# Vector Spaces

Vineet Sahula, *sahula@ieee.org*

Malaviya National Institute of Technology, Jaipur

I Odd Semester 2012

# Groups

1. A non-empty set $\mathcal{G}$ on which a binary operation $\circ$is defined,
2. provided, for $a, b, c \in \mathcal{G}$, the following properties hold-
    2.1 $P_1$: $(a \circ b) \circ c = a \circ (b \circ c)$ Associative law
    2.2 $P_2$: There exists $u \in \mathcal{G}$ such that $u \circ a = a \circ u = a$
    Existence of Identity element
    2.3 $P_3$: For each $a \in \mathcal{G}$, there exists $a^{-1} \in \mathcal{G}$ such that
    $a \circ a^{-1} = a^{-1} \circ a = u$

# Groups...

1. A group is *Abelian*, if the group operation is commutative; else it is *non-abelian*
2. Examples
   2.1 Set $I$ of integers, wrt addition
   2.2 Check set $A = \{-3, -2, -1, 0, 1, 2, 3\}$ wrt addition ?
   2.3 set of cuberoots of '1'
   $\Rightarrow A = \{\omega_1, \omega_2, \omega_3\} = \left\{-\frac{1}{2} + \frac{1}{2}\sqrt{3}\imath, -\frac{1}{2} - \frac{1}{2}\sqrt{3}\imath, 1\right\}$ wrt multiplication

# Properties of groups

# More Examples...(Groups)

1. Cyclic group: A group $\mathcal{G}$is called cyclic if, for some $a \in \mathcal{G}$, every $x \in \mathcal{G}$ is of the form $a^m$, where $m \in I$. The element $a$is called generator of $\mathcal{G}$.
2. Permutation group: The set $S_n$ of $n!$ permutations of $n$ symbols; let us term permutation operation as '$\circ$' then $S_n$ is group wrt this operation; since operation $\circ$ is not commutative, $S_n$ is non-abelian

# Homomorphism

- Let $\mathcal{G}$ be with $\circ$, and $\mathcal{G}'$ with $\Box$ be groups
- Homomorphic mapping means,
  - $\mathcal{G} \to \mathcal{G}' : g \to g'$ such that
    1. every $g \in \mathcal{G}$ has a unique image $g' \in \mathcal{G}'$
    2. if $a \to a'$ and $b \to b'$, then $a \circ b \to a' \Box b'$
    3. And if, every $g' \in \mathcal{G}'$ is an image, then we have a homnomorphism of $\mathcal{G}$ *onto* $\mathcal{G}'$ and $\mathcal{G}'$ is called homomorphic image of $\mathcal{G}$.

# Isomorphism

- If homomorphic mapping is also one-to-one (and is *onto*), i.e.,
  - $g \leftrightarrow g'$
  - $\mathcal{G}$ and$\mathcal{G}'$ are called *isomorphic* & the mapping is called *isomorphism*

# Rings

## Definition

- A non-empty set $\mathcal{R}$ is said to form a ring wrt binary operation addition $(+)$ and multiplication $(\times)$, provided, for arbitratry , the following properties hold:

| | | |
|---|---|---|
| $P_1$: | $(a+b)+c = a+(b+c)$ | *(associative law, +)* |
| $P_2$: | $a+b = b+a$ | *(commutative law, +)* |
| $P_3$: | *there exists* $z \in \mathcal{R}$ *such that* $a+z = z+a$ | *(existence of additive identity)* |
| $P_4$: | *For each* $a \in \mathcal{R}$ *there exists* $-a \in \mathcal{R}$ *such that* $a+(-a) = z$ | *(existence of additive inverse)* |
| $P_5$: | $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ | *(associative law,* $\times$*)* |
| $P_6$: | $a(b+c) = a \cdot b + a \cdot c$ | *(distributive law)* |
| $P_7$: | $(b+c)a = b \cdot a + c \cdot a$ | *(distributive law)* |

# Rings, examples

- Sets $I$, $Q$, $R$ and $C$ are rings
- Set $S = \{a, b\}$ with $+$ and $\times$
  - $\begin{array}{c|cc} + & a & b \\ \hline a & a & b \\ b & b & a \end{array}$ and $\begin{array}{c|cc} \cdot & a & b \\ \hline a & a & b \\ b & b & a \end{array}$
- Set $T = \{a, b, c, d\}$ with $+$ and $\times$
  - $\begin{array}{c|cccc} + & a & b & c & d \\ \hline a & a & b & c & d \\ b & b & a & d & c \\ c & c & d & a & b \\ d & d & c & b & a \end{array}$ and $\begin{array}{c|cccc} \cdot & a & b & c & d \\ \hline a & a & a & a & a \\ b & a & b & a & b \\ c & a & c & a & c \\ d & a & d & a & d \end{array}$
- Set $Q$ with addition ($\oplus$) and multiplication ($\odot$) defined by
  - $a \oplus b = a \cdot b$ and $a \odot b = a + b$
  - is not a ring, as $P_4$, $P_6$, and $P_7$ are not satisfied

# Properties of Rings

- Every ring is an abelian additive group
- There exists a unique aditive element $z$
- Each element has a unique additive inverse
- Cancellation law for addition holds
- $-(-a) = a$,-(a+b)=(-a)+(-b)
- $a \cdot z = z \cdot a = z$
- $a(-b) = -(ab) = (-a)b$

# Homomorphism & Isomorphism

A homomorphism (isomorphism) of the additive group of a ring $\mathcal{R}$into (onto) the additive group of ring $\mathcal{R}'$ which also preserves the second operation, is called a homomorphism (isomorphism) of $\mathcal{R}$ into (onto) $\mathcal{R}'$.

# Euclidean Ring

- Any communitative ring $\mathcal{R}$ having the property that to each $x \in \mathcal{R}$ a non-negative integer $\theta(x)$ can be assigned such that,
  - $\theta(x) = 0$ iff $x = z$, the zero element of $\mathcal{R}$
  - $\theta(x \cdot y) \geqslant \theta(x)$ when $x \cdot y \neq z$
  - for every $\mathcal{R}$ and $y \neq z \in \mathcal{R}$ ,
    - $x = y \cdot q + r \qquad 0 \leq \theta(r) < \theta(y)$

# Integral Domains & Divison Rings

Integral Domains A commucative ring $\mathcal{D}$, with unity and having no divisors of zero, is called an *integral domain*.

Divison Rings A ring $\mathcal{S}$, whose non-zero elements form a multiplicative group, is called a *divison rin*g (*skew field*).

# Divison Rings

- Thus, every divison ring $\mathcal{S}$ has a unity and each of its non-zero elements has a multiplicative inverse.
- Multiplication is however not necessarily commutative.

# Fields

- A ring $\mathcal{S}$, whose non-zero elements form an abelian multiplicative group is called a *field*.
- Every field is an integral domain

# Vector operations

- Scalar multiplication-
  - let vector be $\xi_1 = (a, b)$; the multiplication by 3, a scalar is defined as $3 \cdot \xi_1 = (3a, 3b)$
- Vector addition-
  - for two vectors, $\xi_1 = (a, b)$ and $\xi_1 = (c, d)$, $\xi = \xi_1 + \xi_2 = (a + c, b + d)$
- Let's denote by $V$, the set of all vectors in a plane, i.e. $V = R \times R$
  - $V$ has a zero element $\zeta = (0, 0)$; every $\xi$ has additive inverse; $\Rightarrow$ $V$ is an abelian group
  - for $s, t \in R$ and $\xi, \zeta \in V$; following properties holds
    - $s(\xi + \eta) = s\xi + s\eta \qquad (s + t)\xi = s\xi + t\xi \qquad s(t\xi) = (st)\xi$ $\mathbf{1}\xi = \xi$

# Vector Space

- Let $\mathcal{F}$ be a field and $V$ be an abelian addititve group such that there is a scalr multiplication of $V$ by $\mathcal{F}$, which associates with each $s \in \mathcal{F}$ and $\xi \in V$ the element $s\xi \in V$. Then $V$ is called a vector space over $\mathcal{F}$ provided, with $u$ the unity of $\mathcal{F}$, following holds
  - $s(\xi + \eta) = s\xi + s\eta \qquad (s + t)\xi = s\xi + t\xi \qquad s(t\xi) = (st)\xi$
    $u\xi = \xi$
- Sub space-
  - A non empty $U$ of a vector space $V$ over $\mathcal{F}$ is a *subspace* of $V$ provided $U$ is itself a vector space over $\mathcal{F}$.

# Vector Sub-space

**Theorem** A non-empty subset $U$ of a vector space $V$ over $\mathcal{F}$ is a subspace of $V$ iff $U$ is closed wrt scalar multiplication and vector addition as defined on $V$.

**Theorem** The set $U$ of all linear combinations of an arbitrary set $S$ of vectors ($2^{|S|}$) of a space $V$ is a sub space of $V$.

- In turn vectors of $S$ area called *generators* of the space $U$.
- Let $U = \{k_1\xi_1 + k_2\xi_2 + \cdots k_m\xi_m : k_i \in F\}$ be the space spanned by $S = \{\xi_1, \xi_2, \ldots, \xi_m\}$ a subset of vectors of $V$ over $\mathcal{F}$
- It remains to find minimum set of vectors necessary to span a given space $U$
  - as any $\xi_j$ if can be written as combination of other vectors of $S$, then $\xi_j$ may be excluded from $S$, and remaining vectors will still span $U$.

# Linear Dependence

- $\sum k_i\xi_i = k_1\xi_1 + k_2\xi_2 + \cdots k_m\xi_m = \zeta$
- A non-empty subset $S$ of a vector space $V$ over $\mathcal{F}$ is called *linearly dependent* over $\mathcal{F}$ iff there exists $k_1, k_2, \cdots k_m \in \mathcal{F} : \exists\, k_i \neq z$
- A non-empty subset $S$ of a vector space $V$ over $\mathcal{F}$ is called *linearly independent* over $\mathcal{F}$ iff there exists $k_1, k_2, \cdots k_m \in \mathcal{F} : every\ k_i = z$

**Theorem** If some one of the set $S = \{\xi_1, \xi_2, \ldots, \xi_m\}$ of vectors in $V$ over $\mathcal{F}$ is zero vecor $\zeta$, then necessarily $S$ is a linearly depdent set.

**Theorem** A set of non-zero vectors $S$ of $V$ over $\mathcal{F}$ is also *linearly dependent* iff some one of $\xi_j$can be expressed as linear combination of the vectors $\xi_1, \xi_2, \ldots, \xi_{j-1}$, which precedes it.

**Theorem** Any finite set $S$ of vectors, not all the zero vector, contains a linearly indepdendent subset $U$ which spans the same vector space as $S$.

# Bases of a Vector Space

- A set $S = \{\xi_1, \xi_2, \dots, \xi_m\}$ of vectors of a vector space $V$ over $\mathcal{F}$ is called a basis of $V$ provided
  1. $S$ is linearly independent set,
  2. the vectors of $S$ span $V$
- Let's define unit vectors of $V_n(\mathcal{F})$

$$
\begin{array}{rcl}
\epsilon_1 & = & (u, 0, 0, 0, \dots, 0, 0) \\
\epsilon_2 & = & (0, u, 0, 0, \dots, 0, 0) \\
\vdots & \vdots & \vdots \\
\epsilon_n & = & (0, 0, 0, 0, \dots, 0, u)
\end{array}
$$

- and consider linear combination,
  $\xi = a_1\epsilon_1 + a_2\epsilon_2 + \cdots a_n\epsilon_n = (a_1, a_2, \dots, a_n) \quad a_i \in \mathcal{F}$
- If $\xi = \zeta$, then $a_1, = a = \dots = a_n = z$; and hence $E = (\epsilon_1, \epsilon_2, \dots, \epsilon_n)$ is a linearly independent set.

# Bases of a Vector Space

Theorem If $S = \{\xi_1, \xi_2, \ldots, \xi_m\}$ is a basis of the vector space $V$ over $\mathcal{F}$ and $T = \{\eta_1, \eta_2, \ldots, \eta_n\}$ is any linearly independent set of vectors of $V$, then $n \leqslant m$.

Theorem As a consequence, if If $S = \{\xi_1, \xi_2, \ldots, \xi_m\}$ is a basis of the vector space $V$ over $\mathcal{F}$, then any $m + 1$ vectors of $V$ necessarily form a linearly dependent set.

Theorem Every basis of a vector space $V$ over $\mathcal{F}$has the same number of elements. This number is called *dimension* of $V$.

# Sub-spaces of a vector

- Let $V$, of dimension $n$, be a vector space over $\mathcal{F}$ and $U$, of dimension $n < m$ having $B = \{\xi_1, \xi_2, \ldots, \xi_m\}$ as basis, be a sub-space of $V$. Then, only $m$ of the unit vectors of $V$ can be written as linear combination of elements of $B$; hence there exist vectors of $V$ which are not in $U$.
  - $k_1\xi_1 + k_2\xi_2 + \cdots + k_m\xi_m + k\eta_1 = \zeta \qquad \forall k_i, k \in F$
  - now $k = z$ since otherwise $k^{-1} \in F$, and $\eta_1 = k^{-1}(-k_1\xi_1 - k_2\xi_2 - \cdots - k_m\xi_m)$, and $\eta_1 \in U$, which is contrary to definition of $\eta_1$ , hence PROVED.

**Theorem** If $B = \{\xi_1, \xi_2, \ldots, \xi_m\}$ is basis of $U \subset V$, $V$ having dimension $n$, there exist vectors $\eta_1, \eta_2, \ldots, \eta_{n-m}$ in $V$ such that $B \cup \{\eta_1, \eta_2, \ldots, \eta_{n-m}\}$ is basis of $V$.

**Theorem** If, in $V_n(R)$, a vector $\eta$ is orthogonal to each vector of the set $\{\xi_1, \xi_2, \ldots, \xi_m\}$, then $\eta$ is orthogonal to every vector of the space spanned by this set.

# Vector Spaces over R

- Let's focus on to vector space $V = V_n(R)$ over $R$.
  - for 2-dimensional vetors, $\xi = (a_1, a_{2)}$ and $\eta = (b_1, b_2)\cos\theta = \frac{a_1 b_1 + a_2 b_2}{|\xi| \cdot |\eta|}$
  - Hence, inner product is defined as, $\xi \cdot \eta = a_1 b_1 + a_2 b_2$
  - For n-dimensional $V_n(R)$, for all $\xi = (a_1, a_2, \ldots, a_n)$ and $\eta = (b_1, b_2, \ldots, b_n)$
    - $\xi \cdot \eta = \sum a_i b_i$
- Suppose in $V_n(R)$, a vector $\eta$ is orthogonal to each vector of the set $\{\xi_1, \xi_2, \ldots, \xi_m\}$, then $\eta$ is orthogonal to every vector of the space spanned by this set.

# Linear Transformations

- A linear transformation of a vector space $V(\mathcal{F})$ into a vector space $W(\mathcal{F})$ over the same field $F$ is a mapping $T$ of $V(\mathcal{F})$ into $W(\mathcal{F})$ for which
  - $(\xi_i + \xi_j)\, T = \xi_i T + \xi_j T$
  - $(s\xi_i)\, T = s\,(\xi_i T)$

# Linear Transformations, Ex.

- A linear transformation examples (pp 150/Schaum)
  - In cases, when $W(\mathcal{F}) = V(\mathcal{F})$, i.e. $T$ is mapping of $V(\mathcal{F})$ into itself,
  - $T : (x, y) \to (x \cos\alpha - y \sin\alpha, x \sin\alpha + y \cos\alpha)$
- Any linear transformation of a vector space into itself can be described completely by exibiting its effect on the unit basis vectors of the space.
- If $T$ is a transformation of $V(\mathcal{F})$ into itself and $W$ is a subspace of $V(\mathcal{F})$, then $W_T$ is also a subspace of $V(\mathcal{F})$; here $W_T = \{\xi T : \xi \in W\}$ is image of $W$ under $T$

# Algebra of Linear Transformations

- Let's denote by $\mathcal{A}$the set of all linear transformations of a given vector space $V(\mathcal{F})$ over $F$ into itself and $\mathcal{M}$ the set of all non-singular linear transformations in $\mathcal{A}$.
- Let addition $(+)$ and multiplication $(\cdot)$ on $\mathcal{A}$ defined by
  - $A + B: \ \ \xi(A+B) = \xi A + \xi B$
  - $A \cdot B: \ \ \xi(A \cdot B) = (\xi A)B$
  - scalar multiplication, $kA: \ \ \xi(kA) = (k\xi)A$