

0.1 H10 数学選択

[6] L/K を有限次 galois 拡大とする. $L[x]$ で $f(x) = g_1(x) \dots g_n(x)$ と既約元分解されたとする. $f(x)$ の最小分解体を F で表す. $i \neq j$ として g_i の根 α, g_j の根 β を任意にとって固定する. 既約であるから g_j は β の最小多項式と同伴である. $f(x)$ は K 上で既約であるから, $\sigma \in \text{Gal}(F/K)$ で $\sigma(\alpha) = \beta$ となるものが存在する. $\sigma(g_i)(\beta) = \sigma(g_i(\alpha)) = 0$ であるから $\sigma(g_i)$ は β を根にもつ. L/K が正規拡大であるから $\sigma|_L$ は L 上の K -自己同型である. よって $\sigma(g_i)$ は $L[x]$ の既約多項式である. よって $\sigma(g_i)$ も β の最小多項式と同伴である. すなわち $\deg g_i = \deg \sigma(g_i) = \deg g_j$ である.

[7] (1) $(p, x^2 + 1)$ が $\mathbb{Z}[x]$ 上素イデアル $\Leftrightarrow \mathbb{Z}[x]/(p, x^2 + 1)$ が整域. $\Leftrightarrow (\mathbb{Z}[x]/(p))/((p, x^2 + 1)/(p))$ が整域. $\Leftrightarrow \mathbb{F}_p[x]/(x^2 + 1)$ が整域. $\Leftrightarrow x^2 + 1$ が $\mathbb{F}_p[x]$ 上既約. $\Leftrightarrow -1$ が \mathbb{F}_p 上平方非剰余.

次が成り立つことを示す. -1 が \mathbb{F}_p 上平方剰余 $\Leftrightarrow 4 \mid (p-1)$.

\Rightarrow ある $x \in \mathbb{F}_p^\times$ が存在して $x^2 = -1$ となる. $x^4 = 1$ であるから x は位数 4 の元. よって $4 \mid (p-1)$.

$\Leftarrow 4 \mid |\mathbb{F}_p^\times|$ であるから sylow の定理より位数 4 以上の 2-sylow 部分群が存在する. $x^2 = -1$ をみたす $x \in \mathbb{F}_p^\times$ は高々 2 つであるから $x^2 = -1$ をみたす x が存在する.

以上より $(p, x^2 + 1)$ が $\mathbb{Z}[x]$ 上素イデアル $\Leftrightarrow 4 \nmid p-1$ である.

-1 が平方剰余でないについては平方剰余の相互法則の第一補加法則 $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ から $\frac{p-1}{2}$ が奇数であることと同値である. これは $p-1$ が 4 の倍数でないことと同値である.