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:
   - ($\Longleftarrow$) true by (1)
   - ($\Longrightarrow$) 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:
   - ($\Longleftarrow$) This direction is immediate.
   - ($\Longrightarrow$) 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

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

(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, $\mathcal{P} = \{P : F \to F : P(x) = a_0 + a_1 x + a_2 x^2 \dots, F \subseteq \mathbb{C}\}$ 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
$$a_1 s_1 + \dots a_k s_k + bv = 0$$
Note that $b = 0$. Assume otherwise for contradiction, then
$$bv = -a_1 s_1 - a_2 s_2 \dots - a_k s_k$$
$$v = -\frac{a_1}{b} s_1 - \dots - \frac{a_k}{b} s_k \in span(S)$$
Since $b = 0$,
$$a_1 s_1 + \dots + a_k s_k = 0$$
$$a_1 = \dots = a_n = 0 \quad \text{by linear independence of } s_1, \dots s_n$$
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
$$\sum_{i=1}^{k} a_i s_i = \sum_{i=i}^{k} b_i s_i$$
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

$$ca_1 s_1 + (ca_2 + c_2) s_2 + \ldots (ca_n + c_n) s_n = 0$$

By linearly independence of S,

$$ca_1 = (ca_2 + c_2) = \ldots = (ca_n + c_n) = 0$$

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 $m \leq n$ 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 $m \geq 1$ 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, $m - 1 \leq n$ 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 $m \leq n$. Since we assume that indunction hypothesis is true, $m - 1 \leq n$. This implies either $m = n + 1$ or $m \leq n$.

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 $a_k, m \leq k \leq n$ 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

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

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

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

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): $A \le F^{m\times n}, B \in F^{n\times r}$. 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 $b_1, b_2, \dots b_n \in F, a_{ij} \in F, \forall 1 \le i \le m, 1 \le j \le n$, 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

$$\left(\begin{array}{cccc|c} 1 & & & & b_1 \\ 0 & 1 & & & b_2 \\ & & \ddots & & \vdots \\ 0 & & & 1 & b_r \\ \hline 0 & 0 & \cdots & 0 & b_{r+1} \\ 0 & 0 & \cdots & 0 & \vdots \\ 0 & 0 & \cdots & 0 & b_m \end{array}\right)$$

  - 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

$$\begin{aligned} r &\leq m \\ -r &\geq -m \\ n - r &\geq n - m > 0 \end{aligned}$$

$\tilde{A}x = 0$ 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.
($\Longrightarrow$):

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

($\Longleftarrow$): 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

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

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

$$B=E_kE_{k-1}E_{k-2}\dots E_1A$$

Take

$$P=E_kE_{k-1}E_{k-2}\dots E_1$$

$\Longleftarrow$ Let $B=E_kE_{k-1}\dots E_1A$. Define

$$e_i(A):=E_iA$$

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. Let $A\in Matr_n(F)$

Class 9