

Math 115AH – Honors Linear Algebra

University of California, Los Angeles

Duc Vu

Fall 2020

This is math 115AH – Honors Linear Algebra, a traditional first upper-division course that UCLA math students usually take. It's taught by Professor Elman, and our TA is Harris Khan. We meet weekly on MWF at 2:00pm – 2:50pm for lectures, and our discussion is on TR at 2:00pm – 2:50pm. With regard to book, we use *Linear Algebra 2nd* by *Hoffman and Kunze* for the class. Note that some of the theorems' name are not necessarily the official name of the theorem; it's just a way to assign meaning to a theorem (easier for reference) instead of a tedious section number. Other course notes can be found through my [github](#) site. Please contact me at ducvu2718@ucla.edu if you find any concerning mathematical errors/typos.

Contents

1	Lec 1: Oct 2, 2020	4
1.1	Field	4
2	Lec 2: Oct 5, 2020	6
2.1	Field(Cont'd)	6
2.2	Vector Space	8
3	Lec 3: Oct 7, 2020	10
3.1	Vector Space(Cont'd)	10
3.2	Subspace	13
4	Lec 4: Oct 9, 2020	14
4.1	Span & Subspace	14
4.2	Linear Independence	17
5	Lec 5: Oct 12, 2020	18
5.1	Linear Independence(Cont'd)	18
6	Lec 6: Oct 14, 2020	22
6.1	Bases	22
7	Lec 7: Oct 16, 2020	25
7.1	Replacement Theorem	25
7.2	Main Theorem	26
7.3	A Glance at Dimension	27

8 Lec 8: Oct 19, 2020	28
8.1 Extension and Counting Theorem	28
8.2 Linear Transformation	31
9 Lec 9: Oct 21, 2020	32
9.1 Kernel, Image, and Dimension Theorem	32
9.2 Algebra of Linear Transformation	34
9.3 Linear Transformation Theorems	35
10 Lec 10: Oct 23, 2020	37
10.1 Monomorphism, Epimorphism, and Isomorphism	37
10.2 Existence of Linear Transformation	39
11 Dis 1: Oct 1, 2020	41
11.1 Sets	41
11.2 Functions	41
12 Dis 2: Oct 6, 2020	43
12.1 Field	43
13 Dis 3: Oct 8, 2020	46
13.1 Characteristics of a Finite Field	46
14 Dis 4: Oct 13, 2020	48
14.1 Vector Space and Subspace	48
15 Dis 5: Oct 15, 2020	51
15.1 Linear Independence, Span, & Subspaces	51
16 Dis 6: Oct 20, 2020	55
16.1 Review of Linear Independence & Dependence	55
17 Dis 7: Oct 22, 2020	58
17.1 Review of Linear Independence and Linear Transformation	58
17.2 Hw2 # 1	60

List of Theorems

3.4 Subspace	13
5.6 Toss In	21
6.4 Coordinate	23
6.5 Toss Out	23
7.1 Replacement	25
7.2 Main	26
8.1 Extension	29
8.4 Counting	29
9.4 Dimension	33
10.3 Monomorphism	37
10.5 Isomorphism	38

10.7	Existence of Linear Transformation (UPVS)	40
17.3		60
17.4		60

List of Definitions

1.2	Field	5
2.1	Vector Space	9
3.3	Subspace	13
4.1	Linear Combination	14
4.2	Span	15
4.4	Subspace & Span	16
5.1	Linear Independence & Dependence	18
6.1	Basis	22
6.3	Ordered Basis	22
8.6	Linear Transformation	31
9.1	Kernel(Nullspace)	32
9.2	Range(Image)	33
9.7	Linear Operator	35
9.9	Properties/Consequences of Linear Transformation	36
10.2	Linear Map	37
11.3	Injection & Surjection	42
12.1	(1.2)	44
14.1	(2.1)	48
17.2	(6.1)	59

§1 | Lec 1: Oct 2, 2020

Remark 1.1. To know a definition, theorem, lemma, proposition, corollary, etc., you must

1. Know its precise statement and what it means without any mistake
2. Know explicit example of the statement and specific examples that do not satisfy it
3. Know consequences of the statement
4. Know how to compute using the statement
5. At least have an idea why you need the hypotheses – e.g., know counter-examples,...
6. Know the proof of the statement
7. Know the important (key) steps of in the proof, separate from the formal part of the proof – i.e., the main idea(s) of the proof

THIS IS NOT EASY AND TAKES TIME – EVEN WHEN YOU THINK THAT YOU HAVE MASTERED THINGS.

§1.1 Field

What are the properties of the REAL NUMBERS?

$$\mathbb{R} := \{x | x \text{ is a real no.}\}$$

– at least algebraically?

There are two FUNCTIONS (or MAPS)

- $+: \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$ called ADDITION write $a + b := +(a, b)$
- $\cdot: \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$ called MULTIPLICATION write $a \cdot b := \cdot(a, b)$

that satisfy certain rule e.g., associativity, commutativity,...

Definition 1.2 (Field) — A set F is called a FIELD if there are two functions

- Addition: $+: F \times F \rightarrow F$, write $a + b := +(a, b)$
- Multiplication: $\cdot: F \times F \rightarrow F$, write $a \cdot b := \cdot(a, b)$

satisfying the following AXIOMS(A: addition, M: multiplication, D: distributive)

A1 $(a + b) + c = a + (b + c)$ Associativity

A2 \exists an element $0 \in F \ni a + 0 = a = 0 + a$ Existence of a Zero

A3 $\forall x \in F \exists y \in F \ni x + y = 0 = y + x$ Existence of an Additive Inverse

A4 $a + b = b + a$ Commutativity

M1 $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

M2 (A2) holds and \exists an element $1 \in F$ with $1 \neq 0 \ni a \cdot 1 = a = 1 \cdot a$ Existence of a One

M3 (M2) holds and $\forall 0 \neq x \in F \exists y \in F \ni xy = 1 = yx$ Existence of a Multiplicative Inverse

M4 $x \cdot y = y \cdot x$

D1 $a \cdot (b + c) = a \cdot b + a \cdot c$ Distributive Law

D2 $(a + b) \cdot c = a \cdot c + b \cdot c$

Comments: Let F be a field, $a, b \in F$. Then the following are true

1. $F \neq \emptyset$ (F at least has 2 elements)
2. 0 and 1 are unique
3. If $a + b = 0$, then b is unique write b as $-a$:
if $a + b = a + c$, then

$$\begin{aligned} b &= b + 0 \\ &= b + (a + c) \\ &= (b + a) + c \\ &= (a + b) + c \\ &= 0 + c \\ &= c \end{aligned}$$

4. if $a + b = a + c$, then $b = c$
5. if $a \neq 0$ and $ab = 1 = ba$, then b is unique write a^{-1} for b .
6. $0 \cdot a = 0 \forall a \in F$

$$0 \cdot a + 0 \cdot a = (0 + 0) \cdot a = 0 \cdot a = 0 \cdot a + 0$$

so $0 \cdot a = 0$ by 3.

7. if $a \cdot b = 0$, then $a = 0$ or $b = 0$. If $a \neq 0$, then $0 = a^{-1}(ab) = (a^{-1}a)b = 1b = b$

8. if $a \cdot b = a \cdot c$, $a \neq 0$, then $b = c$

9. $(-a)(-b) = ab$

10. $-(-a) = a$

11. if $a \neq 0$, then $a^{-1} \neq 0$ and $(a^{-1})^{-1} = a$

Example 1.3

$$\mathbb{Q} := \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0 \right\}$$

$\mathbb{R} :=$ set of real no.

$\mathbb{C} := \{a + bi \mid a, b \in \mathbb{R}\}$ with

$$\begin{aligned} (a + b\sqrt{-1}) + (c + d\sqrt{-1}) &= (a + c) + (b + d)\sqrt{-1} \\ (a + b\sqrt{-1}) \cdot (c + d\sqrt{-1}) &= (ac - bd) + (ad + bc)\sqrt{-1} \end{aligned}$$

$\forall a, b, c, d \in \mathbb{R}$

Under usual $+$, \cdot of \mathbb{C}

$$\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$$

are all field and we say \mathbb{Q} is a **subfield** of \mathbb{R} , \mathbb{Q}, \mathbb{R} **subfield** of \mathbb{C} , i.e., they have the same $+$, \cdot , $0, 1$.

\mathbb{Z} is not a field as $\nexists n \in \mathbb{Z} \ni 2n = 1$, so \mathbb{Z} do not satisfy (M3).

Note: To show something is FALSE, we need only one COUNTER-EXAMPLE. To show something is TRUE, one needs to show true for all elements – not just example.

§2 | Lec 2: Oct 5, 2020

§2.1 Field(Cont'd)

Note: \mathbb{Z} does satisfy the weaker properly if $a, b \in \mathbb{Z}$ then

(M3') if $ab = 0$ in \mathbb{Z} , then $a = 0$ or $b = 0$ and all other axioms except M3 hold

1. Let $F = \{0, 1\}$, $0 \neq 1$. Define $+$, \cdot by following table Then F is a field.

Table 1: ADDITION

$+$	0	1
0	0	1
1	1	0

Table 2: MULTIPLICATION

\cdot	0	1
0	0	0
1	0	1

2. \exists fields with n elements for

$$n = 2, 3, 4, 5, 7, 8, 9, 11, 13, 16, 17, 19, \dots$$

[conjecture?]

3. Let F be a field

$$F[t] := \{(\text{formal polynomial in one variable})\}$$

with t , given by

$$(a_0 + a_1t + a_2t^2 + \dots) + (b_0 + b_1t + b_2t^2 + \dots) := (a_0 + b_0) + (a_1 + b_1)t + (a_2 + b_2)t^2 + \dots$$

$$(a_0 + a_1t + a_2t^2 + \dots) \cdot (b_0 + b_1t + b_2t^2 + \dots) := a_0b_0 + (a_0b_1 + a_1b_0)t + \dots$$

Note: $f, g \in F[t]$ are EQUAL iff they have the same COEFFICIENTS (coeffs) for each t^i (if t^i does not occur we assume its coeff is 0.) $F[t]$ is not a field but satisfy all axioms except (M3) but it does satisfy (M3') (compare \mathbb{Z}). Let

$$F(t) := \left\{ \frac{f}{g} \mid f, g \in F[t], g \neq 0 \right\} \quad \text{with}$$

- $\frac{f}{g} = \frac{h}{k}$ if $fk = gh$
- $\frac{f}{g} + \frac{h}{k} := \frac{fk+gh}{gk} \quad \forall f, g, h, k \in F[t]$
- $\frac{f}{g} \cdot \frac{h}{k} := \frac{fh}{gk} \quad g \neq 0, k \neq 0$

is a field, the FIELD of RATIONAL POLYS over F .

Note: the 0 in $F[t]$ is $\frac{0}{f}$, $f \neq 0$, and 1 in $F[t]$ is $\frac{f}{f}$, $f \neq 0$.

4. let F be a field.

$$M_n F := \{A \mid A \text{ is } n \times n \text{ matrix entries in } F\}$$

usual $+$, \cdot of matrices, i.e. for $A, B \in M_n F$, let

$$A_{ij} := i \text{th entry of } A, \text{ etc}$$

Then

$$(A+B)_{ij} := A_{ij} + B_{ij}$$

$$(AB)_{ij} := C_{ij} := \sum_{k=1}^n A_{ik} B_{kj} \quad \forall i, j$$

Note: $A = B$ iff $A_{ij} = B_{ij} \quad \forall i, j$.

If $n = 1$, then

F and M_1F and the “same” so M_1F is a field. If $n > 1$ then M_nF is not a field nor does it satisfy (M3), (M4), (M3’). It does satisfy other axioms with

$$I = I_n := \begin{pmatrix} 1 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & 1 \end{pmatrix}, \quad 0 = 0_n := \begin{pmatrix} 0 & \dots & 0 \\ \vdots & & \vdots \\ 0 & \dots & 0 \end{pmatrix}$$

§2.2 Vector Space

$\mathbb{R}^2 := \{(x, y) | x, y \in \mathbb{R}\} = \mathbb{R} \times \mathbb{R}$ Vector in \mathbb{R}^2 are added as above and if $v \in \mathbb{R}^2$ is a vector,

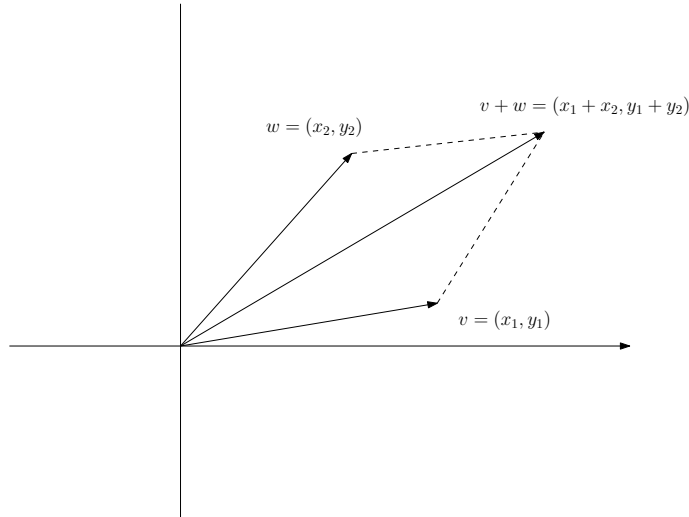


Figure 1: Geometry in \mathbb{R}^2

αv makes sense $\forall \alpha \in F$ by $\alpha(x, y) = (\alpha x, \alpha y)$ called SCALAR MULTIPLICATION. For $+$, scalar mult and $(0, 0)$ is the ZERO VECTOR satisfying various axioms. e.g., assoc, comm, “distributive law...”. To abstractify this

Definition 2.1 (Vector Space) — V is a vector space over F , via $+$, \cdot or $(V, +, \cdot)$ is a vector space over F where

$$\begin{array}{ll} + : V \times V \rightarrow V & \cdot : F \times V \rightarrow V \\ \text{Addition} & \text{Scalar Multiplication} \\ \text{write: } v + w := +(v, w) & \text{write: } \alpha \cdot v := \cdot(\alpha, v) \text{ or } \alpha v \end{array}$$

if the following axioms are satisfied

$$\forall v, v_1, v_2, v_3 \in V, \quad \forall \alpha, \beta \in F$$

1. $v_1 + (v_2 + v_3) = (v_1 + v_2) + v_3$
2. \exists an element $0 \in V \ni v + 0 = v = 0 + v$
3. (2) holds and the element $(-1)v$ in V satisfies

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

or (2) holds and $\forall v \in V \exists w \in V \ni v + w = 0 = w + v$

4. $v_1 + v_2 = v_2 + v_1$
5. $1 \cdot v = v$
6. $(\alpha \cdot \beta) \cdot v = \alpha(\beta \cdot v)$
7. $(\alpha + \beta)v = \alpha v + \beta v$
8. $\alpha(v_1 + v_2) = \alpha v_1 + \alpha v_2$

Elements of V are called **vector**, elements of F **scalars**.

Comments: V : a vector space over F

1. The zero of F is unique and is a scalar. The zero of V is unique and is a vector. They are different (unless $V = F$) even if we write 0 for both – should write $0_F, 0_V$ for the zero of F, V respectively.
2. if $v, w \in V, \alpha \in F$ then

$$\begin{array}{ll} \alpha v + w & \text{makes sense} \\ v\alpha, vw & \text{do not make sense} \end{array}$$

3. We usually write
vector using Roman letter
scalar using Greek letter
exception things like $(x_1, \dots, x_n) \in \mathbb{R}^n, x_i \in \mathbb{R} \forall i$

4. $+: V \times V \rightarrow V$ says

$$\text{if } v, w \in V, \text{ then } v + w \in V$$

write $v, w \in V \xrightarrow{\text{implies}} v + w \in V$. We say V is CLOSED under $+$

5. $\cdot : F \times V \rightarrow V$ says $\alpha \in F, v \in V \rightarrow \alpha v \in V$. We say V is CLOSED under SCALAR MULTIPLICATION.

Example 2.2

F a field, e.g., \mathbb{R} or \mathbb{C}

1. F is a vector space over F with $+, \cdot$ of a field, i.e., the field operation are the vector space operation with $0_F = 0_V$.
2. $F^n := \{\alpha_1, \dots, \alpha_n\} | \alpha_i \in F \forall i$ is a vector space over F under COMPONENT-WISE OPERATION and

$$0_{F^n} := (0, \dots, 0)$$

Even have

$$F_{\text{finite}}^\infty = \{(\alpha_1, \dots, \alpha_n, \dots) | \alpha_i \in F \forall i \text{ with only FINITELY MANY } \alpha_i \neq 0\}$$

3. Let $\alpha < \beta$ in \mathbb{R}

$$I = [\alpha, \beta], \quad (\alpha, \beta), \quad [\alpha, \beta), \quad (\alpha, \beta]$$

including $(\alpha = -\infty, \beta = \infty)$. Let $\text{fxn } I := \{f : I \rightarrow \mathbb{R} | f \text{ a fxn}\}$ called the SET of REAL VALUE FXNS on I .

Define $+, \cdot$ as follows: $\forall f, g \in \text{Fxn } I$,

$$\begin{aligned} f + g & \text{ by } (f + g)(x) := f(x) + g(x) \\ \alpha f & \text{ by } (\alpha f)(x) := \alpha f(x) \quad \forall \alpha \in \mathbb{R} \end{aligned}$$

and 0 by $0(\alpha) = 0 \forall \alpha \in F$. Then $\text{Fxn } I$ is a vector space over \mathbb{R} .

§3 | Lec 3: Oct 7, 2020

§3.1 Vector Space(Cont'd)

Example 3.1

F is a field, e.g. \mathbb{R} or \mathbb{C}

1. F is a vector space over F with $+, \cdot$ of a field, i.e. the field operation are the vector space operation with $0_F = 0_V$.
2. $F^n := \{(\alpha_1, \dots, \alpha_n) | \alpha_i \in F \forall i\}$ is a vector space over F under COMPONENT-WISE OPERATIONS

$$\begin{aligned} (\alpha_1, \dots, \alpha_n) + (\beta_1, \dots, \beta_n) &:= (\alpha_1 + \beta_1, \dots, \alpha_n + \beta_n) \\ \beta(\alpha_1, \dots, \alpha_n) &:= (\beta\alpha_1, \dots, \beta\alpha_n) \end{aligned}$$

with $\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_n \in F$ and $0_{F^n} := (0, \dots, 0)$.

Even have:

$$F^\infty = F_{\text{this}}^\infty : \{(\alpha_1, \dots, \alpha_n, \dots) | \alpha_i \in F \forall i \text{ with only FINITELY MANY } \alpha_i \neq 0\}$$

3. Let $\alpha < \beta$ in \mathbb{R}

$$I = [\alpha, \beta], \quad (\alpha, \beta), \quad [\alpha, \beta), \quad (\alpha, \beta]$$

(including $\alpha = -\infty, \beta = \infty$. Let function $I := \{f : I \rightarrow \mathbb{R} | f \text{ a function}\}$

Define $+, \cdot$ as follows: $\forall f, g \in \text{Fxn } I$,

$$\begin{aligned} f + g & \text{ by } (f + g)(x) := f(x) + g(x) \\ \alpha f & \text{ by } (\alpha f)(x) := \alpha f(x) \quad \forall \alpha \in \mathbb{R} \end{aligned}$$

and 0 by $0(\alpha) = 0 \forall \alpha \in F$. Then $\text{Fxn } I$ is a vector space over \mathbb{R} .

Using this, we get subsets which are also vector space over \mathbb{R} with same $+, \cdot, 0$.

- $C(I) := \{f \in \text{fxn } I | f \text{ continuous on } I\}$
- $\text{Diff } (I) := \{f \in \text{fxn } I | f \text{ differentiable on } I\}$
- $C^n(I) := \{f \in \text{fxn } I | f(n) \text{ then}^{\text{th}} \text{ derivative of } f \text{ and } f \text{ exists on } I \text{ and is cont on } I\}$
- $C^\infty(I) := \{f \in \text{fxn } I | f(n) \text{ exists } \forall n \geq 0 \text{ on } I \text{ and is cont}\}$
- $C^\omega(I) := \{f \in \text{fxn } I | f \text{ converges to its Taylor Series}\}$
(in a neighborhood of every $x \in I$ – be careful at boundary points)
- $\text{Int } (I) := \{f \in \text{fxn } I | f \text{ is integrable on } I\}$

4. $F[t]$ the set of polys, coeffs in F old $+, \cdot$ with scalar mult

$$\alpha(\alpha_0 + \alpha_1 t + \dots + \alpha_n t^n) := \alpha \alpha_0 + \alpha \alpha_1 t + \dots + \alpha \alpha_n t^n$$

5. $\underbrace{F[t]_n}_{\text{truncating } F[t]} := \{0 \in F[t]\} \cup \{f \in F[t] | \deg f \leq n\}$ (not closed under \cdot of polys)
where $\deg f$ = the highest power of t occurring non-trivially in f if $f \neq 0$ is a vector space over F with $+$, scalar mult, 0.

Example 3.2 1. $F^{m \times n} :=$ set of $m \times n$ matrices entries in F where $A \in F^{m \times n}$, $A_{ij} =$ ij^{th} entry of A

$$\begin{aligned} (A + B)_{ij} &:= A_{ij} + B_{ij} \in F & \forall A, B \in F^{m \times n} \\ (\alpha A)_{ij} &:= \alpha A_{ij} \in F & \forall \alpha \in F \end{aligned}$$

$$0 = \begin{pmatrix} 0 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & 0 \end{pmatrix} \text{ (m rows and n columns)}$$

COMPONENTWISE OPERATION! Then $F^{m \times n}$ is a vector space over F , e.g.

$M_n F$ is a vector space over F .

Example to GENERALIZE

Let V be a vector space over F , $\emptyset \neq S$ a set. Set $W := \{f : S \rightarrow V \mid f \text{ a map}\}$. Define $+$, \cdot on W by

$$\begin{aligned} f + g & \quad (f + g)(s) := f(s) + g(s) \in V \\ \alpha f & \quad (\alpha f)(s) := \alpha(f(s)) \in V \\ 0_W & \quad 0(s) = 0_V \quad \text{ZERO FUNCTION} \end{aligned}$$

$\forall f, g \in W; \alpha \in F; s \in S$. Then W is a vector space over F . (of componentwise operation)

2. Let $F \subset K$ be a fields under $+$, \cdot on K . Same 0,1, i.e. F is a SUBFIELD of K e.g. $\mathbb{R} \subset \mathbb{C}$. Then K is a vector space over F by RESTRICTION of SCALARS. i.e., $+$ is $+$ on K . With scalar mult, $F \times K \rightarrow K$ by

$$\underbrace{\alpha v}_{\text{in } K \text{ as a vector space over } F} = \underbrace{\alpha v}_{\text{in } K \text{ as a field}} \quad \forall \alpha \in F \quad \forall v \in V$$

e.g. \mathbb{R} is a vector space over \mathbb{Q} by $\frac{m}{n}r = \frac{mr}{n}$, $m, n \in \mathbb{Z}, n \neq 0, r \in \mathbb{R}$. More generally, let V be a vector space over K , $F \subset K$ subfield, then it is a vector space over F by RESTRICTION of SCALARS.

$$\cdot|_{F \times V} : F \times V \rightarrow V$$

e.g., K^n is a vector space over F (e.g. \mathbb{C}^n is a vector space over \mathbb{R}).

Properties of Vector Space: Let V be a vector space over F . Then $\forall \alpha, \beta \in F, \quad \forall v, w \in V$, we have

1. The zero vector is unique write 0 or 0_V .
2. $(-1)v$ is the unique vector $w \ni w + v = 0 = v + w$ write $-v$.
3. $0 \cdot v = 0$
4. $\alpha \cdot 0 = 0$
5. $(-\alpha)v = -(\alpha v) = \alpha(-v)$
6. if $\alpha v = 0$, then either $\alpha = 0$ or $v = 0$
7. if $\alpha v = \alpha w, \alpha \neq 0$, then $v = w$
8. if $\alpha v = \beta v, v \neq 0$, then $\alpha = \beta$
9. $-(v + w) = (-v) + (-w) = -v - w$
10. can ignore parentheses in $+$

§3.2 Subspace

Definition 3.3 (Subspace) — Let V be a vector space over F , $W \subset V$ a subset. We say W is a **subspace** of V if W is a vector space over F with the operation $+, \cdot$ on V , i.e., $(W, +, \cdot)$ is a vector space over F , via $+: V \times V \rightarrow V$ and $\cdot: F \times V \rightarrow V$ then W is a vector space over F via

- $+=+|_{W \times W}: W \times W \rightarrow W$: restrict the domain to $W \times W$
 - $\cdot=\cdot|_{F \times W}: F \times W \rightarrow W$: restrict the domain to $F \times W$
- i.e. W is closed under $+, \cdot$ from V , $\forall w_1, w_2 \in W \quad \forall \alpha \in F, \quad w_1 + w_2 \in W$ and $\alpha w_1 \in W$ and $0_W = 0_V$.

Theorem 3.4 (Subspace)

Let V be a vector space over F , $\emptyset \neq W \subset V$ a subset. Then the following are equivalent:

1. W is a subspace for V
2. W is closed under $+$ and scalar mult from V
3. $\forall w_1, w_2 \in W, \forall \alpha \in F, \alpha w_1 + w_2 \in W$

Proof. Some of the implication are essentially ??

1) \rightarrow 2) : by def. W is a subspace of V under $+, \cdot$ on V (and satisfies the axioms of a vector space over F) as $0_V = 0_W$.

2) \rightarrow 1) claim: $0_V \in W$ and $0_W = 0_V$: As $\emptyset \neq W \exists w \in W$

By 2) $(-1)w \in W$, hence $0_V = w + (-w) \in W$. Since $0_V + w' = w' = w' + 0_V$ in $V \quad \forall w' \in W$, the claim follows. The other axioms hold for elements of V hence for $W \subset V$.

2) \rightarrow 3) : let $\alpha \in F, w_1, w_2 \in W$. As 2) holds, $\alpha w_1 \in W$ hence also $\alpha w_1 + w_2 \in W$

3) \rightarrow 2) Let $\alpha \in F, w_1, w_2 \in W$. As above and 3)

$$0_V = w_1 + (-w_1) \in W \quad \text{and} \quad 0_V = 0_W$$

Therefore,

$$w_1 + w_2 = 1 \cdot w_1 + w_2 \in W \quad \text{and} \quad \alpha w_1 + \alpha w_1 + 0_V \in W$$

by 3). □

Note: Usually 3) is the easiest condition to check. WARNING: must subsets of a vector space over F are NOT subspace.

Example 3.5

V a vector space over F .

1. $0 := \{0_V\}$ and V are subspace of V

2. Let $I \subset \mathbb{R}$ be an interval (not a point) then

$$C^\omega(I) < C^\infty(I) < \dots < C^n(I) < \dots < C'(I) \\ < \text{Diff } I < C(I) < \text{Int } I < \text{Fxn } I$$

are subspaces of the vector space containing them... where we write

$$A < B \quad \text{if} \quad A \subset B \quad \text{and} \quad A \neq B$$

3. Let F be a field, e.g. \mathbb{R} . Then $F = F[t]_0 < F[t]_1 < \dots < F[t_n] < \dots < F[t]$ are vector spaces over F each a subspace of the vector space over F containing it.
4. If $W_1 \subset W_2 \subset V$, W_1, W_2 subspaces of V , then $W_1 \subset W_2$ is a subspace.
5. If $W_1 \subset W_2$ is a subspace and $W_2 \subset V$ is a subspace, then $W_1 \subset V$ is a subspace.
6. Let $W := \{(0, \alpha_1, \dots, \alpha_n) \mid \alpha_i \in F, \quad 2 \leq i \leq n\} \subset F^n$ is a subspace, but $\{(1, \alpha_2, \dots, \alpha_n) \mid \alpha_i \in F, \quad 2 \leq i \leq n\}$ is not. Why?
7. Every line or plane through the origin in \mathbb{R}^3 is a subspace.

§4 | Lec 4: Oct 9, 2020

§4.1 Span & Subspace

Definition 4.1 (Linear Combination) — Let V be a vector space over F , $v_1, \dots, v_n \in V$ we say $v \in V$ is a LINEAR COMBINATION of v_1, \dots, v_n if $\exists \alpha_1, \dots, \alpha_n \in F \ni v = \alpha v_1 + \dots + \alpha_n v_n$.

Let

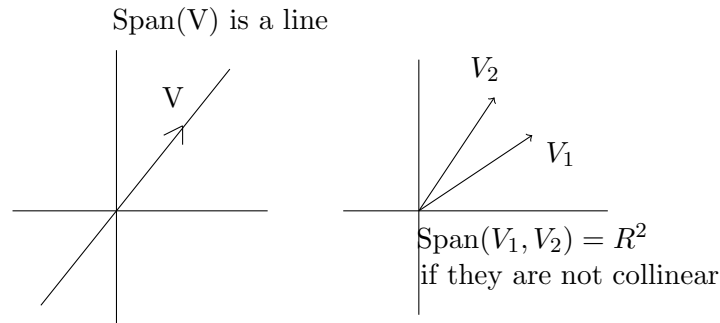
$$\text{Span}(v_1, \dots, v_n) := \{ \text{all linear combos of } v_1, \dots, v_n \}$$

Let $v_1, \dots, v_n \in V$. Then

$$\text{Span}(v_1, \dots, v_n) = \left\{ \sum_{i=1}^n \alpha_i v_i \mid \alpha_1, \dots, \alpha_n \in F \right\}$$

is a subspace of V (by the Subspace Theorem) called the SPAN of v_1, \dots, v_n . It is the (unique) smallest subspace of V containing v_1, \dots, v_n .

i.e., if $W \subset V$ is a subspace and $v_1, \dots, v_n \in W$ then $\text{Span}(v_1, \dots, v_n) \subset W$. We also let $\text{Span } \emptyset := \{0_V\} = 0$, the smallest vector space containing no vectors.



Question: If we view \mathbb{C} as a vector space over \mathbb{R} , then \mathbb{R} is a subspace of \mathbb{C} , but if we view \mathbb{C} as a vector space over \mathbb{C} , then \mathbb{R} is not a subspace of \mathbb{C} (why? What's going on?) – not closed under operation(s).

Definition 4.2 (Span) — Let V be a vector space over F , $\emptyset \neq S \subset V$ a subset. Then, $\text{Span } S :=$ the set of all FINITE linear combos of vectors in S . i.e., if $V \in \text{Span } S$, then

$$\exists v_1, \dots, v_n \in S, \quad \alpha_1, \dots, \alpha_n \in F \ni v = \alpha_1 v_1 + \dots + \alpha_n v_n$$

$\text{Span } S \subset V$ is a subspace. What is $\text{Span } V$?

Example 4.3 1. Let $V = \mathbb{R}^3$.

$$\text{Span}(i + j, i - j, k) = \text{Span} V = \text{Span}(i, j, i + j, k) = \text{Span}(i + j, i - j, k + i)$$

2. Define

$$\text{Symm}_n F := \left\{ A \in M_n F \mid A = A^\top \right\}$$

Recall: A^\top is the transpose of A , i.e.,

$$(A^\top)_{ij} := A_{ji} \quad \forall i, j$$

is a subspace of $M_n F$

3.

$$V = \left\{ \begin{pmatrix} a & c + di \\ c - di & b \end{pmatrix} \mid a, b, c, d \in \mathbb{R} \right\} \subset M_2 \mathbb{C}$$

is NOT a subspace as a vector space over \mathbb{C} , eg,

$$i \begin{pmatrix} a & c + di \\ c - di & b \end{pmatrix} = \begin{pmatrix} ai & -d + ci \\ d + ci & bi \end{pmatrix}$$

does not lie in V if either $a \neq 0$ or $b \neq 0$ (cannot be imaginary). Also V is not a subspace of $M_2 \mathbb{R}$ as a vector space over \mathbb{R} as $V \not\subset M_2 \mathbb{R}$. $V \subset M_2 \mathbb{C}$ is a subspace as a vector space over \mathbb{R} .

4. (Important computational example) Fix $A \in F^{m \times n}$. Let

$$\ker A := \left\{ x \in F^{n \times 1} \mid Ax = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \text{ in } F^{m \times 1} \right\}$$

called the **KERNEL** or **NULL SPACE** of A . $\ker A \subset F^{n \times 1}$ is a subspace and it is the **SOLUTION SPACE** of the system of m linear equations in n unknowns. – which we can compute by Gaussian elimination.

5. Let $W_i \subset V, i \in \underbrace{I}_{\text{indexing set}}$ be subspaces. Then $\bigcap_I W = \bigcap_{i \in I} W_i := \{x \in V \mid x \in W_i \forall i \in I\}$ is a subspaces of V (why?)

6. In general, if $W_1, W_2 \subset V$ are subspaces, $W_1 \cup W_2$ is NOT a subspace.
e.g., $\text{Span}(i) \cup \text{Span}(j) = \{(x, 0) \mid x \in \mathbb{R}\} \cup \{(0, y) \mid y \in \mathbb{R}\}$ is not a subspace

$$(x, y) = (x, 0) + (0, y) \notin \text{Span}(i) \cup \text{Span}(j)$$

if $x \neq 0$ and $y \neq 0$

Definition 4.4 (Subspace & Span) — Let $W_1, W_2 \subset V$ be subspaces. Define

$$\begin{aligned} W_1 + W_2 &:= \{w_1 + w_2 \mid w_1 \in W_1, w_2 \in W_2\} \\ &= \text{Span}(W_1 \cup W_2) \end{aligned}$$

So $w_1 + w_2 \subset V$ is a subspace and the smallest subspace of V containing W_1 and W_2 .

More generally, if $W_i \subset V$ is a subspace $\forall i \in I$ let

$$\sum_I W_i = \sum_{i \in I} W_i := +W_i := \text{Span}\left(\bigcup_I W_i\right)$$

the smallest subspace of V containing $W_i \forall i \in I$. What do elements in $\sum_I W_i$ look like?

Determine the span of vector v_1, \dots, v_n in \mathbb{R}^n

Suppose $v_i = (a_{i1}, \dots, a_{in}), i = 1, \dots, n$. To determine when $w \in \mathbb{R}^n$ lies in $\text{Span}(u_1, \dots, u_n)$ i.e., if $w = (b_1, \dots, b_n) \in \mathbb{R}^n$ when does

$$w = \alpha_1 v_1 + \dots + \alpha_n v_n, \quad \alpha_1, \dots, \alpha_n \in \mathbb{R}$$

What v_i is an $n \times 1$ column matrix $\begin{pmatrix} \alpha_{1i} \\ \vdots \\ a_{ni} \end{pmatrix}$

$$A = (a_{ij}), \quad B = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$$

view w as $\begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$. To solve

$$Ax = B, \quad X = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}$$

is equivalent to finding all the $n \times 1$ matrices B (actually B^\top) s.t.

$$Ax = B$$

when the columns of A are the $v_i(v_i^\top)$.

Note: If $m = n$ an A is invertible then all B work.

§4.2 Linear Independence

We know that \mathbb{R}^n is an n -dimensional vector space over \mathbb{R} . Since we need n coordinates (axes) to describe all vector in \mathbb{R}^n but no fewer will do.

We want something like the following:

Let V be a vector space over F with $V \neq \emptyset$. Can we find distinct vectors $v_1, \dots, v_n \in V$, some n with following properties

1. $V = \text{Span}(v_1, \dots, v_n)$
2. No v_i is a linear combos of $v_1, \dots, v_{i-1}, v_{i+1}, \dots, v_n$ (i.e. we need them all)

Then we want to call V an n -DIMENSIONAL VECTOR SPACE OVER F .

Lemma 4.5

Let V be a vector space over F , $n > 1$. Suppose v_1, \dots, v_n are distinct. Then (2) is equivalent to

$$\text{If } \alpha_1 v_1 + \dots + \alpha_n v_n = \beta_1 v_1 + \dots + \beta_n v_n, \quad \alpha_i, \beta_i \in F \forall i, j$$

i.e. the “coordinates” are unique.

Proof. (\Rightarrow) If not, relabelling the v_i 's, we may assume that $\alpha_1 \neq \beta_1$ in (*), then

$$(\alpha_1 - \beta_1)v_1 = \sum_{i=2}^n (\beta_i - \alpha_i)v_i$$

As $\alpha_1 - \beta_1 \neq 0$ in F , a field, $(\alpha_1 - \beta_1)^{-1}$ exists, so

$$v_1 = \sum_{i=2}^n (\alpha_1 - \beta_1)^{-1}(\beta_i - \alpha_i)v_i \in \text{Span}(v_1, \dots, v_n)$$

a contradiction.

(\Leftarrow) Relabelling, we may assume that

$$v_1 = \alpha_2 v_2 + \dots + \alpha_n v_n, \quad \text{some } \alpha_i \in F$$

Then,

$$1 \cdot v_1 + 0v_2 + \dots + 0v_n = v_1 = 0 \cdot v_1 + \alpha_2 v_2 + \dots + \alpha_n v_n$$

so $1 = 0$, a contradiction. \square

Remark 4.6. The case $n = 1$ is special because there are two possibilities

Case 1: $v \neq 0$: then $\alpha v = \beta v \rightarrow \alpha = \beta$

Case 2: $v = 0$: then $\alpha v = \beta v \forall \alpha, \beta \in F$

So the only time the above lemma is false is when $n = 1$ and $v = 0$. We do not want to say this, so we use another definition.

§5 | Lec 5: Oct 12, 2020

§5.1 Linear Independence(Cont'd)

Definition 5.1 (Linear Independence & Dependence) — Let V be a vector space over F , v_1, \dots, v_n in V all distinct. We say $\{v_1, \dots, v_n\}$ is LINEARLY DEPENDENT if $\exists \alpha_1, \dots, \alpha_n \in F$ not all zero \ni

$$\alpha_1 v_1 + \dots + \alpha_n v_n = 0$$

and $\{v_1, \dots, v_n\}$ is LINEARLY INDEPENDENT if it is NOT linearly dependent, i.e., if for any eqn

$$0 = \alpha v_1 + \dots + \alpha_n v_n, \quad \alpha_1, \dots, \alpha_n \in F,$$

then $\alpha_i = 0 \forall i$, i.e., the only linear comb of v_1, \dots, v_n – the zero vector is the TRIVIAL linear combo (we shall also say that distinct v_1, \dots, v_n are linearly independent if $\{v_1, \dots, v_n\}$ is. More generally, a set $\emptyset \neq S \subset V$ is called LINEARLY DEPENDENT if for some FINITE subset (of distinct elements of S) of S is linearly dependent and it is called LINEARLY INDEPENDENT if every FINITE subset of S (of distinct elements) is linearly independent.

We say $v_i, i \in I$, all distinct are LINEARLY INDEPENDENT if $\{v_i\}_{i \in I}$ is linearly independent and $v_i \neq v_j \forall i, j \in I, i \neq j$.

Remark 5.2. Let V be a vector space over F , $\emptyset \neq S \subset V$ a subset

1. If $0 \in S$, then S is linearly dependent as $1 \cdot 0 = 0$

2. distinct: v_1, \dots, v_n in V are linearly independent iff

- no $v_i = 0$
- $\alpha_1 v_1 + \dots + \alpha_n v_n = \beta_1 v_1 + \dots + \beta_n v_n, \quad \alpha_i, \beta_i \in F$ implies $\alpha_i = \beta_i \forall i$

Note: v, v are linearly dependent if we allow repetitions – and $\{v, v\} = \{v\}$.

For homework, make sure to show this:

Suppose v_1, \dots, v_n are distinct, $n > 2$, no $v_i = 0$. Suppose no v_i is a scalar multiple of another $v_j, j \neq i$. It does not follow that v_1, \dots, v_n are linearly independent (in general).

Example 5.3 (counter-example)

$(1, 0), (0, 1), (1, 1)$ in $V = \mathbb{R}^2$
 $(1, 0), (0, 1)$ are linearly indep. but not $(1, 0), (0, 1)$, and $(1, 1)$.

Remark 5.4. Let $\emptyset \neq T \subset S$ be a subset. If T is linearly dependent, so is S . Then the contraposition is also true: if S is linearly indep., so is T .

More remarks:

1. Let $0 \neq v \in V$. Then $\{v\}$ is linearly independent and

$$Fv := \text{Span}(v)$$

is called a LINE in V :

$$\alpha v = 0 \rightarrow \alpha = 0$$

2. $u, v, w \in V \setminus \{0\}$ and $v \notin \text{Span}(w)$ (equivalently, $w \notin \text{Span}(v)$), then $\{v, w\}$ is linearly indep. and $\text{span}(v, w)$ is called a PLANE in V .
3. $(1, 1), (-2, -2)$ are linearly dep. in \mathbb{R}^2 .
4. $(1, 1), (2, -2)$ are linearly indep. in \mathbb{R}^2 (show coefficients are equal to each other and to 0).
5. More generally,

$$v_i = (a_{i1}, \dots, a_{in}) \text{ in } \mathbb{R}^n, \quad i = 1, \dots, m \text{ (distinct)}$$

Then

$$\exists \alpha_1, \dots, \alpha_m \in \mathbb{R} \text{ not all } 0 \ni \alpha_1 v_1 + \dots + \alpha_m v_m = 0$$

iff v_1, \dots, v_m are linearly dep – iff $\exists \alpha_1, \dots, \alpha_m \in \mathbb{R}$ not all 0 s.t.

$$\alpha_1(a_{11}, \dots, a_{1m}) + \dots + \alpha_m(a_{m1}, \dots, a_{mn}) = 0$$

iff the matrix

$$A = \begin{pmatrix} a_{11} & \dots & a_{1m} \\ \vdots & & \\ a_{m1} & \dots & a_{mn} \end{pmatrix}$$

with rows v_i row reduced to echelon form with a zero row. Also,

$$B = A^\top = \begin{pmatrix} a_{11} & \dots & a_{m1} \\ \vdots & & \\ a_{1m} & \dots & a_{mn} \end{pmatrix}$$

i.e., write the vectors v_i as columns then

$$\underbrace{B}_{n \times m} \underbrace{X}_{m \times 1} = 0$$

has a NON-TRIVIAL solution, i.e.,

$$\ker B \neq 0$$

where

$$\ker B := \{X \in F^{m \times 1} \mid BX = 0\}$$

the kernel of B .

6. Let $f_1, \dots, f_n \in C^{n-1}(I)$, $I = (\alpha, \beta)$, $\alpha < \beta$ in \mathbb{R} and

$$\alpha_1 f_1 + \dots + \alpha_n f_n = \underbrace{0}_{\text{the zero func}}$$

i.e., $(\alpha_1 f_1 + \dots + \alpha_n f_n)(x) = 0 \quad \forall x \in (\alpha, \beta)$. Taking the derivatives $(n-1)$ times and put them in matrix form, we have

$$\begin{pmatrix} f_1 & \dots & f_n \\ f_1' & \dots & f_n' \\ \vdots & \dots & \vdots \\ f_1^{n-1} & \dots & f_n^{n-1} \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ \vdots \\ 0 \end{pmatrix}$$

In particular, the Wronskian of f_1, \dots, f_n is not the zero func, i.e., $\exists x \in (\alpha, \beta) \ni W(f_1, \dots, f_n)(x) \neq 0$. This means that the matrix above is invertible for some $x \in (\alpha, \beta)$. Then, $\alpha_1 = 0, \dots, \alpha_n = 0$ by Cramer's rule – only the trivial soln.

Conclusion: $W(f_1, \dots, f_n) \neq 0 \rightarrow \{f_1, \dots, f_n\}$ is linearly indep.

WARNING: the converse is false.

Example 5.5 (of the conclusion)

Let $\alpha < \beta$ in \mathbb{R} .

1. $\sin x, \cos x$ are linearly indep. on (α, β) .
2. We need some (sub) defns for this example.

For $x \in \mathbb{R}$, define the map

$$e_x : \mathbb{R}[t] \rightarrow \mathbb{R} \text{ by}$$

$$g = \sum a_i t^i \mapsto g(x) := \sum a_i x^i \text{ called EVALUATION at } x.$$

We call a map $f : \mathbb{R} \rightarrow \mathbb{R}$ (or some $f : I \rightarrow \mathbb{R} (I \subset \mathbb{R})$) a POLYNOMIAL FUNCTION if

$$\exists P_f = \sum_{i=1}^n a_i t^i \in \mathbb{R}[t]$$

and

$$f(x) = e_x P_f = P_f(x) = \sum_{i=1}^n a_i x^i \quad \forall x \in \mathbb{R}$$

i.e., the function arising from a (formal) polynomial by evaluation at each x . We let

$$\mathbb{R}[x] := \{f : \mathbb{R} \rightarrow \mathbb{R} \mid f \text{ a poly fcn} \}$$

Note: Polynomial fcn's are defined on all of \mathbb{R} . $\mathbb{R}[x]$ is a vector space over \mathbb{R} .

Warning: if we replace \mathbb{R} by F , $F[t]$ may be “very different” from $F[x]$, e.g., let $F = \{0, 1\}$. Then

$$t, t^2 \in F[t], \quad t \neq t^2 \quad \text{but} \quad P_t = P_{t^2}$$

Now we can give our example using Wronskians

$$\{1, x, \dots, x^n\}$$

is linearly indep. on (α, β) assuming $\alpha < \beta$.

HOMEWORK: Let $\alpha_1, \dots, \alpha_n \in \mathbb{R}$ be distinct, then

$$e^{\alpha_1 t}, \dots, e^{\alpha_n t}$$

are linearly indep. on (α, β) . THINK OVER IT!

Theorem 5.6 (Toss In)

Let V be a vector space over F , $\emptyset \neq S \subset V$ a linearly indep. subset. Suppose that $v \in V \setminus \text{Span } S$. Then $S \cup \{v\}$ is linearly indep.

Proof. Suppose this is false which is $S \cup \{v\}$ is linearly dep. Then $\exists v_1, \dots, v_n \in S$ and $\alpha, \alpha_1, \dots, \alpha_n \in F$ some n not all zero s.t.

$$\alpha v + \alpha_1 v_1 + \dots + \alpha_n v_n = 0$$

Case 1: $\alpha = 0$

Then $\alpha_1 v_1 + \dots + \alpha_n v_n = 0$ not all $\alpha_1, \dots, \alpha_n$ zero so $\{v_1, \dots, v_n\}$ is linearly dep., a contradiction.

Case 2: $\alpha \neq 0$

Then α^{-1} exists.

$$v = -\alpha^{-1}\alpha_1 v_1 - \dots - \alpha^{-1}\alpha_n v_n$$

is a linear combo of v_1, \dots, v_n , i.e., $v \in \text{Span}(v_1, \dots, v_n)$ – a contradiction. Therefore, $S \cup \{v\}$ is linearly indep. \square

Corollary 5.7

Let V be a vector space over F and $v_1, \dots, v_n \in V$ linearly indep. if

$$\text{Span}(v_1, \dots, v_n) < V$$

then $\exists v_{n+1} \in V \ni v_1, \dots, v_n, v_{n+1}$ are linearly indep. and

$$\text{Span}(v_1, \dots, v_n) < \text{Span}(v_1, \dots, v_{n+1}) \subset V$$

Question 5.1. Why can't we get a linearly indep. set spanning any vector space over F using this theorem?

Ans: Certainly we may not get a finite set. We shall only be interested in the case, much of the time, when such a finite linearly indep. set spans our vector space over F .

Example 5.8

$(1, 3, 1) \in \mathbb{R}^3$ is linearly indep. but $\text{Span}(1, 3, 1) < \mathbb{R}^3$.
 $(1, 1, 0) \notin \text{Span}(1, 3, 1)$ so $(1, 3, 1), (1, 1, 0)$ are linearly indep. Similarly for $(0, 0, 1)$.
 $\mathbb{R}^3 = \text{Span}((1, 3, 1), (1, 1, 0), (0, 0, 1))$

§6 | Lec 6: Oct 14, 2020

§6.1 Bases

Definition 6.1 (Basis) — Let $\emptyset \neq V$ be a vector space over F . A **BASIS** B for V is a linearly indep. set in V and spans V . i.e.,

1. $V = \text{Span } B$.
2. B is linearly indep.

We say V is a **FINITE DIMENSIONAL VECTOR SPACE OVER F** if there exists B for V with finitely many elements, i.e., $|B| < \infty$.

Notation: If $V = 0$, we say V is a finite dimensional vector sapce over F of **DIMENSION ZERO**.

Goal: To show if V is finite dimensional vector space over F with bases B and b then $|B| = |b| < \infty$. This common integer is called the **DIMENSION** of V .

Example 6.2

Let V be a vector space over F , $S \subset V$ a linearly indep. set. Then S is a basis for $\text{Span } S$.

Warning: S is not a subspace just a subset.

Definition 6.3 (Ordered Basis) — If V is a finite dimensional vector space over F with a basis $B = \{v_1, \dots, v_n\}$ we called it an **ORDERED BASIS** if the given order of v_1, \dots, v_n is to be used, i.e., the i^{th} vector in B is the i^{th} in the written list, e.g., $\{v_1, v_2, v_4, v_3, \dots\}$ then v_4 is the 3rd element in the ordered list if we want B to be ordered in this way.

Theorem 6.4 (Coordinate)

Let V be a finite dimensional vector space over F with basis $B = \{v_1, \dots, v_n\}$ and $v \in V$. Then $\exists! \alpha_1, \dots, \alpha_n \in F \ni v = \alpha_1 v_1 + \dots + \alpha_n v_n$. We call $\alpha_1, \dots, \alpha_n$ the COORDINATE of v relative to the basis B and call α_i the i^{th} coordinate relative to B .

Proof. Existence: By defn, $V = \text{Span } B$, so if $v \in V$

$$\exists \alpha_1, \dots, \alpha_n \in F \ni v = \alpha_1 v_1 + \dots + \alpha_n v_n$$

Uniqueness: Let $v \in V$ and suppose that $\alpha_1 v_1 + \dots + \alpha_n v_n = \beta_1 v_1 + \dots + \beta_n v_n$, for some $\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_n \in F$. Then

$$(\alpha_1 - \beta_1)v_1 + \dots + (\alpha_n - \beta_n)v_n = 0$$

Since B is linearly indep,

$$\alpha_i - \beta_i = 0 \quad \text{for } i = 1, \dots, n$$

□

Question 6.1. Does the above theorem hold if the basis B is not necessarily finite? If so prove it!

Exercise 6.1. Let V be a vector space over F , $v_1, \dots, v_n \in V$ then

$$\text{Span}(v_1, \dots, v_n) = \text{Span}(v_2, \dots, v_n) \iff v_1 \in \text{Span}(v_2, \dots, v_n)$$

Make sure to PROVE THIS

Note: For induction, you CAN'T assume n in the induction hypothesis is special in any way except it is greater than 1. Also, you can start induction at $n = 0$, i.e., show $P(0)$ true (or at any $n \in \mathbb{Z}$).

Theorem 6.5 (Toss Out)

Let V be a vector space over F . If V can be spanned by finitely many vector then V is a finite dimensional vector space over F . More precisely, if

$$V = \text{Span}(v_1, \dots, v_n)$$

then a subset of $\{v_1, \dots, v_n\}$ is a basis for V .

Proof. If $V = 0$, there is nothing to prove. So we may assume that $V \neq 0$. Suppose that $V = \text{Span}(v_1, \dots, v_n)$. We can use induction on n and show a subset of $\{v_1, \dots, v_n\}$ is a basis.

- $n = 1$: $V = \text{Span}(v_1) \neq 0$ as $V \neq 0$, so $v_1 \neq 0$. Hence $\{v_1\}$ is linearly indep and it is the basis.

- Assume $V = \text{Span}(w_1, \dots, w_n)$ – the induction hypothesis – to be true. Then a subset of w_1, \dots, w_n is a basis for V . Now suppose that $v = \text{Span}(v_1, \dots, v_{n+1})$. To show a subset of $\{v_1, \dots, v_{n+1}\}$ is a basis for V , we need to show if $\{v_1, \dots, v_{n+1}\}$ is linearly indep., then it is a basis for V and it spans V and we are done. So let us assume that $\{v_1, \dots, v_{n+1}\}$ is linearly dep. Hence,

$$\exists \alpha_1, \dots, \alpha_{n+1} \in F \text{ not all zero } \ni$$

$$\alpha_1 v_1 + \dots + \alpha_{n+1} v_{n+1} = 0$$

Assume $\alpha_{n+1} \neq 0$, then

$$v_{n+1} = -\alpha_{n+1}^{-1} \alpha_1 v_1 - \dots - \alpha_{n+1}^{-1} \alpha_n v_n$$

lies in $\text{Span}(v_1, \dots, v_n)$. By the Exercise above,

$$V = \text{Span}(v_1, \dots, v_{n+1}) = \text{Span}(v_1, \dots, v_n)$$

By the induction hypo, a subset of $\{v_1, \dots, v_n\}$ is a basis for V .

□

Example 6.6 1. Let $e_i = \{(0, \dots, 0, 1, 0, \dots)\} \in F^n$

$$s = s_n := \{e_1, \dots, e_n\} \subset F^n$$

If $v \in F^n$, then

$$v = (\alpha_1, \dots, \alpha_n) = \alpha_1 e_1 + \dots + \alpha_n e_n$$

since $\alpha_i \in F$, so $F^n = \text{Span } s$. If $0 = \alpha_1 e_1 + \dots + \alpha_n e_n = (\alpha_1, \dots, \alpha_n) = (0, \dots, 0)$, then $\alpha_i = 0 \forall i$. So s is linearly indep. Hence s is a basis for F^n called the standard basis. More generally, let

$e_{ij} \in F^{m \times n}$ be the $m \times n$ matrix with all entries 0 except in the i th place.

Then $s_{mn} := \{e_{ij} | 1 \leq i \leq m, 1 \leq j \leq n\}$ is a basis for $F^{m \times n}$ called the STANDARD BASIS for $F^{m \times n}$ – same proof – everything is done componentwise.

2. $V = F[t] := \{\text{polys in } t, \text{ coeffs in } F\}$ ($F = \mathbb{R}$). Let $f \in V$. Then, there exists $n \geq 0$ in \mathbb{Z} and $\alpha_0, \dots, \alpha_n$ in F s.t.

$$f = \alpha_0 + \alpha_1 t + \dots + \alpha_n t^n$$

So $B = \{t^n | n \geq 0\} = \{1, t, t^2, \dots\}$ spans V and by defn if

$$\alpha_0 + \alpha_1 t + \dots + \alpha_n t^n = \underbrace{0}_{\text{zero poly}}$$

then $\alpha_i = 0$ for all i so B is linearly indep. Hence B is a basis for $F[t]$. B is not a finite set. We shall see that $F[t]$ is not a finite dimensional vector space over F .

How?

3. $F[t]_n := \{f \in F[t] \mid f = 0 \text{ or } \deg f \leq n\} \subset F[t]$ is spanned by $\{1, t, t^2, \dots, t^n\}$. It is a subset of linearly indep. set. $\{1, t, t^2, \dots\} = \{t^n \mid n \geq 0\}$ so also linearly indep. and therefore a basis.
4. $\{1, \sqrt{-1}\}$ is a basis for \mathbb{C} as a vector space over \mathbb{R} . $\{1\}$ is a basis for C as a vector space over \mathbb{C} (indeed, if F is a field, F is a vector space over F and if $0 \neq \alpha \in F$, then α^{-1} exists and $x = x\alpha^{-1}\alpha \in \text{Span } F$ so $\{\alpha\}$ is a basis. e.g., $\{\pi\}$ is a basis for \mathbb{R} as a vector space over \mathbb{R}).
5. $\{e^{-x}, e^{3x}\}$ is a basis for

$$V := \{f \in \mathbb{C}^2(-\infty, \infty) \mid f'' - 2f' - 3f = 0\}$$

a vector space over \mathbb{R} .

6. Given $v_1, \dots, v_n \in F^n$, you know how to find $W = \text{Span}(v_1, \dots, v_n)$. Note: If $m > n$ then rows reducing A^\top must lead to a zero row so v_1, \dots, v_m cannot be linearly indep. If $m = n$ we can see if

$$\det A^\top = 0 \quad (\text{or } \det A = 0)$$

then linearly dep. And if

$$\det A^\top \neq 0 \quad (\text{or } \det A \neq 0)$$

then linearly indep.

§7 | Lec 7: Oct 16, 2020

§7.1 Replacement Theorem

Theorem 7.1 (Replacement)

Let V be a vector space over F , $\{v_1, \dots, v_n\}$ a basis for V . Suppose that $v \in V$ satisfies

$$v = \alpha_1 v_1 + \dots + \alpha_n v_n, \quad \alpha_1, \dots, \alpha_n \in F, \alpha_i \neq 0$$

Then

$$\{v_1, \dots, v_{i-1}, v, v_{i+1}, \dots, v_n\}$$

is also a basis for V .

Proof. Changing notation, we may assume $\alpha_1 \neq 0$. To show $\{v_1, v_2, \dots, v_n\}$ is a basis for V , we have to show $\{v, v_2, \dots, v_n\}$ spans V . Since

$$v = \alpha_1 v_1 + \dots + \alpha_n v_n, \quad \alpha_1 \neq 0$$

α_1^{-1} exists, so

$$v_1 = \alpha_1^{-1} v - \alpha_1^{-1} \alpha_2 v_2 - \dots - \alpha_1^{-1} \alpha_n v_n$$

lies in $\text{Span}(v, v_2, \dots, v_n)$. By Exercise ...,

$$V = \text{Span}(v, v_1, \dots, v_n) = \text{Span}(v, v_2, \dots, v_n)$$

So $\{v, v_2, \dots, v_n\}$ spans V . Thus, $\{v, v_2, \dots, v_n\}$ is linearly indep.

Suppose $\exists \beta_1, \beta_2, \dots, \beta_n \in F$ not all 0 \ni

$$\beta v + \beta_2 v_2 + \dots + \beta_n v_n = 0$$

Case 1: $\beta = 0$

Then $\beta_2 v_2 + \dots + \beta_n v_n = 0$ not all $\beta_i = 0$. So $\{v_2, \dots, v_n\}$ is linearly dep., a contradiction.

Case 2: $\beta \neq 0$, so β^{-1} exists.

Then using (*), we see

$$v = 0 \cdot v_1 - \beta^{-1} \beta_2 v_2 - \dots - \beta^{-1} \beta_n v_n = \alpha_1 v_1 + \dots + \alpha_n v_n$$

As $\{v_2, \dots, v_n\}$ is a basis, by the Coordinate Theorem, we have

$$\alpha_1 = 0 \quad \text{and} \quad \alpha_i = \beta^{-1} \beta_i$$

a contradiction. □

Question 7.1. In the Replacement Theorem, do we need the basis to be finite?

Ans: I think it can be infinite ...

§7.2 Main Theorem

Theorem 7.2 (Main)

Suppose V is a vector space over F with $V = \text{Span}(v_1, \dots, v_n)$. Then any linearly indep. subset of V has at most n elements.

Proof. We know that a subset of $B = \{v_1, \dots, v_n\}$ is a basis for V by Toss Out Theorem. So we may assume B is a basis for V . It suffices to show any linearly indep. set in V has at most $|B| = n$ elements where B is a basis. Let $\{w_1, \dots, w_m\} \subset V$ be linearly indep. where no $w_i = 0$. To show $m \leq n$, the idea is to use Toss In and Toss out in conjunction with the Replacement Theorem.

Claim 7.1. After changing notation, if necessary, for each $k \leq n$

$$\{w_1, \dots, w_k, v_{k+1}, \dots, v_n\}$$

is a basis for V .

Suppose we have shown the above claim for $k = n$. Apply the claim to $k = n$ if $m > k$, then $\{w_1, \dots, w_{n+1}\}$ is linearly dep., a contradiction as $\{w_1, \dots, w_n\}$ is a basis. Thus, we prove the claim for $m \leq n$ as needed. We prove it by induction on k . BY the argument above, we may assume $k \leq n$.

- $k = 1$: As $w_1 \in \text{Span } B = \text{Span } (v_1, \dots, v_n)$ and $w_1 \neq 0$, $\exists \alpha_1, \dots, \alpha_n \in F$ not all 0
 \ni

$$w_1 = \alpha_1 v_1 + \dots + \alpha_n v_n$$

Changing notation, we may assume $\alpha_1 \neq 0$. By the Replacement Theorem,

$$\{w_1, v_2, \dots, v_n\} \text{ is a basis for } V$$

- Assume the claim hold for $k(k < n)$.
- We must show the claim holds for $k + 1$,

$$\{w_1, \dots, w_k, v_{k+1}, \dots, v_n\} \text{ is a basis for } V$$

We can write

$$0 \neq w_{k+1} = \beta_1 w_1 + \dots + \beta_k w_k + \alpha_{k+1} v_{k+1} + \dots + \alpha_n v_n$$

for some (new) $\beta_1, \dots, \beta_k, \alpha_{k+1}, \dots, \alpha_n \in F$ not all 0

Case 1: $\alpha_{k+1} = \alpha_{k+2} = \dots = \alpha_n = 0$

Then $w_{k+1} \in \text{Span}(w_1, \dots, w_k)$, hence $\{w_1, \dots, w_{k+1}\}$ is linearly dep., a contradiction.

Case 2: $\exists i \ni \alpha_i \neq 0$:

Changing notation, we may assume $\alpha_{k+1} \neq 0$. By the Replacement Theorem

$$\{w_1, \dots, w_{k+1}, v_{k+2}, \dots, v_n\}$$

is a basis for V . This completes the induction step thus prove the claim and establish the theorem. \square

§7.3 A Glance at Dimension

Corollary 7.3

Let V be a finite dimensional vector space over F , B_1, B_2 two bases for V . Then $|B_1| = |B_2| < \infty$. We call $|B_1|$ the dimension of V , write $\dim V = \dim_F V = |B_1|$ (dropping F if F is clear).

Proof. By defn of finite dimensional vector space over F , \exists a basis b for V with $|b| < \infty$. By the Main Theorem, $|B| \leq |b|$, if B is a basis for V , so B is finite. Again by the Main Theorem, $|b| \leq |B|$ if B is a basis for V , so $|b| = |B|$ for any basis B of V . \square

The corollary above says $\dim V$ is well-defined for all finite dimensional vector space over F , i.e., “ \dim ” : {finite dimensional vector space over $F \rightarrow \mathbb{Z}^+ \cup \{0\}$ } is a function.

Warning: F makes a difference.

Example 7.4

$$\begin{aligned}\dim_{\mathbb{C}} \mathbb{C} &= 1 && \text{basis } \{1\} \\ \dim_{\mathbb{R}} \mathbb{C} &= 2 && \text{basis } \{1, \sqrt{-1}\} \\ \dim_{\mathbb{Q}} \mathbb{C} &=?\end{aligned}$$

Corollary 7.5

$$\dim_F F^n = n.$$

Corollary 7.6

$$\dim_F F^{m \times n} = mn.$$

Corollary 7.7

$$\dim_F F[t]_n = 1 + n.$$

Note: If V is a finite dimensional vector space over F with bases B , then the Replacement Theorem allows us to find many other bases.

Corollary 7.8

Let V be a finite dimensional vector space over F , $n = \dim V$, $\emptyset \neq S \subset V$ a subset. Then

- If $|S| > n$, then S is linearly dep.
- If $|S| < n$, then $\text{Span } S < V$.

Proof. • First bullet point: The Main Theorem says:

A maximal linearly indep. set in V is a basis and can have at most n elements by Toss In Theorem.

- Second bullet point: By Toss Out Theorem, we can assume that S is linearly indep., so it cannot be a basis by Corollary ?.

□

Question 7.2. What is $\dim_{\mathbb{R}} M_n(\mathbb{C})$?

§8 | Lec 8: Oct 19, 2020

§8.1 Extension and Counting Theorem

Theorem 8.1 (Extension)

Let V be a finite dimensional vector space over F , $W \subset V$ a subspace. Then every linearly independent subset S in W is finite and part of a basis for W which is a finite dimensional vector space over F .

Proof. Any linearly indep. set in W is linearly indep. subset S in V so $|S| \leq \dim V < \infty$ by the Main Theorem. In particular,

$$\dim \text{Span} S \leq \dim V$$

if $W = \text{Span } S$, we are done.

If not, $\exists w_1 \in W \setminus \text{Span } S$, and hence $S_1 = S \cup \{w_1\}$ is linearly indep. by Theorem and

$$|S_1| = |S \cup \{w_1\}| = |S| + 1 \leq \dim V$$

if $\text{Span } S_1 < W$, then $\exists w_2 \in W \setminus \text{Span } S_1$, so $S_2 = S \cup \{w_1, w_2\} \subset W$ is linearly indep., hence

$$|S_2| = |S| + 2 \leq \dim V$$

Continuing in this manner, we must stop when $n \leq \dim V - \dim \text{Span } S$ as $\dim V < \infty$. So S is a part of a basis for W and W is a finite dimensional vector space over F . \square

Think about the proof for this

Corollary 8.2

Let V be a finite dimensional vector space over F . Then any linearly indep. set in V can be EXTENDED to a basis for V , i.e., is part of a basis for V . We often call this special case the **Extension Theorem**.

Corollary 8.3

Let V be a finite dimensional vector space over F , $W \subset V$ a subspace. Then W is a finite dimensional vector space over F and $\dim W \leq \dim V$ with equality iff $W = V$.

Proof. Left as exercise. \square

Theorem 8.4 (Counting)

Let V be a finite dimensional vector space over F , $W_1, W_2 \subset V$ subspaces. Suppose that both W_1 and W_2 are finite dimensional vector space over F . Then

1. $W_1 \cap W_2$ is a finite dimensional vector space over F .
2. $W_1 + W_2$ is a finite dimensional vector space over F .
3. $\dim W_1 + \dim W_2 = \dim(W_1 + W_2) + \dim(W_1 \cap W_2)$.

Proof. 1. $W_1 \cap W_2 \subset W_i, i = 1, 2$, so it is a finite dimensional vector space over F by corollary 8.2.

2. Let B_i be a basis for $W_i, i = 1, 2, \dots$. Then $W_1 + W_2 = \text{Span}(B_1 \cup B_2)$ and

$$|B_1 \cup B_2| \leq |B_1| + |B_2| < \infty$$

So $W_1 + W_2$ is a finite dimensional vector space over F by Toss Out.

3. Let $B = \{v_1, \dots, v_n\}$ be a basis for $W_1 \cap W_2$. Extend B to a basis

$$b_1 = \{v_1, \dots, v_n, y_1, \dots, y_r\} \text{ for } W_1$$

$$b_2 = \{v_1, \dots, v_n, z_1, \dots, z_s\} \text{ for } W_2$$

using the Extension Theorem.

Claim 8.1. $b_1 \cup b_2 = \{v_1, \dots, v_n, y_1, \dots, y_r, z_1, \dots, z_s\}$ is a basis for $W_1 + W_2$ and has $n + r + s$ elements. So if we show the claim, the result will follow.

Certainly,

$$\text{Span}(b_1 \cup b_2) = \text{Span } b_1 + \text{Span } b_2 = W_1 + W_2$$

So we need only to show $b_1 \cup b_2$ is linearly indep. Suppose this is false. Then

$$0 = \alpha_1 v_1 + \dots + \alpha_n v_n + \beta_1 y_1 + \dots + \beta_r y_r + \gamma_1 z_1 + \dots + \gamma_s z_s \quad (*)$$

for some $\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_r, \gamma_1, \dots, \gamma_s$ in F not all zero.

Case 1: All the $\gamma_i = 0$. Since b_1 is linearly indep., this is a contradiction.

Case 2: Some $\gamma_i \neq 0$.

Changing notation, we may assume $\gamma_1 \neq 0$. Since b_2 is a basis, (*) leads to an equation

$$0 \neq z = \gamma_1 z_1 + \dots + \gamma_s z_s = -\alpha_1 v_1 - \dots - \alpha_n v_n - \beta_1 y_1 - \dots - \beta_r y_r$$

Therefore, $0 \neq z$ lies in $\text{Span } b_2 \cap \text{Span } b_1 = W_2 \cap W_1$. So we can write $z \in W_1 \cap W_2$ using basis B as

$$0 \neq z = \delta_1 v_1 + \dots + \delta_n v_n \quad \text{some } \delta_1, \dots, \delta_n \in F$$

Thus $W_2 = \text{Span } b_2$, we have

$$\delta_1 v_1 + \dots + \delta_n v_n - 0z_1 + \dots + 0z_s = z = 0v_1 + \dots + 0v_n + \gamma_1 z_1 + \dots + \gamma_s z_s$$

By the Coordinate Theorem, $\gamma_1 = 0$, a contradiction.

□

Corollary 8.5

Let V be a vector space over F , $W_1, W_2 \subset V$ finite dimensional subspaces of V . Then

$$\dim(W_1 + W_2) = \dim W_1 + \dim W_2$$

iff

$$W_1 \cap W_2 = \emptyset$$

In this case, we write $W_1 + W_2 = W_1 \oplus W_2$ called the DIRECT SUM.

§8.2 Linear Transformation

In mathematics, whenever you have a collection of objects, one studies maps between them that preserves any special properties of the objects in the collection and tries to see what information can be gained from such maps.

Definition 8.6 (Linear Transformation) — Let V, W be a vector space over F . A map $T : V \rightarrow W$ is called a Linear Transformation, write $T : V \rightarrow W$ is linear if $\forall v_1, v_2 \in V, \forall \alpha \in F$

- $T(v_1 + v_2) = T(v_1) + T(v_2)$.
- $T(\alpha v_1) = \alpha T(v_1)$.
- $T(0_V) = 0_W$.

Notation: We write Tv for $T(v)$.

Remark 8.7. Let V, W be a vector space over F , $T : V \rightarrow W$ a map.

1. If T satisfies 1) and 2), then it satisfies 3):

$$0_W + T(0_V) = T(0_V) = T(0_V + 0_V) = T(0_V) + T(0_V)$$

$$\text{so } 0_W = T(0_V).$$

2. T is linear iff $T(\alpha v_1 + v_2) = \alpha T v_1 + T v_2 \quad \forall v_1, v_2 \in V, \forall \alpha \in F$.
3. If T is linear, $\alpha_1, \dots, \alpha_n \in F, v_1, \dots, v_n \in V$, then

$$T \left(\sum_{i=1}^n \alpha_i v_i \right) = \sum_{i=1}^n \alpha_i T v_i$$

We leave a proof of 2) and 3) as exercises.

Example 8.8

Let V, W be a vector space over F . The followings are linear transformations

1. $0_{V,W} : V \rightarrow W$ by $v \mapsto 0_W$.
2. $V = W$, $1_V : V \rightarrow V$ by $v \mapsto v$.

A linear transformation $T : V \rightarrow V$ is called a **Linear Operator**.

3. If $\emptyset \neq Z \subset W$ is a subset, then we have a map

$$\text{inc} : Z \rightarrow W$$

given by $z \mapsto z$ called the **Inclusion Map**. Then, Z is a subspace of V iff $\text{inc} : Z \hookrightarrow W$ is linear.

Note: $\text{inc} = \underbrace{1_W|_Z}_{\text{Restriction map}}.$

This is the Subspace Theorem.

4. $T : F^n \rightarrow F^{n-1}$ by $(\alpha_1, \dots, \alpha_n) \mapsto (\alpha_1, \dots, \overbrace{i}^{\text{omit}}, \dots, \alpha_n)$ for a fixed i .
5. $T : F^n \rightarrow F$ by $(\alpha_1, \dots, \alpha_n) \mapsto \alpha_i$ for a fixed i .
6. $T : \mathbb{R}^{n-1} \rightarrow \mathbb{R}^n$ by $(\alpha_1, \dots, \alpha_{n-1}) \mapsto (\alpha_1, \dots, \alpha_{i-1}, 0, \alpha_i, \dots, \alpha_n)$ for fixed i .
7. $T : \mathbb{R} \rightarrow \mathbb{R}^n$ by $\alpha \mapsto (0, 0, \dots, \alpha, 0, \dots, 0)$ for fixed i .
8. If $\alpha < \beta$ in \mathbb{R} , $D : C'(\alpha, \beta) \rightarrow C(\alpha, \beta)$ by $f \mapsto f'$.
9. If $\alpha < \beta$ in \mathbb{R} , $\text{Int} : C(\alpha, \beta) \rightarrow C'(\alpha, \beta)$ by $f \mapsto \int f$ where $\int f$ is the antiderivative – constant of integration 0.
10. Fix $\alpha \in F$, then $\lambda\alpha : V \rightarrow V$ by $v \mapsto \alpha v$. Left translation by α .
11. Let $A \in F^{m \times n}$. Define

$$T : F^{n \times 1} \rightarrow F^{m \times 1} \text{ by } T \cdot X = A \cdot X$$

$$\text{i.e. } \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} \mapsto A \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}$$

Matrices can be viewed as linear transformation. We should see the converse is true IF V is a finite dimensional vector space over F . It is not true in general.

§9 | Lec 9: Oct 21, 2020

§9.1 Kernel, Image, and Dimension Theorem

Definition 9.1 (Kernel(Nullspace)) — Let V, W be a vector space over F , $T : V \rightarrow W$ linear set

$$N(T) = \ker T := \{v \in V | Tv = 0_W\}$$

called the nullspace or kernel of T .

Definition 9.2 (Range(Image)) — Let V, W be a vector space over F , $T : V \rightarrow W$ linear set

$$\begin{aligned}\text{im } T = T(V) &:= \{w \in W \mid \exists v \in V \ni Tv = w\} \\ &= \{Tv \mid v \in V\}\end{aligned}$$

called the range or image of T .

Proposition 9.3

Let $T : V \rightarrow W$ be linear. Then

1. $\ker T \subset V$ is a subspace.
2. $\text{im } T \subset W$ is a subspace.

Proof. Left as exercise. □

Theorem 9.4 (Dimension)

Let $T : V \rightarrow W$ be linear with V is a finite dimensional vector space over F . Then

1. $\text{im } T$ and $\ker T$ are finite dimensional vector space over F .
2. $\dim V = \dim \ker T + \dim \text{im } T$.

Note: $\dim \ker T$ is also called the NULLITY of T and $\dim \text{im } T$ is also called the RANK of T .

Proof. Let $n = \dim V$.

$\ker T \subset V$ is a subspace, V is a finite dimensional vector space over F so $\ker T$ is a finite dimensional vector space over F and $\dim \ker T \leq \dim V = n$. Say $m = \dim \ker T$.

Let $\mathcal{B}_0 = \{v_1, \dots, v_m\}$ be a basis for $\ker T$. By the Extension Theorem $\exists \mathcal{B} = \{v_1, \dots, v_m, \dots, v_n\}$ a basis for V .

Claim 9.1. Tv_{m+1}, \dots, Tv_n are linearly indep. (in particular, distinct) and

$$\mathcal{C} = \{Tv_{m+1}, \dots, Tv_n\}$$

is a basis for $\text{im } T$.

If we prove the claim above, then $\text{im } T$ is a finite dimensional vector space over F of dimension $n - m$ and we are done.

Step 1: \mathcal{C} spans $\text{im } T$:

Let $w \in \text{im } T$. By definition, $\exists v \in V \ni Tv = w$. As \mathcal{B} is a basis for $V \exists \alpha_1, \dots, \alpha_n \in F \ni$

$$v = \alpha_1 v_1 + \dots + \alpha_n v_n$$

Hence

$$\begin{aligned} w = T(v) &= T(\alpha_1 v_1 + \dots + \alpha_n v_n) = \alpha_1 T v_1 + \dots + \alpha_n T v_n \\ &= \alpha_1 0_W + \dots + \alpha_m 0_W + \alpha_{m+1} T v_{m+1} + \dots + \alpha_n T v_n \end{aligned}$$

lies w $\text{Span}(\mathcal{C})$ (as $v_1, \dots, v_m \in \ker T$).

Case 2: \mathcal{C} is linearly indep.

Suppose $\alpha_{m+1}, \dots, \alpha_n \in F$ and

$$\alpha_{m+1} T v_{m+1} + \dots + \alpha_n T v_n = 0_W$$

Then

$$0_W = T(\alpha_{m+1} v_{m+1} + \dots + \alpha_n v_n)$$

So $\alpha_{m+1} v_{m+1} + \dots + \alpha_n v_n \in \ker T$. By defn, \mathcal{B}_0 is a basis for $\ker T$. So $\exists \beta_1, \dots, \beta_m \in F \ni$

$$\alpha_{m+1} v_{m+1} + \dots + \alpha_n v_n = \beta_1 v_1 + \dots + \beta_m v_m$$

Hence

$$0 = -\beta_1 v_1 - \dots - \beta_m v_m + \alpha_{m+1} v_{m+1} + \dots + \alpha_n v_n$$

As \mathcal{B} is a basis for V , it is linearly indep, so $\beta_1 = 0, \dots, \beta_m = 0, \alpha_{m+1} = 0, \dots, \alpha_n = 0$ (Coordinate Theorem) and the claim follows. \square

Note: Let V be a finite dimensional vector space over F , $W \subset V$ a subspace, V/W the quotient space, then $- : V \rightarrow V/W, v \mapsto \bar{v} = v + W$ and $\dim V/W = \dim V - \dim W$.

§9.2 Algebra of Linear Transformation

We want to study the set of all linear transformation from a vector space over F V to a vector space over F W . Let V, W be a vector space over F . Set

$$L(V, W) := \{T : V \rightarrow W | T \text{ is linear}\}$$

Check: if $T, S \in L(V, W), \alpha \in F$, then $\alpha T + S \in L(V, W)$. Since we know $\mathcal{F}(V, W) = \{f : V \rightarrow W | f \text{ a map}\}$ is a vector space over F , by the Subspace Theorem, $L(V, W) \subset \mathcal{F}(V, W)$ is a subspace.

Proposition 9.5

Let V, W be a vector space over F , then $L(V, W) \subset \mathcal{F}(V, W)$ is a subspace.

Now we know if we have maps

$$f : X \rightarrow Y \quad \text{and} \quad g : Y \rightarrow Z,$$

we have the COMPOSITE MAP

$$g \circ f : X \rightarrow Z \quad \text{by} \quad (g \circ f)(x) = g(f(x)) \forall x \in X$$

where \circ is called the COMPOSITION (and often omitted when clear). Then we have

need
recheck

Proposition 9.6

Let V, W, X, U be vector space over F , $T, T' : V \rightarrow W$, $S, S' : W \rightarrow X$, $R : X \rightarrow U$ all be linear. Then,

1. $S \circ T : V \rightarrow W$ is linear. (the composition of linear transformations is linear).
2. $R \circ (S \circ T) = (R \circ S) \circ T$ and linear.
3. $S \circ (T + T') = S \circ T + S \circ T'$ and linear.
4. $(S + S') \circ T = S \circ T + S' \circ T$ and linear.

Proof.

$$\begin{aligned}(S \circ T)(\alpha v_1 + v_2) &= S(T(\alpha v_1 + v_2)) = S(\alpha T v_1 + T v_2) \\ &= \alpha S \circ T(v_1) + S \circ T(v_2)\end{aligned}$$

$\forall v_1, v_2 \in V, \alpha \in F$.

The rest are left as exercises. □

Definition 9.7 (Linear Operator) — Let V be a vector space over F , $T : V \rightarrow V$ linear, so a linear operator is defined as

$$\begin{aligned}T^n &:= \underbrace{T \circ \dots \circ T}_n \quad \text{if } n \in \mathbb{Z}^+ \\ T^0 &= 1_V\end{aligned}$$

Proposition 9.8

Let V be a vector space over F . Then $L(V, V)$ under $+$ and \circ of functions $V \rightarrow V$ satisfies all the axioms of a field except possibly (M3) and (M4) with

$$\begin{aligned}\text{one} &= 1_V : V \rightarrow V \quad \text{by } v \mapsto v \\ \text{zero} &= 0_V : v \mapsto 0\end{aligned}$$

We say $L(V, V)$ is a (non-commutative) ring of $M_n F$.

§9.3 Linear Transformation Theorems

Definition 9.9 (Properties/Consequences of Linear Transformation) — Let $T : V \rightarrow W$ be linear. We say that T is

1. a **MONOMORPHISM** (write mono or monic) or **NONSINGULAR** if T is 1 – 1. (i.e., injective).
2. an **EPIMORPHISM** (write epi or epic) if T is onto (i.e., surjective).
3. an **ISOMORPHISM** (write iso) or **INVERTIBLE** if T is bijective and $T^{-1} : W \rightarrow V$ is linear. We say V, W vector spaces over F are **ISOMORPHIC** (write $V \cong W$) if \exists an isomorphism $S : V \rightarrow W$, we also write an isomorphism $S : V \rightarrow W$ as $S : V \xrightarrow{\sim} W$

Remark 9.10. $V \cong W$ vector space over F means that we cannot take V and W apart algebraically.

Example 9.11

$F^{n+1} \cong F[t]_n$ as $F^{n+1} \rightarrow F[t]_n$ by $(\alpha_0, \dots, \alpha_n) \mapsto \alpha_0 + \alpha_1 t_1 + \dots + \alpha_n t^n$ is an isomorphism with inverse $F[t]_n \rightarrow F^{n+1}$ by $\alpha_0 + \alpha_1 t + \dots + \alpha_n t^n \mapsto (\alpha_0, \dots, \alpha_n)$

$$\begin{aligned} T^{-1}(\alpha w_1 + w_2) &= T^{-1}(\alpha T v_1 + T v_2) = T^{-1}(T(\alpha v_1 + v_2)) \\ &= T^{-1}T(\alpha v_1 + v_2) \\ &= \alpha v_1 + v_2 \\ &= \alpha T^{-1} w_1 + T^{-1} w_2 \quad \square \end{aligned}$$

Corollary 9.12

Let $T : V \rightarrow W$ be a monomorphism. Then $V \cong \text{im} T$ via T .

Remark 9.13. If V, W, X are vector space over F , then

1. $V \cong V$
2. $V \cong W \rightarrow W \cong V$
3. $V \cong W$ and $W \cong X$ then $V \cong X$

In algebra, isomorphisms are usually easier to check than are one might assume, because the following result is often true.

Proposition 9.14

Let $T : V \rightarrow W$ be linear. Then T is an isomorphism iff T is bijective.

Proof. (\rightarrow) immediate.

(\leftarrow) Let $T^{-1} : W \rightarrow V$ be the set inverse of $T : V \rightarrow W$, so

$$T \circ T^{-1} = 1_W \quad \text{and} \quad T^{-1} \circ T = 1_V$$

In particular, if $v \in V$ and $w \in W$,

$$w = Tv \quad \text{iff} \quad T^{-1}w = v$$

Let $w_1, w_2 \in W$, $\alpha \in F$. To show

$$T^{-1}(\alpha w_1 + w_2) = \alpha T^{-1}w_1 + T^{-1}w_2$$

T is onto so

$$\exists v_i \in V \ni Tv_i = w_i, i = 1, \dots$$

Hence, we have

$$\begin{aligned} T^{-1}(\alpha w_1 + w_2) &= T^{-1}(\alpha Tv_1 + Tv_2) = T^{-1}(T(\alpha v_1 + v_2)) \\ &= T^{-1}T(\alpha v_1 + v_2) = \alpha v_1 + v_2 \\ &= \alpha T^{-1}w_1 + T^{-1}w_2 \end{aligned}$$

□

§10 | Lec 10: Oct 23, 2020

§10.1 Monomorphism, Epimorphism, and Isomorphism

Corollary 10.1

Let $T : V \rightarrow W$ be a monomorphism. Then $V \cong \text{im } T$ via T .

Definition 10.2 (Linear Map) — Let $T : V \rightarrow W$ be linear. We say T takes linearly independent sets to linearly independent sets if $v_i, i \in I$ are linearly independent in V (in particular, distinct). Then, $Tv_i, i \in I$ are linearly indep. in W . ($Tv_i \neq Tv_j$ if $i \neq j$ in I)

Theorem 10.3 (Monomorphism)

Let $T : V \rightarrow W$ be linear. Then the followings are true

1. T is 1-1, so it's monomorphism.
2. T takes linearly indep. sets in V to linearly indep. sets in W .
3. $\ker T = 0 := \{0_V\}$.
4. $\dim \ker T = 0$.

Proof. • 3) iff 4) is the defn of the 0-space.

- 1) \rightarrow 2) It suffices to show that T takes finite linearly indep. sets in V to linearly indep. sets in W .

Suppose that $v_1, \dots, v_n \in V$ are linearly indep. and $\alpha_1, \dots, \alpha_n \in F$ satisfy

$$0_W = \alpha_1 T v_1 + \dots + \alpha_n T v_n$$

Then

$$T(0_V) = 0_W = T(\alpha_1 v_1 + \dots + \alpha_n v_n)$$

As T is $1 - 1$

$$0_V = \alpha_1 v_1 + \dots + \alpha_n v_n$$

Since v_1, \dots, v_n are linearly indep. $\alpha_i = 0, i = 1, \dots, n$ as needed.

- 2) \rightarrow 3) Let $v \in \ker T$. Then $Tv = 0_W$. If $v \neq 0$, then $\{v\}$ is linearly indep. By 2) $Tv \neq 0_W$ as then $\{Tv\}$ is linearly indep. So $v = 0$.
- 3) \rightarrow 1) If $Tv_1 = Tv_2, v_1, v_2 \in V$, then

$$0_W = Tv_1 - Tv_2 = T(v_1 - v_2)$$

So $v_1 - v_2 = 0_V$ by 3), i.e., $v_1 = v_2$ □

Remark 10.4. The Monomorphism Theorem says $\ker T$ measures the deviation of T from being $1 - 1$.

Note: In the Monomorphism Theorem, we do not assume that V or W is a finite dimensional vector space over F .

Theorem 10.5 (Isomorphism)

Suppose $T : V \rightarrow W$ is linear with $\dim V = \dim W < \infty$, i.e., V, W are finite dimensional vector space over F of the same dimension. Then the followings are true

1. T is an isomorphism.
2. T is a monomorphism.
3. T is an epimorphism.
4. If $\mathcal{B} = \{v_1, \dots, v_n\}$ is a basis for V , then $\{Tv_1, \dots, Tv_n\}$ is a basis for W (so Tv_1, \dots, Tv_n are distinct), i.e., T takes basis of V to basis of W .
5. There exists a basis \mathcal{B} of V that maps to a basis of W .

Remark 10.6. 1. The condition that $\dim V = \dim W < \infty$ is crucial

Come up with a counter example

2. Let $V \cong W$ with V, W be finite dimensional vector space over F . So $\dim V = \dim W$. Let $S : V \rightarrow W$ be linear. Then S may or may not be an isomorphism, e.g., if S is the zero map then it is not an isomorphism unless $V = 0$. The theorem only says that \exists an isomorphism and any such satisfies the theorem.
3. Let $f : A \rightarrow B$ be a map of finite sets with $|A| = |B|$. Then f is a bijection iff f is an injection iff f is a surjection.

Proof. (of Theorem)

- 1) \rightarrow 2) follows by defn.
- 2) \rightarrow 3) By the Dimension Theorem

$$\dim W = \dim V = \dim \ker T + \dim \operatorname{im} T$$

Thus, T is onto iff $\operatorname{im} T = W$ iff $\dim W = \dim \operatorname{im} T$ (by the Corollary to the Existence Theorem) iff $\dim \ker T = 0$ iff T is 1-1.

- 3) \rightarrow 1) as 3) \rightarrow 2) and 1) = 2) + 3) by the Proposition ?
- 2) \rightarrow 4) Let $\{v_1, \dots, v_n\}$ be a basis for V . By the Monomorphism Theorem, Tv_1, \dots, Tv_n are linearly indep. in W , so

$$n \leq \dim W = \dim V = n$$

Hence $\{Tv_1, \dots, Tv_n\}$ also spans as $\dim W = \dim V$.

- 4) \rightarrow 5) \rightarrow 3) are clear.

□

§10.2 Existence of Linear Transformation

The next result is really the defining property of finite dimensional vector space and linear transformation.

Theorem 10.7 (Existence of Linear Transformation (UPVS))

– (Universal Property of Vector Space) Let V be a finite dimensional vector space over F , $\mathcal{B} = \{v_1, \dots, v_n\}$ a basis for V and W an arbitrary vector space over F . Let $w_1, \dots, w_n \in W$, not necessarily distinct. Then

$$\exists! T : V \rightarrow W \text{ linear } \ni Tv_i = w_i \forall i$$

We can write this in an other way as follows:

Let $B \hookrightarrow V$ be a basis for V , V a finite dimensional vector space over F and W a vector space over F . Given a diagram,

$$\begin{array}{ccc} B \hookrightarrow V & & \\ \searrow f & \text{of sets and} & \\ & \text{set maps} & \\ & W & \end{array}$$

then $\exists! T : V \rightarrow W$ linear \ni

$$\begin{array}{ccc} B \hookrightarrow V & & \\ \searrow f & \text{inc} & \downarrow T \\ & W & \end{array}$$

commutes, i.e., $T \circ \text{inc} = f$.

Proof. Define $T : V \rightarrow W$ as follows: let $v \in V$. The $\exists! \alpha_1, \dots, \alpha_n \in F \ni v = \alpha_1 v_1 + \dots + \alpha_n v_n$ by the Coordinate Theorem. Define

$$Tv = T(\alpha_1 v_1 + \dots + \alpha_n v_n) := \alpha_1 w_1 + \dots + \alpha_n w_n$$

Since the α_i ARE UNIQUE, this defines a map – we say $T : V \rightarrow W$ is WELL – DEFINED. Certainly, $Tv_i = w_i, i = 1, \dots, n$. To show T is linear, let $v = \sum_{i=1}^n \alpha_i v_i, v' = \sum_{i=1}^n \beta_i v_i, \alpha, \alpha_i, \beta_j \in F \forall i, j$. Then

$$\begin{aligned} T(\alpha v + v') &= T\left(\alpha \sum_{i=1}^n \alpha_i v_i + \sum_{i=1}^n \beta_i v_i\right) \\ &= T\left(\sum_{i=1}^n (\alpha \alpha_i + \beta_i) v_i\right) = \sum_{i=1}^n (\alpha \alpha_i + \beta_i) w_i \\ &= \alpha \sum_{i=1}^n \alpha_i w_i + \sum_{i=1}^n \beta_i w_i = \alpha Tv + Tv' \end{aligned}$$

as needed. This shows existence.

Uniqueness: Let $T : V \rightarrow W$ by (*) and $S : V \rightarrow W$ linear s.t. $Sv_i = w_i \forall i$. To show $S = T$, let $v = \sum_{i=1}^n \alpha_i v_i, \alpha_i \in F$ unique, $i = 1, \dots, n$. Then $Tv = \sum_{i=1}^n \alpha_i Tv_i = \sum_{i=1}^n \alpha_i w_i$ which is equivalent to

$$= \sum_{i=1}^n \alpha_i Sv_i = S\left(\sum_{i=1}^n \alpha_i v_i\right) = Sv$$

So $S = T$ and we have proven uniqueness. \square

Remark 10.8. The theorem says a linear transformation from a finite dimensional vector space over F is completely determined by what it does to a fixed basis. i.e., as there are no non-trivial RELATIONS on linear combos of elements in \mathcal{B} , the only relation in $\text{im } T$ will arise from the kernel of T .

§11 | Dis 1: Oct 1, 2020

Overview of the class:

- HW – 20%
- Takehome Midterm – 20(25)%
- Midterm – 20(0)%
- Final – 40(55)%

Note: For starred homework problems, we can resubmit these problems (if we did not get full credit for it).

Plan:

1. Proofs
2. Sets
3. Functions

§11.1 Sets

- \mathbb{N} = set of natural numbers = $\{1, 2, 3, 4, \dots\}$
- \mathbb{Z} = set of integers = $\{\dots, -2, -1, 0, 1, 2, \dots\}$
- \mathbb{Q} = set of rational numbers = $\{\frac{a}{b} : a, b \in \mathbb{Z}, b \neq 0\}$
- \mathbb{R} = set of real numbers(number line)
- \mathbb{C} = set of complex numbers = $\{a + bi | a, b \in \mathbb{R}\}$
- \mathbb{R}^2 = (xy)-plane = $\{(a, b) : a, b \in \mathbb{R}\}$

Notation: subset – \subseteq , proper subset – \subsetneq (subset and not equal), empty subset – \emptyset .

§11.2 Functions

What is a set?

– A collection of elements

Example 11.1 • $A = \{\text{cat}, \text{dog}\}$

- $B = \{1, 2, 3\}$

$$\bullet C = \mathbb{R}^2$$

So what is a function?

$$f : \underbrace{A}_{\text{set called the domain of } f} \mapsto \underbrace{B}_{\text{this set is called the codomain of } f}$$

In general, **range** and **codomain** are two different things.

Given any element $a \in A$, it gives an element $f(a) \in B$.

Example 11.2 • $f : \mathbb{R} \mapsto \mathbb{R}$ given by $f(x) = x^2$ for any $x \in \mathbb{R}$

- $g : \mathbb{R} \mapsto \left(-\frac{\pi}{2}, \frac{\pi}{2}\right)$ given by $g(\theta) = \tan(\theta)$
- Is $h(x) = \frac{1}{x}$ a function? No – Poorly defined. If $\mathbb{R} \mapsto \mathbb{R}$ is included, still not defined because of $h(0)$

$h : \mathbb{R} \setminus \{0\} \mapsto \mathbb{R}$ is a function

- $k : (0, 1) \mapsto \mathbb{R}$ given by $k(x) = x^2$. Still a function but it's different from $f : \mathbb{R} \mapsto \mathbb{R}$ given by $f(x) = x^2$

Note: Domain and codomain are part of the function

- $T : \mathbb{R}^2 \mapsto \mathbb{R}^2$ given by $T(a, b) = (a + b, a - b)$. Yes, this is a function
- $S : \mathbb{R}^3 \mapsto \mathbb{R}^2$ given by

$$S(x, y, z) = \begin{bmatrix} 3 & 2 & 1 \\ 4 & 4 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix}$$

This is also a function. S and T are linear transformations (functions from one vector space to another)

Definition 11.3 (Injection & Surjection) — A function $f : A \mapsto B$ is injective (one-to-one) if for any $a_1, a_2 \in A$, if $f(a_1) = f(a_2)$ then $a_1 = a_2$.

A function $f : A \mapsto B$ is surjective (onto) if for all $b \in B$, there is an $a \in A$ such that $f(a) = b$.

Example 11.4

Let $T : \mathbb{R}^2 \mapsto \mathbb{R}^2$ be given by $T(a, b) = (a + b, a - b)$. Show T is injective. Show T is surjective.

Suppose $T(x_1, y_1) = T(x_2, y_2)$, then $(x_1 + y_1, x_1 - y_1) = (x_2 + y_2, x_2 - y_2)$. So,

$$x_1 + y_1 = x_2 + y_2$$

$$x_1 - y_1 = x_2 - y_2$$

Solve the above system of linear equations, we obtain $(x_1, y_1) = (x_2, y_2)$. We conclude

T is injective. □

T is surjective?

Let $(c, d) \in \mathbb{R}^2$ be arbitrary. We want to show there exists an $(a, b) \in \mathbb{R}^2$ with $T(a, b) = (c, d)$

$$a + b = c$$

$$a - b = d$$

$$a = \frac{c + d}{2}$$

$$b = \frac{c - d}{2}$$

Note: $(a, b) \in \mathbb{R}^2$ is a valid input.

Take $a = \frac{c+d}{2}$ and $b = \frac{c-d}{2}$. Then,

$$\begin{aligned} T(a, b) &= \left(\frac{c+d}{2} + \frac{c-d}{2}, \frac{c+d}{2} - \frac{c-d}{2} \right) \\ &= \left(\frac{2c}{2}, \frac{2d}{2} \right) \\ &= (c, d) \end{aligned}$$

Since $(c, d) \in \mathbb{R}^2$ was arbitrary, we conclude T is surjective □

§12 | Dis 2: Oct 6, 2020

§12.1 Field

Definition 12.1 ((1.2)) — A field consists of a set F with two elements $0, 1 \in F$ ($0 \neq 1$) and two operations, multiplication (\cdot) and addition ($+$)
 $(F, +)$

- $+$ is associative
- $+$ is commutative
- has an additive identity (0)
- has an additive inverse

”abelian group”

(F^*, \cdot) (everything except 0) — $F \setminus \{0\} = F^*$

- assoc
- comm
- has an identity (1)
- has mult inverse

”abelian group”

Finally, distributive prop also holds

$$\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$$

Linear Algebra works over any field! (Not just \mathbb{R} like we did in lower div Lin Alg class).

Claim 12.1. Let F be a field. Let $\alpha \in F$ be an arbitrary element of the field. Then $0\alpha = 0$

Proof. Note since $0 + 0 = 0$

$$0\alpha = (0 + 0)\alpha$$

However, by the dist. prop,

$$(0 + 0)\alpha = 0\alpha + 0\alpha$$

Then $0\alpha = 0\alpha + 0\alpha$. Subtract 0α from both sides (i.e. add its additive inverse to both sides)

$$-(0\alpha) + (0\alpha) = -(0\alpha) + 0\alpha + 0\alpha$$

So,

$$0 = 0 + 0\alpha = 0\alpha$$

So, $0\alpha = 0$

□

Claim 12.2. Let F be a field, and let $\alpha, \beta \in F$ s.t. $\alpha\beta = 0$. Then either $\alpha = 0$ or $\beta = 0$.

Proof. If $\alpha = 0$, there is nothing to show. Suppose $\alpha \neq 0$. We want to show $\beta = 0$. Since $\alpha \neq 0$, $\alpha \in F^*$ has a multiplicative inverse $\alpha^{-1} \in F^*$.

Since $\alpha\beta = 0$, we can mult both sides by α^{-1} on the left to get $\alpha^{-1}(\alpha\beta) = \alpha^{-1}(0) = 0$. Moreover, by associativity,

$$\alpha^{-1}(\alpha\beta) = (\alpha^{-1}\alpha)\beta = 1\beta = \beta$$

Hence, $\beta = 0$. So, $\beta = 0$ as desired.

□

Example 12.2

$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields. \mathbb{Z} is not a field.

Example 12.3

$\underbrace{\mathbb{Z}/12\mathbb{Z}}_{\text{integers mod 12}} = \{0, 1, 2, 3, \dots, 11\}$

Clock arithmetic. Addition is clock addition:

$$2 + 11 = 1$$

Multiplication is "clock mult"

$$2 \cdot 11 = 10$$

Multiply and add like normal but then subtract multiples of 12 until you get an element of the set.

- Additive identity: 0
- Multiplicative identity: 1

Is $\mathbb{Z}/12\mathbb{Z}$ a field?

- additive inverse ✓
- identity ✓
- comm ✓
- assoc ✓
- mult inverse $\dots \implies$ NO!

Or different argument:

$$2 \cdot 6 = 0^-$$

But $2 \neq 0$ and $6 \neq 0$. This violates a property of fields:

$$\alpha\beta = 0 \implies \alpha = 0 \text{ or } \beta = 0$$

So $\mathbb{Z}/12\mathbb{Z}$ can't be a field.

Example 12.4

$\mathbb{Z}/3\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}\}$

- additive id: 0
- mult id: 1

Mult inv:

$$1 \cdot 1 = 1$$

$$2 \cdot 2 = 1 \checkmark$$

Additive inverse:

$$0 + 0 = 0$$

$$1 + 2 = 0 \checkmark$$

$\mathbb{Z}/3\mathbb{Z}$ is a field!

When is $\mathbb{Z}/n\mathbb{Z}$ is a field?

- $n = 2$: yes
- $n = 3$: yes
- $n = 4$: no
- $n = 13$: yes
- \vdots

Same sort of argument works whenever n is composite.

$\mathbb{Z}/p\mathbb{Z}$ is a field for p prime. Proof uses Bezat lemma (Euclidean algorithm)

Example 12.5

$$\mathbb{Z}/7\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \dots, \bar{6}\}$$

Everything has a mult.inverse

§13 | Dis 3: Oct 8, 2020

§13.1 Characteristics of a Finite Field

Let F be a finite field. Then, there must be a repeat in the following list:

$$1, 1+1, 1+1+1, \dots$$

If there wasn't a repeat, clearly, this would be an infinite list of distinct elements in F . Then we have for some $j < k$

$$\underbrace{1+1+1\dots+1}_{j \text{ times}} = \underbrace{1+1+\dots+1}_{k \text{ times}}$$

So, $0 = \underbrace{1+1+\dots+1}_{k-j \text{ times}}$ $k-j > 0$. Thus, in a finite field, adding 1 to itself repeatedly must at some point give 0. (need to add up 1 to itself at most $|F|$ number of times)

Claim 13.1. There is no field with 10 elements and $1 + 1 = 0$

Proof. Let F be a field of 10 elements with $1 + 1 = 0$. Let's list the elements

$$0, 1, \alpha (\alpha \neq 0, 1)$$

Is $\alpha + 1$ already on my list?

$$\begin{aligned} \alpha + 1 = 0 &\implies \alpha + 1 + 1 = 0 + 1 = 1 \implies \alpha = 1 \\ \alpha + 1 = 1? &\implies \alpha = 0 \\ \alpha + 1 = \alpha? &\implies 1 = 0 \end{aligned}$$

None are possible so $\alpha + 1$ is not on our list so far

$$0, 1, \alpha, \alpha + 1, \beta$$

Then, $\beta + 1$ isn't on the list.

$$0, 1, \alpha, \alpha + 1, \beta, \beta + 1$$

Notice $\alpha + \beta$ isn't on the list yet and so is $\alpha + \beta + 1$. There are 8 elements in F . Since $|F| = 10$, let $\gamma \in F$ be something not on the list so far and $\alpha + 1$ is not on the list so far, so it must be the last element of F .

$$0, 1, \alpha, \alpha + 1, \beta, \beta + 1, \alpha + \beta, \alpha + \beta + 1, \gamma, \gamma + 1$$

But then $\gamma + \alpha$ is not on the list. This would give an 11th ... but $|F| = 10$ contradiction \square

Note: **Characteristics:** the number of times you add 1 to get 0 in a field. For the case of characteristics 2, EVERYTHING IS ITS OWN ADDITIVE INVERSE.

Claim 13.2. There is no field of 10 elements with $1 + 1 \neq 0$ and $1 + 1 + 1 = 0$

Proof. List the element:

$$0, 1, 2, \alpha, \alpha + 1, \alpha + 2, \beta, \beta + 1, \beta + 2, \gamma$$

But then $\gamma + 1$ isn't on this list. – Contradiction. \square

What if $1 + 1 + 1 + 1 = 0$?

$$\begin{aligned} \underbrace{(1+1)}_x + \underbrace{(1+1)}_x &= 0 \\ x + x &= 0 \\ x(1+1) &= 0 \\ (1+1)(1+1) &= 0 \end{aligned}$$

So either $(1+1) = 0$ or $(1+1) = 0$. We already ruled out $1 + 1 = 0$.

Can $1 + 1 + 1 + 1 = 0$? List the element

$$0, 1, 2, 3, 4, \alpha, \alpha + 1, \alpha + 2, \alpha + 3, \alpha + 4$$

What is 2α ? Trick: $2 \cdot 3 = (1+1)(1+1+1) = \underbrace{1+1+1+1+1}_0 + 1 = 1$

Can $2\alpha = 0$? $\implies \alpha = 0$ or $2 = 0$. Can $2\alpha = 1$? Mult both sides by 3

$$3 \cdot 2\alpha = 3$$

$\implies \alpha = 3$ (nope!)

$$2\alpha = 2? \quad 2\alpha = 3? \quad 2\alpha = 4?$$

Proceed similarly and we can see that $1 + 1 + 1 + 1 + 1 \neq 0$

$$1 + 1 + 1 + 1 + 1 + 1 = 0?$$

$$(1 + 1)(1 + 1 + 1) = 0$$

$1 + 1 = 0$ or $1 + 1 + 1 = 0$ (but we already ruled out both cases). Now,

$$1 + 1 + 1 + 1 + 1 + 1 + 1 = 0?$$

List:

$$0, 1, 2, 3, 4, 5, 6, \alpha, \alpha + 1, \alpha + 2$$

$\alpha + 3$ is not on this list.

- $8 = 0$? We can have $(1 + 1)(1 + 1)(1 + 1) = 0$ but $(1 + 1) = 0$ also ruled out.
- $9 = 0 \implies (1 + 1 + 1) = 0$ also ruled out.
- $10 = 0 \implies (1 + 1) = 0$ or $(1 + 1 + 1 + 1 + 1) = 0$ which is also ruled out above.

So there are no fields with 10 elements. \square

§14 | Dis 4: Oct 13, 2020

§14.1 Vector Space and Subspace

Definition 14.1 ((2.1)) — A vector space over a field F is a set V with some additional structure:

$(V, +)$ is an abelian group (V has addition which is assoc, comm, add. inv, add. iden)

Scalar mult

$$\cdot : F \times V \rightarrow V$$

with

$$1_F \cdot v = v \quad \forall v \in V$$

$$(\alpha\beta) \cdot v = \alpha(\beta v) \quad \forall \alpha, \beta \in F, v \in V$$

$$(\alpha + \beta)v = \alpha v + \beta v$$

$$\alpha(v + w) = \alpha v + \alpha w$$

We're overloading $+$ and \cdot . In F :

$$\alpha + \beta, \quad \alpha \cdot \beta$$

In V :

$$v + w, \quad \alpha \cdot v$$

We say $S \subseteq V$ is a subspace if

1. It is closed under addition.
2. It is closed under scalar multiplication.
3. It is not empty.

OR

4. $0 \in S$

Then, S will automatically become a vector space over the same field(it inherits the nice properties from V).

Example 14.2 (Abstract Vector Space)

In general, vector spaces might not always have nice geometric descriptions like in $\mathbb{R}, \mathbb{R}^2, \mathbb{R}^3$, etc

1. $\underbrace{\mathbb{R}[t]}_{\substack{\text{set of all polynomials in } t \text{ with real coeff} \\ n \in \mathbb{Z}, n \geq 0.}} = \{a_0 + a_1t + a_2t^2 + \dots + a_nt^n : a_i \in \mathbb{R} \forall i\}$ and
2. $\mathbb{R}[t]_n$: set of all polynomials in t with real coeff and degree $\leq n$.
 $\mathbb{R}[t]_2 = \{a + bt + ct^2, \quad a, b, c \in \mathbb{R}\}$
3. $M_n(\mathbb{R}), \mathbb{R}^{n \times n}$: set of n by n matrices with real coeff.

$$M_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{R} \right\}$$

4. Is $GL_2(\mathbb{R})$ a subspace of $M_2(\mathbb{R})$ (as an \mathbb{R} -vector space)?

$$GL_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{R} \text{ and is invertible} \right\}$$

$GL_2(\mathbb{R}) \subseteq M_2(\mathbb{R})$. No it is not a subspace.

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \notin GL_2(\mathbb{R})$$

Example 14.3 1. $C[a, b] = \{f : [a, b] \rightarrow \mathbb{R} : f \text{ is continuous}\}$ is a vector space over \mathbb{R} (with usual/natural choice of addition and scalar mult).

2. $W = \{f \in C[a, b] : f(a) = 0\} \subseteq C[a, b]$

Is W is a subspace?

- $0 \in W$ since $0(a) = 0$
- Let $f, g \in W$. Since $f \in W, f(a) = 0, g \in W, g(a) = 0$. Hence, $(f + g)(a) = f(a) + g(a) = 0 + 0 = 0$. Thus, $f + g \in W$.
- Let $f \in W$ and $\alpha \in \mathbb{R}$. Then

$$\begin{aligned}\alpha(f)(a) &= \alpha(f(a)) \\ &= \alpha(0) \\ &= 0\end{aligned}$$

Thus, $W \subseteq C[a, b]$ is a subspace.

\mathbb{C} is a 2-dimensional vector space over \mathbb{R} . $\{1, i\}$ will form a basis of \mathbb{C} as an \mathbb{R} - vector space.

$\left\{ \begin{array}{l} \text{Linearly Indep.} \\ \text{Span all of } \mathbb{C} \end{array} \right. \implies \text{Every complex number can be uniquely written as } a + bi \text{ where } a, b \in \mathbb{R}$

\mathbb{C} is also a vector space over the field \mathbb{C} . It is a 1-dimensional vector space over \mathbb{C} .

Basis (every complex number can be written as $z \cdot 1$ for some $z \in \mathbb{C}$): $\{1\}$ will work (don't need i , it is allowed to be a scalar).

\mathbb{C} is also a vector space over \mathbb{Q} . As a \mathbb{Q} - vector space, \mathbb{C} is infinite dimensional!

Proof. (sketch) \mathbb{C} is uncountably infinite. There's too many of them for us to be able to write each as a \mathbb{Q} - linear combos of some finite list of vectors.

Alternative: $1, \pi, \pi^2, \pi^3, \dots$ is an infinite list of vectors (elements of \mathbb{C}) which are linearly indep. over \mathbb{Q} . \square

Example 14.4

Let V be a vector space over a field F . We define V^* , the dual vector space, as

$$V^* = \{T : V \rightarrow F \mid T \text{ is } F\text{-linear}\}$$

Then V^* is also a vector space over F .

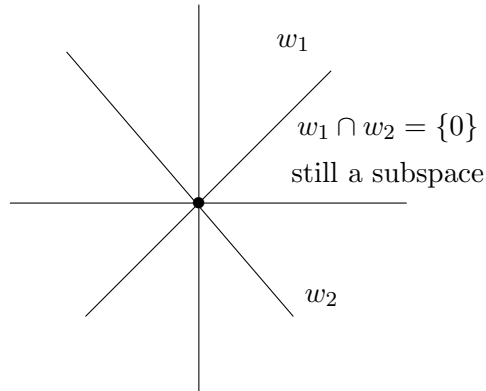
Relatedly, if V, W are F - vector spaces, then

$$L(V, W) = \{T : V \rightarrow W \mid T \text{ is } F\text{-linear}\}$$

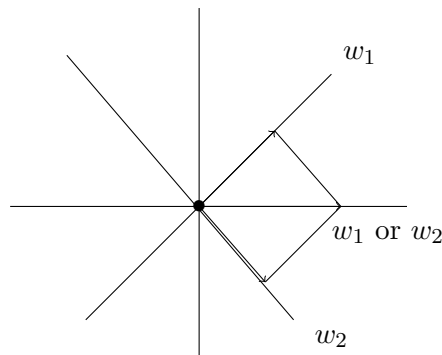
is also a vector space.

Note: Let V be a vector space over F . The intersection of subspaces of V will still be a subspace of V

Example:



Let V be a vector space over F . The union of subspaces of V might not be a subspace.



not closed under addition in general

Note:

$$A \cup B = \{v \in V : v \in A \text{ or } v \in B\}$$

$$A + B = \{v \in V : \text{there exists } a \in A, b \in B \ni a + b = v\}$$

§15 | Dis 5: Oct 15, 2020

§15.1 Linear Independence, Span, & Subspaces

Problem 15.1. Let \mathbb{F} be a field on V be a vector space over \mathbb{F} . Let $\alpha \in \mathbb{F}$ be arbitrary. Show $\alpha \cdot \vec{0} = \vec{0}$.

Proof. Let $\alpha \in \mathbb{F}$ be arbitrary. Note:

$$\alpha \cdot \vec{0} = \alpha(\vec{0} + \vec{0}) = \alpha \cdot \vec{0} + \alpha \cdot \vec{0}$$

Adding the additive inverse of $\alpha \cdot \vec{0}$ to both sides we see

$$\begin{aligned} -(\alpha \cdot \vec{0}) + \alpha \cdot \vec{0} &= \left(-(\alpha \cdot \vec{0}) + \alpha \cdot \vec{0} \right) + \alpha \cdot \vec{0} \\ \vec{0} &= \vec{0} + \alpha \cdot \vec{0} \end{aligned}$$

Thus, $\vec{0} = \alpha \cdot \vec{0}$ as desired. □

Problem 15.2. If $\alpha \in \mathbb{F}$ and $\vec{v} \in V$ satisfy $\alpha \vec{v} = \vec{0}$, then either $\alpha = 0$ or $\vec{v} = \vec{0}$.

Proof. If $\alpha = 0$, we're done. If $\alpha \neq 0$, it has a mult. inverse, $\alpha^{-1} \in F^x$. Then

$$\begin{aligned}\alpha^{-1}(\alpha \vec{v}) &= (\alpha^{-1}\alpha) \cdot \vec{v} \\ &= 1_{\mathbb{F}} \cdot \vec{v} = \vec{v}\end{aligned}$$

On the other hand, since $\alpha \vec{v} = \vec{0}$, we have

$$\alpha^{-1}(\alpha \vec{v}) = \alpha^{-1}(\vec{0}) = \vec{0}$$

So we see that if $\alpha \neq 0$ then $\vec{v} = \vec{0}$. This completes the proof. \square

Problem 15.3. a) Find a nonempty subset $U \subseteq \mathbb{R}^2$ which is closed under scalar mult but is not a subspace of \mathbb{R}^2 (over \mathbb{R}).

b) Find a nonempty subset $U \subseteq \mathbb{R}^2$ which is closed under addition but is not a subspace.

a) Take $U = \text{span} \left\{ \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\} \cup \text{span} \left\{ \begin{pmatrix} -1 \\ 1 \end{pmatrix} \right\}$. One can show U is closed under scalar mult but not under addition.

b) Left as exercise.

Let V be a vector space over \mathbb{F} . For $u, w \subseteq V$ subspaces, define

$$u + w = \{ \vec{u} + \vec{w} : \vec{u} \in U, \vec{w} \in W \}$$

Claim 15.1. $u + w \subseteq V$ is also a subspace.

Proof. (Sketch)

- Show $0 \in u + w$.
- Show $u + w$ is closed under $+$.
- Show $u + w$ is closed under scalar mult.

\square

Let $v_1, \dots, v_k \in V$. Define

$$\text{span}(\{v_1, \dots, v_k\}) = \left\{ \sum_{i=1}^k \alpha_i v_i : \alpha_i \in \mathbb{F} \right\} \subseteq V$$

(it's the set of all \mathbb{F} -linear combinations of v_1, \dots, v_k).

Claim 15.2. $\text{Span}(\{v_1, \dots, v_k\}) \subseteq V$ is a subspace of V .

If $S \subseteq V$ is an infinite subset of V , we can still define $\text{span}(S)$ as the set of all finite linear combos.

$$\sum_{i=1}^k \alpha_i v_i \quad \text{where } \alpha_i \in \mathbb{F}, v_i \in S$$

$\text{Span}(S) \subseteq V$ is also a subspace.

Example 15.1

$\mathbb{F} = \mathbb{R}, V = \mathbb{R}^3$.

$$U = \text{span} \left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \right\} = x\text{-axis}$$

$$W = \text{span} \left\{ \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \right\} = xy\text{-plane}$$

What is $u + w$?

$u + w = xy\text{-plane}$.

Claim: $u + w = \text{span} \left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \right\}$

Proof. Let $\vec{x} \in u + w$. Then there exists $\vec{u} \in U$ and $\vec{w} \in W$ s.t. $\vec{x} = \vec{u} + \vec{w}$. Since

$$\vec{u} \in U = \text{span} \left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \right\}, \text{ there exists an } \alpha \in \mathbb{R} \text{ with } \vec{u} = \alpha \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}. \text{ Similarly, since } \vec{w} \in$$

$$W = \text{span} \left\{ \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \right\}, \text{ there exists } \beta, \gamma \in \mathbb{R} \text{ with } \vec{w} = \beta \cdot \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} + \gamma \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \beta \\ \beta + \gamma \\ 0 \end{pmatrix}.$$

Hence,

$$\begin{aligned} \vec{x} = \vec{u} + \vec{w} &= \begin{pmatrix} \alpha \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} \beta \\ \beta + \gamma \\ 0 \end{pmatrix} \\ &= (\alpha + \beta) \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + (\beta + \gamma) \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \end{aligned}$$

$$\text{Thus, } \vec{x} \in \text{span} \left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \right\}. \text{ This shows } U + W \subseteq \text{span} \left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \right\}.$$

Conversely, suppose $\vec{x} \in \text{span} \left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \right\}$. Then, there exists real number $a, b \in \mathbb{R}$ s.t.

$$\vec{x} = a \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + b \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$$

Note: $a \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \in \text{span} \left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \right\}$. Meanwhile,

$$b \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = 0 \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} + b \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \in \text{span} \left\{ \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \right\}$$

Thus, there exists vectors $\vec{u} \in U$ and $\vec{w} \in W$ namely $\vec{u} = a \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$ and $\vec{w} = b \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$ and

$\vec{w} = b \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$ s.t. $\vec{x} = \vec{u} + \vec{w}$. Thus, $\vec{x} \in u + w$. This shows

$$\text{span} \left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \right\} \subseteq U + W$$

We showed earlier that

$$U + W \subseteq \text{span} \left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \right\}$$

We conclude $U + W = \text{span} \left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \right\}$. □

More generally, one can show $\text{span}(S) + \text{span}(T) = \text{span}(S \cup T)$.

Let V be a vector space over \mathbb{F} . Let $S \subseteq V$ be any subset. Properties of $\text{span}(S)$:

- $\text{span}(S) \subseteq V$ is a subspace.
- $S \subseteq \text{span}(S)$.
- If W is a subspace of V and $S \subseteq W$, then $\text{span}(S) \subseteq W$.

Suppose v_1, \dots, v_n span V . (i.e., $\text{span}(v_1, \dots, v_n) = V$. Show $v_1, v_2 - v_1, v_3 - v_2, \dots, v_n - v_{n-1} = V$).

Notation: Let $w_i = v_i - v_{i-1}$ if $i > 1$ and $w_1 = v_1$.

Proof. We'll show $\forall i \text{span}(w_1, \dots, w_n)$ for $i = 1, \dots, n$. Use induction

- For $i = 1$, $v_1 = w_1 \in \text{span}(w_1, \dots, w_n)$.
- Suppose $v_k \in \text{span}(w_1, \dots, w_n)$ where $k < n$.
-

$$\begin{aligned} v_{k+1} &= v_{k+1} - v_k + v_k \\ &= w_{k+1} + v_k \end{aligned}$$

Since $w_{k+1} \in \text{span}(w_1, \dots, w_n)$ and $v_k \in \text{span}(w_1, \dots, w_n)$ and since $\text{span}(w_1, \dots, w_n) \subseteq V$ is a subspace, we have $v_{k+1} = w_{k+1} + v_k \in \text{span}(w_1, \dots, w_n)$. By induction, we get

$$v_1, \dots, v_n \in \text{span}(v_1, \dots, v_n) \subseteq \text{span}(w_1, \dots, w_n)$$

But $\text{span}(v_1, \dots, v_n) = V$. So, we have

$$V \subseteq \text{span}(w_1, \dots, w_n) \subseteq V$$

So $\text{span}(w_1, \dots, w_n) = V$. □

§16 | Dis 6: Oct 20, 2020

§16.1 Review of Linear Independence & Dependence

Let V be a vector space over \mathbb{F} . Recall $v_1, \dots, v_k \in V$ are linearly indep. if for any $\alpha_1, \dots, \alpha_k \in \mathbb{F}$ with $\sum_{i=1}^k \alpha_i v_i = 0$, we have $\alpha_i = 0$ for $i = 1, \dots, k$.

To show $v_1, \dots, v_k \in V$ are linearly indep:

Suppose we have $\alpha_1, \dots, \alpha_m \in \mathbb{F}$ with

$$\alpha_1 v_1 + \alpha_2 v_2 + \dots + \alpha_k v_k = 0$$

Try to show $\alpha_1 = 0, \alpha_2 = 0, \dots, \alpha_k = 0$.

Example 16.1

$$V = \mathbb{F}^3. \text{ Let } v_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, v_2 = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, v_3 = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}.$$

Claim 16.1. v_1, v_2, v_3 are linearly indep.

Proof. Let $\alpha, \beta, \gamma \in \mathbb{F}$ s.t.

$$\alpha v_1 + \beta v_2 + \gamma v_3 = \vec{0}$$

Then, we have

$$\alpha \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + \beta \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} + \gamma \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

So,

$$\begin{pmatrix} \alpha + \beta + \gamma \\ \beta + \gamma \\ \gamma \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

From this we see:

$$\alpha + \beta + \gamma = 0$$

$$\beta + \gamma = 0$$

$$\gamma = 0$$

Solve the above system, we have $\alpha = 0, \beta = 0, \gamma = 0$. Thus $\{v_1, v_2, v_3\}$ are linearly indep. \square

Example 16.2

Let V be a vector space over \mathbb{F} . Let $\vec{v}, \vec{w} \in V$. Set $\vec{x} = \vec{v} + \vec{w}$, $\vec{y} = \vec{v} - \vec{w}$, and $\vec{z} = 4\vec{v} + 2\vec{w}$.

Claim 16.2. $\{\vec{x}, \vec{y}, \vec{z}\}$ are linearly dep.

Proof. Observe $3\vec{x} + \vec{y} = \vec{z}$, so $3\vec{x} - \vec{y} - \vec{z} = \vec{0}$. This is a nontrivial linear combos. So, $\{\vec{x}, \vec{y}, \vec{z}\}$ are linearly dep. \square

Remark 16.3. More generally, any 3 vectors in $\text{span}(\vec{v}, \vec{w})$ are necessarily going to be linearly dep. But this requires proof!

V is a vector space over \mathbb{F} .

Claim 16.3. $\vec{v}, \vec{w} \in V$ are linearly dep $\iff \vec{v}$ is a multiple of \vec{w} or \vec{w} is a multiple of \vec{v} .

Proof. Suppose $\vec{v}, \vec{w} \in V$ are linearly dep. Then, $\exists \alpha, \beta \in \mathbb{F}$ not both 0 with $\alpha\vec{v} + \beta\vec{w} = \vec{0}$.

Case 1: $\alpha \neq 0$

Then we have $\alpha\vec{v} = -\beta\vec{w}$. Since $\alpha \neq 0$, we have $\alpha^{-1} \in \mathbb{F}^\times$. Then $\alpha^{-1}\alpha\vec{v} = \alpha^{-1}(-\beta\vec{w})$. So

$$\vec{v} = \underbrace{-\alpha^{-1}\beta}_{\in \mathbb{F}} \vec{w}$$

Thus, in this case, \vec{v} is a multiple of \vec{w} .

Case 2: $\alpha = 0$

In this case, $\beta \neq 0$ (since α, β are not both 0). Then $0\vec{v} + \beta\vec{w} = \vec{0}$. So, $\vec{0} + \beta\vec{w} = \vec{0}$ and thus $\beta\vec{w} = \vec{0}$. Then either $\beta = 0$ or $\vec{w} = \vec{0}$. But $\beta \neq 0$, so $\vec{w} = \vec{0} = 0 \cdot \vec{v}$. Hence, in this case, \vec{w} is a multiple of \vec{v} .

Conversely, suppose \vec{v} is a multiple of \vec{w} . Then there is an $\alpha \in \mathbb{F}$ with $\vec{v} = \alpha\vec{w}$. So,

$$1\vec{v} - \alpha\vec{w} = \vec{0}$$

The coefficient of \vec{v} is nonzero. Thus, this is a nontrivial linear combos of \vec{v} and \vec{w} which gives $\vec{0}$. Hence \vec{v} and \vec{w} are linearly dep. A similar argument works in the case where \vec{w} is a multiple of \vec{v} . \square

Example 16.4

$$f : \mathbb{R} \rightarrow \mathbb{R} \quad f(x) = \sin x$$

$$g : \mathbb{R} \rightarrow \mathbb{R} \quad g(x) = \cos x$$

$f, g \in C(\mathbb{R})$ where $C(\mathbb{R}) = \{h : \mathbb{R} \rightarrow \mathbb{R} | h \text{ is continuous}\}$, \mathbb{R} - vector space. Show f, g are linearly indep.

Proof. Suppose we have $\alpha, \beta \in \mathbb{R}$ with $\alpha f + \beta g = \underbrace{0}_{\text{zero function}} \in C(\mathbb{R})$. Then for any

$x \in \mathbb{R}$,

$$(\alpha f + \beta g)(x) = 0(x) = 0$$

So,

$$\alpha \sin(x) + \beta \cos(x) = 0$$

Plugging in $x = 0$, we see

$$\alpha \sin(0) + \beta \cos(0) = 0$$

so, $\beta = 0$. Plugging in $x = \frac{\pi}{2}$, we see

$$\alpha \sin\left(\frac{\pi}{2}\right) + \beta \cos\left(\frac{\pi}{2}\right) = 0$$

So, $\alpha = 0$. We have $\alpha = 0, \beta = 0$. Thus, f and g are linearly indep in $C(\mathbb{R})$, as desired. \square

Claim 16.4. $e^x, e^{4x} \in C(\mathbb{R})$ are linearly indep.

Proof. Suppose we have $\alpha, \beta \in \mathbb{R}$ with $\alpha e^x + \beta e^{4x} = 0 \in C(\mathbb{R})$. That is, for any $x \in \mathbb{R}$,

$$\alpha \cdot e^x + \beta \cdot e^{4x} = 0$$

Then for any real number x , we have

$$\beta = -\alpha e^x \cdot e^{-4x} = -\alpha e^{-3x}$$

For any $x \in \mathbb{R}$, we have $\beta = -\alpha e^{-3x}$ (but β is a constant).

- At $x = 1$, $\beta = \alpha e^{-3}$.
- At $x = 0$, $\beta = -\alpha$.

So $\alpha e^{-3} = -\alpha$, which gives

$$\alpha(1 - e^{-3}) = 0$$

Thus either $\alpha = 0$ or $e^{-3} = 1$. So $\alpha = 0$. Then $\beta = -\alpha = -0 = 0$. So $\alpha = 0, \beta = 0$, as desired. \square

V is a vector space over \mathbb{F} . True or false:

1. If $v_1, \dots, v_k \in V$ are linearly indep., and $\alpha \neq 0 \in \mathbb{F}$, then $\alpha v_1, \dots, \alpha v_k$ are also linearly indep. – **TRUE**
2. If $v_1, \dots, v_k \in V$ are linearly dep., and $\alpha \neq 0 \in \mathbb{F}$, then $\alpha v_1, \dots, \alpha v_k$ are also linearly indep. – **TRUE**
3. $v_1, \dots, v_k \in V$ are linearly indep., and $w \in V$, then $v_1 + w, v_2 + w, \dots, v_k + w$ are linearly indep. as well. – **FALSE**
4. $v_1, \dots, v_k \in V$ are linearly dep., and $w \in V$, then $v_1 + w, v_2 + w, \dots, v_k + w$ are linearly indep. as well. – **FALSE**

Claim 16.5. $v_1, \dots, v_k \in V$ are linearly indep., $\alpha \neq 0 \in \mathbb{F}$. Then $\alpha v_1, \dots, \alpha v_k \in V$ are also linearly indep.

Proof. Suppose we have $\beta_1, \dots, \beta_k \in \mathbb{F}$ with $\beta_1(\alpha v_1) + \beta_2(\alpha v_2) + \dots + \beta_k(\alpha v_k) = \vec{0}$. Then

$$(\beta_1 \alpha) v_1 + \dots + (\beta_k \alpha) v_k = 0$$

Since v_1, \dots, v_k are linearly indep., this gives

$$\beta_i \alpha = 0 \quad \text{for all } i = 1, \dots, k$$

So either $\beta_i = 0$ or $\alpha = 0$ for each $i = 1, \dots, k$. But, $\alpha \neq 0$. So $\beta_i = 0$ for each $i = 1, \dots, k$. Thus, $\alpha v_1, \dots, \alpha v_k$ are linearly indep. \square

Claim 16.6. Let $v_1, \dots, v_k \in V$ be linearly dep, $\alpha \neq 0 \in \mathbb{F}$. Then $\alpha v_1, \dots, \alpha v_k \in V$ are also linearly dep.

Proof. Suppose $\alpha v_1, \dots, \alpha v_k$ are actually linearly dep. Taking $\alpha^{-1} \neq 0 \in \mathbb{F}$ by previous claim, multiplying through by α^{-1} keeps the list linearly indep. Then, $v_1, \dots, v_k \in V$ are linearly indep. Contradiction! Thus, by contradiction, $\alpha v_1, \dots, \alpha v_k$ are also linearly dep. \square

Claim 16.7. $v_1, \dots, v_k \in V$ and $w \in V$. Then $v_1 + w, \dots, v_k + w$ maybe linearly dep. or linearly indep. depending on the choice of w .

Proof. Take $\vec{w} = -\vec{v}_1$. Then

$$\vec{v}_1 + \vec{w} = \vec{0}$$

Then

$$1(\vec{v}_1 + \vec{w}) + 0(\vec{v}_2 + \vec{w}) + \dots + 0(\vec{v}_k + \vec{w}) = \vec{0}$$

This gives a nontrivial linear combos. So not linearly indep. \square

Claim 16.8. $v_1, \dots, v_k \in V$ linearly dep., $\vec{w} \in V$. Then $\vec{v}_1 + \vec{w}, \dots, \vec{v}_k + \vec{w}$ maybe linearly dep. or indep. depending on the choice of $\vec{w} \in V$.

Proof. Left as exercise. (Actually for the choice of $\vec{w} \in \text{Span}(v_1, \dots, v_k)$ the proof is right below. \square

§17 | Dis 7: Oct 22, 2020

§17.1 Review of Linear Independence and Linear Transformation

Proof. Since $v_1 + w, \dots, v_k + w \in V$ are linearly dep., there exists scalars $a_1, \dots, a_k \in \mathbb{F}$, not all 0, s.t.

$$a_1(v_1 + w) + \dots + a_k(v_k + w) = 0$$

Then we have

$$\sum_{i=1}^k a_i v_i + \sum_{i=1}^k a_i w = 0$$

So,

$$-\left(\sum_{i=1}^k a_i\right) w = \sum_{i=1}^k a_i v_i$$

Let $\beta = -\sum_{i=1}^k a_i \in \mathbb{F}$. Then $\beta \vec{w} = \sum_{i=1}^k a_i \vec{v}_i$. Suppose $\beta = 0$. Then this would read

$$0 = \sum_{i=1}^k a_i \vec{v}_i$$

Since v_1, \dots, v_k are linear indep., this gives $\alpha_i = 0$ for all $i = 1, \dots, k$. Yet, we choose $\alpha_1, \dots, \alpha_k$ not all 0. Contradiction!

So $\beta \neq 0$. Hence,

$$\vec{w} = \beta^{-1} \sum_{i=1}^k a_i v_i = \sum_{i=1}^k (\beta^{-1} a_i) v_i$$

which in the span of v_1, \dots, v_k , as desired. \square

Corollary 17.1

$v_1, \dots, v_k \in V$ are linearly indep., $w \in V$, and $w \notin \text{span}(v_1, \dots, v_k)$. Then $v_1 + w, \dots, v_k + w$ are also linearly indep.

Claim 17.1. $v_1, \dots, v_k \in V$ are linearly indep., $w \in V$ and $w \notin \text{span}(v_1, \dots, v_k)$. Then v_1, \dots, v_k, w are linearly indep.

Proof. Suppose we have $a_1, \dots, a_{k+1} \in \mathbb{F}$ with

$$a_1 v_1 + \dots + a_k v_k + a_{k+1} w = 0$$

Case 1: $a_{k+1} = 0$.

Then, we have

$$a_1 v_1 + \dots + a_k v_k = 0$$

Since v_1, \dots, v_k are linearly indep., we have $a_1 = 0, \dots, a_k = 0$. Hence in this case, all coeffs are 0, as desired.

Case 2: $a_{k+1} \neq 0$

Then we have

$$-a_{k+1} w = a_1 v_1 + \dots + a_k v_k$$

Since $-a_{k+1} \neq 0$, it has a mult. inverse $\beta \in \mathbb{F}$. Then we have

$$\vec{w} = \beta a_1 v_1 + \dots + \beta a_k v_k \in \text{span}(v_1, \dots, v_k)$$

But $\vec{w} \notin \text{span}(v_1, \dots, v_k)$. So we have a contradiction. So a_{k+1} must be 0. By the previous case, $a_1 = 0, \dots, a_{k+1} = 0$. Thus, v_1, \dots, v_k, w are linearly indep., as desired. \square

Definition 17.2 ((6.1)) — (v_1, \dots, v_m) is a basis for V if

1. $v_1, \dots, v_m \in V$ are linearly indep.
2. $\text{span}(v_1, \dots, v_m) = V$.

Theorem 17.3

Every vector space has a basis.(potentially an infinite list of vectors)

Theorem 17.4

If (v_1, \dots, v_m) and (w_1, \dots, w_l) are both bases for V , then $l = m$.

Define $\dim V = \#$ of elements in any basis of V .

Proposition 17.5

Let V be a vector space with $\dim V = n$. Suppose v_1, \dots, v_n are linearly indep. Then, $\text{span}(v_1, \dots, v_n) = V$. So, v_1, \dots, v_n is a basis of V .

Proposition 17.6

Let V be a vector space with $\dim V = n$. Suppose $\text{span}(v_1, \dots, v_n) = V$. Then, v_1, \dots, v_n are linearly indep. So (v_1, \dots, v_n) is a basis of V .

Recall T is injective \iff whenever $T(x) = T(y)$ we have $x = y$. T is surjective \iff for all $\vec{w} \in W$, there is a $\vec{v} \in V$ s.t. $T(\vec{v}) = \vec{w}$.

From the perspective of list of vectors,

- $v_1, \dots, v_k \in V$ are linearly indep. in V , then $T(v_1), \dots, T(v_k)$ are also linearly indep in $W \iff T$ is injective.
- T is surjective \iff if $v_1, \dots, v_k \in V$ have $\text{span}(v_1, \dots, v_k) = V$, then $T(v_1), \dots, T(v_k) \in W$ satisfy $\text{span}(T(v_1), \dots, T(v_k)) = W$.
- T is bijective $\iff T$ is injective and surjective \iff if $v_1, \dots, v_k \in V$ are a basis of V , then $T(v_1), \dots, T(v_k) \in W$ are a basis of W .

From the perspective of subspace,

$$\ker(T) \subseteq V = \{v \in V : T(v) = 0\}$$

$$\text{im}(T) \subseteq W = \{T(\vec{v}) : \vec{v} \in V\}$$

- T is injective $\iff \ker T = \{0\}$.
- T is surjective $\iff \text{im}(T) = W$.
- T is bijective $\iff \ker T = \{0\}$ and $\text{im } T = W$.

§17.2 Hw2 # 1

Let $V \neq 0$ be a vector space over \mathbb{F} . Suppose V can be spanned by one vector, say $V = \text{span}(\vec{x})$ for some $\vec{x} \in V$. Let $W \subseteq V$ be a subspace. Then, either $W = \{0\}$ or $W = V$.

Proof. Let $W \subseteq V$ be a subspace of V , and suppose $W \neq \{0\}$. We want to show $W = V$. Let $\vec{w} \in W \setminus \{0\}$, i.e. $\vec{w} \in W, \vec{w} \neq 0$. Since $\vec{w} \in W$, we have $\text{span}(\vec{w}) \subseteq W$. Meanwhile, $\vec{w} \in W \subseteq V = \text{span}(\vec{x})$. So there is an $\alpha \in \mathbb{F}$ with $\vec{w} = \alpha\vec{x}$. If $\alpha = 0$, this would give $\vec{w} = \vec{0}$ but $\vec{w} \neq \vec{0}$. So we have $\alpha \neq 0$. But then $\alpha \in \mathbb{F}^\times$ has a mult. inv $\alpha^{-1} \in \mathbb{F}^\times$, so $\vec{x} = \alpha^{-1}\vec{w} \in \text{span}(\vec{w})$.

Thus, $\text{span}(\vec{x}) \subseteq \text{span}(\vec{w})$. So we have

$$V = \text{span}(\vec{x}) \subseteq \text{span}(\vec{w}) \subseteq W \subseteq V$$

So all containments must be equality. Thus, $W = V$.

Part 2: Suppose $V \neq 0$ has $V = \text{span}(\vec{v}, \vec{w})$ where $\vec{v}, \vec{w} \in V$ are linearly indep.

Claim 17.2. If $W \subseteq V$, then either $W = 0$, $W = V$, or $W = \text{span}(\vec{w})$ for some $\vec{w} \in V \setminus \{0\}$.

Setup: Let $W \subseteq V$ be a subspace with $W \neq 0$ and $W \neq V$. Consider nonzero vector $\vec{w}_1 \in W \setminus \{0\}$. Suppose $\text{span}(\vec{w}_1) \neq W$. Then, find some $\vec{w}_2 \in W \setminus \text{span}(\vec{w}_1)$. Argue

- \vec{w}_1, \vec{w}_2 are linearly indep.

- In fact, they span all of V .

Assume they don't, find $\vec{w}_3 \in V \setminus \text{span}(\vec{w}_1, \vec{w}_2)$

- $\vec{w}_1, \vec{w}_2, \vec{w}_3$ are linearly indep.

- Ch2, Thm 4: V cannot have a list of linearly indep. vectors with more than 2 elements. \square