Vector Spaces

Summer 2016

July 4, 2016

Section 1

Vector spaces

Definition

A **vector space** is a set V that is closed both under addition of its members and under scalar multiplication. Namely if $x, y \in V$ then $x + y \in V$ and, when α is a scalar, $\alpha x \in V$.

- (This definition is loose. For a more formal discussion, see sections 27.1 and 27.6 in Simon and Blume)
- element of a vector space is called a **vector**
- A vector space must include the origin (or more formally the 'zero element').

Definition

A **subspace** of a vector space V is a subset of V that is closed under addition of its members and under scalar multiplication.

- A subspace of a vector space is sometimes called a linear subspace.
- A subspace of a vector space is itself a vector space.

Example (Euclidean space)

$\mathbb{R}^n$ over the field $\mathbb{R}$ is a vector space in which vector addition and scalar multiplication are defined in the usual way.

Example

Subspaces of $\mathbb{R}^2$:

- the $\mathbb{R}^2$ itself
- any straight line passing through the origin
- the origin

Vector spaces of functions

Example

Let $V =$ all continuous functions from $[0, 1]$ to $\mathbb{R}$. For $f, g \in V$, define $f + g$ by $(f + g)(x) = f(x) + g(x)$. Define scalar multiplication as $(\alpha f)(x) = \alpha f(x)$. Then this is a vector space.

Example

More examples:

- The set of all k times continuously differentiable functions on $\mathbb{R}$.
- The set of all polynomials of degree less than or equal to k.

Definition

Let V be a vector space and $v_1, ..., v_k \in V$. A **linear combination** of $v_1, ..., v_k$ is any vector

$$c_1 v_1 + ... + c_k v_k$$

where $c_1, ..., c_k$ are scalars.

- Question: How can we be sure that $c_1 v_1 + ... + c_k v_k \in V$?
- A simple linear combination includes the operations of vector addition and of scalar multiplication.

Definition

Let V be a vector space and $W \subseteq V$. The **span** of W is the set of all finite linear combinations of elements of W and denoted by $span(W)$.

- The **span** of any $W \subseteq V$ is a linear subspace.

Example

Let V be the vector space of all functions from $[0, 1]$ to $\mathbb{R}$. The span of $\{1, x, ..., x^n\}$, all defined on $[0, 1]$, is the set of all polynomials of degree less than or equal n on $[0, 1]$.

Definition

A set of vectors $v_1, \ldots, v_k \in V$, is **linearly independent** if the only solution to

$$\sum_{j=1}^{k} c_j v_j = 0$$

is $c_1 = c_2 = \ldots = c_k = 0$.

Definition

A **basis** of a vector space V is any set of linearly independent vectors $b_1, ..., b_k$ such that $V = span\{b_1, ..., b_k\}$.

Definition

The **dimension** of a vector space, V, is the cardinality of the largest set of linearly independent elements in V and is denoted by $dim(V)$.

Example

A basis for $\mathbb{R}^n$ is $e_1 = (1, 0, ..., 0)$, $e_2 = (0, 1, 0, ..., 0)$, ..., $e_n = (0, ..., 0, 1)$. This basis is called the **standard basis** of $\mathbb{R}^n$.

Example

What is the dimension of each of the examples of vector spaces above? Can you find a basis for them?

Basis gives coordinates

Lemma

Let $\{b_1, ..., b_k\}$ be a basis for a vector space V. Then $\forall v \in V$ there exists a unique $v_1, ..., v_k \in \mathbb{F}$ and such that $v = \sum_{i=1}^{k} v_i b_i$

Proof.

- B spans V, so such $(v_1, ..., v_k)$ exist.
- Suppose there exists another such $(v_1', ..., v_k')$. Then

$$\begin{aligned} v = \sum v_i b_i = \sum v_i' b_i \\ \sum v_i b_i - \sum v_i' b_i =0 \\ \sum (v_i - v_i)' b_i =0. \end{aligned}$$

□

Dimension $=$ |Basis |

- If B is a basis for a vector space V and $I \subseteq V$ is a set of linearly independent elements then $|I| \leq |B|$.
- Any two bases for a vector space have the same cardinality.

Section 2

Linear transformations

Definition

A **linear transformation** (aka linear function) is a function, A, from a vector space V to a vector space W such that $\forall v_1, v_2 \in V$,

$$A(v_1 + v_2) = Av_1 + Av_2$$

and

$$A(av_1) = aAv_1$$

for all scalars a.

Theorem

For any linear transformation, A, from $\mathbb{R}^n$ to $\mathbb{R}^m$ there is an associated m by n matrix,

$$\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}$$

where a_{ij} is defined by $Ae_j = \sum_{i=1}^m a_{ij} e_i$. Conversely, for any m by n matrix, there is an associated linear transformation from $\mathbb{R}^n$ to $\mathbb{R}^m$ defined by $Ae_j = \sum_{i=1}^n a_{ij}$.

Proof.

- Let A be a linear transformation from $\mathbb{R}^n$ to $\mathbb{R}^m$
- $b_1, b_2, .., b_n$ basis for $\mathbb{R}^n$
- $\forall v \in V\ \exists \alpha_j \in \mathbb{R}$ s.t. $v = \sum_{j=1}^n \alpha_j b_j$
- $Av = \sum_{j=1}^n \alpha_j A b_j$ so only need Ab_j to determine A
- $d_1, ..., d_m$ basis for $\mathbb{R}^m$, so

$$Ab_j = \sum_{i=1}^m a_{ij} d_i.$$

$\square$

Section 3

Matrix operations and properties

Addition

- $A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}, B = \begin{pmatrix} b_{11} & \cdots & b_{1n} \\ \vdots & \ddots & \vdots \\ b_{m1} & \cdots & b_{mn} \end{pmatrix}$
- Linear transformation implies $(A+B)x = Ax + Bx$

$$\begin{aligned} (A+B)e_i &= Ae_i + Be_i \\ &= \sum_{j=1}^{n} a_{ij}e_j + \sum_{j=1}^{n} b_{ij}e_j \\ &= \sum_{j=1}^{n} (a_{ij} + b_{ij})e_j, \end{aligned}$$

- so $A + B = \begin{pmatrix} a+b_{11} & \cdots & a+b_{1n} \\ \vdots & \ddots & \vdots \\ a+b_{m1} & \cdots & a+b_{mn} \end{pmatrix}$.

Addition properties

1. $A + (B + C) = (A + B) + C$,
2. $A + B = B + A$,
3. $A + \mathbf{0} = A$, where $\mathbf{0}$ is an m by n matrix of zeros, and
4. $A + (-A) = \mathbf{0}$ where $-A = \begin{pmatrix} -a_{11} & \cdots & -a_{1n} \\ \vdots & \ddots & \vdots \\ -a_{m1} & \cdots & -a_{mn} \end{pmatrix}$.

Scalar multiplication

- Linear transformation requires $A\alpha x = \alpha Ax$
- so,

$$\alpha A = \begin{pmatrix} \alpha a_{11} & \cdots & \alpha a_{1n} \\ \vdots & \ddots & \vdots \\ \alpha a_{m1} & \cdots & \alpha a_{mn} \end{pmatrix}$$

The space of matrices is a vector space

- $L(\mathbb{R}^n, \mathbb{R}^m) \equiv$ all m by n matrices $\equiv$ all linear transformations from $\mathbb{R}^n$ to $\mathbb{R}^m$ with addition and multiplication as above is a vector space
  - Question: $L(\mathbb{R}^n, \mathbb{R}^m)$ is isomorphic to what other vector space that we have seen?
- $L(V, W) \equiv$ all linear transformations from $V \to W$ is a vector space

Matrix multiplication

- Multiplication $\equiv$ composition of linear transformations
- $A : \mathbb{R}^n \to \mathbb{R}^m$, $B : \mathbb{R}^p \to \mathbb{R}^n$.
- Consider $A(Be_k)$

$$
\begin{aligned}
A(Be_k) =& A(\sum_{j=1}^{n} b_{jk} e_i) \\
=& \sum_{j=1}^{n} b_{jk} A e_i \\
=& \sum_{j=1}^{n} b_{jk} \left(\sum_{l=1}^{m} a_{ij} e_l \right) \\
=& \sum_{l=1}^{m} \left(\sum_{j=1}^{n} a_{ij} b_{jk} \right) e_l \\
=& \begin{pmatrix} \sum_{j=1}^{n} a_{1j} b_{j1} & \cdots & \sum_{j=1}^{n} a_{1j} b_{jp} \\ \vdots & \ddots & \vdots \\ \sum_{j=1}^{n} a_{mj} b_{j1} & \cdots & \sum_{j=1}^{n} a_{mj} b_{jp} \end{pmatrix} e_l \\
=& (AB) e_l.
\end{aligned}
$$

Multiplication properties

1. $A(BC) = (AB)C$
2. $A(B + C) = AB + AC$ and $(A + B)C = AC + BC$
3. $AI_n = A$ where A is m by n and I_n is the identity linear transformation from $\mathbb{R}^n$ to $\mathbb{R}^n$ such that $I_n x = x \forall x \in \mathbb{R}^n$
4. Not commutative

Definition

A real **inner product space** is a vector space over the field $\mathbb{R}$ with an additional operation called the inner product that is function from $V \times V$ to $\mathbb{R}$. We denote the **inner product** of $v_1, v_2 \in V$ by $\langle v_1, v_2 \rangle$. It has the following properties:

1. $\langle v_1, v_2 \rangle = \langle v_2, v_1 \rangle$
2. $\langle av_1 + bv_2, v_3 \rangle = a \langle v_1, v_3 \rangle + b \langle v_2, v_3 \rangle$ for $a, b \in \mathbb{R}$
3. $\langle v, v \rangle \geq 0$ and equals 0 iff $v = 0$.

Example

$\mathbb{R}^n$ with the inner product, $< x, y >= \sum_{i=1}^{n} x_i y_i$, is an inner product space.

Example

$\mathcal{L}^2(0,1)$ with $\langle f, g \rangle \equiv \int_0^1 f(x)g(x)dx$ is an inner product space.

Transpose

Definition

Given a linear transformation, A, from a real inner product space V to a real inner product space W, the **transpose** of A, denoted A^T (or often A') is a linear transformation from W to V such that $\forall v \in V, w \in W$

$$\langle Av, w \rangle = \left\langle v, A^T w \right\rangle .$$

Transpose for matrices

- $$\langle Av, w\rangle = \sum_{i=1}^{m}\left(\sum_{j=1}^{n} a_{ij}v_j\right) w_i = \sum_{i=1}^{m}\sum_{j=1}^{n} a_{ij}w_i v_j$$
- $$\left\langle v, A^T w\right\rangle = \sum_{j=1}^{n} v_j \left(\sum_{i=1}^{m} a_{ji}^T w_i\right) = \sum_{i=1}^{m}\sum_{j=1}^{n} a_{ji}^T w_i v_j$$
- If $\langle Av, w\rangle = \left\langle v, A^T w\right\rangle$, for any v and w we must have $a_{ji}^T = a_{ij}$
- The transpose of a matrix simply swaps rows for

Transpose properties

1. $(A+B)^T = A^T + B^T$
2. $(A^T)^T = A$
3. $(\alpha A)^T = \alpha A^T$
4. $(AB)^T = B^T A^T$.
5. $\mathrm{rank} A = \mathrm{rank} A^T$

Types of matrices

Definition
A **column vector** is any m by 1 matrix.

Definition
A **row vector** is any 1 by n matrix.

Definition
A **square** matrix has the same number of rows and columns.

Definition

A **diagonal** matrix is a square matrix with non-zero entries only along its diagonal, i.e. $a_{ij} = 0$ for all $i \neq j$.

Definition

An **upper triangular** matrix is a square matrix that has non-zero entries only on or above its diagonal, i.e. $a_{ij} = 0$ for all $j > i$. A **lower triangular** matrix is the transpose of an upper triangular matrix.

Definition

A matrix is **symmetric** if $A = A^T$.

Definition

A matrix is **idempotent** if $AA = A$.

Definition

A **permutation** matrix is a square matrix of 1's and 0's with exactly one 1 in each row or column.

Definition

A **nonsingular** matrix is a square matrix whose rank equals its number of columns.

Definition

An **orthogonal** matrix is a square matrix such that $A^T A = I$.

Invertibility

Definition

Let A be a linear transformation from V to W. Let B be a linear transfromation from W to V. B is a **right inverse** of A if $AB = I_V$. Let C be a linear tranfromation from V to W. C is a **left inverse** of A if $CA = I_W$.

Lemma

If A is a linear transformation from V to V and B is a right inverse, and C a left inverse, then $B = C$.

Lemma

Let A be a linear tranformation from V to V, and suppose A is invertible. Then A is nonsingular and the unique solution to $Ax = b$ is $x = A^{-1}b$.

Lemma

If A is nonsingular, then A^{-1} exists.

Corollary

A square matrix A is invertible if and only if $\mathrm{rank} A$ is equal to its number of columns.

Properties of matrix inverse

1. $(AB)^{-1} = B^{-1}A^{-1}$
2. $(A^T)^{-1} = (A^{-1})^T$
3. $(A^{-1})^{-1} = A$

Section 4

Determinants

Determinants

- Determinant: geometry and invertibility
- Invert 2 by 2 matrix by Gauss-Jordan elimination:

$$\begin{pmatrix} a & b & 1 & 0 \\ c & d & 0 & 1 \end{pmatrix} \simeq \begin{pmatrix} a & b & 1 & 0 \\ 0 & \frac{ad-bc}{a} & -\frac{c}{a} & 1 \end{pmatrix}$$

$$\simeq \begin{pmatrix} a & b & 1 & 0 \\ 0 & 1 & -\frac{c}{ad-bc} & \frac{a}{ad-bc} \end{pmatrix}$$

$$\simeq \begin{pmatrix} a & 0 & \frac{ad}{ad-bc} & \frac{-ba}{ad-bc} \\ 0 & 1 & -\frac{c}{ad-bc} & \frac{a}{ad-bc} \end{pmatrix}$$

$$\simeq \begin{pmatrix} 1 & 0 & \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ 0 & 1 & -\frac{c}{ad-bc} & \frac{a}{ad-bc}. \end{pmatrix}$$

- Needed $ad - bc \neq 0$.

Definition

Let A be an n by n matrix consisting of column vectors $a_1, ..., a_n$. The determinant of A is the unique function such that

1. $\det I_n = 1$.
2. As a function of the columnes, $\det$ is an alternating form: $\det(A) = 0$ iff $a_1, ..., a_n$ are linearly dependent.
3. As a function of the columnes, $\det$ is multi-linear:

$$\det(a_1, ..., ba_j + cv, ..., a_n) = b\det(A) + c\det(a_1, ..., v, ...a_n)$$

- 1 natural, needed for volume interpretation
- 2 ensures $\det A = 0$ iff A singular

Lemma

Let A be an n by n matrix. The A is singular if and only if the columns of A are linearly dependent.

Corollary

A is nonsingular if and only if $\det A \neq 0$.

- 3 is related to volume interpretation
- Consider diagonal matrices, volume interpretation require multi-linearity

Definition

The **determinant** of a square matrix A is defined recursively as

1. For 1 by 1 matrices, $\det A = a_{11}$
2. For n by n matrices,

$$\det A = \sum_{j=1}^{n} (-1)^{1+j} a_{1j} \det A_{-1,-j}$$

where $A_{-i,-j}$ is the $n-1$ by $n-1$ matrix obtained by deleting the ith row and jth column of A.

- **minor:** $\det A_{-i,-j}$
- **cofactor:** $(-1)^{i+j} \det A_{-i,-j}$

Determinant properties

Theorem

The two definitions of the determinant, (37) and (40), are equivalent.

1. $\det A^T = \det A$
2. $\det(AB) = (\det A)(\det B)$
3. $\det A^{-1} = (\det A)^{-1}$
4. Usually, $\det(A+B) \neq \det A + \det B$
5. If A is diagonal, $\det A = \prod_{i=1}^{n} a_{ii}$
6. If A is upper or lower triangular $\det A = \prod_{i=1}^{n} a_{ii}$.

Theorem

Let A be nonsingular. Then,

1. $A^{-1} = \frac{1}{\det A}\begin{pmatrix} \det A_{-1,-1} & \cdots & (-1)^{1+n}\det A_{-n,-1} \\ \vdots & \ddots & \vdots \\ (-1)^{1+n}\det A_{-1,-n} & \cdots & (-1)^{n+n}\det A_{-n,-n} \end{pmatrix}$
2. *(**Cramer's rule**) The unique solution to $Ax = b$ is*

$$x_i = \frac{\det B_i}{\det A}$$

where B_i is the matrix A with the ith column replaced by b.

Section 5

Normed vector spaces

Normed vector spaces

- Measure of length or distance

Definition

A **normed vector space**, $(V, \mathbb{F}, +, \cdot, \|\cdot\|)$, is a vector space with a function, called the **norm**, from V to $\mathbb{F}$ and denoted by $\|v\|$ with the following properties:

1. $\|v\| \geq 0$ and $\|v\| = 0$ iff $v = 0$,
2. $\|\alpha v\| = |\alpha| \, \|v\|$ for all $\alpha \in \mathbb{F}$,
3. The triangle inequality holds:

$$\|v_1 + v_2\| \leq \|v_1\| + \|v_2\|$$

for all $v_1, v_2 \in V$.

Examples

Example

$\mathbb{R}^3$ is a normed vector space with norm

$$\|x\| = \sqrt{x_1^2 + x_2^2 + x_3^2}.$$

This norm is exactly how we usually measure distance. For this reason, it is called the Euclidean norm.
More generally, for any n, $\mathbb{R}^n$, is a normed vector space with norm

$$\|x\| = \sqrt{\sum_{i=1}^{n} x_i^2}.$$

Section 6

Inner product spaces

Inner product spaces

Definition

A real **inner product space** is a vector space over the field $\mathbb{R}$ with an additional operation called the **inner product** that is function from $V \times V$ to $\mathbb{R}$. We denote the inner product of $v_1, v_2 \in V$ by $\langle v_1, v_2 \rangle$. It has the following properties:

1. $\langle v_1, v_2 \rangle = \langle v_2, v_1 \rangle$
2. $\langle av_1 + bv_2, v_3 \rangle = a \langle v_1, v_3 \rangle + b \langle v_2, v_3 \rangle$ for $a, b \in \mathbb{R}$
3. $\langle v, v \rangle \geq 0$ and equals 0 iff $v = 0$.

- The norm of an inner product space is defined as

$$\|x\| = \sqrt{\langle x, x \rangle}.$$

Example

- $\mathbb{R}^n$ equipped with the inner product

$$\langle x, y \rangle = \sum_{i=1}^{n} x_i y_i = x^T y$$

is an inner product space.

- Norm induced by the inner product is the Euclidean norm

$$\|x\| = \sqrt{\langle x, x \rangle} = \sqrt{\sum_{i=1}^{n} x_i^2}$$

Angle between Two Vectors

Theorem (Law of cosine)

Let $u, v \in \mathbb{R}^n$, then the angle θ between them satisfies

$$\|u\| \, \|v\| \cos(\theta) = \langle u, v \rangle \, .$$

Corollary (Cauchy-Schwarz inequality)

Let $u, v \in \mathbb{R}^n$, then we have

$$| \langle u, v \rangle | \leq \|u\| \, \|v\|$$

- (Note) In fact, the Cauchy-Schwarz inequality holds more generally in any inner product space.

Theorem (Triangle inequality)

Let $x, y \in V$, an inner product space, then we have

$$\|x + y\| \leq \|x\| + \|y\| .$$

Proof.

$$\begin{aligned}
\|x+y\|^2 &= \|x\|^2 + 2\langle x, y\rangle + \|y\|^2 \\
&\leq \|x\|^2 + 2\left|\langle x, y\rangle\right| + \|y\|^2 \\
&\leq \|x\|^2 + 2\|x\|\,\|y\| + \|y\|^2 \; Cauchy - Schwartz \\
&= (\|x\| + \|y\|)^2
\end{aligned}$$

Since norms are nonnegative, taking square roots gives the result. $\square$

Orthogonality

Definition

Let x and y be vectors in an inner product space. Then we say x and y are **orthogonal** iff $\langle x, y \rangle = 0$.

Theorem (Pythagoras theorem)

Let $x, y \in V$, an inner product space, be orthogonal to each other. Then we have

$$\|x + y\|^2 = \|x\|^2 + \|y\|^2$$

Proof.

$$\|x + y\|^2 = \|x\|^2 + 2\langle x, y \rangle + \|y\|^2$$

Orthogonality of x and y implies $\langle x, y \rangle = 0$ and the result follows. $\square$

Section 7

Row, column, and null space

Row space

Definition

Let A be an m by n matrix. The **row space** of A, denoted $\mathrm{Row}(A)$, is the space spanned by the row vectors of A.

- $\mathrm{Row}(A) \subseteq \mathbb{R}^n$

Lemma

Performing Gaussian elimination does not change the row space of a matrix.

Proof.

Let $a_1, ..., a_m$ be the row vectors of A. Each step of Gaussian elimination transforms some a_j into $a_j + ga_k$ with $k \neq j$ or $g \neq -1$. Can show that

$$\mathrm{span}(a_1, ..., a_m) = \mathrm{span}(a_1 + ga_k, ..., a_m).$$

$\square$

Corollary

The dimension of the row space of a matrix is equal to its rank.

Column space

Definition

Let A be an m by n matrix. The **column space** of A, denoted $\mathrm{Col}(A)$, is the space spanned by the column vectors of A.

- $\mathrm{Col} A \subseteq \mathbb{R}^m$

Lemma

Let A be an m by n matrix. Then $Ax = b$ has a solution iff $b \in \mathrm{Col}(A)$.

Definition

A column of a matrix, A, is **basic** if the corresponding column of the row echelon form, A_r, contains a pivot.

Theorem

The basic columns of A form a basis for $\mathrm{Col}(A)$.

Proof.

Let A be $m \times n$ and denote its columns as $v_1, \ldots, v_n$. Let A_r be the row echelon form of A and denotes its columns as $w_1, \ldots, w_n$. Let $w_{i_1}, \ldots, w_{i_k}$ be the basic columns of A_r. Each has more zeros, so $w_{i_1}, \ldots, w_{i_k}$ are linearly independent. By definition of row echelon form, the final $m - k$ rows of A_r are all zero. Therefore $\dim \mathrm{Col}(A_r) \leq k$, and $w_{i_1}, \ldots, w_{i_k}$ must be a basis for $\mathrm{Col}(A_r)$. □

Continued.

Now we show that $v_{i_1}, \ldots, v_{i_k}$ are a basis for $\mathrm{Col}(A)$. Suppose

$$c_1 v_{i_1} + \ldots + c_k v_{i_k} = 0.$$

Then we could do Gaussian elimination to convert this system to

$$c_1 w_{i_1} + \ldots + c_k w_{i_k} = 0.$$

$w_{i_1}, \ldots, w_{i_k}$ are linearly independent so $c_1 = 0, \ldots c_k = 0$. Add any other $v_j, j \notin \{i_1, \ldots, i_k\}$, then by the same argument there must exist a non-zero c than solves

$$c_1 v_{i_1} + \ldots + c_k v_{i_k} + c_j v_j = 0.$$

Thus, $v_{i_1}, \ldots, v_{i_k}$ is a basis for $\mathrm{Col}(A)$. $\square$

Corollary

The dimensions of the row and column spaces of any matrix are equal.

Corollary

$\mathrm{rank} A = \mathrm{rank} A^T$.

Null space

Definition

Let A be m by n. The set of solutions to the homogeneous equation $Ax = 0$ is the **null space** (or kernel) of A, denoted by $\mathcal{N}(A)$ (or $\mathrm{Null}(A)$).

Definition

Let $V \subseteq \mathbb{R}^n$ be a linear subspace, and let $c \in \mathbb{R}^n$ be a fixed vector. The set

$$\{x \in \mathbb{R}^n : x = v + c \text{ for some } v \in V\}$$

is called the set of **translates** of V by c, and is denoted $c + V$. Any set of translates of a linear subspace is called an **affine** space.

Lemma

Let $Ax = b$ be an m by n system of linear equations. Let x_0 be any particular solution. Then the set of solutions is $x_0 + \mathcal{N}(A)$.

Proof.

Let $w \in x_0 + \mathcal{N}(A)$. Then

$$\begin{aligned} Aw &= A(x_0) + A(\underbrace{w - x_0}_{\in \mathcal{N}(A)}) \\ &= b + 0. \end{aligned}$$

Let w be a solution to $Ax = b$. Then

$$A(w - x_0) = Aw - Ax_0 = 0$$

so $w - x_0 \in \mathcal{N}(A)$ and $w \in x_0 + \mathcal{N}(A)$. $\square$

Theorem

Let A be an m by n matrix. Then $\mathrm{dim}\mathcal{N}(A) = n - \mathrm{rank}A$

Proof.

- Let $u_1, \ldots, u_k$ be a basis for $\mathcal{N}(A)$. We can add $u_{k+1}, \ldots, u_n$ to $u_1, \ldots, u_k$ to form a basis for $\mathbb{R}^n$.
- Show that $Au_{k+1}, \ldots, Au_n$ are a basis for the column space
    - linearly independent
    - span $\mathrm{Col}A$.

$\square$

Relationship among row, column, and null spaces

- $\mathrm{Col}(A) = \mathrm{Row}(A^T) \subseteq \mathbb{R}^m$
- $\mathrm{Row}(A) = \mathrm{Col}(A^T) \subseteq \mathbb{R}^n$
- $\mathcal{N}(A) \subseteq \mathbb{R}^n$ and $\mathcal{N}(A^T) \subseteq \mathbb{R}^m$
- Let $x \in \mathcal{N}(A)$, $y \in \mathrm{Row}(A)$, what is $\langle x, y \rangle$?