Tutorial 3: Linear maps, null space, range, rank-nullity theorem

(The "pf"s are sketchy. You should NOT write like this in exam.)

Linear maps (Throughout, all v.s. are over a same field $\mathbb{F}$.)

Def 3.1. (linear maps)

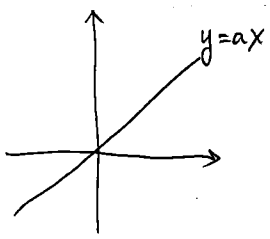
A (set theoretic) map $T: V \to W$ between two vector spaces V, W is <u>linear</u> if

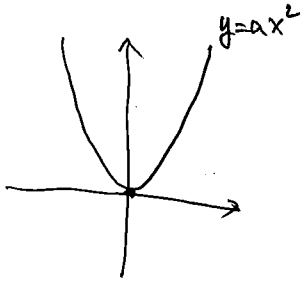
(i) $T(v_1+v_2) = Tv_1 + Tv_2$. the first $+_V$ is addition in V, the second is $+_W$ in W.

(ii) $T(av) = a(Tv)$ $\quad a \in \mathbb{F}$.

Remark. (i) In general, a map between algebraic (vector space) structures is a set map that preserve the structure. (linear)

(ii) $x \longmapsto y = ax$ is linear $\qquad$ $x \longmapsto y = ax^2$ is not linear





Eg. Differentiation and integration are linear maps.

Take $\mathbb{F}=\mathbb{R}$. $V = C(\mathbb{R})$ = space of all continuous functions $[0,1] \to \mathbb{R}$.

"Pf". (i) $(f_1+f_2)' = f_1' + f_2'$ $\quad$ so $'$ is linear from $C(\mathbb{R})$ to $C(\mathbb{R})$.

$(af_1)' = af_1'$

(ii) $\int_0^1 f_1+f_2 = \int_0^1 f_1 + \int_0^1 f_2$

$\int_0^1 af = a\int_0^1 f$ $\quad$ so $\int_0^1$ is linear from $C(\mathbb{R})$ to $C(\mathbb{R})$ □.

Eg. Matrix transpose is linear map.

Over $\mathbb{F}$ arbitrary, take $V = M_n(\mathbb{F})$. $^t: M_n(\mathbb{F}) \to M_n(\mathbb{F})$ is linear.

"pf". $(A+B)^t = A^t + B^t$.

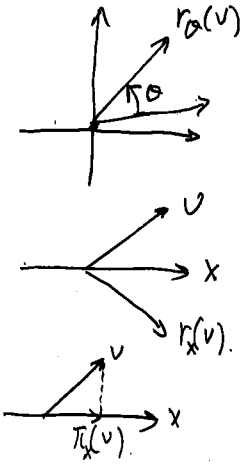
$(aA)^t = aA^t$. □.

Eg. Linear map may not look linear: find a linear map $\mathbb{R} \to \mathbb{R}_{>0}$ over $\mathbb{R}$?

$C_x: \mathbb{R} \to \mathbb{R}$, $a \mapsto a+t$ translation is NOT linear. Why?

Eg. Rotation, reflection, projection are all linear.

Take $\mathbb{F}=\mathbb{R}$, $V=\mathbb{R}^2$.



Rotation by θ: $\begin{pmatrix} v_1 \\ v_2 \end{pmatrix} \xrightarrow{r_\theta} \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \end{pmatrix}$.

Reflection about x-axis: $\begin{pmatrix} v_1 \\ v_2 \end{pmatrix} \xrightarrow{r_x} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \end{pmatrix}$

Projection onto x-axis: $\begin{pmatrix} v_1 \\ v_2 \end{pmatrix} \xrightarrow{\pi_x} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \end{pmatrix}$

"pf." This is a special case of the below example. □

Eg. Left-multiplication by a matrix is linear.

Over any $\mathbb{F}$, $V=\mathbb{F}^n$. Let $A \in M_n(\mathbb{F})$. Define the left-multiplication map

$$\begin{aligned} L_A : \mathbb{F}^n &\to \mathbb{F}^n \\ v &\longmapsto Av \end{aligned}$$

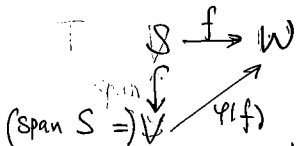
This is a linear map.

"pf." $A(v_1+v_2) = Av_1 + Av_2$.

$A(av_1) = a(Av_1)$. □

Remark. Every linear map between finite dimensional v.s. is actually of this form, called matrix representation. We will study that later.

Linear maps and basis



Upshot: Every linear map is determined by its value on a basis!

This makes our life easier. To be precise, we state this in the

Proposition 3.2. Let V be a vector space with basis $S=\{e_i\}_{i\in I} \subseteq V$. Let W be another v.s. Then

$$\underset{\text{linear maps}}{\mathrm{Hom}_{\mathbb{F}}(V,W)} \cong \underset{\text{set bijection}}{\mathrm{Map}_{\mathrm{Set}}(S,W)}$$

($\cong$: set bijection; $\mathrm{Map}_{\mathrm{Set}}(S,W)$: set maps/functions.)

"pf." Define $\varphi: \mathrm{Map}_{\mathrm{Set}}(S,W) \to \mathrm{Hom}_{\mathbb{F}}(V,W)$ called extend by linearity

$$f \longmapsto \varphi(f) : V$$

where $\varphi(f)(v) = \varphi(f)\left(\sum_{\text{finite}} a_i e_i\right) \overset{3.2}{=} \sum_{\text{finite}} a_i f(e_i)$, $v = \sum_{\text{finite}} a_i e_i$

This is well-defined as $\{a_i, i\in I\}$ are unique by property of basis.

For injectivity, $\varphi(f_1)=\varphi(f_2) \Rightarrow \varphi(f_1)\big|_S = \varphi(f_2)\big|_S \Rightarrow f_1=f_2$.

For surjectivity, take $g\in \mathrm{Hom}_{\mathbb{F}}(V,W)$, define $f(e_i):=g(e_i)$, $e_i\in S$, so $f\in \mathrm{Map}_{\mathrm{Set}}(S,W)$.

Then $g=\varphi(f)$. □

Remark. Whenever you want to do something for linear maps, it suffices to do it on a basis, and extend by linearity.

Eg. $\mathrm{Hom}_{\mathbb{F}}(V,W)=\{$all linear maps between two v.s. $V, W\}$ is again a vector space.

"pf:" $(f_1+f_2)(v):= f_1(v)+f_2(v)$.

$((f_1+f_2)(av):= f_1(av)+f_2(av) = a(f_1(v)+f_2(v))$

$\Rightarrow f_1+f_2 \in \mathrm{Hom}_{\mathbb{F}}(V,W)$.

$(af_1)(v) = a\cdot f(v)$.

$(af)(bv) = a\cdot f(bv) = abf(v)$

$\Rightarrow af_1 \in \mathrm{Hom}_{\mathbb{F}}(V,W)$.

($0(v):=0_W$ is also linear $\Rightarrow 0\in \mathrm{Hom}_{\mathbb{F}}(V,W)$.) "Checking" axioms are omitted. □

Eg. Matrix multiplication: composition of linear maps are linear. $U\xrightarrow{T}V\xrightarrow{S}W$

For $T\in \mathrm{Hom}_{\mathbb{F}}(U,V)$, $S\in \mathrm{Hom}_{\mathbb{F}}(V,W)$ we have $S\circ T\in \mathrm{Hom}_{\mathbb{F}}(U,W)$.

As compositions are not commutative, even for $U=V=W$, $T\circ S \neq S\circ T$ in general.

Upshot: This is the reason why matrix multiplication is not commutative.

Rank-nullity theorem (/First isomorphism theorem if you take 2070)

* Thm3.3: For a linear map $T: V\to W$. We have.

(i) $V=\ker T \oplus V/\ker T$ ← quotient space.

(ii) $V/\ker T \cong \mathrm{range}(T)$ (isomorphism = linear + bijection)

not examinable.

basis for V:	v_1 v_2 ($\ker T$)	$v_3, \cdots, v_n$.
basis for V/W:		$v_3+\ker T, \cdots, v_n+\ker T$.
basis for range T:		$T(v_3), \cdots, T(v_n)$.

As a result, $\dim V = \dim \ker T + \dim \mathrm{range}\, T$ if $\dim V<\infty$.

For this to make sense, we need to define quotient space.

This page is Not examinable

Def. 3.4 (quotient vector space).

For a v.s. V and a subspace $W \subseteq V$. We define the quotient vector space by

$$V/W := \{ v+W \mid v \in V \}, \text{ where } v+W := \{ v+w \mid w \in W \}$$ called cosets

[Note: $v+W = w+W$ iff $v-w \in W$]

addition: $(v_1+W)+(v_2+W) := (v_1+v_2)+W$.

scalar multiplication: $a(v+W) := av+W$.

You may verify this is also a vector space.

Problem: $\oplus$ does not make sense unless we realize V/W as a subspace of V.

Proposition 3.5. Any basis $\mathcal{E}_1$ of W ($\subseteq V$) can be extended to $\mathcal{E}_1 \cup \mathcal{E}_2$ of V. We have.

$$\overline{\mathcal{E}_2} = \{ v+W \mid v \in \mathcal{E}_2 \}$$

is a basis of V/W.

pf. Exercise. □

Proposition 3.6. If $\mathcal{E}_1$ is a basis of W, and $\overline{\mathcal{E}_2} = \{ v+W \mid v \in \mathcal{E}_2 \subseteq V \} \subseteq V/W$ is a basis of V/W.

Then $\mathcal{E}_1 \cup \mathcal{E}_2$ is a basis of V.

pf. Exercise. □

(Cor 3.7.) We can find a vector subspace $W' = \operatorname{span} \mathcal{E}_2$ of V with

(i) $W' \cong V/W$ ← span $\overline{\mathcal{E}_2}$.

(ii) $V = W \oplus W'$ ← span $\mathcal{E}_2$ / span $\mathcal{E}_1$.

By the above extension of basis technique. (So V/W can be viewed as a subspace of V if we do not distinguish W' and V/W as above.)

This finishes the proof of (i) in Thm 3.3.

For (ii), define a map,

$$V/\ker T \longrightarrow \text{range}(T)$$

$$v+\ker T \longmapsto T(v)$$

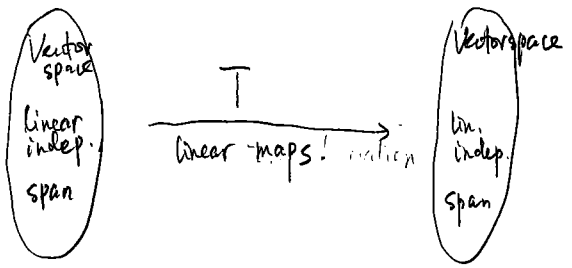
This is well-defined as if $v-w \in \ker T$, $T(v) = T(v-w+w) = T(v-w)+T(w) = T(w)$.

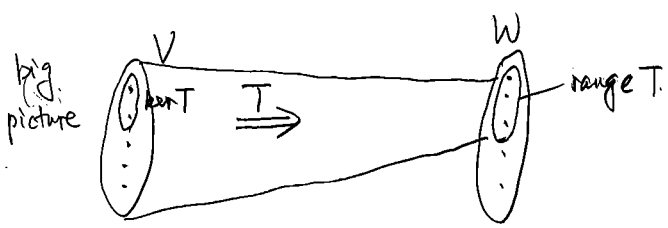
This is injective as $T(v) = T(w) \Rightarrow T(v-w) = 0 \Rightarrow v-w \in \ker T \Rightarrow v+w+\ker T = 0+\ker T$ in $V/\ker T$.

This is surjective by definition of range. □ 3.3.

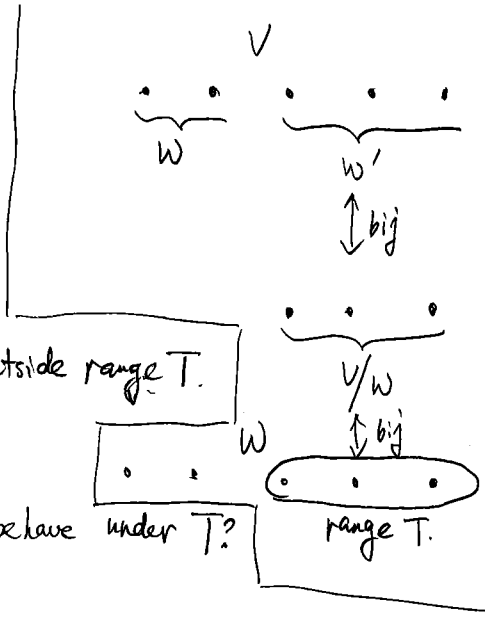
This page in inside syllabus.

Linear maps & lin. indep/span





dots means basis.



Note that we get no control on what is outside range T.
We may WLOG replace W by range T.

Q: How do linear indep. sets / spanning sets behave under T?

Ans: Summarized in following !

Prop 3.8. Let $V \xrightarrow{T} W$ be the linear maps between two vector spaces V, W.

Let $S \subseteq V$ be a subset.

(i) If T injective, then $T(S)$ lin indep $\Rightarrow$ S linearly independent in V. (actually $\Leftrightarrow$ HW2)

(ii) If T surjective, then S spanning set $\Rightarrow$ $T(S)$ is spanning set of W.

"pf". (i). Let $S' \subseteq S$ by any finite subset. Then $T(S') \subseteq T(S)$ is a finite subset of a linearly independent set, hence linearly independent. Now for $s_i \in S'$, $a_i \in \mathbb{F}$,

$$\sum_{i=1}^n a_i s_i = 0 \Rightarrow T\left(\sum_{i=1}^n a_i s_i\right) = T(0) = 0. \Rightarrow \sum_{i=1}^n a_i T(s_i) = 0 \overset{T(S') \text{ lin.indep.}}{\Longrightarrow} a_i = 0 \text{ for all } i = 1, \dots, n.$$

As T is inj, $T(s_i)$ are distinct in $T(S)$.

This is true for every finite subsets S'. By def, S is lin. indep.

(ii). For any $w \in W$, $\exists v \in V$ s.t. $T(v) = w$ as T surjective. As $\operatorname{span} S = V$, we have $v = \sum_{i=1}^n a_i s_i$ for some $a_i \in \mathbb{F}$, $s_i \in S$. But then

$$w = T(v) = T\left(\sum_{i=1}^n a_i s_i\right) = \sum_{i=1}^n a_i T(s_i) \subseteq \operatorname{span} T(S).$$

□

Remark. (i) This is actually "abstract non-sense". Trivially true but very useful for writting proofs.

(ii). Notice the "duality" between lin indep. V.S. span again!

The first "duality" is

lin indep
span

For $S' \subseteq S$. S lin. indep $\Rightarrow$ S' lin. indep.
S' spanning $\Rightarrow$ S spanning.

(iii) If T is bijective, both are iff (HW2). (c.f. Q1 of Tutorial 2).

This page is inside syllabus

Pf of prop 3.5-3.6. Let $\langle W \subseteq V$ with $\mathcal{E}_1$ basis of W, extend to a basis $\mathcal{E}_1 \cup \mathcal{E}_2$ of V. Let $W' = \operatorname{span} \mathcal{E}_2$.
Obviously $V = W \oplus W'$. We wish to show $W' \cong V/W$ by basis maps $\mathcal{E}_2 \longmapsto \bar{\mathcal{E}}_2$.
Consider the natural quotient map $V \xrightarrow{T} V/W$ T is obviously linear and surjective.
$v \longmapsto \bar{v} = v + W$.

By prop 3.8, one direction for spanning set is automatic!

It remains to show

(i). $\mathcal{E}_2$ is lin. indep. $\Leftrightarrow T(\mathcal{E}_2) = \bar{\mathcal{E}}_2$ is linearly indep.

(ii). $T(\mathcal{E}_2) = \bar{\mathcal{E}}_2$ spans $V/W \Rightarrow \mathcal{E}_2$ spans W'.

Indeed, for (i), ($\Rightarrow$): $\sum a_i \bar{v}_i \overset{(v_i \in \mathcal{E}_2)}{=} \bar{0} \Rightarrow \sum a_i (v_i + W) = 0 + W \Rightarrow \left(\sum a_i v_i\right) + W = 0 + W \Rightarrow \sum a_i v_i \in W \Rightarrow \sum a_i v_i = \sum b_j w_j$ $w_j \in \mathcal{E}_1$.
As $\mathcal{E}_1 \cup \mathcal{E}_2$ are lin. indep. $\Rightarrow a_i = b_j = 0 \ \forall i, j$. ($v_i \notin \operatorname{span}\{\mathcal{E}_1 \cup \{v_j\}\}$.)
($\Leftarrow$). $\sum a_i v_i = 0 \Rightarrow \sum a_i (v_i + W) = 0 + W \Rightarrow \sum a_i \bar{v}_i = 0$ ($v_i \in \mathcal{E}_2$) and $\bar{v}_i \neq \bar{v}_j$ as $v_i - v_j \notin W$. As $\bar{v}_i \in \bar{\mathcal{E}}_2$ distinct, lin. indep. $a_i = 0 \ \forall i$.

for (ii), for $w' \in W' = \operatorname{span} \mathcal{E}_2$. As $\bar{\mathcal{E}}_2$ spans V/W.
$\bar{w}' = \sum a_i \bar{v}_i$ for some $v_i \in \mathcal{E}_2, a_i \in \mathbb{F}$. $\Leftrightarrow w' - \sum a_i v_i \in W$. But $w' - \sum a_i v_i \in W'$ and $W \cap W' = \{0\}$.

$\Rightarrow w' - \sum a_i v_i = 0$. $\Rightarrow W' \subseteq \operatorname{span} \mathcal{E}_2$. $\square$.

Remark. (i) You may see prop 3.8 simplifies half of the proof!

(ii) The "abstract nonsense" like prop 3.8 and (ii) of 3.3 are studied systematically in a subject called category theory.

(iii) This concludes the proof of rank-nullity.

(iv). By prop 3.8 (i), range(T) measures "How many linearly independent variables T preserved."
$\ker(T)$ measures "How much T fails to measure linear independence."
For vector spaces, "dim $\ker T$ + dim range T = total size of linearly independent set in V = dim V."

Warning: If V is not finite dimensional, we need to assume (AoC) (Axiom of choice.) in order to show every linearly independent set can be extended to a basis.

This page is non-examinable.

Def. Partially ordered set (poset) is a set P with a order $\leq$ s.t.

(i) $a \leq a$

(ii) $a \leq b$, $b \leq a \Rightarrow a = b$.

(iii). $a \leq b$, $b \leq c$, $c \leq a$

$\leq$ is called totally ordered if any two elements are comparible, i.e., either $a \leq b$ or $b \leq a$ for $\forall a, b$.

Axiom: (Zorn's Lemma) Let P be a poset.

If Any chain/totally ordered set P has an upper bound in P, then the set P has a maximal element.

Remark. This is equivalent to Axiom of choice (AOC).

Prop. Every lin. indep. can be extended to a basis of V. (Every vector space has a basis.)

pf. Let $S \subseteq V$ be lin. indep. Consider

$$\mathcal{A} = \{ T \subseteq V : S \subseteq T,\ T \text{ is lin. indep} \}.$$

Every chain in $\mathcal{A}$ has an upper bound. (take union).

Then by Zorn's lemma, $\mathcal{A}$ has a maximal element R.

We claim $\langle R \rangle = V$

Suppose $\langle R \rangle \subsetneq V$, then $\exists v \in V \quad v \notin \langle R \rangle$.

Then $R \subsetneq R \cup \{v\} \in \mathcal{A}$. contradiction of maximality of R.

so we must have $\langle R \rangle = V$, and R is a basis.

This proves every vector space has a basis.

HW1. Feedback.

$W \leq V$.

Q1.3.31 (a). If $v+W$ is a subspace of V, then $v \in W$.

Attempt: As $v = v+0 \in v+W$. and W is a subspace.

$-v \in v+W$.

So $-2v \in W$.

As W is a subspace.

$(\frac{1}{2}) \cdot (-2v) = v \in W$.

This is false proof if $F = F_2 = \{0, 1\}$. Here,

$2 = 0$. so no notion of $-\frac{1}{2}$ in F_2!

(b). What would you do to prove $A = B$ two sets equal?

$A \subseteq B$: $\forall a \in A$, $\exists b \in B$ s.t. $a = b$.

$B \subseteq A$: $\forall b \in B$, $\exists a \in A$ s.t. $a = b$.

Q1.3.11. $W = \{ f \in P(F) \mid f(x) = 0$ or $f(x)$ has degree $n \} \leq P(F)$ for $n \geq 1$?

What is the degree of a polynomial?

Eg. $7x^2y^3 + x^5 + 7$ is of degree 5

degree 5, deg 5, deg 0.

If $f = \sum_{i=1}^{n} f_i$ where f_i are monomials.

$\deg f = \max\{ \deg f_i \}$ convention: degree of constant function is 0.

where degree of a monomial is the sum of powers of all indeterminates.

$f = f_1 + f_2 + f_3$

$7x^2y^3 \quad x^5 \quad 7$.

$\deg f_1 = 2+3 = 5$, $\deg f_2 = 5$, $\deg f_3 = 0$.

$\deg f = \max\{5, 5, 0\} = 5$.

Q1.3.26. What is the difference between $+$ and $\oplus$?

Def. Let $U_1, \cdots, U_m \subseteq V$ subspaces.

The <u>direct sum</u> $U_1 \oplus \cdots \oplus U_m$ is the <u>sum</u> $U_1 + \cdots + U_m$ AND

$u_1 + \cdots + u_m = 0$ $u_i \in U_i \Rightarrow u_i = 0$ for all $i = 1, \cdots, n$.

Prop. Let $U_1, U_2 \leq V$ subspaces. Then U_1+U_2 is a direct sum iff $U_1 \cap U_2 = \{0\}$.

Warning: This is NOT true for $n>2$, i.e., it will NOT be sufficient to check.

$U_i \cap U_j = \{0\}$ for all pair of (i,j) with $i \neq j$.

Ex: $\mathbb{F}^3$ as v.s over $\mathbb{F}$.

$U_1 := \{(x,y,0) \in \mathbb{F}^3 : x,y \in \mathbb{F}\}$.

$U_2 := \{(0,0,z) \in \mathbb{F}^3, z \in \mathbb{F}\}$.

$U_3 := \{(0,y,y) \in \mathbb{F}^3 : y \in \mathbb{F}\}$.

Note that $U_1 \cap U_2 = \{0\}$, $U_2 \cap U_3 = \{0\}$, and $U_1 \cap U_3 = \{0\}$.

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

$(0,1,0) \in U_1$, $(0,0,1) \in U_2$, $(0,-1,-1) \in U_3$

Direct sum and direct product

① If $U_1, U_2 \leq V$ subspace, with $U_1 \cap U_2 = \{0\}$, then $U_1 \oplus U_2$ is the direct sum.

- $U_1 \oplus U_2 = \{u_1+u_2 \mid u_1 \in U_1, u_2 \in U_2\}$ as sets.
- $+ : (U_1 \oplus U_2) \times (U_1 \oplus U_2) \longrightarrow U_1 \oplus U_2$

  $((a_1+b_1), a_2+b_2) \longmapsto \underbrace{(a_1+a_2)}_{U_1} + \underbrace{(b_1+b_2)}_{U_2}$.
- $* : \mathbb{F} \times (U_1 \oplus U_2) \longmapsto U_1 \oplus U_2$

  $a * (a_1+b_1) \longmapsto \underbrace{(aa_1)}_{U_1} + \underbrace{(ab_1)}_{U_2}$.

② For any two vector spaces V_1, V_2, not necessarily subspace of another vector space, we can form a direct product / cartesian product $V_1 \times V_2$:

- $V_1 \times V_2 = \{(a,b) \mid a \in V_1, b \in V_2\}$ as sets.
- $+ : (V_1 \times V_2) \times (V_1 \times V_2) \longmapsto V_1 \times V_2$

  $((a_1,b_1), (a_2,b_2)) \longmapsto (\underbrace{(a_1+b_1)}_{V_1}, \underbrace{(a_2+b_2)}_{V_2})$.
- $* : \mathbb{F} \times (V_1 \times V_2) \longmapsto V_1 \times V_2$

  $a * (a_1,b_1) \longmapsto (\underbrace{aa_1}_{V_1}, \underbrace{ab_1}_{V_2})$

③ As $U_1, U_2 \leq V$ with $U_1 \cap U_2 = \{0\}$, then $U_1 \oplus U_2 \cong U_1 \times U_2$

pf. We define a linear map $T: U_1 \oplus U_2 \to U_1 \times U_2$ by

$$\sum_{i=1}^{n}(a_i+b_i) \longmapsto \left(\sum_{i=1}^{n} a_i, \sum_{i=1}^{n} b_i\right).$$

$a_i \in U_1,\ b_i \in U_2$

This is well-defined as $\sum_{i=1}^{n}(a_i+b_i) = \sum_{j=1}^{m}(a_j'+b_j') \Rightarrow \underbrace{\sum_{i=1}^{n} a_i - \sum_{j=1}^{m} a_j'}_{\in U_1} = \underbrace{\sum_{j=1}^{m} b_j' - \sum_{i=1}^{n} b_i}_{\in U_2} \subseteq U_1 \cap U_2 = \{0\}$.

Hence $\sum_{i=1}^{n} a_i = \sum_{j=1}^{m} a_j'$ and $\sum_{j=1}^{m} b_j' = \sum_{i=1}^{n} b_i$.

T is injective as $\left(\sum_{i=1}^{n} a_i, \sum_{i=1}^{n} b_i\right) = (0,0) \Rightarrow \sum_{i=1}^{n} a_i = 0$ and $\sum_{i=1}^{n} b_i = 0. \Rightarrow \sum_{i=1}^{n}(a_i+b_i) = 0.$

T is surjective by definition of $U_1 \times U_2$. □

Remark. We also say $\oplus$ we defined in ① is <u>internal</u> direct sum as U_1 and U_2 are subspaces of another vector space.

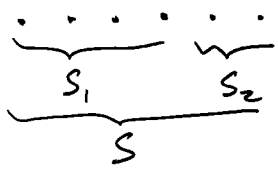
× we defined in ② is <u>external</u> direct sum as there is no such restriction.

Because of ③ we see internal direct sum is just a special case of direct product. In some literature, × is also denoted as $\oplus$.

Fact of life: $\{0\}$ is not a linearly independent set as $a \cdot 0 = 0 \not\Rightarrow a = 0$.

<u>Direct sum, sum and basis</u> Throughout, Let V be a vector space and $S \subseteq V$ be a <u>linearly independent</u> set.

Fact: Suppose $S = S_1 \amalg S_2$. Then $\langle S \rangle = \langle S_1 \rangle \oplus \langle S_2 \rangle$, with S, S_1, S_2 being basis of respective vector space.



pf. We use prop. at the top of P3-9.

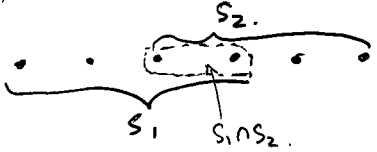
$\langle S_1 \rangle + \langle S_2 \rangle \subseteq \langle S \rangle$ is obvious, as $\langle S_1 \rangle + \langle S_2 \rangle$ is the smallest vector space containing $\langle S_1 \rangle$ and $\langle S_2 \rangle$.

$\langle S \rangle \subseteq \langle S_1 \rangle + \langle S_2 \rangle$ is also clear, as elements of $\langle S \rangle$ are of the form $\sum a_i s_i$ $s_i \in S$.

But $S = S_1 \amalg S_2$, $\sum a_i s_i = \sum a_i s_i' + \sum a_i s_i''$ where $s_i' \in S_1$, $s_i'' \in S_2$.

As the union is disjoint, $\langle S_1 \rangle \cap \langle S_2 \rangle = 0$, otherwise $\sum a_i s_i = \sum b_j s_j'$ $s_i \in S_1, s_j' \in S_2$ gives $\sum a_i s_i - \sum b_j s_j' = 0$ a non-trivial linear combination of elements in S. $\not\Rightarrow$ S is lin. indep. □

Fact. $\langle S_1 \cup S_2 \rangle = \langle S_1 \rangle + \langle S_2 \rangle$; $\langle S_1 \cap S_2 \rangle = \langle S_1 \rangle \cap \langle S_2 \rangle$ ... (Rmk we assume S is lin. indep).



pf. Exercise.

Remark. (The set of all subspaces, $\cap$, $+$) form a bounded modular lattice. (see page 13).

The "zero element" in a vector space may not be 0.

Ex: $(\mathcal{P}(X), \triangle)$ is a v.s. over $\mathbb{F}_2$. Its zero element is ϕ.

Ex: $(\mathbb{R}_{>0}, \cdot)$ is a v.s. over $\mathbb{R}$.

$$+ : \mathbb{R}_{>0} \times \mathbb{R}_{>0} \longrightarrow \mathbb{R}_{>0}$$
$$(x, y) \longmapsto xy$$

$$* : \mathbb{R} \times \mathbb{R}_{>0} \longrightarrow \mathbb{R}_{>0}$$
$$(z, x) \longmapsto x^z = e^{z \ln x}.$$

Its zero element is 1.

If V is infinite dimensional, $\dim V$ is not defined. $\infty - \infty$ is not defined!

$M_n(\mathbb{F}) \neq \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix}$ ← an element.
↑ a set.

$$M_n(\mathbb{F}) = \left\{ \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} : a_{ij} \in \mathbb{F} \right\}.$$

Q: What is a basis for $M_n(\mathbb{F})$?

A: $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \longleftrightarrow \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix}$.

$$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} + \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} = \begin{pmatrix} a_1+a_2 & b_1+b_2 \\ c_1+c_2 & d_1+d_2 \end{pmatrix} \qquad \begin{pmatrix} a_1 \\ b_1 \\ c_1 \\ d_1 \end{pmatrix} + \begin{pmatrix} a_2 \\ b_2 \\ c_2 \\ d_2 \end{pmatrix} = \begin{pmatrix} a_1+a_2 \\ b_1+b_2 \\ c_1+c_2 \\ d_1+d_2 \end{pmatrix}.$$

$$r \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} ra & rb \\ rc & rd \end{pmatrix} \qquad r \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = \begin{pmatrix} ra \\ rb \\ rc \\ rd \end{pmatrix}.$$

so we have $M_n(\mathbb{F}) \cong \mathbb{F}^{n^2}$ as vector spaces.

$\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \cdots \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \cdots \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$ is a basis for $\mathbb{F}^{n^2}$, so $\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & \cdots & & 0 \\ \vdots & & & \vdots \\ 0 & \cdots & & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & & 0 \\ \vdots & & & & \vdots \\ 0 & \cdots & & & 0 \end{pmatrix} \cdots \begin{pmatrix} 0 & 0 & \cdots & 0 \\ \vdots & & & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$

is a basis for $M_n(\mathbb{F})$.

Q. $M_n(\mathbb{F}) \overset{\varphi}{\cong} \mathbb{F}^{n^2}$, then why do we care about $M_n(\mathbb{F})$? $\mathbb{F}^{n^2}$ seems more convenient?

A: We see addition is not dependent on positions of entries, as they are defined entriwise. But multiplication does!

$$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}\begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} = \begin{pmatrix} a_1a_2+b_1c_2 & a_1b_2+b_1d_2 \\ c_1a_2+d_1c_2 & c_1b_2+d_1d_2 \end{pmatrix} \xrightarrow{\varphi} \begin{pmatrix} a_1a_2+b_1c_2 \\ a_1b_2+b_1d_2 \\ c_1a_2+d_1c_2 \\ c_1b_2+d_1d_2 \end{pmatrix}$$

But this is not our usual definition for $\mathbb{F}^{n^2}$:

$$\begin{pmatrix} a_1 \\ b_1 \\ c_1 \\ d_1 \end{pmatrix} \times \begin{pmatrix} a_2 \\ b_2 \\ c_2 \\ d_2 \end{pmatrix} = \begin{pmatrix} a_1a_2 \\ b_1b_2 \\ c_1c_2 \\ d_1d_2 \end{pmatrix}$$ ← different!

Also, $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} e \\ f \end{pmatrix}$ can be defined, but $\begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix}\begin{pmatrix} e \\ f \end{pmatrix}$ is not usually defined!

So the correct way to view a matrix is not through vector spaces, but Linear maps! In particular, $M_n(\mathbb{F})$ represent $\mathrm{Hom}_{\mathbb{F}}(\mathbb{F}^n, \mathbb{F}^n)$.

That is why we have matrix multiplication and matrix-vector multiplication.

matrix multiplication ↔ $T_1 \circ T_2 : V_1 \xrightarrow{T_2} V_2 \xrightarrow{T_1} V_3$

matrix-vector multiplication ↔ $V_1 \xrightarrow{T} V_2$, $T(v_1) \in V_2$, $v_1 \in V_1$.

Note that the collection of linear maps is also a vector space, indeed,

$$M_n(\mathbb{F}) \cong \mathbb{F}^{n^2} \cong \mathrm{Hom}_{\mathbb{F}}(\mathbb{F}^n, \mathbb{F}^n)$$

as vector spaces over $\mathbb{F}$.

But unlike $\mathbb{F}^{n^2}$ (not a ring), $M_n(\mathbb{F}) \cong \mathrm{Hom}_{\mathbb{F}}(\mathbb{F}^n, \mathbb{F}^n)$ as rings (if you took 2070).

Homework. Prove or give a counterexample:

For a linear map $T: V \to W$, $S \subseteq V$ a subset.

$T(S)$ is a linearly independant set $\Rightarrow$ S is linearly independent set.

out of syllabus

Lattice of subspace. Let V be a v.s. / $\mathbb{F}$.

Let $\mathcal{S} = \{\text{subspaces of } V\}$.

Then $(\mathcal{S}, +, \cap)$ form a bounded modular lattice.

Def. (lattice). A partially ordered set $(\mathcal{L}, \leq)$ is a lattice if

(i). $\forall a, b \in \mathcal{L}$, $\exists\, c \in \mathcal{L}$ that is • $a \leq c$, $b \leq c$ (upper bound).

• $\forall\, d \in \mathcal{L}$ with $a \leq d$, $b \leq d$, we have $c \leq d$ (Least).

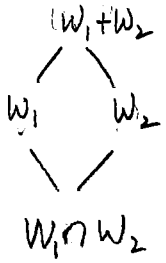
denote such c as $a \vee b$ called join or least upper bound. (Note that c is automatically unique)

(ii) $\forall a, b \in \mathcal{L}$, $\exists\, c' \in \mathcal{L}$ that is • $c' \leq a$, $c' \leq b$ (lower bound)

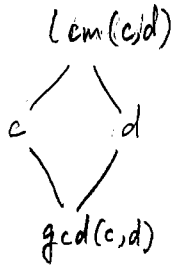
• $\forall\, d' \in \mathcal{L}$ with $d' \leq a$ and $d' \leq b$, we have $d' \leq c'$ (greatest).

denote such c' as $a \wedge b$ called meet or greatest lower bound. (c' is also unique).

Eg.



$(\mathcal{S}, \leq)$.



$(\mathbb{Z}_+, |)$

↑ divisible.

Def. (bounded, modular).

A lattice $(\mathcal{L}, \leq, \wedge, \vee)$ is

(i) bounded if it has greatest element and least element. (they are essentially unique),

(ii) modular if $\forall a, b, x \in \mathcal{L}$, $a \leq b \Rightarrow a \vee (x \wedge b) = (a \vee x) \wedge b$.

Eg. $(\mathcal{S}, \leq)$ is bounded as V is the greatest element and $\{0\}$ is the least element.

modular as $W_1 + (W_2 \cap W_3) = (W_1 + W_2) \cap W_3$ if $W_1 \leq W_3$. (Ex).

$(\mathbb{Z}_+, |)$ is not bounded as it has no greatest element.

is not modular as $\text{lcm}(3, \gcd(2,4)) = 6 \neq 2 = \gcd(\text{lcm}(3,2), 4)$ (Ex)