

§1 Lecture 02-14

$$T : V \rightarrow V$$

If $p_T(x)$ factors into linear factors, (for example if the field F is algebraically closed, then every irreducible polynomial is linear), then

$$V = \bigoplus_{\lambda \in \text{spec}(T)} V_{[\lambda]}$$

$$\text{Generalized eigenspace for } \lambda: V_{[\lambda]} = \{v : (T - \lambda)^j(v) = 0\}$$

$$\text{Eigenspace for } \lambda: V_{\lambda} = \{v : (T - \lambda)(v) = 0\}$$

$$V_{\lambda} = V_{[\lambda]} \Leftrightarrow (x - \lambda) | p_T(x) \text{ but } (x - \lambda)^2 \nmid p_T(x)$$

T is diagonalizable $\Leftrightarrow p_T(x)$ factors into distinct linear factors.

Theorem 1.1

T diagonalizable $\Leftrightarrow p_T(x)$ factors into distinct linear factors.

Example 1.2

$F = \mathbb{Z}/p\mathbb{Z}$. T satisfies $T^p = T \Rightarrow T$ satisfies $x^p - x \Rightarrow p_T(x)$ divides $x^p - x$.

This implies $p_T(x) = (x - \lambda_1)(\cdots)(x - \lambda_r)$, $\lambda_1 \neq \lambda_2 \neq \cdots \neq \lambda_r$. Therefore T is diagonalizable.

Example 1.3

$T^n = 1 \Rightarrow p_T(x)$ divides $x^n - 1$.

If $x^n - 1$ factors into distinct linear factors in F , then T is diagonalizable.

Conversely, if all T satisfying $T^n = 1$ are diagonalizable, then $x^n - 1$ factors into distinct linear factors.

In order to prove the converse, we need to show that $\exists T$ such that $p_T(x) = x^n - 1$.

$$\begin{aligned} V = F^n &= Fe_1 \oplus \cdots \oplus Fe_n \\ T(e_j) &= e_{j+1} \quad (j = 1, \dots, n-1) \\ T(e_n) &= e_1 \end{aligned}$$

Proposition 1.4

If $p(x) \in F[x]$, then \exists a vector space V over F , and $T : V \rightarrow V$ such that $p_T(x) = p(x)$.

Proof. Let $V = F[x]/(p(x))$. $\dim V = n$.

$$\begin{aligned} T(g(x) + (p(x))) &= xg(x) + (p(x)) \\ f(T)(g(x) + (p(x))) &= f(x)g(x) + (p(x)) \end{aligned}$$

If we want $f(T) = 0$ then $f(T)(1 + (p(x))) = 0 \Rightarrow f(x) + (p(x)) \Rightarrow p(x) | f(x) \Rightarrow p(x) = p_T(x)$ \square

Example 1.5

When is it possible to factor $x^n - 1$ in the following fields? $F = \mathbb{Q}$. Then $n \leq 2$.
 $F = \mathbb{R}$, then $n \leq 2$. $F = \mathbb{C}$, then any n . $F = \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.