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 $\mathbb{F} \subset \mathbb{F}[x] \subset \mathbb{F}(x)$.