
Contents

1	Linear Equation	3
1.1	Fields	3
1.2	Matrices	4
1.3	Row-Reduced Echelon	6
2	Vector Spaces	7
2.1	Subspaces	8
2.2	Span	8

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

$$\underbrace{1 + 1 + \dots + 1}_n = 0 \tag{1.1}$$

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 is a prime number and $k \in \mathbb{N}$. Also for 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

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

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

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

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 matrices 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 **invertible** 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:

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n = y_1 \\ a_{21}x_1 + a_{22}x_2 + \dots + a_{2n}x_n = y_2 \\ \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mn}x_n = y_m \end{cases} \quad (1.2)$$

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

$$(c_1 a_{11} + c_2 a_{21} + \dots + c_m a_{m1})x_1 + \dots + (c_1 a_{1n} + c_2 a_{2n} + \dots + c_m a_{mn})x_n = c_1 y_1 + \dots + c_m y_m$$

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

Definition (Equivalent 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 represented in form of matrices $AX = Y$ where

$$A = \begin{bmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \dots & a_{mn} \end{bmatrix} \in \mathcal{M}_{m \times n}(\mathbb{F}) \text{ and } X = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}, Y = \begin{bmatrix} y_1 \\ \vdots \\ y_m \end{bmatrix}$$

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 row 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 necessarily 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 .

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

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

Transitive $A \sim B \implies A = p_1 p_2 \dots p_k B$, $B \sim C \implies B = q_1 q_2 \dots q_m C$ 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 row which has a non-zero entry.
3. if rows $1, \dots, r$ are the non-zero rows of A , and if the leading non-zero entry of row i occurs in column k_i , then $k_1 < k_2 < \dots < k_r$.

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 **elementary matrix** if it can be obtained from the \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. $\alpha + \beta = 0$.
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 $c(x_1, x_2, \dots, x_n) = (cx_1, cx_2, \dots, cx_n)$.

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 $\alpha_1, \alpha_2, \dots, \alpha_n$ if there exists scalars $c_1, c_2, \dots, c_n \in \mathbb{F}$ such that:

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

2.1 Subspaces

Let V be a vector space over field \mathbb{F} . A subspace 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 $\alpha_1 \notin W_1$. 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 infinite field \mathbb{F} . If W_1, W_2, \dots, W_n are subspaces of V and $V \subset \cup W_i$, then there exists k such that $V = W_k$.*

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 subspaces of V which contains S and is denoted by $\text{span } S$. That is, $\text{span } S = \bigcap_{S \subset W} W$. By Corollary 2.2, $\text{span } S$ is a linear subspace. Obviously, $\text{span } S$ is the smallest subspace containing S because if there were $S \subset K \subset \text{span } S$ since by definition $\text{span } S = \bigcap W \subset K$, then $K = \text{span } S$.

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

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

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

$$\text{span } S = \{c_1\alpha_1 + \dots + c_n\alpha_n \mid \alpha_i \in S, c_i \in \mathbb{F}, n \in \mathbb{N}\}$$

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