Linear Algebra done Horribly

Sabarno Saha
sabarnohere@gmail.com
IISERK

Contents

1 Introduction

This is small concise set of notes from the MA2102: Linear Algebra course taught at IISERK. This course was taught by Dr. Soumya Bhattacharya.

We will start from the basic definitions of groups and fields, and then build up to the definition of a **Vector Space**. In Vector spaces we talk about , basis vectors, Direct sums and different theorems most importantly the **rank nullity theorem**. Then we move on to Linear Transformations. After thar we move onto the concept of invariant subspaces and everything-eigen i.e. eigen vectors and eigenvalues. Then we move onto the concept of Dual spaces, which is pretty important in context of QMech. From there we move onto bilinear operators, of which we will be studying the dot and the hermitian product in detail. The final topic of this will be the spectral theorem, which gives us a very powerful way to diagonalize matrices.

1.1 What we will cover

- Vector Spaces
- Linear Operators
- Dual Spaces
- Bilinear Operators
- **The Final Boss:** The Spectral Theorem

1.2 References

- Algebra by Michael Artin
- Introduction to Linear Algebra by Hoffman and Kunze
- Linear Algebra done right by Sheldon Axler(The fourth edition has a public access E-book)

2 Algebraic Jiu-Jitsu

Definition 2.1 (Binary operation): A binary operation is a map from $f : S \times S \to S$, and f is defined to be a **binary operator**.

Definition 2.2 (Group):

A set S with a binary operation $\circledast$ is a group $\mathrm{G} = (S, \circledast)$ if it satisfies the following axioms:

1. **Assosciativity**
   $a \circledast (b \circledast c) = (a \circledast b) \circledast c \ \forall \ a, b, c \in S$
2. **Identity**
   $\exists i_s \in S$ s.t. $\forall s \in S$
   $$a \circledast i_s = i_s \circledast a = a$$
3. **Inverse**
   $\forall \ a \in S \ \exists \ b \in S$
   $$a \circledast b = b \circledast a = i_s$$

Definition 2.3 (Subgroup): Let $(G, \circledast)$ be a group. If $(H, \circledast)$ is a group and $H \subset G$, then $(H, \circledast)$ is asubgroup of $(G, \circledast)$.

Theorem 2.1:

Every group has a unique identity operator.

Proof: Let $(G, \circledast)$ be a group. Let $i_g, j_g \in G$ be two identity operators of the group. We have $i_g = i_g \circledast j_g = j_g$ by definition. Thus $i_g = j_g$. Thus the identity operator is unique. $\square$

Theorem 2.2 (Unique Inverse):
Let $(G, \circledast)$ be a group. Let $a \in G$. Then a has a unique inverse.

Proof: We have $a \in G$. Let there be two inverses of a, $b, c \in G$. Thus $a \circledast b = b \circledast c = i_g$ and $a \circledast c = c \circledast a = i_g$ where $i_g \in G$ is the identity in G. Then we have

$$b = b \circledast i_g = b \circledast (a \circledast c) = (b \circledast a) \circledast c = i_g \circledast c = c$$

Thus $b = c$ i.e. the inverse of $a \in G$ is unique. $\square$

Definition 2.4 (Abelian Group): Let $(G, \circledast)$ be a group, s.t. $a, b \in G$. If $a \circledast b = b \circledast a$, then we say that $\circledast$ is a commutative operator, and $(G, \circledast)$ is a commutative or an **abelian group**

Definition 2.5 (Semigroup): A set S with a binary operation $\circledast$ is a semigroup G = $(S, \circledast)$ if **Assosciativity** is satisfied.

Definition 2.6 (Monoid): Let $(S, \circledast)$ be a semigroup. If S has an identity element, then $(S, \circledast)$ is a monoid.

Definition 2.7 (Ring):

A set R with binary operations $+, *$ is called a ring $(R, +, *)$ if it satisfies the following axioms:
1. $(R, +)$ is an abelian group.
2. $(R, *)$ is a monoid.
3. $*$ is distributive over $+$
   $a * (b + c) = a * b + a * c$ and $(b + c) * a = b * a + c * a$

Definition 2.8 (Commutative Ring): A ring $(R, +, *)$ is a commutative ring if $*$ is a commutative operator.

Definition 2.9 (Field):

A commutative ring $(F, +, *)$ is a field is $F^* := (F \setminus \{0\}, *)$ is also an abelian group, where $0 \in F$ is the identity operator of the group $(F, +)$

2.1 Deinition of a Vector Space

Whew, that was a whole lot of jargon. Now, after the whole jiu-jitsu routine is over, we can finally define what we want to actually define what a **Vector Space** is.

Definition 2.1.1 (Vector Space):
A vector space $\mathbb{V}$ is a non-empty set defined over a field $\mathbb{F}$ with a binary operation $+$ and a binary function $\cdot$ such that

1. The binary operation, called vector addition or simply addition assigns to any two vectors $v, w \in V$ a third vector in $\mathbb{V}$ which is commonly written as $v + w$, and called the sum of these two vectors.
2. The binary function, called scalar multiplication,assigns to any scalar $a \in \mathbb{F}$ and any vector $v \in \mathbb{V}$, another vector in $\mathbb{V}$, which is denoted $a \cdot v$.

The definition above is from wikipedia. I got bored of defining stuff, so I copied this one . However, we can alternately redefine vector spaces without explicitly defining the previous definitions, given below. I prefer the above method of defining, as it breaks up the definitions into smaller definitions, and makes us familiar with commonly used structures in algebra.

Definition 2.1.2 (Vector Space): Alternate but ultimately the same definition

Let $\mathbb{F}$ be a field, and let V be a set. Then $(V, +, \cdot)$ is a vector space over F if and only if the following axioms hold:

1. **Closure under addition:** For all u, $v \in V$, $u + v \in V$.
2. **Commutativity of addition:** For all u, $v \in V$, $u + v = v + u$.
3. **Associativity of addition:** For all u, v, $w \in V$, $(u + v) + w = u + (v + w)$.
4. **Existence of zero vector:** There exists an element $0 \in V$ such that for all $v \in V$, $v + 0 = v$.
5. **Existence of additive inverses:** For all $v \in V$, there exists an element $-v \in V$ such that $v + (-v) = 0$.
6. **Scalar multiplication by 1:** For all $v \in V$, $1 \cdot v = v$, where 1 is the multiplicative identity of $\mathbb{F}$.
7. **Distributive property over addition:** For all a, $b \in \mathbb{F}$ and $v \in V$, $a(v + w) = (a \cdot v) + (a \cdot w)$.
8. **Distributive property over scalar addition:** For all a, $b \in \mathbb{F}$ and $v \in V$, $(a + b) \cdot v = (a \cdot v) + (b \cdot v)$.

We finally end the part where we have to define a lot of algebraic structures, but they lead to some fun discussions. From here, armed with the defintion of vector spaces we move forward with our crusade into Linear Algebra, by exploring certain properties of Vector spaces.

3 Vectors Spaces

Definition 3.1 (Subspace):

Let $\mathbb{V}$ be a vector space over a field $\mathbb{F}$. Let $W \subset \mathbb{V}$. If $\forall\ w, w' \in W$ we have $aw + bw' \in W\ \forall a, b \in \mathbb{F}$, then W is a subspace of $\mathbb{V}$

A comment on Notation:

We are representing vectors spaces with $\mathbb{V}$ which is notation for $\mathbb{V} := (V, +, \odot)$ where $+$ is the binary operation and $\odot$ is the binary function called scalar multiplication. Whenever we write $W \subset \mathbb{V}$, we mean $W \subset V$. Same goes for elements of the vector space. When we write $w \in \mathbb{V}$, we mean w is an element of the underlying set V.

Definition 3.2 (Span):

Let $s = \{v_1, v_2, ..., v_n\}$ be a set of vectors. Then the span of s denoted by span(s) is defined to be

$$\text{span}(s) = \{c_1 v_1 + c_2 v_2 + ... + c_n, v_n | \forall\ c_1, c_2, ..., c_n \in \mathbb{F}\}$$

Proposition 3.1:

Let $\mathbb{V}$ be a vector space over a field $\mathbb{F}$ and $\mathbb{W}$ be a subspace. Let $S \subset \mathbb{V}$ such that $S \subset \mathbb{W}$. Then span$(S) \subset \mathbb{W}$.

Proof: We proceed by induction. Let $s = \{v_1, v_2, ..., v_n\}$
Base Case(n=2)
Given $v_1, v_2 \in \mathbb{W}$, from the definition of a subspace, we have $c_1 v_1 + c_2 v_2 \in \mathbb{W}\ \forall c_1, c_2 \in \mathbb{F}$. Thus span$(\{v_1, v_2\}) \subset \mathbb{W}$.
Induction Hypothesis
Assume that $c_1 v_1 + c_2 v_2 + ... + c_n v_n \in \mathbb{W}$. We need to show that $c_1 v_1 + c_2 v_2 + ... + c_{n+1} v_{n+1} \in \mathbb{W}$. Let $\lambda = c_1 v_1 + c_2 v_2 + ... + c_n v_n$. We have $c_1 v_1 + c_2 v_2 + ... + c_{n+1} v_{n+1} = \lambda + c_{n+1} v_{n+1} \in \mathbb{W}$ using our base case. Thus we have shown span$(s) \subset \mathbb{W}$.

$\square$

Proposition 3.2: Given a subset $S \subset \mathbb{V}$. span(S) is a subspace of $\mathbb{V}$.

Proof:

Let $S = \{v_1, v_2, ..., v_n\}$ Let $w, w' \in$ span(S). Thus $\exists a_1, a_2, ..., a_n \in \mathbb{F}$ and $\exists b_1, b_2, ..., b_n \in \mathbb{F}$ s.t. $w = a_1 v_1 + a_2 v_2 + ... + a_n v_n$ and $w' = b_1 v_1 + b_2 v_2 + ... + b_n v_n$. Let $\alpha, \beta \in \mathbb{F}$.

$$\begin{aligned}
\alpha w + \beta w' &= \alpha(a_1 v_1 + ... + a_n v_n) + \beta(b_1 v_1 + ... + b_n v_n) \\
&= \sum_{i=1}^{n} (\alpha a_i + \beta b_i) v_i \\
&= \sum_{i=1}^{n} c_i v_i \qquad (\text{where } c_i = (\alpha a_i + \beta b_i) v_i\ )
\end{aligned}$$

Thus $\alpha w + \beta w' = \sum_{i=1}^{n} c_i v_i \in \text{span}(S)$. Thus span$(S)$ is subspace of $\mathbb{V}$. □

Definition 3.3 (Linear Relation):

Let $v_1, ..., v_n \in \mathbb{V}$. If $\exists\ c_1, ..., c_n \in \mathbb{F}$ s.t. not all c_i's are zero and if $c_1 v_1 + ... + c_n v_n = 0$. We call this a **linear relation** among the given set of vectors.

Definition 3.4 (Linear Independence):

Let $v_1, ..., v_n \in \mathbb{V}$. If $\nexists$ any linear relation among $v_1, ..., v_n$. We say that the set of vectors are **linearly independent**.

(Rephrased)

Let $v_1, ..., v_n \in \mathbb{V}$. Then if for $c_1, ..., c_n \in \mathbb{F}$

$$c_1 v_1 + ... + c_n v_n \Rightarrow c_1 = c_2 = ... = c_n = 0$$

Then $v_1, ..., v_n$ are linearly independent.

Definition 3.5 (Basis):

A linearly independent ordered set of vectors that span a vector space is called a basis.

One small convention necessary for the next theorem. We take span(ϕ) =$\{0\}$

Proposition 3.3: Let $\mathbb{V}$ be any vector space with a basis $\mathbb{B} := (v_1, v_2, ..., v_n)$. Then every vector in $\mathbb{V}$ has a **unique** expression of the form

$$c_1 v_1 + ... + c_n v_n$$

where $c_1, ..., c_n \in \mathbb{F}$.

Proof: Suppose $\exists v \in \mathbb{V}$ such that there exists two expressions of the form $v = c_1 v_1 + ... + c_n v_n$ and $v = d_1 v_1 + ... + d_n v_n$. Then we have

$$\begin{aligned} v - v = c_1 v_1 + ... + c_n v_n - (d_1 v_1 + ... + d_n v_n) &= 0 \\ \Rightarrow (c_1 - d_1) v_1 + ... + (c_n - d_n) v_n &= 0 \\ \text{Since } \ v_1, ..., v_n \text{ is a linearly independent set} \\ \Rightarrow c_i - d_i = 0 \ \forall \ i \in \mathbb{N}_n \\ \Rightarrow c_i = d_i \end{aligned}$$

Thus two expressions are the same. Thus we have a unique expression of v using $\mathbb{B}$. □

Proposition 3.4:

Let $\mathbb{V}$ be a vector space and let $S \subset \mathbb{V}$ be an ordered set of vectors. Let $v \in \mathbb{V}$ be any vector. Define $S' := (S, v) := (v_1, ..., v_n, v)$ where $S = (v_1, ..., v_n)$. Then we have

$$v \in \text{span } (S) \Longleftrightarrow \text{span } (S) = \text{span } (S')$$

Proof: $(\Longrightarrow)$ Given $v \in \text{span}(S)$ and $S' = (S, v)$ □

Proposition 3.5:

Let $L = (v_1, ..., v_n)$ be a linearly independent set and let $v \in A$ be any vector. Then the set $L' = (L, v)$ is a linearly independent set $\Longleftrightarrow v \notin \text{span}(L)$.

Proof: We will prove the contrapositive i.e. $v \in \text{span } (L) \Longleftrightarrow L'$is a linearly dependent set
$(\Longrightarrow)$
We know $v \in \text{span}(L)$. Thus $\exists \ c_1, c_2, ..., c_n \in \mathbb{F}$ s.t.

$$\begin{aligned} c_1 v_1 + ... + c_n v_n = v \\ c_1 v_1 + ... + c_n v_n - v = 0 \end{aligned}$$

Since coefficient of v is -1, we have a linear relation among L and v. L' is a linearly dependent set.

$(\Longleftarrow)$
L' is a linearly dependent set. Thus $\exists c_1, ..., c_n, c_{n+1} \in \mathbb{F}$ and $\exists c_i, c_i \neq 0$ s.t.

$$c_1 v_1 + ... + c_n v_n + c_{n+1} v_{n+1} = 0$$

Now $c_{n+1} \neq 0$ or $c_{n+1} = 0$.

<u>Case 1:</u> $c_{n+1} = 0$
Since $c_{n+1} = 0$, then we have

$$c_1 v_1 + ... + c_n v_n = 0$$

But we know that L is an linearly independent set, thus $c_1 = c_2 = ... = c_n = 0$. But $\exists c_i \neq 0$. Thus $c_{n+1} \neq 0$.

<u>Case 2:</u> $c_{n+1} \neq 0$
We thus have,

$$
\begin{aligned}
& c_1 v_1 + \ldots + c_n v_n + c_{n+1} v_{n+1} = 0 \\
\implies & v = -\frac{1}{c_{n+1}}(c_1 v_1 + \ldots + c_n v_n) \\
\implies & v = d_1 v_1 + \ldots + d_n v_n
\end{aligned}
$$

Thus $v \in \text{span}(L)$.

□

Definition 3.6 (Finite Dimensional Vector spaces):

Every vector space $\mathbb{V}$ over a field $\mathbb{F}$, that has spanning set with a finite number of elements is called a Finite Dimensional Vector Space.

Proposition 3.6:

Let $\mathbb{V}$ be a finite dimensional vector spaces and let S be a finite and ordered set that spans $\mathbb{V}$. Then S contains a basis of $\mathbb{V}$.

Proof:

Let $S := \{v_1, v_2, ..., v_n\}$. If L is linearly independent, we are done. If not $\exists$ a linear relation among the elements. Thus $\exists c_1, ..., c_n \in \mathbb{F}$ and for some $k, c_k \neq 0$. Thus

$$
v = -\frac{c_1}{c_k} v_1 - \ldots - \frac{c_n}{c_k} v_k
$$

Let $S' := S \setminus \{v_k\}$. Then $v \in \text{span}(S')$. By propostion 3.4, $\text{span}(S) = \text{span}(S') = \mathbb{V}$ Thus we keep repeating this process until we obtain a linearly independent list that still spans $\mathbb{V}$. Thus we can reduce the entire spanning set to a basis $\mathbb{B}$ of $\mathbb{V}$. □

Proposition 3.7:

Let $\mathbb{V}$ be a finite dimensional vector space. Then any linearly independent subset $L \subset \mathbb{V}$ is extendable to a basis of $\mathbb{V}$.

Proof:

We know that $\mathbb{V}$ is finite dimensional. $\exists$ a finite set S s.t. $\text{span}(S) = \mathbb{V}$. If $S \subset L$, then we have $\text{span}(S) \subset \text{span}(L)$. We also have $\text{span}(L) \subset \mathbb{V}$

$$
\begin{aligned}
& \text{span }(S) = \mathbb{V} \\
& \text{span }(L) \subset \mathbb{V} \\
& \text{span }(S) \subset \text{span }(L) \\
& \implies \mathbb{V} \subset \text{span }(L)
\end{aligned}
$$

Thus $\text{span}(L) = \mathbb{V}$. Thus L is a basis $\mathbb{B}$.

Otherwise, $\mathrm{span}(L) \subset \mathrm{span}(S)$. Then $\exists v \in S\ s.t. v \notin \mathrm{span}(L)$. Let us then define $L' := (L, v)$. Since $v \notin \mathrm{span}(L)$, L' is a linearly independent set as well by proposition 3.5. The list will terminate as we have finite dimensional spanning set, after a certain point $\mathrm{span}(L_{\text{new}}) = \mathbb{V}$. □

Proposition 3.8:

Let S and L be two finite subsets of a vector space $\mathbb{V}$ s.t. $\mathrm{span}(S) = \mathbb{V}$ and L is linearly independent.Then $|L| \leq |S|$.

Proof:

Let $|S| = m$ and $|L| = n$ and let $S := (v_1, ..., v_m)$ and $L := (w_1, ..., w_n)$ □

4 Linear Maps

5 Everything Eigen

6 Dual Basis

7 Bilinear Forms

8 The Final Boss: The Spectral Theorem

9 Bibliography