MATB24 Lecture Notes

Joshua Concon

University of Toronto Scarborough – Summer 2017

Pre-reqs are MATA23, which is Linear Algebra I. Instructor is Dr. Louis de Thanhoffer de Volcsey. I highly recommend sitting at the front since he likes to teach with the blackboards. If you find any problems in these notes, feel free to contact me at conconjoshua@gmail.com.

Contents

1 Wednesday, May 3, 2017

Before he got to the definition of fields, Dr. Louis de Thanhoffer de Volcsey talked a lot about how MATB24 was simply going to be a generalization of everything in MATA23 and various specific examples of fields as well as practical applications, but since fields were never defined, I will omit all of that stuff since it does not really make any sense without the formal definition of fields.

In the definition of the field, the lecturer presents the unique additive identity as 0, the unique additive inverse as $(-a)$ for a, the unique multiplicative identity as 1, and the unique multiplicative inverse of a as (a^{-1}). Although this is true for fields like $\mathbb{R}$, this is misleading, as the inverses and identities are supposed to be general, and thinking of the additive inverse for example as $(-a)$ is not necessarily true for some fields.

Take for example the field $\mathbb{Z}_2 = \{0, 1\}$ (This is essentially all of $\mathbb{Z}$ but each element a becomes the remainder of $a/2$, so $0, 1, 2, 3, 4, 5$ becomes $0, 1, 0, 1, 0, 1$).

If you consider the case when $a = 1$, the additive inverse of 1 is 1 (i.e. $1 + 1 = 0$). So using the definition of $(-a)$ as the additive inverse in this case is confusing since $(-a) = a = 1$. So in the definition of a field, these are all generalized.

1.1 Fields

Fields

A field ($\mathbb{F}$) is a set with two operations:

- $+ : \mathbb{F} \times \mathbb{F} \longrightarrow \mathbb{F}$
- $\circ : \mathbb{F} \times \mathbb{F} \longrightarrow \mathbb{F}$

And these two operations must satisfy all of the following axioms:
(Axioms are for $\forall a, b, c \in \mathbb{F}$)
Axioms for $+$:

- associative: $(a + b) + c = a + (b + c)$
- commutative: $a + b = b + a$
- (unique) additive identity: $\exists j \in \mathbb{F} : j + a = a$
- (unique) additive inverse: $\exists k \in \mathbb{F} : k + a = j$ where j is the unique additive identity

Axioms for $\circ$:

- associative: $(a \circ b) \circ c = a \circ (b \circ c)$
- commutative: $a \circ b = b \circ a$
- (unique) multiplicative identity: $\exists q \in \mathbb{F} : q \circ a = a$
- (unique) multiplicative inverse: $\exists w \in \mathbb{F} \setminus \{j\} : w \circ a = q$ where q is the unique multiplicative identity and j is the unique additive identity

Axioms for both:

- distributive: $a \circ (b + c) = (a \circ b) + (c \circ a)$

Example 1: Is $\mathbb{Z}$ a field?

Solution 1: No, since $2 \in \mathbb{Z}$ has no multiplicative inverse in $\mathbb{Z}$ (i.e. $\nexists a \in \mathbb{Z} : 2a = 1$), however, $\mathbb{Q}$ is a field and solves this problem.

2 Friday, May 5, 2017

2.1 Vector Spaces

Vector spaces are, in the paraphrased words of the lecturer, "simply the generalization of the real-valued vectors from MATA23". So they are a collection of elements where each element is in a field ($\mathbb{F}$).

The following definition of Vector Spaces is also slightly inconsistent when compared to the lecture and the textbook definition to be more general for reasons provided before (for the definition of a field). Like a single mother who is pulled into a conversation with her child about the missing paternal figure, I would prefer to just tell a more truthful definition now that may be more abstract and slightly harder to understand in order to be more consistent, rather than clearing up disinformation later.

Vector Spaces

A Vector Space over the field $\mathbb{F}$ is a set V with the following operations:

- $+ : V \times V \longrightarrow V$ (vector addition)
- $\circ : \mathbb{F} \times V \longrightarrow V$ (scalar multiplication)

And these two operations must satisfy all of the following axioms:
(axioms are for $\forall v, w, u \in V$ and $\forall a, b \in \mathbb{F}$)
Axioms for $+$:

- associative: $(v + w) + u = v + (w + u)$
- commutative: $v + w = w + v$
- existence of the zero vector: $\exists n \in V : n + v = v$ (n must also be unique)
- existence of the inverse vector: $\exists b \in V : b + v = n$ where n is the zero vector and b is unique for each vector v.

Axioms for $\circ$:

- associative: $(ab) \circ v = a \circ (b \circ v)$
- preservation of scale: $\exists j \in \mathbb{F} : j \circ v = v$ (j is usually 1 here)

Axioms for both:

- distributive: $(a + b) \circ v = (a \circ v) + (b \circ v)$
  $a \circ (v + w) = (a \circ v) + (a \circ w)$

Example 1: Prove the distributive axiom for $\mathbb{F}^n$ which is a vector space over $\mathbb{F}$ with operations $(+, \circ)$ from the real numbers ($\mathbb{R}$) and:

- $v = (v_1, ..., v_n) \in \mathbb{F}^n$
- $w = (w_1, ..., w_n) \in \mathbb{F}^n$
- $a, b \in \mathbb{F}$

Solution 1: Since we are using the $(+, \circ)$ operations from the real numbers, then we know that...

- $v + w = (v_1 + w_1, ..., v_n + w_n)$
- $a \circ v = (a \circ v_1, ..., a \circ v_n)$

Consider $a \circ (v + w)$

$$\begin{aligned} a \circ (v + w) &= a \circ (v_1 + w_1, ..., v_n + w_n) \\ &= (a \circ (v_1 + w_1), ..., a \circ (v_n + w_n)) \\ &= ((a \circ v_1) + (a \circ w_1), ..., (a \circ v_n) + (a \circ w_n)) \\ &= ((a \circ v_1) + ... + (a \circ v_n)) + ((a \circ w_1) + ... + (a \circ w_n)) \\ &= (a \circ (v_1, ..., v_n)) + (a \circ (w_1, ..., w_n)) \\ &= (a \circ v) + (a \circ w) \end{aligned}$$

Consider $(a + b) \circ v$

$$\begin{aligned} (a + b) \circ v &= (v_1, ..., v_n) \\ &= (((a + b) \circ v_1), ..., ((a + b) \circ v_n)) \\ &= ((a \circ v_1) + (b \circ v_1), ..., (a \circ v_n) + (b \circ v_n)) \\ &= ((a \circ v_1), ..., (a \circ v_n)) + ((b \circ v_1), ..., (b \circ v_n)) \\ &= (a \circ (v_1, ..., v_n)) + (b \circ (v_1, ..., v_n)) \\ &= (a \circ v) + (b \circ v) \end{aligned}$$

Example 2: $\mathbb{M}_{k,l}(\mathbb{F})$ which is all $k \times l$ matrices with coefficients in $\mathbb{F}$.
This is also field, for example:
($\forall M, N \in \mathbb{M}_{k,l}(\mathbb{F})$, $\forall a \in \mathbb{F}$ and $\forall i, j : 1 \leq i \leq k, 1 \leq j \leq l$)

- $M + N = (M + N)$ where $(M + N)_{ij} = M_{ij} + N_{ij}$ (ij^{th} entry addition)
- 0 is the zero matrix where $0_{ij} = 0$
- $a \circ M = (aM)$ where $(aM)_{ij} = a(M_{ij})$ (scalar multiplication)
- $M + (-M) = 0$ where $(-M)_{ij} = -(M_{ij})$ (existence of the inverse vector)

Example 3: $\mathbb{M}^1_{k,l}(\mathbb{F})$ (all $k \times l$ matrices with coefficients in $\mathbb{F}$ and $\forall M \in \mathbb{M}^1_{k,l}(\mathbb{F})$, $M_{1,1} = 1$)

This is not a Vector Space because scalar multiplication does not work if

the scalar being multiplied by is not 1. (i.e. if $a \neq 1$ then $a(M_{1,1}) = a \neq 1$)

Example 4: $\mathbb{M}^0_{k,l}(\mathbb{F})$ however, is a vector space, since
$\forall a \in \mathbb{F}$ and $\forall M \in \mathbb{M}^0_{k,l}(\mathbb{F})$, that $a(M_{1,1}) = a \cdot 0 = 0$.

Example 5: $P(\mathbb{F})$ which is all the polynomials over the field $\mathbb{F}$, defined by:

$$P(\mathbb{F}) = \langle \sum_{i=1}^{n} \alpha_i \cdot x^i \rangle$$

This is also a Vector Space, here are some examples of how the operations work.

- $\sum_{i=1}^{n} \alpha_i \cdot x^i + \sum_{i=1}^{n} \beta_i \cdot x^i = \sum_{i=1}^{n} (\alpha_i + \beta_i) \cdot x^i$ (vector addition)
- $\gamma \sum_{i=1}^{n} \alpha_i \cdot x^i = \sum_{i=1}^{n} (\gamma \alpha_i) \cdot x^i$ (scalar multiplication)

Example 6: Take any set X, V is a vector space over $\mathbb{F}$
$V^X = \{functions : X \longrightarrow V\}$ is a vector space over $\mathbb{F}$
Consider $f, g \in V^X$, $\forall \alpha \in \mathbb{F}$

$$(f + g)(x) = f(x) + g(x)$$

3 Wednesday, May 10, 2017

3.1 Basics of Vector Spaces

Basic Example of a Vector Space: $\mathbb{F}^n$

Definition: Subspace

A subspace W of a vector space V is a non-empty subset of V with the following axioms:

- $\forall w_1, w_2 \in W : w_1 + w_2 \in W$
- $\forall \alpha \in \mathbb{F}, w \in W : \alpha \cdot w \in W$

Example 1: Is $P(\mathbb{F}) = \{\sum_{i=0}^{\infty} \alpha_i \cdot x^i : \alpha_i \in \mathbb{F}\}$ a subspace?

Solution 1: $0 \in P(\mathbb{F})$, therefore $P(\mathbb{F})$ is non-empty.

Consider $\forall w, v \in P(\mathbb{F})$ and $\forall r \in \mathbb{F}$
where $w = \sum_{i=0}^{\infty} w_i \cdot x^i$ and $v = \sum_{i=0}^{\infty} v_i \cdot x^i$

$$w + w = \sum_{i=0}^{\infty} w_i \cdot x^i + \sum_{i=0}^{\infty} v_i \cdot x^i = \sum_{i=0}^{\infty} (w_i + v_i) \cdot x^i \in P(\mathbb{F})$$

$$rw = r \sum_{i=0}^{\infty} w_i \cdot x^i = \sum_{i=0}^{\infty} (r \cdot w_i) \cdot x^i \in P(\mathbb{F})$$

Therefore $P(\mathbb{F})$ is a subspace

Example 2: Is $P_n(\mathbb{F}) = \{\sum_{i=0}^{\infty} \alpha_i \cdot x^i : \alpha_i \in \mathbb{F}, \text{ degree} = n\}$ a subspace?

Solution 2: Consider $1 + 2x + 3x^2, -3x^2 \in P_2(\mathbb{F})$

$$1 + 2x + 3x^2 + (-3x^2) = 1 + 2x \text{ which is not in } P_2(\mathbb{F})$$

Therefore $P_n(\mathbb{F})$ is not a vector space.

Note: The easiest way to check if something (V) is not a vector space is to check if $0 \in V$.

Example 3: Are all matrices A with $det(A) = 0$

Solution 3: Consider $UT_n(\mathbb{F}) = \{M \in M_{m,n}(\mathbb{F}) | M_{ij} = 0, i \geq j\}$
Take $M_1, M_2 \in UT_n(\mathbb{F})$

$$(M_1 + M_2)_{ij} = M_{1ij} + M_{2ij} = 0 + 0 = 0, \forall i, j$$
$$\forall \alpha \in \mathbb{F} : (\alpha M)_{ij} = \alpha(M_{ij}) = \alpha \cdot 0 = 0$$

Therefore $UT_n(\mathbb{F})$ is a subspace.

3.2 Operations on Subspaces

Considering subspaces U, W of a vector space V

- $(U \cap W) = \{v \in V : v \in U, v \in W\}$ is a subspace
- $(U + W) = \{u + w : u \in U, w \in W\}$ is also a subspace
- However, $(U \cup W)$ is not a subspace because of the following example: Consider in $P(\mathbb{F})$ the subspaces $U = \{\alpha x : \alpha \in \mathbb{F}\}$ and $W = \{\alpha x^2 : \alpha \in \mathbb{F}\}$ and $U \cup W$ is not a subspace since it does not contain $x + x^2$, and so is not closed under vector addition.

Recall: if $v_1, ..., v_n$ is a basis, then all vectors are of the form $\sum_i \alpha_i v_i$

- $sp\{v_1, ..., v_n\} = \{\sum_i \alpha_i v_i : \alpha_i \in \mathbb{F}\}$

Result: $sp(v_1, ..., v_n)$ is the smallest subspace containing $\{v_1, ..., v_n\}$

Proof. (Proof of Result)
Take $u, w \in sp(v_1, ..., v_n)$, so $u = \sum_i \alpha_i v_i, w = \sum_i \beta_i v_i$
so this implies that $u + w = \sum_i \alpha_i v_i + \sum_i \beta_i v_i = \sum_i (\beta_i + \alpha_i) v_i$.
And Taking a $\gamma \in \mathbb{F} : \gamma u = \gamma \sum_i \alpha_i v_i = \sum_i (\alpha_i \cdot \gamma) v_i$
So now we assume W is the subspace containing $\{v_1, ..., v_n\}$

$$\longrightarrow \forall \alpha \in \mathbb{F}, \alpha_i x_i \in W$$
$$\longrightarrow sp\{v_1, ..., v_n\} \in W$$

so $sp\{v_1, ..., v_n\}$ is the smallest subspace containing $\{v_1, ..., v_n\}$ since for every subspace W containing $\{v_1, ..., v_n\}$, they must also contain $sp\{v_1, ..., v_n\}$ ■

Example 4: $sp\{1, 1+x, x^2-1\} \in P(\mathbb{F})$?

Solution 4: A good war to check if a set is a subspace is to write the subspace as a span.

$$\begin{aligned} sp\{1, 1+x, x^2-1\} &= a + b(1+x) + c(x^2-1) | a, b, c \in \mathbb{F} \\ &= (a+b-c) + bx + cx^2 | a, b, c \in \mathbb{F} \\ &= P_{\leq 2}(\mathbb{F}) \in P(\mathbb{F}) \end{aligned}$$

Example 5: $sp\{e_1, e_2\} = sp\{(1,0),(0,1)\} \in M_{m,n}(\mathbb{F})$

E_{ij} has a coefficient of 0 everywhere except for a coefficient of 1 in entry (i, j)

Note:

$$\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = aE_{11} + bE_{12} + cE_{21}dE_{22}$$

Example 5:

$$\begin{aligned} sp\{v_1, v_2, v_1+v_2\} &= av_1 + bv_2 + c(v_1+v_2) | a, b, c \in \mathbb{F} \\ &= (a+c)v_1 + (b+c)v_2 | a, b, c \in \mathbb{F} \\ &= sp\{v_1, v_2\} \end{aligned}$$

So when do we know that we have the minimum amount of terms to generate a Vector Space from a span of these terms?

Definition: Linearly Dependent

A vector V is **linearly dependent** of vectors $\{v_1, ..., v_n\}$ if it is a linear combination of them.

So if $v = (v_1, ..., v_n)$ is linearly dependent of $\{u_1, ..., u_n\}$ then

$$sp\{v_1, ..., v_n\} = sp\{u_1, ..., u_n\}$$

A set of vectors is linearly independent if no vector is linearly dependent on the other vectors in the set.

Fact: a set is linearly independent if $\sum_i a_i v_i = 0 \longrightarrow \forall a_i = 0$

Proof. Assume $\sum_i a_i v_i = 0 \longrightarrow \forall a_i = 0$ and that some vector

$$v_i = \sum_{j \neq i} a_j v_j, u_0 = \sum_{j=0} a_j v_j$$

$$|v_0 - a_1 v_1 - a_2 v_2 - ... - a_n v_n| = 0$$

Assume that $\sum_i a_i v_i = 0$ (linearly independence)
Assume that for some coefficient is not 0, say $a_1 \neq 0$.

$$a_1 v_1 + \sum_{i \geq 2} a_i v_i = 0, v_1 = \sum_{i \geq 2} (\frac{-a_i}{a_1}) v_i$$

This shows that v_1 is a linear combination of the other vectors, which violates our assumption that all these vectors v_i are linearly independent. So it must be the case that $\sum_i a_i v_i = 0, \forall a_i = 0$ implies linear independence ■

4 Friday, May 12, 2017

4.1 Bases of Vector Spaces

Definition: A Basis of Vector Spaces

A basis for V is a spanning set that is linearly independent

Result: A spanning set $\{v_1, ..., v_n\}$ for V is a basis $\iff \forall v, \exists a_i, v = \sum_{i=1}^{n} a_i v_i$

Proof. (Proof of Result)
Proof of $\longrightarrow$
$\forall v, \exists a_i, v = \sum_{i=1}^{n} a_i v_i$, so since every vector v can be made with the vectors $\{v_1, ..., v_n\}$, so this is a basis.

Proof of $\longleftarrow$
For this, we need to show uniqueness. Consider $v = \sum_{i=1}^{n} b_i v_i$

$$\begin{aligned} v = \sum_{i=1}^{n} b_i v_i &\longrightarrow 0 = \sum_{i=1}^{n} (a_i - b_i) v_i \\ &\longrightarrow a_i - b_i = 0 \\ &\longrightarrow a_i = b_i \end{aligned}$$

Since these vectors are unique, this basis is unique, so every vector in V can be formed by a linear combination of these unique vectors. ■

Corollary: Assume we have a finite basis of size n.
Define a function

$$\{v_1, ..., v_n\} : V \mapsto \mathbb{F}^n, v \mapsto (a_1, ..., a_n) \text{ such that } v = \sum a_i v_i$$

These are the coordinates of the vector v with respect to the basis $\{v_1, ..., v_n\}$

1. Every vector space has a basis, sometimes, this basis can be mysterious, such as:
   $\mathbb{R}^{\mathbb{R}}$, which does not have a basis that can be written.

   More precisely: every spanning set becomes a basis after removing linearly dependent vectors.

Corollary: Consider spanning set $A = \{v_1, ..., v_n\}$ and basis $B = \{w_1, ..., w_n\}$.
A being a spanning set implies $m \leq n$. B being a basis implies that $n \leq m$. Both of these imply that $n = m$

2. Bases a Vector Space V always have the same number of elements between other bases of V.

Definition: Dimension

The number of elements in the basis of a Vector Space V is called the dimension of V.

Example 1: $\mathbb{F}^n = [e_1, ..., e_n]$ is a basis.
$\forall v \in V$ where V is a Vector Space. $v = (v_1, ..., v_n) = \sum_{i=1}^{n} v_i \cdot e_i$

Corollary: Any set of n linearly independent vectors is a basis, and every vector can be represented as such:

$$\mathbb{F} \mapsto \mathbb{F}^n : v \mapsto (v_1, ..., v_n)$$

Consider $M_{m,n}(\mathbb{F})$ elementary matrices, where $E_{i,j}$ has 0 in all of it's entries except for a 1 at position (i, j).

Basis for $M_{m,n}(\mathbb{F})$: