Thrn
it's a Fact

Linear Algebra

튜터링

8. Permutations

Ex 4.2.8 $A \in F^{m\times n}$, $B \in F^{n \times m}$. $m > n$. Then $\det(AB) = 0$

$\square$ ① $F^m \xrightarrow{B} F^n \xrightarrow{A} F^m$ $\qquad m \times m$

$\mathrm{col}(AB) \leq \mathrm{col}(A) \longrightarrow \mathrm{rank}(AB) \leq n$

$m = \mathrm{nullity}(AB) + \mathrm{rank}(AB) \leq \mathrm{nullity}(AB) + n \quad 0 < m-n \leq \mathrm{nullity}(AB)$

Ex 4.2.9 $m < n$.

Show by example that both $\det(AB) = 0$ & $\det(AB) \neq 0$ possible.

$F^{2\times 3}$, $F^{3 \times 2}$

$$\begin{bmatrix} 1 & & \\ & 1 & \end{bmatrix} \begin{bmatrix} 1 & \\ & 1 \\ & \end{bmatrix} = \begin{bmatrix} 1 & \\ & 1 \end{bmatrix}$$

Th 4.4	$\mathcal{P}(F)$ vs $F[x]$	
공통점	set of polynomials	
차이점	functions dim $\leq \|F\|$	algebraic objects dim $=\infty$

$F = \mathbb{Z}_2 \qquad x^2 + x \ , \ 0$

as fct $\quad x=0 \to 0^2+0=0$

$\quad x=1 \to 1^2+1=0 \implies x^2+x=0$

$\hookrightarrow x = 0$ or 1 ($\forall$, $\cdots$)

as alg obj $\quad x^2+x \neq 0$

$\hookrightarrow x$ is "new object not in F"

$|F| = 4 \quad 0, 1, w, w+1$

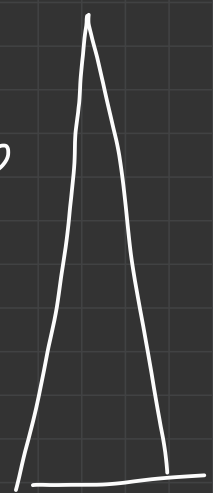
algebraic object $\leftarrow$ set w/ operation (binary operator)

$\hookrightarrow$
$\cdot : G \times G \to G$
$+ : R \times R \to R$
$\cdot : R \times M \to M$
$\vdots$

1 binary operator objects

$$\begin{tikzcd}
 & \text{magma} \arrow[dl, no head] \arrow[dr, no head] & \\
\text{quasi group} \arrow[d, no head] & & \text{semi group} \arrow[d, no head] \\
\text{loop} \arrow[dr, no head] & & \text{monoid} \arrow[dl, no head] \\
 & \text{group} &
\end{tikzcd}$$

연산의 규칙



group $(G, +)$ (or $(G, \cdot)$)

$+ : G \times G \longrightarrow G$ s.t.

- $(a+b)+c = a+(b+c)$ (associativity)
- $\exists e \in G$ s.t. $a+e = e+a = a$ $\forall a \in G$ (identity)
- $\forall a \in G$ $\exists b$ s.t. $a+b = b+a = e$ (inverse) → $b = -a$ (or $b = a^{-1}$ in $\cdot$)

notation

notation

if $+$ → $e = 0$

if $\cdot$ → $e = 1$

If a group G satisfies $\forall a, b \in G$ $a+b = b+a$, we call G an abelian group

2 operators Ring / Module

Ring $(R, +, \cdot)$

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

If a ring R has e s.t. $ae = ea = a$ $\forall e$, denote $e = 1$ and

R is called a unital ring

If R has no elt s.t. $ab = 0$ but $a, b \neq 0$,

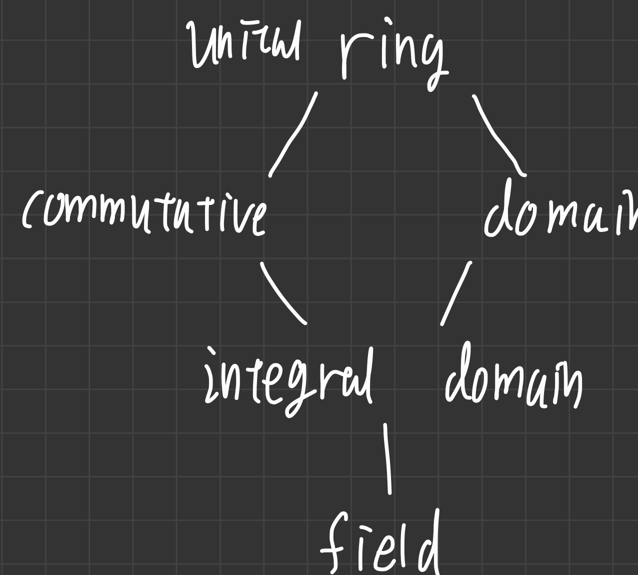
R is called an domain.

If $\forall a,b \in R$ 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 elt has multiplicative inverse, R is called a $\boxed{\text{field.}}$

i.e. $(R - \{0\}, \times)$ is a group



scalar multiplication $\longrightarrow$ module

Let R be a ring and $(M,+)$ abelian group.

If $\exists \cdot : R \times M \longrightarrow M$ (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, $1 \cdot m = m$

If R is a field, we say M is 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

$F[x]$: polynomial ring

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

$\Rightarrow F[x]$ $\boxed{\text{vector space}}$ & $\alpha(p(x)q(x)) = (\alpha p(x))q(x) = p(x)(\alpha q(x))$

$\Rightarrow F[x]$ is a F-algebra

$a_n x^n + \cdots + a_0 = b_m x^m + \cdots + b_0 \Longleftrightarrow$ ① $m = n$
② $\forall i \; a_i = b_i$

$\longrightarrow x^2 + x$ 와 0 을 구분 가능 in $\mathbb{Z}_2$

Permutation S_n is a group $\left(S_n = \{f : \{1, \cdots, n\} \to \{1, \cdots, n\} \mid f \text{ bij}\}\right.$

① $\tau_1, \tau_2 \in S_n \to \tau_1 \circ \tau_2 \in S_n$

② $(\tau_1 \circ \tau_2) \circ \tau_3 = \tau_1 \circ (\tau_2 \circ \tau_3)$

③ Let $i(x) = x \to \tau \circ i = i \circ \tau = \tau$ $\left(\Rightarrow \exists \text{ identity}\right)$

④ $\tau \circ \tau^{-1} = \tau^{-1} \circ \tau = i.$ $\left(\Rightarrow \exists \text{ inverse}\right)$

Notation $\tau \in S_n$

① $\tau = (\tau(1), \cdots, \tau(n)) \overset{\text{or}}{=} \begin{pmatrix} 1 & 2 & \cdots & n \\ \tau(1) & \tau(2) & & \tau(n) \end{pmatrix}$

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

$\langle 2\ 3\ 5 \rangle = \langle 3\ 5\ 2 \rangle = \langle 5\ 2\ 3 \rangle$

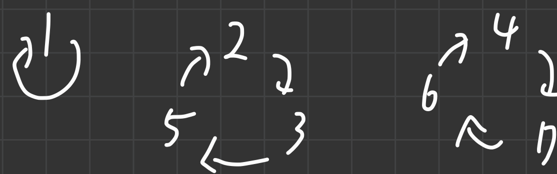
③ cycle notation $\langle k\ \tau(k)\ \tau^2(k)\ \cdots\ \tau^{\ell}(k) \rangle$

ex) $\tau = (1\ 3\ 5\ 7\ 2\ 4\ 6) = \langle 2\ 3\ 5 \rangle \langle 4\ 7\ 6 \rangle$

$\tau(1) = 1$

$\tau(2) = 3 \quad \tau(3) = 5 \quad \tau(5) = 2$

$\tau(4) = 7 \quad \tau(7) = 6 \quad \tau(6) = 4$



- two cycles are disjoint if $\langle a_1\ a_2 \cdots a_k\rangle, \langle b_1\ b_2 \cdots b_l\rangle$

$$\{a_1, \cdots, a_k\} \cap \{b_1, \cdots, b_l\} = \emptyset$$

$$\Downarrow$$

they commute $\langle a_1 \cdots a_k\rangle\langle b_1 \cdots b_l\rangle = \langle b_1 \cdots b_k\rangle\langle a_1 \cdots a_l\rangle$

& $\langle a_1 \cdots a_k\rangle = \langle a_2 \cdots a_k\ a_1\rangle = \cdots = \langle a_k\ a_1\ a_2 \cdots a_{k-1}\rangle$

$\Rightarrow$ By choose $a_i \in \min\{a_1, \cdots, a_k\}$, we can determine a cycle unique way.

- every permutation is a composition of disj cycles

① if τ is cyclic, done.

② choose a cycle $\langle 1\ \tau(1) \cdots\rangle, \langle n_1\ \tau(n_1) \cdots\rangle$, and so on.

$$n_1 = \min\{1, \cdots, n\} - \{1, \tau(1), \cdots\}$$

- Every permutation is a composition of transposes.

ETS only cyclic one.

Using induction on a length of cyclic

length $=2$, done.

$$\langle i\ \tau(i)\ \cdots\ \tau^{k-1}(i)\rangle = [i\ \tau(i)]\langle \tau(i)\ \cdots\ \tau^{k-1}(i)\rangle$$

or $$= \langle i\ \tau(i)\ \cdots\ \tau^{k-2}(i)\rangle[\tau^{k-2}(i)\ \tau^{k-1}(i)]$$

- $\operatorname{sgn}(\tau) = (-1)^{\#\text{ of transposes of } \tau}$

- $\tau = \tau_1 \cdots\cdots \tau_k$ where τ_i's are transposes

  $\Rightarrow \tau^{-1} = \tau_k \cdots \tau_1$ $\quad (\because \tau_i^2 = id)$

  $\Rightarrow \operatorname{sgn}(\tau) = \operatorname{sgn}(\tau^{-1})$

- $\operatorname{sgn}(\tau_1 \tau_2) = \operatorname{sgn}(\tau_1)\operatorname{sgn}(\tau_2)$ (multiplicative)

Ex 4.2.6 (b) $f: S_n \longrightarrow S_n$ by $f(\tau) = \tau^{-1}$ is bijection.

남은 내용 $L: V \to V$

★ eigen value & eigen vector (LA의 모든 것)

$\lambda \in F$ $x \in V - \{0\}$

s.t. $L(x) = \lambda x$

- diagonalize $A \in F^{n \times n}$

if $\exists (\lambda_i, x_i)$ $i = 1, \cdots, n$ s.t. $\{x_1, \cdots, x_n\}$ lin indp, define $X = [x_1 | \cdots | x_n]$

$D = \mathrm{diag}(\lambda_1, \cdots, \lambda_n)$

$$\to AX = [Ax_1 | \cdots | Ax_n] = [\lambda x_1 | \cdots | \lambda x_n]$$

$$= [x_1 | \cdots | x_n] \begin{bmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{bmatrix} = XD \to A = XDX^{-1}$$

- Jordan canonical form

$$A = X \begin{bmatrix} B_1 & & \\ & \ddots & \\ & & B_k \end{bmatrix} X^{-1} \qquad B_i \in F^{n_i \times n_i}, \quad \Sigma n_i = n$$

$$B_i = \begin{bmatrix} \lambda_i & 1 & & \\ & \lambda_i & 1 & \\ & & \ddots & \ddots \\ & & & \lambda_i \end{bmatrix}$$

$$X = [x_1^1 \mid x_2^1 \cdots \mid \cdots \mid x_1^k \mid \cdots \mid x_{n_k}^k]$$

$$Ax_1^i = \lambda_i x_1^i, \quad Ax_j^i = \lambda_i x_j^i + x_{j-1}^i$$

- Singular Value Decomposition (LA2)

$$A = U\Sigma V^T \quad \text{for } A \in \mathbb{R}^{m\times n}$$

$$A = U\Sigma V^* \quad \text{for } A \in \mathbb{C}^{m\times n}$$

singular value $\sigma \leftarrow$ e.val of $A^TA = \lambda \geq 0$ & $\sigma = \sqrt{\lambda}$

- 그외 LU 분해, QR 분해, PLU 분해, ...
  - └ Cholesky factorization