数理解析研究所講究録
第 235 巻 1975 年 26-43

Metacyclic群を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 $GF(p)$ 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．ここでは，$G \rhd (\sigma)$，$G/(\sigma)$ がアーベル群となる有限非アーベル群Gを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 $2m$ の正二面体群，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

ア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ζを含むとき，$\Gamma(n)=\{n, \zeta, 1-\zeta^i; i=0,1,2,\cdots,n\}$とする。

(ii) 環が連結であるとは，0，1以外に巾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（$G=(\sigma)$と記す）のとき，G－ガロア拡大を(σ)－巡回拡大とよぶ。$U(B)\supsetneqq\Gamma(n)$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$\{x^i; i=0,1,2,\cdots,n-1\}$はB上一次独立な基底で，$A=B\oplus xB\oplus\cdots\cdots\oplus x^{n-1}B$となる。またAがB上の$(\sigma)$－強巡回拡大であることと$A/B$が$(\sigma)$－正規底をもつガロア拡大であることとは同値である。

(iv) Bを$GF(p)$上の多元環，$G=(\sigma)$を位数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$\{x^i; i=0,1,2,\cdots,p-1\}$はB上の一次独立な基底で，$A=B\oplus xB\oplus\cdots\oplus x^{p-1}B$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 $\rho:\sum X^i a_i+(X^p-X-u)A[X]\longrightarrow\sum(X+v)^i\sigma(a_i)+(X^p-X-u)A[X]$ で B 上 (ρ)-巡回拡大となり, ρ の位数は p^2, $\rho|A=\sigma$ である. この $\{u,v\}$ を 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)-強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 $A=\oplus_{i=0,j=0}^{m-1\ \ 1}x^iy^jB\cong B[X,Y]/(X^m-(d+Ye),Y^2-b)B[X,Y]$ ($f(X,Y)+(X^m-(d+Ye),Y^2-b)B[X,Y]\longrightarrow f(x,y)$) として得られ, $f(x,y)=\sum_{i=0,j=0}^{m-1\ \ 1}x^iy^jb_{ij}$ ($b_{ij}\in B$) を A の任意の元としたとき $\sigma(f(x,y))=f(x\zeta,y)$, $\tau(f(x,y))=f(x^{-1}c,-y)$ 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

るから $A = T \oplus xT \oplus \cdots \oplus x^{m-1}T$，$x \in U(A)$, $\sigma(x) = x\mathfrak{f}^2$, $T = B \oplus yB$, $y \in U(T)$，$\tau(y) = -y$ となる．$\sigma(x\tau(x)) = x\mathfrak{f}^2\sigma\tau(x) = x\mathfrak{f}^2\tau\sigma^{-1}(x) = x\mathfrak{f}^2\tau(x)\mathfrak{f}^{-2} = x\tau(x)$，$x\tau(x) = x\tau(x)$ より $x\tau(x) \in A^{D_m} = B$ を得る．すなわち，$\tau(x) = x^{-1}c$，$c \in U(B)$ である．$x^m \in T = B \oplus yB$ であるから，$x^m = d + ye\ (d, e \in B)$ であるが $(d+ye)^{-1}c^m = x^{-m}c^m = \tau(x^m) = \tau(d+ye) = d - ye$ である．今 $y^2 = b\ (\in U(B))$ とすれば，$c^m = (d+ye)(d-ye) = d^2 - be^2$ である．

$B[X, Y] \ni f(X, Y) = \sum X^iY^jb_{ij}$ に対して，$f(x, y) = \sum x^iy^jb_{ij} \in A$ を対応させると，この対応は環全型であり，その核は $(X^m-(d+Ye), Y^2-b)B[X,Y]$ を含む．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 で割ることによって，$g(X,Y) = h(X,Y)(X^m-(d+Ye)) + k(X,Y)(Y^2-b) + \sum_{i=0,j=0}^{m-1,\ 1} X^iY^jb_{ij}$ とできる．$0 = g(x,y) = \sum_{i=0,j=0}^{m-1,\ 1} x^iy^jb_{ij}$ であるから $b_{ij} = 0$ 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．$f(Y) \longrightarrow f(-Y)$ 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．$(d+ye)(d-ye) = d^2-be^2 = c^m \in U(B)$ であるから 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，$\sigma(\sum_{i=0}^{m-1} x^it_i) = \sum_{i=0}^{m-1}(x\mathfrak{f}^2)^it_i\ (t_i \in T)$ で σ を定義すれば

$\sigma(x^m)=(x\zeta^2)^m=x^m=d+ye=\sigma(d+ye)$, $\sigma^m(x)=x\zeta^{2m}=x$ 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．ここで$\tau(\sum_{i=0}^{m-1}x^i t_i)=\sum_{i=0}^{m-1}(x^{-1}c)^i\tau^*(t_i)$とすれば，$\tau(x^m)=x^{-m}c^m=(d+ye)^{-1}c^m=(d+ye)^{-1}(d^2-be^2)=(d+ye)^{-1}\cdot(d+ye)(d-ye)=(d-ye)=\tau(d+ye)$，$\tau^2(x)=\tau(x^{-1}c)=x$，$\tau^2(y)=y$より，$\tau$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，$\sigma\tau(f(x,y))=\sigma(f(x^{-1}c,-y))=f(x^{-1}\zeta^{-2}c,-y)$，$\tau\sigma^{-1}(f(x,y))=\tau(f(x\zeta^{-2},y))=f(x^{-1}c\zeta^{-2},-y)$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$8=2^3$の非アーベル群は正二面体群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　$U(B)\supseteq\Gamma(4)$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$b,c\in U(B)$，$d,e\in B$が存在するこ

とである．

さらに，Bを連結とするとき，Aが連結であるための必要十分条件は

(2) 連立方程式

$$\begin{cases} d - X^2 - Y^2 b = 0 \\ e - 2XY = 0 \end{cases}$$ がB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) $d^2 - be^2 = bc^4$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，$A = \oplus_{i=0}^{3} \oplus_{j=0}^{1} x^i y^j B \cong B[X, Y]/(X^4 - (d + Ye), Y^2 - b)B[X, Y]$ $(f(X, Y) + (X^4 - (d + Ye), Y^2 - b)B[X, Y] \longrightarrow f(x, y))$ として得られ，$f(x, y)$をAの任意の元とすれば，$\sigma(f(x, y)) = f(xi, y)$，$\tau(f(x, y)) = f(x^{-1}yc, y)$である．さらにBが連結であるとき，Aが連結であ必要十分条件は(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$A=T[x] \cong T[X]/(X^4-(d+ye))T[X]$ $(f(X)+(X^4-(d+ye))T[X] \longrightarrow f(x))$が連結であることと$A^{\sigma^2}=T[x^2] \cong T[Z]/(Z^2-(d+ye))T[Z]$ $(f(Z)+(Z^2-(d+ye))T[Z] \longrightarrow f(x^2))$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Q-ガロア拡大，$A^\sigma=T$とすれば，$A=T \oplus xT \oplus \cdots \oplus x^3T$，$x \in U(A)$，$\sigma(x)=x\zeta$，$T=B \oplus yB$，$y \in U(T)$，$\tau(y)=-y$である．$x^4=d+ye$，$y^2=b$とする．$\sigma(x\tau(x))=x \cdot \zeta\sigma\tau(x)=x\zeta\tau(x)\zeta^{-1}=x\tau(x)$より$\tau(x)=x^{-1}t$，$t \in U(T)$である．一方，$-x=\sigma^2(x)=\tau^2(x)=xt^{-1}\tau(t)$より$\tau(t)=-t$となるから，$t=yc$，$c \in U(B)$でなければならない．すなわち，$\tau(x)=x^{-1}yc$である．$x^{-4}b^2c^4=x^{-4}(yc)^4=\tau(x^4)=\tau(d+ye)=d-ye$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$GF(p)$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 $(\alpha,\beta)\,(\neq(0,0))\in GF(p)\times GF(p)$ 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 $\{(x\alpha+y\beta)^i;\ i=0,1,\cdots,p-1\}$ が B 上一次独立であることが知られる．$T\supseteq B[x\alpha+y\beta]\cong B[Z]/(Z^p-Z-(a\alpha+b\beta))B[Z]$ で，$B[x\alpha+y\beta]$ は連結であるから，$Z^p-Z-(a\alpha+b\beta)$ は既約，したがってすべての $c\in B$ 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 $f(x)=\sum_{i=0}^{p-1}x^ic_i$ $(c_i\in B)$ が $f(x)^p-f(x)=b$ を満たすとしよう．$f(x)^p-f(x)=(\sum_{i=0}^{p-1}x^ic_i)^p-\sum_{i=0}^{p-1}x^ic_i=\sum_{i=0}^{p-1}(x+a)^ic_i^p-\sum_{i=0}^{p-1}x^ic_i=b$ であるから $c_{p-1}^p-c_{p-1}=0$．ここで，B が連結であることに注意すれば，$c_{p-1}\in GF(p)$ 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，$u=\binom{p-1}{p-2}c_{p-1}^p=(p-1)c_{p-1}\neq0$ 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，$c_{p-1}=c_{p-2}=\cdots=c_2=0$ で $f(x)=xc_1+$

c_0を得る．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，$c_1\in GF(p)$ 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$GF(2)$上の多元環とする．

(i)　$A=\oplus_{i=0,j=0,k=0}^{1,1,1} x^iy^jz^kB=B[X,Y,Z]/(X^2-X-a,\ Y^2-Y-b,\ Z^2-Z-Xa)B[X,Y,Z]$ 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)　$A=\oplus_{i=0,j=0,k=0}^{1,1,1} x^iy^jz^kB=B[X,Y,Z]/(X^2-X-a,\ Y^2-Y-b,\ Z^2-Z-X(a+b)-Yb)B[X,Y,Z]$ 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$(\alpha,\beta)(\neq(0,0))\in GF(2)\times GF(2)$と任意の$c\in B$に対して，$c^2-c\neq a\alpha+b\beta$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$\sigma'(f(x,$

$y)=f(x+1,y)$, $\tau'(f(x,y))=f(x,y+1)$ によって $H=(\sigma')\times(\tau')$-ガロア拡大となる．$A=T[z]\cong T[Z]/(Z^2-Z-xa_0)T[Z]$ で A/T は分離拡大となり，$\sigma(t_0+zt_1)=\sigma'(t_0)+(z+x)\sigma'(t_1)$ と定義すれば，$\sigma(z^2-z)=(z+x)^2-(z+x)=(z^2-z)+(x^2-x)=xa+a=(x+1)a=\sigma'(xa)$，$\sigma^4(zt)=\sigma^2(z+1)\sigma'^4(t)=zt$ 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 $\tau(t_0+zt_1)=\tau'(t_0)+z\tau'(t_1)$ と定義すれば $\tau(z^2-z)=z^2-z=xa_0=\tau'(xa)$ より τ は位数2の A の自己同型と考えてよい．$\sigma\tau(f(x,y,z))=\sigma(f(x,y+1,z))=f(x+1,y+1,z+x)$，$\tau\sigma^{-1}(f(x,y,z))=\tau(f(x+1,y,z+x))=f(x+1,y+1,z+x)$ より $\sigma\tau=\tau\sigma^{-1}$ を得て，$(\sigma,\tau)=D_4$ を得る．$A^{D_4}=B$，A/T，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，$T=B[x,y]\cong B[X,Y]/(X^2-X-a,Y^2-Y-b)B[X,Y]$ $(f(X,Y)+(X^2-X-a,Y^2-Y-b)B[X,Y]\longrightarrow f(x,y))$，$a,b\in B$ 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．次に十分性を証明しよう．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．$A=T[Z]/(Z^2-Z-Xa)$

T[Z] は (ii) 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の巾等元とする．$\sigma^2(e)+e$ はTの巾等元であるから $\sigma^2(e)+e=1$ 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)．さらに．$\sigma^2(\sigma(e)+e)=\sigma^3(e)+\sigma^2(e)=\sigma(\sigma^2(e))+e+1=\sigma(e)+1+e+1=\sigma(e)+e$ 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 $\sigma(e)\in A^{\sigma}\subseteqq A^{\sigma^2}\subseteqq T$ 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，(iii)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Q-ガロア拡大である．逆も同様の手法で得られる．

§ $|G|=p^3$, p：奇素数の場合

この節では，Bは $GF(p)$ 上の多元環，Gは位数 p^3（pは奇素数）の群，$H=(\sigma')\times(\tau')$ は位数 p^2 の基本アーベル群とする．このときGは $G_1=(\sigma,\tau)$, $\sigma^{p^2}=\tau^p=1$, $\sigma\tau=\tau\sigma^{p+1}$ か，$G_2=(\sigma,\tau,\rho)$, $\sigma^p=\tau^p=\rho^p$, $\sigma\tau=\tau\sigma\rho$, $\sigma\rho=\rho\sigma$, $\tau\rho=\rho\tau$ 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．

$T^{\tau'}/B$の適当な(σ', p)−生成系$\{u, v\}$に対して

(1)　$\tau'(u) - u = t^p - t$

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

(3)　$T_{\tau'}(t) = 0$

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)　$T_{\sigma'}(v) = T_{\tau'}(w) = 0$

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

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

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．$G_1(T) = \{\eta(t) \mid t \in T, \eta \in G_1\} \subseteqq T$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 $T^{\sigma'} = B[y]$ 上 (σ')－巡回拡大であるから，(σ', p)－生成系 $\{u, v\}$ を有し，A には $A = T \oplus zT \oplus \cdots \oplus z^{p-1}T$，$z^p - z = u$ 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(1)－(3)を満たす H－ガロア拡大とする．$A = T[z] = T[Z]/(Z^p - Z - u)T[Z]$ 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．$\sigma\tau(zt') = \sigma((z+t)\tau'(t')) = (z+v+\sigma'(t))\sigma'\tau'(t') = (z+v+t+\tau'(v)-v+1)\sigma'\tau'(t') = (z+t+\tau'(v)+1)\sigma'\tau'(t')$，$\tau\sigma^{p+1}(zt') = \tau[(z+v+1)\sigma'(t')] = (z+t+\tau'(v)+1)\sigma'\tau'(t')$ より $\sigma\tau = \tau\sigma^{p+1}$，すなわち，$(\sigma, \tau) \cong G_1$ を得る．$A^{G_1} = T^H = B$ であり，A/A^{σ^p}，A^{σ^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．A/T^σが(σ)-巡回拡大であるから，[3]よりTが連結ならAは連結である．

(ii) AをG_2-ガロア拡大，$T=A^\rho$とする．$G|T\cong H$で，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．さらに$A=T\oplus zT\oplus\cdots\oplus z^{p-1}T$，$z^p-z=u\in T$，$\rho(z)=z+1$となる$z\in A$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$\sigma(z)=z+v$，$\tau(z)=z+w$，$v,w\in A^\rho=T$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．$\sigma'(u)=\sigma'(z^p-z)=z^p+v^p-z-v=u+v^p-v$，$\tau'(u)=\tau(z^p-z)=z^p+w^p-z-w=u+w^p-w$で，$z+v+\sigma'(w)=\sigma(z+w)=\sigma\tau(z)=\tau\sigma\rho(z)=\tau\sigma(z+1)=\tau(z+v+1)=z+w+\tau'(v)+1$より$v+\sigma'(w)=w+\tau'(v)+1$を得る．

$A=T[z]=T[Z]/(Z^p-Z-u)T[Z]$とすれば$\rho(\sum_{i=0}^{p-1}z^it_i)=\sum_{i=0}^{p-1}(z+1)^it_i$で，$A/T$は$(\rho)$-巡回拡大となる．$\sigma(\sum_{i=0}^{p-1}z^it_i)=\sum_{i=0}^{p-1}(z+v)^i\sigma'(t_i)$，$\tau(\sum_{i=0}^{p-1}z^it_i)=\sum_{i=0}^{p-1}(z+w)^i\tau'(t_i)$で$\sigma$，$\tau$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 の自己同型となる．$\sigma\tau(zt)=\sigma[(z+w)\tau'(t)]=(z+v+\sigma'(w))\sigma'\tau'(t)$, $\tau\sigma\rho(zt)=\tau\sigma[(z+1)t]=\tau[(z+v+1)\sigma'(t)]=(z+w+\tau'(v)+1)\cdot\tau'\sigma'(t)=(z+v+\sigma'(w))\sigma'\tau'(t)$ より $\sigma\tau=\tau\sigma\rho$, $\sigma\rho(zt)=\sigma((z+1)t)=(z+v+1)\sigma'(t)$, $\rho\sigma(zt)=\rho[(z+v)\sigma'(t)]=(z+v+1)\sigma'(t)$ より，$\sigma\rho=\rho\sigma$, $\tau\rho(zt)=\tau[(z+1)t]=(z+w+1)\tau'(t)$, $\rho\tau(zt)=\rho[(z+w)\tau'(t)]=(z+1+w)\tau'(t)$ より $\tau\rho=\rho\tau$ となる．これから，$(\sigma,\tau,\rho)\cong G_2$ 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，$1\leqq k<p-1$ とすると，$1^k+2^k+\cdots+(p-1)^k\equiv 0\ (\mathrm{mod.}\ p)$ である．

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

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

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

証明　(i)　略

(ii) (1) $T_\sigma(x^k b) = x^k b + (x+1)^k b + \cdots\cdots + (x+p-1)^k b$
$= p x^k b + x^{k-1}\binom{k}{k-1}(1+2+\cdots+p-1)b + \cdots + x^i\binom{k}{i}(1^{k-i}+\cdots+(p-1)^{k-i})b$
$+ \cdots\cdots + (1^k + 2^k + \cdots\cdots + (p-1)^k)b$ であるから (i) より主張が得られる．

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

系 1　B を $GF(p)$ 上の多元環とする．

(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 $(\alpha, \beta)(\neq(0,0)) \in GF(p) \times GF(p)$ 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 $(\alpha, \beta)(\neq(0,0)) \in GF(p) \times GF(p)$ 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$(\sigma',p)$-生成系である．$t=y+x$とおけば，$T_{\tau'}(t)=0$，$\tau'(u)-u=a+h=t^p-t$，$\sigma'(t)-t=1$，$\tau'(v)-v=0$より，$T$には定理4(i)の条件を満たすこれが存在する．

(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)の条件を満足する$u,v,w$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$t^p-t=u$を満たすと

しょう．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．$t^p - t = (x+a)f_1(y)^p + f_0(y)^p - xf_1(y) - f_0(y) = x(f_1(y)^p - f_1(y)) + af_1(y)^p + f_0(y)^p - f_0(y) = xa + y(a+h)$ より，$f_1(y)^p - f_1(y) = a$ 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. of Okayama Univ., vol. 15 (1971), 81-90.

[4] T. Nagahara and A. Nakajima, On strongly cyclic extensions of commutative rings, ~~Maths.~~ J. of Okayama Univ., vol. 15 (1971), 91 - 100.