# MT2123 - Advanced Linear Algebra

Nachiketa Kulkarni

# Contents

**1 Fields and Vector Spaces** **1**
- 1.1 Groups . . . . . . . . 1
- 1.2 Rings . . . . . . . . 1
- 1.3 Fields . . . . . . . . 1
  - 1.3.1 Detour 1 - Finite Fields . . . . . . . . 2

**2 Linear Transformations** **3**

# Chapter 1

# Fields and Vector Spaces

## 1.1 Groups

**Definition** A group $\langle G, * \rangle$ is a set $G$ with a binary operation $*$ such that the following axioms are satisfied:

1. Closure: For all $a, b \in G$, $a * b \in G$.
2. Associativity: For all $a, b, c \in G$, $a * (b * c) = (a * b) * c$.
3. Identity Element: There exists an element $I \in G$ such that for all $I \in G$, $a * I = I * a = a$. Here, $I$ is called as the identity element of $*$ in $G$.
4. Inverse: corresponding to every element $a \in G$, there exists an element $a' \in G$ such that $a{*}a' = a'{*}a = I$. Here, $a'$ is called as the inverse of $a$ in $G$.

## 1.2 Rings

**Definition** A ring $\langle R, +, \cdot \rangle$ is a set $R$ with two binary operations $+$ and $\cdot$, which we call addition and multiplication, such that the following axioms are satisfied:

1. $\langle R, + \rangle$ is an abelian/commutative group.
2. Multiplication is associative: For all $a, b, c \in R$, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
3. Distributive Property: For all $a, b, c \in R$, the Left Distributive Law, $a \cdot (b + c) = a \cdot b + a \cdot c$ and Right Distributive Law, $(a + b) \cdot c = a \cdot c + b \cdot c$.

## 1.3 Fields

**Definition** A field $\langle F, +, \cdot \rangle$ is a set $F$ with two binary operations $+$ and $\cdot$, which we call addition and multiplication, such that the following axioms are satisfied:

1. Closure: For all $a, b \in F$, $a + b \in F$ and $a \cdot b \in F$.
2. Associativity: For all $a, b, c \in F$, $a + (b + c) = (a + b) + c$ and $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
3. Commutativity: For all $a, b \in F$, $a + b = b + a$ and $a \cdot b = b \cdot a$.
4. Identity Elements: There exist two elements $I, O \in F$ such that for all $a \in F$, $I \cdot a = a$ and $O + a = a$. Here, $I$ is called as the multiplicative identity and $O$ is called as the additive identity.
5. Additive Inverse: For all $a \in F$, there exists an element $-a \in F$ such that $a + (-a) = O$. Here, $-a$ is called as the additive inverse of $a$.

6. Multiplicative Inverse: For all $a \neq O \in F$, there exists an element $a^{-1} \in F$ such that $a \cdot a^{-1} = I$. Here, $a^{-1}$ is called as the multiplicative inverse of $a$.

7. Distributivity: For all $a, b, c \in F$, the Left Distributive Law, $a \cdot (b+c) = a \cdot b + a \cdot c$ and Right Distributive Law, $(a+b) \cdot c = a \cdot c + b \cdot c$.

### 1.3.1 Detour 1 - Finite Fields

another long wall of text

# Chapter 2

# Linear Transformations

long wall of text incoming