

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

Dr.Olga Danilkina

UM-SJTU Joint Institute



May 19, 2020

# Today 5/15/2020

## Today 5/15/2020

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 5/19/2020

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

### Remarks:

1. If  $n < m$  then  $\text{rank } A \leq n < m \Rightarrow$  infinitely many OR no solutions
2. If  $n = m$  and
  - a.  $\text{rank } A = n \Rightarrow$  there exists a unique solution
  - b.  $\text{rank } A < n \Rightarrow$  infinitely many OR no solutions

## Examples

1. Is  $\text{rank} \begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 3 \\ 1 & 3 & 6 \end{pmatrix} = 3$ ?

2. Are the following matrices in rref?

a.  $\begin{pmatrix} 0 & 1 & 2 & 3 \end{pmatrix}$     b.  $\begin{pmatrix} 1 & 2 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$     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  $3 \times 1$  and  $3 \times 2$  matrices in rref.

4. Solve the linear system

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

# 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  $(a_1 \ a_2 \ a_3)$  and a

column-matrix  $\begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix}$  is

$$(a_1 \ a_2 \ a_3) \begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix} = a_1 b_1 + a_2 b_2 + a_3 b_3$$

# Matrix Algebra

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

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

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

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

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

## 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  $\text{trace}(A)$ .
2. Compute  $A_G^2$  and  $\text{trace}(A_G^2)$ . Find a good interpretation for  $A_G^2$ ,  $\text{trace}(A_G^2)$ .

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

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

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

## 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  $v_j$

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

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

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

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



# Linear Combinations

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

$$\bar{y} = \text{span}(\bar{x}_1, \dots, \bar{x}_k)$$

**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  $A = (\bar{a}_1 \quad \bar{a}_2 \quad \dots \quad \bar{a}_n)$ .

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

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.  $\forall A \quad \exists(-A): A + (-A) = O$
5.  $I_n A = A I_n = A$
6.  $\alpha(A + B) = \alpha A + \alpha B \quad \forall \alpha \in \mathbb{R} \text{ or } \mathbb{C} \quad \forall A, B$
7.  $(\alpha + \beta)A = \alpha A + \beta A \quad \forall \alpha, \beta \in \mathbb{R} \text{ or } \mathbb{C} \quad \forall A$
8.  $(\alpha\beta)A = \alpha(\beta A) \quad \forall \alpha, \beta \in \mathbb{R} \text{ or } \mathbb{C} \quad \forall A$
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.  $AB = BA$ ,  $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ ? Find  $B$ .

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

Today 5/19/2020

Today 5/19/2020

1. Number fields and linear spaces.
2. Abelian groups and linear spaces. Cyclic groups.
3. Rings, commutative rings, integral domain.
4. Fields.
5. Linear subspaces.

# 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  $\mathbb{Q}$ .
- ▶  $\mathbb{F} = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$
- ▶  $\mathbb{F} = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} : a, b, c \in \mathbb{Q}\}$

# Abelian Groups

**Definition:** A set  $A$  with a binary operation  $+: A \times A \rightarrow A$ , i.e.  $x, y \rightarrow x + y$ , 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**    $(\mathbb{Q}, +)$  **Yes**    $(\mathbb{R}, +)$  **Yes**.
- ▶  $(\mathbb{Z}, \cdot), (\mathbb{R}, \cdot)$  **no multiplicative inverses**
- ▶  $(\mathbb{Q} \setminus \{0\}, \cdot)$  **Yes**    $(\mathbb{R} \setminus \{0\}, \cdot)$  **Yes**

# Rings

Define one more operation on an abelian group  $\Rightarrow$  a ring, provided the elements of the set satisfy some properties with respect to this new operation.

**Definition:** A **ring**  $\{R, +, \times\}$  is a set  $R$  of objects s.t  $\{R, +\}$  is an abelian group and

- ▶  $R$  is closed w.r.t.  $\times$
- ▶  $a \times (b \times c) = (a \times b) \times c \quad \forall a, b, c \in R$
- ▶  $a \times (b + c) = a \times b + a \times c, (a + b) \times c = a \times c + b \times c \quad \forall a, b, c \in R$

**Examples:**

1.  $\{\mathbb{Z}, +, \times\}, \{\mathbb{R}, +, \times\}$
2. Let  $n \in \mathbb{N}$ . The set of all square matrices  $M_{n \times n}$  is a ring under matrix addition and matrix multiplication.

**Definition:** A ring  $R$  is commutative if the multiplication operation  $\times$  is commutative for all elements in the ring:

$$a \times b = b \times a \quad \forall a, b \in R$$

# Integral Domains

**Definition:** An **integral domain**  $\{R, +, \times\}$  is a commutative ring that obeys the following two additional properties:

1. The set  $R$  must include an identity element for the multiplicative operation. It should be possible to symbolically designate an element of the set  $R$  as '1' so that

$$a \times 1 = 1 \times a = a$$

2. Let 0 denote the identity element for the addition operation. If a multiplication of any two elements  $a$  and  $b$  of  $R$  results in 0, that is if  $a \times b = 0$ , then either  $a$  or  $b$  must be 0.

**Examples:**  $\{\mathbb{Z}, +, \times\}$ ,  $\{\mathbb{R}, +, \times\}$



# Modular Arithmetic

**Definition:** We say that  $a, b \in \mathbb{Z}$  are **congruent modulo  $n$** ,  $n \in \mathbb{Z}$  and write  $a \equiv b \pmod{n}$  if  $a$  and  $b$  have the same remainder after division by  $n$ .

Recall, that  $\forall a \in \mathbb{Z}, d \in \mathbb{Z}_+ \exists! q, r \in \mathbb{Z} : 0 \leq r < d, a = d \cdot q + r$

**Example:**  $7 + 3 \pmod{6} = 4, 12 \pmod{7} = 5$

**Lemma:**

$$a \equiv b \pmod{n} \Leftrightarrow n \mid a - b \quad (a - b = k \cdot n)$$

1.  $a \equiv a \quad \forall a \in \mathbb{Z}$
2.  $a \equiv b \Rightarrow b \equiv a \quad \forall a, b \in \mathbb{Z}$
3.  $a \equiv b, c \equiv d \Rightarrow a \pm c \equiv b \pm d \quad \forall a, b, c, d \in \mathbb{Z}$
4.  $a \equiv b, c \equiv d \Rightarrow a \cdot c \equiv b \cdot d \quad \forall a, b, c, d \in \mathbb{Z}$
5.  $a \equiv b \Rightarrow a^j \equiv b^j, j \geq 1 \quad \forall a, b \in \mathbb{Z}$

$\mathbb{Z}_n$ 

**Definition:** We denote  $\mathbb{Z}_n$  all integers modulo  $n$  ( $n > 0$ ):

$$\mathbb{Z}_n = \{[0], [1], \dots, [n-1]\}$$

**Remark:**  $\forall a \in \mathbb{Z} \quad [a] = [a']$  iff  $a \equiv a'$ .

**Example:**  $\mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\}$  We can just write

$$\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$$

$$\forall [a], [b] \in \mathbb{Z}_b: \quad [a] \pm [b] = [a \pm b], \quad [a] \cdot [b] = [a \cdot b]$$

**Example:** Write out addition and multiplication in  $\mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_4$ .

# Cyclic Groups

**Definition:** An Abelian group is **cyclic** if  $A$  is **generated** by an element:  $\exists a \in A: A = \langle a \rangle, \quad \langle a \rangle = \{na, n \in \mathbb{Z}\}$

**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  $\mathbb{F} \times V \rightarrow V$  is defined and satisfies the following properties:
  - ▶  $\exists 1 \in \mathbb{F}: 1 \cdot v = v \quad \forall v \in V$
  - ▶  $(\alpha + \beta)v = \alpha v + \beta v \quad \forall \alpha, \beta \in \mathbb{F}, \forall v \in V$
  - ▶  $\alpha(v + w) = \alpha v + \alpha w \quad \forall \alpha \in \mathbb{F}, \forall v, w \in V$
  - ▶  $(\alpha\beta)v = \alpha(\beta v) \quad \forall \alpha, \beta \in \mathbb{F}, \forall v \in V$

**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  $f: [a, b] \rightarrow \mathbb{R}$

# 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  $l_\infty$  of all bounded sequences of scalars.
- ▶ The set  $l_p = \{\bar{x} = (x_1, x_2, \dots) : \sum_{i=1}^{\infty} |x_i|^p < +\infty\}$  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  $\mathbb{Z}_4$ ,  $2 \cdot 2 = 4 = 0 \pmod{4} \Rightarrow 2$  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.

$$\mathbb{Z}_n$$

1. Is  $\mathbb{Z}_n$  a group? If so, what is the group operator?
2. Is  $\mathbb{Z}_n$  an abelian group?
3. Is  $\mathbb{Z}_n$  a ring?  $\mathbb{Z}_n$  is more than a commutative ring, but not quite an integral domain. What does it mean?
4. Why is  $\mathbb{Z}_n$  not an integral domain?

# 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.  $u_1, u_2 \in U \rightarrow u_1 + u_2 \in U$
3.  $\alpha \in \mathbb{K}, u \in U \rightarrow \alpha u \in U$

**Examples:**



# Interesting Problems

1. Find an abelian group  $V$  and a field  $F$  for which  $V$  is a vector space over  $F$  in at least two different ways, that is, there are two different definitions of scalar multiplication making  $V$  a linear space over  $F$ .
2. Find a linear space  $V$  over  $F$  and a subset  $S \subset V$  that is
  - ▶ a subspace of  $V$ , and
  - ▶ a vector space using operations that differ from those of  $V$ .

# Linear Independence

**Definition:** Let  $U_1, \dots, U_m$  be linear subspaces of  $V$ .

The **direct sum**  $U_1 \oplus \dots \oplus U_m$  of  $U_1, \dots, U_m$  is a linear space s.t. any of its elements can be *uniquely* represented as

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

**Examples:**

1.  $U = \{(x, y, 0) \in \mathbb{R}^3 : x, y \in \mathbb{R}\}, \quad W = \{(0, 0, z) \in \mathbb{R}^3 : z \in \mathbb{R}\}$

$$\mathbb{R}^3 = U \oplus W$$

2.  $U_i = \{(0, \dots, 0, x_i, 0, \dots, 0) \in \mathbb{R}^n : x_i \in \mathbb{R}\}, \quad i = 1, \dots, n$

$$\mathbb{R}^n = U_1 \oplus \dots \oplus U_n$$

3.  $U_1 = \{(x, y, 0) \in \mathbb{R}^3 : x, y \in \mathbb{R}\}, \quad U_2 = \{(0, 0, z) \in \mathbb{R}^3 : z \in \mathbb{R}\}$   
 $U_3 = \{(0, y, y) \in \mathbb{R}^3 : y \in \mathbb{R}\}$

$$\mathbb{R}^3 \neq U_1 \oplus U_2 \oplus U_3$$

$$(0, 0, 0) = (0, 0, 0) + (0, 0, 0) + (0, 0, 0)$$

$$(0, 0, 0) = (0, 1, 0) + (0, 0, 1) + (0, -1, -1)$$

# Linear Independence

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

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

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

**Definition:** If

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

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

## Linear Independence: Examples

## 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  $v_1, \dots, v_m \in V$  are linearly independent then non of  $v_i, i = 1, \dots, m$ , is redundant.

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

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

# Normed Linear Spaces

**Definition:** Let  $X$  be a linear space over a scalar field  $\mathbb{K}$ . A real-valued function  $\|\cdot\|: X \rightarrow \mathbb{R}$  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.  $C[a, b]$ :  $\|f(t)\| = \max_{t \in [a, b]} |f(t)|$ ,  $\|f(t)\| = \int_a^b |f(t)| dt$

4.  $l^\infty$ :  $\|\bar{x}\| = \sup_{i=1..\infty} |x_i|$

5.  $l^p$ :  $\|\bar{x}\|_p = \left( \sum_{i=1}^{\infty} |x_i|^p \right)^{1/p}$ ,  $p \geq 1$

6.  $\mathbb{M}_{n \times m}$ :  $\|A\| = \sqrt{\text{trace}(A^T A)}$  **Frobenius norm** this def. works for real matrices

## Basis

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

1.  $V = \text{span}(v_1, \dots, v_m)$ , and
2.  $v_1, \dots, v_m$  are linear independent.

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

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

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

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

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

$\Rightarrow B = \{\bar{v}_1, \bar{v}_2\}$  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  $a_1, \dots, a_p \in V$  are linearly independent and  $V = \text{span}(b_1, \dots, b_q)$ , then  $p \leq q$ .

**Remark:** All bases of a linear space have the same number of elements.

**Remark:** If  $\dim V = m$ , then any  $m$  linearly independent elements form a basis in  $V$ , and any span of  $V$  consisting of  $m$  vectors forms a basis as well.

**Example:**

# 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.

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

Consider the linearly independent vectors with vectors that span  $\mathbb{R}^3$ :

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

Eliminating linearly dependent vectors from this system, you obtain basis elements:

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

# Basis

## Examples

1.  $U = \text{span}(2, 3, 4), (9, 6, 8))$  is a linear subspace of  $\mathbb{R}^3$ , and  $(2, 3, 4), (9, 6, 8), (0, 1, 0)$  is a basis for  $\mathbb{R}^3$

$$\text{Let } W = \text{span} \left\{ \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \right\} \Rightarrow V = U \oplus W$$

2. Let  $M = \{p(t) \in P_2(\mathbb{R}) : p(1) = 0\}$ .

# Dimension

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

**Examples:**

1.  $\dim \mathbb{R}^n = n$

# Dimension

## Examples:

2.  $\dim C[a, b] = \infty$

3.  $\dim \mathbb{M}_{2 \times 2} = 4$

# Dimension

## Examples:

4.  $\dim P_n(\mathbb{R}) = n + 1$

5.  $\dim U \oplus W = \dim U + \dim W$

# Bases

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

- ▶ Is the standard basis  $e_i = (0, \dots, \underbrace{1}_{i\text{th}}, \dots, 0)$  a "good" basis in  $\mathbb{R}^n$ ?
- ▶ It gives us only the coordinates of a point. Can we form bases that keep other information?



# Lagrange Interpolation

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

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

are linearly independent.

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

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

- ▶ The coefficients  $c_j$  equal

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