Math 121A: Linear Algebra

Eli Griffiths

November 13, 2023

Table of Contents

Introduction

1.1 Fields

A field is an algebraic structure intended to capture the properties of the rational and real numbers.

Definition 1.1 (Field). A field $\mathbb{F}$ is a set $\mathbb{F}$ equipped with an additon and multiplication operator such that

1. Elements commute under both operations
2. Associativity holds for both operators
3. $\exists 1, 0 \in \mathbb{F}$ such that $\lambda + 0 = \lambda$ and $\lambda 1 = \lambda$ for all $\lambda \in \mathbb{F}$
4. $\forall \lambda \in \mathbb{F}, \exists! \gamma \in \mathbb{F}$ such that $\lambda + \gamma = 0$
5. $\forall \lambda \in \mathbb{F}$ where $\lambda \neq 0$, $\exists! \gamma \in \mathbb{F}$ such that $\lambda\gamma = 0$

Consider a prime number p. It is then possible to construct the field $\mathbb{F}_p$ where

$$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$$

Consider the simplest example, $\mathbb{F}_2 = \{0, 1\}$. It is clear that this makes up a field as 1 has a multiplicative and additive inverse. In the case of $\mathbb{F}_4 = \{0, 1, 2, 3\}$, 2 has no multiplicative inverse and hence isnt a field. In general, if $a, b \neq 0$ and $ab = 0$, then a and b do not have inverses.

Proof. Let $a, b \in \mathbb{F}$. Assume towards contradiction that $ab = 0$ and that a or b have inverses. WLOG, assume that there is a $c \in F$ such that $ac = 1$. ■

1.2 Vector Spaces

Definition 1.2 (Vector Space). Let $\mathbb{F}$ be a field. A vector space V over a field $\mathbb{F}$ is a set V equipped with addition and scalar multiplication such that

1. $(V, +)$ is an abelian group
2. $(V, \cdot)$ is associative and distributive, that is $\forall a, b \in \mathbb{F}$ and $\forall u, v \in V$
   (a) $a(u + v) = au + av$
   (b) $(a + b)v = av + bv$
3. $\exists! 1 \in \mathbb{F}$ such that $\forall v \in V$, $1v = v$

Example 1.1. Let $\mathbb{F}$ be a field and $n \in \mathbb{N}$. Let

$$\mathbb{F}^n = \{(a_1, a_2, a_3, \ldots) : a_i \in \mathbb{F}\}$$

where

$$(a_1, a_2, a_3, \ldots) + (b_1, b_2, b_3, \ldots) = (a_1 + b_1, a_2 + b_2, a_3 + b_3, \ldots)$$
$$e \cdot (a_1, a_2, a_3, \ldots) = (ea_1, ea_2, ea_3, \ldots)$$

Then $(\mathbb{F}^n, +, \cdot)$ is a vector space. This gives rise to all the familiar vector spaces $\mathbb{C}^n, \mathbb{R}^n, \mathbb{Q}^n, \ldots$

***Remark*.** If $K \supset F$ are fields, then $(K, +, \cdot)$ is a vector space over F

Theorem 1.1. Let V be a vector space and $u, v, w \in V$. Then $u + w = v + w$ implies $u = v$.

Proof. Im too lazy :P ■

There are more exotic examples of vector spaces. Consider the set of continuous, real value functions over the interval $[0, 1]$.

Example 1.2.

$$C = \{f : [0, 1] \to \mathbb{R} \mid f \text{ is continuous}\}$$

This set can be turned into a vector space by defining the following operations

$$+ \Rightarrow (f + g)(x) = f(x) + g(x)$$
$$\cdot \Rightarrow (cf)(x) = cf(x)$$

1.2.1 Subspaces

Definition 1.3 (Subspace). Let V be a vector space over a field $\mathbb{F}$. A subset $W \subset V$ is called a subspace if W is also a vector space over $\mathbb{F}$.

Theorem 1.2. Let $W \subset V$ be a non-empty subset of V. W is a subspace of V if and only if

1. W is closed under $+$

   $$w_1 + w_2 \in W, \forall w_1, w_2 \in W$$

2. W is closed under $\cdot$

   $$cw \in W, \forall w \in W, c \in \mathbb{F}$$

An equivalent formulation of the conditions is that W is closed under linear combination, or symbolically

$$c_1 w_1 + c_2 w_2 \in W, \forall c_1, c_2 \in \mathbb{F}, w_1, w_2 \in W$$

Consider the vector space $\mathbb{R}^2$. After some time, it becomes clear that the only subspaces of $\mathbb{R}^2$ are $\{\vec{0}\}$ and $\{c(a,b) | c \in \mathbb{R}\}$ where $a, b \in \mathbb{R}$ (aka all lines that go through the origin). If a line does not go through the origin of $\mathbb{R}^2$, then it's clear it fails to be a subspace. Examine the line $y + x = 1$. Since it does not contain the zero vector, it fails to be closed under scalar multiplication as any vector in $y + x = 1$ will become the zero vector.

Example 1.3 (Polynomial Space). Let $\mathcal{P}_n(\mathbb{F}) := \left\{a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0 : a_i \in \mathbb{F}\right\}$. $\mathcal{P}_n(\mathbb{F})$ is a vector space $\forall n \in \mathbb{N}_0$. Additionally, $\mathcal{P}_{n-1}(\mathbb{F})$ is a subspace of $\mathcal{P}_n(\mathbb{F})$.

Example 1.4 (Matrix Space). Let $M_{n\times m}(\mathbb{F}) := \left\{\begin{pmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nm} \end{pmatrix} : a_{ij} \in \mathbb{F}\right\}$. Then $M_{n\times m}(\mathbb{F})$ is a vector space. An example subspace of $M_{n\times m}(\mathbb{F})$ is the set of upper triangular matrices.

Theorem 1.3 (Trivial Subspaces). For every non-zero vector space V, it has at least two subspaces $\{\vec{0}\}$ and V.

Theorem 1.4 (Subspace Construction). Let V_1, V_2 be subspaces of V over $\mathbb{F}$. Then

1. $V_1 \cap V_2$ is a subspace
2. $V_1 + V_2 = \{v_1 + v_2 : v_1 \in V_1, v_2 \in V_2\}$ is a subspace
3. $V_1 \cup V_2$ is a subspace if and only if $V_1 \subset V_2$ or $V_2 \subset V_1$

1.3 Span and Independence

Definition 1.4 (Linear Combination). Let V be a vector space and $v_1, v_2, \ldots, v_n \in V$. A linear combination of $\{v_1, v_2, \ldots, v_n\}$ is a vector of the form

$$c_1 v_1 + c_2 v_2 + \ldots + c_n v_n$$

where $c_i \in \mathbb{F}$.

Definition 1.5 (Span). The span of a set of vectors $\{v_1, v_2, \ldots, v_n\}$ is the set of all linear combinations of those vectors. It is denoted by span $\{v_1, v_2, \ldots, v_n\}$. For an infinite set of vectors, an alternative definition helps

$$\text{span}(S) = \bigcap_{\substack{w \supseteq S \\ w \leq V}} W = \text{Smallest subspace that contains } S$$

Definition 1.6 (Subset Independence). Let S be a subset of a vector space V.

1. If every non-empty finite subset of S is linearly independent, S is called indepen-

dent.

2. If there exists a non-empty finite subset of S that is linearly dependent, S is called dependent.

1.4 Basis and Dimension

Definition 1.7. A maximal independent set of vectors is a independent subset of a vector space that, if any other vector is added from the vector space, would be become dependent. That is, given a maximally independent subset $W = \{v_1, v_2, v_3, \ldots\}$, $u \in \text{span}(W)$.

Definition 1.8 (Basis). Let $\{u_1, u_2, u_3, \ldots\} \subset V$. Then $\{u_1, u_2, u_3, \ldots\}$ is a basis of V if every vector $v \in V$ can be uniquelly written as $v = c_1u_1 + c_2u_2 + \ldots$ with $c_i \in \mathbb{F}$. Equivalently, it is a basis if

1. $V = \text{span}\{u_1, u_2, u_2, \ldots\}$
2. $\{u_1, u_2, u_2, \ldots\}$ is independent

Theorem 1.5. Let $V = \text{span}\{v_1, v_2, \ldots, v_n\}$ and $W = \{v_1, v_2, \ldots, v_r\}$ be a maximally independent subset of V. Then W is a basis for V.

Proof. Since W is maximally independent, $v_i \in W$ for $1 \le i \le n$. Therefore $V = \text{span}(W)$. Since W is independent and spans V, it is a basis for V. ■

Corollary 1.1. Let $V = \{v_1, v_2, \ldots, v_n\}$. Any maximally independent subset of V forms a basis of V over $\mathbb{F}$.

Theorem 1.6. If S is an independent subset of a vector space V, it can be extended to a basis of V (by the Axiom of Choice).

Theorem 1.7. Let $R = \{v_1, v_2, \ldots, v_n\}$ and $W = \{w_1, w_2, \ldots, w_m\}$ be bases of V over $\mathbb{F}$. Then $m = n$.

Proof. Since R is a basis, $w_i = \sum_{j=1}^{n} a_j v_j$. This can be expressed in matrix form

$$\begin{pmatrix} w_1 \\ \vdots \\ w_m \end{pmatrix} = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix} \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}$$

Since W is also a basis, $v_i = \sum_{j=1}^m b_j w_j$ meaning

$$\begin{pmatrix} w_1 \\ \vdots \\ w_m \end{pmatrix} = \underbrace{\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}}_{A} \underbrace{\begin{pmatrix} b_{11} & \cdots & b_{1m} \\ \vdots & & \vdots \\ b_{m1} & \cdots & b_{nm} \end{pmatrix}}_{B} \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix}$$

This means that $AB = I$. By starting with W instead of R, it follows that $BA = I$. Therefore A and B are invertible meaning they must be square, hence $n = m$. ∎

Definition 1.9 (Dimension). The dimension of a vector space V is the number of vectors in a basis of V.

Theorem 1.8. Let W be a subspace of V such that $\dim V = n < \infty$. If $\dim W = \dim V$, $W = V$.

Proof. ∎

Linear Maps

2.1 Linearity

Definition 2.10 (Linear Map). A map $T : V \to W$ is linear if $T(au+bv) = aT(u)+bT(v)$ for all $a, b \in \mathbb{F}$ and $u, v \in V$.

Theorem 2.9. If $\{v_1, v_2, \ldots, v_n\}$ is a basis of V,

$$T(a_1v_1 + a_2v_2 + \ldots + a_nv_n) = a_1T(v_1) + a_2T(v_2) + \ldots a_nT(v_n)$$

A linear map can be defined just by declaring the images of a vector spaces basis vectors as the map has to obey linearity over a basis. This leads to a natural formulation of a linear map as a matrix where the columns are the images of the basis vectors under T.

Definition 2.11 (Null Space and Range). Let $T : V \to W$ be F-linear. Then

1. $N(T) = \{v \in V : T(v) = 0\}$ is a subspace of V
2. $R(T) = T(V) = \{T(v) : v \in V\}$ is a subspace of W

Theorem 2.10. Let $T : V \to W$ be F-linear. Then

$$\begin{aligned} \dim V &= \dim(N(T)) + \dim(R(T)) \\ &= \operatorname{nullity} T + \operatorname{rank} T \end{aligned}$$

Proof. Let S be a basis of $N(T)$. Then $\#S = \operatorname{nullity} T$. S can be extended to be a basis of V with some S' such that $S \cup S'$ is a basis. Therefore

$$\dim V = \#(S \cup S') = \#S + \#S' = \operatorname{nullity} T + \#S$$

■

Theorem 2.11. $T : V \to W$ is one-to-one if and only if $N(T) = \{0\}$

Proof. The forward direction follows by considering $T(v_1) = T(v_2)$ and settting v_2 to zero. Consider the backwards direction. If $T(v_1) = T(v_2)$, then $T(v_1 - v_2) = 0$. Therefore $v_1 - v_2 \in N(T) = \{0\}$ meanimg $v_1 - v_2 = 0$. Hence $v_1 = v_2$ meaning T is one-to-one. ■

Theorem 2.12. Let $T : V \to V$ be a linear map where $\dim V = n < \infty$. Then T is bijective.

Proof. By the dimension formula,

$$n = \dim V = \operatorname{nullity} T + \operatorname{rank} T$$

If T is injective, then

$$\begin{aligned}
\operatorname{nullity} T = 0 &\implies \operatorname{rank} T \\
&\implies \operatorname{rank} T = n \\
&\implies R(T) = V
\end{aligned}$$

■

2.1.1 Change of Matrix

Theorem 2.13. Let $T : V \to V$ be linear with V having two bases β and β'.

Matrices

3.1 Elementary Matrices

Definition 3.12 (Elementary Matrix). An elementary matrix is a matrix obtained by doing on the types of operations on a $n \times n$ identity matrix

1. Exchange two rows (or columns) $\implies$ Type I
2. Multiply a row (or column) $\implies$ Type II
3. Add a row to a row (or column to column) $\implies$ Type III

It will be useful to have notation to refer to each type of elementary matrix. For Type I, E_{ij} will indicate swapping row i and j. For Type II, E_λ represents a row multiplication and Type III will be represented by $E(\lambda)$.

The following are the common inverses and relationships between the elementary matrices

$$\begin{aligned} E_{ij}^{-1} &= E_{ij} & E_{ij}^2 &= I \\ E_{\lambda}^{-1} &= E_{\lambda^{-1}} & E_\lambda E_{\lambda^{-1}} &= I \end{aligned}$$

Theorem 3.14 (Application of Elementary Operations). Let $A \in M_{n\times n}(\mathbb{F})$. Let E be an elementary operation/matrix. Then

$$A \xrightarrow{\text{Row operation } E} EA$$
$$A \xrightarrow{\text{Col. operation } E} AE$$

3.2 Rank of Matrices

Recall that the rank of a linear transformation $T : V \to W$ is $\operatorname{rank} T = \dim T[V]$. Therefore it would make sense to extend this to matrices as they represent linear transformations.

Definition 3.13 (Rank of a Matrix). Let $A \in M_{m\times n}(\mathbb{F})$. Then the rank of A is defined as the rank of the linear transformation $L_A : \mathbb{F}^n \to \mathbb{F}^m : x \mapsto Ax$.

It is also the case that rank of a linear transformation is preserved in any matrix representation. This can be stated as a theorem:

Theorem 3.15 (Rank Across Representation). Let $T : V \to W$ be linear and let β be a basis of V and γ a basis of W. Then

$$\operatorname{rank} T = \operatorname{rank}[T]_\beta^\gamma$$

Proof. ■

Theorem 3.16 (Rank and General Linear Group). Let $A \in M_{m\times n}(\mathbb{F})$ and $P \in GL_m(\mathbb{F})$, $Q \in GL_n(\mathbb{F})$. Then

1. $\operatorname{rank}(PA) = \operatorname{rank}(A)$
2. $\operatorname{rank}(AQ) = \operatorname{rank}(A)$
3. $\operatorname{rank}(PAQ) = \operatorname{rank}(A)$

Theorem 3.17 (Rank of Matrix). For any matrix A,

$$\operatorname{rank} A = \dim(C(A)) = \text{Max number of linearly independent columns}$$

Determinants

4.1 Determinant of 2×2

Definition 4.14. Let $A \in M_{2\times 2}(\mathbb{F})$ with $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Then $\det A = |A| = ad - bc$.

Remark. The determinant has some properties. Let $A = \begin{pmatrix} A_1 & A_2 \end{pmatrix}$ denote the matrix A. Then

1. $\det \begin{pmatrix} A_1 & A_2 \end{pmatrix}$ is bilinear in A_1 and A_2
2. $\det \begin{pmatrix} A_1 & A_1 \end{pmatrix} = 0$
3. $\det \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 1$

Similar statements hold for a 3×3. The determinant can be expressed however for any $n \times n$ matrix.

4.2 Determinant of $n \times n$

Definition 4.15 (Determinant). Let $A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} = \begin{pmatrix} A_1 & \cdots & A_n \end{pmatrix}$. For $1 \leq i, j \leq n$, let A_{ij} = the submatrix of A with row i and column j removed. Let $1 \leq k \leq n$. Then

$$\det A = |A| = \sum_{j=1}^{n} (-1)^{j+k} a_{kj} \det\left(A_{kj}\right) \qquad \text{(Row Expansion)}$$

$$\det A = |A| = \sum_{i=1}^{n} (-1)^{i+k} a_{ik} \det(A_{ik}) \qquad \text{(Column Expansion)}$$

Definition 4.16 (Multilinear Map). A map $f : V_1 \times \ldots \times V_n \longrightarrow \mathbb{F}$ is a multilinear map if for each $1 \leq i \leq n, v_i$ is held constant then $f(v_1, \ldots, v_i, \ldots, v_n)$ is a linear function of v_i.

A multi-linear map is called *alternating* if it equals 0 when two adjacent coordinates are the same. Note that then the determinant can be expressed as a multilinear map since an $n \times n$ matrix can be represented as an element in $\underbrace{\mathbb{F}^n \times \ldots \mathbb{F}^n}_{n \text{ times}}$.

Theorem 4.18 (Multilinearity of Determinant). Write $A = \begin{pmatrix} A_1 & \cdots & A_n \end{pmatrix} \in M_{n\times n}(\mathbb{F})$. Then $\det \begin{pmatrix} A_1 & \cdots & A_n \end{pmatrix}$ is multilinear in A's columns.

Proof. This is true for the case $n = 2$. Proceed with induction to show it holds for $n \geq 2$. Let $n \in \mathbb{N}$ be fixed and assume that the determinant is multilinear over n columns. Note that for some $(n+1) \times (n+1)$ matrix A that

$$\det A = \sum_{j=1}^{n+1} (-1)^{1+j} a_{1j} \det\left(A_{1j}\right)$$

If $j \neq k$, then a_{ij} is independent of column k and A_{ij} will be linear in A_k, meaning $a_{ij}A_{ij}$ will be linear in A_k. If $j = k$, then $a_{ij} = a_{ik}$ and linear in A_k. Note that A_{1k} is independent of A_k meaning $a_{ik} \det\{A_{ik}\}$ is linear in A_k. Therefore the sum $\sum_{j=1}^{n+1} (-1)^{1+j} a_{ij} \det\left(A_{ij}\right)$ is linear in A_k. ■

Theorem 4.19. Write $A = \begin{pmatrix} A_1 & \cdots & A_n \end{pmatrix} \in M_{n \times n}(\mathbb{F})$. Then $\det \begin{pmatrix} A_1 & \cdots & A_n \end{pmatrix}$ is alternating.

List of Theorems

List of Definitions