# Contents

**1 Linear Equation** **3**
1.1 Fields . . . . . 3
1.2 Matrices . . . . . 4
1.3 Row-Reduced Echelon . . . . . 6

# 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*

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

2. Addition and multiplication are *associative*

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

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.

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

**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 $c_k \in F,\ k = 1, \dots, n$:

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

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 $r_{\text{th}}$ 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 $4 \times 3$ 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.