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* 2^{nd} by *Hoffman and Kunze* for the class. Other course notes can be found through my blog site, `ductuanvu.wordpress.com/notes/`. Please contact me at ducvu2718@ucla.edu if you find any concerning mathematical errors/typos.

Contents

§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?

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

– at least algebraically?
There are two FUNCTIONS (or MAPS)

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

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

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

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

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

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

A2 $\exists$ an element $0 \in F \ni a + 0 = a = 0 + a$ Exitence 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 $\in F$ with $1 \neq 0 \ni a \cdot 1 = a = 1 \cdot a$ Existence of a One

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

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

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

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

<u>Comments</u>: 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

$$
\begin{aligned}
&\mathbb{Q} := \left\{\frac{a}{b} | a, b \in \mathbb{Z}, b \neq 0\right\} \\
&\mathbb{R} := \text{set of real no.} \\
&\mathbb{C} := \{a + bi | a, b \in \mathbb{R}\} \text{ with}
\end{aligned}
$$

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

$\forall a, b, c, d \in \mathbb{R}$
Under usual $+, \cdot$ of 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 <u>not</u> a field as $\nexists n \in \mathbb{Z} \ni 2n = 1$, so $\mathbb{Z}$ do not satisfy (M3).

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

§2 Lec 2: Oct 5, 2020

§2.1 Field(Cont'd)

<u>*Note*</u>: $\mathbb{Z}$ 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

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

[conjecture?]

3. Let F be a field

$$F[t] \coloneqq \{(\text{formal polynomial in one variable}\}$$

with t, given by

$$(a_0 + a_1 t + a_2 t^2 + \ldots) + (b_0 + b_1 t + b_2 t^2 + \ldots) \coloneqq (a_0 + a_1) + (a_1 + b_1)t + (a_2 + b_2)t^2 + \ldots$$
$$(a_0 + a_1 t + a_2 t^2 + \ldots) \cdot (b_0 + b_1 t + b_2 t^2 + \ldots) \coloneqq a_0 b_0 + (a_0 b_1 + a_1 b_0)t + \ldots$$

<u>*Note*</u>: $f, g \in F[t]$ 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 <u>not</u> a field but satisfy all axioms except (M3) but it does satisfy (M3') (compare $\mathbb{Z}$). Let

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

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

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

<u>*Note*</u>:the 0 in $F[t]$ is $\frac{0}{f}$, $\quad f \neq 0$, and 1 in $F[t]$ is $\frac{f}{f}$, $f \neq 0$.

4. let F be a field.

$$M_n F \coloneqq \{A | A \text{an} n \times n \text{matrix entries in} F\}$$

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

$$A_{ij} \coloneqq ij^{\text{th}} \text{ entry of A, etc}$$

Then

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

<u>*Note*</u>: $A = B$ iff $A_{ij} = B_{ij} \;\; \forall i, j$.

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

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

§2.2 Vector Space

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

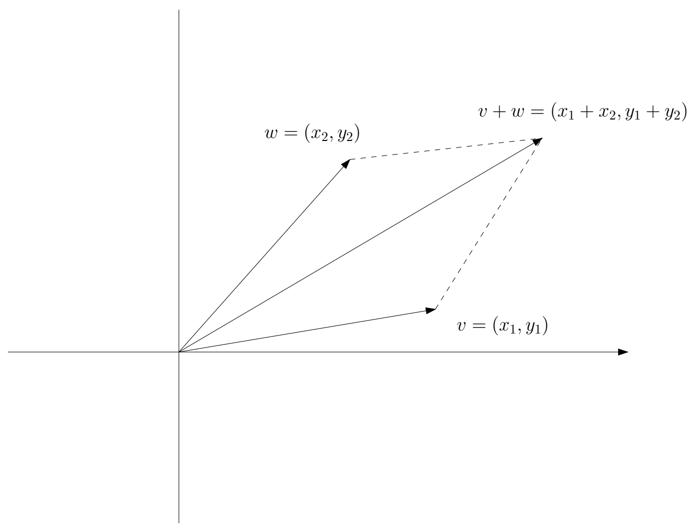


Figure 1: Geometry in $\mathbb{R}^2$

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

$$+ : V \times V \to V \qquad \cdot : F \times V \to V$$
$$\text{Addition} \qquad \text{Scalar Multiplication}$$
$$\text{write:} v + w := +(v, w) \qquad \text{write:} \alpha \cdot v := \cdot(\alpha, v) \text{ or } \alpha v$$

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 $0 \in V \ni \quad v + 0 = v = 0 + v$
3. (2) holds and the element $(-1)v$ in V satisfies

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

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

   $$\alpha v + w \quad \text{makes sense}$$
   $$v\alpha, vw \quad \text{do not make sense}$$

3. We usually write

   vector using Roman letter

   scalar using Greek letter

   exception things like $(x_1, \ldots, x_n) \in \mathbb{R}^n, x_i \in \mathbb{R} \forall i$
4. $+ : V \times V \to V$ says

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

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

5. $\cdot : F \times V \to V$ says $\alpha \in F, v \in V \to \alpha v \in V$. 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. $F^n := \{\alpha_1, \ldots, \alpha_n\} | \alpha_i \in F \forall i$ is a vector space over F under COMPONENT-WISE OPERATION and
$$0_{F^n} := (0, \ldots, 0)$$
Even have
$$F^\infty_{\text{finite}} = \{(\alpha_1, \ldots, \alpha_n, \ldots\} | \alpha_i \in F \forall i \text{ with only FINITELY MANY } \alpha_i \neq 0$$

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 fxn $I := \{f : I \to \mathbb{R} | f \text{ a fxn}\}$ called the SET of REAL VALUE FXNS on I.

   Define $+, \cdot$ as follows: $\forall f, g \in \text{Fxn } I$,
$$\begin{aligned} &f + g \quad \text{by } (f+g)(x) := f(x) + g(x) \\ &\alpha f \quad \text{by } (\alpha f)(x) := \alpha f(x) \quad \forall \alpha \in \mathbb{R} \end{aligned}$$
and 0 by $0(\alpha) = 0 \forall \alpha \in F$. Then 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. $F^n \coloneqq \{(\alpha_1, \dots, \alpha_n) | \alpha_i \in F \forall i\}$ is a vector space over F under COMPONENT-WISE OPERATIONS

$$(\alpha_1, \dots, \alpha_n) + (\beta_1, \dots, \beta_n) \coloneqq (\alpha_1 + \beta_1, \dots, \alpha_n + \beta_n)$$
$$\beta(\alpha_1, \dots, \alpha_n) \coloneqq (\beta\alpha_1, \dots., \beta\alpha_n)$$

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

Even have:

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

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 $I \coloneqq \{f : I \to \mathbb{R} | f \text{ a function}\}$

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

$$f + g \quad \text{by} \quad (f + g)(x) \coloneqq f(x) + g(x)$$
$$\alpha f \quad \text{by} \quad (\alpha f)(x) \coloneqq \alpha f(x) \quad \forall \alpha \in \mathbb{R}$$

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

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

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

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

$$\alpha(\alpha_0 + \alpha_1 t + \ldots + \alpha_n t^n) \coloneqq \alpha\alpha_0 + \alpha\alpha_1 t + \ldots + \alpha\alpha_n t^n$$

5. $\underbrace{F[t]_n}_{\text{truncating} F[t]} \coloneqq \{0 \in F[t]\} \cup \{f \in F[t] | \text{deg} f \leq n\}$ (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 $+$, scalr mult,0.

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

$$(A+B)_{ij} := A_{ij} + B_{ij} \in F \qquad \forall A, B \in F^{m\times n}$$
$$(\alpha A)_{ij} := \alpha A_{ij} \in F \qquad \forall \alpha \in F$$
$$0 = \begin{pmatrix} 0 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & 0 \end{pmatrix} \text{(m rows and n columns)}$$

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 $W := \{f : S \to V | f \text{ a map}\}$. Define $+, \cdot$ on W by

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

$\forall f, g \in W; \alpha \in F; s \in S$. 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 SCARLARS.

   i.e., $+ = +$ on K. With scalar mult, $F \times K \to K$ by

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

   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.

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

   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 $\forall \alpha, \beta \in F$, $\forall v, w \in V$, 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 — 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., $(V, +, \cdot)$ is a vector space over F, via $+ : V \times V \to V$ and $\cdot : F \times V \to V$ then W is a vector space over F via

- $+ = +/_{W \times W} : W \to W$: restrict the domain to $W \times W$
- $\cdot = \cdot|_{F \times W} : F \times W \to W$: 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

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) $\to$ 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) $\to$ 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 $\forall w' \in W$, the claim follows. The other axioms hold for elements of V hence for $W \subset V$.
2) $\to$ 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) $\to$ 2) Let $\alpha \in F$, $w_1, w_2 \in W$. As above and 3)

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

Therefore,

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

by 3). ☐

<u>*Note*</u>:Usually 3) is the easiest condition to check. WARNING: must subsets of a vector space over F are NOT subspaces.

Example 3.5

V a vector space over F.

1. $0 \coloneqq \{0_V\}$ and V are subspace of V
2. Let $I \subset \mathbb{R}$ be an interval (not a point) then
$$C^\omega(I) < C^\infty(I) < \ldots < C^n(I) < \ldots < C'(I)$$
$$< \text{Diff I} < C(I) < \text{Int I} < \text{Fxn I}$$
are subspaces of the vector space containing then. . . where we write
$$A < B \quad \text{if} \quad A \subset B \quad \text{and } A \neq B$$
3. Let F be afield, e.g $\mathbb{R}$. Then $F = F[t]_0 < F[t]_1 < \ldots < F[t_n] < \ldots < F[t]$ are vector space 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 subspace of V,then $W_1 \subset W_2$ is a subspaces.
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 $W \coloneqq \{(0, \alpha_1, \ldots, \alpha_n | \alpha_i \in F, \quad 2 \le i \le n\} \subset F^n$ is a subspace, but $\{(1, \alpha_2, \ldots, \alpha_n | \alpha_i \in F, \quad 2 \le i \le n\}$ is not. Why?
7. Every line or plane through the origin in $\mathbb{R}^3$ is a subspace.

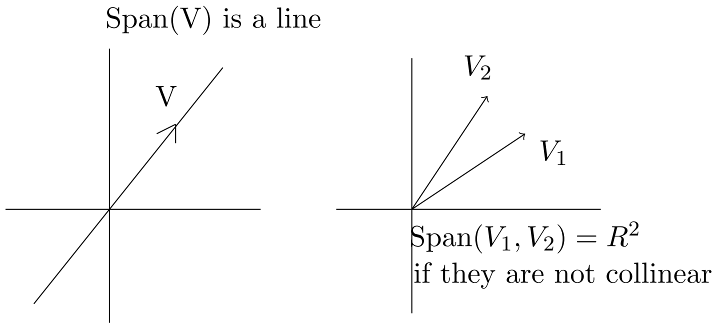
§4 Lec 4: Oct 9, 2020

§4.1 Span & Subspace

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

Let
$$\text{Span}(v_1, \ldots, v_n) \coloneqq \{\text{ all linear combos of} v_1, \ldots, v_n\}$$
Let $v_1, \ldots, v_n \in V$. Then
$$\text{Span}(v_1, \ldots, v_n) = \left\{ \sum_{i=1}^n \alpha_i v_i | \alpha_1, \ldots, \alpha_n \in F \right\}$$
is a subspace of V (by the Subspace Theorem) called the SPAN of $v_1, \ldots, v_n$. It is the (unique) smallest subsapce of V containing $v_1, \ldots, v_n$.

i.e., if $W \subset V$ is a subspace and $v_1, \ldots, v_n \in W$ then $\text{Span}(v_1, \ldots, v_n) \subset W$. We also let Span $\emptyset \coloneqq \{0_V\} = 0$, 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 $\mathbb{Q}$ is 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 — Let V be a vector space over $F, \emptyset \neq S \subset V$ a subset. Then, Span S := the set of all FINITE linear combos of vectors in S. i.e., if $V \in$ Span S, then

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

Span $S \subset V$ is a subspace. What is 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
$$\text{Symm}_n F := \left\{A \in M_n F | A = A^\top\right\}$$
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. $$V = \left\{\begin{pmatrix} a & c+di \\ c-di & b \end{pmatrix} | a, b, c, d \in \mathbb{R}\right\} \subset M_2 C$$
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 $V \subsetneq M_2\mathbb{R}$. $V \subset M_2\mathbb{C}$ is a subspace as a vector space over $\mathbb{R}$.

4. (Important computational example) Fix $A \in F^{m\times n}$. Let
$$\ker A := \left\{x \in F^{n\times 1} | Ax = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \text{ in } F^{m\times 1}\right\}$$
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 $W_i \subset V_i, i \in \underbrace{I}_{\text{indexing set}}$ be subspaces. Then $\bigcap_I W = \bigcap_{i\in I} W_i := \{x \in V | x \in W_i \quad \forall i \in I\}$ 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., Span(i) $\cup$ Span(j) $= \{(x, 0) | x \in \mathbb{R}\} \cup \{(0, y) | y \in \mathbb{R}\}$ is not a subspace
$$(x, y) = (x, 0) + (0, y) \notin \quad \text{Span(i)} \cup \text{Span(j)}$$
if $x \neq 0$ and $y \neq 0$

Definition 4.4 — Let $W_1, W_2 \subset V$ be subspaces. Define

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

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

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

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

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 $v_1, \ldots, v_n$ in $\mathbb{R}^n$

Suppose $v_i = (a_{i_1}, \ldots, a_{ni}, i = 1, \ldots, n$. To determine when $w \in \mathbb{R}^n$ lies in $\operatorname{Span}(u_1, \ldots, u_n$) i.e., if $w = (b_1, \ldots, b_n) \in \mathbb{R}^n$ when does

$$w = \alpha_1 v_1 + \ldots + \alpha_n v_n, \qquad \alpha_1, \ldots, \alpha_n \in \mathbb{R}$$

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

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

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 $v_1 \ldots, v_n \in V$, some n with following properties

1. $V = \text{Span}(v_1, \ldots, v_n\ )$
2. No v_i is a linear combos of $v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_n$ (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 $v_1, \ldots, v_n$ are distinct. Then (2) is equivalent to

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

i.e. the "coordinates" are unique.

Proof. (-¿)If not, relabelling the $v_i's$, we may assume that $\alpha_1 \neq \beta_2$ 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

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

a contradiction.
(¡-) Relabelling, we may assume that

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

Then,

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

so $1 = 0$, a contradiction. □

Remark 4.6. The case $n = 1$ is special because there are two possibilities
Case 1: $v \neq 0$: then $\alpha v = \beta v \to \alpha = \beta$
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 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

§5.1 Sets

- $\mathbb{N}$ = set of natural numbers $= \{1, 2, 3, 4, \ldots\}$
- $\mathbb{Z}$ = set of integers $= \{\ldots, -2, -1, 0, 1, 2, \ldots\}$
- $\mathbb{Q}$ = set of rational numbers $= \left\{\frac{a}{b} : a, b \in \mathbb{Z},\ b \neq 0\right\}$
- $\mathbb{R}$ = 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 – $\emptyset$.

§5.2 Functions

What is a set?

– A collection of elements

Example 5.1
- $A = \{\text{cat, dog}\}$
- $B = \{1, 2, 3\}$
- $C = \mathbb{R}^2$

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 thing.

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

Example 5.2

- $f : \mathbb{R} \mapsto \mathbb{R}$ 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 differemt 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 5.3 — 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 5.4

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,

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

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 $T(a, b) = (c, d)$

$$\begin{aligned} a + b &= c \\ a - b &= d \\ a &= \frac{c + d}{2} \\ b &= \frac{c - d}{2} \end{aligned}$$

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 □

§6 Dis 2: Oct 6, 2020

§6.1 Field

Definition 6.1 — 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 6.1. 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 $0\alpha = 0\alpha + 0\alpha$. Substract 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 6.2. 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 6.2

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

Example 6.3

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

Clock arithmetic. Addition is clock addition:

$$2 + 11 = 1$$

Multiplication is "clock mult"

$$2 \cdot 11 = 10$$

Multiply and add like normal but then substract nultiples 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 ... $\implies$ NO!

Or <u>different argument</u>:

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

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 6.4
$\mathbb{Z}/3\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}\}$

- additive id: 0
- mult id: 1

Mult inv:

$$\begin{aligned} 1 \cdot 1 &= 1 \\ 2 \cdot 2 &= 1 \checkmark \end{aligned}$$

Additive inverse:

$$\begin{aligned} 0 + 0 &= 0 \\ 1 + 2 &= 0 \checkmark \end{aligned}$$

$\mathbb{Z}/3\mathbb{Z}$ 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.
$\mathbb{Z}/p\mathbb{Z}$ <u>is</u> a field for p prime. Proof uses Bezat lemma (Eucledian algorithm)

Example 6.5

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

Everything has a mult.inverse

§7 Dis 3: Oct 8, 2020

§7.1 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 $j < k$

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

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

Claim 7.1. 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?

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

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 11^{th} ... but $|F|=10$ contradiction ☐

<u>*Note*</u>: 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 7.2. 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. ☐

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 $1+1+1+1+1=0$? 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. $\square$