MATH 3140 Notes

Contents

1 Class 1

1.1 Fields

Definition 1.1. (Field): A field F is a set with two binary operations

$$+ : F \times F \to F, \ (x, y) \mapsto x + y$$

$$\cdot : F \times F \to F, \ (x, y) \mapsto x \cdot y$$

that satisfy these properties:

- (A0) existence of additive identity or neutral element: there is $0 \in F$ such that $x + 0 = x$ for all $x \in F$
- (A1) additive commutativity: for all $x, y \in F$, $x + y = y + x$
- (A2) additive associativity: for all $x, y, z \in F$, $x + (y + z) = (x + y) + z$
- (A3) existence of additive inverse: for all $x \in F$ there is y such that $x + y = 0$
- (M0) existence of multiplicative identity or neutral element: there is $1 \in F, 1 \neq 0$ such that $x \cdot 1 = 1 \cdot x = x$ for all x
- (M1) multiplicative commutativity: for all $x, y \in F$, $x \cdot y = y \cdot x$
- (M2) multiplicative associativity: for all $x, y, z \in F$, $x \cdot (y \cdot z) = (x \cdot y) \cdot z$
- (M3) existence of multiplicative inverse: for all $x \in F, x \neq 0$ there is y such that $x \cdot y = 1$
- (D) distributivity: for all $x, y, z \in F$, $(x + y) \cdot z = x \cdot z + y \cdot z$

Remark. $\{0\}$ is not a field because we require that the multiplicative identity be distinct from 0. If we allowed $0 = 1$, then F is the trivial field, i.e., $F = \{0\}$.

Remark. The smallest field is $F_2 = \{0, 1\}$ with addition and multiplication defined as:

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

Remark. If $(F, +, \cdot)$ is a field, then $0 \cdot x = 0$ for all x.

Proof. Proof

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

Adding the additive inverse of $0 \cdot z$ to both sides, we get

$$0 = 0 \cdot z$$

✓

Remark. The additive and multiplicative inverses are unique.

Proof. Let $x \in F$, suppose y, z are both additive inverses of x.

$$\begin{aligned} y &= y \\ y &= y + 0 \\ y &= y + (x + z) \\ y &= (y + x) + z \\ y &= z \end{aligned}$$

✓

Remark. Since the additive and multiplicative inverses are unique, we denote the additive inverse and multiplicative inverse of x respectively as $-x$ and x^{-1}.

Definition 1.2. (Group): A set G with a binary operation $*$ is a group if it has

- existence of inverse
- existence of identity
- associativity

Remark. Note that commutativity is not required. A group with commutativity is known as a **commutative group**.

Definition 1.3. (Field): $(F, +, \cdot)$ is a field if

- $(F, +)$ is a commutative group
- $(F \setminus \{0\}, \cdot)$ is a commutative group
- distributive properties hold

2 Class 2

2.1 Vector Spaces

Definition 2.1. (Vecotr Space): A vector space over a field F, denoted V, is a set with two operations

- $+ : V \times V \to V, (u, v) \mapsto u + v$
- $\cdot : V \times V \to V, (u, v) \mapsto u \cdot v$

Such that

- (V): $(V, +)$ is a commutative group
- (SM1): $a \cdot (v + w) = a \cdot v + a \cdot w$ for all $a \in F, v, w \in V$
- (SM2): $(a + b) \cdot v = a \cdot v + b \cdot v$ for all $a, b \in F, v \in V$
- (SM3): $(a \cdot b) \cdot v = a \cdot (b \cdot v)$ for all $a, b \in F, v \in V$
- (SM4): $1 \cdot v = v$ for all $v \in V$

Remark. If V is a vector space, we refer to elements of V as vectors. As a corollary to the above axioms, we have the following properties:

- $0 \cdot v = \mathbf{0}$ for $0 \in F$, all $v \in V$
- $a \cdot \mathbf{0} = \mathbf{0}$ for all $a \in F$
- The additive inverse of v is unique and denoted $-v$
- Subtraction is defined as $v - w := v + (-w)$ for all $v, w \in V$
- For all $v \in V$, $(-1) \cdot v = -v$
  - Proof: $\mathbf{0} = 0 \cdot v = (1 + (-1)) \cdot v = v + (-1) \cdot v$

2.2 Subspaces

Definition 2.2. (Subspace): Let $(V, +)$ be a vector space over F, a subset $U \subseteq V$ is a subspace if U is a vector space, denoted

$$U \leq V$$

Remark. If $W \leq V$, $0_W = 0_V$.

Proof.

$$\begin{aligned} 0_W &= 0_W + 0_V \\ &= 0_W + 0_V + (-0_W) \\ &= 0_V \end{aligned}$$

✓

3 Class 3

3.1 Subspaces, cont'd

Proposition 3.1. (Subspace Test): Let V be a vector space over F, $W \subseteq V$, then $W \leq V$ if and only if

1. W is non-empty
2. W is closed under addition
3. W is closed under scalar multiplication

Proof. ($\implies$): If $W \leq V$, then $0_V \in W$ hence $W \neq \emptyset$. 2 and 3 are true so that $+$ and $\cdot$ are well defined.

($\impliedby$): Assume $1, 2, 3$, take $w \in W$ arbitrary. By 3, $-1 \cdot w = -w \in W$. By 2, $-w + w = 0 \in W$.

By 2 and 3, $+$ and $\cdot$ are well defined in W. All other properties are true because they are true in V. ✓

3.2 Intersections of subspaces and spans

Theorem 3.2. (Intersection of subspaces): Let $\{w_i\}_{i \in I}$ be a collection of subspaces in V. Then

$$W = \bigcap_{i \in I} W_i$$

is a subspace of V. *The intersection of arbitrarily many subspaces of V is a subspace of V*

Proof.

1. Since $0 \in w_i$ for all i, $0 \in W$
2. Take $u, v \in W$ arbitrary

$$\begin{aligned} u, v \in W &\implies u, v \in W_i \text{ for all } i \\ &\implies u + v \in W_i \text{ for all } i \\ &\implies u + v \in W \end{aligned}$$

3. Take $u \in W$, $a \in F$ arbitrary,

$$\begin{aligned} u \in W &\implies u \in W_i \text{ for all } i \\ &\implies au \in W_i \text{ for all } i \\ &\implies au \in W \end{aligned}$$

✓

Definition 3.3. (Span): Let V be a vector space over F, $S \subseteq V$, the span of S is defined by

$$< S >= \bigcap_{S \subseteq W \leq V} W$$

The span of a set S is the intersection of all subspaces in V containing the set S

Remark.

- by intersection of subspaces theorem, the span is a subspace, $< S > \leq V$,
- when $< S >= V$, S is called a generating set for V
- If there exists $S \subseteq V$, $< S >= V$, and S is finite, then V is finitely generated
- $< S >$ is also denoted $span(S)$

Definition 3.4. (Linear Combination): Let S be a subset of V, a vector space over F. A linear combination of elements of S is an element $v \in V$ that can be written as

$$v = \sum_{i=1}^{k} a_i s_i$$

for some $s_i \in S, a_i \in F, k \in \mathbb{N}$
A linear combination of elements of S is a finite sum of elements of S

Theorem 3.5. (Span and Linear Combination): Let V be a subspace over F and S a subset of V, $S \neq \emptyset$, then

$$< S >= span(S) = \{\sum_{i=1}^{k} a_i s_i : a_i \in F, s_i \in S, k \in \mathbb{N}\}$$

Proof. Let $L = \{\sum_{i=1}^k a_i s_i : a_i \in F, s_i \in S, k \in \mathbb{N}\}$. We want to show that $L =< S >$

$(L \subseteq < S >)$:

$S \subseteq < S >$ by definition. Since S is closed under addition and scalar multiplication, and $\sum a_i s_i \in < S >$. Hence $L \subseteq < S >$.

$(< S > \subseteq L)$:

We show that L is a subspace that contains S. Since $< S >$ is the intersection of all subspaces that contain S, $< S >$ is a subset of L.

$S \subseteq L$ since for any $s \in S$, $s = 1 \cdot s \in L$.

We then show that L is a subspace.

- Existence of 0: take all $a_i = 0$ in $\sum a_i s_i$,
- Closure under addition: for any $\sum_{i=1}^k a_i s_i, \sum_{i=1}^l b_i t_i \in L$, their sum is still a linear combination of S
- Closure under scalar multiplication

$$a\left(\sum_{i=1}^k b_i s_i\right) = \sum_{i=1}^k (ab_i)s_i$$

Hence

$$< S >= \bigcap_{S \subseteq W \leq V} W \subseteq L$$

✓

3.3 Sums of subspaces

Definition 3.6. (Sum of subspace): Let W_i be a set where each W_i is a subspace of V for all $i \in I$
The sum of W_i is defined as

$$\sum_{i \in I} W_i =< \bigcup_{i=I} W_i >$$

The sum of W_i is the span of the union of W_i. The sum of W_i is the set of all linear combinations of elements in the union of W_i.

Proposition 3.7. (Sum of subspaces as finite sums): Let $W_i \leq V$ for all $i \in I$, then $w \in \sum_{i=I} W_i \Leftrightarrow$ there exists a finite subset $J \subseteq I$ and $w_i \in W_i$ so that

$$w = \sum_{i \in J} w_i$$

The subspace spanned by $\bigcup_{i \in I} W_i$ is the set of finite sums of elements of W_i.

Remark. The union of subspaces is not necessarily a subspace.

$$span(e_1) \cup span(e_2) = \text{ union of two lines } \rightarrow \text{ not a subspace}$$

However,

$$span(span(e_1) \cup span(e_2)) \leq V$$

Proof. Define

$$W = \{w \in V \text{ s.t. } w = \sum_{i \in J} W_i \text{ for } J \subseteq I, J \text{ finite}\}$$

WTS $W = \sum_{i \in J} W_i =< \bigcup_{i \in I} W_i >$

Claim 1 W is a subspace of V

Claim 2 $\bigcup_{i \in I} W_i$ is a subset of W

Claim 3 $W \subset span\left(\bigcup_{i \in I} W_i\right)$ because any $w \in W$ is a linear combination of elements of $\bigcup_{i \in I} W_i$

Hence

$$\bigcup_{i \in I} W_i \subseteq W \subseteq span\left(\bigcup_{i \in I} W_i\right)$$

Also span $\left(\bigcup_{i\in I} W_i\right)$ is the smallest subset containing $\bigcup_{i\in I} W_i$, hence

$$span\left(\bigcup_{i\in I} W_i\right) \subseteq W$$

Hence

$$W = span\left(\bigcup_{i\in I} W_i\right)$$

✓

4 Class 4

4.1 Direct Sums and Complements

Definition 4.1. (Direct Sum): Let V be a vector space over F, $W_1, W_2 \leq V$ is the direct sum of W_1 and W_2 if

- $V = W_1 + W_2$
- $W_1 \cap W_2 = \{0\}$

denoted

$$V = W_1 \bigoplus W_2$$

Proposition 4.2. (Direct sum and unique representation): Let V be a vector space over F and W_1 and W_2 be subspaces of V. V is the direct sum of W_1 and W_2 if and only if every element of V can be uniquely written as

$$v = w_1 + w_2$$

for some $w_1 \in W_1, w_2 \in W_2$

Proof. ($\implies$): for any $v \in V$, there is $w_1 \in W_1, w_2 \in W_2$ such that $v = w_1 + w_2$, by definition of direct sum.

To show that this is unique, assume

$$\begin{aligned} v = w_1 + w_2 = w_1' + w_2', w_1, w_1' \in W_1, w_2, w_2' \in W_2 \\ \implies w_1 - w_1' = w_2 - w_2' \end{aligned}$$

Since

$$\begin{aligned} w_1 - w_1' \in W_1, w_2 - w_2' \in W_2 \\ w_1 - w_1' = w_2 - w_2' \in W_1 \cap W_2 = \{0\} \end{aligned}$$

Hence $w_1 = w_1', w_2 = w_2'$

($\impliedby$): Since every $v \in V$ can be written $v = w_1 + w_2 \in W_1 + W_2$, $V = W_1 + W_2$.
To show that the intersubsection is trivial, take $w \in W_1 \cap W_2$,

$$\begin{aligned} w &= w + 0 \quad w \in W_1, 0 \in W_2 \\ &= 0 + w \quad 0 \in W_1, w \in W_2 \end{aligned}$$

If $w \neq 0$, there would be multiple ways to write w as the sum of elements of W_1, W_2, hence w has to be 0 and the intersubsection is trivia. ✓

Definition 4.3. (Complement): Let V be a vector space over F, $W \leq V$. A subspace $X \leq V$ is said to be the **Complement** of W if

$$V = W \bigoplus X$$

Remark. Complements are **not** unique. For example, $V = \mathbb{R}^2, W_1 = span(e_1)$, there are multiple choices of complements, such as $span(e_2), span(e_3)$.

Theorem 4.4. (Existence of Complement): Let V be a finitely generated vector space over F. Given any subspace $W \leq V$, we can find a complement in V.

Proof. Since V is finitely generated, there exists a finite set $S \subseteq V$ that spans V

$$S := \{s_1, s_2, \dots s_k\} \text{ such that } V = span(S)$$

A subspace $X \leq V$ such that $V = W \bigoplus X$ can be constructed recursively.
Consider s_1

- Case 1: $s_1 \in W$: $X_1 := \{0\}$
- Case 2: $s_1 \notin W$: $X_1 := span(s_1)$

We claim that in either case, $X_1 \bigcap W = \{0\}$ and $s_1 \in W + X_1$. Note that

- $s_1 \in W + X_1$ is true by construction
- for $X_1 \cap W = \{0\}$,
  - case 1: this is trivially true
  - case 2: say $v \in W \cap X_1$, then $v = as_1$ for some a, then either $a = 0$ or $a^{-1}v = s_1 \in W$, which is a contradiction. Hence $v = 0$

Consider s_2:

- Case 1: $s_2 \in W$: $X_2 := X_1$
- Case 2: $s_2 \notin W$: $X_2 := X_1 + span(s_2)$

We claim that in either case, $X_2 \bigcap W = \{0\}$ and $s_2 \in W + X_2$. Note that

- $s_2 \in W + X_2$ is true by construction
- for $X_2 \cap W = \{0\}$,
  - case 1: this is trivially true
  - case 2: say $v \in W \cap X_2$, then $v = x_1 + as_2$ for some a, then either $a = 0$ or $as_2 = v - x_1 \in W \implies s_2 = a^{-1}(w - x_1) \in W + X_1$, which is a contradiction. Hence $v = 0$

With this method of construction, we find subspaces $X_1 \dots X_k$,

$$X_1 \subseteq X_2 \dots \subseteq X_k$$

such that

$$\{s_1, \dots s_k\} \in W + X_k, W \cap X_k = \{0\}$$

Hence

$$\begin{aligned} span(s_1, \dots s_k) &\subseteq W + X_k \\ V &\subseteq W + X_k \\ V &= W \bigoplus X_k \end{aligned}$$

Note that $W + X_k \subseteq V$ naturally because we are working with subspaces of V. ✓

4.2 Basis and dimension

Definition 4.5. (Linear Independence, finite case): Let V be a vector space over F, $S = \{s_1, \dots s_n\} \subseteq V$. S is said to be linearly independent if

$$a_1 s_1 + a_2 s_2 \dots a_n s_n = 0 \implies a_1 = a_2 = \dots a_n = 0$$

Remark. $S = \{s_1, s_2, \dots s_n\}$ is linearly dependent if it is not linearly independent.

Definition 4.6. (Linear Independence, infinite case): $S \subseteq V$ is linearly dependent if every finite subset of S is linearly independent.

Remark. By convention, $\emptyset$ is linearly independent, and

$$span\,(\emptyset) = \{0\}$$

Since $\{0\}$ is the smallest subspace that contains $\emptyset$.

Lemma 4.7. Let V be a vector space over F, then

1. $S \subseteq V, 0 \in S$ then S is linearly dependent.
2. $\{v\} \subseteq V$ is linearly dependent if and only if $v = 0$
3. For $n \geq 2$ distinct vectors $\{s_1, s_2, \dots s_n\}$, the list of vectors is linearly dependent if and only if there is some s_i that is a linear combination of the others.

Proof.

1. Proof: $1 \cdot 0 = 0$, there are infinitely many non-trivial representations of 0.
2. Proof:
   - $(\impliedby)$ true by (1)
   - $(\implies)$ take some non-trivial representation of 0, i.e. $av = 0, a \neq 0$, multiply by multiplicative inverse, $a^{-1}av = a^{-1}0 \implies v = 0$
3. Proof:
   - $(\impliedby)$ This direction is immediate.
   - $(\implies)$ By linear dependence, there is a non-trivial representation of 0. I.e. there exists $a_1, \dots a_n \in F$, not all 0 such that

     $$a_1 s_1 + \dots + a_n s_n = 0$$

     WLOG, say $a_k \neq 0$, rewriting,

     $$a_k s_k = -\sum_{i=1, i\neq k}^{n} a_i s_i \implies s_k = -\frac{1}{a_k} \sum_{i=1, i\neq k}^{n} a_i s_i$$

✓

✓

Lemma 4.8. Let V be a vector space over F, $S \subseteq V$, finite. The following are equivalent

1. S is linearly independent
2. Every element of $span(S)$ can be uniquely represented as a linear combination of elements of S.

Proof. (1) $\implies$ (2): Take $v \in span(S)$ and assume $v = \sum_{i=1}^{k} a_i s_i = \sum_{i=1}^{k} b_i s_i$, then

$$\sum_{i=1}^{k} (a_i - b_i) s_i = 0$$
$$\implies a_i - b_i = 0 \text{ for all } i, \text{ by linear independence of } s_i$$
$$\implies a_i = b_i \text{ for all } i$$

(2) $\implies$ (1): Take $a_1, a_2, \ldots a_n \in F$, so that $a_1 s_1 + \ldots + a_n s_n = 0$. Since the trivial representation is **a** representation of 0, and representations are unique, the trivial representation is the only representation. Hence $a_1 = a_2 \ldots = a_n = 0$. ✓

5 Class 5

5.1 Basis, cont'd

Definition 5.1. (Basis): Let V be a vector space over F. A subset $S \subseteq V$ is a **basis** if

1. $span(S) = V$
2. S is linearly independent.

Example. 1. $\{(1,0),(0,1)\}$ and $\{(1,1),(1,-1)\}$ are basis for $\mathbb{R}^2$

2. $\{e_1, e_2, \dots e_n\}$ are a basis for F^n
3. The subspace of all polynomial functions over F, $\mathcal{P} = \{P : F \to F : P(x) = a_0 + a_1x + a_2x^2 \dots, F \subseteq \mathbb{C}\}$ has basis
$$S = \{x^n : n \in \mathbb{Z}_{\geq 0}\} = \{1, x, x^2 \dots\}$$

Lemma 5.2. Let S be a linearly independent subset of V. Suppose $v \in V, v \notin span(S)$, then $\bar{S} = S \cup \{v\}$ is also linearly independent.

Proof. Take $\{s_1, \dots s_k\} \subseteq S$ and $a_1, \dots a_k, b$ such that
$$a_1s_1 + \dots a_ks_k + bv = 0$$
Note that $b = 0$. Assume otherwise for contradiction, then
$$bv = -a_1s_1 - a_2s_2 \dots - a_ks_k$$
$$v = -\frac{a_1}{b}s_1 - \dots - \frac{a_k}{b}s_k \in span(S)$$
Since $b = 0$,
$$a_1s_1 + \dots + a_ks_k = 0$$
$$a_1 = \dots = a_n = 0 \quad \text{by linear independence of } s_1, \dots s_n$$
Hence $\bar{S}$ is linearly independent.

✓

Theorem 5.3. (Basis): Let V be a finitely generated vector space over F, and $S \subseteq V$. The following are equivalent

1. S is a basis of V
2. S is a minimal system of generators for V
3. Every element of V can be uniquely written as a linear combination of elemenets of S
4. S is a maximal linearly independent subset of V.

Proof. (1) $\implies$ (2): WTS S being a basis implies S is a minimal spanning set.

Since S is finite, we can write $S = \{s_1, \dots s_k\}$. Since S is a basis, $span(S) = V$. Take $s \in S$ arbitrary. Let $S' = S \setminus \{s\}$. Since S is linearly independent, $s \notin span(S')$. Hence we have found an element of V that is not in $span(S')$

(2) $\implies$ (3): WTS S being a minimal spanning set implies unique representation.

Assume S is a minimal set of generators for V. Take $a_i \in F, b_i \in F$ such that
$$\sum_{i=1}^{k} a_is_i = \sum_{i=i}^{k} b_is_i$$
Assume for contradiction that there is some $i \leq j \leq k$ such that $a_j \neq b_j$. Then,
$$(a_j - b_j)s_j = \sum_{i=1, i\neq j}^{k} (b_i - a_i)s_i$$
$$\implies s_j = \sum_{i=1, i\neq j}^{k} \frac{b_i - a_i}{a_j - b_j}s_i \quad \text{since } (a_j - b_j) \neq 0$$
And we have found an element of S that is a lienar combination of other elements of S.
$$S' := S \setminus \{s_j\} \subset S, span(S') = V$$
This contradicts the minimality of S. Hence $a_i = b_i$ for all i.

(3) $\implies$ (4) WTS unique representation implies maximal linear independence.

Since $0 \cdot S_1 + 0 \cdot S_2 + \ldots + 0 \cdot S_k = 0$, and representations are unique,

$$a_1 s_1 + a_2 s_2 + \ldots + a_k s_k \implies a_1 = a_2 = \ldots = 0$$

Hence S is linearly independent.

To show S is maximally linearly independent, take any $v \in V \setminus S$. By hypothesis, (assuming (3))

$$v = a_1 s_1 + a_2 s_2 + \ldots + a_k s_k$$

Hence,

$$a_1 s_1 + a_2 s_2 + \ldots + a_k s_k - v = 0$$

,
Therefore, $S \cup \{v\}$ is not linearly independent.

(4) $\implies$ (1). WTS that maximal linear independence implies S is a basis.

It suffices to show that $span(S) = V$. Assume towards a contradiction otherwise, then $span(S) \neq V, \exists v \in V \setminus span(S)$. By lemma,

$$\bar{S} = S \cup \{v\}$$

is also linearly independent. $S \subset \bar{S}$. This contradicts the assumption that S is maximally linearly independent. ✓

Corollary 5.4. Every finitely generated vector space V has a basis.

Proof. Since V is finitely generated, we can find $S \subseteq V$ finite s.t. $span(S) = V$.

We can successively remove elements from S until it is a minimal set of generators.

✓

Remark. Any vector space has a basis.

5.2 Dimension

Lemma 5.5. (Exchange Lemma): Let V be a F-vector space with basis $S = \{s_1, \ldots s_n\}$. Let w be

$$w = a_1 s_1 + \ldots + a_n s_n$$

If k is such that $a_k \neq 0$, then

$$S' := \{s_1, \ldots s_{k-1}, w, s_{k+1}, \ldots s_n\}$$

is also a basis.

Proof. WLOG assume $a_1 \neq 0$. $S' = \{w, s_2, \ldots s_n\}$.

(1) WTS that $span(S') = span(S) = V$.
Since $a_1 \neq 0$,

$$w = a_1 s_1 + \ldots + a_n s_n$$
$$s_1 = \frac{1}{a_1} w - \frac{a_2}{a_1} s_1 - \frac{a_3}{a_1} s_3 - \ldots \frac{a_n}{a_1} s_n \in span(S')$$

Hence

$$S \subseteq span(S') \implies V \subseteq span(S')$$

also

$$span(S') \leq V \implies span(S') \subseteq V$$

Hence $V = span(S')$.

(2) WTS that S' linearly independent.
Take $c, c_2, \ldots c_n \in F$ so that

$$cw + c_2 s_2 + \ldots c_n s_n = 0$$

Since $w = a_1 s_1 + \ldots a_n s_n$, substituting, we get

$$c a_1 s_1 + (c a_2 + c_2) s_2 + \ldots (c a_n + c_n) s_n = 0$$

By linearly independence of S,

$$c a_1 = (c a_2 + c_2) = \ldots = (c a_n + c_n) = 0$$

Hence

$$c = c_2 = \ldots = c_n = 0$$

✓

Theorem 5.6. (Exchange Theorem): Let V be a F-vector space with basis $S = \{s_1, \dots s_n\}$. Let $T = \{t_1, t_2, \dots t_m\}$ be a linear independent subset of V. Then $m \le n$ and there are m elements in S which can be exchanged with elements of T to obtain a new basis, i.e. we can form

$$\{t_1, t_2, \dots t_m, s_{m+1}, \dots s_n\}$$

Proof.
By induction in m.

Case $m = 0$ is immediate.

Assume that $m \ge 1$ and that the Exchange Theorem is true for $m - 1$. Let $T = \{t_1, \dots t_m\}$. $T_0 = \{t_1, \dots t_{m-1}\}$ is linearly independent as well.

By induction hypothesis, $m - 1 \le n$ and after relabelling, S is $\{t_1, \dots t_{m-1}, s_m, s_{m+1}, \dots s_n\}$.

(1) We want to show that $m \le n$. Since we assume that indunction hypothesis is true, $m - 1 \le n$. This implies either $m = n + 1$ or $m \le n$.

If $m - 1 = n$, then $\{t_1, \dots t_{m-1}\}$ is a new basis. However, $\{t_1, \dots t_m\}$ is linearly independent. This contradicts with the fact that basis are maximally linearly independent. Hence $m = n$

(2) Since $\{t_1, \dots t_{m-1}, s_m, \dots s_n\}$ is a basis, we can write

$$t_m = \sum_{i=1}^{m-1} a_i t_i + \sum_{i=m}^{n} a_i s_i$$

Rearranging, we get

$$a_1 t_1 + \dots a_{m-1} t_{m-1} - tm = -a_m s_m - \dots - a_n s_n$$

Since $\{t_1, \dots t_m\}$ is lienarly independent, the LHS is non-zero, and there must be some $a_k, m \le k \le n$ such that $a_k \neq 0$.

By exchange lemma, in the basis $\{t_1, \dots t_{m-1}, s_m \dots s_n\}$, we can replace s_k with t_m, to get a new basis

$$S\ \{s_k\} \cup \{t_m\}$$

✓

Corollary 5.7. (Basis extension theorem): Let V be a finitely-generated F-vector space. Every linearly independent set $\{t_1, \dots t_m\}$ can be extended to form a basis for V. I.e. we can find

$$t_{m+1}, \dots t_n \in V \text{ such that } S = \{t_1, \dots t_m, t_{m+1}, \dots t_n\}, n \ge m$$

Proof. By exhange theorem, consider any basis S. T is a linearly independent set. We can choose $t_{m+1}, \dots t_n$ to be $s_{m+1}, \dots, s_n$ respectively. ✓

6 Class 6

6.1 Basis, cont'd

Corollary 6.1. (Bases have equan cardinality): If V has a finite basis of n elements, then any other basis of V is finite with exactly n elements.

Proof. Let $S = \{s_1, \dots s_n\}$ be a basis of V with n elements.

Any other basis has to be finite. Otherwise, we would have an infinitely linearly independent set. In particular, we can find $n+1$ linearly independent vectors, which contradicts the exchange theorem.

If anther basis has k elements, by exchange theorem, taking the other basis to be the linearly independent set, $k \leq n$. Also by exchange theorem, $n \leq k$. Hence $n = k$. ✓

Definition 6.2. (Dimension): Let V be a F-vector space over V. Then

$$\dim V = \begin{cases} \infty \text{ if } V \text{ not finitely generated} \\ n \text{ if } V \text{ has a basis of } n \text{ elements} \end{cases}$$

Remark. "finitely generated" means "finite dimensional". Henceforth we will use "finite dimensional".

Remark. $\dim F^n = n$, because $\{e_1, \dots e_n\}$ is a basis.

Corollary 6.3. Let V be a finite-dimensional F-vector space $W <$ is a proper subspace (i.e. $W \leq V, W \neq V$), then

$$\dim W < \dim V$$

Proof. Let $n = \dim V$. We can't ahve more than n linearly independen vectors in V. Hence $\dim W < \infty$.

Let $m = \dim W$, and $\{w_1, \dots w_n\}$ be a basis for W. Since $W \subset V$, there is $u \in V \setminus \{W\}$.

$$v \notin span(w_1, \dots w_n)$$

Hence $w_1, \dots w_n, u$ is linearly indepdent.

$$\dim V \geq m + 1 > m = \dim W$$

✓

Theorem 6.4. (Dimension of sum of subspaces): Let V be a finite-dimensional F-vector space. Let W_1, W_2 be subspaces of V. Then

1. $\dim(W_1 + W_2) = \dim W_1 + \dim W_2 - \dim(W_1 \cap W_2)$
2. If $W_1 \cap W_2 = \{0\}$, then $\dim(W_1 \bigoplus W_2) = \dim W_1 + \dim W_2$

Proof.
(1) $\implies$ (2): $\emptyset$ is a basis of $\{0\}$, so $\dim\{0\} = 0$.

(1): Let $d_0 = \dim(W_1 \cap W_2), d_1 = \dim W_1, d_2 = \dim W_2$. Let $T = \{t_1, t_2, \dots t_{d_0}\}$ be a basis for $W_1 \cap W_2$. Complete T to be a basis of W_1 and W_2.

$$\beta_{W_1} = T \cup S, S = \{s_1, \dots s_{d_1 - d_0}\}$$
$$\beta_{W_2} = T \cup R, R = \{r_1, \dots r_{d_2 - d_0}\}$$

Claim: $\beta = T \cup S \cup R$ is a basis for $W_1 + W_2$.

If claim were true, then

$$\begin{aligned} \dim(W_1 + W_2) &= |T| + |S| + |R| \\ &= d_0 + (d_1 - d_0) + (d_2 - d_0) \\ &= d_1 + d_2 - d_0 \\ &= \dim W_1 + \dim W_2 - \dim(W_1 \cap W_2) \end{aligned}$$

WTS $(T \cup S \cup R)$ spanning:

Since $\langle T \cup S \rangle = W_1, \langle T \cup R \rangle = W_2$,

$$W_1 + W_2 \subseteq \langle T \cup S \cup R \rangle$$

We also have $\langle T \cup S \cup R \rangle \subseteq W_1 + W_2$. Hence

$$\langle T \cup S \cup R \rangle = W_1 + W_2$$

WTS $(T \cup S \cup R)$ linearly independent:

Suppose

$$\begin{aligned} 0 &= \sum_{i=1}^{d_0} a_i t_i + \sum_{j=1}^{d_1 - d_0} b_j s_j + \sum_{k=1}^{d_2 - d_0} c_k r_k \\ &= v_0 + v_1 + v_2 \end{aligned}$$

Then

$$v_0 + v_1 = -v_2 \in W_1 \cap W_2$$

Since $v_0 \in W_1 \cap W_2, v_1 \in W_1, (v_0 + v_1) \in W_1, -v_2 \in W_2$.

Since $v_0 + v_1 \in W_1 \cap W_2$, we can express it in terms of the basis

$$v_0 + v_1 = -v_2 = \sum_{i=1}^{d_0} \lambda_i t_i = \sum_{i=1}^{d_0} a_i t_i + \sum_{j=1}^{d_1 - d_0} b_j s_j$$

Since $T \cup S$ is a basis for W_1, by the fact that representations are unique, we know that all $b_j = 0$.

Now we have

$$0 = v_0 + v_2 = \sum_{i=1}^{d_0} a_i t_i + \sum_{k=1}^{d_2 - d_0} c_k r_k$$

Since $T \cup R$ is a basis for W_2, $a_i = c_k = 0$ for all i, k. ✓

7 Class 7

7.1 Matrices and Systems of linear equations

Definition 7.1. (Matrix): A $m \times n$ matrix over field F is an array of elements $a_{ij} \in F$ of the form

$$A = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{bmatrix}$$

Where m is the bumber of rows and n is the number of columns.

We denote $Mat_{m\times n}(F)$ the set of all such matrices, or $F^{m\times n}$.

. *A_{ij} denotes the (i, j) entry of matrix $A \in Mat_{m\times n}(F)$.*

Remark. $F^{m\times n}$ is a vector space with sum and scalar multiplication defined entrywise.

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

Proof. We present a basis with mn elements. Consider

$$\{E^{ij}\}_{1\leq i\leq m, 1\leq j\leq n}$$

Where

$$\left(E^{ij}\right)_{kl} = \begin{cases} 1 \text{ if } (k, l) = (i, j) \\ 0 \text{ otherwise} \end{cases}$$

✓

Definition 7.2. (Matrix Multiplication): $A \leq F^{m\times n}, B \in F^{n\times r}$. Then, $AB \in F^{m\times r}$ is defined by

$$(AB)_{ij} = \sum_{k=1}^{n} A_{ik}B_{kj}$$

I.e. the (i, j)-th entry of AB is the dot product of the i-th row of A with the j-th column of B.

Remark. Properties of matrix multiplication

- In general, for $A, B \in F^{n\times m}$, $AB \neq BA$
- $A \in F^{m\times n}, B \in F^{n\times r}, C \in F^{r\times s}$, $(AB)C = A(BC)$.

Definition 7.3. (Systems of linear equations): Let $b_1, b_2, \dots b_n \in F, a_{ij} \in F, \forall 1 \leq i \leq m, 1 \leq j \leq n$, the set of equations

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \dots + a_{2n}x_n = b_2 \\ \quad\vdots \\ a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mn}x_n = b_m \end{cases}$$

is called a system of m-linear equations in n unknowns.

Remark. In matrix notation, let A, B

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \dots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} \in F^{m\times n}$$

$$b = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix} \in F^{m\times 1}$$

The system of m-linear equations in n variables is denoted

$$Ax = b$$

Where

$$x = \begin{pmatrix} x_1 \\ x_2 \\ \dots \\ x_n \end{pmatrix} \in F^{n\times 1}$$

Definition 7.4. (Homogeneity): A system $Ax = b$ is homogenous if $b = 0 \in F^n$. Otherwise it is inhomogenous.

Remark. A homogenous system has at least one solution with $x = 0$. Otherwise, this is not guaranteed.

Definition 7.5. (Solution set): The solution set of a linear system $Ax = b$ is the set of elements in $F^{n\times 1}$ such that $Ax = b$

$$\{x \in F^{n\times 1} : Ax = b\}$$

Remark. If the system is homogenous, then the solution set is a subspace.

7.2 Echelon form and Row-reduced echelon form

Definition 7.6. (Echelon form): $A \in F^{m\times n}$ is in echelon form if

1. There exists some $r, 1 \le r \le m$ so that every row of index less than or equal to r has at least 1 non-zero entry, and every row of index greater than r is zero
2. for every $i \le r$, consider the lowest index j_i that has a non-zero entry, i.e.
$$j_i := \min\{1 \le j \le n : a_{j_i} \neq 0\}$$
Then
$$a_{ij_i} = 1$$
3. $j_1 \le j_2 \le j_3 \dots < j_r$

Remark. The a_{ij_i} are referred to as pivots.

- If A is in echelon form, then we can find the solution set.
- By relabelling the variables, assume we have pivots in the first r columns, $Ax = b$ becomes
$$\left(\begin{array}{cccc|c} 1 & & & & b_1 \\ 0 & 1 & & & b_2 \\ 0 & & \ddots & & \vdots \\ 0 & & & 1 & b_r \\ \hline 0 & 0 & \cdots & 0 & b_{r+1} \\ 0 & 0 & \cdots & 0 & \vdots \\ 0 & 0 & \cdots & 0 & b_m \end{array}\right)$$
  - If there is some $i > r$ for which $b_i \le 0$, then there is no solution.
  - If all $b_i = 0$ for $i > r$, the variables $x_1, x_2, \dots x_r$ can be solved in terms of the variables $x_{r+1}, x_{r+2}, \dots x_n$

Definition 7.7. (Row-reduced echelon form): A is in the row-reduced echelon form if A is in the echelon form and all entries above the pivots are zero.

Definition 7.8. (Elementary row operations):

- **RO1**: Exchange 2 different rows
- **RO2**: Add λ times i-th row to the j-th row where $\lambda \in F \setminus \{0\}, i \neq j$ and replacing row j with the result
- **RO3**: Multiply a row by a non-zero scalar in F

Theorem 7.9. (Row-reduced echelon form):

1. Every matrix A can be put into row-reduced echelon form using finitely many elementary row operations
2. If $Ax = b$ is a system of linear equations and $(\tilde{A}|\tilde{b})$ is the matrix obtained from $(A|b)$ by performing the row operations that **put A in row-reduced echelon form**, then they have the same solution set

Remark. $(A|b)$ denotes the $m \times (n+1)$ matrix obtained from A by appending $b \in F^{m\times 1}$ to $A \in F^{m\times n}$.

Proof.

(1): Assume $A \in F^{m \times n}, A \neq 0$, find the first non-zero column of A,

$$j_1 := \min\{1 \leq j \leq n : a_{ij} \neq 0 \text{ for some } i\}$$

- If $A_{1j_1} \neq 0$, multiply the first row by $(A_{1j_1})^{-1}$ (RO3), i.e. *creating a pivot in the first row* in the $(1, j_1)$ position. We can make every other entry of that column 0 (finite number of RO2).
- If $A_{1j_1} = 0$, let $i_1 \neq 1$ be the first non-zero entry in the j_1 column and exchange row 1 with row i_1 (RO1)

$$\begin{pmatrix} 0 & \cdots & 0 & 1 & \dots & \dots & \dots \\ 0 & \cdots & 0 & 0 & & & \\ \vdots & & \vdots & \vdots & & A_2 & \\ 0 & \cdots & 0 & 0 & & & \end{pmatrix}$$

Repeat the process with A_2 to get the result after finitely many steps. Finally, we use RO2 to convert the matrix from echelon form to row-reduced echelon form.

(2): It suffices to show that each elementary row operation does not change the solution set. RO1 and RO3 are obvious.

For RO2, let

$$(1) \begin{cases} a_{i1}x_1 + a_{i2}x_2 + \ldots + a_{in}x_n = b_i \\ a_{j1}x_1 + a_{j2}x_2 + \ldots + a_{jn}x_n = b_j \end{cases}$$

$$(2) \begin{cases} a_{i1}x_1 + a_{i2}x_2 + \ldots + a_{in}x_n = b_i \\ (a_{j1} + a_{i1})x_1 + (a_{j2} + a_{i2})x_2 + \ldots + (a_{jn} + a_{in})x_n = b_j \end{cases}$$

Suppose $\boldsymbol{x}$ satisfies (1), add $\lambda 1.1$ to 1.2, then 2.2 holds. Hence $\boldsymbol{x}$ is also a solution for (2). Likewise, if $\boldsymbol{x}$ is a solution to (2), do $2.2 - \lambda 1.1$, then 1.2 also holds.

✓

Corollary 7.10. If $A \in F^{m \times n}$ and $m < n$ then $Ax = 0$ has a non-trivial solution.

Proof. Let $\tilde{A}$ be the row-reduced echelon form of A, then by theorem above,

$$Ax = 0 \Leftrightarrow \tilde{A}x = 0$$

The matrix $\tilde{A}$ has $0 \leq r \leq m$ non-zero rows which corresponds to the number of pivots, which is the number of non-free variables. $\tilde{A}$ has $n - r$ free variables

$$r \leq m$$
$$-r \geq -m$$
$$n - r \geq n - m > 0$$

$\tilde{A}x = 0$ has a non-trivial solution by taking all free variables say 1. ✓

Corollary 7.11. Let $A \in F^{n \times n}$ and $\tilde{A}$ be the row-reduced echelon form of A. Then, $\tilde{A}$ is the identity if and only if $x = 0$ is the unique solution to $Ax = 0$.

Proof.
($\implies$):

$$\begin{aligned} \tilde{A} = I \implies Ax = 0 &\Leftrightarrow \tilde{A}x = 0 \\ &\Leftrightarrow Ix = 0 \\ &\Leftrightarrow x = 0 \end{aligned}$$

($\impliedby$): Assume $x = 0$ is the only solution to $Ax = 0$. Then $\tilde{A}$ does not have free variables, $r \geq n$. However, $r \leq n$ always. Hence $r = n$. Therefore $\tilde{A} = I$. ✓

8 Class 8

8.1 Elementary Matrices and Invertible Matrices

Definition 8.1. (Elementary matrix) An elementary matrix is a matrix that can be obtained from the identity matrix by a single elementary row operation.

Example. In $\mathbb{R}^2$, the following are elementary matrices

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}, \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix},$$

for $a \in \mathbb{R}, a \neq 0$

Theorem 8.2. Let e be an elementary row operation and let $E = e(I)$ be the corresponding matrix of size $m \times m$.

Then $e(A) = EA$ for every $m \times n$ matrix A

Proof. RO1:

RO2: replace row r by row r + $c\times$ row r.

$$E_{ik} = \begin{cases} \delta_{ik}, i \neq r \\ \delta_{rk} + c + \delta_{sk}, i = r \end{cases}$$

Then

$$(EA)_{ij} = \sum_{k=1}^{m} E_{ik} A_{kj} = \{ A_{ik}, i \neq r, A_{rj} + cA_{sj}, i = r$$

RO3:

✓

Example. Let e be the row operation of adding 2 tiomes the first row to the second row, and

$$A = \begin{pmatrix} 2 & 3 & 4 & 5 \\ 1 & 1 & 0 & 1 \end{pmatrix}$$

$$e(A) = \begin{pmatrix} 2 & 3 & 4 & 5 \\ 5 & 7 & 8 & 11 \end{pmatrix}$$

Also,

$$E = e(I) = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$$

$$EA = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 2 & 3 & 4 & 5 \\ 1 & 1 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 3 & 4 & 5 \\ 5 & 7 & 8 & 11 \end{pmatrix}$$

Corollary 8.3. Let $A, B \in F^{m \times n}$, A can be transformed into B by a finite series of elementary matrices if and only if $B = PA$, where P is some product of elementary matrices.

Proof. $\implies$: If one can take A into B with row operations $e_1, e_2, \ldots e_k$, in this order, let $E_i = e_i(I)$, then

$$B = E_k E_{k-1} E_{k-2} \ldots E_1 A$$

Take

$$P = E_k E_{k-1} E_{k-2} \ldots E_1$$

$\impliedby$ Let $B = E_k E_{k-1} \ldots E_1 A$. Define

$$e_i(A) := E_i A$$

We can follow the row operations dictated by the E_i's to get from A to B. ✓

Definition 8.4. If A can be transformed into B by a series of finitely many row operations, then so can B be transformed into A (i.e. row operations can be reversed), and A and B are called row equivalent matrices.

Definition 8.5. (Invertible matrices) $A \in Matr_n(F)$ is **invertible** if there exists $B \in Matr_n(F)$ such that

$$AB = BA = I_n$$

in which case B is denoted A^{-1}

Remark. If B exists, then it is unique.

Proof. Suppose B, C both inverses of A

$$B = B = IB = (CA)B = C(AB) = C$$

✓

Example. Elementary matrices are invertible

$$E_1 = \begin{pmatrix} \lambda & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

has inverse

$$E_1^{-1} = \begin{pmatrix} \lambda^{-1} & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$E_2 = \begin{pmatrix} 1 & 0 & \lambda \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

has inverse

$$E_2^{-1} = \begin{pmatrix} 1 & 0 & -\lambda \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Theorem 8.6. (Product of invertible matrices are invertible) Let $A, B \in Matr_n(F)$

1. if A invertible, then $(A^{-1})^{-1} = A$
2. if A, B invertible, then AB is invertible, and

$$(AB)^{-1} = B^{-1}A^{-1}$$

Proof.
(1) follows from the symmetry of the definition of inverses

$$A(A^{-1}) = A^{-1}A = I$$

Hence A undoes A^{-1}.
(2)

$$(AB)(B^{-1}A^{-1}) = ABB^{-1}A^{-1}$$

$$= AIA^{-1}$$

✓

8.2 Linear Maps

8.2.1 Linearity

Definition 8.7. (Linear Maps) Let V, W be F-vector spaces. A map $\phi : V \to W$ is linear if

1. $\phi(v_1 + v_2) = \phi(v_1) + \phi(v_2)$
2. $\phi(cv) = c\phi(v)$

Remark. If $\phi : V \to W$ is linear, then $\phi(0_V) = 0_W$

Proof. Take $c = 0$, $\phi(0v) = \phi(0_V) = 0\phi(v) = 0_W$ ✓

8.2.2 Injectivity, surjectivity, and isomorphisms

Definition 8.8. (Injective) A map $\phi : X \to Y$ between X and Y is said to be **injective** if for $x, x' \in X$

$$\phi(x) = \phi(x') \implies x = x'$$

Definition 8.9. (Surjective) A map $\phi : X \to Y$ between X and Y is said to be **surjective** if for every $y \in Y$, there exists $x \in X$ such that

$$phi(x) = y$$

Example. $\phi : \mathbb{R} \to \mathbb{R}, x \mapsto x^2$ is not injective since $\phi(1) = \phi(01)$.

Note also that

- $\phi : \mathbb{R} \to \mathbb{R}_{\geq 0}$ is surjective but not injective
- $\phi_{\geq 0} : \mathbb{R} \to \mathbb{R}_{\geq 0}$ is surjective and injective

Definition 8.10. (Bijective) If $\phi : X \to Y$ is injective and surjective, then we say that ϕ is bijective.

Definition 8.11. (Isomorphism) A bijective linear map $\phi : V \to W$ between F-vector spaces is called an isomorphism.

When there is an isomorphism between V and W, we say that V, W are isomorphic.

$$V \cong W$$

8.2.3 Image and kernels

Definition 8.12. (Image, kernel) Let $\phi : V \to W$ be a linear map between F-vector spaces, the image is defined as

$$\mathrm{Im}(\phi) := \phi(V) = \{\phi(v) : v \in V\}$$

The kernel is defined as

$$\ker(\phi) = \{v \in V : \phi(v) = 0\}$$

Example. Examples of linear maps, their kernals and images.

1. $\phi : V \to \{0\}, v \mapsto 0$, is a linear map called the zero map
$$Im(\phi) = \{0\}, \ker(\phi) = V$$
2. $\phi : V \to V, v \mapsto v$ is called the identity map
$$Im(\phi) = V, \ker(\phi) = \{0\}$$
3. $V = \{a + bx : a, b \in F\}$ for variable x is the set of linear polynomials. V is a subspace of the space of of all linear maps from F to F. Let $\phi : V \to W, a + bx \mapsto b$. ϕ is linear because
$$\phi((a + bx) + \lambda(c + dx)) = b + \lambda d = \phi(a + bx) + \lambda(c + dx)$$
$$Im(\phi) = F, \ker(\phi) = \{a : a \in F\} = \text{ set of constant polynomials}$$

Proposition 8.13. Let $\phi : V \to W$ be a linear map between F-vector spaces. Then

$$\ker(\phi) \leq V, Im(\phi) \leq W$$

Proof.
$\phi(0_v) = 0_w$ hence $0_v \leq W, 0 \in \ker(\phi), 0 \in Im(\phi)$.
Take $v_1, v_2 \in \ker(\phi), a \in F$

$$\phi(v_1 + av_2) = \phi(v_1) + a\phi(v_2) = 0 \implies v_1 + av_2 \in \ker(\phi)$$

Take $w_1, w_2 \in \mathrm{Im}(\phi), a \in F$. We know that there exists v_1, v_2 such that

$$\phi(v_1) = w_1, \phi(v_2) = w_2$$

Hence

$$\phi(v_1 + av_2) = \phi(v_1) + a\phi(v_2) = w_1 + aw_2$$
$$\implies w_1 + aw_2 \in Im(\phi)$$

✓

9 Class 9

9.1 Isomorphism, cont'd

Proposition 9.1. Let V, W be F-vector spaces and $\varphi : V \to W$ linear. Then

1. φ injective $\Leftrightarrow Im(\varphi) = W$
2. φ surjective $\Leftrightarrow \ker(\varphi) = \{0\}$
3. φ is bijective $\Leftrightarrow \mathrm{Im}(\varphi) = W$ and $\ker(\varphi) = \{0\}$

Proof.
1) By definition.

3) By consequence of (1) and (2)

2) $\implies$ Assume φ injective, then v_1, v_2 distinct implies $\varphi(v_1) \neq \varphi(v_2)$. Since φ linear, we know that $\varphi(0) = 0$.

$\Longleftarrow$ Assume $\ker(\varphi) = \{0\}$, consider v_1, v_2 such that $\varphi(v_1) = \varphi(v_2)$.

$$\begin{aligned} &\varphi(v_1) - \varphi(v_2) = 0 \\ \implies &\varphi(v_1 - v_2) = 0 \\ \implies &v_1 - v_2 \in \ker(\varphi) \\ \implies &v_1 - v_2 = 0 \\ \implies &v_1 = v_2 \end{aligned}$$

✓

Proposition 9.2. Let U, V, W be vector spaces over F, and

$$\varphi : U \to V, \psi V \to W$$

both linear.

Then,

1. $\psi \circ \varphi$ is linear where $\psi \circ \varphi(u) = \psi(\varphi(u))$
2. If φ is injective, then its inverse φ^{-1} is also linear.

Proof. Left as exercise. ✓

Theorem 9.3. (Isomorphism theorem) Let V, W be finite dimensional vector spaces over F, and $S = \{s_1, s_2, \ldots s_n\}$ a basis for V.

let $t_1, t_2, \ldots t_n \in W$ not necessarily distinct. Then, there exists a **unique linear map** $\varphi : V \to W$ such that

$$\varphi(s_i) = t_i$$

for all $i = 1, 2, \ldots n$.
Moreover

1. φ is surjective $\Leftrightarrow$ $span\{t_1, t_2, \ldots t_n\} = W$
2. φ is injective $\Leftrightarrow t_1, t_2 \ldots t_n$ linearly independent in W
3. φ is an isomorphism $\Leftrightarrow \{t_1, t_2, \ldots t_n\}$ is a basis.

Proof.
We first show existence and uniqueness of φ. Define

$$\begin{aligned} \varphi :&V \to W \\ \sum_{i=1}^{n} a_i s_i &\mapsto \sum_{i=1}^{n} a_i t_i \end{aligned}$$

Since $\{s_1, s_2, \ldots s_n\}$ is a basis, every vector of U is uniquely written as $v = \sum_{i=1}^{n} a_i s_i$ and φ is well defined.

To show that φ is linear,

$$\begin{aligned}
&\varphi\left(\sum_{i=1}^{n} a_i s_i + \sum_{i=1}^{n} b_i s_i\right)\\
=&\varphi\left(\sum_{i=1}^{n}(a_i + b_i)s_i\right)\\
=&\sum_{i=1}^{n}(a_i + b_i)t_i\\
=&\sum_{i=1}^{n} a_i t_i + \sum_{i=1}^{n} b_i t_i\\
=&\varphi\left(\sum_{i=1}^{n} a_i s_i\right) + \varphi\left(\sum_{i=1}^{n} b_i t_i\right)
\end{aligned}$$

Also

$$\begin{aligned}
&\varphi\left(c\sum_{i=1}^{n} a_i s_i\right)\\
=&\varphi\left(\sum_{i=1}^{n}(ca_i)s_i\right)\\
=&\sum_{i=1}^{n}(ca_i)t_i\\
=&c\sum_{i=1}^{n} a_i t_i\\
=&c\varphi\left(\sum_{i=1}^{n} a_i s_i\right)
\end{aligned}$$

To show that φ is unique, note that for any $a_1, a_2, \dots a_n$,

$$\varphi\left(\sum_{i=1}^{n} a_i s_i\right) = \sum_{i=1}^{n} a_i t_i$$

Proof of (1)

$\Longleftarrow:$ Assume $\mathit{span}\,(t_1, t_2, \dots t_n) = W$. Let $w \in W$, WTS there exists $v \in V$ such that $\varphi(v) = w$.

Since we know that $t_1, \dots t_n$ spans W, there exists $b_1, b_2, \dots b_n$ such that

$$w = \sum_{i=1}^{n} b_i t_i$$

Define v to be

$$v := \sum_{i=1}^{n} b_i s_i \in V$$

Then

$$\varphi(v) = \varphi\left(\sum_{i=1}^{n} b_i s_i\right) = \sum_{i=1}^{n} b_i t_i = w$$

$\implies$ Assume φ surejective, for any $w \in W$, WTS that $w \in \mathit{span}\,(t_1, t_2, \dots t_n)$.

Since φ surjective, we know that there is some v such that $\varphi(v) = w>$

Since $s_1, s_2, \dots s_n$ is a basis, there exists $a_1, a_2, \dots a_n$ such that

$$v = \sum_{i=1}^{n} a_i s_i$$

Apply φ

$$w = \varphi(v) = \sum_{i=1}^{n} a_i t_i \in \mathit{span}\,(t_1, t_2, \dots t_n)$$

Proof of (2):

$\implies$ Suppose φ injective, WTS that $t_1, t_2, \dots t_n$ is linearly independent.

Take $c_1, c_2, \dots c_n$ such that

$$c_1 t_1 + c_2 t_2 + \dots c_n t_n = 0$$

Define v as

$$v := \sum_{i=1}^{n} c_i s_i$$

Then

$$\varphi(v) = \varphi\left(\sum_{i=1}^{n} c_i s_i\right) = \sum_{i=1}^{n} c_i t_i = 0$$

Hence

$$v = \sum_{i=1}^{n} c_i s_i \in \ker(\varphi)$$

By injectivity,

$$\sum_{i=1}^{n} c_i s_i = 0$$

By linear independence of s_i,

$$c_1 = c_2 = \ldots c_n = 0$$

$\Longleftarrow$: Assume $t_1, t_2, \ldots t_n$ linearly independent, WTS $\ker(\varphi) = \{0\}$.

Take $v \in \ker(\varphi)$ such that $\varphi(v) = 0$. Since $v \in V$, we know that

$$v = \sum_{i=1}^{n} a_i s_i$$

for some $a_1, a_2 \ldots a_n$.

Hence

$$0 = \varphi(v) = \varphi\left(\sum_{i=1}^{n} a_i s_i\right) = \sum_{i=1}^{n} a_i t_i$$

By linear independence of $t_1, t_2, \ldots t_n$, $a_1 = a_2 = \ldots = a_n = 0$. Hence $v = 0$.

Since v was an arbitrary element of $\ker(\varphi)$, we know that

$$\ker(\varphi) = \{0\}$$

Proof of (3): follows from 1 and 2. ✓

Theorem 9.4. Let V, W be finite-dimensional vector spaces over F.

$$\dim V = \dim W \Leftrightarrow V \cong W$$

Proof.

$\Longrightarrow$: Take $\{s_1, s_2, \ldots s_n\}$ a basis for V, $\{t_1, t_2 \ldots t_n\}$ a basis for W. By the isomorphism theorem, the map that takes s_i to t_i is an isomorphism.

$\Longleftarrow$: Suppose $V \cong W$, let $\Phi : V \to W$ be an isomorphism, and let $\dim V = n$.

V has a basis of n elements, say $s_1, s_2, \ldots s_n$.

Define $t_1, t_2 \ldots t_n$

$$t_i := \Phi(s_i)$$

The isomorphism theorem guarantees that $t_1, t_2 \ldots t_n$ is a basis for W, so $\dim W = n$. ✓

Corollary 9.5. If V is a vector space and $\dim W = n$, then

$$V \cong F^n$$

Example. Let

$$\mathcal{P}_2 = \{a_0 + a_1 x + a_2 x^2 : a_0, a_1, a_2 \in \mathbb{R}\}$$

A basis for $\mathcal{P}_2$ is $\{1, x, x^2\}$.

Define

$$\begin{aligned} \varphi : \mathcal{P}_2 &\to \mathbb{R}^3 \\ 1 &\mapsto e_1 \\ x &\mapsto e_2 \\ x^2 &\mapsto e_3 \end{aligned}$$

Then

$$\mathcal{P}_2 \cong \mathbb{R}^3$$

Furthermore, isomorphism theorem tells us that there exists a unique φ that does this.

10 Class 10

10.1 Isomorphisms, cont'd

Corollary 10.1. As a consequence of the isomorphism theorem, then, for V, W finite dimensional F-vector spaces, and $S = \{s_1, s_2, \dots s_n\}$ a basis for V.

A linear map $\phi : V \to W$ is uniquely determined by its values

$$\phi(s_1), \phi(s_2), \dots \phi(s_n)$$

Moreover

1. ϕ injective $\Leftrightarrow \phi(s_1), \phi(s_2), \dots \phi(s_n)$ linearly independent
2. ϕ surjective $\Leftrightarrow span(\phi(s_1), \phi(s_2), \dots \phi(s_n)) = W$
3. ϕ isomorphism $\Leftrightarrow \{\phi(s_1), \phi(s_2), \dots \phi(s_n)\}$ is a basis for W

Corollary 10.2. Let V, W be finite-dimensional F-vector spaces where

$$\dim W = \dim V$$

And $\phi : V \to W$ linear.

TFAE

1. ϕ injective
2. ϕ surjective
3. ϕ isomorphism

Proof. We claim that ϕ injective if and only if ϕ surjective.

$\implies$: If ϕ injective, then $\{\phi(s_1), \phi(s_2) \dots \phi(s_n)\}$ is a linear independent set of vectors of size n in W of dimension n. Hence it constitutes a basis, and ϕ is an isomorphism by the isomorphism theorem. Hence ϕ is surjective.

$\impliedby$ If ϕ surjective, then by isomorphism theorem,

$$span\,(\phi(s_1), \phi(s_2) \dots \phi(s_n)) = W$$

Since $\dim W = n$, $\phi(s_1), \phi(s_2) \dots \phi(s_n)$ must be linearly independent. By isomorphism theorem, ϕ is injective. ✓

10.2 Dimension formula for linear maps

Theorem 10.3. Let $\phi : V \to W$ be a linear map between F vector spaces. If $\{v_1, v_2, \dots v_m\}$ is a basis for $\ker(\phi)$, and $\{\phi(u_1), \phi(u_2) \dots \phi(u_k)\}$ is a basis for $Im(\phi)$, then

$$\{v_1, v_2, \dots v_m, u_1, u_2, \dots u_k\}$$

is a basis for V.

Proof.
We first show that the set is spanning.

Let $v \in V$, then $\phi(v) \in Im(\phi)$. Since $\{\phi(u_1) \dots \phi(u_k)\}$ is a basis for $Im(\phi)$, there exists $a_1, a_2 \dots a_k \in F$ such that

$$\phi(v) = \sum_{i=1}^{k} a_i \phi(u_i)$$

By linearity of ϕ,

$$\phi\left(v - \sum_{i=1}^{k} a_i u_i\right) = 0$$

Hence

$$
\begin{aligned}
& v - \sum_{i=2}^{k} a_i u_i \in \ker(\phi) \\
\implies & v - \sum_{i=1}^{k} a_i u_i = \sum_{j=1}^{m} b_j v_j \\
\implies & v = \sum_{i=1}^{k} a_i u_i + \sum_{j=1}^{m} b_j v_j \\
\implies & span\,(u_1, u_2 \dots u_k, v_1, v_2 \dots v_n) = V
\end{aligned}
$$

To show linear independence, take $c_i, d_j \in F$ such that

$$\sum_{j=1}^{m} c_j v_j + \sum_{i=1}^{k} d_i u_i = 0$$

Then

$$
\begin{aligned}
0 = \phi(0) = \phi\left(\sum_{j=1}^{m} c_j v_j + \sum_{i=1}^{k} d_i u_i\right) \\
\implies \sum_{j=1}^{m} c_j \phi(v_j) + \sum_{i=1}^{k} d_i \phi(u_i) = 0 \\
\implies \sum_{i=1}^{k} d_i \phi(u_i) = 0 \text{ since } v_j\text{'s form a basis for the kernel} \\
\implies d_1 = d_2 = \dots d_k = 0 \text{ by linear independence of } \phi(u_i)\text{'s}
\end{aligned}
$$

Also,

$$\sum_{j=1}^{m} c_j v_j = 0 \implies c_1 = c_2 = \dots c_m = 0 \text{ by linear independence of } v_j\text{'s}$$

✓

Corollary 10.4. (Dimension formula): let $\phi : V \to W$ linear, then

$$\dim V = \dim \ker(\phi) + \dim Im(\phi)$$

Definition 10.5. Let $\phi : V \to W$ where V, W are F-vector spaces. The **nullity** of ϕ is

$$nullity(\phi) = \dim \ker(\phi)$$

The rank of ϕ is

$$\text{rank}(\phi) = \dim Im(\phi)$$

Remark. Another way to express the dimension formula is

$$\dim V = nullity(\phi) + \text{rank}(\phi)$$
$$\dim V = \dim null(\phi) + \dim \text{Im}(\phi)$$

10.3 The algebra of endomorphisms

Definition 10.6. (Ring): A ring is a set R with 2 operations

$$
\begin{aligned}
+ :& R \times R \to R, (a, b) \mapsto a + b \\
\cdot :& R \times R \to R, (a, b) \mapsto a \cdot b
\end{aligned}
$$

so that

- (R1): $(R, +)$ is a commutative group
- (R2): multiplication is associative. For all $a, b, c \in R$
$$(a \cdot b) \cdot c = a \cdot (b \cdot c)$$
- (R3): distributivity holds
$$
\begin{aligned}
(a + b) \cdot c = a \cdot c + b \cdot c \\
a \cdot (b + c) = a \cdot ba \cdot c
\end{aligned}
$$

a
If other than $R1, R2, R3$,

- R satisfies $a \cdot b = b \cdot a$: R is said to be a **commutative ring**
- R contains 1 such that $1 \cdot a = a \cdot 1 = a$, R is said to be a ring with unity, and 1 is called the **identity** or **unit** of R.

Definition 10.7. An F-vector space $(V, +, \cdot)$ with a map $\circ : V \times V \to V$ called multiplication is said to be an F-algebra if

1. $(V, +, \circ)$ is a ring with unit

2. For all $a \in F, v, w \in V$,
$$a \cdot (v \circ w) + (a \cdot v) \circ w = v \circ (a \cdot w)$$

Example. Consider the ring of polynomials in the indeterminate x and coefficients in $\mathbb{R}$
$$\mathbb{R}[x] = \{a_0 + a_1 x + \dots a_n x^n : n \in \mathbb{N}_0, a_1 \in \mathbb{R}\}$$
$\mathbb{R}[x]$ is a ring with unit with the usual addition and multiplication of polynomials, and the unit is the constant polynomial 1.

Moreover, $\mathbb{R}[x]$ is an $\mathbb{R} - algebra$.

Remark. For any ring $\mathbb{R}$, if the unit exists, then it is unique.

Assume $1, 1'$ are both units
$$\begin{aligned} 1 &= 1' \cdot 1 \text{ since } 1' \text{ unit} \\ &= 1' \text{ since } 1 \text{ unit} \end{aligned}$$

Definition 10.8. (Homomorphisms) Let V, W be F-vector spaces. The set of all linear maps from V to W (homomorphisms) is denoted
$$Hom_F(V, W)$$

Definition 10.9. (Endomorphisms) Let V be F-vector space. The set of all linear maps from V to itself (endomorphism) is denoted
$$End_F(V, W)$$

Definition 10.10. (General linear group) Let V be F-vector space. The set of all isomorphisms from V to itself (general linear maps) is denoted
$$Gl(V)$$

Remark. A general linear map is an endomorphism and a homomorphism
$$Gl(V) \subseteq End_F(V) = Hom_F(V, V)$$

Theorem 10.11. Let V, W be vector spaces over F. Given $T_1, T_2 \in Hom_F(V, V), a \in F$. Define addition and scalar multiplication of linear maps with
$$(T_1 + T_2)v := T_1(v) + T_2(v)$$
$$(aT_1)(v) = a(T_1(v))$$
for all $v \in V$.

Then $T_1 + T_2$ and aT_1 are also linear maps from V to W.

Hence, $Hom_F(V, W)$ with addition and scalar multiplication is a vector space over F.

Proof. Left as exercise ✓

Remark. Let F be a field, V, W F-vector spaces. Then

1. $Hom_F(V, W)$ is avector space
2. $End_F(V)$ is an F-algebra with composition of linear maps as multiplication
3. $Gl(V)$ is a group with respect to composition of homomorphisms.

Note that once we restrict to the set of invertible linear maps, we have the existence of inverses and hence group properties.

10.4 Coordinates and matrices

For this section, let $S = (s_1, s_2 \dots s_n)$ denote an **ordered basis** to emphasize that order matters.

10.4.1 Coordinates and change of basis

Definition 10.12. (Coordinates) Let $S = (s_1, s_2, \dots s_n)$ be a basis for V. Then, for arbitrary $v \in V$, v can be uniquely written as

$$v = \sum_{i=1}^{n} a_i s_i$$

The a_i's are called the **coordinates** of v with respect to S. We denote this

$$[v]_S = \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix}$$

The map $\gamma_S : V \to F^n$ is called the **coordinate representation** of V with respect to S

$$\begin{aligned} \gamma_S : V &\to F^n \\ v &\mapsto [v]_S \end{aligned}$$

Remark. The coordinate representation map is an isomorphism.

Proof. Proof that γ_S is linear: left as exercise.

Note that for $1 \leq i \leq n$

$$\gamma_S(s_i) = e_i \in F^n$$

The basis $s_1, s_2, \dots s_n$ is mapped to the standard basis $e_1, e_2, \dots e_n$ of F^n. By the isomorphism theorem, γ_S is an isomorphism. ✓

Proposition 10.13. Let V be an F-vector space. Let $S = (s_1, s_2, \dots s_n)$, $T = (t_1, t_2, \dots t_n)$ be bases of V.

1. There are uniquely determined $c_{ij}, d_{ij} \in F$ so that

$$s_j = \sum_{i=1}^{n} c_{ij} t_i$$

$$t_i = \sum_{j=1}^{n} d_{ji} s_j$$

2. For $v \in V$ arbitrary, there exists some a_j's and b_i's such that

$$v = \sum_{j=1}^{n} a_j s_j = \sum_{i=1}^{n} b_i t_i$$

   The coordinates are related by

$$b_i = \sum_{i=1}^{n} c_{ij} a_j$$

$$a_j = \sum_{j=1}^{n} d_{ji} b_i$$

3.

$$\sum_{j=1}^{n} c_{kj} d_{ji} = \delta_{ki} = \begin{cases} 1 \text{ if } k = i \\ 0 \text{ otherwise} \end{cases}$$

Proof. (1): follows immediately from the fact that S, T are bases for V.

(2): Writing v in terms of s_j

$$\begin{aligned} v &= \sum_{j=1}^{n} a_j s_j \\ &= \sum_{j=1}^{n} a_j \sum_{i=1}^{n} c_{ij} t_i \text{ by substituting expression for } s_j \\ &= \sum_{i=1}^{n} \left(\sum_{j=1}^{n} c_{ij} a_j \right) t_i \end{aligned}$$

On the other hand,

$$v = \sum_{i=1}^{n} b_i t_i$$

By unique representation,

$$b_i = \sum_{j=1}^{n} c_{ij} a_j$$

Similarly, starting from

$$\begin{aligned} v &= \sum_{i=1}^{n} b_i t_i \\ &= \sum_{i=1}^{n} b_i \left(\sum_{i=1}^{n} d_{ji} s_j \right) \\ &= \sum_{j=1}^{n} \left(\sum_{i=1}^{n} d_{ji} b_i \right) s_j \end{aligned}$$

By unique representation

$$a_j = \sum_{i=1}^{n} d_{ji} b_i$$

Proof of (3):

$$\begin{aligned} s_j &= \sum_{i=1}^{n} c_{ij} t_i \\ &= \sum_{i=1}^{n} c_{ij} \left(\sum_{k=1}^{n} d_{ki} s_k \right) \\ &= \sum_{k=1}^{n} \left(\sum_{i=1}^{n} d_{ki} c_{ij} \right) s_k \end{aligned}$$

At the same time

$$s_j = \sum_{k=1}^{n} \delta_{kj} s_k$$

Hence, by unique representation

$$\sum_{i=1}^{n} d_{ki} c_{ij} = \delta_{kj}$$

✓

11 Class 11

Definition 11.1. (Change of basis matrix)

$$C_{S\to T} = \begin{pmatrix} c_{11} & c_{12} & \dots & c_{1n} \\ c_{21} & c_{22} & \dots & c_{2n} \\ \vdots & \vdots \ddots & \vdots & \\ c_{n1} & c_{n2} & \dots & c_{nn} \end{pmatrix}$$

Where the i-th column is the coordinates of s_i with respect to basis T, is called the **basis change matrix** from S to T

Remark. If $v = \sum_{j=1}^{n} a_j s_j = \sum_{i=1}^{n} b_i t_i$ then

$$[v]_T = C_{S\to T}[v]_S$$

Similarly, if $C_{T\to S} = [d_{ij}]$ where

$$t_j = \sum_{i=1}^{n} d_{ij} s_i$$

then

$$[v]_S = C_{T\to S}[v]_T$$

Therefore, the proposition from Class 10 can be rephrased as

$$[v]_T = C_{S\to T}[v]_S, [v]_S = C_{T\to S}[v]_T$$

and

$$C_{S\to T}C_{T\to S} = I = C_{T\to S}C_{S\to T}$$

11.1 Representation of linear maps

Definition 11.2. Let V, W be F-vector spaces, $S = (s_1, s_2, \dots s_n)$ basis for V. $T = (t_1, t_2, \dots t_m)$ basis for W. Let $\phi : V \to W$ linear.

There are uniquely determined coefficients $d_{ij} \in F$ such that

$$\phi(s_j) = \sum_{i=1}^{m} d_{ij} t_i$$

for all $1 \le j \le n$.

The matrix

$$[\phi]_{S\to T} = [d_{ij}]_{1\le i\le m, 1\le j\le n}$$

is the $m \times n$ matrix representing ϕ with respect to bases S and T.

Remark. If $\phi = Id_V : V \to V, v \mapsto v$, and S, T bases for F

$$[Id_V]_{S\to T} = C_{S\to T}$$

Proposition 11.3. Let V, W be F-vector spaces.

Let $[v]_S = \gamma_S(v)$ be the coordinate representation of v with respect to S.
Let $[\phi(v)]_T = \gamma_T(\phi(v))$ be the coordinate representation of $\phi(v)$ with respect to T, then

$$[\phi(v)]_T = [\phi]_{S\to T}\,[v]_S$$

Proof. Let

$$v = \sum_{i=1}^{n} a_j s_j \in V.$$

Let d_{ij} be defined by

$$\phi(s_j) = \sum_{i=1}^{m} d_{ij} t_i$$

then

$$\begin{aligned}
\phi(v) &= \sum_{j=1}^{n} a_j \phi(s_j) \\
&= \sum_{j=1}^{n} a_j \sum_{i=1}^{m} d_{ij} t_i \\
&= \sum_{i=1}^{m} \left(\sum_{j=1}^{n} d_{ij} a_j \right) t_i
\end{aligned}$$

Therefore

$$\begin{aligned}
[\phi(v)]_T &= \begin{bmatrix} \sum\limits_{j=1}^{n} d_{ij} a_j \\ \sum\limits_{j=1}^{n} d_{2j} a_j \\ \vdots \\ \sum\limits_{j=1}^{n} d_{mj} a_j \end{bmatrix} \\
&= [d_{ij}] \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix} \\
&= [\phi]_{S \to T} [v]_S
\end{aligned}$$

✓

Theorem 11.4. Let V, W be F-vector spaces with $S = (s_1, s_2, \ldots s_n)$, $T = (t_1, t_2, \ldots t_n)$ bases respectively.

The map

$$\begin{aligned}
D_{S \to T} : Hom_F(V, W) &\to F^{m \times n} \\
\phi &\mapsto D_{S \to T}(\phi) = [\phi]_{S \to T}
\end{aligned}$$

is an isomorphism of F-vector spaces.

Proof. We want to show that $D_{S \to T}$ is linear and bijective.

(1) Linearity:
Let $\phi, \psi \in Hom_F(V, W)$ and $c \in F$.

Let a_{ij} such that $\phi(s_j) = \sum\limits_{i=1}^{n} a_{ij} t_i$. Let b_{ij} such that $\psi(s_j) = \sum\limits_{i=1}^{n} b_{ij} t_i$

Then,

$$\begin{aligned}
(\phi + c\psi)(s_j) &= \phi(s_j) + c\psi(s_j) \\
&= \sum_{i=1}^{n} (a_{ij} + cb_{ij}) t_i
\end{aligned}$$

Hence

$$\begin{aligned}
[\phi + c\psi]_{S \to T} &= [(a_{ij} + cb_{ij})]_{ij} \\
&= [a_{ij}] + c [b_{ij}] \\
&= [\phi]_{S \to T} + c [\psi]_{S \to T}
\end{aligned}$$

Hence $D_{S \to T}$ is linear.

(2): Injectivity $D_{S \to T}$ is injective because if $\phi, \psi \in Hom_F(V, W)$, such that

$$[\phi]_{S \to T} = [\psi]_{S \to T}$$

Then

$$\phi(s_j) = \psi(s_j)$$

Since S is a basis and ϕ, ψ linear, this implies $\phi = \psi$

✓

12 Class 12

13 Class 13

14 Class 14

14.1 Quotients, cont'd

Recall from last time (homomorphism theorem) that if $\varphi : V \to W$ is a linear map between F-vector spaces, then

$$\tilde{\varphi} : V/\ker\varphi \to Im\varphi, [v] \mapsto \varphi(v)$$

is well defined isomorphism.

Corollary 14.1. Every linear map $\varphi : V \to W$ factors as

$$\varphi = i \circ \overline{\varphi} \circ \pi$$

where

- $\pi : V \to V/\ker\varphi$ is the canonical projection
- $i : Im\varphi \to W$ is the inclusion map
- $\overline{\varphi} : V/\ker\varphi \to Im\phi$ is isomorphism

Proposition 14.2. (Dimension of a quotient space) Let V be a finite dimensional vector space over F, and let $W \leq V$, then

$$\dim(V/W) = \dim V - \dim W$$

Proof. Say $\dim W = m$. Take $(w_1, \dots, w_m)$ basis for W. Extend it to a basis of V, $S = (w_1, w_2, \dots w_m, v_{m+1}, v_{m+2}, \dots v_n)$ basis of V.

WTS that $([v_{m+1}], [v_{m+2}] \dots [v_n])$ is a basis for V/W.

Let $v \in V$ Since S is a basis for V

$$\begin{aligned}
v &= a_1 w_1 + \dots a_m w_m + a_{m+1} v_{m+1} + \dots a_n v_n \\
\implies [v] &= [a_1 w_1 + \dots a_m w_m] + [a_{m+1} v_{m+1} + \dots a_n w_n] \\
\\
\implies [v] &= [0] + a_{m+1}[v_{m+1}] + \dots a_n [v_n]
\end{aligned}$$

Hence $[v_{m+1}], \dots [v_n]$ spans V/W.

To show linear independence, let

$$b_{m+1}[v_{m+1}] + \dots b_n [v_n] = 0$$

for some $b_{m+1}, \dots b_n$.

$$\begin{aligned}
b_{m+1}[v_{m+1}] + \dots b_n [v_n] &= 0 \\
\implies \left[\sum_{i=m+1}^{n} b_i v_i\right] &= [0]
\end{aligned}$$

That is,

$$\sum_{i=m+1}^{n} b_i v_i \in W$$

By linear independence of v_i's in S,

$$b_{m+1} = \dots = b_n = 0$$

Hence,

$$\begin{aligned}
\dim(V/W) &= \#\{[v_{m+1}], \dots [v_n]\} \\
&= n - m \\
&= \dim V - \dim W
\end{aligned}$$

✓

Corollary 14.3. (New proof of dimension formula for linear maps)

Let $\varphi : V \to W$ be a linear map between F-vector spaces.

$$\dim V = \dim\ker\varphi + \dim Im\varphi$$

Proof. By the homomorphism theorem,

$$\dim V/\ker\varphi \cong Im\varphi$$

Then

$$\dim V/\ker\varphi = \dim Im\varphi \text{ by Homomorphism Theorem}$$
$$\dim V \ker\varphi = \dim V - \dim\ker\varphi \text{ by above proposition}$$

Hence

$$\dim V = \dim\ker\varphi + \dim Im\varphi$$

✓

Example. (Quotient capturing Taylor expansion)

Let $V = C^\infty[-1,1]$ be the space of smooth real-valued functions on $[-1,1]$ and fix $d \in \mathbb{N}_{\geq 0}$.

Define

$$W_d = \{f \in C^\infty[-1,1] \text{ s.t. } f^{(k)}(0) = 0, k = 0,1,2,\dots d\} \leq V$$

W_d consists of functions whose Taylor polynomial of degree d at 0 vanishes completely.

Then the quotient

$$V/W_d$$

is naturally isomorphic to the space of polynomials of degree at most d.

The isomorphism is induced by the map

$$\Phi : C^\infty[-1,1] \to \mathcal{P}_d, f \mapsto \Phi(f)(x) = f(0) + f'(0)x + \frac{1}{2!}f''(0)x^2 + \dots \frac{1}{d!}f^{(d)}(0)x^d$$

One has

$$V/W_d = V/\ker\Phi \cong Im\Phi = P_d$$

Example. Recall $V = \mathbb{R}^2, W = span(1,0)$.

Now, we know that

$$\dim V/W = \dim\mathbb{R}^2 - \dim W = 1$$

14.2 Linear Functionals

14.2.1 Dual space

Definition 14.4. (Linear Functionals) Let V be an F-VS. A linear map $f : V \to F$ is alos called a **linear functional**.

Definition 14.5. Let F be a field and V be a F-vector space. The dual space is defined as

$$V^* := Hom_F(V, F)$$

i.e. the vector space of all linear functionals on V.

Example. Examples of linear functionals

- sum of constants of polynomial Let $V = \mathcal{P}_d(\mathbb{R})$, then
$$f : \mathcal{P}_d(\mathbb{R}) \to \mathbb{R}, a_0 + a_1x + \dots a_dx^d \mapsto a_0 + a_1 + \dots a_d$$
- evaluation map Let $V = C^0[-1,1]$, then
$$F_0 : C^0[-1,1] \to \mathbb{R}, g \mapsto g(0)$$
- integration map
$$\Phi : C[a,b] \to \mathbb{R}, f \mapsto \int_a^b f(x)dx$$
- linear functional in F^n Fix $a_1, a_2, \dots a_n \in F$, define
$$f : F^n \to F, \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \mapsto a_1v_1 + \dots a_nv_n$$

Counter examples of linear functionals

- finding the length
$$f : \mathbb{R}^3 \to \mathbb{R}, (x,y,z) \mapsto \sqrt{x^2 + y^2 + z^2}$$
is not a linear functional.
$$f(-(1,0,0)) \neq -f(1,0,0)$$
- product of coordinates
$$F : \mathbb{R}^2 \to \mathbb{R}, (x,y) \mapsto xy$$

is not a linear functional. Take $v_1 = (1, 0), v_2 = (0, 1)$

$$F(v_1) = F(v_2) = 0$$
$$F(v_1) + F(v_2) = 0 \neq F(v_1 + v_2) = 1$$

Remark. Every linear functional in F^n has the form

$$f : F^n \to F, \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \mapsto a_1 v_1 + \dots a_n v_n$$

Proof. Let $g \in (F^n)^*$, then

$$g(v) = g \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} = g(v_1 e_1 + \dots v_n e_n)$$
$$= v_1 g(e_1) + \dots v_n g(e_n) \text{ by linearity of } g.$$

if you define $a_i = g(e_i), 1 \leq i \leq n$, then

$$g(v) = \sum_{i=1}^{n} a_i \pi_i$$

✓

Theorem 14.6. Let V be a vector space over F with basis $S = (s_1, s_2, \dots s_n)$. Then

1. $\dim V^* = \dim V$
2. Let f_i be linear map such that

$$f_i(s_j) = \delta_{ij} = \begin{cases} 1 \text{ if } j = i \\ 0 \text{ otherwise} \end{cases}$$

Then $S^* = (f_1, f_2, \dots f_n)$ is a basis for V^*.

Remark. Recall $\dim W = m, \dim V = n$,

$$\dim Hom_F(V, W) = mn$$

Proof.
Proof of (1):

$$\dim V^* = \dim Hom_F(V, F)$$
$$= \dim V \times \dim F$$
$$= \dim V$$

Proof of (2): since we know that $\dim V^* = n$, it suffices to show that $S^* = (f_1, f_2, \dots f_n)$ linearly independent in V^*.

We take a linear combination of S^* that gives the 0 functional.

$$a_1 f_1 + a_2 f_2 + \dots + a_n f_n = 0$$

Apply functionals at s_j

$$(a_1 f_1 + a_2 f_2 + \dots + a_n f_n)(s_j) = 0(s_j) = 0$$
$$\implies a_1 f_1(s_j) + a_2 f_2(s_j) + \dots + a_n f_n(s_j) = 0$$
$$\implies a_j f_j s_j = 0$$
$$\implies a_j = 0$$

This is true for all $1 \leq j \leq n$, therefore $S^* = (f_1, f_2, \dots f_n)$ linearly independent. ✓

Definition 14.7. $S^* = (f_1, f_2, \dots f_n)$ from theorem above is called the dual basis of S.
Each f_i is denoted

$$f_i = S_i^*$$

Example. Let $V = F^n$, and $S = (e_1, e_2, \dots e_n)$ is the standard basis where $e_i = (0, 0, \dots 1, \dots, 0)^T$ (only nonzero element is 1 at the i-th position).

Then

$$
\begin{aligned}
e_i^* \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} &= e_i^* \left(\sum_{j=1}^{n} v_j e_j \right) \\
&= \sum_{j=1}^{n} v_j e_i^*(e_j) \\
&= v_i e_i^*(e_i) \\
&= v_i
\end{aligned}
$$

14.2.2 Duality Theorem

Definition 14.8. Since V^* is again a vector space over F. Define the bidual space as

$$V^{**} := (V^*)^* = Hom_F(V^*, F)$$

Remark. If $\dim V < \infty$,

$$\dim(V^{**}) = \dim V^* = \dim V$$

Theorem 14.9. Let V be a finite-dimensional F-vector space. Then, there exists a natural isomorphism

$$\Theta : V \to V^{**} = Hom_F(V^*, F), v \mapsto \theta(v) = \theta_v$$

Where

$$\theta_v(f) = f(v) \text{ for all } f \in V^*$$

i.e. θ_v is an evaluation functional (taking linear functionals to scalars).