LA8 Permutations

KYB

Thrn, it's a Fact

mathrnfact@gmail.com

July 17, 2021

Overview

Ch4. Determinants and Eigenvalues
4.2 Further Properties of the Determinant Function

Ex 4.2.8

$A \in F^{m\times n}$, $B \in F^{n\times m}$ and $m > n$. Then $\det(AB) = 0$.

Ex 4.2.9

If $m < n$, show by example that both $\det(AB) = 0$ and $\det(AB) \neq 0$ are possible.

$\mathcal{P}(F)$ v.s. $F[x]$

- 공통점 : set of polynomials
- 차이점 :
  - $\mathcal{P}(F)$: as functions (so $\dim \leq |F|$)
  - $F[x]$: new algebraic objects (and $\dim = \infty$)

Example

Let $F = \mathbb{Z}_2$ and $x^2 + x, 0$.

- As functions: $x^2 + x = 0$
- As algebraic objects: $x^2 + x \neq 0$

Algebraic Object (set with some operations) : magma, quasi group, semi group, loop, monoid, group, etc.

Group

A group $(G, +)$ where $+ : G \times G \to G$ is

- $(a + b) + c = a + (b + c)$ (associativity)
- there exists $e \in G$ such that $a + e = e + a = a$ for all $a \in G$ (identity)
- for all $\in G$, there exists $b \in G$ such that $a + b = b + a = e$ (inverse)

If a group G satisfies $a + b = b + a$ for all $a, b \in G$, G is called an abelian group.

Ring and Module

A ring $(R, +, \cdot)$ is

- $(R, +)$ is an abelian group (and denote additive identity 0)
- $(ab)c = a(bc)$
- $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$.

If a ring R has e such that $ae = ea = a$ for all a, denote $e = 1$ and R is called a unital ring.

If R has no element such that $ab = 0$ but $a, b \neq 0$, R is called an domain.

If for all $a, b \in R$ satisfies $ab = ba$, R is called a commutative ring.

If R is commutative and domain, R is called an integral domain.

If an integral domain R satisfies every nonzero element has multiplicative inverse, R is called a field.

Let R be a ring and $(M, +)$ be an abelian group. If $\cdot : R \times M \to M$, (denote $r \cdot m = rm$) satisfies

- $r(m_1 + m_2) = rm_1 + rm_2$
- $(r_1 r_2)m = r_1(r_2 m)$
- if R has 1, then $1 \cdot m = m$,

M is called a R-module.

If R is a field, M is called a vector space over R.

If M is itself a ring and $r(m_1 m_2) = (rm_1)m_2 = m_1(rm_2)$, we call M a R-algebra.

$F[x]$ is a polynomial ring.

$$\cdot : F \times F[x] \to F[x] \text{ by } \alpha(a_n x^n + \cdots a_0) = \alpha a_n x^n + \cdots \alpha a_0$$

Then $F[x]$ is a vector space and $\alpha(p(x)q(x)) = (\alpha p(x))q(x) = p(x)(\alpha q(x))$. Thus $F[x]$ is a F-algebra.

Here,

$$a_n x^n + \cdots a_0 = b_m x^m + \cdots b_0 \iff m = n \text{ and } a_i = b_i \text{ for all } i$$

by definition.

Permutation

S_n is a group.

Some Notation

Let $\tau = S_n$.

(1) $\tau = (\tau(1), \cdots, \tau(n))$

(2) $[i, j](k) = \begin{cases} j & k = i \\ i & k = j \\ k & \text{otherwise} \end{cases}$

(3) Cycle notation $\langle k, \tau(k), \tau^2(k), \cdots, \tau^l(k) \rangle$.

- Two cycles $\langle a_1, \cdots, a_k \rangle$ and $\langle .1, \cdots, b_l \rangle$ are said to be disjoint if $\{a_1, \cdots, a_k\} \cap \{b_1, \cdots, b_l\} = \varnothing$. In this case, they commute, that is,

$$\langle a_1, \cdots, a_k \rangle \langle b_1, \cdots, a_l \rangle = \langle b_1, \cdots, b_l \rangle \langle a_1, \cdots, a_k \rangle$$

- $\langle a_1, \cdots, a_k \rangle = \langle a_2, \cdots, a_k, a_1 \rangle \cdots = \langle a_k, a_1, \cdots, a_{k-1} \rangle$ Thus by choosing $a_i = \min\{a_1, \cdots, a_k\}$, we can determine a cycle in a unique way.
- Every permutation is a composition of disjoint cycles.
- Every permutation is a composition of transposes.
- $\operatorname{sgn}(\tau) = (-1)^n$ where n is the number of transposes of τ.
- If $\tau = \tau_1 \cdots \tau_k$ where τ_i's are transposes, then

$$\tau^{-1} = \tau_k \cdots \tau_1$$

  and this implies $\operatorname{sgn}(\tau) = \operatorname{sgn}(\tau^{-1})$.
- $\operatorname{sgn}(\tau_1 \tau_2) = \operatorname{sgn}(\tau_1) \operatorname{sgn}(\tau_2)$.

Ex 4.2.6(b)

$f : S_n \to S_n$ by $f(\tau) = \tau^{-1}$ is bijection.

The End