MT2123 - Advanced Linear Algebra

Nachiketa Kulkarni

Contents

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

Theorem 1: $\mathbb{Z}_n$ is a field if and only if n is a prime number.

Proof: Let n be any Positive Integer. We can trivially show that for all n, Closure and Associativity of addition and multiplication, Additive Identity, Multiplicative Identity and Additive Inverse, Distributivity rules are satisfied. The only property we need to show is the existence of Multiplicative Inverse.

Case 1: n is a composite number with factors a, b. Assume $\mathbb{Z}_n$ is a field. As, a and b are factors of n, they are less the n, and hence belong to $\mathbb{Z}_n$. Now, $a \cdot b = 0$ in $\mathbb{Z}_n$, but the product of two non-zero elements cannot be zero in a field. Hence, $\mathbb{Z}_n$ cannot be a field, when n is composite.

Case 2: n is a prime number. We need to show that for all $a \neq 0 \in \mathbb{Z}_n$, there exists an element $a^{-1} \in \mathbb{Z}_n$ such that $a \cdot a^{-1} = 1$.
Let us take an element $a \in \mathbb{Z}_n$ such that $a \neq 0$. Now, we know that the GCD of a and n is 1. Hence, by Bézout's Identity, there exist integers x, y such that $ax + ny = \gcd(a, n) = 1$. Applying modulo n, we get $ax \equiv 1 \pmod{n}$. Hence, x is the multiplicative inverse of a in $\mathbb{Z}_n$.

1.4 Vector Spaces

Definition A Vector Space, defined over a field F of scalers, is a set of objects V with two operations, Vector addition and Scalar Multiplication and follows the following axioms:

1. Closure: For all $u, v \in V$, $u + v \in V$.

2. Commutative: for all $u, v \in V$, $u + v = v + u$.

3. Associativity: For all $u, v, w \in V$, $u + (v + w) = (u + v) + w$.

4. Additive Identity: There exists an element $O \in V$ such that for all $u \in V$, $O + u = u$.

5. Additive Inverse: For all $u \in V$, there exists an element $-u \in V$ such that $u + (-u) = O$.

6. Scalar Multiplication: For all $a \in F$ and $u \in V$, $a \cdot u \in V$. It has the following properties:
   (a) Multiplication by I: If I is the Multiplicative identity of F, then $I \cdot u = u$.
   (b) Unambiguous: for all $a, b \in F$ and $u \in V$, $(a \cdot b) \cdot u = a \cdot (b \cdot u)$.
   (c) Distributive: For all $a \in F$ and $u, v \in V$, $a \cdot (u + v) = a \cdot u + a \cdot v$ and $(a + b) \cdot u = a \cdot u + b \cdot u$.
   (d) Distributive: For all $a, b \in F$ and $u \in V$, $(a + b) \cdot u = a \cdot u + b \cdot u$.

1.5 Subspaces

Chapter 2

Linear Transformations

long wall of text incoming