

(B, ρ) - separable closures について

岡山大理 永原 賢 (Takasi Nagahara)

§0 序

B は単位元 1 をもつ (可換とは限らない) 環とし,
 ρ は B の一つの (環) 自己同型とする。

B のイデアル $\mathfrak{A}$ が 0 , B で, $\rho(\mathfrak{A}) \subset \mathfrak{A}$ となるものが存在しないとき, B は ρ -単純であるという。

論文 [2], [3] の §3 における結果は基礎環 B が
両側単純環である場合についてであった。この論文
は [2, §3] の結果を B が ρ -単純である場合へ拡張す
ることと, ガロア対応および (B, ρ) -分離閉包とよばれる
ものに関する考察である。その進め方は [3, §3] に
沿って行う。

以下この論文においては, B は ρ -単純であると仮定
し, B の拡大環はすべて B と単位元を共有するものと
する。

まず, 以下よく使われる分離拡大, ガロア拡大の

定義を述べておこう。

A は B の拡大環とする。 写像

$$A \otimes_B A \longrightarrow A; a_1 \otimes a_2 \longrightarrow a_1 a_2$$

が両側 A -加群の準同型として分解するとき, A は B の分離拡大であるという。

また, A の B -自己同型より成る一つの有限群 G で次の条件をみたすものが存在するとき, A は B の G -ガロア拡大であるという。

i) $A(G) (= \{a \in A \mid \sigma(a) = a \text{ for all } \sigma \in G\})$ が B と一致する,

ii) A は条件

$$\sum_i x_i \sigma(y_i) = \delta_{i, \sigma} \text{ for all } \sigma \in G$$

($\delta_{i, \sigma}$ はクロネッカーのデルタ) をみたすような元 $x_1, x_2, \dots, x_m, y_1, \dots, y_n$ を含む。

上述に関連して, A/B の中間環 T に対し, $G(T)$ で
もって $\{\sigma \in G \mid \sigma(t) = t \text{ for all } t \in T\}$ をあらわすことにする。

拡大 A/B に対し, A/B を含む B の G -ガロア拡大 N/B で, $N(G(A)) = A$ をみたすようなものが存在するとき拡大 A/B はガロア型であるという。

さて, p に関する B の歪多項式環

$$B[X; p] = \sum_i X^i B \quad ; \quad \alpha X = X p(\alpha) \quad (\alpha \in B)$$

を R であらわし, R の元 f で次の条件をみたすものの全体を $R_{(0)}$ であらわす:

- 1) f の最高次係数は 1,
- 2) $Rf = fR$.

このとき, 任意の $f \in R_{(0)}$ に対し

$$3) \quad Xf = fX$$

の成り立つことが示される。

3) は, B が p -単純であることに注意すれば,

[1, Lemma 1 とその証明] から分る。

以下, C をもって $B(p)$ の中心とあらわす。このとき, 任意の $f \in R_{(0)}$ に対し, その係数は C に含まれる, よって $R_{(0)} \subset C[X] \subset R$ が成り立つ。さて, $f \in R_{(0)}$ に対し, 剰余環 $C[X]/fC[X]$ は $\{1, X, \dots, X^{n-1}\}$ (但し, $X = X + fC[X]$, $n = \deg f$) を基とする自由 C -加群である。この加群から C への trace map を t_r であらわすとき, $\|t_r(x^i x^j)\|$ ($0 \leq i, j < n$) の行列式を f の判別式とよび $d(f)$ であらわす。 $f = X^2 + Xa + b$ のときは $d(f) = a^2 - 4b$ である。

さて, $f \in R_{(0)}$ に対し,
 剰余環 R/fR が B の分離拡大のとき, f は分離的
 であるという, また,
 剰余環 R/fR が B のガロア型拡大のとき, f はガロア
 型であるという, さらに
 $d(f)$ が B の単元のとき, f は λ -分離的であるという。

$p = 1$ (恒等写像) のときは $R_{(0)}$ の元に対し, ガロア
 型と分離的とは同値な概念であることが証明されてい
 る。しかし, $p \neq 1$ のときは, ガロア型でない分離多項
 式の存在する場合のあることが知られている (cf. §3)。

一般には ($p \neq 1$ であっても) ガロア型多項式は分離
 的であり, また, λ -分離(的)多項式はガロア型, 従って
 分離的である (cf. [2])。

§1 $R_{(0)}$ の λ -分離多項式の分解環

定義. $f \in R_{(0)}$ とし, $\deg f = n$ とする.

(I) B の拡大環 A が $(B$ 上) 次の条件を満たす元 $\alpha_1, \dots, \alpha_n$ で生成されるとき, それを f の $(B$ 上の) 分解環とよぶ:

$$a) \quad \alpha_i \alpha_j = \alpha_j \alpha_i \quad (1 \leq i, j \leq n)$$

$$b) \quad b \alpha_i = \alpha_i \rho(b) \quad (b \in B, 1 \leq i \leq n)$$

c) f は $C[\alpha_1, \dots, \alpha_n][X]$ の多項式として

$$f = (X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_n)$$

と分解される.

以下では, $U = \{\alpha_1, \dots, \alpha_n\}$ とおき, A を $B[U]$ なる如く略記することにする.

(II) f の分解環で, 単純環となるものを f の単純分解環とよぶ.

次の定理 1.1 および 1.2 は [2, Theorem 11] の拡張である.

定理 1.1. $f \in R_{(0)}$ は λ -分離的とする. このとき, f は単純分解環をもつ. また, f の任意の単純分解環 $B[U], B[V]$ に対し, $B[U]$ から $B[V]$ への B -環同型 ψ で $\psi(U) = V$ を満たすものが存在する.

定義. $f \in R_{(0)}$ は Λ -分離的とし, $S = B[U]$ は f の単純分解環とする。このとき, G_f でもって, $\sigma(U) = U$ とみたす S の B -自己同型全体のなす群とあらわす。

また, ρ は U の上では恒等写像であるような S の自己同型に拡張される, この ρ と同じ ρ とあらわす。

S の部分環 T で $\rho(T) = T$ かつ, ρ -単純であるものと S の ρ -単純部分環とよぶ。

定理 1.2. $f \in R_{(0)}$ は Λ -分離的とし, $S = B[U]$ は f の単純分解環とする。このとき,

- i) S は G_f -ガロア拡大である。
- ii) G_f の部分群全体の集合 $\mathcal{G}_f$ と S の B を含む ρ -単純部分環の全体の集合 $\mathcal{I}_f$ との間に 1 対 1 のガロア対応が存在する:

$$\begin{array}{ccc} \mathcal{G}_f & \longleftrightarrow & \mathcal{I}_f \\ \downarrow \psi & & \downarrow \psi \\ H = G_f(T) & \longleftrightarrow & T = S(H) \end{array}$$

注意. B が両側単純環 (ρ -単純環の特別な場合) であっても $\mathcal{I}_f$ は両側単純でない ρ -単純部分環を含むことがある (cf. §3).

§2. (B, P) - A -分離閉包

定義. B の拡大環 Ω が次の条件をみたすとき,
それを (B, P) - A -分離閉包とよぶ:

- i) Ω は (両側) 単純環である.
- ii) Ω は次のような Γ の部分集合 Γ を含む;
 - a) $\alpha\beta = \beta\alpha, b\alpha = \alpha p(b)$ for all $\alpha, \beta \in \Gamma$ and $b \in B$,
 - b) Ω は B 上 Γ で生成される,
 - c) 各 $\alpha \in \Gamma$ に対して, $f(\alpha) = 0$ となるような A -分離多項式 $f (\in R_{(0)})$ が存在する,
 - d) 任意の A -分離多項式 $g \in R_{(0)}$ に対して, Γ の有限部分集合 F で, $B[F]$ が g の分解環となるようなものが存在する.

以下では, 上記のような (B, P) - A -分離閉包を $B[\Gamma]$ なる如く略記しよう.

定理 2.1. (B, P) - A -分離閉包は存在する. また, 任意の (B, P) - A -分離閉包 $\Omega_1 = B[\Gamma_1], \Omega_2 = B[\Gamma_2]$ に対して, Ω_1 から Ω_2 への B -環同型 ψ で $\psi(\Gamma_1) = \Gamma_2$ をみたすものが存在する.

定義. $\Omega = B[\Gamma]$ は (B, ρ) - $\mathcal{A}$ -分離閉包とする. このとき, G によって, $\sigma(\Gamma) = \Gamma$ とみたす Ω の B -自己同型全体のなす群とあらわす. また, ρ は Γ の上では恒等写像であるような Ω の自己同型に拡張される, これと同じ ρ であらわす. §1 における定義と同じように, Ω の部分環 T で, $\rho(T) = T$ かつ, ρ -単純であるものと ρ -単純部分環とよぶ.

定理 2.2. Ω は (B, ρ) - $\mathcal{A}$ -分離閉包とする. このとき,

i) $\Omega(G) = B$ で, 拡大 Ω/B は G に関する局所^{有限次}ガロア拡大である, 即ち, Ω の任意の有限部分集合 F に対し, F を含む Ω/B の単純中間環 T で, $\rho(T) = T$, $\sigma(T) = T$ for all $\sigma \in G$, かつ B の有限 $G|T$ (G の T への制限) がガロア拡大となるものが存在する.

ii) G の (有限位相に関する) 部分群全体の集合 $\mathcal{G}$ と Ω の B を含む ρ -単純部分環全体の集合 $\mathcal{I}$ との間には 1 対 1 のガロア対応が存在する:

$$\begin{array}{ccc} \mathcal{G} & \longleftrightarrow & \mathcal{I} \\ \downarrow & & \downarrow \\ H = G(T) & \longleftrightarrow & T = \Omega(H) \end{array}$$

§3. 例.

$R_{(0)}$ の多項式が $R_{(0)}$ の 1 次以上の多項式の積としてあらわせないとき, それは $R_{(0)}$ において既約であるという, また, $R_{(0)}$ の既約多項式であるともいう。

$R_{(0)}$ の任意の A -分離多項式は $R_{(0)}$ の既約多項式の積として一意的にあらわされる, このとき, 各因子は A -分離的である。 $R_{(0)}$ において既約である A -分離多項式を, 簡単に, $(R_{(0)})$ の既約 A -分離多項式とよぶ。

(cf. [2, Theorem 19])

(I). $F = GF[4]$ とし, ρ は F の位数 2 の自己同型とする。このとき, $F[X; \rho]$ の元 $X^2 + 1$ は分離的であるが, A -分離的でない。また, X は A -分離的であるが 2 次以上の A -分離多項式は $(F[X; \rho])$ には存在しない。このとき, (F, ρ) - A -分離閉包は F と考える。

(II). $\mathbb{R}$ は実数体とし, $\mathbb{C}$ は複素数で $\mathbb{C} = \mathbb{R} + \mathbb{R}i$, $i^2 = -1$ とする。さらに ρ で $\mathbb{C}$ の $\mathbb{R}$ -自己同型 $(a + bi \rightarrow a - bi, a, b \in \mathbb{R})$ をあらわし, $R = \mathbb{C}[X; \rho]$ とおく。このとき,

i). $R_{(0)}$ の既約 A -分離多項式の次数は 1, 2, 4 のみである。次数が 1 のときは, X (自明な場合),

次数が 2 のときは $X^2 + a$; $a \neq 0 \in \mathbb{R}$,

次数が 4 のときは $X^2 + aX + b$; $a, b \in \mathbb{R}$, $a^2 - 4b < 0$
なる形をしている。

ii). Δ は $\mathbb{R}$ 上の四元数体とし, $\Delta = \mathbb{C} + \mathbb{C}j$
($j^2 = -1$, $aj = jp(a)$ for $a \in \mathbb{C}$) とする。このとき,
 $X^2 + 1$ の単純分解環は Δ と同型である。また, $X^2 - 1$ の
 Δ 上の単純分解環は $\Delta \otimes_{\mathbb{R}} \mathbb{C}$ と同型である。従って,
これは $(X^2 + 1)(X^2 - 1) = X^4 - 1$ の $\mathbb{C}$ 上の単純分解環である。

さらに, これが $(\mathbb{C}, p)$ - $\mathcal{A}$ -分離閉包 Ω と同型になるこ
とが示される。

一方, $X^2 - 1$ の単純分解環は $(\mathbb{R})_2$ ($\mathbb{R}$ 上の 2 次の完全
行列環) と同型であり, この上の $X^2 + 1$ の単純分解環
は $(\mathbb{R})_2 \otimes_{\mathbb{R}} \mathbb{C}$ と同型である。従って,

$$\Omega \cong \Delta \otimes_{\mathbb{R}} \mathbb{C} \cong (\mathbb{R})_2 \otimes_{\mathbb{R}} \mathbb{C} \cong (\mathbb{C})_2$$

が成り立つ。

また, 既約 $\mathcal{A}$ -分離多項式 $X^4 + 1$ の単純分解環を
 $\mathbb{C}[E]$ とすると, $\Omega \cong \mathbb{C}[E]$ であって, 任意の $\alpha \in E$ に対し
て $\Omega \cong \mathbb{C}[\alpha] \cong \mathbb{R}/(X^4 + 1)\mathbb{R}$ (剰余環) である。

iii). さうして, 拡大 $\Omega/\mathbb{C}$ のガロア群 $G, \mathcal{G}, \mathcal{I}$
を調べる。ここで, $\Omega = \Delta \otimes_{\mathbb{R}} \mathbb{R}$ と考えてよう。

さて,

σ_1 は Ω の $\mathbb{C} \otimes \mathbb{C}$ -自己同型 ; $j \otimes 1 \rightarrow -j \otimes 1$

σ_2 は Ω の $\Delta \otimes 1$ -自己同型 ; $1 \otimes i \rightarrow -1 \otimes i$

とする。明らかに $\sigma_1^2 = 1$, $\sigma_2^2 = 1$ である。

このとき, $X^2 + 1$ の単純分解環は $\Delta = \mathbb{C}[j \otimes 1, -j \otimes 1]$ であり,

Δ 上の $X^2 - 1$ の単純分解環は $\Omega = \Delta[j \otimes i, -j \otimes i]$ である。

従って, $f = X^4 - 1$ の単純分解環は

$$\Omega = \mathbb{C}[j \otimes 1, -j \otimes 1, j \otimes i, -j \otimes i]$$

となる。これより, $\Omega/\mathbb{C}$ のガロア群 $G (= G_f)$ は直積

$(\sigma_1) \times (\sigma_2)$ とあらわされる。このとき,

$$\Omega(\sigma_1) = \mathbb{C} \otimes \mathbb{C}, \quad \Omega(\sigma_2) = \Delta \otimes 1 \cong \Delta, \quad \Omega(\sigma_1 \sigma_2) = \mathbb{C}[j \otimes i, -j \otimes i]$$

となり, $\Omega(\sigma_1 \sigma_2)$ は $X^2 - 1$ の分解環である。従って,

$$\mathcal{G} = \{1, (\sigma_1), (\sigma_2), (\sigma_1 \sigma_2), G\}$$

$$\mathcal{I} = \{\Omega, \mathbb{C} \otimes \mathbb{C}, \Delta \otimes 1 \cong \Delta, \Omega(\sigma_1 \sigma_2) \cong (\mathbb{R})_2, \mathbb{C} \otimes 1 \cong \mathbb{C}\}$$

である。ここで, $\mathbb{C} \otimes \mathbb{C}$ は単純環ではないが p -単純である。

References

- [1] T. Nagahara: A note on separable polynomials in skew polynomial rings of automorphism type, Math. J. Okayama Univ. 22 (1980), 73-76.
- [2] T. Nagahara: On splitting rings of separable skew polynomials, Math. J. Okayama Univ. 26 (1984), 71-85.
- [3] 永原 賢: 分離多項式の分解環について,
第30回代数学シンポジウム報告集, 1984, 285-297
- [4] T. Nagahara: A note on imbeddings of non-commutative separable extensions in Galois extensions, Houston Journal of Math. 12 (1986), 411-417.