Determinant

Seanie Lee, Jonghwan Jang

23 March 2019

Definition 1. $\mu : \mathbf{V} \times \mathbf{V} \times \cdots \mathbf{V} \longrightarrow \mathbb{R}$ *is n-linear form on* $\mathbf{V}$
if $\mu(\ldots, \boldsymbol{v} + c\boldsymbol{w}, \ldots) = \mu(\ldots, \boldsymbol{v}, \ldots,) + c\mu(\ldots, \boldsymbol{w}, \ldots)$

Definition 2. *μ: n-linear form on $\boldsymbol{V}$. μ is alternating n-linear from, if* $\mu(\ldots, \boldsymbol{v}, \ldots, \boldsymbol{v}, \ldots) = 0$

Note. μ: alternating n-linear form on $\boldsymbol{V} \iff \mu(\ldots, \boldsymbol{v}, \ldots, \boldsymbol{w}, \ldots) = -\mu(\ldots, \boldsymbol{w}, \ldots, \boldsymbol{v}, \ldots)$

Proof. $\Longrightarrow$ Suppose that $\mu(\ldots, \boldsymbol{v} + \boldsymbol{w}, \ldots, \boldsymbol{v} + \boldsymbol{w}, \ldots) = 0 \quad \boldsymbol{v}, \boldsymbol{w} \in \boldsymbol{V}, c \in \mathbb{R}$. Since μ is n-linear form,

$$\mu(\ldots, \boldsymbol{v}, \ldots, \boldsymbol{v} + \boldsymbol{w}, \ldots) + \mu(\ldots, \boldsymbol{w}, \ldots, \boldsymbol{v} + \boldsymbol{w}, \ldots) = 0$$
$$\mu(\ldots, \boldsymbol{v}, \ldots, \boldsymbol{w}, \ldots) + \mu(\ldots, \boldsymbol{v}, \ldots, \boldsymbol{v}, \ldots) + \mu(\ldots, \boldsymbol{w}, \ldots, \boldsymbol{w}, \ldots) + \mu(\ldots, \boldsymbol{w}, \ldots, \boldsymbol{v}) = 0$$

Since $\mu(\ldots, \boldsymbol{v}, \ldots, \boldsymbol{v}) = \mu(\ldots, \boldsymbol{w}, \ldots, \boldsymbol{w}, \ldots) = 0, \quad \mu(\ldots, \boldsymbol{v}, \ldots, \boldsymbol{w}, \ldots) = -\mu(\ldots, \boldsymbol{w}, \ldots, \boldsymbol{v}, \ldots)$
$\therefore \mu(\ldots, \boldsymbol{v}, \ldots, \boldsymbol{w}, \ldots) = -\mu(\ldots, \boldsymbol{w}, \ldots, \boldsymbol{v}, \ldots)$
$\Longleftarrow$ Suppose that $\mu(\ldots, \boldsymbol{v}, \ldots, \boldsymbol{v}. \ldots) = -\mu(\ldots, \boldsymbol{v}, \ldots, \boldsymbol{v}, \ldots)$

$$\begin{aligned}
\mu(\ldots, \boldsymbol{v}, \ldots, \boldsymbol{v}. \ldots) &= -\mu(\ldots, \boldsymbol{v}, \ldots, \boldsymbol{v}, \ldots) \\
2\mu(\ldots, \boldsymbol{v}, \ldots, \boldsymbol{v}) &= 0 \\
\mu(\ldots, \boldsymbol{v}, \ldots, \boldsymbol{v}) &= 0
\end{aligned}$$

$\square$

Note.

$$\begin{aligned}
\mathbb{R}^n \times \cdots \times \mathbb{R}^n &\approx \mathfrak{M}_{n \times n}(\mathbb{R}) \\
(\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_n) &\hookleftarrow A = (\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_n)
\end{aligned}$$

Theorem 3. *Alternating n-linear form on $\mathbb{R}^n$ with $\mu(\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n) = 1$ is "determinant". i.e.* $\mu = \det$

Definition 4. *A group $\boldsymbol{G}$ consists of a set on which binary operation * is defined so that for each pair of elements a, b in $\boldsymbol{G}$ there is a unique element $a * b$ in $\boldsymbol{G}$, such that following conditions hold.*

(1). $(a * b) * c = a * (b * c) \quad \forall a, b, c \in \boldsymbol{G}$

(2). $\exists e \in \boldsymbol{G} a * e = e * a = a \quad \forall a \in \boldsymbol{G}$

(3). $a * b = b * a \quad \forall a, b \in \boldsymbol{G}$

Definition 5. *The groups that obey the axiom of commutativity are abelian groups*

Example 1. $(\mathbb{Z},+),(\mathbb{Q},+),(\mathbb{R},+),(\mathbb{C},+),(\mathfrak{M}_{n\times n}(\mathbb{R}),+)$ *are abelian. But* $(\mathfrak{M}_{n\times n}(\mathbb{R}),\times)$ *is not abelian, because it is not guranteed an inverse always exits* $\forall A \in \mathfrak{M}_{n\times n}$

Definition 6. $GL_n(R) := \{A \in \mathfrak{M}_{n\times n}(\mathbb{R}) | A \text{ is invertible}\}$ *and it is called general linear group.*

Note. $(GL_n(\mathbb{R}),\times)$ *is group but non-abelian*

Definition 7. *If* $\boldsymbol{H} \subseteq \boldsymbol{G}$ *and* $(\boldsymbol{H},*)$ *is also group, then* $\boldsymbol{H}$ *is subgroup of* $\boldsymbol{G}$ *and wrote* $\boldsymbol{H} \leq \boldsymbol{G}$

Theorem 8 (Subgroup Test). $\boldsymbol{H} \leq \boldsymbol{G} \iff ab^{-1} \in \boldsymbol{H} \quad \forall a,b \in \boldsymbol{H}$

Proof. $\Longrightarrow$ it is trivial to prove. proof omitted
$\Longleftarrow$ Suppose that $ab^{-1} \in \boldsymbol{H} \quad \forall a,b \in \boldsymbol{H}$

$$\begin{aligned} b := b^{-1}, &\text{ then } ab \in \boldsymbol{H} \\ b := a, &\text{ then } aa^{-1} = e \in \boldsymbol{H} \\ a := e, &\text{ then } b^{-1} \in \boldsymbol{H} \end{aligned}$$

$\therefore \boldsymbol{H}$ is group ☐

Example 2. $2\mathbb{Z} :== \{2a | a \in \mathbb{Z}\} \leq \mathbb{Z}$

Proof. $\forall a,b \in \mathbb{Z} \quad 2a + (-2b) = 2(a-b) \in 2\mathbb{Z} \quad \therefore 2\mathbb{Z} \leq \mathbb{Z}$ ☐

Definition 9. $n \in \mathbb{N}, [n] := \{1,2,\ldots,n\}$. σ *is permutation if* $\sigma : [n] \longrightarrow [n]$ *is bijection.*

Definition 10. $\mathfrak{S}_n := \{\sigma | \sigma : \text{permutation on } [n]\}\mathfrak{S}_n$ *is symmetric group and* $(\mathfrak{S}_n, \circ)$ *is a group.*

Definition 11. $\iota(a) = a \quad \forall a \in [n], \iota : [n] \longrightarrow [n]$

Note

(1). $\mathfrak{S}_n$ is non abelian group

(2). For convenience, we will write $\sigma \in \mathfrak{S}_n$ as follows. $\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$

Theorem 12. *Define an equivalence relation on* $[n]$ *for fixed* $\sigma \in \mathfrak{S}_n$ *as follows.*
$a \sim b \iff b = \sigma^k(a) \quad k \in \mathbb{Z}$. *Then* $\sim$ *is equivalence relation on* $[n]$

Proof. 1. reflexive
$a = \sigma^0(a) = a \quad \forall a \in [n]$
$\therefore a \sim a$

2. symmetric
Suppose that $a \sim b$. i.e. $b = \sigma^k(a)$
Since $(\sigma^k)^{-1} = (\sigma^{-1})^k, a = \sigma^{-k}(b)$
$\therefore b \sim a$

3. transitive
   Suppose that $a \sim b, b \sim c$. i.e. $b = \sigma^k(a), c = \sigma^l(b)$
   Since $c = \sigma^k(\sigma^l(a))$, $c = \sigma^{k+l}(a)$
   $\therefore c \sim a$

$\square$

Definition 13. $[a]_{eq} := \{b \in [n] \,|a \sim b\}$ *is orbit of a*

Example 3. $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 1 & 3 & 6 & 5 \end{pmatrix}$, $[1]_{eq} = \{1, 2, 4, 3\} = [2]_{eq} = [4]_{eq} = [3]_{eq}$
$[5]_{eq} = [6]_{eq} = \{5, 6\}$

Definition 14. $\mu \in \mathfrak{S}_n (n \geq 2)$ *is a cycle if the number of orbit whose size is geq 2 is at most 1.*

Theorem 15. *Every permutation is the product of disjoint cycles*

Note. disjoint cycle: the intersection of two maximum orbits in each cycle is empty and disjoint cycles are commutative

Definition 16. *A cycle of* $\sigma \in \mathfrak{S}_n$ *is transposition if* $|\sigma| = 2$

Theorem 17. *Every cycle is a product of transpositions. In general,* $(a_1 \cdots a_n) = (a_1\, a_n) \cdots (a_1\, a_2)$

Example 4. $\sigma = (2\,4\,5) = (2\,5)(2\,4) \in \mathfrak{S}_5$

$$2 \mapsto 4 \mapsto 4$$
$$4 \mapsto 2 \mapsto 5$$
$$5 \mapsto 5 \mapsto 2$$

Note.

$$\begin{aligned} \iota &= (1\,2)(1\,2) \\ &= (1\,2)(1\,2)(3\,4)(3\,4) \\ &= (1\,2)(1\,2)(3\,4)(3\,4) \cdots (n-1\; n)(n-1\; n) \end{aligned}$$

Definition 18. $\sigma \in \mathfrak{S}_n$ *is even if it is a product of transpositions where the number of transition is even, otherwise* σ *is odd.*

Definition 19. $\mathscr{A}_n := \{\sigma \in \mathfrak{S}_n | \sigma is\ even\}$*; the alternating subgroup of* $\mathfrak{S}_n$

Theorem 20.

$$\begin{aligned} sgn : \mathfrak{S}_n &\longrightarrow \{-1, 1\} \\ \sigma &\mapsto \begin{cases} -1 & \sigma \in \mathfrak{S}_n \setminus \mathscr{A}_n \\ +1 & \sigma \in \mathscr{A}_n \end{cases} \end{aligned}$$

sgn is group homomorphism (operation preserving).

Definition 21. $\mathfrak{B} = \{\boldsymbol{V}_1, \ldots, \boldsymbol{v}_n\}$ *: ordered basis for* $\boldsymbol{V}$, $\sigma \in \mathfrak{S}_n, \mathfrak{B}^\sigma := \{\boldsymbol{v}_{\sigma(1)}, \ldots \boldsymbol{v}_{\sigma(n)}\}$.
Permutation matrix is $[Id]_{\mathfrak{B}}^{\mathfrak{B}^\sigma}$

Example 5. $\mathfrak{B} = \{\boldsymbol{v}_1, \boldsymbol{v}_2, \boldsymbol{v}_3\}, \sigma = (1\,3\,2), \mathfrak{B}^\sigma = \{\boldsymbol{v}_3, \boldsymbol{v}_1, \boldsymbol{v}_2\}$

$$[Id]_{\mathfrak{B}}^{\mathfrak{B}^\sigma} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$