数理解析研究所講究録
第628巻1987年166-177

(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$\mathfrak{a} \neq 0$, Bで，$\rho(\mathfrak{a}) \subset \mathfrak{a}$となるものが存在しないとき，Bは$\rho$-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

$$\sum_i x_i\sigma(y_i)=\delta_{1,\sigma} \quad \text{for all } \sigma\in G$$

（$\delta_{1,\sigma}$ はクロネッカーのデルタ）をみたすような元 x_1, $x_2,\cdots,x_n$, $y_1,\cdots,y_n$ 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，ρ に関する B の歪多項式環

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

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) $Xf = fX$

の成り立つことが示される。

3) は，B が ρ-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 でもって $B(\rho)$ の中心をあらわす．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 $\{1, x, \cdots, x^{n-1}\}$ (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 $\delta(f)$ であらわす。$f = X^2 + Xa + b$ のときは $\delta(f) = a^2 - 4b$ 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

$\delta(f)$ が B の単元のとき，f は Δ-分離的であるという。

$\rho = 1$（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，$\rho \neq 1$ 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（$\rho \neq 1$ であっても）ガロア型多項式は分離的であり，また，Δ-分離(的)多項式はガロア型，従って分離的である（cf. [2])。

§1 $R_{(\sigma)}$ の Δ-分離多項式の分解環

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

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

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

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

c) f は $C[\alpha_1, \cdots, \alpha_n][X]$ 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, $U = \{\alpha_1, \cdots, \alpha_n\}$ 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, 両側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. $f \in R_{(\sigma)}$ は Δ-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 $\psi(U) = V$ をみたすものが存在する。

定義. $f \in R_{(0)}$ は Δ-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，$\sigma(U) = U$ をみたす S の B-自己同型全体のなす群をあらわす。

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，これを同じ ρ であらわす。

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

定理 1.2. $f \in R_{(0)}$ は Δ-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 $\mathfrak{g}_f$ と S の B を含む ρ-単純部分環の全体の集合 $\mathfrak{T}_f$ との間に 1 対 1 のガロア対応が存在する：

$$\begin{array}{ccc} \mathfrak{g}_f & \longleftrightarrow & \mathfrak{T}_f \\ \Psi & & \Psi \\ H = G_f(T) & \longleftrightarrow & T = S(H) \end{array}$$

注意. B が両側単純環（ρ-単純環の特別な場合）であっても $\mathfrak{T}_f$ 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,ρ)-Δ-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,ρ)-Δ-分離閉包とよぶ：

i) Ω は（両側）単純環である。

ii) Ω は次のような一つの部分集合 Γ を含む；

a) $\alpha\beta=\beta\alpha$, $b\alpha=\alpha\rho(b)$ 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 Δ-分離多項式 $f\ (\in R_{(0)})$ が存在する，

d) 任意の Δ-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,ρ)-Δ-分離閉包を $B[\Gamma]$ なる如く略記しよう。

定理 2.1. (B,ρ)-Δ-分離閉包は存在する。 また，任意の (B,ρ)-Δ-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)-Δ-分離閉包とする。このとき，Gでもって，$\sigma(\Gamma)=\Gamma$をみたすΩのB-自己同型全体のなす群をあらわす。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，これを同じ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-単純であるものをρ-単純部分環とよぶ。

定理2.2. Ωは(B,ρ)-Δ-分離閉包とする。このとき，

i) $\Omega(G)=B$で，拡大Ω/BはGに関する局所が有限次ロア拡大である，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）閉部分群全体の集合$\mathcal{G}$とΩのBを含むρ-単純部分環全体の集合$\mathcal{T}$との間に1対1のガロア対応が存在する：

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

§3. 例.

$R_{(\sigma)}$ の多項式が $R_{(\sigma)}$ 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 $R_{(\sigma)}$ において既約であるという，また，$R_{(\sigma)}$ の既約多項式であるともいう。

$R_{(\sigma)}$ の任意の Δ-分離多項式は $R_{(\sigma)}$ 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 Δ-分離的である。 $R_{(\sigma)}$ において既約である Δ-分離多項式を，簡単に，（$R_{(\sigma)}$の）既約 Δ-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，Δ-分離的でない。 また，X は Δ-分離的であるが2次以上の Δ-分離多項式は（$F[X;\rho]$には）存在しない。このとき，(F,ρ)-Δ-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 でもって，$\mathbb{C}$ の $\mathbb{R}$-自己同型（$a+bi \to a-bi$, $a,b \in \mathbb{R}$）をあらわし，$R = \mathbb{C}[X;\rho]$ とおく。このとき，

i). $R_{(\sigma)}$ の既約 Δ-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，$\Delta = \mathbb{C} + \mathbb{C}j$（$j^2=-1$, $aj = j\rho(a)$ 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 $(\mathbb{C}, \rho)$-Δ-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。よって，

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

が成り立つ。

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

iii). さいごに，拡大 Ω/C のガロア群 G, $\mathfrak{g}$, $\mathfrak{I}$ を調べる。ここで，$\Omega = \Delta \otimes_{\mathbb{R}} \mathbb{R}$ として考えよう。

さて，

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

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

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,

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

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

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

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

である。ここで, $\mathbb{C}\otimes\mathbb{C}$ は単純環ではないが ρ-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: 分離歪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.