

involution をもつガロア拡大

阪市大 神崎照夫

1. Rosenberg-Ware の定理の拡張

一般に単位元をもつ非可換環を考える。 A を involution $A \rightarrow A; a \mapsto \bar{a}$, $(\overline{ab} = \bar{b}\bar{a}, \overline{a+b} = \bar{a} + \bar{b}, \overline{\bar{a}} = a, a, b \in A)$ をもつ環とする。有限生成射影的 A -左加群 M 及び写像 $f: M \times M \rightarrow A$ が $\overline{f(x, y)} = f(y, x)$, $f(ax + by, z) = af(x, z) + bf(y, z)$, $(x, y \in M, a, b \in A)$ をみたすとき、 $f = (M, f)$ をエルミット A -左加群とよぶ。特に写像 $M \rightarrow \text{Hom}_A(M, A): x \mapsto f(-, x)$ が 1 対 1 写像をなすとき、 f は非退化であるとなう。環 $A \supset B$ が次の条件をみたすとき、 involution をもつ G -ガロア拡大とよぶ。即ち、 1) $A \supset B$ は G -ガロア拡大、即ち G は環 A の有限個の自己同型写像からなる群で $A^G = B$ をみたし、 $\sum_i x_i y_i = 1$, $\sum_i x_i \sigma(y_i) = 0$ ($\sigma \neq I \in G$) を満たす A の元 $x_1, \dots, x_n, y_1, \dots, y_n$ (G -ガロアシステムとよぶ) が存在。 2) A は $\overline{\sigma(a)} = \sigma(\bar{a})$, $\forall \sigma \in G, a \in A$, を満たす involution をもつ。
 $A \supset B$ が involution をもつ G -ガロア拡大ならば A は次の

様にエルミット B -左加群と見られる。 C を A の中心とし、 $C_0 = \{c \in C; \bar{c} = c\}$ の単元の全体 $\mathbb{U}_C(A)$ に対し、 $t_G^u(a) = \sum_{\sigma \in G} \sigma(ua)$ $u \in \mathbb{U}_C(A)$, $a \in A$, $t_G^1 = t_G$ とおく。任意の $u \in \mathbb{U}_C(A)$ に対し、 $b_t^u: A \times A \rightarrow B$ を $b_t^u(x, y) = t_G^u(xy)$ と定義するとき、 $b_t^u = (A, b_t^u)$ は非退化エルミット B -左加群をなす (非退化であることは、 $u\bar{y} = \sum_i x_i t_G^u(y_i \bar{y}) = \sum_i x_i b_t^u(y_i, y)$ ($\forall y \in A$)、及び、 $f \in \text{Hom}_B(A, B)$ は $f(x) = t_G^u(\bar{u}x \sum_i x_i f(y_i)) = b_t^u(x, \sum_i x_i f(y_i))$ と表わされることより)。 involution をもつ G -ガロア拡大に於て、 involution が特に恒等写像の場合、環は必然的に可換環となり普通の意味の G -ガロア拡大になる。この場合自明な involution をもつ G -ガロア拡大とよぶ事とする。

エルミット B -左加群 $(\mathbb{U}, g)$ に対し、 $\mathbb{U}^* = \text{Hom}_B(\mathbb{U}, B)$ を、 $(bf)(x) = f(x)\bar{b}$, $(b \in B, f \in \mathbb{U}^*, x \in \mathbb{U})$ によって B -左加群と見て、直和 $\mathbb{U} \oplus \mathbb{U}^*$ を作り、 $h_g: (\mathbb{U} \oplus \mathbb{U}^*) \times (\mathbb{U} \oplus \mathbb{U}^*) \rightarrow B$; $(x+f, x'+f') \rightsquigarrow \overline{f(x')} + f(x) + g(x, x')$ によって定義されたエルミット B -左加群 $(\mathbb{U} \oplus \mathbb{U}^*, h_g)$ を考える。この様な $(\mathbb{U} \oplus \mathbb{U}^*, h_g)$ に isometric なエルミット B -左加群を metabolic B -左加群とよぶ (エルミット B -左加群 (M, g) , (M', g') に於て $g'(\varphi(m), \varphi(n)) = g(m, n)$ ($m, n \in M$) を満たす B -同型写像 $\varphi: M \rightarrow M'$ を isometry とよび、 (M, g) と (M', g') は isometric

であるとする)。又 $I: B \times B \rightarrow B; (x, y) \mapsto x\bar{y}$ によって定義されたエルミット B -左加群 (B, I) を $\langle 1 \rangle_B$ で表わす。

定義 *involution* をもつ G -ガロア拡大 $A \supset B$ が次の条件を満たす $U_c(A)$ の元 u をもつとき、 $A \supset B$ は奇数型であるとする。即ち、 (A, b_t^u) は、或る *metabolic* B -左加群 (N, h_m) と $\langle 1 \rangle_B$ の直交和に *isometric* である： $(A, b_t^u) \cong \langle 1 \rangle_B \perp (N, h_m)$ 。

Scharlau の定理 ([5] p. 195, Th. 1.6) より体の場合に次の定理を得る。

定理 1. 体 K, L に対し、 $L \supset K$ を *involution* をもつ G -ガロア拡大とする。 $L \supset K$ が奇数型である為の必要十分条件は $[L: K] = \text{奇数}$ である。

証明、 $L \supset K$ が奇数型ならば、明らかに $[L: K] = \text{奇数}$ 。逆に $[L: K] = 2m+1$ とする。先づ、 $L \supset K$ が自明な *involution* をもつ G -ガロア拡大である場合を考える。適当な $a \in K$ に対して、 $L = K[a] = K \oplus Ka \oplus \dots \oplus Ka^{2m}$ 。 $f: L \rightarrow K$ を、 $f(1) = 1$, $f(a^i) = 0$, $i = 1, 2, \dots, 2m$ で定義された K -1次写像とする。

(L, b_t^1) の非退化性から、 $b_t^1(x, u) = f(x)$ ($x \in L$) を満たす L の元 $u \neq 0$ が存在する。 $b_t^u(x, y) = f(xy)$, ($x, y \in L$), $(L, b_t^u) = K \perp (Ka \oplus \dots \oplus Ka^{2m})$, $(K, b_t^u) = \langle 1 \rangle_K$ である。 $(Ka \oplus \dots \oplus Ka^{2m})$ は次に示す補題 1 を用いて *metabolic* B -左加群となることが得られる。次に $L \supset K$ を自明でない *involution* をもつ G -ガロ

ア拡大とする。 $L_0 = \{x \in L; \bar{x} = x\}$, $K_0 = L_0 \cap K$ と置く。
 このとき、 $[L:K] = \text{奇数}$ より $[L:L_0] = [K:K_0] = 2$ を得る。よ
 って、 $L = K \cdot L_0 \cong K \otimes_{K_0} L_0$, $L_0 \supset K_0$ は自明な *involution* をもつ
 G -ガロア拡大、従って、前述の場合より $\cup_c(L) = \{c \in L_0; c \neq 0\}$
 の元 u が存在し、 $(L_0, b_t^u) \cong \langle 1 \rangle_{K_0} \perp (N, h)$, (N, h) は或る
metabolic K_0 -左加群となる。従って、 $(L, b_t^u) \cong (K \otimes_{K_0} L_0, b_t^u)$
 $\cong \langle 1 \rangle_K \perp (K \otimes_{K_0} N, h')$ となり、 $(K \otimes_{K_0} N, h')$ は又 *metabolic* K -左
 加群、故に $L \supset K$ は奇数型である。

補題 1. B を *involution* をもつ環、 (M, φ) を非退化エル
 ミット B -左加群とする。 (M, φ) が *metabolic* B -左加群である為
 の必要十分条件は、 $N = N^\perp$ を満たす M の直和因子 N が存在
 することである (但し $N^\perp = \{x \in M; \varphi(x, y) = 0 \ \forall y \in N\}$)。

証明 (M, φ) が *metabolic* ならば、 $(M, \varphi) \cong (\cup \oplus \cup^*, h_\varphi)$ 、
 $(\cup^*)^\perp = \cup^*$ 、従って $\cup^*$ に同型な M の直和因子 N で $N^\perp = N$ を満
 たすものがある。逆に $\varphi = (M, \varphi)$ が $M = N \oplus N'$, $N^\perp = N$ を満
 たす B -部分加群 N をもつとする。写像 $N \rightarrow (N')^* = \text{Hom}_B(N', B)$
 $; x \mapsto \varphi(-, x)$ は B -同型写像となり、 $(N' \oplus N'^*, h_\varphi)$ は写像 M
 $= N \oplus N' \rightarrow (N')^* \oplus N'; x + x' \mapsto \varphi(-, x) + x'$ により (M, φ)
 に *isometric* になる。故に (M, φ) は *metabolic* B -左加群である。

標数 $\neq 2$ の体 K 及びその拡大体 L について次の結果が知ら
 れている。I. Springer の定理 ([8] 又は [5] p.198 参照) $[L:K]$

= 奇数のとき、体 K 上の 2 次形式 q が L 上で isotropic ならば q は K 上で isotropic である。即ち体 K 上の 2 次形式から作られる Witt ring $W(K)$ から体 L 上の Witt ring $W(L)$ への係数拡大で生ずる写像 $W(K) \rightarrow W(L)$ が単写である。II. Rosenberg-Ware の定理 ([6] 又は [5] p.214 参照). $L \supset K$ を奇数位数のガロア群 G をもつガロア拡大とする。 G の元 σ 、 L 上の 2 次形式 $q = \langle a_1, a_2, \dots, a_n \rangle$ ($a_i \in L$) に対し、 $\sigma(q) = \langle \sigma(a_1), \sigma(a_2), \dots, \sigma(a_n) \rangle$ によって $W(L)$ に G の元の作用を定義するとき、 $W(L)$ は G -ring をなす。 $W(L)^G = \{ [q] \in W(L) : \sigma([q]) = [q], \forall \sigma \in G \}$ は $W(L)$ の部分環で、係数拡大により生ずる準同型写像 $W(K) \rightarrow W(L)$ は $W(K)$ から $W(L)^G$ への同型写像を与える。この定理は [7] に於て可換半局所環にまで拡張されている。こゝではこの定理をより一般的な環に於ける involution をもつ奇数型 G -ガロア拡大に拡張する。

再び $A \supset B$ を involution をもつ G -ガロア拡大とする。 A 上の (又は B 上の) 非退化エルミット左加群と isometry とから成るカテゴリーは直交和 $\perp$ を演算に持ち、metabolic 左加群からなる部分カテゴリーをもつ。良く知られる様に Witt-Grthendieck 群 $WG(A)$ (又は $WG(B)$)、Witt 群 $W(A)$ (又は $W(B)$) を構成することが出来る。今 $q = (M, \varphi)$ をエルミット A -左加群とする。 $\sigma \in G$ に対し、 $\sigma^*(q)$ を次の様に定義する。

$\sigma^*(f) = ({}_sM, \sigma f)$, ${}_sM$ は加群としては M と等しく、 A の元 a の作用を $a \cdot m = \sigma(a)m$ によって定義した A -左加群を意味し、 σf は、 $\sigma f: {}_sM \times {}_sM \rightarrow A; (x, y) \mapsto \sigma(f(x, y))$ を表わす。 $\sigma^*(f)$ はエルミット A -左加群となる。 f が非退化ならば $\sigma^*(f)$ も非退化である。写像 $t_f: A \rightarrow B$ に対し、エルミット A -左加群 $f = (M, f)$ からエルミット B -左加群 $t_{f*}(f) = ({}_B M, t_f f)$ が $t_f f(x, y) = t_f(f(x, y))$, $x, y \in M$ によって定義され、 f が非退化ならば $t_{f*}(f)$ も非退化となる。エルミット B -左加群 $h = (N, h)$ に対し、写像 $i: B \hookrightarrow A$ によって、エルミット A -左加群 $i^*(h) = (A \otimes_B N, ih)$ が $ih: (A \otimes_B N) \times (A \otimes_B N) \rightarrow A; (a \otimes x, a' \otimes x') \mapsto a h(x, x') a'$ で定義される。 h が非退化ならば $i^*(h)$ も非退化となる。 σ^* ($\sigma \in G$), t_{f*} , i^* は metabolic 左加群を metabolic 左加群に移すから Witt 群の準同型写像 $\sigma^*: W(A) \rightarrow W(A)$, $t_{f*}: W(A) \rightarrow W(B)$, $i^*: W(B) \rightarrow W(A)$ をひき起こす事は、容易に知られる。 $G^* = \{\sigma^*: W(A) \rightarrow W(A); \sigma \in G\}$, $W(A)^{G^*} = \{[f] \in W(A); \sigma^*([f]) = [f]; \forall \sigma^* \in G^*\}$ と置く。 $T_{G^*} = \sum_{\sigma \in G} \sigma^*$ は $W(A)$ から $W(A)^{G^*}$ の中への準同型写像を与える。次の定理が得られる。

定理 2. B を可換環、 A を (一般に非可換) B -多元環とする。 $A \supset B$ が involution をもつ奇数型 G -ガロア拡大ならば、

1) $i^*: W(B) \rightarrow W(A)$ は単写、 $i^*(W(B)) = T_{G^*}(W(A))$ であり従って、 $W(B) \cong T_{G^*}(W(A))$ である。

2). $t_{\mathcal{G}^*}: W(A) \rightarrow W(B)$ は全字かつ分解, $\ker t_{\mathcal{G}^*} = \ker T_{\mathcal{G}^*}$.
従って, $W(A) \cong T_{\mathcal{G}^*}(W(A)) \oplus \ker T_{\mathcal{G}^*} = i^*(W(B)) \oplus \ker t_{\mathcal{G}^*}$.

3) もし A が可換環ならば, $T_{\mathcal{G}^*}(W(A)) = W(A)^{\mathcal{G}^*}$, 従って
 $i^*: W(B) \rightarrow W(A)^{\mathcal{G}^*}$ は同型写像である。

この定理と前定理とより, 次の結果が得られる。

系1. L, K を体, $L \supset K$ を *involution* をもつ G -ガロア拡大とする. もし $|G| = [L:K] = \text{奇数}$ ならば, $i^*: W(K) \rightarrow T_{\mathcal{G}^*}(W(L)) = W(L)^{\mathcal{G}^*}$ は同型写像, かつ $t_{\mathcal{G}^*}: W(A) \rightarrow W(B)$ は全字かつ分解, 従って, $W(L) \cong W(A)^{\mathcal{G}^*} \oplus \ker t_{\mathcal{G}^*}$ である。

以下この節では定理2の証明を行なう。その爲に、

定理3. $A \supset B$ を *involution* をもつ G -ガロア拡大とする。
 $W(A)$ 上で等式 $i^* \circ t_{\mathcal{G}^*} = T_{\mathcal{G}^*}$ が成り立つ。

証明 $\mathcal{G} = (M, \mathcal{G})$ を非退化エルミット A -左加群とする。 A の G -ガロアシステム $x_1, \dots, x_n, y_1, \dots, y_n$, 及び各 $\sigma \in G$ に対し, A -準同型写像 $e_{\sigma}: A \otimes_B M \rightarrow A \otimes_B M; a \otimes m \mapsto \sum_i a \sigma(x_i) \otimes y_i m$ が定義される事は、等式 $e_{\sigma}(ac \otimes m) = e_{\sigma}(a \otimes \sigma(c)m)$, ($\forall c \in A$) が成立する事より知られる。簡単な計算から、 $e_{\sigma} \circ e_{\sigma} = e_{\sigma}$,

$e_{\sigma} \circ e_{\tau} = 0$ ($\sigma \neq \tau$), $\sum_{\sigma \in G} e_{\sigma} = I$ が示される。従って $A \otimes_B M = \sum_{\sigma \in G} \oplus e_{\sigma}(A \otimes_B M)$. 写像 $\zeta_{\sigma}: {}_{\sigma}M \rightarrow e_{\sigma}(A \otimes_B M); m \mapsto e_{\sigma}(1 \otimes m)$ は A -同型写像をなし、 $A \otimes_B M$ は $\sum_{\sigma \in G} \oplus {}_{\sigma}M$ に A -同型になる。一方 $i^* \circ t_{\mathcal{G}^*}(\mathcal{G}) = (A \otimes_B M, i_{\mathcal{G}} \mathcal{G})$ に於て、次の等式が得られる。

$$it_{\mathbb{G}} f(e_{\sigma}(1 \otimes m), e_{\sigma}(1 \otimes n)) = \sigma(f(m, n)),$$

$$it_{\mathbb{G}} f(e_{\sigma}(1 \otimes m), e_{\tau}(1 \otimes n)) = 0 \quad (\sigma \neq \tau).$$

これは $i^*t_{\mathbb{G}^*}(f) = (A \otimes_B M, it_{\mathbb{G}} f) = \sum_{\sigma \in \mathbb{G}} \perp e_{\sigma}(A \otimes_B M)$,

又、 ζ_{σ} は $\sigma^*(f) = (\sigma M, \sigma f)$ から $i^*t_{\mathbb{G}^*}(f)$ の部分空間 $e_{\sigma}(A \otimes_B M)$ への isometry を与える事を意味する。従って $i^*t_{\mathbb{G}^*}(f) \cong \sum_{\sigma \in \mathbb{G}} \perp \sigma^*(f)$ を得る。

定理4. B を可換環、 A を B -多元環、 $A \supset B$ は involution をもつ奇数型 $\mathbb{G}$ -ガロア拡大とする。 u を $(A, b_t^u) \cong \langle 1 \rangle_B \perp h_m$ (h_m : metabolic) を満たす $\coprod_{\sigma \in \mathbb{G}} (A)$ の元とするとき、 $W(B)$ 上で等式 $t_{\mathbb{G}^*}^u \circ i^* = I$, エルミット A -左加群としての isometry $\sum_{\sigma \in \mathbb{G}} \perp \sigma^*(\langle u \rangle) \cong \langle 1 \rangle_A \perp i^*(h_m)$ が成立する。但し $\langle u \rangle$ は、 $A \times A \rightarrow A : (x, y) \mapsto ux\bar{y}$ によって定義されたエルミット A -左加群を表わす。

証明 $f = (M, f)$ を非退化エルミット B -左加群とする。エルミット B -左加群として $t_{\mathbb{G}^*}^u \circ i^*(f) = (A \otimes_B M, t_{\mathbb{G}}^u i f) \cong (A, b_t^u) \otimes (M, f)$ が成立する事が、 $t_{\mathbb{G}}^u i f(a \otimes m, a' \otimes m') = t_{\mathbb{G}}(ua f(m, m') \bar{a}') = t_{\mathbb{G}}(ua \bar{a}') f(m, m') = b_t^u(a, a') \cdot f(m, m')$ より知られる。よって、 B が可換環である事に注意して、 $t_{\mathbb{G}^*}^u \circ i^*(f) \cong (\langle 1 \rangle_B \perp h_m) \otimes f \cong f \perp h_m \otimes f$ 、 $h_m \otimes f$ は又 metabolic B -左加群となり、 $t_{\mathbb{G}^*}^u \circ i^* = I$ が得られる。 (A, b_t^u) の定義より、 $b_t^u \cong t_{\mathbb{G}^*}(\langle u \rangle)$ が知られる。従って、定理3から

$$i^* \circ t_{G^*}(\langle u \rangle) \cong \sum_{\sigma \in G} \perp \sigma^*(\langle u \rangle), \quad \sum_{\sigma \in G} \perp \sigma^*(\langle u \rangle) \cong i^* \circ t_{G^*}(\langle u \rangle) \cong i^*(b_t^u) \\ = i^*(\langle 1 \rangle_B \perp h_m) = \langle 1 \rangle_A \perp i^*(h_m) \quad \text{を得る.}$$

定理2の証明. $U_c(A)$ の任意の元 u に対し、エルミット A -左加群 $g = (M, g)$ の u による scaling ${}^u g = (M, {}^u g)$ を ${}^u g: M \times M \rightarrow A; (x, y) \mapsto {}^u g(x, y)$ により定義する. u による scaling は $W(A)$ の自己同型字像をひき起こす. 今 u を定理4に於ける様にとる. u による scaling でひき起こされる自己同型字像 $\mu: W(A) \rightarrow W(A)$ に対し、 $t_{G^*}^u = t_{G^*} \circ \mu$. 定理4より、 $t_{G^*}^u \circ i^* = I$ 、従って、 $t_{G^*} \circ \mu \circ i^* = I$. 故に $i^*: W(B) \rightarrow W(A)$ は単字、 $t_{G^*}: W(A) \rightarrow W(B)$ は全字かつ分解する. 定理3より、 $i^* \circ t_{G^*} = T_{G^*}$ 、従って、 $i^* = T_{G^*} \circ \mu \circ i^*$ 故に $\text{Im } i^* = \text{Im } T_{G^*}$, $\text{Ker } t_{G^*} = \text{Ker } T_{G^*}$ となり、 $i^*: W(B) \rightarrow T_{G^*}(W(A))$ は同型字像、 $W(A) = \mu \circ i^*(W(B)) \oplus \text{Ker } t_{G^*} \cong i^*(W(B)) \oplus \text{Ker } t_{G^*}$.

もし A が可換環ならば、 $W(A)$ は $\perp$ 及び $\otimes$ によって導入された加法と乗法に關し可換環をなし単位元 $[\langle 1 \rangle_A]$ をもつ. $W(A)^{G^*}$ はその部分環をなし、 $T_{G^*}(W(A))$ は $W(A)^{G^*}$ のイデアルをなす. 定理4より、 $[\langle 1 \rangle_A] \in T_{G^*}(W(A))$ 、従って $T_{G^*}(W(A)) = W(A)^{G^*}$ を得る. 故に $i^*: W(B) \rightarrow W(A)^{G^*}$ は同型字像である.

2. 半局所環に於ける involution をもつ奇数型ガロア拡大.

A, B を可換環、 $A \supset B$ は involution をもつ G -ガロア拡大とする. $A \supset B$ が奇数型ならば容易に $|G| = \text{奇数}$ が示される ($|M|$

は集合 M の元の個数を表わす)。今次の命題を考える。

(命題 0) involution をもつ G -ガロア拡大が奇数型である爲の必要十分条件は $|G| = \text{奇数}$ である。

定理 5. A, B を可換半局所環、 $A \supset B$ は involution をもつ G -ガロア拡大とする。次の各場合には (命題 0) は真である。

(場合 I) involution は自明で、 B の各極大イデアル $\mathfrak{m}$ に対し $|B/\mathfrak{m}| \geq |G|$ であるとき、

(場合 II) involution は自明でなく、 B の各極大イデアル $\mathfrak{m}$ に対し、次の 2 条件が満たされるとき、: 1) $|B/\mathfrak{m}| \geq |G|^2$,
2) もし $\overline{\mathfrak{m}} = \mathfrak{m}$ ならば、 A の involution は $A/\mathfrak{m}A$ の自明でない involution を引き起こす。

(場合 III) B は極大イデアル $\mathfrak{m}$ をもつ局所環で、 A の involution は自明でなく、 $A/\mathfrak{m}A$ 上に自明な involution を引き起こし、 $|B/\mathfrak{m}| \geq |G|$ 、かつ $B/\mathfrak{m}$ は標数 $\neq 2$ の体か又は有限体であるとき。

以下この節ではこの定理の証明を行なう。

補題 2. A, B を半局所環、 $A \supset B$ は自明な involution をもつ G -ガロア拡大とする。もし B の各極大イデアル $\mathfrak{m}$ に対し、 $|B/\mathfrak{m}| \geq |G|$ ならば、次の事柄が成り立つ。

1) $A = B[a] = B \oplus Ba \oplus \cdots \oplus Ba^{n-1}$ ($n = |G|$) かつ $\{a^i : 0 \leq i < n\}$ は A の B -基底となる A の元 a が存在し、 a の $B[X]$ に属する最小多項式 $F(X) = X^n + d_1 X^{n-1} + \cdots + d_n$ に於て、 d_n は B で可逆的。

2) $h(1)=1$, $h(a^i)=0$, $i=1, 2, \dots, n-1$, によって定義された B -1次写像 $h: A \rightarrow B$ に対し、 $h(x) = t_G(ux) = b'_t(u, x)$ ($\forall x \in A$) を満たす A の可逆元 u が存在する。

証明. 始め B は体であると仮定する. A のすべての原始中等元を $e_1, e_2, \dots, e_m$ とするとき、 $A = Ae_1 \oplus \dots \oplus Ae_m$ は Be_i のガロア拡大体 Ae_i ($i=1, 2, \dots, m$) の直和である. $G_1 = \{\sigma \in G; \sigma(e_i) = e_i\}$, $\sigma_i(e_i) = e_i$ ($i=1, 2, \dots, m$) と置く. $|G| = m|G_1|$. $Ae_i \supset Be_i$ は G_1 -ガロア拡大であり、 $\sigma_i: Ae_i \rightarrow Ae_i$ は B -多元環として同型写像である. $B[X]$ の分離的既約多項式 $f(x)$ が存在して、 $Ae_i \cong B[X]/(f(x))$, $i=1, 2, \dots, m$. B の元 $b_1=0, b_2, \dots, b_m$ を適当に選んで $f(x+b_1), f(x+b_2), \dots, f(x+b_m)$ が互に異なる多項式になる様にする事が出来る. B の代数的閉体に於ける $f(x)=0$ のすべての根を $\alpha_1, \alpha_2, \dots, \alpha_\ell$ ($\ell=|G_1|$) とする. もし $b_1=0, b_2, \dots, b_r$ ($1 \leq r < m$) を、 $f(x+b_1), f(x+b_2), \dots, f(x+b_r)$ が互に相異なる多項式となる様に B から選んでたとする. $|B| \geq |G| = m\ell > r\ell$ より、 $\alpha_i - b_{r+1} \neq \alpha_i - b_j$, $i=1, 2, \dots, \ell$, $j=1, 2, \dots, r$, を満たす B の元 b_{r+1} を選ぶ事が出来る. よって帰納的に $b_1, b_2, \dots, b_m$ を選ぶ事が出来る. $F(x) = f(x+b_1)f(x+b_2)\dots f(x+b_m)$ と置く. 従って、

$B[X]/(F(x)) \cong B[X]/(f(x+b_1)) \oplus \dots \oplus B[X]/(f(x+b_m)) \cong Ae_1 \oplus \dots \oplus Ae_m = A$. よって、 $A = B[a] = B \oplus Ba \oplus \dots \oplus Ba^{n-1}$ となる $a \in A$ が存在し、 a の $B[X]$ に於ける最小多項式は $F(x) = x^n + d_1x^{n-1} + \dots + d_n$

となる。 $f(X+b_i)$ は既約であるから $d_n \neq 0$ である。 $h: A \rightarrow B$ を $h(1)=1$, $h(a^i)=0$, $i=1, 2, \dots, n-1$ によって定義された B -1次写像とする。 (A, b'_t) の非退化性より、 $h(x)=b'_t(x, u)=t_{\mathcal{G}}(xu)$ ($x \in A$) を満たす $u \in A$ が存在する。 u は A の可逆元である事を示す。 $\Omega = \{x \in A; xu=0\}$ と置く。 $h(x)=t_{\mathcal{G}}(xu)$ ($x \in A$) より $\Omega \subset \text{Ker } h = Ba \oplus \dots \oplus Ba^{n-1}$ を得る。 任意の $x \in \Omega$ に対し、 $x = b'_1 a + b'_2 a^2 + \dots + b'_{n-1} a^{n-1}$ と表わされる。 $(a^{n-1} + d_1 a^{n-2} + \dots + d_{n-1} a)x = (a^n + d_1 a^{n-1} + \dots + d_{n-1} a)(b'_1 + b'_2 a + \dots + b'_{n-1} a^{n-2}) = -d_n(b'_1 + b'_2 a + \dots + b'_{n-1} a^{n-2}) \in \Omega \subset Ba \oplus \dots \oplus Ba^{n-1}$ 。 故に $d_n b'_1 = 0$ 従って $b'_1 = 0$, $b'_2 a + \dots + b'_{n-1} a^{n-2} \in \Omega$ 。 再びこれを繰り返して、 $b'_1 = b'_2 = \dots = b'_{n-1} = 0$ 即ち $x=0$ を得る。 よって $\Omega = 0$ 。 A は Artin 環であるから、 u は可逆的である。 次に B を一般の半局所環とする。 B の Jacobson 根基 J に対し、 剰余環 B/J のすべての原始中等元を $e_1, e_2, \dots, e_t$ とする。 $A/JA \supset B/J e_i$ ($i=1, 2, \dots, t$) 及び $A/JA = \sum_{i=1}^t A/JA e_i \supset \sum_{i=1}^t B/J e_i$ は共に G -ガロア拡大である。 $B/J e_i$ は体であり、 前述より $A/JA e_i = B/J e_i[\alpha_i] = B/J e_i \oplus B/J e_i \alpha_i \oplus \dots \oplus B/J e_i \alpha_i^{n-1}$ を満たす $A/JA e_i$ の元 α_i が存在する ($i=1, \dots, t$)。 $\alpha = \alpha_1 + \alpha_2 + \dots + \alpha_t$ と置くと、 $A/JA = B/J \oplus B/J \alpha \oplus \dots \oplus B/J \alpha^{n-1}$ であり、 $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$ は A/JA の B/J -基底をなす。 A に於ける α の代表元 a を取れば、 中山の補題により、 $A = B \oplus Ba \oplus \dots \oplus Ba^{n-1}$ となり、 $\{1, a, \dots, a^{n-1}\}$ は A の B -

基底をなす。又 a の $B[X]$ に於ける最小多項式を $F(X) = X^n + d_1 X^{n-1} + \dots + d_n$ と置けば、 d_n は前半より J を法として可逆的であり、従って、 d_n は B に於て可逆的である。 $k(1)=1, k(a^i)=0 \ i=1, 2, \dots, n-1$, により定義された B -1 次写像 $k: A \rightarrow B$ に対し、 $b_t^1(x, u) = t_q(ux) = k(x) \ (x \in A)$ を満たす A の元 u が存在する。前半より u は JA を法として可逆的であるから、 A で又可逆的である。

(場合 I) に於ける定理 5 の証明。 A, B を半局所環、 $A \supset B$ を自明な involution をもつ G -ガロア拡大とし、 $|G|$ = 奇数、 B の各極大イデアル m に対し、 $|B_m| \geq |G|$ と仮定する。補題 2 より、 $A = B \oplus Ba \oplus \dots \oplus Ba^{n-1}$, $\{1, a, \dots, a^{n-1}\}$ は A の B -基底となる $a \in A$ が存在し、 $k(1)=1, k(a^i)=0 \ (1 \leq i \leq n-1)$ により定義された B -1 次写像 $k: A \rightarrow B$ に対し、 $k(x) = t_q(ux) = b_t^u(1, x) \ (x \in A)$ を満たす A の可逆元 u が存在する。よって $(A, b_t^u) = B \perp (Ba \oplus \dots \oplus Ba^{n-1})$ は非退化であり、従って $(Ba \oplus Ba^2 \oplus \dots \oplus Ba^{n-1})$ も非退化となる。 $Ba \oplus Ba^2 \oplus \dots \oplus Ba^{n-1}$ が metabolic B -左加群であることを示す爲に $r = \frac{n-1}{2}$, $N = Ba \oplus \dots \oplus Ba^r$ と置く。補題 1 より $N^\perp \subset N$ を示せば十分である。その爲には $N^\perp \cap (Ba^{r+1} \oplus \dots \oplus Ba^{n-1}) = 0$ が示されれば良い。今 $N^\perp \cap (Ba^{r+1} \oplus \dots \oplus Ba^{n-1})$ の元 $c = b_1 a^{r+1} + \dots + b_r a^{n-1} \neq 0$ が存在すると仮定する。 $b_1 = b_2 = \dots = b_{k-1} = 0, b_k \neq 0$ となる k がある。 $F(X) = X^n + d_1 X^{n-1}$

$+ \dots + d_n$ を a の $B[X]$ に於ける最小多項式、 $L(X) = -(X^{n-r-k} + d_1 X^{n-r-k-1} + \dots + d_{r-k} X)$, $H(X) = d_{r-k+1} X^{r+k} + \dots + d_n$ と置く。このとき、 $F(X) = -L(X)X^{r+k} + H(X)$, $L(a)a^{r+k} = H(a)$ であり、 $L(a) = -(d_{r-k}a + \dots + d_1 a^{n-r-k-1} + a^{n-r-k}) \in N$ である。 $c \in N^\perp$ より

$$\begin{aligned} 0 &= b_t^u(c, L(a)) = h(c \cdot L(a)) \\ &= h((b_k + b_{k+1}a + \dots + b_r a^{n-r-k-1}) a^{r+k} L(a)) \\ &= h((b_k + b_{k+1}a + \dots + b_r a^{n-r-k-1}) H(a)) \\ &= h((b_k + b_{k+1}a + \dots + b_r a^{n-r-k-1})(d_{r-k+1} a^{r+k} + \dots + d_n)) \\ &= b_k d_n. \end{aligned}$$

よって、 $b_k = 0$ となり仮定に反する。即ち $Ba \oplus \dots \oplus Ba^{n-1}$ は metabolic B -部分加群で、 $(A, b_t^u) = \langle 1 \rangle_B \perp (Ba \oplus \dots \oplus Ba^{n-1})$, $A \supset B$ は奇数型である。

補題3. A, B を半局所環、 $A \supset B$ は自明でない involution をもつ G -ガロア拡大、 $|G| = \text{奇数}$ と仮定する。このとき、 A の involution は B の上に自明でない involution をひき起こす。

証明 $A_0 = \{a \in A; \bar{a} = a\}$ と置く。 A の involution が B の上で自明であると仮定すれば、 $A_0 \supset B$ である。 A の involution 及び A の恒等字像からなる群を H で表わすとき、 $A_0 = A^H$ である。 $A \supset A_0$ は H -ガロア拡大である事が次の様に示される。
 $e_1, e_2, \dots, e_m$ を A のすべての原始中等元、 $\bar{e}_{2i-1} = e_{2i}$, $i = 1, 2, \dots, r$, $\bar{e}_j = e_j$, $j = 2r+1, \dots, m$ とする。 $e'_i = e_{2i-1} + e_{2i}$ ($i = 1, 2, \dots, r$), e_j ($j = 2r+1, \dots, m$) は A_0 に属する互に直交する中等元で、

$1 = \sum_{i=1}^r e_i' + \sum_{j=1}^m e_j$ を満たす。 Ae_j は $0, e_j$ 以外に中等元をもたず、 $Ae_j \supset A_0 e_j$ は分離的、 $(Ae_j)^H = A_0 e_j$ であるから、 $Ae_j \supset A_0 e_j$ ($j=2r+1, \dots, m$) は H -ガロア拡大となる。一方 Ae_i' ($i=1, 2, \dots, r$) について、 $Ae_i' = A_0 e_{2i-1} + A_0 e_{2i}$ を満たす。何故ならば、任意の $a \in Ae_i'$ に対し、 $a_0 = a e_{2i-1} + \bar{a} e_{2i}$, $a'_0 = \bar{a} e_{2i-1} + a e_{2i}$ は $A_0 = A^H$ に属し、 $a = a e_{2i-1} + a e_{2i} = a_0 e_{2i-1} + a'_0 e_{2i} \in A_0 e_{2i-1} \oplus A_0 e_{2i}$ を得る。従って、 $Ae_i' = A_0 e_{2i-1} \oplus A_0 e_{2i} \supset A_0 e_i'$ は自明な H -ガロア拡大であり、 $A = \sum_{i=1}^r Ae_i' \oplus \sum_{j=1}^m Ae_j \supset A_0 = \sum Ae_i' \oplus \sum Ae_j$ は H -ガロア拡大となる。故に $|G| = [A : B] = [A : A_0][A_0 : B] = 2 \cdot [A_0 : B]$ 。これは仮定に反する。よって B 上に自明でない involution をひき起こす。

(場合 II) に於ける定理 5 の証明。 A, B を半局所環、 $A \supset B$ を自明でない involution をもつ G -ガロア拡大、 $|G| = \text{奇数}$ 、 B の各極大イデアル m に対し $|B/m| \geq |G|^2$ 、 $\bar{m} = m$ ならば A の involution は A/mA 上自明でない involution をひき起こすと仮定する。 $A_0 = \{a \in A; \bar{a} = a\}$, $B_0 = A_0 \cap B$, H を involution と恒等写像とからなる群とする。 $B \supset B_0$ について、 B の極大イデアル m に対し、もし $\bar{m} \neq m$ ならば $b - \bar{b} \notin m$ を満たす $b \in B$ が、又 $\bar{m} = m$ ならば仮定より又その様な b が存在するから、 [2], Th. 1.3 より $B \supset B_0$ は H -ガロア拡大となることが得られる。今 $x_1, x_2, \dots, x_n, y_1, \dots, y_n$ を B の H -ガロアシステムとする

とき A の任意の元 a は、 $a = \sum_i t_H(ax_i)y_i$ と表わされる。従って、 $A_0 \otimes_{B_0} B \rightarrow A; a_0 \otimes b \mapsto a_0 b$ は全写、 $\sum a_i \otimes b_i \in A_0 \otimes_{B_0} B$ に対し、 $\sum a_i b_i = 0$ ならば、 $\sum a_i \otimes b_i = \sum a_i \otimes t_H(b_i x_j) y_j = \sum t_H(a_i b_i x_j) \otimes y_j = 0$ よって、 $A_0 \otimes_{B_0} B \cong A$ を得る。 B_0 も又半局所環になるから、 B は B_0 -基底 $\{1, v\}$ をもち、これは A の A_0 -基底でもある。 $A_0 \supset B_0$ が G -ガロア拡大となることは次の様に見られる。明らかに $A_0^G = B_0$ 、 A_0 の極大イデアル $\mathfrak{p}_0$ に対し、 $\mathfrak{p} \supset A\mathfrak{p}_0$ なる A の極大イデアル $\mathfrak{p}$ を取る事が出来る。 $A \supset B$ は G -ガロア拡大であるから、各 $\sigma (\neq I) \in G$ に対し、 $a - \sigma(a) \notin \mathfrak{p}$ をみたす $a \in A$ が存在し、 $a = a_0 + a_1 v$, $a_0, a_1 \in A_0$ と表わされる。従って、 $a - \sigma(a) = (a_0 - \sigma(a_0)) + (a_1 - \sigma(a_1))v \notin \mathfrak{p}$ であり、 $a_0 - \sigma(a_0) \notin \mathfrak{p}_0$ 、又は $a_1 - \sigma(a_1) \notin \mathfrak{p}_0$ を得る。[2], Th. 1.3 より $A_0 \supset B_0$ は G -ガロア拡大となる。 B_0 の任意の極大イデアル m_0 に対し、 $m \cap A_0 = m_0$ を満たす A の極大イデアル m を取れば、 $[B/m : B_0/m_0] \leq 2$, $|B/m| \geq \sqrt{|B_0/m_0|} \geq |G|$ を得る。自明な involution をもつ G -ガロア拡大 $A_0 \supset B_0$ に (場合 I) を適用して、 $A_0 \supset B_0$ は奇数型になる。従って、次の補題を用いれば、 $A \supset B$ が奇数型である事を得る。

補題 4. A, B を可換環、 $A \supset B$ は自明でない involution をもつ G -ガロア拡大とする。 $A_0 = \{a \in A; \bar{a} = a\}$, $B_0 = A_0 \cap B$ と置く。もし $A_0 \supset B_0$ が G -ガロア拡大ならば $A \cong A_0 \otimes_{B_0} B$ であ

り、 $A_0 \supset B_0$ が奇数型ならば、 $A \supset B$ も奇数型である。

証明. $x_1, \dots, x_n, y_1, \dots, y_n$ を A_0 の G -ガロアシステムとするとき、 $A_0 \otimes_{B_0} B \rightarrow A; a_0 \otimes b \mapsto a_0 b$ が同型写像であることは、 $a \in A$ に対し、 $a = \sum x_i t_{g_i}(y_i a) \in A_0 B$, $\sum a_i b_i = 0$ ($a_i \in A_0, b_i \in B$) ならば $\sum a_i \otimes b_i = \sum x_j t_{g_j}(y_j a_i) \otimes b_i = \sum x_j \otimes t_{g_j}(y_j a_i b_i) = 0$ より得る。もし $A_0 \supset B_0$ が奇数型ならば、 A_0 の可逆元 u と、metabolic B_0 -加群 h_m が存在して、 $(A_0, b_i^u) \cong \langle 1 \rangle_{B_0} \perp h_m$ となる。 $i: B_0 \hookrightarrow B$ に対し、 $i^*(b_i^u) = (B \otimes_{B_0} A_0, i b_i^u) \cong (A, b_i^u) \cong \langle 1 \rangle_B \perp i^*(h_m)$, $i^*(h_m)$ は又 metabolic B -加群になるから、 $A \supset B$ は奇数型である。

(場合Ⅲ) に於ける定理5の証明. B を極大イデアル m をもつ局所環、 $A \supset B$ は自明でない involution をもつ G -ガロア拡大、 A/mA 上に自明な involution をひき起こすとする。更に $|G| = \text{奇数}$, $|B/m| \geq |G|$ で、 B/m は標数 $\neq 2$ の体か又は有限体と仮定する。補題2より $A = B \oplus B\alpha \oplus \dots \oplus B\alpha^{n-1}$, $\{1, \alpha, \dots, \alpha^{n-1}\}$ は A の B -基底、となる $\alpha \in A$ が存在する。もし B/m が標数 $\neq 2$ の体ならば、2 は B で可逆的、 α の代りに $\frac{\alpha + \bar{\alpha}}{2} = \alpha'$ を取る事が出来、 $\alpha' \equiv \alpha \pmod{mA}$, $\bar{\alpha}' = \alpha'$ を満たす。もし B/m が標数2の有限体ならば、 A/mA は標数2の有限体の直和であり、 $A/mA \rightarrow A/mA; [x] \mapsto [x^2]$ は自己同型写像となり、 $c^2 \equiv \alpha \pmod{mA}$ を満たす $c \in A$ を選ぶ事が出来る。 α の代りに $\alpha' = c \cdot \bar{c}$ を取

るならば、 $a' \equiv a \pmod{mA}$, $\bar{a}' = a'$ が満たされる。以上の理由から、 $A = B \oplus Ba' \oplus \dots \oplus Ba'^{n-1}$, $\{1, a', \dots, a'^{n-1}\}$ は A の B -基底、 $\bar{a}' = a'$ となる A の元 a' を選ぶ事が出来る。従って、 B -1次写像 $h: A \rightarrow B$; $h(1) = 0$, $h(a'^i) = 0$, $i=1, \dots, n-1$, は $\overline{h(x)} = h(\bar{x})$ ($\forall x \in A$) を満たし、 $h(x) = b'_t(x, u) = t_G(x\bar{u})$ ($x \in A$) により定まる A の可逆元 u は、 $b'_t(x, u) = h(x) = \overline{h(\bar{x})} = \overline{t_G(\bar{x}\bar{u})} = t_G(xu) = b'_t(x, \bar{u})$, ($\forall x \in A$) を満たす。従って、 $\bar{u} = u$ であり、 $u \in U_c(A)$ を得る。(場合 I) に於ける証明と全く同様にして、 (A, b'_t) は $\langle 1 \rangle_B$ と metabolic B -左加群の直交和に isometric になり、 $A \supset B$ は奇数型となる。

3. involution をもつ G -ガロア拡大の例

例1. 可換環 B 上の非退化 quadratic B -加群 (V, q) を考える。 (V, q) は直交基底 $v_1, v_2, \dots, v_n$ をもつと仮定する。即ち、 $(V, q) = Bv_1 \perp \dots \perp Bv_n$, 従って、2 及び $q(v_i)$ は B で可逆的である。 P_{v_i} を $P_{v_i}(x) = x - \frac{B_q(x, v_i)}{q(v_i)} v_i$, ($x \in V$) によって定義された Symmetry とする ($i=1, 2, \dots, n$)。 (V, q) の Clifford 多元環を $C(V, q) = C_0(V, q) \oplus C_1(V, q)$ とする。 $C(V, q)$ は $\mathbb{Z}/2$ -次数加群であり $C_0(V, q)$ は 0 次の同次部分、 $C_1(V, q)$ は 1 次の同次部分を表わす。 P_{v_i} は $C(V, q)$ の多元環-自己同型写像 $\hat{P}_i$ に拡張される。 $C(V, q)$ は $\overline{x_1 x_2 \dots x_r} = x_r x_{r-1} \dots x_2 x_1$ ($x_i \in V$) によって定義された involution をもち、 $\hat{P}_i(\bar{y}) = \overline{\hat{P}_i(y)}$, $y \in C(V, q)$ を満たす。 G

を $\hat{p}_1, \hat{p}_2, \dots, \hat{p}_n$ で生成された $C(V, \varphi)$ の自己同型写像からなる群とし、 $A = C(V, \varphi)$ と置く。

定理6. $A = C(V, \varphi)$, B, G を上述のようにする。このとき、 $A \supset B$ は、involution をもつ G -ガロア拡大となり、 $G \cong (\hat{p}_1) \times \dots \times (\hat{p}_n)$ である。

証明. $(V, \varphi) = Bu_1 \perp Bu_2 \perp \dots \perp Bu_n$ に対し、 $A = C(V, \varphi) \supset B$ が G -ガロア拡大であること、及び $G \cong (\hat{p}_1) \times \dots \times (\hat{p}_n)$ であることは n に関する帰納法で示される。 $n=1$ に対して、 $C(Bu_1, \varphi) \cong B[X]/(X^2 - \varphi(u_1))$ は B の分離的2次拡大であり、 $C(Bu_1, \varphi)^{(\hat{p}_1)} = B$ により、 $C(Bu_1, \varphi) \supset B$ は、 $(\hat{p}_1)$ -ガロア拡大となる。 $V_{n-1} = Bu_1 \perp \dots \perp Bu_{n-1}$ に対し、 $C(V_{n-1}, \varphi) \supset B$ は G_{n-1} -ガロア拡大、 $G_{n-1} \cong (\hat{p}_1) \times \dots \times (\hat{p}_{n-1})$ と仮定する。 $V = V_{n-1} \perp Bu_n$ より、 $C(V, \varphi) \cong C(V_{n-1}, \varphi) \hat{\otimes}_B C(Bu_n, \varphi)$ となり、仮定より、 $C(V_{n-1}, \varphi)$ の G_{n-1} -ガロアシステム $x_1, x_2, \dots, x_s, y_1, y_2, \dots, y_s$ 及び $C(Bu_n, \varphi)$ の $(\hat{p}_n)$ -ガロアシステム $u_1, u_2, \dots, u_t, w_1, w_2, \dots, w_t$ が存在する。このとき、 x_i, y_i, u_j, w_j は同次部分から取ることが出来る。 $\{(-1)^{\partial y_i \partial u_j} x_i \otimes u_j, y_i \otimes w_j; 1 \leq i \leq s, 1 \leq j \leq t\}$ は $C(V, \varphi) = C(V_{n-1}, \varphi) \hat{\otimes} C(Bu_n, \varphi)$ の $G = G_{n-1} \otimes (\hat{p}_n)$ -ガロアシステムとなる。又 $C(V, \varphi)^G = C(V_{n-1}, \varphi)^{G_{n-1}} \otimes C(Bu_n, \varphi)^{(\hat{p}_n)} = B$ より、 $C(V, \varphi) \supset B$ は G -ガロア拡大、 $G \cong (\hat{p}_1) \times \dots \times (\hat{p}_n)$ を得る。先に述べた事より、 $A \supset B$ は involution をもつ G -ガロア拡大である事

が知られる。

例2. $A \supset B$ を involution をもつ G -ガロア拡大とする。 A 上の n 次の完全行列環を A_n で表わし、 G の元は成分に作用させる事により、 A_n の自己同型写像に拡張され、その群を再び G で表わす事とする。 $A_n \rightarrow A_n ; (a_{ij}) \mapsto {}^t(\bar{a}_{ij})$ によって A の involution は A_n の involution に拡張される (${}^t(\bar{a}_{ij})$ は (a_{ij}) の転置行列を表わす)。このとき、 $A_n \supset B_n$ は又 involution をもつ G -ガロア拡大となる。 $A \supset B$ が奇数型ならば、 $A_n \supset B_n$ も又奇数型になる事が次のように示される。もし $u \in U_c(A)$ に対し $(A, b_t^u) \cong \langle 1 \rangle_B \perp h_m$, (h_m : metabolic B -左加群) ならば $u \in U_c(A) \subset U_c(A_n)$ であり、 $(A_n, b_t^u) = (B_n \otimes_B A, i b_t^u) \cong \langle 1 \rangle_{B_n} \perp i^*(h_m)$, $i^*(h_m)$ は又 metabolic B_n -左加群となる。但し、 $i: B \hookrightarrow B_n$ によって、 $A_n \supset B_n$ は又奇数型である。

例3. $A \supset B$ を involution をもつ G -ガロア拡大とする。自明な因子団をもつ接合積 $\Delta(A, G) = \sum_{\sigma \in G} A u_\sigma$ を考え、 u_1 はその単位元と仮定する事が出来る。 M を忠実な $\Delta(A, G)$ -左加群で $[u_\sigma(m), u_\tau(n)] = \sigma([m, n])$, ($m, n \in M, \sigma \in G$) を満たす非退化エルミット形式 $[,]: M \times M \rightarrow A$ をもつと仮定する。 $M^G = \{m \in M; u_\sigma m = m, \forall \sigma \in G\}$ は B -左部分加群をなし、 $[,]|_{M^G \times M^G}$ は、 M^G から B への非退化エルミット形式をひき起こす。更に $M = A M^G \cong A \otimes_B M^G$ が満たされる。もし M^G が有限生成射影的 B -加群、

かつ、 B -generator ならば、 $\Lambda = \text{Hom}_A(M, M)$, $\Gamma = \text{Hom}_{A(A, G)}(M, M)$ について、(Λ 及び Γ の元は M の元に右側から作用させる事とする), $[m, n\lambda] = [m\bar{\lambda}, n]$ ($\forall m, n \in M, \lambda \in \Lambda$) によって与えられる involution $\Lambda \rightarrow \Lambda: \lambda \mapsto \bar{\lambda}$ をもち、 G の元 σ に対し、

$$m\sigma'(\lambda) = u_\sigma((u_\sigma^{-1}m)\lambda) \quad (m \in M, \lambda \in \Lambda) \text{ によって定義される}$$

自己同型写像 $\sigma': \Lambda \rightarrow \Lambda$ が定まり、かゝる σ' の全体 G' に対して、 $\Lambda \supset \Gamma$ は involution をもち G' -ガロア拡大となる。このとき、 $G \rightarrow G'; \sigma \mapsto \sigma'$ は同型写像である。(証明は [3] を参照)

以上に於て述べたエルミット加群についての基本概念は [1] による。内容は、[3], [4] の解説である。

参考文献

- [1] H.Bass : Unitary K-theory, Springer lecture notes 343 (1973).
- [2] S.U.Chase, D.K.Harrison and A.Rosenberg : Galois theory and Galois cohomology of commutative rings, Mem. Amer. Math. Soc. No. 52 (1965).
- [3] T.Kanzaki : On Galois extension with involution of rings,
- [4] T.Kanzaki and K.Kitamura : On odd type Galois extension with involution of semi-local rings, Proc. Japan Acad. 51 (1975) 117-122.
- [5] T.Y.Lam : The algebraic theory of quadratic forms, Benjamin (1973).
- [6] A.Rosenberg and R.Ware : The zero-dimensional Galois cohomology of Witt ring, Invention math. 11 (1970), 65-72.
- [7] M.Knebusch, A.Rosenberg and R.Ware : Signatures on semi-local rings, J.

Algebra 26 (1973), 208-250.

[8] T.A.Springer : Sur les formes d'indices zero, C. R. Acad. Sci. 234 (1952)
1517-1519.