vv214: Matrix algebra. Linear spaces. Structure of a linear space.

Dr.Olga Danilkina

UM-SJTU Joint Institute

May 30, 2019

This week

Today

1. More practice with linear systems/rref/rank.
2. Matrix algebra.
3. Number fields and linear spaces.
4. Abelian groups and linear spaces. Cyclic groups.
5. Linear combinations and linear dependence/independence.

Next class

1. Structure of a linear space: basis, dimension.
2. Structure of $\mathbb{R}^n$.

The number of solutions and the rank of the coefficient matrix

Consider a linear system of equations n with m variables $\Rightarrow$ the coefficient matrix A of the system is $A_{n\times m}$.

1. $rank\, A \leq n$, $rank\, A \leq m$
2. If $rank\, A = n$ then the system is consistent.
3. If $rank\, A = m$ then the system has at most one solution.
4. If $rank\, A < m$ then the system either has infinitely many solutions OR inconsistent.

Remarks:

1. If $n < m$ then $rank\, A \leq n < m \Rightarrow$ infinitely many OR no solutions
2. If $n = m$ and

a. $rank\, A = n \Rightarrow$ there exists a unique solution

b. $rank\, A < n \Rightarrow$ infinitely many OR no solutions

Examples

1. Is $rank \begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 3 \\ 1 & 3 & 6 \end{pmatrix} = 3$?
2. Are the following matrices in rref?

$$a. \begin{pmatrix} 0 & 1 & 2 & 3 \end{pmatrix} \quad b. \begin{pmatrix} 1 & 2 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \quad c. \begin{pmatrix} 1 & -1 & 0 & 3 & 0 \\ 0 & 0 & 1 & 4 & 0 \\ 0 & 0 & 1 & 5 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

3. Find all 3×1 and 3×2 matrices in rref.
4. Solve the linear system

$$\left\{ \begin{array}{rcl} 3x_1 + 6x_2 + 9x_3 + 5x_4 + 25x_5 & = & 53 \\ 7x_1 + 14x_2 + 21x_3 + 9x_4 + 53x_5 & = & 105 \\ -4x_1 - 8x_2 - 12x_3 + 5x_4 - 10x_5 & = & 11 \end{array} \right.$$

Matrix Algebra

1. The sum of two matrices $A_{n\times m}$ and $B_{n\times m}$ is the matrix $C_{n\times m}$ s.t.
$$c_{ij} = a_{ij} + b_{ij},\ i = \overline{1,\ n}, j = \overline{1,\ m}.$$
2. The scalar product $\alpha A_{n\times m} = (\alpha a_{ij}), i = \overline{1,\ n}, j = \overline{1,\ m}.$
3. The product of a row-matrix $(a_1 \quad a_2 \quad a_3)$ and a column-matrix $\begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix}$ is
$$(a_1 \quad a_2 \quad a_3)\begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix} = a_1 b_1 + a_2 b_2 + a_3 b_3$$

Matrix Algebra

4. The product of a matrix $A_{n\times m}$ and a vector $\bar{x} \in \mathbb{R}^m$ is

$$A_{n\times m}\bar{x} = \begin{pmatrix} \bar{w}_1 \\ \bar{w}_2 \\ \vdots \\ \bar{w}_n \end{pmatrix} \bar{x} = (def) \begin{pmatrix} (\bar{w}_1, \bar{x}) \\ (\bar{w}_2, \bar{x}) \\ \vdots \\ (\bar{w}_n, \bar{x}) \end{pmatrix}$$

$$= (prop)(\bar{a}_1 \quad \bar{a}_2 \ldots \bar{a}_m)\bar{x} = x_1\bar{a}_1 + x_2\bar{a}_2 + \ldots + x_m\bar{a}_m$$

5. The product of a matrix $A_{n\times k}$ and a matrix $B_{k\times m}$ is

$$AB = (A\bar{b}_1 \quad A\bar{b}_2 \quad \ldots \quad A\bar{b}_m)_{n\times m}$$

Matrix Product: exercises

1. Let $A_G = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$ be the adjacency matrix of a graph G. Compute $trace\,(A)$.

$$trace(A) = a_{11} + a_{22} + a_{33} = 0$$

2. Compute A_G^2 and $trace\,(A_G^2)$. Find the good interpretation for $trace\,(A_G^2)$—the question is still open!

$$(A_G^2)_{ij} = \sum_{k=1}^{3} a_{ik}a_{kj} \Rightarrow \text{we count only terms with } a_{ik}a_{kj} \neq 0$$

$$\Rightarrow a_{ik} \neq 0,\ a_{kj} \neq 0 \iff \underbrace{a_{ik} = a_{kj} = 1}_{v_i \sim v_k \sim v_j} \text{ we count w.r.t } k$$

$$(A_G^2)_{ij} = \text{ the number of common neighbors of } v_i \text{ and } v_j$$

Matrix Product: exercises

3 Compute A_G^3. What are the entries $(A_G^3)_{ij}$?

$$(A_G^3)_{ij} = \sum_{k=1}^{3}\sum_{m=1}^{3} a_{ik}a_{km}a_{mj} \Rightarrow a_{ik}a_{km}a_{mj} \neq 0$$

$$\iff \underbrace{a_{ik} = a_{km} = a_{mj} = 1}_{v_i \sim v_k \sim v_m \sim v_j}$$

$(A_G^3)_{ij}$ is the number of walks of the length 3 from v_i to v_j

$$\boxed{(A_G^m)_{ij} \text{ is the number of walks of the length } m \text{ from } v_i \text{ to } v_j}$$

Remark: Recall, that a walk from v_i to v_j in a graph is a sequence of vertices

$$v_i - -v_p - -v_k - -v_r - -v_s - - \ldots - -v_j$$

The length of a walk is the number of edges in the walk.

Linear Combinations

Definition: If $\bar{y} = \alpha\bar{x}_1 + \ldots + \alpha_k\bar{x}_k$, then $\bar{y}$ is called a linear combination of $\bar{x}_1, \ldots, \bar{x}_k$ OR
we say that $\bar{y}$ is spanned by $\bar{x}_1, \ldots, \bar{x}_k$ and denote

$$\bar{y} = span(\bar{x_1}, \ldots, \bar{x_k})$$

Exercise: Is $\begin{pmatrix} 7 \\ 8 \\ 9 \end{pmatrix}$ a linear combination of $\begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}, \begin{pmatrix} 4 \\ 5 \\ 6 \end{pmatrix}$?

Yes. Solve the system $\begin{cases} 7 = a + 4b \\ 8 = 2a + 5b \\ 9 = 3a + 6b \end{cases} \Rightarrow a = -1,\ b = 2$

Lemma: Let $A = (\bar{a}_1 \quad \bar{a}_2 \quad \ldots \quad \bar{a}_n)$.

$$\bar{b} = span(\bar{a}_1, \ldots, \bar{a}_n) \iff rank\, A = rank\, A|\bar{b}$$

The proof of this statement is an EXTRA problem.

Linear Combinations: exercises

1. Compute $-\bar{a}_1 + 2\bar{a}_2$, $2\bar{a}_1 + 5\bar{a}_2$ for
$$\bar{a}_1 = (-2, 1, 3, 4),\ \bar{a}_2 = (3, 2, -2, 1)$$
2. Let $A = (\bar{a}_1 \quad \bar{a}_2)$. Compute $A\begin{pmatrix} -1 \\ 2 \end{pmatrix}$, $A\begin{pmatrix} 2 \\ 5 \end{pmatrix}$.
3. Compute $\alpha\bar{e}_1 + \beta\bar{e}_2 + \gamma\bar{e}_3$ with
$$\bar{e}_1 = (1, 0, 0),\ \bar{e}_2 = (0, 1, 0),\ \bar{e}_3 = (0, 0, 1)$$
4. Calculate
$$(\bar{e}_1 \quad \bar{e}_2 \quad \bar{e}_3)\begin{pmatrix} \alpha \\ \beta \\ \gamma \end{pmatrix}$$
5. Find a 3 matrix A s.t.
$$A\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}, A\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 4 \\ 5 \\ 6 \end{pmatrix}, A\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 7 \\ 8 \\ 9 \end{pmatrix}$$

Matrix Algebra: properties

1. $A + B = B + A$
2. $A + (B + C) = (A + B) + C$
3. $\exists$ the zero matrix $O = (0)_{ij}$ s.t. $A + O = O + A = A \quad \forall A$
4. $\forall A \quad \exists(-A)\colon A + (-A) = O$
5. $I_n A = A I_n = A$
6. $\alpha(A + B) = \alpha A + \alpha B \quad \forall \alpha \in \mathbb{R}$ or $\mathbb{C} \quad \forall A, B$
7. $(\alpha + \beta)A = \alpha A + \beta A \quad \forall \alpha, \beta \in \mathbb{R}$ or $\mathbb{C} \quad \forall A$
8. $(\alpha\beta)A = \alpha(\beta A) \quad \forall \alpha, \beta \in \mathbb{R}$ or $\mathbb{C} \quad \forall A$
9. $AB \neq BA \quad \forall A, B$

Definition: If $AB = BA$ then matrices A and B commute.

Exercise: Is there a matrix B s.t. $AB = BA$, $\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$? Find B.

$$B = \begin{pmatrix} b_1 & 2/3 b_3 \\ b_3 & b_1 + b_3 \end{pmatrix} = b_1 \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + b_3 \begin{pmatrix} 0 & 2/3 \\ 1 & 1 \end{pmatrix}$$

Number Field

Definition: A subset $\mathbb{F}$ of $\mathbb{C}$ is called a number field provided

1. $1 \in \mathbb{F}$
2. $\forall a, b \in \mathbb{F} \quad a \pm b \in \mathbb{F},\ ab \in \mathbb{F},\ a/b \in \mathbb{F}(b \neq 0)$

Examples:

- $\mathbb{R}$, $\mathbb{C}$
- The set of rational numbers $\mathbb{Q}$.
- $\mathbb{F} = \{a + b\sqrt{2} \colon a, b \in \mathbb{Q}\}$
- $\mathbb{F} = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \colon a, b, c \in \mathbb{Q}\}$

Abelian Groups

Definition: A set A with a binary operation $+ \colon A \times A \to A$, i.e. x, $y \to x + y$, is called an Abelian group provided

1. $x + y = y + x \quad \forall x, y \in A$ (commutativity)
2. $x + (y + z) = (x + y) + z \quad \forall x, y, z \in A$ (associativity)
3. $\exists 0$ s.t. $x + 0 = 0 + x = x \quad \forall x \in A$ (identity)
4. $\forall x \in A\, \exists (-x)$ s.t. $x + (-x) = 0$ (inverse)

Examples:

- $(\mathbb{N}, +)$ no additive inverses
- $(\mathbb{Z}, +)$ Yes $\quad (\mathbb{Q}, +)$ Yes $\quad (\mathbb{R}, +)$ Yes.
- $(\mathbb{Z}, \cdot)$, $(\mathbb{R}, \cdot)$ no multiplicative inverses
- $(\mathbb{Q} \setminus \{0\}, \cdot)$ Yes $\quad (\mathbb{R} \setminus \{0\}, \cdot)$ Yes

Cyclic Groups

Definition: We say that a, $b \in \mathbb{Z}$ are congruent modulo m, $m \in \mathbb{Z}$ and write $a \equiv b \mod m$ if

$$m | a - b \Rightarrow a - b = k \cdot m$$

Example: $7 + 3 \mod 6 = 4$, $12 \mod 7 = 5$
Definition: We denote $\mathbb{Z}_n$ all integers modulo n ($n > 0$).
Example: $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$
Definition: An Abelian group is cyclic if A is generated by an element: $\exists a \in A\colon\ A = \langle a \rangle, \quad \langle a \rangle = \{na,\ n \in \mathbb{Z}\}$

Example: $\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\} \Rightarrow \langle 0 \rangle = \{0\}$, $\langle 1 \rangle = \mathbb{Z}_7$,

$$\langle 2 \rangle = \{0, 2, 4, 6, 1, 3, 5\},\ \langle 3 \rangle = \{0, 3, 6, 2, 5, 1, 4, \} = \mathbb{Z}_7$$

1, 2, 3 are the generators of $\mathbb{Z}_7$. Other generators of $\mathbb{Z}_7$?

Linear Spaces

Definition: A set V is called a linear (vector) spaces over a field $\mathbb{F}$ if

1. $(V, +)$ is an Abelian group.
2. Scalar multiplication $\mathbb{F} \times V \to V$ is defined and satisfies the following properties:
   - $\exists 1 \in \mathbb{F}: \quad 1 \cdot v = v \quad \forall v \in V$
   - $(\alpha + \beta)v = \alpha v + \beta v \quad \forall \alpha, \beta \in \mathbb{F}, \forall v \in V$
   - $\alpha(v + w) = \alpha v + \alpha w \quad \forall \alpha \in \mathbb{F}, \forall v, w \in V$
   - $(\alpha\beta)v = \alpha(\beta v) \quad \forall \alpha, \beta \in \mathbb{F}, \forall v \in V$

Exercise: Show that $0 \cdot v = 0$, $\alpha \cdot 0 = 0$

Examples:

- $\mathbb{R}$ is a vector space over $\mathbb{R}$, $\mathbb{Q}$
- The set $\mathbb{R}[x]$ of all polynomials in x with real coefficients.
- The set $C[a, b]$ of all continuous functions $f : [a, b] \to \mathbb{R}$

Linear Spaces

More Examples:

- The set $\mathbb{M}_{n\times n}$ of all square matrices $n \times n$ with real/complex entries over $\mathbb{R}/\mathbb{C}$
- The set l of all infinite sequences of scalars.
- The set l_∞ of all bounded sequences of scalars.
- The set $l_p = \{\bar{x} = (x_1, x_2, \ldots) \colon \sum_{i=1}^{\infty} |x_i|^p < +\infty\}$ of all

  p-summable sequences.
  Prove:

$$\sum_{i=1}^{\infty} |x_i + y_i|^p \leq 2^p \sum_{i=1}^{\infty} |x_i|^p + 2^p \sum_{i=1}^{\infty} |y_i|^p$$

Field

Is $\mathbb{Z}_n$ a linear space?

- Well, scalar multiplication in $\mathbb{Z}_n$ over number fields is not defined. We define a general field:
- **Definition:** A set $\mathbb{F}$ is called a field provided it is an additive Abelian group with the additive inverse 0 and nonzero elements of $\mathbb{F}$ form a multiplicative Abelian group with the multiplicative inverse 1. AND Multiplication distributes addition

Is $\mathbb{Z}_n$ a field?

- Consider $\mathbb{Z}_4 = \{0, 1, 2, 3\}$.

  In $\mathbb{Z}_4$, $2 \cdot 2 = 4 = 0 \mod 4 \Rightarrow 2$ does not have a multiplicative inverse.

  $\mathbb{Z}_n$ is a field if $n = p$ is a prime number.

  $\mathbb{F}_2 = \mathbb{Z}_2 = \{0, 1\}$ is an important example of a finite field.

This Week

Today:

1. Linear subspaces.
2. Linear independence
3. Basis and dimension.
4. Distance in linear spaces.
5. Lagrange interpolation.

Next class:

1. Linear transformations in 2D and 3D.
2. Inverse linear transformations.

Linear Subspaces

Definition: Let V be a linear space over $\mathbb{K}$.
If $U \subset V$ and U is also a linear space closed w.r.t binary operations defined for V, then we say that U is a linear subspace of V:

1. $0_U = 0_V \in U$
2. $u_1, u_2 \in U \to u_1 + u_2 \in U$
3. $\alpha \in \mathbb{K}$, $u \in U \to \alpha u \in U$

Examples:

1. The linear space of all symmetric matrices ($A^T = A$) is a linear subspace of $\mathbb{M}_{n\times n}(\mathbb{R})$.
2. The linear space of all skew-symmetric matrices ($A^T = -A$) is a linear subspace of $\mathbb{M}_{n\times n}(\mathbb{R})$.
3. The linear space of all polynomials $P_n(\mathbb{R})$ of degree n or less is a linear subspace of $\mathbb{R}[x]$.
4. $U = \{\bar{x} = (x_1, x_2, \ldots) \in l \colon x_{n+2} = x_{n+1} + x_n\}$ is a linear subspace of l. Fibonacci Space

Linear Independence

Definition: Let $U_1, \ldots, U_m$ be linear subspaces of V.
The direct sum $U_1 \oplus \ldots \oplus U_m$ of $U_1, \ldots, U_m$ is a linear space s.t. any of its elements can be *uniquely* represented as

$$u_1 + \ldots + u_m, \quad u_i \in U_i,\ i = 1..m$$

Examples:

1. $U = \{(x, y, 0) \in \mathbb{R}^3 \colon x, y \in \mathbb{R}\},\ W = \{(0, 0, z) \in \mathbb{R}^3 \colon z \in \mathbb{R}\}$
$$\mathbb{R}^3 = U \oplus W$$
2. $U_i = \{(0, \ldots, 0, x_i, 0, \ldots, 0) \in \mathbb{R}^n \colon x_i \in \mathbb{R}\}, \quad i = 1, \ldots, n$
$$\mathbb{R}^n = U_1 \oplus \ldots \oplus U_n$$
3. $U_1 = \{(x, y, 0) \in \mathbb{R}^3 \colon x, y \in \mathbb{R}\},\ U_2 = \{(0, 0, z) \in \mathbb{R}^3 \colon z \in \mathbb{R}\}\ U_3 = \{(0, y, y) \in \mathbb{R}^3 \colon y \in \mathbb{R}\}$
$$\mathbb{R}^3 \neq U_1 \oplus U_2 \oplus U_3$$
$$(0, 0, 0) = (0, 0, 0) + (0, 0, 0) + (0, 0, 0)$$
$$(0, 0, 0) = (0, 1, 0) + (0, 0, 1) + (0, -1, -1)$$

Linear Independence

Definition: Elements $v_1, v_2, \ldots, v_n \in V$ are said to be linearly independent if

$$\alpha_1 v_1 + \alpha_2 v_2 + \ldots + \alpha_n v_n = 0 \Rightarrow \alpha_1 = \ldots = \alpha_n = 0$$

Remark: An infinite set of vectors is said to be linearly independent if *every finite subset is linearly independent*.
Definition: If

$$\alpha_1 v_1 + \alpha_2 v_2 + \ldots + \alpha_n v_n = 0 \Rightarrow \exists \alpha_i \neq 0$$

then the elements $v_1, v_2, \ldots, v_n \in V$ are said to be linearly dependent.

Linear Independence: Examples

1. $\bar{e}_1 = (1,0,0)$, $\bar{e}_2 = (0,1,0)$, $\bar{e}_3 = (0,0,1)$ Yes!!!
2. 1, $\cos 2x$, $\sin 2x$ Yes   1, $\cos 2x$, $\sin^2 x$ No
3. 1, $\sqrt{2}$, $\sqrt{3}$ are linearly independent in $\mathbb{R}$ only if $\mathbb{R}$ is a vector field over $\mathbb{Q}$.
4. $\mathbb{R}[x]$: $f(x) = \prod_{i=1}^{n}(x - \alpha_i) \Rightarrow g_j(x) = \dfrac{f(x)}{x - \alpha_j}$ are linearly independent
5. $M_{2\times 2}$: $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ Yes

Linear Independence: Exercises

1. Show that $\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$ are linearly independent.
2. Show that $\begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$ are linearly dependent.
3. Show that any 3 vectors are linearly dependent in $\mathbb{R}^2$.
4. If elements $v_1, \ldots, v_m \in V$ are linearly independent then non of v_i, $i = 1, \ldots, m$, is redundant.

Definition: A vector v_i is said to be redundant if it is represented as a linear combination of preceding vectors

$$v_i = \alpha_1 v_1 + \ldots + \alpha_{i-1} v_{i-1}$$

Normed Linear Spaces

Definition: Let X be a linear space over a scalar field $\mathbb{K}$. A real-valued function $||\cdot||: X \to \mathbb{R}$ defined on X is called a norm provided

1. $||x|| \geq 0 \quad \forall x \in X$ and $||x|| = 0$ iff $x = 0$
2. $||\alpha x|| = |\alpha| ||x|| \quad \forall x \in X \, \forall \alpha \in \mathbb{K}$
3. $||x + y|| \leq ||x|| + ||y|| \quad \forall x, y \in X$

Normed Linear Spaces: Examples

1. $\mathbb{R}$: $||x|| = |x|$
2. $\mathbb{R}^n$: $||\bar{x}||_\infty = \max_{i=1..n} |x_i|$, $||\bar{x}||_p = \left(\sum_{i=1}^{n} |x_i|^p \right)^{1/p}$, $p \geq 1$
3. $C[a,b]$: $||f(t)|| = \max_{t \in [a,b]} |f(t)|$, $\quad ||f(t)|| = \int_a^b |f(t)|\, dt$
4. l^∞: $||\bar{x}|| = \sup_{i=1..\infty} |x_i|$
5. l^p: $= ||\bar{x}||_p = \left(\sum_{i=1}^{\infty} |x_i|^p \right)^{1/p}$, $p \geq 1$
6. $\mathbb{M}_{n \times m}$: $||A|| = \sqrt{trace(A^T A)}$ Frobenius norm this def. works for real matrices

Basis

Definition: In a lin. space V, elements $v_1, \ldots, v_m$ form a basis if

1. $V = span(v_1, \ldots, v_m)$, and
2. $v_1, \ldots, v_m$ are linear independent.

Remark: If $v_1,\ v_2, \ldots, v_m \in V$ for a basis of V then $\forall x \in V$ there exists a unique representation

$$x = c_1 v_1 + c_2 v_2 + \ldots + c_m v_m, \quad c_1, \ldots, c_m \in \mathbb{K}.$$

Definition: The scalars $c_1, \ldots, c_m$ are called coordinates of $x \in V$ in the basis $v_1, \ldots,\ v_m$.

Example: Let $V = span\left(\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}\right)$.

$$\bar{v}_1 = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \bar{v}_2 = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} \text{ are linearly independent}$$

$$\Rightarrow B = \{\bar{v}_1, \bar{v}_2\} \text{ is a basis in } V$$

$$\bar{u} = (5, 7, 9) \Rightarrow \bar{u} = 3\bar{v}_1 + 2\bar{v}_2 \Rightarrow \bar{u}_B = (3, 2)$$

Basis

Theorem: Any maximal linearly independent set is a basis.
Theorem: If $a_1, \ldots, a_p \in V$ are linearly independent and $V = span(b_1, \ldots, b_q)$, then $p \leq q$.

1. Steinitz exchange principle: $\forall i = 1..p \quad \exists j = 1..q \quad$ s.t. $a_1, \ldots, a_{i-1}, b_j, a_{i+1}, \ldots, a_p$ are linearly independent.
2. If $q > p$ then you will get $a_1, \ldots, a_{i-1}, b_j, a_{i+1}, \ldots, a_p$ linear independent and then $a_1, \ldots, a_{i-1}, a_i, b_j, \ldots, a_p$ can't be linearly independent $\Rightarrow p \leq q$

Remark: All bases of a linear space have the same number of elements.
Remark: If dim $V = m$, then any m linearly independent elements for a basis in V, and any span of V consisting of m vectors forms a basis as well.
Example:

1. The vectors $(1, 2, 3)$, $(4, 5, 8)$, $(9, 6, 7)$, $(-3, 2, 8)$ are not linearly independent in $\mathbb{R}^3$.
2. The vectors $(1, 2, 3, -5)$, $(4, 5, 8, 3)$, $(9, 6, 7, -2)$ do not span $\mathbb{R}^4$

Basis

- Any spanning set of vectors can be reduced to a basis of a linear space.
- Any set of linear independent set of elements can be extended to a basis of a linear space.

$$\mathbb{R}^3\text{: } (2,3,4),\ (9,6,8) \text{ are linearly independent}$$

$$\Rightarrow \begin{pmatrix} 2 \\ 3 \\ 4 \end{pmatrix}, \begin{pmatrix} 9 \\ 6 \\ 8 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$

$$\begin{pmatrix} 2 \\ 3 \\ 4 \end{pmatrix}, \begin{pmatrix} 9 \\ 6 \\ 8 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \text{ is a basis for } \mathbb{R}^3$$

- If V has a finite basis and U is a linear subspace of V, then there exists a linear subspace W of V such that

$$V = U \oplus W$$

Dimension

Definition: The number of elements in the basis is called the dimension of a linear space.

Examples:

1. $\dim \mathbb{R}^n = n$, and
2. $\dim C[a, b] = \infty$
3. $\dim \mathbb{M}_{2\times 2} = 4$
4. $\dim P_n(\mathbb{R}) = n + 1$.
5. $\dim U \oplus W = \dim U + \dim W$
   - $\dim (U + W) = \dim U + \dim W - \dim (U \cap W)$
   - Let $u_1, \ldots, u_m$ be a basis of $U \cap W \Rightarrow$ we can extend it up to the basis $u_1, \ldots, u_m, v_1, \ldots, v_j$ of U and up to the basis $u_1, \ldots, u_m, w_1, \ldots, w_k$ of W.
   - $\dim U = m + j$, $\dim W = m + k$
   - Show that $u_1, \ldots, u_m, v_1, \ldots, v_j, w_1, \ldots, w_k$ is the basis for $U + W \Rightarrow \dim (U + W) = m + j + k = (m + j) + (m + k) - m = \dim U + \dim W - \dim (U \cap W)$

Bases

Q: Why do we need to consider different bases in a linear space?

- Is the standard basis $e_i = (0, \ldots, \underbrace{1}_{i\ th}, \ldots, 0)$ a "good" basis in $\mathbb{R}^n$?
- It gives us only the coordinates of a point. Can we form bases that keep other information?
- Let each coordinate represent brightness of a pixel in an image $\Rightarrow$ the brightness of the whole image is $x_1 + \ldots + x_n$, $x_1 - x_2 + x_3 - \ldots + (-1)^n x_n$ is the "jaggedness" of the image.
- $\mathbb{R}^2$: the vectors $v_1 = (1, 1)$, $v_2 = (1, -1)$ are linearly independent $\Rightarrow \{v_1,\ v_2\}$ is the basis.

$$x = \frac{x_1 + x_2}{2} v_1 + \frac{x_1 - x_2}{2} v_2$$

The coordinates of $x = (x_1, x_2)$ in the basis $\mathfrak{B} = \{v_1,\ v_2\}$ are

$$x_{\mathfrak{B}} = \frac{x_1 + x_2}{2}, \ \frac{x_1 - x_2}{2}$$

Lagrange Interpolation

- You know that p is a polynomial and $deg(p) \leq n-1$. Also $p(\alpha_i) = b_i$, $i = 1, \ldots, n$. Find p.
- The n polynomials

$$g_j = \frac{\prod_{i=1}^{n}(x - \alpha_i)}{x - \alpha_j}$$

  are linearly independent.

  $\Rightarrow g_j$, $j = 1, \ldots, n$ form a basis of $P_{n-1}(\mathbb{R})$.

  $\Rightarrow \forall p \in P_{n-1}(\mathbb{R}) \quad \exists c_j \colon p = \sum_j c_j g_j$
- The coefficients c_j equal

$$c_i = \frac{p(\alpha_i)}{(\alpha_i - \alpha_1) \ldots (\alpha_i - \alpha_{i-1})(\alpha_i - \alpha_{i+1}) \ldots (\alpha_i - \alpha_n)}$$

Lagrange Interpolation

- You want to keep your special code safe and you know 5 reliable friends. Ensure that you need only 3 people to recover your code.
- Consider a polynomial $p = code + p_1 x + p_2 x^2$.
- Choose a_1, a_2, a_3, a_4, a_5 and set $b_i = p(a_i)$.
- Give (a_i, b_i) to your ith friend.

Simplest Coding-Decoding Transformations

- Your location at the JI ($\approx x_1 = 121,\ x_2 = 31$) is sent to the central admin. The coordinates are encoded with the code

$$y_1 = x_1 - x_2$$
$$y_2 = -5x_1 + x_2$$

- The received coordinates are

$$\bar{y} = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} 121 - 31 \\ -5 \cdot 121 + 31 \end{pmatrix} = \begin{pmatrix} 90 \\ -574 \end{pmatrix}$$

- The coding transformation is

$$\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} x_1 - x_2 \\ -5x_1 + x_2 \end{pmatrix} = \underbrace{\begin{pmatrix} 1 & -1 \\ -5 & 1 \end{pmatrix}}_{A} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$$

- A transformation of the form $\bar{y} = A\bar{x}$ is called a linear transformation.

Simplest Coding-Decoding Transformations

- ⋆ How can one find your actual location?
- ⋆ One has to solve the system

$$\begin{cases} x_1 - x_2 = y_1 \\ -5x_1 + x_2 = y_2 \end{cases}$$

- ⋆ $\bar{y} \to \bar{x}$ is the decoding transformation.
- ⋆

$$\begin{cases} x_1 = -\frac{1}{4}y_1 - \frac{1}{4}y_2 \\ x_2 = -\frac{5}{4}y_1 - \frac{1}{4}y_2 \end{cases}$$

- ⋆ The inverse (decoding) transformation is $\bar{x} = B\bar{y}$

$$B = \begin{pmatrix} -\frac{1}{4} & -\frac{1}{4} \\ -\frac{5}{4} & -\frac{1}{4} \end{pmatrix}$$

- ⋆ B is the coefficient matrix of the inverse transformation.

Simplest Coding-Decoding Transformations

Q: Is it possible to find the inverse transformation for any linear transformation?

- ⋆ Consider a linear transformation

$$\begin{cases} y_1 = & x_1 - x_2 \\ y_2 = & -2x_1 + 2x_2 \end{cases}$$

- ⋆

$$\begin{cases} x_1 - x_2 = & y_1 \\ 0 = & 2y_1 + y_2 \end{cases}$$

- ⋆ The system does not have a solution unless $y_2 = -2y_1$, and it gives infinitely many solutions.
- ⋆ The inverse transformation does not exist.
- ⋆ What do you notice about the coefficient matrix

$$A = \begin{pmatrix} 1 & -1 \\ -2 & 2 \end{pmatrix}?$$

Linear Transformations

Definition: A function $T\colon \mathbb{R}^m \to \mathbb{R}^n$ is called a linear transformation if there exists an $n \times m$ matrix A such that $T\bar{x} = A\bar{x} \quad \forall \bar{x} \in \mathbb{R}^m$.

Remark: A linear transformation is a special case of a linear operator:

Let V, U be linear spaces over $\mathbb{K}$. A map $T\colon V \to U$ is a linear operator if

1. $T(v_1 + v_2) = Tv_1 + Tv_2 \quad \forall\, v_1, v_2 \in V$
2. $T(\alpha v) = \alpha Tv \quad \forall\, \alpha \in \mathbb{K}, \forall v \in V$

Examples:

1. $T\colon \mathbb{R}^3 \to \mathbb{R}^2$, $A = \begin{pmatrix} 1 & -2 & 1 \\ 0 & 1 & 2 \end{pmatrix}$
2. The identity transformation

$$I\colon \mathbb{R}^n \to \mathbb{R}^n,\ I = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}$$

Linear Transformations

3 Let $T\bar{x} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \bar{x}$

$$\begin{pmatrix} 0 \\ 2 \end{pmatrix} \to \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 2 \end{pmatrix} = \begin{pmatrix} -2 \\ 0 \end{pmatrix}$$

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \to \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

The rotation through $\frac{\pi}{2}$ in the counterclockwise direction.

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \to \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} -x_2 \\ x_1 \end{pmatrix}$$

$$\Rightarrow \sqrt{x_1^2 + x_2^2} = \sqrt{(-x_1)^2 + x_2^2}$$

Linear Transformations

For a linear transformation with $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, find the inverse linear transformation.

$$\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \bar{y} = T\bar{x} = A\bar{x} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$$

$$\begin{cases} x_1 = & \dfrac{1}{ad-cb}(dy_1 - by_2) \\ x_2 = & \dfrac{1}{ad-cb}(ay_2 - cy_1) \end{cases} \Rightarrow B = \frac{1}{ad-cb} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

$$\bar{x} = B\bar{y}$$

Linear Transformations

Definition: For a matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, the quantity $ad - bc$ is called the determinant of A:

$$\det A = |A| = \begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc$$

If $\det A \neq 0$, then the inverse linear transformation exists and

$$B = A^{-1} = \frac{1}{\det A} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

Lemma: Let $A = (\bar{a}_1 \quad \bar{a}_2)$ be a non-zero matrix. Then

1. $\det A = |\bar{a}_1| \sin\theta |\bar{a}_2|$ where θ is oriented from $\bar{a}_1$ to $\bar{a}_2$, $-\pi < \theta < \pi$
2. The area of the parallelogram spanned by $\bar{a}_1$, $\bar{a}_2$ is $\det A$.
3. $\det A = 0 \Rightarrow \bar{A}_1 || \bar{a}_2$