

単拡大の構造 (平成26年)

単拡大は添加による拡大であるが, 剰余環による拡大とも考えられる.

定 理 k : 体
 $k[X] \in k[X]$ を既約多項式とする.
 \Rightarrow
 $f(X)$ の 分解体 (k の拡大体) が存在する.

証 明

- (i) $\deg f(X) = 1$ のとき $f(X)$ は k 上の一次式だから分解している.
 (ii) $1 \leq \deg f(X) < n$ のとき $f(X)$ は一次式の積に分解していると仮定する.

剰余環 $K = k[X] / (f(X))$ は $x = \alpha_1 \pmod{f(X)}$ を含む体で, 次のように分解する.

$$f(X) = (X - \alpha_1) f_1(X) \quad \deg f_1(X) < n$$

$\deg f_1(X) < n$ だから仮定より k の拡大体 K で $f_1(X)$ は一次式の積に分解する.

- (iii) よって K の拡大体 L 上で一次の積に分解する.

拡大体	多項式環	多項式
$L = K(\alpha_1)$...	$K(X) / (f_1(X))$
$K = k(\alpha)$...	$k[X] / (f(X))$... $f_1(X)$
k	...	$k[X]$... $f(X)$

定 理 剰余環 $K = k[X] / I$ は体である. ただし $I = (f(X))$

証 明 $I + g \in k[X] / I$

$(f, g) = 1$ とする.

$af + bg = 1$ なる a, b がある.

$$(I + a)(I + g) + (I + b)(I + f) = I + 1$$

$I + f$: 零元, $I + 1$: 単位元

$$\therefore (I + a)(I + g) = I + 1$$

$\therefore I + a$ は $I + g$ の逆元

$K = k[X] / I$ は体である.

定 理 体 k 上の n 次多項式を

$$f(X) = X^n + a_1 X^{n-1} + \cdots + a_n \text{ とする.}$$

α を X のイデアル $(f(X))$ を法とする類とする.

即ち, $\alpha \in X \pmod{(f(X))}$ とする.

(i) $f(\alpha) = 0$

(ii) 剰余環 $K = k[X] / (f(X))$ は $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$ を基底とする k 上 n 次元線形空間をなす.

証 明

(i) $\alpha \in X \pmod{(f(X))}$ だから

$$\alpha = \alpha + f(\alpha)$$

$$\therefore f(\alpha) = 0$$

(ii) $k(X) \in k[X]$ とし, $k(X)$ を $f(X)$ で割ったときの剰余を $r(X)$ とする.

$$k(X) = q(X)f(X) + r(X)$$

$$\deg r(X) < \deg f(X) = n$$

$$\therefore r(X) = c_0 + c_1 X + \cdots + c_{n-1} X^{n-1}$$

$$c_0, c_1, \dots, c_{n-1} \in k$$

$$\therefore K = k(\alpha) = r(\alpha) = c_0 + c_1 \alpha + \cdots + c_{n-1} \alpha^{n-1}$$

$$c_0, c_1, \dots, c_{n-1} \in k$$

単拡大体 $k(\alpha)$ は $1, \alpha, \dots, \alpha^{n-1}$ の一次結合で表される.

次に $c_0 + c_1 \alpha + \cdots + c_{n-1} \alpha^{n-1} = 0$ とおくと, $c_0 = c_1 = \cdots = c_{n-1} = 0$

$$\therefore r(X) = c_0 + c_1 X + \cdots + c_{n-1} X^{n-1} \equiv 0 \pmod{(f(X))}$$

$$\therefore f(X) \mid r(X)$$

$$\deg r(X) < \deg f(X) \text{ だから } r(X) = 0$$

$$\therefore c_0 = c_1 = \cdots = c_{n-1} = 0$$

よって, $1, c_0, c_1, \dots, c_{n-1}$ は一次独立である.

引用文献

代数の世界 渡辺 敬一 草場 公邦 著 朝倉書店 2004
ガロアの理論 I スチュワート著 新関 章三 訳 共立出版 1954