26. On Odd Type Galois Extension with Involution of Semi-local Rings*)

By Teruo KANZAKI and Kazuo KITAMURA
Osaka City University, Osaka Kyoiku University

(Comm. by Kenjiro SHODA, M. J. A., Feb. 12, 1975)

1. Introduction. In [3], the notion of odd type G-Galois extension with involution was defined as follows: If $A\supset B$ is a G-Galois extension and A has an involution $A\to A$; $a\leadsto\bar{a}$, which is compatible with every element σ of G, i.e. $\sigma(\bar{a})=\overline{\sigma(a)}$ for all $a\in A$, then $A\supset B$ is called a G-Galois extension with involution. A G-Galois extension with involution $A\supset B$ is called odd type, if A has an element u satisfying the following conditions;

1) u is an invertible element in the fixed subring of the center of A by the involution,

2) a hermitian left B-module (A, b_t^u) defined by $b_t^u: A\times A\to B$; $(x,y)\leadsto t_G(ux\bar{y})=\sum_{\sigma\in G}\sigma(ux\bar{y})$, is isometric to an orthogonal sum of $\langle 1\rangle$ and a metabolic B-module.

If A, B are fields and $A\supset B$ is a G-Galois extension with involution, it was known that $A\supset B$ is odd type if and only if the order of G is odd. In this note, we want to extend this to semi-local rings. When $A\supset B$ is a G-Galois extension with involution of commutative rings, it is easily seen that an odd type G-Galois extension implies $|G|=\text{odd}$. For semi-local rings A and B, we shall show that the converse holds in the following cases:

I. The involution is trivial and $|B/\mathfrak{m}|\geqq|G|$ for every maximal ideal m of B, where $|B/\mathfrak{m}|$ and $|G|$ denote numbers of elements of $B/\mathfrak{m}$ and G, respectively.

II. The involution is non-trivial and for each maximal ideal $\mathfrak{m}$ of B the following conditions are satisfied;

1) $|B/\mathfrak{m}|\geqq 2|G|$, 2) if $\bar{\mathfrak{m}}=\mathfrak{m}$, the involution induces a non-trivial one on $A/\mathfrak{m}A$.

III. B is a local ring with maximal ideal $\mathfrak{m}$, and the involution is non-trivial on A but induces a trivial one on $A/\mathfrak{m}A$. Furthermore, $|B/\mathfrak{m}|\geqq|G|$ and $B/\mathfrak{m}$ is either a field with the characteristic not 2 or a finite field. Throughout this paper, every ring is a commutative semi-local ring with identity and $A\supset B$ denotes a G-Galois extension with involution.

2. Galois extension with trivial involution. Lemma 1. *Let*

---

*) Dedicated to Professor Mutsuo Takahashi on his 60th birthday.

$A\supset B$ be a G-Galois extension with trivial involution and B a field. If $|B|\geqq|G|$, then we have the following;

1) *there is a in A such that $A=B[a]=B\oplus Ba\oplus\cdots\oplus Ba^{n-1}$, $n=|G|$,*

2) *the minimal polynomial $F(X)=X^n+d_1X^{n-1}+\cdots+d_n$ of a has a nonzero constant term; $d_n\neq 0$,*

3) *for a B-linear map $h: A\to B$ defined by $h(1)=1$, $h(a^i)=0$, $i=1,2,\cdots,n-1$, there exists a unit u in A such that $h(x)=t_G(ux)=b_t^1(u,x)$ for all $x\in A$.*

Proof. Let $e_1,e_2,\cdots,e_m$ be the all primitive idempotents in A. Then $A=Ae_1\oplus Ae_2\oplus\cdots\oplus Ae_m$ is a direct sum of fields Ae_i, $i=1,2,\cdots,m$. Put $G_1=\{\sigma\in G;\sigma(e_1)=e_1\}$ and take σ_i in G such that $\sigma_i(e_1)=e_i$, $i=1,2,\cdots,m$. Then we have that $G=\sigma_1G_1\cup\cdots\cup\sigma_mG_1$, $Ae_1\supset Be_1$ is a G_1-Galois extension and $\sigma_i: Ae_1\to Ae_i$ is a B-algebra isomorphism, $i=1,2,\cdots,m$. Therefore, there is a separable and irreducible polynomial $f(X)$ in $B[X]$ such that $Ae_i\cong B[X]/(f(X))$, $i=1,2,\cdots,m$. We can chose $a_1=0$, $a_2,\cdots,a_m$ in A such that $f(X+a_1)$, $f(X+a_2),\cdots,f(X+a_m)$ are mutually distinct. This is shown by induction as follows: Let K be an algebraic closure of B, and $\alpha_1,\alpha_2,\cdots,\alpha_l$ roots of $f(X)=0$ in K, where $l=\deg f(X)=|G_1|$. Suppose $a_1=0$, $a_2,\cdots,a_r$ has been taken for $1\leqq r<m$ so that $f(X+a_1)$, $f(X+a_2),\cdots,f(X+a_r)$ are distinct polynomials. Since $|B|\geqq|G|=|G_1|m=lm>lr$, we can chose a_{r+1} in B such that $\alpha_1-a_{r+1}\neq\alpha_i-a_j$ for $i=1,2,\cdots,l$ and $j=1,2,\cdots,r$. Then we have $f(X+a_{r+1})\neq f(X+a_j)$ for $j=1,2,\cdots,r$. Accordingly, we have distinct irreducible polynomials $f(X+a_1)$, $f(X+a_2),\cdots,f(X+a_m)$. Setting $F(X)=f(X+a_1)f(X+a_2)\cdots f(X+a_m)$, we obtain

$$\begin{aligned} B[X]/(F(X)) &\cong B[X]/(f(X+a_1))\oplus\cdots\oplus B[X]/(f(X+a_m)) \\ &\cong Ae_1\oplus\cdots\oplus Ae_m=A \end{aligned}$$

as B-algebras. Therefore, there is a in A such that $A=B[a]$ and $F(X)=X^n+d_1X^{n-1}+\cdots+d_n$ is the minimal polynomial of a. Since $f(X+a_i)$ is irreducible in $B[X]$, the constant term d_n of $F(X)$ is nonzero. Let $h: A\to B$ be a B-linear map defined by $h(1)=1$ and $h(a^i)=0$, $i=1,2,\cdots,n-1$. Since (A,b_t^1) is non degenerate, there is u in A such that $h(x)=b_t^1(x,u)=t_G(xu)$ for all $x\in A$. We now show that u is invertible in A. Let $\mathfrak{a}$ be the annihilator ideal of u in A. Since $h(\mathfrak{a})=b_t^1(\mathfrak{a},u)=t_G(\mathfrak{a}u)=0$, $\mathfrak{a}$ is contained in $\operatorname{Ker} h=Ba\oplus Ba^2\oplus\cdots\oplus Ba^{n-1}$. For any element $\alpha=b_1a+b_2a^2+\cdots+b_{n-1}a^{n-1}\in\mathfrak{a}$, we have $(a^{n-1}+d_1a^{n-2}+\cdots+d_{n-1})\alpha=(a^n+d_1a^{n-1}+\cdots+d_{n-1}a)(b_1+b_2a+\cdots+b_{n-1}a^{n-2})=-d_nb_1-d_nb_2a-\cdots-d_nb_{n-1}a^{n-2}\in\mathfrak{a}$, and so $-d_nb_1=h(-d_nb_1-d_nb_2a-\cdots-d_nb_{n-1}a^{n-2})=0$. But $d_n\neq 0$, therefore $b_1=0$ and $b_2a+\cdots+b_{n-1}a^{n-2}\in\mathfrak{a}$. Repeating this, we conclude $b_1=b_2=\cdots=b_{n-1}=0$, i.e. $\alpha=0$. Accordingly, we have $\mathfrak{a}=0$, namely, u is invertible in A.

Proposition 1. *Let A,B be semi-local rings and $A\supset B$ a G-Galois extension with trivial involution. We assume that $|B/\mathfrak{m}|\geqq|G|$ for every* *maximal ideal* $\mathfrak{m}$ *in* B. *Then we have the following*;

1) *there is* a *in* A *such that* $1, a, \cdots, a^{n-1}$ *are* B*-free bases of* A; $A=B\oplus Ba\oplus\cdots\oplus Ba^{n-1}$, *and the monic minimal polymomial* $F(X)$ *of* a *has an invertible constant term,*

2) *for a* B*-linear map* $h: A\to B$ *defined by* $h(1)=0$, $h(a^i)=0$, $i=1,2,\cdots,n-1$, *there exists a unit* u *in* A *such that* $h(x)=t_G(ux)$ *for all* $x\in A$, *and so* (A, b_t^u) *is non degenerate.*

Proof. Let J be the radical of B, and $e_1, e_2, \cdots, e_t$ the all primitive idempotents in B/J. Then we have that $A/JA\ e_i\supset B/J\ e_i$, $i=1,2,\cdots,t$, and $A/JA=\sum_{i=1}^t A/JA\ e_i\supset B/J=\sum_{i=1}^t B/J\ e_i$ are G-Galois extensions. Since $B/J\ e_i$ is a field, by Lemma 1, there is α_i in $A/JA\ e_i$ such that $A/JA\ e_i=B/J\ e_i\oplus B/J\ e_i\alpha_i\oplus\cdots\oplus B/J\ e_i\alpha_i^{n-1}$ for $i=1,2,\cdots,t$, where $n=|G|$. Put $\alpha=\alpha_1+\alpha_2+\cdots+\alpha_t$ in A/J, then we have $A/JA=B/J\oplus B/J\ \alpha\oplus\cdots\oplus B/J\ \alpha^{n-1}$. Let a be an element in A which is a representative of α. Then, by Nakayama's lemma, we have $A=B\oplus Ba\oplus\cdots\oplus Ba^{n-1}$ and $1, a, \cdots, a^{n-1}$ are B-free bases of A. Furthermore, by Lemma 1, the minimal polynomial $F(X)=X^n+d_1X^{n-1}+\cdots+d_n$ of a in $B[X]$ has an invertible constant term. Let $h: A\to B$ be a B-linear map defined by $h(1)=1$, $h(a^i)=0$, $i=1,2,\cdots,n-1$. Then there exists u in A such that $h(x)=b_t^1(u,x)=t_G(ux)$ for all $x\in A$. Now, considering at mod J, the element $[u]$ in A/JA is a unit, because by Lemma 1 $[u]e_i$ is a unit in A/JA for every $i=1,2,\cdots,t$. Therefore, u is a unit in A. Accordingly, (A, b_t^u) is non degenerate.

Theorem 1. *Let* A, B *be semi-local rings and* $A\supset B$ *a* G*-Galois extension with trivial involution. We assume that for every maximal ideal* $\mathfrak{m}$ *of* B, $|B/\mathfrak{m}|\geqq|G|$ *and* $|G|$ *is odd. Then* $A\supset B$ *is an odd type* G*-Galois extension.*

Proof. By Proposition 1, A has an element a in A such that $1, a, a^2, \cdots, a^{n-1}$ are B-free bases of A i.e. $A=B\oplus Ba\oplus\cdots\oplus Ba^{n-1}$, and we can take a B-linear map $h: A\to B$ defined by $h(1)=1$, $h(a^i)=0$, $i=1,2,\cdots,n-1$, and a unit u in A such that $h(x)=b_t^1(u,x)=t_G(ux)$ for all $x\in A$. Then we see that $(A, b_t^u)=B\perp(Ba\oplus\cdots\oplus Ba^{n-1})$ is non degenerate and so is $Ba\oplus\cdots\oplus Ba^{n-1}$. We now show that $Ba\oplus\cdots\oplus Ba^{n-1}$ is metabolic. Put $r=(n-1)/2$. It is sufficient to show that $N=Ba\oplus\cdots\oplus Ba^r$ satisfies $N^\perp=N$ ([4], Lemma 1.2). Obviously $N^\perp\supset N$. To show $N^\perp\subset N$, it suffices to show $N^\perp\cap(Ba^{r+1}\oplus\cdots\oplus Ba^{n-1})=0$. Suppose that $c=b_1a^{r+1}+\cdots+b_ra^{n-1}\neq 0$ is in $N^\perp$ and $b_1=\cdots=b_{k-1}=0$ but $b_k\neq 0$. Let $F(X)=X^{n-1}+d_1X^{n-2}+\cdots+d_n$ be a minimal polynomial of a in $B[X]$. By Proposition 1, d_n is a unit in B. Put $-G(X)=X^{n-r-k}+d_1X^{n-r-k-1}+\cdots+d_{r-k}X$ and $H(X)=d_{r-k+1}X^{r+k}+\cdots+d_n$. Then we have $F(X)=-G(X)X^{r+k}+H(X)$ and $0=F(a)=-G(a)a^{r+k}+H(a)$, where $-G(a)=d_{r-k}a+\cdots+d_1a^{n-r-k-1}+a^{n-r-k}$ is in N. By $c\in N^\perp$, we have

$$\begin{aligned}0&=b_t^u(c, G(a))=t_G(ucG(a))=h(cG(a))\\&=h((b_ka^{r+k}+\cdots+b_ra^{n-1})G(a))\\&=h((b_k+b_{k+1}a+\cdots+b_ra^{n-1-r-k})a^{r+k}G(a))\\&=h((b_k+b_{k+1}a+\cdots+b_ra^{n-1-r-k})H(a))\\&=h((b_k+b_{k+1}a+\cdots+b_ra^{n-1-r-k})(d_{r-k+1}a^{r+k}+\cdots+d_n))\\&=b_kd_n.\end{aligned}$$

Since d_n is invertible, $b_k=0$ is concluded. But it is a contradiction to $b_k\neq 0$. Therefore $c=0$, we obtain $N^{\perp}=N$, and $Ba\oplus\cdots\oplus Ba^{n-1}$ is a metabolic B-module. It is concluded that $A\supset B$ is odd type.

3. Galois extension with non-trivial involution. Lemma 2. *Let A, B be semi-local rings and $A\supset B$ a G-Galois extension with non-trivial involution. If $|G|=$odd then the involution induces a non-trivial involution on B.*

Proof. Put $A_0=\{a\in A\,;\,\bar{a}=a\}$. Suppose that the involution of A induces trivial on B. Denote by H the group consisting of the involution and the identity map. We shall show that $A\supset A_0=A^H$ is an H-Galois extension. Let $e_1, e_2, \cdots, e_m$ be the all primitive idempotents in A. We suppose $\bar{e}_{2i-1}=e_{2i}$, $i=1,2,\cdots,r$ and $\bar{e}_j=e_j$, $j=2r+1,\cdots,m$. Put $e_i'=e_{2i-1}+e_{2i}$. Then e_i' and e_j, $1\leqq i\leqq r$, $2r+1\leqq j\leqq m$, are orthogonal idempotents in A_0 and $1=\sum_{i=1}^r e_i'+\sum_{j=2r+1}^m e_j$. For a j, $2r+1\leqq j\leqq m$, Ae_j has no idempotents other than 0 and 1, and $Ae_j\supset A_0e_j$ is a separable extension and so $Ae_j\supset A_0e_j=(Ae_j)^H$ is an H-Galois extension. For an i, $1\leqq i\leqq r$, we have $Ae_i'=A_0e_{2i-1}\oplus A_0e_{2i}$. Because, if a is in Ae_i' then $a_0=ae_{2i-1}+\bar{a}e_{2i}$ and $a_0'=\bar{a}e_{2i-1}+ae_{2i}$ are contained in A_0, and so $a=a_0e_{2i-1}+a_0'e_{2i}$ is contained in $A_0e_{2i-1}\oplus A_0e_{2i}$. Therefore, we have that $Ae_i'=A_0e_{2i-1}\oplus A_0e_{2i}\supset A_0e_i'$ is a trivial H-Galois extension. We conclude that $A=\sum_{i=1}^r Ae_i'\oplus\sum_{j=2r+1}^m Ae_j\supset A_0=\sum_{i=1}^r A_0e_i'\oplus\sum_{j=2r+1}^m A_0e_j$ is an H-Galois extension. Accordingly, $[A:B]=[A:A_0]\cdot[A_0:B]=|H|\cdot[A_0:B]$ is even. This is a contradiction to $[A:B]=|G|=$odd.

Theorem 2. *Let A, B be semi-local rings and $A\supset B$ a G-Galois extension with non-trivial involution. We assume $|G|=$odd and $|B/\mathfrak{m}|\geqq 2|G|$ for every maximal ideal $\mathfrak{m}$ of B. If the involution of A induces a non-trivial involution on $A/\mathfrak{m}A$ for every maximal ideal $\mathfrak{m}$ of B provided $\bar{\mathfrak{m}}=\mathfrak{m}$. Then $A\supset B$ is an odd type G-Galois extension.*

Proof. For any maximal ideal $\mathfrak{m}$ of B, if $\mathfrak{m}\neq\bar{\mathfrak{m}}$ then there is b in B such that $b\in\mathfrak{m}$ and $\bar{b}\notin\mathfrak{m}$, i.e. $b-\bar{b}\notin\mathfrak{m}$, and if $\mathfrak{m}=\bar{\mathfrak{m}}$ then $A/\mathfrak{m}A\supset B/\mathfrak{m}$ is a G-Galois extension with non-trivial involution, and so, by Lemma 2, there is b in B such that $b-\bar{b}\notin\mathfrak{m}$. Accordingly, by [2] Theorem 1.3 (f), we obtain that $B\supset B_0$ is an H-Galois extension. If $A\cong A_0\otimes_{B_0}B$ is established, then $A\cong A_0\otimes_{B_0}B\supset A_0\otimes_{B_0}B_0=A_0$ is an H-Galois extension. Now we show $A\cong A_0\otimes_{B_0}B$. Let $x_1, x_2, \cdots, x_n, y_1, y_2, \cdots, y_n$ be an H-Galois system of B, then any a in A is expressed by $a=\sum_{i=1}^n t_H(ax_i)y_i$ in $A_0\cdot B$. And for $\alpha=\sum_i a_i\otimes b_i$ in the Ker $(A_0\otimes_{B_0}B$

$\to A_0\cdot B)$, we have $\alpha=\sum_i a_i\otimes b_i=\sum_{i,j} a_i\otimes t_H(b_ix_j)y_j=\sum_{i,j} a_it_H(b_ix_j)\otimes y_j$ $=\sum_{i,j} t_H(a_ib_ix_j)\otimes y_j=0$. Therefore we get $A=A_0\cdot B\cong A_0\otimes_{B_0}B$. Since B is a semi-local ring, B_0 is also semi-local. Then B has a B_0-free basis $\{1, v\}$; $B=B_0\oplus B_0v$, and so $A=A_0\otimes_{B_0}B=A_0\oplus A_0v$ is A_0-free module. For any maximal ideal $\mathfrak{p}_0$ of A_0, there is a maximal ideal $\mathfrak{p}$ of A such that $\mathfrak{p}\supset\mathfrak{p}_0A$. Since $A\supset B$ is a G-Galois extension, for each σ in G, there is a in A such that $a-\sigma(a)\notin\mathfrak{p}$. a is expressed by $a=a_0+a_0'v$ in $A=A_0\oplus A_0v$, a_0, $a_0'\in A_0$. Since $(a_0-\sigma(a_0))+(a_0'-\sigma(a_0'))v=a-\sigma(a)\notin\mathfrak{p}$, we have either $a_0-\sigma(a_0)\notin\mathfrak{p}_0$ or $a_0'-\sigma(a_0')\notin\mathfrak{p}_0$. Therefore, $A_0\supset A_0^G=B_0$ is a G-Galois extension. Accordingly, $A_0\supset B_0$ is a G-Galois extension with trivial involution. For any maximal ideal $\mathfrak{m}_0$ of B_0, there is a maximal ideal $\mathfrak{m}$ of B, such that $\mathfrak{m}\cap B_0=\mathfrak{m}_0$. Since $[B:B_0]=2$, we have $[B/\mathfrak{m}: B_0/\mathfrak{m}_0]\leqq 2$ and so $|B_0/\mathfrak{m}_0|\geqq(1/2)|B/\mathfrak{m}|\geqq|G|$. Therefore, by Theorem 1, there is a unit u in A_0 such that $(A_0, b_t^u)\cong\langle 1\rangle_{B_0}\perp h_m$, where h_m is a metabolic B_0-module. Since $A\cong B\otimes_{B_0}A_0$, we conclude (A, b_t^u) $=(B\otimes_{B_0}A_0, ib_t^u)\cong\langle 1\rangle_B\perp i^*h_m$, where i is the inclusion map $B\to A$ and i^*h_m becomes a metabolic B-module (cf. [1] or [4]). Accordingly, $A\supset B$ is an odd type G-Galois extension.

4. Galois extension with non-trivial involution over a local ring. In this section we consider a local ring B with maximal ideal $\mathfrak{m}$ and a G-Galois extension with non-trivial involution $A\supset B$ such that the involution induces a trivial one on $A/\mathfrak{m}A$.

Theorem 3. *Let $A\supset B$ be as above. We assume that the residue field $B/\mathfrak{m}$ is either a field with the characteristic not 2 or a finite field. If $|G|=odd$ and $|B/\mathfrak{m}|\geqq|G|$, then $A\supset B$ is an odd type G-Galois extension with involution.*

Proof. In the proof of Theorem 1, without considering the involution, we had a in A such that $A=B\oplus Ba\oplus\cdots\oplus Ba^{n-1}$ is B-free and the constant term of the minimal polynomial $F(X)$ of a in $B[X]$ is invertible. If the characteristic of $B/\mathfrak{m}$ is not 2, then we can take $a'=(1/2)(a+\bar{a})$ in place of a. Then we have $\overline{a'}=a'$ and $A=B\oplus Ba'\oplus\cdots\oplus Ba'^{n-1}$ is B-free. If characteristic of $B/\mathfrak{m}$ is 2 and $B/\mathfrak{m}$ is a finite field, then the map $B/\mathfrak{m}\to B/\mathfrak{m}$; $[x]\leadsto[x]^2$ is an automorphism of $B/\mathfrak{m}$, therefore there exists c in A such that $[c]^2=[a]$. Then we take $a'=c\bar{c}$ in place of a. We have also $\overline{a'}=a'$ and $A=B\oplus Ba'\oplus\cdots\oplus Ba'^{n-1}$ is B-free. Let $h: A\to B$ be a B-linear map defined by $h(1)=1$, $h(a^i)=0$, $i=1, 2, \cdots, n-1$. Then $\overline{h(x)}=h(\bar{x})$ is satisfied for all x in A. The u which is determined by $h(x)=b_t^1(x, u)=t_G(\bar{u}x)$ for all x in A, is fixed by the involution. Because, we have $b_t^1(\bar{x}, u)=h(\bar{x})=\overline{h(x)}=\overline{t_G(\bar{u}x)}$ $=t_G(u\bar{x})=b_t^1(\bar{x}, \bar{u})$ for all x in A, and so we have $\bar{u}=u$ and (A, b_t^u) is a non degenerate hermitian B-module. Similarly to the proof of Theorem 1, we conclude this theorem.

References

[1] H. Bass: Unitary algebraic K-theory. Springer Lecture Notes, **343**, 57–265 (1972).

[2] S. U. Chase, D. K. Harrison, and A. Rosenberg: Galois theory and cohomology of commutative rings. Memoir A. M. S. No. 52 (1965).

[3] T. Kanzaki: On Galois extension with involution of rings (to appear).

[4] M. Knebusch, A. Rosenberg, and R. Ware: Structure of Witt rings and quotients of abelian group rings. American J. Math., **94**, 119–155 (1972).