Mathematical Preliminaries

Nilanjan Chakraborty

February 6, 2018

1 Introduction

In this document, we will go over some mathematical preliminaries required for this course. We will cover the notions of group, field, vector spaces and subspaces, matrices as linear operators, and the fundamental subspaces associated with a matrix.

2 Group

A set G together with a binary operation, denoted by $\circ$, defined on elements of G is called a group if it satisfies the following properties:

1. *Closure* : If $g_1, g_2 \in G$, then $g_1 \circ g_2 \in G$.
2. *Identity* : $\exists$ an identity element, e, such that $g \circ e = e \circ g = g \ \forall \ g \in G$.
3. *Inverse* : For each $g \in G$, there exists a unique $g^{-1} \in G$ such that $g \circ g^{-1} = g^{-1} \circ g = e$.
4. *Associativity* : If $g_1, g_2, g_3 \in G$, then $(g_1 \circ g_2) \circ g_3 = g_1 \circ (g_2 \circ g_3)$.

2.1 Common Examples of Groups

1. Set of real numbers, $\mathbb{R}$ with the binary operation of addition is a group with 0 as the identity element, and negative as the inverse.
2. Set of real numbers, $\mathbb{R}$ with the binary operation of multiplication is a group with 1 as the identity element, and the reciprocal as the inverse.
3. The set of all rotation matrices in three-dimensional space, i.e., $SO(3)$, with matrix multiplication as the binary operation forms a group, with the (3×3) identity matrix I as the identity element.
4. The set of all planar rotation matrices, i.e., $SO(2)$, with matrix multiplication as the binary operation forms a group, with the (2×2) identity matrix I as the identity element.
5. The set of all rigid body transformations, i.e., $SE(3)$, with matrix multiplication as the binary operation forms a group, with the (4×4) identity matrix I as the identity element.

3 Field

A set F together with two binary operations denoted by $+$ and $\cdot$ (read as addition and multiplication) is called a field if the following are satisfied.

1. The set F along with the operation $+$ forms a group. The additive identity is denoted by 0 and the additive inverse is denoted by $-x$, $\forall x \in F$.

2. The set F along with the operation $\cdot$ forms a group. The multiplicative identity is denoted by 1 and the multiplicative inverse is denoted by x^{-1}, $\forall x \in F$.

3. Multiplication distributes over addition, i.e.,

$$x \cdot (y + z) = x \cdot y + x \cdot z, \quad \forall x, y, z \in F$$

Note that there are a total of nine conditions that needs to be satisfied for a set to be a field. Each of the first two points above consists of four conditions. *The elements of a field are called scalars.*

Examples of Field;

- Set of real numbers $\mathbb{R}$ with the usual definition of addition and multiplication.

- Set of complex numbers $\mathbb{C}$ with the usual definition of addition and multiplication for complex numbers.

4 Vector Space

A vector space, V, over the field F, (sometimes written as $V(F)$), consists of a set of objects called *vectors*, that takes values in F and two operations called vector addition and scalar multiplication such that the following are satisfied:

1. Closure: $(\alpha + \beta) \in V$ and $c\alpha \in V$, $\forall$ $\alpha, \beta \in V$ and $c \in F$. (Note that $c\alpha$ is the multiplication of scalar c with vector α)

2. Addition is commutative, i.e., $\alpha + \beta = \beta + \alpha$, $\alpha, \beta \in V$.

3. Addition is associative, i.e., $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$, $\alpha, \beta, \gamma \in V$.

4. Additive Identity: There exits an element, denoted by 0 in V, such that $\alpha + 0 = \alpha$, $\forall$ $\alpha \in V$.

5. Additive Inverse: There exits an element, denoted by $-\alpha$ in V, such that $\alpha + (-\alpha) = 0$, $\forall$ $\alpha \in V$.

6. Multiplicative Identity: There exists an element $1 \in F$ such that $1\alpha = \alpha$, $\forall \alpha \in V$.

7. $(c_1 c_2)\alpha = c_1(c_2\alpha)$, $\forall c_1, c_2 \in F.\alpha \in V$.

8. $c(\alpha + \beta) = c\alpha + c\beta$, $\forall c \in F, \alpha, \beta \in V$.

9. $(c_1 + c_2)\alpha = c_1\alpha + c_2\alpha)$, $\forall c_1, c_2 \in F.\alpha \in V$.

Example 1: Let the set of real numbers, $\mathbb{R}$, be the field F. The set $V = \mathbb{R} \times \mathbb{R} \times \cdots \times \mathbb{R}$ (n times), denoted by $\mathbb{R}^n$ is the set of all n-tuples with $\alpha \in V$ defined by $\alpha = (x_1, x_2, \cdots, x_n)$, where $x_i \in F$. The set V along with the following definition of addition and scalar multiplication is a vector space. Let $\alpha \in V$ be as defined above and $\beta \in V$ be $\beta = (y_1, y_2, \cdots, y_n)$, where $y_i \in F$, then $\forall \alpha, \beta \in V$ and $c \in \mathbb{R}$

$$\alpha + \beta = (x_1 + y_1, x_2 + y_2, \cdots, x_n + y_n)$$
$$c\alpha = (cx_1, cx_2, \cdots, cx_n)$$

Please note that the + on the left hand side and right hand side have two different meanings. The + on the left hand side is for elements of V and the + on the right hand side is over the elements of the scalar field, which is $\mathbb{R}$ in this case. Thus we are defining the *vector addition* in terms of the *addition* defined on the field. Similarly, we define the scalar multiplication in the vector space in terms of the multiplication operation of the underlying field.

Example 2: The set of all $m \times n$ matrices (denoted by $\mathbb{R}^{m \times n}$) defined over the field $\mathbb{R}$ (i.e., entries of the matrices are real numbers) is a vector space, with the following definition of *vector addition* and *scalar multiplication*.

Addition: Let a_{ij} and b_{ij} be the (i, j)th element of A and B respectively. Then the (i, j)th element of $A + B$ denoted by $(A + B)_{ij}$ is

$$(A + B)_{ij} = a_{ij} + b_{ij}, \quad \forall A, B \in \mathbb{R}^{m \times n}$$

Multiplication: Let $(cA)_{ij}$ be the (i, j)th element of the matrix formed by the scalar product of c and A, where $c \in \mathbb{R}$. Then

$$(cA)_{ij} = ca_{ij}, \quad \forall c \in \mathbb{R}, A \in \mathbb{R}^{m \times n}$$

In other words, we are saying the set of all $m \times n$ matrices with real entries form a vector space. Here again, we are defining the vector addition and scalar multiplication, in terms of the addition and multiplication operations on the underlying field.

Example 3: Let F be any field and S be any non-empty subset of F. Let V be the set of all functions from the set S to the set F. Then V is a vector space over F under the following definitions of *vector addition* and *scalar multiplication*.

Addition: Let f and g be two vectors (i.e., functions) from V. We define $f + g$ as

$$(f + g)(s) = f(s) + g(s), \quad \forall f, g \in V, \quad s \in S$$

Note that the definition of the sum of two functions is point-wise (i.e., for each value, s, belonging to the domain of the function). The left hand side should be read as the sum of the two functions f and g evaluated at s, whereas the + on the right hand side is the addition on the field F, which is the range set of the functions.

Multiplication: The scalar multiplication is defined as

$$(cf)(s) = cf(s), \quad \forall c \in F, f \in V, s \in S.$$

Questions:

1. Show that $SO(3)$ is a group. Is $SO(3)$ a vector space?
2. Show that $SE(3)$ is a group. Is $SE(3)$ a vector space?
3. Show that $so(3)$ and $se(3)$ are vector spaces under the traditional definition of addition and scalar multiplication for matrices.

4.1 Vector Subspace

Let V be a vector space over the field F. A subspace of V is a subset, W of V (symbolically written as $W \subset V$), which is itself a vector space over F with the same vector addition and scalar multiplication operations that are defined on V.

Theorem 4.1. *A non-empty $W \subseteq V$ is a vector space if and only if (also written as iff) for any pair of vectors $\alpha, \beta \in V$ and any scalar $c \in F$, $c\alpha + \beta \in W$.*

A corollary of the above theorem is that any subset W that does not contain the 0 element (or additive identity of V) will not be a subspace.
Example: The real plane $\mathbb{R}^2$ is a vector space. Any straight line in the plane that passes through the origin is a vector subspace. However, any straight line that does not pass through the origin is *not a vector space.*

4.2 Basis of a Vector Space

Before we define a basis of a vector space, we will need some supporting definitions.

Definition 4.1. *Linear Combination:* Let $\alpha_1, \alpha_2, \cdots, \alpha_n \in V$ be n vectors. Then the vector $\beta \in V$ defined by

$$\beta = c_1\alpha_1 + c_2\alpha_2 + \cdots + c_n\alpha_n$$

is called a linear combination of the vectors $\alpha_1, \alpha_2, \cdots, \alpha_n$, where $c_1, c_2, \cdots, c_n, \in F$.

Definition 4.2. *Linear Span:* For a set of vectors $A = \{\alpha_1, \alpha_2, \cdots, \alpha_n\}$, the linear span or simply span of A is defined by

$$\text{span}(A) = \{\beta | \beta = c_1\alpha_1 + c_2\alpha_2 + \cdots + c_n\alpha_n\}$$

for any value of $c_1, c_2, \cdots, c_n, \in F$.

Definition 4.3. *Linearly Dependent or Independent Vectors:* A set of vectors $A = \{\alpha_1, \alpha_2, \cdots, \alpha_n\}$, is said to be linearly dependent if there exists some $c_1, c_2, \cdots, c_n, \in F$ such that

$$c_1\alpha_1 + c_2\alpha_2 + \cdots + c_n\alpha_n = 0$$

If A is not linearly dependent then A is called a system of independent vectors.

Using the definitions of linear independence and span, we can define the basis of a vector space.

Definition 4.4. *Basis:* Let V be a vector space. A basis for V is a linearly independent set of vectors in V whose span is the set V. In other words, a basis of V is a linearly independent set of vectors belonging to V such that any vector in V can be expressed as a linear combination of these vectors.

Examples:

- Consider any two non-collinear vectors in the plane. These two vectors will form a basis for $\mathbb{R}^2$.

- Consider any three non-coplanar vectors in the space. These three vectors will form a basis for $\mathbb{R}^3$.

In general, in the real Euclidean space $\mathbb{R}^n$, the basis formed by the unit vectors is called a *standard basis*. The *dimension* of a vector space is the number of vectors that form a basis of the space. A vector space is called finite dimensional vector space if the number of vectors in its basis is finite (note that it is possible for the number of basis vectors to be infinite).

If B is a basis for a vector space V and $W \subset V$ (i.e., W is a subset of V), then the largest cardinality[1] $B' \subset B$ such that $B' \subset W$ (i.e., B' is also a subset of W) is a basis for W. The dimension of W is the number of vectors in B'.

4.3 Coordinate Representation

Let $\beta \in V$ and $\alpha_1, \alpha_2, \cdots, \alpha_n \in V$ be a basis for V. Let

$$\beta = c_1\alpha_1 + c_2\alpha_2 + \cdots + c_n\alpha_n.$$

Then $(c_1, c_2, \cdots, c_n)$ are the coordinates of β.

Remark 4.1. Please make sure to conceptually distinguish a vector and its representation. Representations are required for numerical computations and they depend on the choice of the basis vectors (there may be infinitely many choices for basis; think about the possible choices in the plane). There can be results obtained that are independent of the representation and these are the results that matter or are generally usable.

4.4 Polynomials

Polynomials are an example of set of functions that form a vector space. The set of polynomials of bounded or unbounded degree forms a vector space as will be formalized below. Let F be a field and let V be the set of all functions $f : F \to F$ of the form.

$$f(x) = c_0 + c_1x + c_2x^2 + \cdots + c_nx^n$$

where $c_0, c_1, c_2, \cdots, c_n, \in F$ are fixed scalars. Note that different values of the scalars define different polynomial functions and we are considering polynomials of degree at most n. Define addition and scalar multiplication in V as $(f+g)(x) = f(x)+g(x)$ and $(cf)(x) = cf(x)$. Then V with the above definitions of addition and scalar multiplication is a vector space (**Can you show it?**).

The standard basis for vector space of polynomials is

$$\{1, x, x^2, \cdots, x^n\}$$

Note that each of the basis elements is a function. The coordinates of a function or polynomial f in this basis is formed by the coefficients of the polynomial, namely, $(c_0, c_1, c_2, \cdots, c_n)$. The dimension of the vector space of polynomials of degree at most n is $n + 1$.

If we consider the polynomials to be of any degree then the standard basis is an infinite basis of the form

$$\{1, x, x^2, \cdots, x^n, x^{n+1}, \cdots\}$$

[1] The cardinality of a set is the number of elements in that set.

Remark 4.2. The notion of function spaces and basis of function spaces permeates a wide variety of application areas. For examples in machine learning notions of neural networks, support vector machines, etc., are applications of representation of functions in some choice of standard basis function. Similarly in signal processing, notions of Fourier series, wavelets, etc., are applications of representation of functions in some choice of standard basis function for a subclass of function spaces.

5 Linear Transformation

Let V and W be vector spaces over the field F. A linear transformation from V into W is a function T from V to W such that

$$T(c\alpha + \beta) = c(T\alpha) + T\beta$$

for all $\alpha, \beta \in V$ and all $c \in F$.
Examples:

1. Let F be a field and let V be the vector space of polynomial functions f from F to F of degree n.

   $$f(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_n x^n$$

   Let

   $$(Df)(x) = c_1 + 2c_2 x + \cdots + nc_n x^{n-1}$$

   Then D is a linear transformation from V to V. Note that the function Df is the derivative of the polynomial function f. Thus what we are saying above is that the derivative is a linear transformation between the vector spaces of polynomial functions.

2. Integration between vector spaces of polynomial functions is also a linear operator.

Any linear transformation from V to W defined over the field F can be written as an $m \times n$ matrix with entries in the field F, where n is the dimension of V and m is the dimension of W. To form the matrix representation of the linear transformation, write down the transformation of each basis vector in V in terms of the basis vectors in W. The coefficients of each transformed basis vector forms a row of the matrix of representation of the linear transformation. Note that the matrix representation of a linear operator depends on the choice of both V and W. Thus, if we change basis, we change the matrix representation of the linear transformation. Thus, intuitively speaking, linear transformation of a vector is akin to matrix multiplication of a vector and we can think of a linear operator as a matrix and vice-versa, and we will use this quite often below. However, please note that there can be multiple matrix representation of the same linear operator (depending on the choice of the basis). So one should understand the underlying linear operator is conceptually more fundamental than its matrix representation (which is important for performing numerical computations).

There is some pair of basis for V and W where the representation of a linear transformation (or linear operator) becomes the simplest (i.e., diagonal or Jordan canonical form). Much of Linear Algebra is based on the study of simplest representation of a linear operator. For a square matrix, which is a transformation from V to V, the eigenvectors of the matrix gives a basis in which the representation of the linear operator is simplest.

5.1 Four Fundamental Subspaces of a Linear Operator (Matrix)

Let V and W be two vector spaces of dimension n and m respectively, over a field F. Let $T : V \to W$ be a linear transformation and $T' : W \to V$ be also a linear transformation (where T' is read as the transpose of T. In other words, consider a matrix T and its transpose. The four fundamental subspaces associated with T are the

1. Range space of T, denoted by $\mathcal{R}(T)$
2. Null space of T, denoted by $\mathcal{N}(T)$
3. Range space of T', denoted by $\mathcal{R}(T')$
4. Null space of T', denoted by $\mathcal{N}(T')$

Definition 5.1. Range Space (Column Space) of T: The range space (or column space) of a linear operator (i.e., matrix) T is defined by

$$\mathcal{R}(T) = \{w | w = Tv, v \in V, w \in W\}.$$

Note that $\mathcal{R}(T) \subset W$ and in fact it is a subspace of W. The rank of T is the dimension of $\mathcal{R}(T)$.

Definition 5.2. Null Space of T: The null space of a linear operator T is defined by

$$\mathcal{N}(T) = \{v | Tv = 0, v \in V, 0 \in W\}.$$

Note that $\mathcal{N}(T) \subset V$ and in fact it is a subspace of V. The nullity of T is the dimension of $\mathcal{N}(T)$.

Definition 5.3. Range Space of transpose of T (Row Space of T): The range space of the transpose of T (or row space of T) is defined by

$$\mathcal{R}(T') = \{v | v = T'w, v \in V, w \in W\}.$$

Note that $\mathcal{R}(T') \subset V$ and in fact it is a subspace of V.

Definition 5.4. Null Space of T': The null space of the linear operator T' is defined by

$$\mathcal{N}(T') = \{w | T'w = 0, w \in W, 0 \in V\}.$$

Note that $\mathcal{N}(T') \subset W$ and in fact it is a subspace of W.

Figure 1 gives a pictorial representation of the four subspaces associated with a linear operator, $T : \mathbb{R}^n \to \mathbb{R}^m$ (which can be represented as a $m \times n$ matrix), and the relationship between them. Note that the null space and row space of T are subspaces of $\mathbb{R}^n$ and the column space and null space of T' are the subspaces of $\mathbb{R}^m$. If the dimension of the column space (i.e., rank of the matrix) of T, is r, then the dimension of the null space of T (called the *nullity* of T will be $n - r$. The dimension of the row space will be r and the dimension of the null space of T' will be $m - r$. Furthermore, the null space and the row space of T are *orthogonal complements* of each other. In other words, any vector in the row space will be orthogonal to any vector in the null space (which can be written as $v'(T'w) = 0, \forall v \in \mathcal{N}(T) and T'w \in \mathcal{R}(T')$. Thus the row space and null space of T will have only the 0 vector in common. Similarly, the column space of T and the null space of T' are also orthogonal complements of each other, i.e., $w'(Tv) = 0, \forall w \in \mathcal{N}(T) and Tv \in \mathcal{R}(T)$.

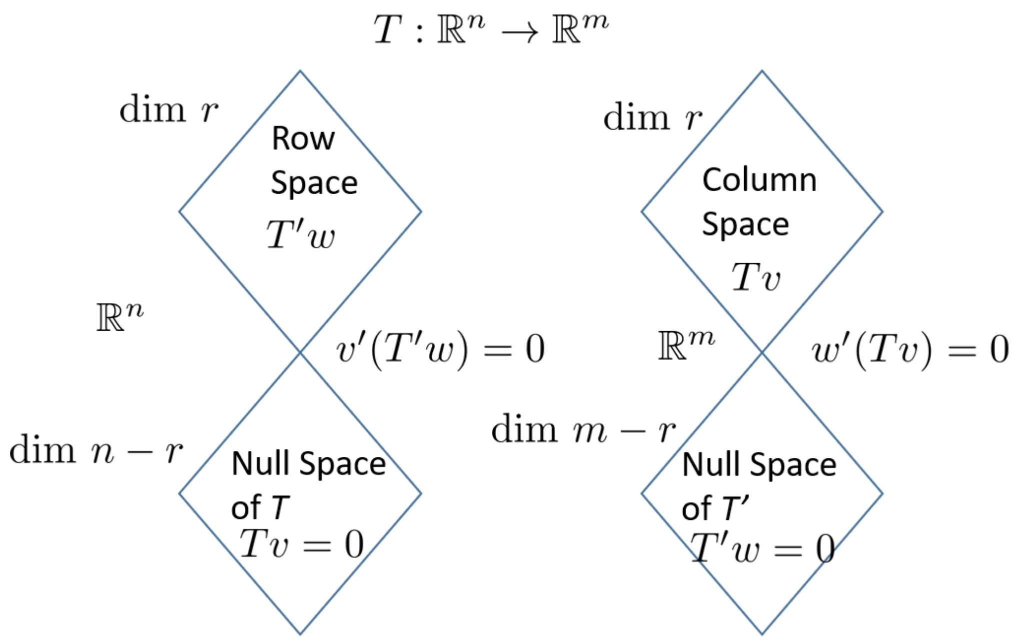

Figure 1: A pictorial depiction of the four fundamental subspaces associated with a matrix.

Example: Let T be the linear operator given by

$$T = \begin{bmatrix} 1 & 0 & 2 & 3 \\ 0 & 1 & 4 & 5 \\ 0 & 0 & 0 & 0 \end{bmatrix} \tag{1}$$

The linear operator T is a map from $\mathbb{R}^4$ to $\mathbb{R}^3$. The rank of T, which is the dimension of the column space of T is 2. For the four fundamental spaces associated with T, one choice of the basis is given below. Note that the subspace is a span of the basis vectors. Thus, specifying the basis vectors imply that we are specifying the entire subspace. The computations here are done using the definition of basis vectors and by inspection. In general, one can compute the null space and range space of a matrix using *singular value decomposition (SVD)*. All decent linear algebra softwares have functions for computing SVD.

Basis for range space of T is

$$\left\{ \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} \right\}$$

Basis for null space of T' is

$$\left\{ \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \right\}$$

Basis for range space of T' is

$$\left\{ \begin{bmatrix} 1 \\ 0 \\ 2 \\ 3 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 4 \\ 5 \end{bmatrix} \right\}$$

Basis for null space of T is

$$\left\{ \begin{bmatrix} -2 \\ -4 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} -3 \\ -5 \\ 0 \\ 1 \end{bmatrix} \right\}$$

6 Applications

The concepts discussed in this document are pre-requisite to understand many results in robotics and other subjects. In the context of robotics, some of the key facts to realize are as follows:

1. The space of rigid body rotations, $SO(3)$, and the space of rigid body transformations, $SE(3)$, are examples of a group. The group operation is the same as that of matrix multiplication. However, it is important to note that they are not vector spaces. Furthermore, these sets are also manifolds (i.e., locally they look like an Euclidean space). Thus, they form a *Lie group*. Although, we have not formally defined manifold and Lie groups yet, we will define them later in class.

2. The spaces $so(3)$ and $se(3)$ are vector spaces. In fact they are the tangent spaces (roughly speaking, think about this as the generalization of the notion of a tangent to a curve) of $SO(3)$ and $SE(3)$ respectively. They form a *Lie algebra*. The fact that $SO(3)$ and $SE(3)$ are Lie groups and $so(3)$ and $se(3)$ are Lie algebras form the mathematical basis of many of the fundamental results in robotics (e.g., the exponential map, non-holonomic control).

3. The concept of linear dependence of a set of vectors is useful in grasping to determine whether a grasp can hold an object without dropping it.

4. The concept of the four fundamental subspaces is widely used in robotics control, with the matrix of interest being the Jacobian matrix from the velocity kinematics equations.