Kanzaki, T.
Osaka J. Math.
12 (1975), 691–702

ON GALOIS EXTENSION WITH INVOLUTION OF RINGS

Dedicated to Professor Kiiti Morita on his 60th birthday

TERUO KANZAKI

(Received December 3, 1974)

1. Introduction

For a Galois extension field L of a field K with Galois gruop G, A. Rosenberg and R. Ware [9] proved that if $[L:K]$ is odd then the Witt ring $W(K)$ is isomorphic to $W(L)^G$. The proof was simplified by M. Knebusch and W. Scharlau [5], and the theorem was generalized by M. knebusch, A. Rosenberg and R. Ware [6] to the case of commutative semilocal rings. In this note, concerning with sesqui-linear forms over a non commutative ring defined in [2], we want to extend the theorem to a case of non commutative rings. In §2 and §3, we difine a *Galois extension with involution* of a ring and an *odd type Galois extension with involution.* From the theorem of Scharlau (cf. [11], [7]), we know that for a Galois extension with involution $L\supset K$ of fields, $L\supset K$ is an odd type Galois extension with involution if and olnly if $[L:K]$ is odd. If $A\supset B$ is a G-Galois extension with involution of rings, then we can prove the isomorphism $i^*\circ t_{G*}(q)=\sum_{\sigma\in G}\perp\sigma^*(q)$ for any sesqui-linear left A-module $q=(M, q)$. This isomorphism is a generalization of the case of fields [4], semilocal rings [6]. If A is an algebra over a commutative ring R, and if $A\supset R$ is an odd type G-Galois extension with involution, then it is obtained that the inclusion map i: $R\to A$ induces a group monomorphism i^*: $W(R)\to W(A)$ of Witt groups of hermitian left modules, and its image is $T_{G*}(W(A))$. Throughout this paper, we assume that every ring has identity element and module is unitary. Furthermore, ring homomorphisms are assumed to correspond identity element to identity element.

2. Sesqui-linear forms

DEFINITION 1. Let A be a ring with involution $A\to A$; $a\rightsquigarrow\bar{a}$, i.e. $\overline{a+b}=\bar{a}+\bar{b}$, $\overline{ab}=\bar{b}\,\bar{a}$ and $\bar{\bar{a}}=a$ for every a, b in A. For a subring B and a finite group G of ring-automorphisms of A, $A\supset B$ is called a *G-Galois extension with involution* if every element in G is compatible with the involution, i.e. $\overline{\sigma(a)}=\sigma(\bar{a})$ for all $a\in A$, $\sigma\in G$, and if $A\supset B$ a G-Galois extension, i.e. $A^G=B$ and there exist elements $x_1, x_2, \cdots x_n$ and $y_1, y_2, \cdots y_n$ in A, called a G-Galois system, such that $\sum x_i y_i = 1$ and $\sum x_i \sigma(y_i) = 0$ for $\sigma \neq I$ in G.

DEFINITION 2. (cf. [2]) Let A be a ring with involution, and M a left A-module. A form q: $M \times M \to A$ is called a sesqui-linear form if it satisfies

$$q(a(m+m'), n) = aq(m, n) + aq(m', n) \quad \text{and}$$
$$q(m, b(n+n')) = q(m, n)\bar{b} + q(m, n')\bar{b}$$

for every $a, b \in A$ and $m, m', n, n' \in M$.

DEFINITION 3. Let $A \supset B$ be a G-Galois extension with involution, C the center of A and C_0 the fixed subring of C by the involution, i.e. $C_0 = \{c \in C; c = \bar{c}\}$. For any $u \in C_0$ let us denote by t_G^u: $A \to B$ a B-linear map defined by $t_G^u(a) = \sum_{\sigma \in G} \sigma(ua)$ for $a \in A$, particularly, when $u=1$, it is denoted by t_G. For a sesqui-linear left A-module $q=(M, q)$, a sesqui-linear left B-module $t_{G*}^u(q) = ({}_B M, t_G^u q)$ and a sesqui-linear left A-module $\sigma^*(q) = ({}_\sigma M, \sigma q)$, for $\sigma \in G$, are defined as follows;

$$t_G^u q\colon M \times M \to B;\ (m, m') \rightsquigarrow t_G^u(q(m, m')), \quad \text{and}$$
$$\sigma q\colon {}_\sigma M \times {}_\sigma M \to A;\ (m, m') \rightsquigarrow \sigma(q(m, m')),$$

where ${}_\sigma M$ is a left A-module defined by a new operation $*$; $a * m = \sigma^{-1}(a)m$, for $a \in A$, $m \in M$. For a sesqui-linear left B-module $h=(N, h)$ and the inclusion map i: $B \to A$, a sesqui-linear left A-module $i^*(h) = (A \otimes_B N, ih)$ is defined by ih: $(A \otimes_B N) \times (A \otimes_B N) \to A$; $ih(a \otimes n, a' \otimes n') = ah(n, n')\bar{a}'$ for $a \otimes n, a' \otimes n' \in A \otimes_B N$.

Lemma 1. *Let $A \supset B$ be a G-Galois extension with invoultion. For any left B-module N there is an A-isomorphism Φ: $A \otimes_B \mathrm{Hom}_B(N, B) \to \mathrm{Hom}_A(A \otimes_B N, A)$ defined by $\Phi(a \otimes f)(a' \otimes n) = a' f(n) \bar{a}$ for $a \otimes f \in A \otimes_B \mathrm{Hom}_B(N, B)$ and $a' \otimes n \in A \otimes_B N$, where the operations by A and B are as follows: $(bf)(x) = f(x)\bar{b}$, for $f \in \mathrm{Hom}_B(N, B)$, $b \in B$, $x \in N$, and $(ag)(y) = g(y)\bar{a}$ for $g \in \mathrm{Hom}_A(A \otimes N, A)$, $a \in A$, $y \in A \otimes_B N$.*

Proof. If $\sum a_i \otimes f_i$ is in Ker Φ, then $\sum f_i(n)\bar{a}_i = \Phi(\sum a_i \otimes f_i)(1 \otimes n) = 0$ for all n in N. Let $x_1, x_2, \cdots x_n$ and $y_1, y_2, \cdots y_n$ be a G-Galois system of A. Then we have $\sum a_i \otimes f_i = \sum_{i,j} x_j t_G(y_j a_i) \otimes f_i = \sum_{i,j} x_j \otimes t_G(y_j a_i) f_i = 0$, since $\sum_i t_G(y_j a_i) f_i = 0$ is obtained by $(\sum_i t_G(y_j a_i) f_i)(n) = \sum_i f_i(n) \overline{t_G(y_j a_i)} = \sum_i t_G(f_i(n) \overline{y_j a_i}) = t_G(\sum_i f_i(n) \bar{a}_i \bar{y}_j) = 0$ for all $n \in N$. Hence Ker $\Phi = 0$. If g is any element in $\mathrm{Hom}_A(A \otimes_B N, A)$, we put f_i: $N \to B$; $f_i(n) = t_G(g(1 \otimes n) x_i)$ for every $n \in N$, $i = 1, 2, \cdots n$. Then f_i is in $\mathrm{Hom}_B(N, B)$ and so $\sum \bar{y}_i \otimes f_i$ is an element in $A \otimes_B \mathrm{Hom}_B(N, B)$ such that $\Phi(\sum \bar{y}_i \otimes f_i) = g$, because $\Phi(\sum \bar{y}_i \otimes f_i)(a \otimes n) = \sum a f_i(n) y_i = \sum a t_G(g(1 \otimes n) x_i) y_i = ag(1 \otimes n) = g(a \otimes n)$ for all $a \otimes n \in A \otimes_B N$.

Lemma 2. *Let $A \supset B$ be a G-Galois extension with involution. If M is a left A-module, then for any element u in the unit group $U(C_0)$ of the fixed subring C_0 of the center of A by the involution, a map*

$$\theta\colon \mathrm{Hom}_A(M, A) \to \mathrm{Hom}_B(M, B); f \rightsquigarrow t^u_G \circ f$$

is a B-isomorphism as left B-modules defined by $(bf)(m)=f(m)\bar{b}$ for $b \in B$, $m \in M$ and $f \in \mathrm{Hom}_A(M, A)$ or $\mathrm{Hom}_B(M, B)$.

Proof. If f is in $\mathrm{Hom}_A(M, A)$ and $t^u_G \circ f=0$, then for any $m \in M$ we have $uf(m)=\sum x_i t_G(y_i uf(m))=\sum x_i(t^u_G \circ f(y_i m))=0$, hence $f=0$. If g is in $\mathrm{Hom}_B(M, B)$, an A-homomorphism $f\colon M \to A$ defined by $f(m)=\sum u^{-1} x_i g(y_i m)$ for $m \in M$, satisfies $t^u_G \circ f(m)=\sum t_G(x_i g(y_i m))=\sum t_G(x_i) g(y_i m)=g(\sum t_G(x_i) y_i m)=g(m)$ for all $m \in M$, therefore $t^u_G \circ f=g$ and so θ is a B-isomorphism.

Proposition 1. *Let $A \supset B$ be a G-Galois extension with involution, and C_0 the subring of the center of A whose element is fixed by the involution.*

1) *If a sesqui-linear left B-module $h=(N, h)$ is non degenerate i.e. $\phi\colon N \to \mathrm{Hom}_B(N, B); n \rightsquigarrow h(-, n)$ and $\psi\colon N \to \mathrm{Hom}_B(N, B); n \rightsquigarrow \overline{h(n, -)}$ are B-isomorphisms, then $i^*(h)=(A \otimes_B N, ih)$ is also non degenerate, where $i\colon B \to A$ is the inclusion map.*

2) *If a sesqui-linear left A-module $q=(M, q)$ is non degenerate, then $t^u_{G*}(q)=$* $({}_B M, t^u_G q)$ and $\sigma^*(q)=({}_\sigma M, \sigma q)$ *are also non degenerate for every $u \in U(C_0)$ and $\sigma \in G$.*

Proof. 1) Let $h=(N, h)$ be a non degenerate sesqui-linear left B-module. Since $\phi\colon N \to \mathrm{Hom}_B(N, B); n \rightsquigarrow h(-, n)$ and $\Phi\colon A \otimes_B \mathrm{Hom}_B(N, B) \to \mathrm{Hom}_A(A \otimes_B N, A)$ are B-isomorphisms, the composition $\Phi \circ (I \otimes \phi)$; $A \otimes_B N \to \mathrm{Hom}_A(A \otimes_B N, A)$ is an A-isomorphism. And, it is obtained that $\Phi \circ (I \otimes \phi)(a \otimes n)= ih(-, a \otimes n)$ for $a \otimes n \in A \otimes_B N$, because $\Phi \circ (I \otimes \phi)(a \otimes n)(a' \otimes n')=\Phi(a \otimes h(-, n))(a' \otimes n')=a' h(n', n)\bar{a}=ih(a' \otimes n', a \otimes n)$ for every $a' \otimes n' \in A \otimes_B N$. For $\psi\colon N \to \mathrm{Hom}_B(N, B); n \rightsquigarrow \overline{h(n, -)}$, similarly, we obtain the isomorphism $\Phi \circ (I \otimes \psi)$; $A \otimes_B N \to \mathrm{Hom}_A(A \otimes_B N, A); a \otimes n \rightsquigarrow \overline{ih(a \otimes n, -)}$. Therefore, $i^*(h)=(A \otimes_B N, ih)$ is non degenerate. 2) Let $q=(M, q)$ be a non degenerate sesqui-linear left A-module. From the following diagram and Lemma 2, we can conclude that $t^u_{G*}(q)$ is non degenerate;

$$\begin{array}{ccc} M & \xrightarrow{\ \phi,\ (\psi)\ } & \mathrm{Hom}_A(M, A) \\ \downarrow{\scriptstyle \phi',\ (\psi')} & \circlearrowright & \swarrow{\scriptstyle \theta} \\ \mathrm{Hom}_B(M, B) & & \end{array}$$

where $\phi', (\psi'),\colon M \to \mathrm{Hom}_B(M, B); m \rightsquigarrow t^u_G q(-, m)$, $(m \rightsquigarrow \overline{t^u_G q(m, -)})$. $\sigma^*(q)$ is obviously non degenerate.

Theorem 1. *Let $A\supset B$ be a G-Galois extension with involution. For any sesqui-linear left A-module $q=(M, q)$, we have an isometry*

$$i^*\circ t_{G*}(q)\cong\sum_{\sigma\in G}\perp\sigma^*(q)\,.$$

Proof. Let $x_1, x_2, \cdots x_n$ and $y_1, y_2, \cdots y_n$ be a G-Galiois system of A. For each $\sigma\in G$, we can define an A-homomorphism $e_\sigma\colon A\otimes_B M\to A\otimes_B M$; $a\otimes m\rightsquigarrow \sum a\sigma(x_i)\otimes y_i m$. Because, for any $c\in A$, we have $e_\sigma(ac\otimes m)=\sum_i ac\sigma(x_i)\otimes y_i m=\sum_{i,j}a\sigma(x_j t_G(y_j\sigma^{-1}(c)x_i))\otimes y_i m=\sum_{i,j}a\sigma(x_j)\otimes t_G(y\sigma^{-1}(c)x_i)y_i m=\sum_j a\sigma(x_j)\otimes y_j \sigma^{-1}(c)m=e_\sigma(a\otimes\sigma^{-1}(c)m)$, particularly, if c is in B, we obtain $e_\sigma(ac\otimes m)=e_\sigma(a\otimes cm)$, therefore e_σ is well defined. Since $e_\sigma(a\otimes m)=e_\sigma(1\otimes\sigma^{-1}(a)m)$ for $a\otimes m\in A\otimes_B M$, the image of e_σ is equal to $e_\sigma(1\otimes M)$. Now, we check identities $e_\sigma\circ e_\tau=\begin{cases}e_\sigma, & \text{for } \sigma=\tau\\ 0, & \text{for } \sigma\neq\tau\end{cases}$, $(\sigma, \tau\in G)$, and $\sum_{\sigma\in G}e_\sigma=I$. For any $a\otimes m\in A\otimes_B M$, we have $e_\sigma\circ e_\tau(a\otimes m)=\sum_i e_\sigma(a\tau(x_i)\otimes y_i m)=\sum_i e_\sigma(a\otimes\sigma^{-1}\tau(x_i)y_i m)=\begin{cases}e_\sigma(a\otimes m), & \text{for } \sigma=\tau\\ 0, & \text{for } \sigma\neq\tau\end{cases}$, and $\sum_{\sigma\in G}e_\sigma(a\otimes m)=\sum_{i,\sigma\in G}a\sigma(x_i)\otimes y_i m=\sum_i at_G(x_i)\otimes y_i m=a\otimes\sum t_G(x_i)y_i m=a\otimes m$. Accordingly, $A\otimes_B M=\sum_{\sigma\in G}\oplus e_\sigma(1\otimes M)$ is obtained. Further, $e_\sigma(1\otimes M)$ and ${}_\sigma M$ are A-isomorphic by an A-homomorphism $\zeta_\sigma\colon {}_\sigma M\to e_\sigma(1\otimes M)$; $m\rightsquigarrow e_\sigma(1\otimes m)$. Because, $\zeta_\sigma(a*m)=\zeta_\sigma(\sigma^{-1}(a)m)=e_\sigma(1\otimes\sigma^{-1}(a)m)=e_\sigma(a\otimes m)=ae_\sigma(1\otimes m)=a\zeta_\sigma(m)$, and if $\zeta_\sigma(m)=e_\sigma(1\otimes m)=\sum_i\sigma(x_i)\otimes y_i m=0$ then by a canonical homomrphism $A\otimes_B M\to M$; $a\otimes m\rightsquigarrow\sigma^{-1}(a)m$, $\zeta_\sigma(m)=0$ is sent to $m=\sum_i x_i y_i m=0$. Thus, $A\otimes_B M=\sum_{\sigma\in G}\oplus e_\sigma(1\otimes M)\cong\sum_{\sigma\in G}\oplus{}_\sigma M$ as left A-modules. Now, we shall show that the subspaces $\{e_\sigma(1\otimes M);\ \sigma\in G\}$ of $i^*t_{G*}(q)=(A\otimes_B M, it_G q)$ are orthogonal each other and $e_\sigma(1\otimes_B M)$ is isometric to $\sigma^*(q)=({}_\sigma M, \sigma q)$ for each $\sigma\in G$. For $m, n\in M$ and $\sigma, \tau\in G$, we have $it_G q(e_\sigma(1\otimes m), e_\tau(1\otimes n))=it_G q(\sum_i\sigma(x_i)\otimes y_i m, \sum_j\tau(x_j)\otimes y_j n)=\sum_{i,j}\sigma(x_i)t_G q(y_i m, y_j n)\tau(x_j)=\sum_{i,j,\gamma\in G}\sigma(x_i)\gamma(q(y_i m, y_j m))\overline{\tau(x_j)}=\sum_{\gamma\in G}\sigma(\sum_i x_i\sigma^{-1}\gamma(y_i))\gamma(q(m, n))\overline{\tau(\sum_j x_j\tau^{-1}\gamma(y_j))}=\begin{cases}\sigma q(m, n) & \text{for } \sigma=\tau\\ 0 & \text{for } \sigma\neq\tau\end{cases}$. Accordingly, we obtain $(A\oplus_B M, it_G q)=\sum_{\sigma\in G}\perp e_\sigma(1\otimes M)$ and an isometry $\zeta_\sigma\colon({}_\sigma M, \sigma q)\to(e_\sigma(1\otimes M), it_G q)$; $m\rightsquigarrow e_\sigma(1\otimes m)$ for each $\sigma\in G$, hence $i^*\circ t_{G*}(q)\cong\sum_{\sigma\in G}\perp\sigma^*(q)$.

3. Witt groups

Let A be a ring with involution.

DEFINITION 4. (cf. [2]) A sesqui-linear left A-module $q=(M, q)$ is called hermitian, if $q(m, n)=\overline{q(n, m)}$ is satisfied for every $m, n\in M$. And, a hermitian left A-module (M, q) is called metabolic, if there exists a hermitian left A-module $(V\oplus V^*, h_g)$ defined by $h_g(v+f, v'+f')=\overline{f(v')}+f'(v)+g(v, v')$, $v, v'\in V, f, f'\in V^*=\mathrm{Hom}_A(V, A)$ for some hermitian left A-module (V, g), and if (M, q) is isometric to $(V\oplus V^*, h_g)$. We shall call that a hermitian left A-module (M, q) is reflexive, (finitely generated projecctive), if M is reflexive i.e. the map $\xi\colon M\to \mathrm{Hom}_A(\mathrm{Hom}_A(M, A), A)$; $\xi(m)(f)=\overline{f(m)}$, $f\in \mathrm{Hom}_A(M, A)$, $m\in M$, is an A-isomorphism, (M is finitely generated projecteve).

Let $\mathfrak{H}_r(A)$, ($\mathfrak{H}_p(A)$), denote the category of non degenerate and reflexive, (finitely generated projective), hermitian left A-modules and their isometries, and $\mathfrak{M}_r(A)$, ($\mathfrak{M}_p(A)$), the subcategory of $\mathfrak{H}_r(A)$, ($\mathfrak{H}_p(A)$), consiting of metabolic left A-modules.[1] Since $\mathfrak{H}_r(A)$ and $\mathfrak{M}_r(A)$, ($\mathfrak{H}_p(A)$ and $\mathfrak{M}_p(A)$), have the product $\perp$, we can construct the Witt-Grothendieck group $GW_r(A)$, ($GW_p(A)$), and the Witt group $W_r(A)$, ($W_p(A)$). We can check that from the inclusion map $i\colon B\to A$, the trace map $t_G^u\colon A\to B$ and σ in G,

$$i^*\colon W_r(B)\to W_r(A),\ (W_p(B)\to W_p(A))\,,$$
$$t_{G*}^u\colon W_r(A)\to W_r(B),\ (W_p(A)\to W_p(B))\,, \quad \text{and}$$
$$\sigma^*\colon W_r(A)\to W_r(A),\ (W_p(A)\to W_p(A))\,,$$

are induced, where $u\in U(C_0)$ and $A\supset B$ is a G-Galois extension with involution.

Lemma 3. *Let $A\supset B$ be a G-Galois extension with involution. If M is a reflexive left B-module, then $A\otimes_B M$ is also a reflexive A-module.*

Proof. If $\xi\colon M\to \mathrm{Hom}_B(\mathrm{Hom}_B(M, B), B)$; $m \rightsquigarrow (f\rightsquigarrow \overline{f(m)})$ is a B-isomorphism, $I\otimes\xi\colon A\otimes_B M\to A\otimes_B \mathrm{Hom}_B(\mathrm{Hom}_B(M, B), B)$ is an A-isomorphism. Since $\Phi\colon A\otimes_B \mathrm{Hom}_B(M, B)\to \mathrm{Hom}_A(A\otimes_B M, A)$; $a\otimes f\rightsquigarrow (a'\otimes m\rightsquigarrow a'f(m)\bar{a})$ is an A-isomorphism, the composition $\Phi'=\mathrm{Hom}(\Phi^{-1}, I)\circ\Phi\colon A\otimes_B \mathrm{Hom}_B(\mathrm{Hom}_B(M, B), B)\to \mathrm{Hom}_A(\mathrm{Hom}_A(M, A), A)$ is also an A-isomorphism, and so is $\Phi'\circ(I\otimes\xi)\colon A\otimes_B M\to \mathrm{Hom}_A(\mathrm{Hom}_A(A\otimes_B M, A), A)$. We can check $\Phi'\circ(I\otimes\xi)(a\otimes m)(f)=\overline{f(a\otimes m)}$ for $f\in \mathrm{Hom}_A(A\otimes_B M, A)$ and $a\otimes m\in A\otimes_B M$; For $f\in \mathrm{Hom}_A(A\otimes_B M, A)$, we put $\Phi^{-1}(f)=\sum b_i\otimes g_i$ in $A\otimes_B \mathrm{Hom}_B(M, B)$, then we have $\Phi'\circ(I\otimes\xi)(a\otimes m)(f)=\Phi(a\otimes\xi(m))(f)=\mathrm{Hom}(\Phi^{-1}, I)\circ(a\otimes\xi(m))(f)=\Phi(a\otimes\xi(m))(\Phi^{-1}(f))=\Phi(a\otimes\xi(m))(\sum b_i\otimes g_i)=\sum b_i\xi(m)(g_i)\bar{a}=\sum b_i g_i(m)\bar{a}=\overline{\sum a g_i(m)\bar{b}_i}=\overline{f(a\otimes m)}$. Thus, $A\otimes_B M$ is reflexive over A.

Lemma 4. *Let $A\supset B$ be a G-Galois extension with involution. If M is a reflexive left A-module, then M is also reflexive over B.*

Proof. Since by Lemma 2, $\theta\colon \mathrm{Hom}_A(M, A)\to \mathrm{Hom}_B(M, B)$; $f\rightsquigarrow t_G\circ f$ is a B-isomorphism, the lemma is obtained from the following commutative diagram;

1) In order that $\mathfrak{H}_r(A)$ becomes a set, we need to do an restriction on the cadinal number of module, for example, $\mathfrak{H}_r(A)\subset\{(M, q);\ \text{cardinal number of } M\leqq\aleph\}$.

$$\begin{array}{ccl} M & \xrightarrow{\ \xi_A\ } & \mathrm{Hom}_A(\mathrm{Hom}_A(M, A), A) \\ & \searrow^{\curvearrowright} & \quad \downarrow \theta \\ & & \mathrm{Hom}_B(\mathrm{Hom}_A(M, A), B) \\ & \xi_B \searrow & \quad \downarrow \mathrm{Hom}(\theta^{-1}, I) \\ & & \mathrm{Hom}_B(\mathrm{Hom}_B(M, B), B)\,. \end{array}$$

The commutativity is as follows; for any $m \in M$ and $f \in \mathrm{Hom}_B(M, B)$, setting $g=\theta^{-1}(f)$ in $\mathrm{Hom}_A(M, A)$, we have $\mathrm{Hom}(\theta^{-1}, I)\circ\theta\circ\xi_A(m)\,(f)=\mathrm{Hom}(\theta^{-1}, I)$ $(t_G\circ\xi_A(m))\,(f)=t_G\circ\xi_A(m)\;(\theta^{-1}(f))=t_G(\overline{g(m)})=\overline{t_G\circ g(m)}=\overline{f(m)}=\xi_B(m)\;(f)$.

Lemma 5. *Let $A\supset B$ be a G-Galois extension with involution, C_0 the fixed subring of the center of A by the involution, and u an element of the unit group $U(C_0)$. If $q=(M, q)$ is in $\mathfrak{M}_r(A)$, $(\mathfrak{M}_p(A))$, then $i^*(q)=(A\otimes_B M, iq)$, $t^u_{G*}(q)=({}_BM, t^u_G q)$ and $\sigma^*(q)=(M, \sigma q)$, for $\sigma\in G$, are in $\mathfrak{M}_r(A)$, $(\mathfrak{M}_p(A))$.*

Proof. This is easily obtained from Lemma 3 and Lmma 4.

Thus, group-homomorphisms of Witt groups i^*, t^u_{G*} and σ^*, for $\sigma\in G$, are well defined. From now on, we shall denote by $W(A)$ one of $W_r(A)$ and $W_p(A)$. We put $G^*=\{\sigma^*\colon W(A)\to W(A);\ \sigma\in G\}$, $T_{G^*}=\sum_{\sigma^*\in G^*}\sigma^*$ and $W(A)^{G^*}=\{[q]\in W(A);\ \sigma^*([q])=[q] \text{ for all } \sigma^*\in G^*\}$.

From Theorem 1 we have

Theorem 2. *Let $A\supset B$ be a G-Galois extension with involution. Then, we have*

$$i^*\circ t_{G*}=T_{G^*} \quad on \quad W(A)\,.$$

Let $A\supset B$ be a G-Galois extension with involution, C_0 the fixed subring of the center of A by the involution. Then easily we have

Lemma 6. *For any $u\in U(C_0)$, a sesqui-linear left B-module (A, b^u_t) defined by $b^u_t\colon A\times A\to B$; $(a, a')\rightsquigarrow t_G(au\bar{a}')$ is non degenerate and hermitian.*

DEFINITION 5. $A\supset B$ is called an *odd type G-Galois extension with involution, if there exists u in $U(C_0)$ such that $(A, b^u_t)\simeq\langle 1\rangle\perp h_m$, $\langle 1\rangle=(B, I)$*; $I(b, b')=b\bar{b}'$, for $b, b'\in B$, and h_m is a metabolic left B-module.

Proposition 2. *Let A be an algebra over a commutative ring R, and $A\supset R$ an odd type G-Galois extension with involution. We suppose that u is in the fixed subring of the center of A by the involution such that u is unit in A and $(A, b^u_t)\simeq\langle 1\rangle\perp h_m$ for a metabolic left R-module $h_m=(N, h_m)$. Then we have $t^u_{G*}\circ i^*=I$ on $W(R)$ and $\sum_{\sigma\in G}\perp\sigma^*\langle u\rangle\simeq\langle 1\rangle\perp i^*(h_m)$ as hermitian left A-modules, where $\langle u\rangle$ denotes a hermitian left A-module defined by a form $A\times A\to A$; $(x, y)\rightsquigarrow xu\bar{y}$.*

Proof. If $q=(M, q)$ is in $\mathfrak{H}_r(R)$, $(\mathfrak{H}_p(R))$, then $t^u_{G*}\circ i^*(q)=(A\otimes_R M, t^u_G iq)$ is also in $\mathfrak{H}_r(R)$, $(\mathfrak{H}_p(R))$. We can check $t^u_G iq=b^u_t\otimes q$ as follows; for any $a\otimes m$, $a'\otimes m'$ in $A\otimes_R M$, we have $t^u_G iq(a\otimes m, a'\otimes m')=t_G(uaq(m, m')\bar{a}')=t_G(ua\bar{a}')q(m, m')$ $=b^u_t(a, a')q(m, m')=b^u_t\otimes q(a\otimes m, a'\otimes m')$. Since R is commutative and A is an R-algebra, the tensor product $(A, b^u_t)\otimes(M, q)=(A\otimes_R M, b^u_t\otimes q)=(A\otimes_R M, t^u_G iq)$ is well defined in $\mathfrak{H}_r(R)$, $(\mathfrak{H}_p(R))$, and so we have $t^u_{G*}\circ i^*(q)=b^u_t\otimes q\cong(\langle 1\rangle\perp h_m)$ $\otimes q\cong(\langle 1\rangle\otimes q)\perp(h_m\otimes q)=q\perp(h_m\otimes q)$. But, by Lemma 3 and Lemma 4, if M is reflexive over R then $A\otimes_R M\cong(R\oplus N)\otimes_R M=M\oplus(N\otimes_R M)$ is also reflexive over R, and hence so is $N\otimes_R M$. Accordingly, $h_m\otimes q=(N\otimes_R M, h_m\otimes q)$ is in $\mathfrak{H}_r(R)$, $(\mathfrak{H}_p(R))$. On the other hand, $h_m\otimes q$ is also metabolic,[2] (cf. [5], Lemma 1.2 and Lemma 1.5). Therefore, we have $t^u_{G*}\circ i^*([q])=[q]$ for all $[q]$ in $W(R)$. Since we have easily $(A, b^u_t)=t_{G*}(\langle u\rangle)$ and $(A, b^u_t)\cong\langle 1\rangle\perp h_m$ as hermitian left R-modules, we obtain $i^*(b^u_t)=i^*\circ t_{G*}(\langle u\rangle)\cong\sum_{\sigma\in G}\perp\sigma^*\langle u\rangle$ by Theorem 1. Therefore $\sum_{\sigma\in G}\perp\sigma^*\langle u\rangle\cong\langle 1\rangle\perp i^*(h_m)$.

Theorem 3. *Let A be an algebra over a commutative ring R, and $A\supset R$ an odd type G-Galois extension with involution. Then we have*

1) *i^*: $W_r(R)\to W_r(A)$ and i^*: $W_p(R)\to W_p(A)$ are injective,*

2) *t_{G*}: $W_r(A)\to W_r(R)$ and t_{G*}: $W_p(A)\to W_p(R)$ are sujective and split, and so $W_r(A)\cong i^*(W_r(R))\oplus Ker\ t_{G*}$, $W_p(A)\cong i^*(W_p(R))\oplus Ker\ t_{G*}$,*

3) Ker $t_{G*}=$Ker T_{G^*}, Im $i^*=$Im T_{G^*}, *i.e. i^*: $W_r(R)\to T_{G^*}(W_r(A))$ and i^*: $W_p(R)\to T_{G^*}(W_p(A))$ are isomorphisms.*

Furthermore, if A is commutative, then we have $T_{G^*}(W_r(A))=W_r(A)^{G^*}$ and $T_{G^*}(W_p(A))=W_p(A)^{G^*}$, i.e. i^*: $W_r(R)\to W_r(A)^{G^*}$ and i^*: $W_p(R)\to W_p(A)^{G^*}$ are isomorphisms.

Proof. Let C_0 be the fixed subring of the center of A by the involution. For any $u\in U(C_0)$ and a sesqui-linear left A-module $q=(M, q)$, the scaling ${}^uq=(M, {}^uq)$ by u is defined to be ${}^uq$: $M\times M\to A$; $(m, n)\leadsto uq(m, n)$. If $q=(M, q)$ is non degenerate, or hemitian, then so is ${}^uq=(M, {}^uq)$, respectively. If q is metabolic then so is ${}^uq$. Therefore, a scaling $[q]\leadsto[{}^uq]$ defines a group-automorphism μ of the Witt group W(A). Take u in $U(C_0)$ such that $(A, b^u_t)\cong\langle 1\rangle\perp h_m$. Since by Proposition 2 $t^u_{G*}\circ i^*=I$, we have that i^*: W$(R)\to$W(A) is injective and $I=t^u_{G*}\circ i^*=t_{G*}\circ\mu\circ i^*$. Therefore, it is obtained that t_{G*}: W$(A)\to$W(R) is surjective and split, and W$(A)=$Ker $t_{G*}\oplus\mu\circ i^*(W(R))\cong$Ker $t_{G*}\oplus i^*($W$(R))$. Since by Theorem 1 $i^*\circ t_{G*}=T_{G^*}$ on W(A), we have $i^*=i^*\circ t_{G*}\circ\mu\circ i^*=T_{G^*}\circ\mu\circ i^*$, and so i^*: W$(R)\to T_{G^*}(W(A))$ is an isomorphism and Ker $t_{G*}=$Ker T_{G^*}. If A is a commutative ring, then W(A) becomes a commutative ring with identity $[\langle 1\rangle]$. T_{G^*}: W$(A)\to$W$(A)^{G^*}$ is a ring-homomorphism, and $T_{G_*}($W$(A))$ is an ideal of W$(A)^{G^*}$. But by Proposition 2 $T_{G^*}(\langle u\rangle)=\langle 1\rangle\perp i^*(h_m)$ and $i^*(h_m)$ is a metabolic

2) See Appendix.

left A-module. Therefore, $[\langle 1\rangle]=T_{G^*}([\langle u\rangle])$ is in $T_{G^*}(\mathrm{W}(A))$, and so $T_{G^*}(\mathrm{W}(A))=\mathrm{W}(A)^{G^*}$.

4. Examples

In this section, we expose some examples of Galois extension with involution.

EXAMPLE 1. Let L, K be fields and $L\supset K$ a G-Galois extension with non trivial involution. Put $L_0=\{a\in L;\ a=\bar{a}\}$ and $K_0=L_0\cap K$. Then we have two cases;

Case I; $K\neq K_0$, then $L\supset L_0$ and $K\supset K_0$ are quadratic extensions, G induces the Galois group of $L_0\supset K_0$, and $L=L_0K=L_0\otimes_{K_0}K$.

Case II; $K=K_0$, then $L\supset L_0\supset K$ and $[L:K]=|G|$ is even.

Proposition 3. (cf. [11]) *Let L, K be fields and $L\supset K$ a G-Galois extension with involution. Then $L\supset K$ odd type if and only if $|G|=[L:K]=$odd.*

Proof. If $L\supset K$ is odd type then obviously $[L:K]=$odd. We shall show the converse. Firstly, we suppose that $L\supset K$ is a G-Galois extension with trivial involution and $|G|=$odd. Then there is an a in L such that $L=K[a]$. Put $[L:K]=2m+1$. From the proof of Scharlau's theorem (cf. [7], Th. 1.6, p. 195), we have that a K-linear map f: $L\rightarrow K$ defined by $f(1)=1$ and $f(a^i)=0$ for $i=1, 2, \cdots, 2m$, defines a non degenerate bilinear left K-module (L, b_t^u) by $b_t^u(x, y)=f(xy)$ for $x, y\in L$, where $u\in L$ is determined by $b_t^1(u, -)=f$. Then we have $(L, b_t^u)=K\perp(Ka\oplus Ka^2\oplus\cdots\oplus Ka^{2m})$, where $K=\langle 1\rangle$, and $Ka\oplus\cdots\oplus Ka^{2m}$ is a metabolic subspace, because $Ka\oplus\cdots\oplus Ka^m$ is a total isotropic subspace of it. Accordingly, $L\supset K$ is odd type. Secondaly, suppose that $L\supset K$ is a G-Galois extension with non trivial involution, and $|G|=$odd. By Case I, the involution is non trivial on K, i.e. $K\neq K_0$, and so $L=L_0K\cong L_0\otimes_{K_0}K$. Since $L_0\supset K_0$ becomes a G-Galois extension with trivial involution, $L_0\supset K_0$ is odd type, and so there is u in L_0 such that (L_0, b_t^u) is isometric to the orthogonal sum of $\langle 1\rangle$ and some metabolic K_0-subspace h_m. Then we have $(L, b_t^u)\cong i^*(L_0, b_t^u)=(K\otimes_{K_0}L_0, ib_t^u)\cong i^*(\langle 1\rangle)\perp i^*(h_m)=\langle 1\rangle\perp i^*(h_m)$ as hermitian K-modules, and $i^*(h_m)$ becomes a metabolic K-module. Thus, $L\supset K$ is odd type.

Corollary 1. *Let $L\supset K$ be fields and a G-Galois extension with involution. If $|G|=$odd, then the inclusion map i: $K\rightarrow L$ induces an isomorphism of hermitian Witt groups; i^*: $W(K)\rightarrow T_{G^*}(W(L))=W(L)^{G^*}$.*

EXAMPLE 2. Let R be a commutative ring, (V, q) a non degenerate quadratic R-module having a orthogonal base; $(V, q)=Rv_1\perp Rv_2\perp\cdots\perp Rv_n$. Then 2 and $q(v_i)$ $i=1, 2, \cdots n$ are invertible in R. Let ρ_{v_i} be a symmetry defined by

v_i, i.e. $\rho_{v_i}(x)=x-\dfrac{B_q(x, v_i)}{q(v_i)}v_i$ for $x\in V$. The Clifford algebra $C(V, q)=C_0(V, q)\oplus C_1(V, q)$ is a separable and $Z/(2)$-graded R-algebra (cf. [1], [8]). Each ρ_{v_i} is extended to an algebra-automorphism $\hat{\rho}_i$ of $C(V, q)$, for $i=1, 2, \cdots n$, and $\hat{\rho}_i$ is homogeneous i.e. $\hat{\rho}_i(C_j(V, q))=C_j(V, q), j=0,1$. $C(V, q)$ has an involution defined by $\overline{(x_1x_2\cdots x_r)}=x_r\cdots x_2x_1$ for $x_i\in V$. Then $\hat{\rho}_i$ is compatible with this involution. Let G be a group of automorphisms of $C(V, q)$ generated by $\hat{\rho}_1, \hat{\rho}_2, \cdots\hat{\rho}_n$. Then, we can show that $C(V, q)\supset R$ is a G-Galois extension with involution.

Proposition 4. *Let $C(V, q)$, $\hat{\rho}_1, \hat{\rho}_2, \cdots \hat{\rho}_n$ and G be as above. Then $C(V, q)\supset R$ is a G-Galois extension with involution, and $G=(\hat{\rho}_1)\times(\hat{\rho}_2)\times\cdots\times(\hat{\rho}_n)$.*

Proof. If $n=1$, $C(Rv_1, q)\cong R[X]/(X^2-q(v_1))$ is a separable quadratic extension of R, and so $C(Rv_1, q)\supset R$ is a Galois extension with Galois group $(\hat{\rho}_1)$ (cf. [8]). Suppose that $n>1$ and $C(Rv_1\oplus\cdots\oplus Rv_{n-1}, q)\supset R$ is a Galois extension with Galois group $(\hat{\rho}_1)\times(\hat{\rho}_2)\times\cdots\times(\hat{\rho}_{n-1})$. Since $Rv_1\oplus\cdots\oplus Rv_n=(Rv_1\oplus\cdots\oplus Rv_{n-1})\perp Rv_n$, it is well known that $C(Rv_1\oplus\cdots\oplus Rv_n, q)=C(Rv_1\oplus\cdots\oplus Rv_{n-1}, q)\hat{\otimes}C(Rv_n, q)$, where $\hat{\otimes}$ denotes the graded tensor product over R. Let $x_1, \cdots x_s$ and $y_1, \cdots y_s$ be a $(\hat{\rho}_1)\times\cdots\times(\hat{\rho}_{n-1})$-Galois system of $C(Rv_1\oplus\cdots\oplus Rv_{n-1}, q)$ and $u_1, \cdots u_t$ and $w_1, \cdots w_t$ a $(\hat{\rho}_n)$-Galois system of $C(Rv_n, q)$. x_i, y_i and u_j, w_j are chosen as homogeneous elements in $C(Rv_1\oplus\cdots\oplus Rv_{n-1}, q)$ and $C(Rv_n, q)$, respectively. Then, $\{(-1)^{\partial y_i\partial u_j}x_i\otimes u_j;\ 1\leqq i\leqq s,\ 1\leqq j\leqq t\}$ and $\{y_i\otimes w_j;\ 1\leqq i\leqq s,\ 1\leqq j\leqq t\}$ are a $(\hat{\rho}_1)\times\cdots\times(\hat{\rho}_{n-1})\times(\hat{\rho}_n)$-Galois system of $C(Rv_1\oplus\cdots\oplus Rv_n, q)=C(Rv_1\oplus\cdots\oplus Rv_{n-1}, q)\hat{\otimes}C(Rv_n, q)$, where ∂u_j and ∂y_i denete the degree of u_j and y_i. Because, $\sum_{i,j}(-1)^{\partial y_i\partial u_j}x_i\otimes u_j\cdot\sigma\times\tau(y_i\otimes w_j)=\sum_{i,j}x_i\sigma(y_i)\otimes u_j\tau(w_j)=\begin{cases}1\otimes 1; & \sigma\times\tau=I\times I\\ 0\ ; & \sigma\times\tau\neq I\times I\end{cases}$, for $\sigma\in(\hat{\rho}_1)\times\cdots\times(\hat{\rho}_{n-1})$ and $\tau\in(\hat{\rho}_n)$. Since $C(Rv_1\oplus\cdots\oplus Rv_{n-1}, q)\hat{\otimes}C(Rv_n, q)=C(Rv_1\oplus\cdots\oplus Rv_{n-1}, q)\otimes C(Rv_n, q)$ as R-modules and $(C(Rv_1\oplus\cdots\oplus Rv_{n-1}, q)\otimes C(Rv_n, q))^{(\hat{\rho}_1)\times\cdots\times(\hat{\rho}_n)}=C(Rv_1\oplus\cdots\oplus Rv_{n-1}, q)^{(\hat{\rho}_1)\times\cdots\times(\hat{\rho}_{n-1})}\otimes C(Rv_n, q)^{(\hat{\rho}_n)}=R\otimes R=R$, we have that $C(Rv_1\oplus\cdots\oplus Rv_n, q)\supset R$ is a Galois extension with Galois group $(\hat{\rho}_1)\times\cdots\times(\hat{\rho}_n)$. Thus, the proposition is obtained by induction.

EXAMPLE 3. Let $A\supset B$ be a G-Galois extension with involution. The $n\times n$-matrix ring A_n over A has an invoution $A_n\to A_n$; $(a_{ij})\rightsquigarrow {}^t(\bar{a}_{ij})$, where ${}^t(\ \ )$ denotes the transpose matrix. Then, $A_n\supset B_n$ is also a G-Galois extension with involution. Furthermore, if $A\supset B$ is odd type, then so is $A_n\supset B_n$. Because, we suppose that u is a unit in the fixed subring C_0 of the center of A by the involution, and (A, b_t^u) is a orthogonal sum of $\langle 1\rangle$ and a metabolic B-left module $h_g=(N, h_g)$. Then $A_n\cong B_n\otimes_B A$ as B_n-left modules and C_0 is the fixed subring of the center of A_n by the involution. Therefore, we have $(A_n, b_t^u)\cong(B_n\otimes_B A, i\, b_t^u)\cong i^*\langle 1\rangle\perp i^*h_g=\langle 1\rangle\perp i^*h_g$ as sesqui-linear B_n-left modules, and i^*h_g is a metabolic B_n-module, where $i: B\hookrightarrow B_n$.

Using the Morita context, Example 3 is extended as follows;

EXAMPLE 4. (cf. [2], Chap. I, 8.) Let $A\supset B$ be a G-Galois extension with involution, $\Delta(A, G)=\sum_{\sigma\in G}\oplus Au_\sigma$ a crossed product of A and G with a trivial factor set, and M a faithful left $\Delta(A, G)$-module. We may assume that u_I is the identity element in $\Delta(A, G)$, and A is a subring of $\Delta(A, G)$. We suppose that M has a non degenerate hermitian form $[\ ,\ ]$: $M\times M\to A$ satisfying $[u_\sigma(m), u_\sigma(n)]=\sigma([m, n])$ for every $\sigma\in G$ and $m, n\in M$. Put $\Lambda^0=\mathrm{Hom}_A(M, M)$ and $\Gamma^0=\mathrm{Hom}_{\Delta(A,G)}(M, M)$, then M is regarded as right Λ-module and so as A- Λ-bimodule. We can define an involution $\Lambda\to\Lambda$; $\lambda\leadsto\bar\lambda$ by $[m, n\lambda]=[m\bar\lambda, n]$ for every $m, n\in M$ (cf. [2], p. 61). For each $\sigma\in G$, a ring-automorphism σ': $\Lambda\to\Lambda$ is defined by $m\sigma'(\lambda)=u_\sigma((u_\sigma^{-1}(m))\lambda)$ for $m\in M$ and $\lambda\in\Lambda$. Put $G'=\{\sigma'; \sigma\in G\}$. Since $u_\sigma u_\tau=u_{\sigma\tau}$ in $\Delta(A, G)$, the map $G\to G'$; $\sigma\leadsto\sigma'$ is a group homomorphism. We can easily check $\Lambda^{G'}=\Gamma$. For any $\lambda\in\Lambda$, $\sigma'\in G'$, $\sigma'(\bar\lambda)=\overline{\sigma'(\lambda)}$ is satisfided; for any $m, n\in M$, we have $[m\sigma'(\bar\lambda), n]=[u_\sigma(u_\sigma^{-1}(m)\bar\lambda), n]=\sigma([u_\sigma^{-1}(m)\bar\lambda, u_\sigma^{-1}(n)]=\sigma([u_\sigma^{-1}(m), u^{-1}(n)\lambda])=[m, n\sigma'(\lambda)]=[m\overline{\sigma'(\lambda)}, n]$. Put $M^G=\{m\in M; u_\sigma(m)=m$ for all $\sigma\in G\}$, then M^G becomes a left B-module. We can show that if M^G is finitely generated projective and generator over B, then $\Lambda\supset\Gamma$ is also a G'-Galois extension with involution and $G'\cong G$. Now, we shall prove this. We denote by $(\ ,\ )$ a sesqui-linear form $M\times M\to\Lambda$ defined by $[m, m']m''=m(m', m'')$ for every m, m' and $m''\in M$ (see [2], p. 61).

Lemma 7. *Under above conditions, we have $M=AM^G\cong A\otimes_B M^G$, and $[\ ,\ ]$ induces a non degenerate hermitian form $[\ ,\ ]|M^G\times M^G$ over B.*

Proof. Let $x_1, \cdots x_n$ and $y_1, \cdots y_n$ be a G-Galois system of A. For any $m\in M$, m is written as $m=\sum_{i,\sigma\in G}x_i\sigma(y_i)u_\sigma(m)=\sum_{i,\in G}x_iu_\sigma(y_im)=\sum_i x_it_G(y_im)$, and is contained in AM^G, where $t_G(y_im)=\sum_{\sigma\in G}u_\sigma(y_im)$ is in M^G. If $\sum_i a_i\otimes m_i$ is an element in $A\otimes_B M^G$ such that $\sum a_im_i=0$, then we have $\sum a_i\otimes m_i=\sum_{i,j} x_jt_G(y_ja_i)\otimes m_i=\sum_{i,j}x_j\otimes t_G(y_ja_i)m_i=\sum_j x_j\otimes t_G(y_j\sum a_im_i)=0$. Therefore, $M=AM^G\cong A\otimes_B M^G$ is obtained. Since $\sigma([m, n)]=[u_\sigma(m), u_\sigma(n)]$ for every $\sigma\in G$ and $m, n\in M$, $[\ ,\ ]'=[\ ,\ ]|M^G\times M^G$ defines a hermitian B-form $[\ ,\ ]'$: $M^G\times M^G\to B$. By $M=AM^G$, $[M^G, m]'=0$ implies $m=0$. If f is any element in $\mathrm{Hom}_B(M^G, B)$, then $I\otimes f$ is in $\mathrm{Hom}_A(M, A)$, hence there is an element m in M such that $f=[-, m]$. But, $f(n)$ is in B for all $n\in M^G$, then we have $[n, m]=f(n)=\sigma([n, m])=[u_\sigma(n), u_\sigma(m)]=[n, u_\sigma(m)]$ for all $n\in M^G$, $\sigma\in G$, and so $m=u_\sigma(m)$ for all $\sigma\in$ G, i.e. $m\in M^G$. Therefore, $[\ ,\ ]'$ is non degenerate.

Proposition 5. *If M^G is finitely generated projective and generator over B,* *then $\Lambda\supset\Gamma$ is a G'-Galois extension with involution, and $G'\cong G$.*

Proof. Let $x_1, \cdots x_n$ and $y_1, \cdots y_n$ be G-Galois system of A. Since M^G is a finitely generated projective and generator B-module, and $[\ ,\ ]|M^G\times M^G$ is non degenerate, hence there exist $m_1, \cdots m_r$ and $n_1, \cdots n_r$, $u_1, \cdots u_s$ and $v_1, \cdots v_s$ in M^G such that $\sum_i[m_i, n_i]=1$, $I=\sum_i[-, u_i]v_i=\sum_i(u_i, v_i)$. Put $m'_{ij}=\bar{x}_j u_i n'_{ij}=y_j v_i$. Then we have $\sum_{i,j}(m'_{ij}, u_\sigma(n'_{ij}))=\sum_{i,j}(x_j u_i, u_\sigma(y_j v_i))=\sum_{i,j}[-,x_j u_i]\sigma(y_j)u_\sigma(v_i)=\sum_{i,j}[-, u_i]x_j\sigma(y_j)v_i=\begin{cases}\sum_j[-, u_i]v_i; & \text{for } \sigma=I\\ 0 & ; \text{ for } \sigma\neq I\end{cases}=\begin{cases}1; & \text{for } \sigma=I\\ 0; & \text{for } \sigma\neq I\end{cases}$. Since n'_{ij} is expressed as $n'_{ij}=\sum_k[m_k, n_k]n'_{ij}=\sum_k m_k(n_k, n'_{ij})$, we have $\sum_{i,j,k}(m'_{ij}, m_k)\sigma'((n_k, n'_{ij}))=\sum_{i,j,k}(m'_{ij}, u_\sigma(m_k(n_k, n'_{ij})))=\sum_{i,j}(m'_{ij}, u_\sigma(n'_{ij}))=\begin{cases}1; \text{ for } \sigma=I\\ 0; \text{ for } \sigma\neq I\end{cases}$. Therefore, $\{(m'_{ij}, m_k);\ 1\leqq i\leqq s\leqq,\ 1\leqq j\leqq n,\ 1\leqq k\leqq r\}$ and $\{(n_k, n'_{ij});\ 1\leqq i\leqq s,\ 1\leqq j\leqq n,\ 1\leqq k\leqq r\}$ are G'-Galois system of Λ and $G\cong G'$. Thus $\Lambda\supset\Gamma$ is a G'-Galois extension with involution.

Corollary 2. *Let A be an algebra over a commutative ring R, and $A\supset R$ a G-Galois extension with involution. If M is a faithful left $\Delta(A, G)$-module such that M is finitely generated projective over A and M has a non degenerate hermitian form $[\ ,\ ]\ M\times M\to A$ satisfying $\sigma([m, n])=[u_\sigma(m), u_\sigma(n)]$ for all $n, m\in M$ and $\sigma\in G$, then $\Lambda=\mathrm{Hom}_A(M, M)\supset\Gamma=\mathrm{Hom}_{\Delta(A,G)}(M, M)$ is a G-Galois extension with involution.*

Proof. Since, under the condition of the corollary, we have $t_G(A)=R$ and $M=AM^G\cong A\otimes_B M^G$, we conclude that M^G is a direct summand of M as R-module. Therefore M^G is finitely generated projective and generator over R, and by Proposition 5 $\Lambda\supset\Gamma$ is a G'-Galois extension with involution and $G\cong G'$.

Appendix

Let R be a commutative ring.

Lemma A. ([5], Lemma 1.2) *Let (M, q) be a non degenerate hermitian R-module. Then (M, q) is metabolic if and only if there is an R-direct summand N of M such that $N^\perp=N$.*

Lemma B. (cf. [5], Lemma 1.5) *Let (M, q) be any non-degenerate hermitian R-module and (N, h_m) a metabolic R-module such that N is a projective R-module. If $(N, h_m)\otimes(M, q)=(N\otimes_R M, h_m\otimes q)$ is non degenerate, then $(N, h_m)\otimes(M, q)$ is also metabolic.*

Proof. Suppose $(N, h_m)\cong(U\oplus U^*, h_g)$, where $U^*=\mathrm{Hom}_R(U, R)$ and (U, g) is a hermitian R-module. By Lemma A, it is sufficient to show $(U^*\otimes M)^\perp=U^*\otimes M$ in $(U\otimes M\oplus U^*\otimes M, h_g\otimes q)$. If $\sum u_i\otimes m_i$ is in $(U^*\otimes M)^\perp\cap(U\otimes M)$, then we have $h_g\otimes q(\sum u_i\otimes m_i, f\otimes x)=\sum h_g(u_i, f)\,q(m_i, x)=\sum f(u_i)\,q(m_i, x)=$

$q(\sum f(u_i)m_i, x)=0$, for every $x\in M$ and $f\in U^*$, hence $\sum f(u_i)m_i=0$ for every $f\in U^*$. Since U is projective over R, there exist $\{f_j\in U^*; j\in I\}$ and $\{v_j\in U; j\in I\}$ such that $x=\sum_{j\in I}v_jf_j(x)$ for all $x\in U$. Accordingly, $\sum u_i\otimes m_i=\sum_{i,j\in I} v_jf_j(u_i)\otimes m_i=\sum_{j\in I}v_j\otimes\sum_i f_i(u_i)m_i=0$. We obtain that $(U^*\otimes M)^{\perp}\cap(U\otimes M)=0$ and so $(U^*\otimes M)^{\perp}=U^*\otimes M$.

OSAKA CITY UNIVERSITY

References

[1] H. Bass: Topics in Algebraic K-theory, Tata Institute Notes, 41, Bombay, 1967.

[2] H. Bass: *Unitary K-theory,* Springer lecture notes, 343, 1973.

[3] T. Kanzaki: *Non-commutative quadratic extension of a commutative ring,* Osaka J. Math. **10** (1973), 597–605.

[4] M. Knebusch and W. Scharlau: *Über das Verhalten der Witt-Gruppe bei galoischen Körpererweiterungen,* Math. Ann. **193** (1971), 189–196.

[5] M. Knebusch, A. Rosenberg and R. Ware: *Structure of Witt rings and quotient of aberian group rings,* Amer. J. Math. **94** (1972), 119–155.

[6] M. Knebusch, A. Rosenberg and R. Ware: *Signatures on semilocal rings,* J. Algebra **26** (1973), 208–250.

[7] T.Y. Lam: The Algebraic Theory of Quadratic Forms, Benjamin 1973.

[8] A. Micali and O.E. Villamayor: *Sur Les algebras de Clifford.* II, J. Reine Angew. Math. **242** (1970), 61–90.

[9] A. Rosenberg and R. Ware: *The zero-dimensional Galois cohomology of Witt ring,* Invent. Math. **11** (1970), 65–72.

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

[11] W. Scharlau: *Quadratic reciprocity law,* J. Number Theory **4** (1972), 78–97.

[12] W. Scharlau: *Zur Pfistersch Theorie der quadratischen Formen,* Invent. Math. **6** (1969), 327–328.