

Metacyclic 群とガロア群にもつ

ガロア拡大について

信大 理学部 岸本量夫

B を標数 $p \neq 0$ の素体 $\text{GF}(p)$ 上の多元環, G を位数 p^e の基本アーベル群とするとき, B が G -ガロア拡大を有するための必要十分条件, また B が正則元として, ある正整数 n , 1 の原始 n 乗根 ζ , $\{1-\zeta^i; i=0, 1, \dots, n-1\}$ を含むとき, 位数 n のアーベル群 G に対して, B が G -強ガロア拡大を有するための必要十分条件は [1], [2], [3], [4] 等で知られている. ここで, $G \supseteq (n)$, $G/(n)$ がアーベル群となる有限非アーベル群 G とガロア群にもつ環のガロア拡大の構成について考えたい.

このような群の例として, 位数 $2m$ の正四面体群, 位数 p^3 の p 群等がある.

§ 準備

以下, 用いられる記号, 用語, (すでに知られている) 定理の説明をするが, 環はすべて可換環, 環の分離拡大, ガロ

$\mathcal{P}$ 拡大の概念は既知のこととする。

(i) B は単位元を持つ環とする。正整数 n に対して, B が 1 の原始 n 乗根を含むとき, $\Gamma(n) = \{n, \zeta, 1-\zeta^i; i=0, 1, 2, \dots, n\}$ とする。

(ii) 環が連結であるとは, 0, 1 以外に中等元をもたないことと定義する。

(iii) G が σ から生成される位数 n の巡回群 ($G = \langle \sigma \rangle$ と記す) のとき, G -ガロア $\mathcal{P}$ 拡大を (σ) -巡回拡大とよぶ。 $U(B) \supseteq \Gamma(n)$ で A を B 上の (σ) -巡回拡大とする。 A の正則元 x で $\sigma(x) = x\zeta$ となる元が存在するとき, A を B 上の (σ) -強巡回拡大とよぶ。

A が B の (σ) -強巡回拡大なるための必要十分条件は, A の正則元 x で $x^n \in U(B)$ となる元が存在することである。このとき $\{x^i; i=0, 1, 2, \dots, n-1\}$ は B 上一次的独立な基底で, $A = B \oplus xB \oplus \dots \oplus x^{n-1}B$ となる。また A が B 上の (σ) -強巡回拡大であることは A/B が (σ) -正則基底をもつガロア $\mathcal{P}$ 拡大であることとは同値である。

(iv) B を $\text{GF}(p)$ 上の多項式環, $G = \langle \sigma \rangle$ と位数 p の巡回群とする。 A が B 上の (σ) -巡回拡大であるための必要十分条件は A の元 x で $x^p - x \in B$ となる元が存在することである。このとき $\{x^i; i=0, 1, 2, \dots, p-1\}$ は B 上の一次的独立な基底で, $A = B \oplus xB \oplus \dots \oplus x^{p-1}B$ である。さらに, A には $T_\sigma(v) = \sum_{i=0}^{p-1} \sigma^i(v)$

$= 1$, $\sigma(u) - u = v^p - v$ となる元 $\{u, v\}$ が存在し, $A' = A[X]/(X^p - X - u)A[X]$ は $f: \sum X^i a_i + (X^p - X - u)A[X] \rightarrow \sum (X+v)^i \sigma(a_i) + (X^p - X - u)A[X]$ で $B \pm (f)$ -巡回拡大となり, f の位数は p^2 , $f|A = \sigma$ である. この $\{u, v\}$ は A/B の (σ, p) -生成系という.

§ $G = D_m$ の場合

$G = D_m = (\sigma, \tau)$, $\sigma^m = \tau^2 = 1$, $\sigma \tau = \tau \sigma^{-1}$ とする.

定理 1 $U(B) \supseteq \Gamma(2m)$ とする.

B が A/A^σ , A^σ/B がそれぞれ (σ) -強巡回拡大, (τ) -巡回拡大であるような D_m -ガロア拡大 A を有するための必要十分条件は

(1) $d^2 - be^2 = c^m$ となる $b, c \in U(B)$, $d, e \in B$ が存在することである.

この場合 $A = \bigoplus_{i=0}^{m-1} x^i y^j B \cong B[X, Y]/(X^m - (d + Ye), Y^2 - b)B[X, Y]$ ($f(X, Y) + (X^m - (d + Ye), Y^2 - b)B[X, Y] \rightarrow f(x, y)$) とし得るから, $f(x, y) = \sum_{i=0}^{m-1} x^i y^j b_{ij}$ ($b_{ij} \in B$) は A の任意の元と見て $\sigma(f(x, y)) = f(x^2, y)$, $\tau(f(x, y)) = f(x^{-1}c, -y)$ である.

証明 A を上記の条件を満足する D_m -ガロア拡大, $T = A^{D_m}$ とする. A/T は (σ) -強巡回拡大, T/B は (τ) -強巡回拡大である.

るから $A = T \oplus xT \oplus \cdots \oplus x^{m-1}T$, $x \in U(A)$, $\sigma(x) = xj^2$, $T = B \oplus yB$, $y \in U(T)$, $\tau(y) = -y$ とある. $\sigma(x\tau(x)) = xj^2\sigma\tau(x) = xj^2\tau\sigma^{-1}(x) = xj^2\tau(x)j^{-2} = x\tau(x)$, $x\tau(x) = x\tau(x)$ より $x\tau(x) \in A^{D_m} = B$ と得る. 同様に, $\tau(x) = x^{-1}c$, $c \in U(B)$ とある. $x^m \in T = B \oplus yB$ とあるから, $x^m = d + ye$ ($d, e \in B$) とあるが $(d+ye)^{-1}c^m = x^{-m}c^m = \tau(x^m) = \tau(d+ye) = d - ye$ とある. 今 $y^2 = b$ ($b \in U(B)$) とすれば, $c^m = (d+ye)(d-ye) = d^2 - be^2$ とある.

$B[X, Y] \ni f(X, Y) = \sum x^i Y^j b_{ij}$ に対し $f(x, y) = \sum x^i y^j b_{ij} \in A$ と対応させると, この対応は環全型であり, その核は $(x^m - (d+ye), Y^2 - b)B[X, Y]$ である. 核の任意の元 $g(X, Y)$ に対し, それを $(x^m - (d+ye))$ で割り, その剰余を $Y^2 - b$ で割ると 1 によ, て, $g(X, Y) = h(X, Y)(x^m - (d+ye)) + k(X, Y)(Y^2 - b) + \sum_{i=0}^{m-1} \sum_{j=0}^1 x^i Y^j b_{ij}$ とできる. $0 = g(x, y) = \sum_{i=0}^{m-1} \sum_{j=0}^1 x^i y^j b_{ij}$ とあるから $b_{ij} = 0$ となり, 核が $(x^m - (d+ye), Y^2 - b)B[X, Y]$ に一致することが知られる.

次に十分性を証明しよう. $f(Y) \rightarrow f(-Y)$ で定義される $B[Y]$ の対応は B の自己同型 τ^* を引き起し $(\tau^*(b_0 + yb_1) = b_0 - yb_1)$, T/B は (τ^*) -強巡回拡大である. $(d+ye)(d-ye) = d^2 - be^2 = c^m \in U(B)$ とあるから T の正則元, したがって $A = T[X]/(x^m - (d+ye)T[X])$ は T 上の分離拡大となる. X の剰余類 x に対して, $\sigma(\sum_{i=0}^{m-1} x^i t_i) = \sum_{i=0}^{m-1} (xj^2)^i t_i$ ($t_i \in T$) と σ を定義すれば

$\sigma(x^m) = (xj^2)^m = x^m = d + ye = \sigma(d + ye)$, $\sigma^m(x) = xj^{2m} = x$ か
 ら σ は位数 m の A の T -自己同型となり, A/T は (σ) -強巡回
 拡大である. $\therefore \tau(\sum_{i=0}^{m-1} x^i t_i) = \sum_{i=0}^{m-1} (x^{-1}c)^i \tau^*(t_i)$ と書
 けば, $\tau(x^m) = x^{-m}c^m = (d+ye)^{-1}c^m = (d+ye)^{-1}(d^2 - be^2) = (d+ye)^{-1}$
 $\cdot (d+ye)(d-ye) = (d-ye) = \tau(d+ye)$, $\tau^2(x) = \tau(x^{-1}c)$
 $= x$, $\tau^2(y) = y$ より, τ は位数 2 の A の自己同型となる. A
 の任意の元 $f(x, y)$ に対して, $\sigma\tau(f(x, y)) = \sigma(f(x^{-1}c, -y)) =$
 $f(x^{-1}j^2c, -y)$, $\tau\sigma^{-1}(f(x, y)) = \tau(f(xj^{-2}, y)) = f(x^{-1}cj^{-2}, -y)$
 であるから $(\sigma, \tau) = D_m$, $A^{D_m} = (A^\sigma)^\tau = T^\tau = B$, A/T , T/B
 がそれぞれ分離拡大であるから, A/B は分離拡大である.

§ $|G| = 8$ の場合

位数 $8 = 2^3$ の非 p -バル群は正四面体群 D_4 と, $Q = (\sigma, \tau)$
 , $\sigma^4 = 1$, $\sigma^2 = \tau^2$, $\sigma\tau = \tau\sigma^{-1}$ で定義される四元数群であ
 る. この場合は次の定理が得られる.

定理 2 $U(B) \geq \Gamma(4)$ とする.

(i) B が A/A^σ , A^σ/B がそれぞれ (σ) -強巡回拡大, (τ) -強
 巡回拡大である D_4 -ガロア拡大 A を有するための必要十分条
 件は

(1) $d^2 - be^2 = c^4$ となる $b, c \in U(B)$, $d, e \in B$ が存在する =

とである。

さらに, B を連結とすると, A が連結であるための必要十分条件は

(2) 連立方程式

$$\begin{cases} d - x^2 - y^2 b = 0 \\ e - 2xy = 0 \end{cases} \quad \text{が } B \text{ で解を有さない。}$$

(3) $b \notin U(B)^2 = \{u^2 \mid u \in U(B)\}$ である。

(ii) B が A/A^σ , A^σ/B がそれぞれ (σ) -強巡回拡大, (τ) -強巡回拡大である $\mathbb{Q}$ -ガロア拡大 A を有するための必要十分条件は

(1) $d^2 - be^2 = b^2 c^4$ となる $b, c \in U(B)$, $d, e \in B$ が存在することである。

この場合, $A = \bigoplus_{i=0}^3 \bigoplus_{j=0}^1 x^i y^j B \cong B[X, Y] / (X^4 - (d + Ye), Y^2 - b) B[X, Y] \ (f(X, Y) + (X^4 - (d + Ye), Y^2 - b) B[X, Y] \rightarrow f(x, y))$ として得られ, $f(x, y)$ を A の任意の元とすれば, $\sigma(f(x, y)) = f(x^3, y)$, $\tau(f(x, y)) = f(x^{-1}y^3, y)$ である。さらに B が連結であるとき, A が連結である必要十分条件は (i) の (2), (3) を満たすことである。

証明 (i) 前半は定理 1 の証明で示した。 $T = B[Y] / (Y^2 - b)$

$B[Y]$ が連結であるための必要十分条件は, $Y^2 - b$ が既約, したがって $b \notin U(B)^2$ である [4]. 次に $A = T[x] \cong T[x]/(x^4 - (d + ye)T[x])$ ($f(x) + (x^4 - (d + ye)T[x]) \rightarrow f(x)$) が連結であることと $A^{\sigma^2} = T[x^2] \cong T[z]/(z^2 - (d + ye)T[z])$ ($f(z) + (z^2 - (d + ye)T[z]) \rightarrow f(z)$) が連結であることと同値である [4]. したがって A の連結性は T の任意の元 $b_0 + yb_1$ ($b_0, b_1 \in B$) に対し $(b_0 + yb_1)^2 \neq d + ye$ と同値である. この条件は (2) と同値である.

(ii) A/B を $\mathbb{Q}$ -ガロワ拡大, $A^{\sigma} = T$ とすれば, $A = T \oplus xT \oplus \cdots \oplus x^3T$, $x \in U(A)$, $\sigma(x) = x^3$, $T = B \oplus yB$, $y \in U(T)$, $\tau(y) = -y$ である. $x^4 = d + ye$, $y^2 = b$ とする. $\sigma(x\tau(x)) = x$, $\tau\sigma(x) = x\tau(x)^{-1} = x\tau(x)$ より $\tau(x) = x^{-1}t$, $t \in U(T)$ である. 一方, $-x = \sigma^2(x) = \tau^2(x) = x t^{-1} \tau(t)$ より $\tau(t) = -t$ となるから, $t = yc$, $c \in U(B)$ となければならぬ. すなわち, $\tau(x) = x^{-1}yc$ である. $x^{-1}b^2c^4 = x^{-1}(yc)^4 = \tau(x^4) = \tau(d + ye) = d - ye$ より, $b^2c^4 = x^4(d - ye) = (d + ye)(d - ye) = d^2 - be^2$ となる.

十分性は定理 1 のそれと同様の方法で証明できる.

補題 1 B を $\text{GF}(p)$ 上の連結多元環とする. $T = B[X, Y]/(X^p - X - a, Y^p - Y - b)B[X, Y]$ ($a, b \in B$) が連結であるための

必要十分条件は, 任意の $(\alpha, \beta) (\neq (0, 0)) \in \text{GF}(p) \times \text{GF}(p)$ に対して, $c^p - c = a\alpha + b\beta$ となる $c \in B$ が存在しないことである.

証明 連結な $T = B[x, y]$ (x, y は X, Y の剰余類) において, $\sigma(f(x, y)) = f(x+1, y)$, $\tau(f(x, y)) = f(x, y+1)$ がそれぞれ T の B -自己同型であることを使って $\{(x\alpha + y\beta)^i; i=0, 1, \dots, p-1\}$ が B 上一次独立であることを知られる. $T \cong B[x\alpha + y\beta] \cong B[z]/(z^p - z - (a\alpha + b\beta))B[z]$ で, $B[x\alpha + y\beta]$ は連結であるから, $z^p - z - (a\alpha + b\beta)$ は既約, 1 にかゝってすべての $c \in B$ に対して $c^p - c \neq a\alpha + b\beta$ である.

逆にすべての $c \in B$ に対して $c^p - c \neq a\alpha + b\beta$ としよう. $\beta = 0$ とすれば, $c^p - c \neq a$ が得られるから $B[x] \cong B[x]/(x^p - x - a)$ $B[x]$ は連結である. 次に $T \cong B[x][Y]/(Y^p - Y - b)B[x][Y]$ であるから $Y^p - Y - b$ が $B[x]$ で既約を示せばよい. 仮に $f(x) = \sum_{i=0}^{p-1} x^i c_i$ ($c_i \in B$) が $f(x)^p - f(x) = b$ を満たすとしてみよう. $f(x)^p - f(x) = (\sum_{i=0}^{p-1} x^i c_i)^p - \sum_{i=0}^{p-1} x^i c_i = \sum_{i=0}^{p-1} (x+a)^i c_i^p - \sum_{i=0}^{p-1} x^i c_i = b$ であるから $c_{p-1}^p - c_{p-1} = 0$. ここで, B が連結であることを注意すれば, $c_{p-1} \in \text{GF}(p)$ である. 次に $(\binom{p-1}{p-2} c_{p-1}^p + a + c_{p-2}^p - c_{p-2} = 0$ から, $u = (\binom{p-1}{p-2} c_{p-1}^p = (p-1)c_{p-1} \neq 0$ ならば, $a = (c_{p-2}(-u^{-1}))^p - c_{p-2}(-u^{-1})$ となって, $x^p - x - a$ の既約性に反する. 同様の議論を繰返せば, $c_{p-1} = c_{p-2} = \dots = c_2 = 0$ で $f(x) = x c_1 +$

C_0 と得る。これから $(xC_1 + C_0)^p - (xC_1 + C_0) = x(C_1^p - C_1) + C_1^p a + (C_0^p - C_0) = b$ となるが、 $C_1 \in \text{GF}(p)$ であるから $C_0^p - C_0 = a(-C_1) + b$ となり条件に反する。

定理 3 B を $\text{GF}(2)$ 上の多元環とする。

$$(i) \quad A = \bigoplus_{i=0}^1 \bigoplus_{j=0}^1 \bigoplus_{k=0}^1 x^i y^j z^k B = B[X, Y, Z] / (X^2 - X - a, Y^2 - Y - b, Z^2 - Z - c)$$

$B[X, Y, Z]$ は $\sigma(f(x, y, z)) = f(x+1, y, z+x)$, $\tau(f(x, y, z)) = f(x, y+1, z)$ で B 上の D_4 -ガロア拡大となる。

$$(ii) \quad A = \bigoplus_{i=0}^1 \bigoplus_{j=0}^1 \bigoplus_{k=0}^1 x^i y^j z^k B = B[X, Y, Z] / (X^2 - X - a, Y^2 - Y - b, Z^2 - Z - X(a+b) - Yb)$$

$B[X, Y, Z]$ は $\sigma(f(x, y, z)) = f(x+1, y, z+y+x)$, $\tau(f(x, y, z)) = f(x, y+1, z+y)$ で B 上の Q -ガロア拡大となる。

(iii) B は常に D_4 -ガロア拡大, Q -ガロア拡大を有する。

(iv) B が連結のとき, 連結な D_4 -ガロア拡大 A が存在するための必要十分条件は, 任意の $(\alpha, \beta) (\neq (0, 0)) \in \text{GF}(2) \times \text{GF}(2)$ と任意の $c \in B$ に対して, $c^2 - c \neq \alpha a + \beta b$ となる $a, b \in B$ が存在することである。

(v) B が連結のとき, 連結な D_4 -ガロア拡大が存在すれば, 連結な Q -ガロア拡大が存在する。またこの逆も成立する。

証明 (i) $T \cong B[X, Y] / (X^2 - X - a, Y^2 - Y - b) B[X, Y]$ は $\sigma(f(x,$

$y) = f(x+1, y)$, $\tau'(f(x, y)) = f(x, y+1)$ により $H = (\sigma') \times (\tau')$ が Γ の拡大となる. $A = T[z] \cong T[Z]/(Z^2 - Z - x_0)T[Z]$ で A/Γ は分離拡大となり, $\sigma(x_0 + zt_1) = \sigma'(x_0) + (z+1)\sigma'(t_1)$ と定義すれば, $\sigma(z^2 - z) = (z+1)^2 - (z+1) = (z^2 - z) + (1^2 - 1) = x_0 + a = (x+1)a = \sigma'(xa)$, $\sigma^4(zt) = \sigma^2(z+1)\sigma^4(t) = zt$ であるから σ は位数 4 の A の自己同型と考えてよい. 次に $\tau(x_0 + zt_1) = \tau'(x_0) + z\tau'(t_1)$ と定義すれば $\tau(z^2 - z) = z^2 - z = x_0 = \tau'(xa)$ より τ は位数 2 の A の自己同型と考えてよい. $\sigma\tau(f(x, y, z)) = \sigma(f(x, y+1, z)) = f(x+1, y+1, z+1)$, $\tau\sigma^{-1}(f(x, y, z)) = \tau(f(x+1, y, z+1)) = f(x+1, y+1, z+1)$ より $\sigma\tau = \tau\sigma^{-1}$ を得て, $(\sigma, \tau) = D_4$ と得る. $A^{D_4} = B$, A/Γ , T/B が分離拡大であるから A は D_4 -ガロア拡大である.

(ii) (i) と同様の方法で証明できる.

(iii) (i), (ii) から明らかである.

(iv) A を連結な D_4 -ガロア拡大, $T = A^{\sigma^2}$ とすれば, $D_4 | T = H = (\sigma') \times (\tau')$ は位数 4 の基本アーベル群で, T の自己同型群となるから, $T = B[X, Y] \cong B[X, Y]/(X^2 - X - a, Y^2 - Y - b)B[X, Y]$ ($f(X, Y) + (X^2 - X - a, Y^2 - Y - b)B[X, Y] \rightarrow f(X, Y)$), $a, b \in B$ となる. T が連結であることに注意すれば, 補題 1 より主張が得られる. 次に T の分離性を証明しよう. 補題 1 から $T \cong B[X, Y]/(X^2 - X - a, Y^2 - Y - b)B[X, Y]$ は連結である. $A = T[Z]/(Z^2 - Z - x_0)$.

$T[Z]$ は (i) より D_4 -ガロア拡大であるから, A が連結である
ことを示せば十分である. e を A の中等元とする. $\sigma^2(e) + e$
は T の中等元であるから $\sigma^2(e) + e = 1$ とする. ($\sigma^2(e) + e = 0$
ならば $\sigma^2(e) = e \in A^{\sigma^2} = T$ から, $e = 0$ または 1 を得る). ま
さに, $\sigma^2(\sigma(e) + e) = \sigma^3(e) + \sigma^2(e) = \sigma(\sigma^2(e)) + e + 1 = \sigma(e)$
 $+ 1 + e + 1 = \sigma(e) + e$ から, 再び $\sigma(e) + e \in T$ であり, これ
を 1 と仮定してよい. $\sigma^2(e) + e = \sigma(e) + e$ より $\sigma^2(e) = \sigma(e)$
となり $\sigma(e) \in A^{\sigma} \subseteq A^{\sigma^2} \subseteq T$ となり, 結局 $e = 1$ または 0 を得
る.

(v) A を連結な D_4 -ガロア拡大とすれば, (ii) の条件を満た
す a, b が存在する. したがって, $T = B[X, Y]/(X^2 - X - a, Y^2 - Y - b)$
 $B[X, Y]$ が連結であるが $A = T[Z]/(Z^2 - Z - X(a+b) - Yb)$ $T[Z]$ が
連結であることは, (iv) と同様の方法で示される. (iii) から A は
 $\mathbb{Q}$ -ガロア拡大である. 逆も同様の方法で得られる.

§ $|G| = p^3$, p : 奇素数の場合

この節では, B は $\text{GF}(p)$ 上の多項式環, G は位数 p^3 (p は奇
素数) の群, $H = \langle \sigma \rangle \times \langle \tau \rangle$ は位数 p^2 の基本アーベル群とする. こ
のとき G は $G_1 = \langle \sigma, \tau \rangle$, $\sigma^p = \tau^p = 1$, $\sigma\tau = \tau\sigma^{p+1}$ か, $G_2 = \langle \sigma$
 $\tau, \rho \rangle$, $\sigma^p = \tau^p = \rho^p$, $\sigma\tau = \tau\sigma\rho$, $\sigma\rho = \rho\sigma$, $\tau\rho = \rho\tau$ である.

定理 4 (i) B が G_1 -ガロア拡大 A を有するための必要十分条件は, B が次の条件を満たす元 t を含む H -ガロア拡大 T を有することである.

T/B の適当な (σ', τ) -生成系 $\{u, v\}$ に対して

$$(1) \quad \tau'(u) - u = t^p - t$$

$$(2) \quad \sigma'(t) - t = \tau'(v) - v + 1$$

$$(3) \quad T_{\tau'}(t) = 0$$

特に B が連結の場合, A が連結である必要十分条件は, T が連結であることである.

(ii) B が G_2 -ガロア拡大 A を有するための必要十分条件は, B が次の条件を満たす元 u, v, w を含む H -ガロア拡大 T を有することである.

$$(1) \quad T_{\sigma'}(v) = T_{\tau'}(w) = 0$$

$$(2) \quad \sigma'(u) = u + v^p - v, \quad \tau'(u) = u + w^p - w$$

$$(3) \quad v + \sigma'(w) = w + \tau'(v) + 1$$

特に T が連結の場合, A が連結であるようにとれる.

証明 (i) A を G_1 -ガロア拡大, $T = A^{\sigma^p}$ とする. $G_1(T) = \{\eta(t) \mid t \in T, \eta \in G_1\} \subseteq T$ であることは容易に知られるから $G_1|T \cong H$ で, T の自己同型群である. $\sigma|T = \sigma', \tau|T = \tau'$ とすれば, $T = B[x, y] \cong B[X, Y] / (X^p - X - a, Y^p - Y - b) B[X, Y]$,

$\sigma'(f(x, y)) = f(x+1, y), \tau'(f(x, y)) = f(x, y+1)$ である。 T は $T^{\sigma'} = B[y] \oplus (\sigma')$ -巡回拡大であるから, (σ', p) -生成系 $\{u, v\}$ を取り, A には $A = T \otimes_{\mathbb{Z}} T \otimes \cdots \otimes_{\mathbb{Z}} T$, $z^p - z = u$ となる z が存在し, $\sigma(zt) = (z+v)\sigma'(t)$ は位数 p^2 の自己同型となる。 $\sigma^p(-z + \tau(z)) = -(z+1) + \sigma^p \tau(z) = -(z+1) + \tau \sigma^p(z) = -(z+1) + \tau(z+1) = -z + \tau(z)$ から $\tau(z) = z + t, t \in A^{\sigma^p} = T$ である。
 $z = \tau^p(z) = z + T\tau'(t)$ から $T\tau'(t) = 0$ を得る。 $\tau'(u) - u = \tau(z^p - z) - (z^p - z) = z^p + t^p - z - t - z^p + z = t^p - t, z + v + \sigma'(t) = \sigma(z+t) = \sigma \tau(z) = \tau \sigma^{p+1}(z) = \tau(z+v+1) = z+t + \tau'(v) + 1$ である。

次に, T を条件 (i) - (3) を満たす H -ガロワ拡大と見る。 $A = T[z] = T[\mathbb{Z}] / (z^p - z - u) T[\mathbb{Z}]$ とする。 $\sigma(\sum_{i=0}^{p-1} z^i t_i) = \sum_{i=0}^{p-1} (z+v)^i \sigma'(t_i)$ で σ を定義すれば, σ は位数 p^2 の A の自己同型となり $\sigma|_T = \sigma'$ である。 次に $\tau(\sum_{i=0}^{p-1} z^i t_i) = \sum_{i=0}^{p-1} (z+t)^i \tau'(t_i)$ で τ を定義すれば, $\tau(z^p - z) = z^p + t^p - (z+t) = u + t^p - t = \tau'(u)$ で, $\tau^p(z) = z + T\tau'(t) = z$ から τ は位数 p の A の自己同型である。 $\sigma \tau(zt') = \sigma((z+t)\tau'(t')) = (z+v+\sigma'(t))\sigma'\tau'(t') = (z+v+t+\tau'(v)-v+1)\sigma'\tau'(t') = (z+t+\tau'(v)+1)\sigma'\tau'(t'), \tau \sigma^{p+1}(zt') = \tau[(z+v+1)\sigma'(t')] = (z+t+\tau'(v)+1)\sigma'\tau'(t') \neq \sigma \tau = \tau \sigma^{p+1}$, すなわち, $(\sigma, \tau) \cong G_1$ を得る。 $A^{G_1} = T^H = B$ であり, $A/A^{\sigma^p}, A^{\sigma^p}/B$ はそれぞれ分離拡大であるから A/B は分離拡大である。

3. A/T が (σ) -巡回拡大であるから, [3]より T が連続なら A は連続である.

(ii) A は G_2 -ガロア拡大, $T = A^p$ とする. $G|T \cong H \mathbb{Z}^n$, T/B は H -ガロア拡大である. $\sigma|T = \sigma'$, $\tau|T = \tau'$ とおけば, $T = B[x, y] \cong B[X, Y] / (X^p - X - a, Y^p - Y - b) B[X, Y]$, $\sigma'(f(x, y)) = f(x+1, y)$, $\tau'(f(x, y)) = f(x, y+1)$ である. $\uparrow$ より $A = T \oplus_{\mathbb{Z}} T \oplus \cdots \oplus_{\mathbb{Z}} T^{p-1}$, $z^p - z = u \in T$, $\rho(z) = z+1$ とする. $z \in A$ が存在する. $\rho(-z + \sigma(z)) = -(z+1) + \rho\sigma(z) = -(z+1) + \sigma\rho(z) = -(z+1) + \sigma(z) + 1 = -z + \sigma(z)$, $\rho(-z + \tau(z)) = -(z+1) + \rho\tau(z) = -(z+1) + \tau\rho(z) = -(z+1) + \tau(z+1) = z + \tau(z)$ より $\sigma(z) = z+v$, $\tau(z) = z+w$, $v, w \in A^p = T$ である. $z = \sigma^p(z) = z + T\sigma'(v)$, $z = \tau^p(z) = z + T\sigma'(w)$ からそれぞれ $T\sigma'(v) = T\sigma'(w) = 0$ を得る. $\sigma'(u) = \sigma'(z^p - z) = z^{p+v^p} - z - v = u + v^p - v$, $\tau'(u) = \tau(z^p - z) = z^{p+w^p} - z - w = u + w^p - w$ より, $z + v + \sigma'(u) = \sigma(z+w) = \sigma\tau(z) = \tau\sigma(z) = \tau\sigma(z+1) = \tau(z+v+1) = z+w+\tau'(v)+1$ より $v + \sigma'(u) = w + \tau'(v) + 1$ を得る.

$A = T[z] = T[Z] / (Z^p - Z - u) T[Z]$ とすれば $\rho(\sum_{i=0}^{p-1} z^i t_i) = \sum_{i=0}^{p-1} (z+1)^i t_i$, A/T は (ρ) -巡回拡大である. $\sigma(\sum_{i=0}^{p-1} z^i t_i) = \sum_{i=0}^{p-1} (z+v)^i \sigma'(t_i)$, $\tau(\sum_{i=0}^{p-1} z^i t_i) = \sum_{i=0}^{p-1} (z+w)^i \tau'(t_i)$ であり, σ, τ を定義すれば, $\sigma(z^p - z) = z^{p+v^p} - z - v = u + v^p - v = \sigma'(u)$, $\tau(z^p - z) = z^{p+w^p} - z - w = u + w^p - w$, $\sigma^p(z) = z + T\sigma'(v) = z$, $\tau^p(z) =$

$z + T\sigma'(w) = z$ より, σ, τ はそれぞれ位数 p の A の自己同型と仮定する. $\sigma\tau(z+t) = \sigma[(z+w)\tau'(t)] = (z+v+\sigma'(w))\sigma'\tau'(t)$,
 $\tau\sigma\tau(z+t) = \tau\sigma[(z+1)t] = \tau[(z+v+1)\sigma'(t)] = (z+w+\tau'(v)+1)\cdot$
 $\tau'\sigma'(t) = (z+v+\sigma'(w))\sigma'\tau'(t)$ より $\sigma\tau = \tau\sigma\tau$, $\sigma\tau(z+t) = \sigma[(z+1)t] = (z+v+1)\sigma'(t)$, $\tau\sigma(z+t) = \tau[(z+w)\tau'(t)] = (z+w+1)\tau'(t)$ より $\tau\sigma = \sigma\tau$ となる. これから, $(\sigma, \tau, \tau) \cong G_2$ であり, $A^{G_2} = B$, A/T , T/B が分離拡大であるから A/B は分離拡大である. T が連結であるとき, A が連結であるようにとれることは後に証明する.

補題 2 (i) p を素数, $1 \leq k < p-1$ とすると, $1^k + 2^k + \dots + (p-1)^k \equiv 0 \pmod{p}$ である.

(ii) B を $\text{GF}(p)$ 上の多項式環, $A = B \oplus xB \oplus \dots \oplus x^{p-1}B$ を B 上の (σ) -巡回拡大とする ($\sigma(x) = x+1$).

(1) $T_\sigma(x^k h) = 0$ ($0 \leq k < p-1$), $T_\sigma(x^{p-1} h) = -h$ ($k=p-1$) である.

(2) A の元 $g(x) = \sum_{i=0}^{p-2} x^i h_i$ は適当な $f(x) \in A$ により $\sigma(f(x)) = f(x)$ と表わされる.

証明 (i) 略

(i) (1) $T_0(x^k h) = x^k h + (x+1)^k h + \dots + (x+p-1)^k h$
 $= p x^k h + x^{k-1} \binom{k}{k-1} (1+2+\dots+p-1) h + \dots + x^i \binom{k}{i} (1^{k-i} + \dots + (p-1)^{k-i}) h$
 $+ \dots + (1^k + 2^k + \dots + (p-1)^k) h$ であるから (i) より主張が得られる。

(2) 任意の $0 \leq k < p-1$ に対し, $k+1$ は正則元であり $\sigma((k+1)^{-1} x^{k+1} h) - (k+1)^{-1} x^{k+1} h = x^k h + \sum_{j=0}^{k-1} x^j c_j$ ($c_j \in B$) であるから, 帰納法により, 主張が得られる。

系 1 B を $\text{GF}(p)$ 上の多環とする。

(i) B は常に G_1 -ガロア拡大を有する。

(ii) B が連結のとき, 連結な G_1 -ガロア拡大が存在するための必要十分条件は, 任意の $(\alpha, \beta) (\neq (0, 0)) \in \text{GF}(p) \times \text{GF}(p)$ と B の任意の元 c に対して $c^p - c \neq a\alpha + b\beta$ となる $a, b \in B$ が存在することである。

(iii) B は常に G_2 -ガロア拡大を有する。

(iv) B が連結のとき, 任意の $(\alpha, \beta) (\neq (0, 0)) \in \text{GF}(p) \times \text{GF}(p)$ と B の任意の元 c に対し $c^p - c \neq a\alpha + b\beta$ となる $a, b \in B$ が存在すれば, B は連結な G_2 -ガロア拡大をもつ。

証明 (i) $T = B[x, y] = B[X, Y] / (X^p - x - a, Y^p - y - b) B[x, y]$ は H -ガロア拡大である。 $\sigma'(x) = x + 1$ とする。今 $v = -$

x^{P-1} とすれば, 補題 2, (ii), (1) から $T_{\sigma'}(v) = 1$, $v^P - v = -(x+a)^{P-1} + x^{P-1} = -(\sum_{i=0}^{P-1} \binom{P-1}{i} x^i a^{P-1-i})$ であるから補題 2, (ii), (2) から, 適当な $f(x) \in B[x]$ で $\sigma'(f(x)) - f(x)$ と表わされる。
 $u = f(x) + y(a+h)$ とおけば $\sigma'(u) - u = \sigma'(f(x)) - f(x) = v^P - v$ であるから, $\{u, v\}$ は $T/B[y]$ の (σ', p) -生成系である。
 $t = y + x$ とおけば, $T_{\tau'}(t) = 0$, $\tau'(u) - u = a+h = x^P - x$, $\sigma'(t) - t = 1$, $\tau'(v) - v = 0$ より, T には定理 4(i) の条件を満たす t が存在する。

(ii) 定理 4(i) と補題 1 から明らかである。

(iii) (i) と同様, $T = B[x, y] \cong B[X, Y]/(X^P - X - a, Y^P - Y - h)B[X, Y]$ は $\sigma'(x) = x+1$, $\tau'(y) = y+1$ で H -ガロア拡大である。
 $v = x$, $w = x+y+1$, $u = xa + y(a+h)$ とすれば, $T_{\sigma'}(v) = T_{\sigma'}(w) = 0$, $\sigma'(u) = (x+1)a + y(a+h)$, $u + v^P - v = xa + y(a+h) + x^P - x = (x+1)a + y(a+h)$, $\tau'(u) = xa + (y+1)(a+h)$, $u + w^P - w = xa + y(a+h) + (a+h) = xa + (y+1)(a+h)$, $v + \sigma'(w) = x + x + y + 2 = 2(x+1) + y$, $w + \tau'(v) + 1 = x + y + 1 + x + 1 = 2(x+1) + y$ であるから定理 3(ii) の条件を満たす u, v, w が T に存在する。

(iv) 条件から (iii) における T は連結と仮定してよい。(iii) における u に対して $x^P - x - u$ が既約を示せば十分である。 $T \ni t = \sum_{i=0}^{P-1} x^i f_i(y)$ ($f_i(y) \in B[y]$) が $x^P - t = u$ を満たすと

しよ。このとき補題1の証明と同様の方法で, $t = xf_1(y) + f_0(y)$ となる。 $t^p - t = (x+a)f_1(y)^p + f_0(y)^p - xf_1(y) - f_0(y) =$
 $= x(f_1(y)^p - f_1(y)) + af_1(y)^p + f_0(y)^p - f_0(y) = xa + y(a+h)$ となり, $f_1(y)^p - f_1(y) = a$ となり $x^p - x - a$ の $B[y][X]$ における既約性に反する。これで定理3 (ii) の残りの部分も証明されたことになる。

文献

- [1] K. Kishimoto, On Abelian extensions of rings I, Math. J. of Okayama Univ., vol.14(1970), 159-174.
- [2] K. Kishimoto, On Abelian extensions of rings II, Math. J. of Okayama Univ., vol.15(1971), 57-70.
- [3] T. Nagahara and A. Nakajima, On cyclic extensions of commutative rings, Math. J. Okayama Univ., vol.15(1971), 81-90.
- [4] T. Nagahara and A. Nakajima, On strongly cyclic extensions of commutative rings, Math. J. of Okayama Univ., vol. 15(1971), 91-100.