Vector Spaces

Saravanan Vijayakumaran
sarva@ee.iitb.ac.in

Department of Electrical Engineering
Indian Institute of Technology Bombay

July 31, 2014

Vector Spaces

Let V be a set with a binary operation $+$ (addition) defined on it. Let F be a field. Let a multiplication operation, denoted by $\cdot$, be defined between elements of F and V. The set V is called a vector space over F if

- V is a commutative group under addition
- For any $a \in F$ and $\mathbf{v} \in V$, $a \cdot \mathbf{v} \in V$
- For any $\mathbf{u}, \mathbf{v} \in V$ and $a, b \in F$

$$\begin{aligned} a \cdot (\mathbf{u} + \mathbf{v}) &= a \cdot \mathbf{u} + b \cdot \mathbf{v} \\ (a + b) \cdot \mathbf{v} &= a \cdot \mathbf{v} + b \cdot \mathbf{v} \end{aligned}$$

- For any $\mathbf{v} \in V$ and $a, b \in F$

$$(ab) \cdot \mathbf{v} = a \cdot (b \cdot \mathbf{v})$$

- Let 1 be the unit element of F. For any $\mathbf{v} \in V$, $1 \cdot \mathbf{v} = \mathbf{v}$

Binary Operations

Definition

A binary operation on a set A is a function from $A \times A$ to A

Examples

- Addition on the natural numbers $\mathbb{N}$
- Subtraction on the integers $\mathbb{Z}$

Definition

A binary operation $\star$ on A is associative if for any $a, b, c \in A$

$$a \star (b \star c) = (a \star b) \star c$$

Definition

A binary operation $\star$ on A is commutative if for any $a, b \in A$

$$a \star b = b \star a$$

Groups

Definition

A set G with a binary operation $\star$ defined on it is called a group if

- The operation $\star$ is associative
- There exists an $e \in G$ such that for any $a \in G$

$$a \star e = e \star a = a.$$

  The element e is called the identity element of G
- For every $a \in G$, there exists an element $b \in G$ such that

$$a \star b = b \star a = e$$

Examples

- Addition on the integers $\mathbb{Z}$
- Modulo m addition on $\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}$

Commutative Groups

Definition

A group G is called a commutative group if its binary operation is commutative.

Commutative groups are also called abelian groups.

Examples

- Addition on the integers $\mathbb{Z}$
- Modulo m addition on $\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}$
- Examples of non-abelian groups?

Fields

Definition

A set F together with two binary operations $+$ and $*$ is a field if

- F is a commutative group under $+$. The identity under $+$ is called the zero element of F.
- The set of non-zero elements of F is a commutative group under $*$. The identity under $*$ is called the unit element of F.
- For any $a, b, c \in F$

$$a * (b + c) = a * b + a * c$$

Examples

- $\mathbb{R}$ with usual addition and multiplication
- $\mathbb{Q}$ with usual addition and multiplication
- $\mathbb{F}_2 = \{0, 1\}$ with mod 2 addition and usual multiplication

Vector Spaces

Let V be a set with a binary operation $+$ (addition) defined on it. Let F be a field. Let a multiplication operation, denoted by $\cdot$, be defined between elements of F and V. The set V is called a *vector space* over F if

- V is a commutative group under addition
- For any $a \in F$ and $\mathbf{v} \in V$, $a \cdot \mathbf{v} \in V$
- For any $\mathbf{u}, \mathbf{v} \in V$ and $a, b \in F$

$$\begin{aligned} a \cdot (\mathbf{u} + \mathbf{v}) &= a \cdot \mathbf{u} + b \cdot \mathbf{v} \\ (a + b) \cdot \mathbf{v} &= a \cdot \mathbf{v} + b \cdot \mathbf{v} \end{aligned}$$

- For any $\mathbf{v} \in V$ and $a, b \in F$

$$(ab) \cdot \mathbf{v} = a \cdot (b \cdot \mathbf{v})$$

- Let 1 be the unit element of F. For any $\mathbf{v} \in V$, $1 \cdot \mathbf{v} = \mathbf{v}$

$\mathbb{F}_2^n$ is a vector space over $\mathbb{F}_2$

- Addition in $\mathbb{F}_2^n$ is defined as component-wise addition modulo 2
- Multiplication between elements of $\mathbb{F}_2$ and $\mathbf{v} \in \mathbb{F}_2^n$ is defined as follows

$$
\begin{aligned}
0 \cdot \mathbf{v} &= \mathbf{0} \\
1 \cdot \mathbf{v} &= \mathbf{v}
\end{aligned}
$$

- $\mathbb{F}_2^n$ is a commutative group under addition
- All other properties are easy to verify

Subspaces

Definition

Let V be vector space over a field F. A subset S of V is called a subspace of V if it is also a vector space over F.

Theorem

Let S be a nonempty subset of a vector space V over a field F. Then S is a subspace of V if

- *For any $\mathbf{u}, \mathbf{v} \in S$, $\mathbf{u} + \mathbf{v}$ also belongs to S.*
- *For any $a \in F$ and $\mathbf{u} \in S$, $a \cdot \mathbf{u}$ is also in S.*

Questions? Takeaways?