有限次代数拡大の基本的な不等式

L/K: 有限次 (代数) 拡大

$K \subset L \subset \Omega$: 代数閉体

$$\#\mathrm{Aut}(L/K) \leq \#\mathrm{Emb}_K(L, \Omega) \leq [L : K]$$

特に $L = K(x)$: 単拡大のときは、

$f(X) := \mathrm{Irr}(x/K; X) \in K[X]$

: x の K 上の最小多項式として、

$$\#(\mathrm{Conj}(x, K) \cap L) \leq \#\mathrm{Conj}(x, K) \leq \deg f$$

$L = K(x), f(X) = \mathrm{Irr}(x/K; X) \in K[X]$ の時

$$\#(\mathrm{Conj}(x, K) \cap L) \leq \#\mathrm{Conj}(x, K) \leq \deg f$$

左の等号 $\iff \mathrm{Conj}(x, K) \subset K(x)$

$\iff K(x)/K$: 正規

右の等号 $\iff f$ の根の個数が $(\deg f)$ 個

$\iff f$: **重根**なし

$\iff f' \neq 0$

$$f: \text{ **重根あり** } \iff \gcd(f, f') \neq 1$$

特に f **: 既約とすると、**

$$\begin{aligned} f: \text{ **重根あり** } &\iff \gcd(f, f') \neq 1 \\ &\iff \gcd(f, f') = f \\ &\iff f | f' \\ &\iff f' = 0 \end{aligned}$$

これが起こり得るのは標数が $p > 0$ **のとき**

標数 (characteristic)

$$\exists ! \iota : \boldsymbol{Z} \longrightarrow K : \textbf{環準同型}$$
$$1 \longmapsto 1_K$$

$\mathrm{Ker} f =: (p)$ **(**p **は素数または** 0**)**

$\mathrm{ch} K := p$ **: 体** K **の標数**

(1_K **を幾つ足したら** 0_K **になるかという個数)**

Frobenius 同型

$\mathrm{ch}K = p > 0$ **のとき、**

$$\begin{aligned} \varphi_p : K &\longrightarrow K \\ x &\longmapsto x^p \end{aligned}$$

: 体の (中への) 同型

"Frobenius 同型"

即ち、

$$(a+b)^p = a^p + b^p$$

$$(ab)^p = a^p b^p$$

(正標数に特有の現象)

有限体

$\boldsymbol{F}_p := \boldsymbol{Z}/p\boldsymbol{Z}$: 標数 $p > 0$ の素体

有限体の位数は $q = p^r$ に限る ($\boldsymbol{F}_p$ の r 次拡大)

逆に $q = p^r$ に対し、位数 q の有限体が
(同型を除いて／固定した代数閉体内に)
一意に存在 ($=: \boldsymbol{F}_q$)

$\boldsymbol{F}_q$ は $X^q - X$ の根全体と一致

$\boldsymbol{F}_q^\times$ は位数 $(q-1)$ の巡回群