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**

重根

$f(X) \in K[X],\ K \subset \Omega,\ a \in \Omega$ に対し

f が $X = a$ で (少なくとも) m **重根**

$$\iff \exists g(X) \in \Omega[X] : f(X) = (X-a)^m g(X)$$

$$\iff f(a) = f'(a) = \cdots = f^{(m-1)}(a) = 0$$

$$\left(\begin{array}{rl} \text{丁度 } m \text{ 重} & \iff (X-a) \nmid g(X) \\ & \iff g(a) \neq 0 \\ & \iff f^{(m)}(a) \neq 0 \\ \multicolumn{2}{c}{\text{この時、} (X-a)^m \| f(X) \text{ とも書く}} \end{array}\right)$$

重根

$$f \text{ が } X = a \text{ で重根} \iff f(a) = f'(a) = 0$$
$$\iff (X-a) | f(X), f'(X)$$
$$\iff (X-a) | \gcd(f, f')$$

従って、

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

ところで、

$x \in \overline{K}, f(X) = \mathrm{Irr}(x/K; X) \in K[X]$ **の時、**
f **は** $K[X]$ **内で既約であった。**

重根

$$
\begin{aligned}
f \text{ が } X = a \text{ で重根} &\iff f(a) = f'(a) = 0 \\
&\iff (X-a) | f(X), f'(X) \\
&\iff (X-a) | \gcd(f, f')
\end{aligned}
$$

従って、

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

ところで、

$x \in \overline{K}, f(X) = \mathrm{Irr}(x/K; X) \in K[X]$ **の時、**
f **は** $K[X]$ **内で既約であった。**

$x \in \overline{K}, f(X) = \mathrm{Irr}(x/K; X) \in K[X]$ の時、
f は $K[X]$ 内で既約であった。

f : 既約とすると、

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

ところで、$\deg f' < \deg f$ だから、$f' = 0$
これは f が定数の時しかあり得ないから、

f : 既約 $\Longrightarrow$ f : 重根なし

と言いたい所だが $\cdots$

$x \in \overline{K}, f(X) = \mathrm{Irr}(x/K; X) \in K[X]$ の時、
f は $K[X]$ 内で既約であった。

f：既約とすると、

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

ところで、$\deg f' < \deg f$ だから、$f' = 0$
これは f が定数の時しかあり得ないから、

f：既約 $\Longrightarrow f$：重根なし

と言いたい所だが $\cdots$

例: $f(X) = X^p \in \boldsymbol{F}_p[X], \quad \boldsymbol{F}_p = \boldsymbol{Z}/p\boldsymbol{Z}$
(p: 素数)

この時、$f'(X) = pX^{p-1} = 0$ **!! (**$p = 0$ **だから)**

この例は安直過ぎて f**: 既約ではないが、**
次のような例もある。

例: $f(X) = X^p - T \in \boldsymbol{F}_p(T)[X]$

$f(X)$ **は** $\boldsymbol{F}_p(T)$ **上既約で、**$f'(X) = 0$ **!!**
$\longrightarrow$ **これは重根？**

例: $f(X) = X^p \in \boldsymbol{F}_p[X], \quad \boldsymbol{F}_p = \boldsymbol{Z}/p\boldsymbol{Z}$
(p**: 素数)**

この時、$f'(X) = pX^{p-1} = 0$ **!! (**$p = 0$ **だから)**

この例は安直過ぎて f**: 既約ではないが、**
次のような例もある。

例: $f(X) = X^p - T \in \boldsymbol{F}_p(T)[X]$

$f(X)$ **は** $\boldsymbol{F}_p(T)$ **上既約で、**$f'(X) = 0$ **!!**
$\longrightarrow$ **これは重根？**

しかし、例えば Q 上では
$p = 0$ などということは起こらず、

$$\deg f' = \deg f - 1$$

$$f' = 0 \Longrightarrow f : \text{定数}$$

が言えるので、

$$f \text{ : 既約} \Longrightarrow f \text{ : 重根なし}$$

が確かに成り立つ。

この状況を区別する概念
$\cdots$ 標数 (characteristic)

しかし、例えば Q 上では
$p = 0$ などということは起こらず、

$$\deg f' = \deg f - 1$$

$$f' = 0 \Longrightarrow f : \text{定数}$$

が言えるので、

$$f : \text{既約} \Longrightarrow f : \text{重根なし}$$

が確かに成り立つ。

この状況を区別する概念
$\cdots$ **標数** (characteristic)

有限 abel 群の構造定理

G: 有限 abel 群に対し

$$\exists! n_1, \ldots, n_r \geq 1 : G \simeq \boldsymbol{Z}/n_1\boldsymbol{Z} \times \cdots \times \boldsymbol{Z}/n_r\boldsymbol{Z}$$

$$(n_1 | \cdots | n_r)$$

特に、

$$G：\text{巡回群} \iff r = 1$$