0.1 H17 数学選択

L (1) 二次方程式は $x^2, x^2+1, x^2+x, x^2+x+1$ の 4 つである．このうち既約なものは根を $\mathbb{F}_2$ に持たないもの，すなわち x^2+x+1 である．

(2) 二次のモニック多項式は p^2 個ある．可約なモニック多項式は $(x-\alpha)(x-\beta)$ の形である．$\alpha \neq \beta$ に対して $(x-\alpha)(x-\beta) = (x-\beta)(x-\alpha)$ であることを踏まえると可約なモニック多項式の個数は $(p^2-p)/2+p = (p^2+p)/2$ である．

よって既約なモニック多項式の個数は $p^2-(p^2+p)/2 = (p^2-p)/2$ である．

(3)$x^2+1 \in \mathbb{F}_p[x]$ が既約 $\Leftrightarrow -1$ が平方剰余

-1 が平方剰余なら $^\exists x \in \mathbb{F}_p^\times$ が $x^4=1$ である．すなわち $\mathbb{F}_p$ は位数 4 の部分群を持つから $4|(p-1)$ である．

逆に $4|(p-1)$ なら sylow の定理から位数が 4 以上の 2-sylow 部分群 H が存在する．$x^2=1$ となる x は ± 1 のみであるから，位数が 4 以上であることより $^\exists x \in H$ が $x^2=-1$ である．よって -1 は平方剰余である．

すなわち x^2+1 が既約 $\Leftrightarrow p \equiv 1 \mod 4$ である．

M (1)$f^2 = \mathrm{id}$ より f は対角化可能であり F 上ベクトル空間として $V = W_1 \oplus W_{-1}$ と分解できる．ここで W_i は固有値 i の固有空間である．

$\varphi\colon V \to V_f; v \mapsto v+f(v)$ とすれば $\ker\varphi = W_{-1}$ である．全射でもあるから $\dim_F V_f = \dim_F V - \dim_F W_{-1}$ である．$W = W_1$ であるから $\dim_F W = \dim_F V - \dim_F W_{-1}$ である．よって $\dim_F V_f = \dim_F W$ である．

$f(v+f(v)) = f(v)+f^2(v) = f(v)+v$ より $V_f \subset W$ である．よって $V_f = W$ である．

K/F は二次拡大であるから $\sigma(\alpha) = -\alpha$ なる $\alpha \in K$ が存在する．W の F 上の基底 $\{v_1, v_2, \ldots, v_m\}$ をとる．

$\{\alpha v_1, \alpha v_2, \ldots, \alpha v_m\}$ は W_{-1} の基底となる．$v \in W_{-1}$ に対して $\alpha v \in W$ より $\alpha v = \sum_{i=1}^m a_i v_i$ より $\alpha^2 v = \sum_{i=1}^m a_i \alpha v_i, \alpha^2 \in F$ より W_{-1} を生成する．また $\sum c_i \alpha v_i = 0 \quad (c_i \in F)$ なら $\sum c_i v_i = 0$ であるから $c_i = 0$ である．よって $\{\alpha v_1, \alpha v_2, \ldots, \alpha v_m\}$ は W_{-1} の基底となる．

$u \in V$ に対して $u = u_1 + u_{-1} \quad (u_1 \in W_1, u_{-1} \in W_{-1})$ と一意にあらわせる．$u_1 \in W$ より $u_1 = \sum_{i=1}^m a_i v_i$ と表せる．また $u_{-1} = \sum_{i=1}^m b_i \alpha v_i$ と表せる．よって $u = \sum_{i=1}^m (a_i + b_i\alpha) v_i$ と表せる．すなわち $\{v_1, v_2, \ldots, v_m\}$ は K 上で V を生成する．

$\sum (a_i + b_i\alpha) v_i = 0 \quad (a_i, b_i \in F)$ とする．$\sum a_i v_i = 0 \in W, \sum b_i \alpha v_i = 0 \in W_{-1}$ である．よって $a_i = b_i = 0$ である．すなわち $\{v_1, v_2, \ldots, v_m\}$ は K 上で V の基底となる．

よって $m = n$ である．すなわち $\dim_F W = n$ である．