 = 0$.

Thus \mathbf{u}' cannot be expressed as a linear combination, where a_3 is nonzero. We cannot exchange \mathbf{v}_3 with \mathbf{u}' and still generate V .

Exchange lemma

Lemma: Let Y generate a vector space V over \mathbb{K} . If for a vector $u \in V$ exist $v_1, \dots, v_n \in Y$ and $a_1, \dots, a_n \in \mathbb{K}$ such that $u = \sum_{i=1}^n a_i v_i$, where $a_i \neq 0$ for some i , then $\mathcal{L}((Y \setminus v_i) \cup u) = V$.

Proof: $u = a_1 v_1 + \dots + a_i v_i + \dots + a_n v_n \Rightarrow v_i = \frac{1}{a_i} \left(u - \sum_{j \neq i} a_j v_j \right)$.

Write any $w \in V$ as a linear combination of elements from Y .

If v_i occurs in this combination, substitute the above for v_i .

We get w as a linear combination of elements from $(Y \setminus v_i) \cup u$.

In the finite case, if $Y = \{v_1, \dots, v_n\}$ and $w = \sum_{j=1}^n b_j v_j$

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

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.:

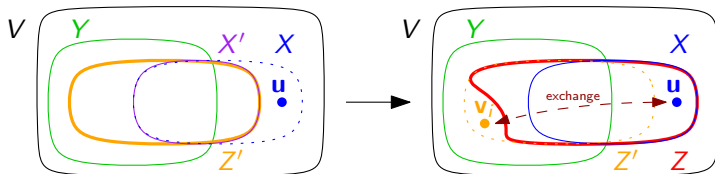
$$\blacktriangleright \mathcal{L}(Z) = V \quad \blacktriangleright X \subseteq Z \quad \blacktriangleright |Z| = |Y| \quad \blacktriangleright Z \setminus X \subseteq Y$$

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

Otherwise choose any $u \in X \setminus Y$ and set $X' = X \setminus u$.

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:

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



Apply exchange lemma for u and $Z' = \{v_1, \dots, v_n\}$.

Since X is linearly independent, $a_i \neq 0$ for some $v_i \in Z' \setminus X$.

Then $Z = Z' \cup u \setminus v_i$ satisfies all four properties.

Example in $V = \mathbb{Z}_2^4$

The proof yields an iterative procedure where we gradually replace the vectors $\{\mathbf{u}_1, \dots, \mathbf{u}_k\} = X \setminus Y$ with suitable vectors from Y , which yields a sequence $Z_0 = Y, Z_1, \dots, Z_k = Z$.

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 $Z_2 = Z =$

$\{(1, 1, 0, 0)^T, (0, 1, 0, 0)^T, (0, 0, 1, 0)^T, (1, 1, 0, 1)^T, (1, 1, 1, 1)^T\}$.

E.g. step 2. matches to the proof for $\mathbf{u} = (1, 1, 0, 1)^T$ and $Z' = Z_1$.

Consequences of the 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.:

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

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: The *dimension* of a finitely generated vector space V is the cardinality of any of its bases. It is denoted by $\dim(V)$.

Examples:

- ▶ $\dim(\mathbb{K}^n) = n$
- ▶ $\dim(\mathcal{R}(\mathbf{A})) = \text{rank}(\mathbf{A})$
- ▶ 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 .

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

Proof: Extend a basis X of the intersection $U \cap V$ to a basis Y of U as well as to a basis Z of V . Then $|Y| + |Z| = |X| + |Y \cup Z|$.