Contents

Chapter 1

Linear Equation

1.1 Fields

The set $\mathbb{F}$ together with two operation $+$, addition, and $\cdot$, multiplication, that satisfy the follwings is called a **field**. For all $x, y, z \in \mathbb{F}$

1. Addition and multiplication are *commutative*

$$x + y = y + x \qquad x \cdot y = y \cdot x$$

2. Addition and multiplication are *associative*

$$x + (y + z) = (x + y) + z \qquad x \cdot (y \cdot z) = (x \cdot y) \cdot z$$

3. Multiplication distributes over addition

$$x \cdot (y + z) = x \cdot y + x \cdot z$$

4. There exists an element 0, zero, in $\mathbb{F}$ such that $x + 0 = x$.

5. There exists an element 1 , one, in $\mathbb{F}$ such that $x \cdot 1 = x$.

6. For each element $x \in \mathbb{F}$ there corresponds a unique element $y \in \mathbb{F}$ such that $x + y = 0$. y is commonly denoted as $-x$.

7. For each non-zero element $x \in \mathbb{F}$ there corresponds a unique element $y \in \mathbb{F}$ such that $x \cdot y = 1$. y is commonly denoted as x^{-1} or $\frac{1}{x}$.

8. $\mathbb{F}$ is closed under addition and multiplication.

$$x + y \in \mathbb{F} \qquad x \cdot y \in \mathbb{F}$$

Definition (Characteristics): Let n be the least number such that

$$\underbrace{1 + 1 + \ldots 1}_{n} = 0 \tag{1.1}$$

then n is the **characteristics** of $\mathbb{F}$. If for a field there exists no such n, then its characteristics is 0.

Theorem 1.1. *If $\mathbb{F}$ is a finite field, then the number of elements of $\mathbb{F}$ must be in form of p^k where p isa prime number and $k \in \mathbb{N}$. Also fro every number in such form there exists a unique $\mathbb{F}$ with p^k elements.*

If $\mathbb{F}$ is a field then the set of all polynomials with the coefficients in $\mathbb{F}$ is denoted by $\mathbb{F}[x]$, that is

$$\mathbb{F}[x] = \left\{ \sum_{i=0}^{n} a_i x^i \;\middle|\; a_i \in \mathbb{F}\, \forall i,\ n \in \mathbb{N} \right\}$$

Cleary $\mathbb{F}[x]$ does not have a multiplicative inverse for some of its non-zero elements. Define $\mathbb{F}(x)$ as follow

$$\mathbb{F}(x) = \left\{ \frac{f(x)}{g(x)} \;\middle|\; f(x)\,, g(x) \in \mathbb{F}[x]\,,\ g(x) \neq 0 \right\}$$

which is a field. Also, note that $\mathbb{F} \subset \mathbb{F}[x] \subset \mathbb{F}(x)$.

1.2 Matrices

Let us denote the set of all metrices of size $m \times n$ with elements in $\mathbb{F}$ by $\mathcal{M}_{m\times n}(\mathbb{F})$ and if $m = n$ then it is equivalently denoted as $\mathcal{M}_n(\mathbb{F})$.

Matrix $A \in \mathcal{M}_n(\mathbb{F})$ is said to be **invertiable** or **non-singular** if there exists a matrix $B \in \mathcal{M}_n(\mathbb{F})$ such that $AB = BA = \mathbb{I}_n$.

Consider the following system of linear equations:

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \ a_{1n}x_n = y_1 \\ a_{21}x_1 + a_{22}x_2 + \ a_{2n}x_n = y_2 \\ \quad\vdots \\ a_{m1}x_1 + a_{n2}x_2 + a_{mn}x_n = y_m \end{cases} \tag{1.2}$$

with all $a_{ij} \in \mathbb{F}$. Then if $c_k \in F,\ k = 1, \dots, n$:

$$(c_1a_{11} + c_2a_{21} + \dots c_m a_{m1})x_1 + \dots + (c_1a_{1n} + c_2a_{2n} + \dots c_m a_{mn})x_n = c_1y_1 + \dots + c_m y_m$$

is **linear combination** of the Equation (1.2).

Definition (Equaivalent Systems): Two systems are considered equivalent if each equation in one system is a linear combination of the other system.

Proposition 1.2. *Equivalent systems of linear equations have exactly the same solution.*

The linear system, Equation (1.2), can be represent in form of matrices $AX = Y$ where $A = \begin{bmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \\ a_{n1} & \dots & a_{mn} \end{bmatrix} \in \mathcal{M}_{m\times n}(\mathbb{F})$ and $X = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}, Y = \begin{bmatrix} y_1 \\ \vdots \\ y_m \end{bmatrix}$ then the solutions of Equation (1.2) are exactly the same as $AX = Y$.

1.2.1 Elementary Row Operations

Consider a matrix $A \in \mathcal{M}_{m\times n}(\mathbb{F})$, we define three elementary row operations on A:

1. multiplication of one row by a non-zero scalar c, denoted by $e_r(c)$.
2. replacement of r_{th} row of A by row r plus c times row $s \neq r$ that is $r_{\text{new}} = r + cs$ and it is denoted by $e_{rs}(c)$
3. Interchange two rows e_{rs}.

Theorem 1.3. *To each elementary row operation e there corresponds an elementary row operation e^{-1}, of the same type as e, such that $e^{-1}(e(A)) = e(e^{-1}(A)) = A$ for any A.*

Proof. It is easily verified by hand. ∎

Definition (Row-equivalent): If A and B are $m \times n$ matrices over $\mathbb{F}$, we say that B is **row-equivalent** to A if B can be obtained from A by a finite sequence of elementary row operation.

Theorem 1.4. *If A and B are row equivalent, the homogenous systems of linear equations $AX = 0$ and $BX = 0$ have exactly the same solution.*

Definition (Row-reduced): A matrix $A \in \mathcal{M}_{m\times n}(\mathbb{F})$ is **row-reduced** if it satisfies

1. the first non-zero entry in each non-zero rwo of A is equal to 1.
2. each column of A which contains the leading non-zero entry of some row has all its other entries 0.

Example 1.1. for example the following matrices are row-reduced

$$\begin{bmatrix} 0 & 0 & 1 \\ 1 & 2 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

Theorem 1.5. *Every $m \times n$ matrix over $\mathbb{F}$ is row-equivalent to a row-reduced matrix. However, note that, row-reduced matrices are not necessairly unique.*

Each of the three elementary row operations have an equivalent $m \times n$ matrix such that, if it is multiplied from left to A, it is equivalent to that operation. For example consider the row operations on a 4×3 matrix A.

$$e_2(c) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & c & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad e_{14}(c) = \begin{bmatrix} 1 & 0 & 0 & c \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad e_{14} = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$$

Similary, one can define column operations as well, however, when considering their equivalent matrix, it must be multiplied from right to A. Furthermore, row-equivalence is an equivalence relationship, that is

Definition:

Reflexive $A \sim A$.

Symmetric $A \sim B \implies A = p_1 p_2 \dots p_k B \implies B = p_1^{-1} p_2^{-1} \dots p_k^{-1} A \implies B \sim A$.

Transivite $A \sim B \implies A = p_1 p_2 \dots p_k B,\ B \sim C \implies B = q_1 q_2 \dots q_m C$ and therefore $A = p_1 p_2 \dots p_k q_1 \dots q_m C \implies A \sim C$

1.3 Row-Reduced Echelon

A matrix $A \in \mathcal{M}_{m\times n}(\mathbb{F})$ is called a **row-reduced echelon** matrix if:

1. A is row reduced.
2. every row of A which has all its entries 0 occurs below every rwo which has a non-zero entry.
3. if rows $1, \ldots, r$ are the non-zero row of A, and if the leading non-zero entry of row i occurs in column k_i, then $k_1 < k_2 < \cdots < k_r$.

Theorem 1.6. *Every $m \times n$ matrix A is row-equivalent to a row-reduced echelon matrix.*

Definition (Elementary matrix): An $m \times n$ matrix is said to be an **elemntary matrix** if it can be obtained from the from $\mathbb{I}_m$ matrix by means of a single elementary row operation.

Chapter 2

Vector Spaces

A **vector space**, also called **linear space**, consist of the followings:

1. a field $\mathbb{F}$ of scalars.
2. a set V of vectors.
3. a vector addition $+$, with the following properties:
   (a) V is closed under addition.
   (b) addition is commutative.
   (c) addition is associative.
   (d) addition has a unique identity element 0.
   (e) for each vector $\alpha \in V$, $\exists \beta \in V$ s.t. $a + b = 0$.
4. a scalar multiplication with the following properties:
   (a) V is closed under scalar multiplication.
   (b) $(c_1 c_2)\alpha = c_1(c_2\alpha)$.
   (c) $c(\alpha + \beta) = c\alpha + c\beta$.
   (d) $(c_1 + c_2)\alpha = c_1\alpha + c_2\alpha$
   (e) scalar multiplication has a unique identity element 1.

Example 2.1. $V = \mathbb{R}$ and $\mathbb{F} = \mathbb{R}$ is a vector space. Furthermore, $V = \mathbb{R}^n$ over $\mathbb{F} = \mathbb{R}$ is a vector space with the scalar multiplication $c(x_1, x_2, \ldots, x_n) = (cx_1, cx_2, \ldots, cx_n)$.

Example 2.2. $V = \mathbb{R}$ and $\mathbb{F} = \mathbb{Z}$ is not a vector space as $\mathbb{Z}$ is not a field.

Definition: A vector $\beta \in V$ is said to be a **linear combination** of the vectors $\alpha_1, \alpha_2, \ldots, \alpha_n$ if there exists scalars $c_1, c_2, \ldots, c_n \in \mathbb{F}$ such that:

$$\beta = c_1\alpha_1 + c_2\alpha_2 + \cdots + c_n\alpha_n = \sum_{i=1}^{n} c_i\alpha_i$$

2.1 Subspaces

Let V be a vector space over field $\mathbb{F}$. A susbspace of V is a subset W of V which is itself a vector space over $\mathbb{F}$ with the operations of vector addition and scalar multiplication on V.

Theorem 2.1. *A non-empty subset W of V is a subspace of V if and only if for each pair of vectors $\alpha, \beta \in W$ and each scalar $c \in \mathbb{F}$ the vector $c\alpha + \beta \in W$.*

Proof. Necessity: Suppose W is a non-empty subset of V with the above property. Since W is not empty then there exists a vector $\alpha \in W$ and therefore, $(-1)\alpha + \alpha = 0 \in W$. For each $c \in \mathbb{F}$, $c\alpha + 0 = c\alpha \in W$. Finally, if $\beta \in W$ as well then $1\alpha + \beta \in W$. Therefore, W satisfies all the conditions and is a linear subspace of V.

Sufficiency: If W is a subspace of V and $\alpha, \beta \in W$ with $c \in \mathbb{F}$ then $c\alpha + \beta \in W$. ∎

Corollary 2.2. *Let V be a vector space over $\mathbb{F}$. The intersection of any collection subspaces of V is a subspace of V.*

Theorem 2.3. *Let V be a vector space and W_1 and W_2 be two subspaces of V such that $W_1 \cap W_2$ is a subspace of V. Then $W_1 \subset W_2$ or $W_2 \subset W_1$.*

Proof. For the sake of contradiction assume neither $W_1 \subset W_2$ nor $W_2 \subset W_1$. Then, there are vectors α_1 and α_2 such that $\alpha_1 \in W_1$ but $\alpha_2 \notin W_2$ and similarly $\alpha_2 \in W_2$ but $\alpha_2 \notin W_1$. Since $\alpha_1 + \alpha_2 \in W_1 \cup W_2$, then $\alpha_1 + \alpha_2 \in W_1$ or $\alpha_1 + \alpha_2 \in W_2$ which is a contradiction. ∎

Theorem 2.4. *Let V be a vector space over the inifinite field $\mathbb{F}$. If $W_1, W_2, \ldots, W_n$ are subspaces of V and $V \subset \cup W_i$, then there exists k such that $V = W_k$.*

Proof. too long, do it urself bitch. ∎

2.2 Span

Definition: Let S be a set of vector in a vector space V. The subspace spanned by S is defined to be the intersection of all subsapces of V which contains S and is denoted by $\operatorname{span} S$. That is, $\operatorname{span} S = \bigcap_{S \subset W} W$. By Corollary 2.2, $\operatorname{span} S$ is a linear subspace. Obviously, $\operatorname{span} S$ is the smallest subspace containing S because if there were $S \subset K \subset \operatorname{span} S$ since by definition $\operatorname{span} S = \cap W \subset K$, then $K = \operatorname{span} S$.

Example 2.3. Let $S = \{0\}$ then $\operatorname{span} S = \bigcap_{\{0\} \subset W} W = \{0\}$. Moreover:

$$\operatorname{span} \emptyset = \{0\} \qquad \operatorname{span} V = V$$

Theorem 2.5. *Let V is a vector space and $S \neq \emptyset$*

$$\operatorname{span} S = \{c_1\alpha_1 + \cdots + c_n\alpha_n \mid \alpha_i \in S,\ c_i \in \mathbb{F},\ n \in \natural\}$$

Proof. Let L be the set describe above. Clearly, $S \subset L$ and L is a subsapce of V hence $\operatorname{span} S \subset L$. Since $S \subset \operatorname{span} S$ and $\operatorname{span} S$ is closed under addition and scalar multiplication then $c_1\alpha_1 + \cdots + c_n\alpha_n \in \operatorname{span} S$ hence $L \subset \operatorname{span} S$. ∎

Definition: If $S_1, S_2, \ldots, S_k$ are subsets of a vector space V, the set of all sums

$$\alpha_1 + \alpha_2 + \cdots + \alpha_k$$

where $\alpha_i \in S_i$ is called the **sum** of subsets $S_1, S_2, \ldots, S_k$ and is denoted by

$$S_1 + \cdots + S_k = \{\alpha_1 + \alpha_2 + \cdots + \alpha_k \mid \alpha_i \in S_i\}$$

Theorem 2.6. *Let $W_1, W_2, \ldots, W_k$ be subspaces of vector space V. Then*

$$W = W_1 + W_2 + \cdots + W_k$$

is a subspaces of V. Moerover, $W = \operatorname{span} \cup W_i$.

Proof. Let $\alpha \in \operatorname{span} \cup W_i$ and $\beta \in W$. By Theorem 2.5, $\alpha = \alpha_1 + \cdots + \alpha_n$ where $\alpha_i \in \cup W_i$. Define $\alpha_1' = \sum_{\alpha_i \in W_1} \alpha_i$, $\alpha_2' = \sum_{\alpha_i \in W_2,\, \alpha_i \notin W_1} \alpha_i$ and so on. Clearly, $\alpha = \alpha_1' + \alpha_2' + \cdots + \alpha_k'$ thus $\alpha \in W$ and $\operatorname{span} \cup W_i \subset W$. By definition, $\beta = \beta_1 + \cdots + \beta_k$ where $\beta_i \in W_i$ and therefore, $\beta_i \in \cap W_i \subset \operatorname{span} \cup W_i$. Since $\operatorname{span} \cup W_i$ is a subspace of V then $\beta \in \operatorname{span} \cup W_i$ which implies $W = \operatorname{span} \cup W_i$. ■

2.3 Basis and Dimension

Definition (Linearly dependent): A set S of vector space V is said to be **linearly dependent**if there are $c_1, \ldots, c_n \in \mathbb{F}$ where at least one of the c_i is non-zero and $\alpha_1, \ldots, \alpha_n$ such that

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

Furthermore, S is **linearly independent** if it is not linearly dependent. That is, if $c_1\alpha_1 + \cdots + c_n\alpha_n = 0$ then $c_i = 0$ for all $i = 1, \ldots, n$.

Corollary 2.7. *If S is linearly dependent and $S \subset S'$ then S' is linearly dependent as well. If S is linearly independent and $S' \subset S$ then S' is linearly independent.*

Definition (Basis): Let V be a vector space over field $\mathbb{F}$. $S \subset V$ is a **basis** of V if it is linearly indepenent and spans V. Additionally, V is finite dimensional if V has a finite basis.

Theorem 2.8. *Let V be a vector space which is spanned by a $\beta_1, \ldots, \beta_m$. Then any independent subset of V contains at most m elements.*

Proof. needs matrices maybe. ■

Corollary 2.9. *If V is a finite dimensional vector space then any two bases of V have the same finite number of elements.*

Proof. Let α, β be two bases of V. By Theorem 2.8, $|\alpha| \le |\beta|$ and $|\beta| \le |\alpha|$ therefore they must have the same number of elements. Since, there exists a finite basis γ then α and β must be finite as well. ■

Definition (Dimension): **Dimension** of a finite dimensional vector space V, denoted by $\dim V$ is the number of elements of one of its basis.

Example 2.4. $\dim\{0\} = 0$ since $\operatorname{span}\emptyset = \{0\}$ and therefore $\dim\{0\} = |\emptyset| = 0$.

Corollary 2.10. *Let V be a finite dimensional vector space and let $n = \dim V$. Then*

1. *any subset of V whichi has more then n elements is linearly dependent.*
2. *no subset of V which contains fewer than n vectors can span V.*

Proof. 1. It is an immediate consequence of Theorem 2.8.

2. If there was a set $\beta = \{\beta_1, \dots, \beta_m\}$ with $m < n$ such that $V = \operatorname{span}\beta$ then there must be a basis β' such that $|\beta'| \leq m$. Which contradicts Corollary 2.9 ■

Lemma 2.11. *Let S be a linearly independent subset of vector space V. Suppose β is a vector in V not spanned by S. Then the set $S \cap \{\beta\}$ is linearly independent.*

Proof. Suppose $\alpha_1, \dots, \alpha_m$ are distinct vectors in S and that

$$c_1\alpha_1 + \cdots + c_m\alpha_m + b\beta = 0 \tag{2.1}$$

then if $b \neq 0$

$$\beta = -\frac{1}{b}(c_1\alpha_1 + \cdots + c_m\alpha_m)$$

and thus $\beta \in \operatorname{span} S$ which is a contradiction. ■

Theorem 2.12. *If W is a subspace of a finite dimensional vector space V then every linealy independent subset of W is finite and part of a basis of V and W.*