

【訂正情報】

商品コード: 110-9340

ISBN : 9784800593405

初学者のために何度も書き直した 基礎からの「ガロア理論」

初歩の概念から最新の応用までをていねいに解説

◎本書の記述において下記のような誤りがありました。

訂正してお詫び申し上げます。 【2025 年 10 月 21 日現在】

- 第 1 刷, p. 119, 1～6 行目

訂正前: $f(x)$ は,

$$f(\bar{0}) = f(\bar{1}) = \bar{1} \neq \bar{0}$$

と定理 31 (1) (因数定理) により 1 次式で割り切れないこと,

$$f(x) = (x^2 + ax + 1)(x^2 + bx + 1)$$

を満たす $\mathbb{F}_2$ の元 a, b が存在しないことから既約であり, $f(x) = g(x^2)$ の形に表せるから定理 35 により分離的でない.

訂正後: (1～6 行目を削除し, 次の文章をもとの 11 行目の直後に入れる)

$f(x)$ は

$$f(x) = (x^2 + x + \bar{1})^2 = g(x)^2$$

と表せ, $g(x)$ は $\mathbb{F}_2$ 上既約な分離多項式で重根をもたないから, $f(x)$ は分離的である.

- 第 1 刷, p. 186, 24～28 行目

訂正前: HN の任意の元 $hn, h'n'$ ($h, h' \in H, n, n' \in N$) に対して

$$(hn)(h'n') = h(nh')n' = h(h'n)n' = (hh')(nn'),$$

$$(hn)^{-1} = n^{-1}h^{-1} = n^{-1}h^{-1}nn^{-1} = n^{-1}nh^{-1}n^{-1} = h^{-1}n^{-1}$$

も HN の元になる

訂正後: HN の任意の元 $hn, h'n'$ ($h, h' \in H, n, n' \in N$) に対して, $h'^{-1}nh'$, $hn^{-1}h^{-1} \in N$ であり, よって

$$(hn)(h'n') = hh'h'^{-1}nh'n' = (hh')((h'^{-1}nh')n'),$$

$$(hn)^{-1} = h^{-1}hn^{-1}h^{-1} = h^{-1}(hn^{-1}h^{-1})$$

も HN の元になる

- 第 1 刷, p. 236, 2 行目

訂正前: $\sigma: L \rightarrow L'$

訂正後: $\tilde{\sigma}: L \rightarrow L'$

- 第 1 刷, p. 238, 7 行目

訂正前: 有限次拡大

訂正後: 有限次ガロア拡大

- 第 1 刷, p. 242, 2 行目

訂正前: m_i は $p_i - 1$ 倍して初めて p_i の倍数になる

訂正後: m_i は $p_i - 1$ 乗して初めて p_i の倍数になる

- 第 1 刷, p. 244, 3 行目

訂正前: (1) が成り立つ

訂正後: (1) が成り立つ.

- 第 1 刷, p. 247, 11~12 行目の間

訂正前: (記述なし)

訂正後: (この正誤表の別紙の文章を入れる)

- 第 1 刷, p. 247, 12~14 行目

訂正前: 証明 (1) L は, 仮定により K 上のある多項式 $f(x)$ の K 上の最小分解体であるから, M 上の多項式とみなした $f(x)$ の M 上の最小分解体でもある. よって, L/M はガロア拡大である.

訂正後: 定理 81 の証明 (1) L は, 補題 (3) により K 上のある分離多項式 $f(x)$ の K 上の最小分解体であるから, M 上の多項式とみなした $f(x)$ (これも分離多項式) の M 上の最小分解体でもある. よって, 補題 (3) により L/M はガロア拡大である.

- 第 1 刷, p. 248, 21 行目

訂正前: ガロア拡大

訂正後: 正規拡大

- 第 1 刷, p. 249, 3~4 行目の間

訂正前: (記述なし)

訂正後: また, 補題 (2) により L/K は分離拡大であるから, L/K はガロ

ア拡大である.

- 第 1 刷, p. 249, 4~7 行目

訂正前 : L が K 上の多項式 $f(x)$ の K 上の最小分解体であるとし, α の K 上の最小多項式を $g(x)$ とする. このとき, $L' = L(\alpha)$ は K 上の多項式 $f(x)g(x)$ の最小分解体であるから, L'/K はガロア拡大であり, したがって (1) により L'/K' はガロア拡大である.

訂正後 : 補題 (3) により, K 上の分離多項式 $f(x) = (x - \alpha_1) \cdots (x - \alpha_n)$ ($\alpha_i \in L$) で $L = K(\alpha_1, \dots, \alpha_n)$ を満たすものが存在する. このとき, $L' = K'(\alpha_1, \dots, \alpha_n)$ が成り立つから, L' は K' 上の多項式とみなした $f(x)$ (これも分離多項式) の K' 上の最小分解体である. よって, 補題 (3) により L'/K' はガロア拡大である.

【別紙】

証明には、次の補題を用いる.

《補題》 L/K を体の有限次拡大とし、 L'/K が正規拡大であるような L の拡大体 L' (例えば L に K 上の生成元の共役元をすべて添加した体) をとる. また、 M を L/K の中間体とする. このとき、

$$(1) (a) \quad \# \text{Hom}_M(L, L') \cdot \# \text{Hom}_K(M, L') = \# \text{Hom}_K(L, L')$$

$$(b) \quad L/K \text{ が分離拡大} \iff \# \text{Hom}_K(L, L') = [L : K]$$

$$(2) \quad L/K \text{ が分離拡大} \iff L/M, M/K \text{ が分離拡大}$$

$$(3) \quad L/K \text{ がガロア拡大} \iff L \text{ が } K \text{ 上のある分離多項式の最小分解体が成り立つ.}$$

補題の証明

(1) (a) 全単射 $\text{Hom}_M(L, L') \times \text{Hom}_K(M, L') \rightarrow \text{Hom}_K(L, L')$ を利用して、[定理 78](#) と同様に示される.

(b) まず、 $L = K(\alpha)$ のとき、 $\text{Hom}_K(L, L')$ の元 σ は $\sigma(\alpha)$ の値で決まるから、 α の K 上の最小多項式 $f(x)$ について $\# \text{Hom}_K(L, L') \leq \deg f(x) = [L : K]$ が成り立ち、等号成立は $f(x)$ が重根をもたない、つまり α が K 上分離的であるときに限ることに注意する.

($\implies$) を示す. L は $L = K(\alpha_1, \dots, \alpha_r)$ の形に表せるから、 $K_0 = K$, $K_i = K_{i-1}(\alpha_i)$ ($1 \leq i \leq r$) とすると、 L/K が分離拡大であるならば、各番号 i ($1 \leq i \leq r$) に対して α_i は K 上分離的であり、よって K_{i-1} 上分離的であるから、 $\# \text{Hom}_{K_{i-1}}(K_i, L') = [K_i : K_{i-1}]$ が成り立ち、辺々を掛け合わせると (a) により $\# \text{Hom}_K(L, L') = [L : K]$ が得られる.

($\impliedby$) を示すため、 $\# \text{Hom}_K(L, L') = [L : K]$ が成り立つとする. α を L の元として $M = K(\alpha)$ とおく. このとき、(a) により $[L : K] = \# \text{Hom}_M(L, L') \cdot \# \text{Hom}_K(M, L') \leq [L : M][M : K] = [L : K]$, よって $\# \text{Hom}_K(M, L') = [M : K]$ が成り立つから、上記の注意により α は K 上分離的である. ゆえに、 L/K は分離的である.

(2) ($\implies$) を示すため、 L/K が分離拡大であるとする.

- L の各元 α に対して、 α の M 上の最小多項式 $g(x)$ は α の K 上の最小多項式 $f(x)$ を割り切り、 $f(x)$ は重根をもたないから、 $g(x)$ は重根をもたず、よって α は M 上分離的である. ゆえに、 L/M は分離的である.
- M の各元は L に属するから K 上分離的であり、 M/K は分離的である.

($\impliedby$) を示すため、 $L/M, M/K$ が分離拡大であるとする. α を L の元、 $f(x) = x^n + c_{n-1}x^{n-1} + \dots + c_0$ ($c_i \in M$) を α の M 上の最小多項式として、 $E = K(c_0, \dots, c_{n-1})$ とおく. $f(x)$ は E 上の多項式であり、 L/M が分離的であることにより $f(x)$ は重根をもたないから、 α は E 上分離的である. よって、(1) の注意により $\# \text{Hom}_E(E(\alpha), L') = [E(\alpha) : E]$ である.

また、 $M \supset E \supset K$ で、 M/K が分離拡大であることから、 $(\implies)$ により E/K は分離拡大で、(1)(b) により $\#\mathrm{Hom}_K(E, L') = [E : K]$ である。辺々を掛け合わせると (1)(a) により $\#\mathrm{Hom}_K(E(\alpha), L') = [E(\alpha) : K]$ が得られるから、(1)(b) により $E(\alpha)/K$ は分離拡大で、 α は K 上分離的である。ゆえに、 L/K は分離拡大である。

- (3) $(\implies)$ を示す。 L/K が有限次ガロア拡大であるとき、[定理 77](#) により L は K 上のある多項式 $f(x)$ の最小分解体であり、 $f(x)$ を割り切るような K 上の既約多項式はその根が K 上分離的であることにより重根をもたないから、 $f(x)$ は分離的である。

$(\impliedby)$ を示す。 L が K 上の分離多項式 $f(x) = (x - \alpha_1) \cdots (x - \alpha_n)$ ($\alpha_i \in L$) の最小分解体であるとする。このとき、[定理 77](#) により、 L/K は正規拡大である。また、 $K_0 = K$, $K_i = K_{i-1}(\alpha_i)$ ($1 \leq i \leq n$) とする。各番号 i ($1 \leq i \leq n$) に対して、 α_i の K_{i-1} 上の最小多項式 $g_i(x)$ は α_i の K 上の最小多項式 $f_i(x)$ を割り切って $f(x)$ の約多項式である $f_i(x)$ は重根をもたないから α_i は K_{i-1} 上分離的で、(1) の注意と (1)(b) により K_i/K_{i-1} は分離的である。ゆえに、(2) により L/K は分離拡大である。