

Title	On Galois extensions over commutative rings
Author(s)	Takeuchi, Yasuji
Citation	Osaka Journal of Mathematics. 1965, 2(1), p. 137-145
Version Type	VoR
URL	<a href="https://doi.org/10.18910/4803">https://doi.org/10.18910/4803</a>
rights	
Note	

*Osaka University Knowledge Archive : OUKA*

<https://ir.library.osaka-u.ac.jp/>

Osaka University

## ON GALOIS EXTENSIONS OVER COMMUTATIVE RINGS

YASUJI TAKEUCHI

(Received January 30, 1965)

In [2], M. Auslander and O. Goldman introduced the notion of Galois extension of commutative rings. Recently, in [5], S. U. Chase, D. K. Harrison and A. Rosenberg gave a generalization of the fundamental theorem of Galois theory.

In the first section of this note, we shall extend to a case of non-commutative rings the definition of Galois extension which is defined by Chase, Harrison and Rosenberg in the case of commutative rings. Then we shall establish a half of the fundamental theorem of Galois theory by the method that is completely similar to the method used by Chase, Harrison and Rosenberg.

In the second section, we shall study on a Galois extension over commutative rings and we shall show that if a ring  $\Gamma$  is an inner Galois extension of its center  $C$ , then  $\Gamma$  is generated by units of  $\Gamma$  over  $C$ .

### 1. Galois extensions

Throughout this note it is assumed that every ring has the identity element, every subring has the common identity element and every group is of finite order.

Let  $\Gamma$  be a ring,  $\Lambda$  a subring of  $\Gamma$  and  $G$  a finite group of automorphisms of  $\Gamma$  which fix all elements of  $\Lambda$ . We shall denote a crossed product of  $\Gamma$  and  $G$  with trivial factor set by  $\Delta(\Gamma, G)$  i.e.  $\Delta(\Gamma, G)$  is a free  $\Gamma$ -module  $\sum_{\sigma \in G} \Gamma \sigma$  with the elements of  $G$  as free generators, in which a multiplication is defined by  $(a\sigma)(b\tau) = a\sigma(b)\sigma\tau$  for  $a, b \in \Gamma, \sigma, \tau \in G$ . Then  $\Gamma$  is a left  $\Delta(\Gamma, G)$ -module by setting  $(a\sigma) \cdot x = a\sigma(x)$  for  $a, x \in \Gamma, \sigma \in G$ . Let  $\phi$  be a homomorphism of  $\Delta(\Gamma, G)$  into  $\text{Hom}(\Gamma_\Lambda, \Gamma_\Lambda)$  defined by  $\phi(a\sigma)(x) = a\sigma(x)$  for  $a, x \in \Gamma, \sigma \in G$ . For  $u \in \Delta(\Gamma, G)$  and  $x \in \Gamma$ ,  $\phi(u)(x)$  will be denoted by  $u(x)$ . On the other hand  $ux$  will mean the product of  $u$  and  $x$  in  $\Delta(\Gamma, G)$ .  $t_G$  will denote  $\sum \sigma$  which is the sum of all elements of  $G$  in  $\Delta(\Gamma, G)$  and  $\phi(\sum \sigma)$  will be also written by  $t_G$ . By  $\Gamma^G$  we shall mean the fixed ring of  $\Gamma$  by  $G$ , i.e.  $\Gamma^G$  is the set of elements

of  $\Gamma$  left invariant by  $G$ .

**DEFINITION.** Let  $\Gamma, \Lambda$  and  $G$  be as above. Then  $\Gamma$  is called a *Galois extension of  $\Lambda$  relative to a group  $G$*  if the following conditions hold:

- (1) There exists an element  $z$  of  $\Gamma$  such that  $t_G(z)=1$ .
- (2)  $\Lambda = \Gamma^G$
- (3) There are elements  $x_1, x_2, \dots, x_n$  and  $y_1, y_2, \dots, y_n$  of  $\Gamma$  such that for all  $\sigma$  in  $G$

$$\sum_{i=1}^n x_i \sigma(y_i) = \begin{cases} 1 & \text{if } \sigma=1 \\ 0 & \text{if } \sigma \neq 1. \end{cases}$$

When  $\Gamma$  is a Galois extension of  $\Lambda$  relative to a group  $G$  we shall denote this situation by  $(\Gamma, \Lambda, G)$  and call  $x_1, x_2, \dots, x_n$  and  $y_1, y_2, \dots, y_n$  as above *Galois generators of  $(\Gamma, \Lambda, G)$* .

**Theorem 1.** *If  $\Gamma$  is a Galois extension of  $\Lambda$  relative to a group  $G$  and  $H$  is a subgroup of  $G$ , then  $\Gamma$  is a Galois extension of  $\Gamma^H$  relative to  $H$ . Moreover if  $H$  is a normal subgroup of  $G$ ,  $\Gamma^H$  is a Galois extension of  $\Lambda$  relative to the factor group  $G/H$ .*

*Proof.* Since  $\Gamma$  is a Galois extension of  $\Lambda$  relative to  $G$ , there is an element  $z_0$  of  $\Gamma$  such that  $t_G(z_0)=1$ . Now we shall show that there is an element  $z$  of  $\Gamma$  such that  $t_H(z)=1$ . Let  $\sigma_1, \sigma_2, \dots, \sigma_h$  be coset representatives for  $G/H$  where  $\sigma_1=1$ . Then we have  $t_H(\sum_{i=1}^h \sigma_i(z_0)) = t_G(z_0) = 1$  and  $\sum_{i=1}^h \sigma_i(z_0)$  is an element of  $\Gamma$ . Let  $x_1, x_2, \dots, x_n$  and  $y_1, y_2, \dots, y_n$  be Galois generators of  $(\Gamma, \Lambda, G)$ . Then we have for any  $\tau$  in  $H$

$$\sum_{i=1}^n x_i \tau(y_i) = \begin{cases} 1 & \text{if } \tau=1 \\ 0 & \text{if } \tau \neq 1. \end{cases}$$

Therefore  $\Gamma$  is a Galois extension of  $\Gamma^H$  relative to  $H$ .

Assume that  $H$  is a normal subgroup of  $G$ . It is clear that  $G/H$  is a finite group of automorphisms of  $\Gamma^H$  if we define the operation by  $(\sigma H)(x) = \sigma(x)$  for  $\sigma \in G, x \in \Gamma^H$  and that  $(\Gamma^H)^{G/H} = \Lambda$ . Set  $z_1 = \sum_{i=1}^h \sigma_i(z_0)$ . Then we have for  $k=1, 2, \dots, k$

$$\begin{aligned} \sum_{i=1}^n t_H(z_1 x_i) \sigma_k(t_H(y_i)) &= \sum_{i=1}^n \sum_{\tau, \rho \in H} \tau(z_1) \tau(x_i) \sigma_k \rho(y_i) \\ &= \sum_{i=1}^n \sum_{\tau, \rho \in H} \tau(z_1) \tau(x_i \tau^{-1} \sigma_k \rho(y_i)) \\ &= \begin{cases} 1 & \text{if } k=1 \\ 0 & \text{if } k \neq 1 \end{cases} \end{aligned}$$

where  $t_H(z_1 x_i)$  and  $t_H(y_i)$  ( $i=1, 2, \dots, n$ ) are elements of  $\Gamma^H$ . Therefore  $\Gamma^H$  is a Galois extension of  $\Lambda$  relative to  $G/H$ .

**Lemma 1.** *If  $\Gamma$  is a Galois extension of  $\Lambda$  relative to a group  $G$ , then  $\Lambda$  is a direct summand of  $\Gamma$  as  $\Lambda$ -module.*

Proof. Since  $t_G$  maps  $\Gamma$  onto  $\Lambda$ , it is clear that  $\Lambda$  is a direct summand of  $\Gamma$  as  $\Lambda$ -module.

**Lemma 2.** *Let  $\Gamma$  be a ring,  $G$  a group of automorphisms of  $\Gamma$  and  $\Lambda$  a subring of  $\Gamma$  which is contained in  $\Gamma^G$ . If there are elements  $x_1, x_2, \dots, x_n$  and  $y_1, y_2, \dots, y_n$  of  $\Gamma$  which satisfy the following condition (C): for all  $\sigma \in G$*

$$\sum_{i=1}^n x_i \sigma(y_i) = \begin{cases} 1 & \text{if } \sigma = 1 \\ 0 & \text{if } \sigma \neq 1, \end{cases}$$

*then  $\Gamma$  is a projective Frobenius extension of  $\Lambda$  with  $t_G$  as a Frobenius homomorphism, so that we have  $t_G \cdot \Gamma \cong \text{Hom}(\Gamma_\Lambda, \Gamma_\Lambda)$  as left  $\Lambda$ -right  $\Gamma$ -modules and  $t_G \cdot \Gamma$  is a free  $\Gamma$ -module with  $t_G$  as a generator. Moreover if  $\Lambda$  is a commutative ring and  $\Gamma$  is an algebra over  $\Lambda$ , then  $\Gamma$  is separable over  $\Lambda$ .*

Proof. Let  $x_1, x_2, \dots, x_n$  and  $y_1, y_2, \dots, y_n$  be elements of  $\Gamma$  which satisfy the condition (C). Then we have for all  $z$  in  $\Gamma$

$$\sum_{i=1}^n x_i t_G(y_i z) = \sum_{\sigma \in G} \left( \sum_{i=1}^n x_i \sigma(y_i) \right) \sigma(z) = z$$

and

$$\sum_{i=1}^n t_G(z x_i) y_i = \sum_{\sigma \in G} \sum_{j=1}^n \sigma(z) \sigma(x_j \sigma^{-1}(y_j)) = z$$

By Cor. 1 to Theorem 1 in [9],  $\Gamma$  is a projective Frobenius extension of  $\Lambda$  with  $t_G$  as a Frobenius homomorphism, so that we have  $t_G \cdot \Gamma \cong \text{Hom}(\Gamma_\Lambda, \Gamma_\Lambda)$ .

Now assume that  $\Lambda$  is a commutative ring and  $\Gamma$  is an algebra over  $\Lambda$ . We consider the element  $\sum_{i=1}^n x_i \otimes y_i^0$  in  $\Gamma \otimes_\Lambda \Gamma^0$ . Then we have for all  $x$  in  $\Gamma$

$$\begin{aligned} \sum_{i=1}^n x x_i \otimes y_i^0 &= \sum_{i,j=1}^n x_j t_G(y_j x x_i) \otimes y_i^0 = \sum_{i,j=1}^n x_j \otimes (t_G(y_j x x_i) y_i)^0 \\ &= \sum_{j=1}^n x_j \otimes x^0 y_j^0. \end{aligned}$$

A mapping  $\alpha$  of  $\Gamma$  into  $\Gamma \otimes_\Lambda \Gamma^0$  defined by  $\alpha(x) = \sum_{i=1}^n x x_i \otimes y_i^0$  for  $x \in \Gamma$  is a  $\Gamma \otimes_\Lambda \Gamma^0$ -homomorphism and splits whence  $\sum_{i=1}^n x_i y_i = 1$ . Since  $\Gamma$  is

$\Gamma \otimes_{\Lambda} \Gamma^0$ -projective,  $\Gamma$  is a separable algebra over  $\Lambda$ .

**Lemma 3.** *Let  $\Gamma$ ,  $\Lambda$  and  $G$  be as above.  $\Gamma$  is a Galois extensions of  $\Lambda$  relative to  $G$  if and only if the following conditions hold:*

- (a)  $t_G(\Gamma) = \Lambda$
- (b) *There are elements  $x_1, x_2, \dots, x_n$  and  $y_1, y_2, \dots, y_n$  of  $\Gamma$  such that for all  $\sigma$  in  $G$*

$$\sum_{i=1}^n x_i \sigma(y_i) = \begin{cases} 1 & \text{if } \sigma = 1 \\ 0 & \text{if } \sigma \neq 1. \end{cases}$$

*Proof.* It is trivial that the conditions (a) and (b) hold if  $\Gamma$  is a Galois extension of  $\Lambda$  relative to  $G$ . Conversely, assume that the conditions (a) and (b) hold. It follows from the condition (a) that there exists an element  $z$  of  $\Gamma$  such that  $t_G(z) = 1$ . Then we have  $x = xt_G(z) = t_G(xz)$  for any  $x$  in  $\Gamma^G$ . It is clear that  $\Lambda$  is contained in  $\Gamma^G$ , hence  $\Lambda = \Gamma^G$ . Therefore  $\Gamma$  is a Galois extension of  $\Lambda$  relative to  $G$ .

**Proposition 1.** *Let  $R$  be a commutative ring and  $\Gamma_i, \Lambda_i$  ( $i=1, 2$ ) algebras over  $R$  such that  $\Lambda_1 \otimes_R \Lambda_2$  is not zero. If  $\Gamma_i$  is a Galois extension of  $\Lambda_i$  relative to a group  $G_i$  for  $i=1, 2$ , then  $\Gamma_1 \otimes_R \Gamma_2$  is a Galois extension of  $\Lambda_1 \otimes_R \Lambda_2$  relative to the group  $G_1 \times G_2$ , where  $G_1 \times G_2$  is regarded as a group of automorphisms of  $\Gamma_1 \otimes_R \Gamma_2$  by means of  $(\sigma_1 \times \sigma_2)(x_1 \otimes x_2) = \sigma_1(x_1) \otimes \sigma_2(x_2)$  for  $\sigma_i \in G_i, x_i \in \Gamma_i$ .*

*Proof.* By Lemma 1,  $\Lambda_1 \otimes_R \Lambda_2$  is a direct summand of  $\Gamma_1 \otimes_R \Gamma_2$ . Therefore  $\Lambda_1 \otimes_R \Lambda_2$  is a subring of  $\Gamma_1 \otimes_R \Gamma_2$ , so that  $\Gamma_1 \otimes_R \Gamma_2 \neq 0$ . Let  $x_1^{(\epsilon)}, x_2^{(\epsilon)}, \dots, x_{n(\epsilon)}^{(\epsilon)}$  and  $y_1^{(\epsilon)}, y_2^{(\epsilon)}, \dots, y_{n(\epsilon)}^{(\epsilon)}$  be Galois generators of  $(\Gamma_i, \Lambda_i, G_i)$ . Then we have for all  $\sigma_1 \times \sigma_2$  in  $G_1 \times G_2$

$$\begin{aligned} & \sum_{k=1}^{n(1)} \sum_{j=1}^{n(2)} (x_k^{(1)} \otimes x_j^{(2)}) \{(\sigma_1 \times \sigma_2)(y_k^{(1)} \otimes y_j^{(2)})\} \\ &= \sum_{k=1}^{n(1)} \sum_{j=1}^{n(2)} x_k^{(1)} \sigma_1(y_k^{(1)}) \otimes x_j^{(2)} \sigma_2(y_j^{(2)}) \\ &= \begin{cases} 1 & \text{if } \sigma_1 \times \sigma_2 = 1 \\ 0 & \text{if } \sigma_1 \times \sigma_2 \neq 1 \end{cases} \end{aligned}$$

where  $x_k^{(1)} \otimes x_j^{(2)}$  and  $y_k^{(1)} \otimes y_j^{(2)}$  are elements of  $\Gamma_1 \otimes_R \Gamma_2$ . Since we have  $t_{G_1 \times G_2}(\Gamma_1 \otimes_R \Gamma_2) = \Lambda_1 \otimes_R \Lambda_2$ ,  $\Gamma_1 \otimes_R \Gamma_2$  is a Galois extensions of  $\Lambda_1 \otimes_R \Lambda_2$  relative to  $G_1 \times G_2$  from Lemma 3.

**2. Galois extensions over commutative rings**

We shall now study on Galois extensions over commutative rings.

**Lemma 4.** *Let  $\Gamma$  be a ring,  $G$  a group of automorphisms of  $\Gamma$  and  $\Lambda$  a subring of the fixed ring  $\Gamma^G$ . If  $\Gamma$  is a projective Frobenius extension of  $\Lambda$  with  $t_G$  as a Frobenius homomorphism, then the subring  $\Gamma \cdot t_G \cdot \Gamma$  of  $\Delta(\Gamma, G)$  is isomorphic to  $\text{Hom}(\Gamma_\Lambda, \Gamma_\Lambda)$ .*

*Proof.* Assume that  $\Gamma$  is a projective Frobenius extension of  $\Lambda$  with  $t_G$  as a Frobenius homomorphism. Then we have  $t_G \cdot \Gamma \cong \text{Hom}(\Gamma_\Lambda, \Gamma_\Lambda)$ . It follows from Prop. A. 1 in [1] that a mapping  $\mu : \Gamma \otimes_\Lambda \text{Hom}(\Gamma_\Lambda, \Gamma_\Lambda)$  into  $\text{Hom}(\Gamma_\Lambda, \Gamma_\Lambda)$  defined by  $\mu(z \otimes f)(x) = zf(x)$  for  $x, z \in \Gamma, f \in \text{Hom}(\Gamma_\Lambda, \Gamma_\Lambda)$  is an isomorphism. If  $\nu$  is a mapping of  $\Gamma \otimes_\Delta t_G \cdot \Gamma$  into  $\Delta(\Gamma, G)$  defined by  $\nu(x \otimes t_G y) = xt_G y$  for  $x, y \in \Gamma$ , then we have  $\mu = \phi\nu$ . Therefore  $\nu(\Gamma \otimes_\Delta t_G \cdot \Gamma) (= \Gamma \cdot t_G \cdot \Gamma)$  is isomorphic to  $\text{Hom}(\Gamma_\Lambda, \Gamma_\Lambda)$ .

**REMARK.** [cf. 7, 8] We can show by using Lemmas 2 and 4 that a ring  $\Gamma$  is a Galois extension of its subring  $\Lambda$  relative to a group  $G$  if and only if the following conditions hold :

- (a)  $t_G(\Gamma) = \Lambda$
- (b)  $\Gamma$  is a finitely generated projective right  $\Lambda$ -module,
- (c)  $\Delta(\Gamma, G)$  is isomorphic to  $\text{Hom}(\Gamma_\Lambda, \Gamma_\Lambda)$  by  $\phi$ .

Let  $R$  be a commutative ring. If  $M$  is a finitely generated projective  $R$ -module,  $M \otimes_R R_{\mathfrak{p}}$  is  $R_{\mathfrak{p}}$ -free for all non zero prime ideals  $\mathfrak{p}$  of  $R$ . If  $R_{\mathfrak{p}}$ -module  $M \otimes_R R_{\mathfrak{p}}$  is of rank  $n$  for all non zero prime ideals  $\mathfrak{p}$  of  $R$ , we call  $n$  the rank of  $M$  and denote it by  $\text{rank}_R M$  [cf. 3].

**Proposition 2.** *Let  $\Gamma$  be a ring and  $R$  a subring of  $\Gamma$  which is an integral domain and is contained in the center of  $\Gamma$ . Then  $\Gamma$  is a Galois extension of  $R$  relative to a group  $G$  if and only if the following conditions hold :*

- (a)  $\text{rank}_R \Gamma = |G|$
- (b)  $t_G(\Gamma) = R$
- (c)  $\Gamma$  is a projective Frobenius extension of  $R$  with  $t_G$  as a Frobenius homomorphism.

*Proof.* Assume that  $\Gamma$  is a Galois extension of  $R$  relative to  $G$ . Then it is clear that the conditions (b) and (c) hold. Now we shall prove that the condition (a) holds.  $\Gamma \otimes_R R_{\mathfrak{p}}$  is a free  $R_{\mathfrak{p}}$ -module for all non zero prime ideal  $\mathfrak{p}$  of  $R$ . Set  $\text{rank}_{R_{\mathfrak{p}}} \Gamma \otimes_R R_{\mathfrak{p}} = n$ . Then we have  $\text{rank}_{R_{\mathfrak{p}}}$

$\text{Hom}(\Gamma \otimes_R R_p, \Gamma \otimes_R R_p) = n^2$  and  $\text{rank}_{R_p} \Delta(\Gamma \otimes_R R_p, G) = n|G|$ . It follows from Remark that  $\Delta(\Gamma \otimes_R R_p, G)$  is isomorphic to  $\text{Hom}(\Gamma \otimes_R R_p, \Gamma \otimes_R R_p)$ , so that we have  $n = |G|$ . By the definition of rank of projective module, we get  $\text{rank}_R \Gamma = |G|$ .

Conversely, assume that the conditions (a), (b) and (c) hold. Then by Lemma 4  $\Gamma \cdot t_G \cdot \Gamma$  is isomorphic to  $\text{Hom}_R(\Gamma, \Gamma)$  by  $\phi$  where  $\Gamma \cdot t_G \cdot \Gamma$  is a subring of  $\Delta(\Gamma, G)$ . By the condition (a), the factor  $R$ -module  $\Delta(\Gamma, G)/\Gamma \cdot t_G \cdot \Gamma$  is a torsion module. Since the  $R$ -module  $\Delta(\Gamma, G)$  is torsion free,  $\Delta(\Gamma, G)$  is isomorphic to  $\text{Hom}_R(\Gamma, \Gamma)$ . It follows from the condition (b) and Remark that  $\Gamma$  is a Galois tension of  $R$  relative to  $G$ .

**Lemma 5.** *Let  $S$  be a commutative ring with no idempotent other than 0 or 1 and  $R$  a subring of  $S$ . Then  $S$  is a Galois extension of  $R$  relative to a group  $G$  if and only if the following conditions hold:*

- (a)  $R = S^G$
- (b)  $S$  is a separable algebra over  $R$
- (c)  $S$  is a finitely generated projective module over  $R$ .

Proof. See Theorem 1.3 in [5].

**Lemma 6.** *Let  $\Gamma_1$  be a ring,  $\Gamma_2$  a subring of  $\Gamma_1$  and  $G$  a finite group of automorphisms of  $\Gamma_1$  and  $\Gamma_2$ . If the fixed rings of  $\Gamma_1$  and  $\Gamma_2$  by  $G$  are the same ring  $\Lambda$  and there are elements  $x_1, x_2, \dots, x_n$  and  $y_1, y_2, \dots, y_n$  of  $\Gamma_2$  such that for all  $\sigma$  in  $G$*

$$\sum_{i=1}^n x_i \sigma(y_i) = \begin{cases} 1 & \text{if } \sigma = 1 \\ 0 & \text{if } \sigma \neq 1, \end{cases}$$

then we have  $\Gamma_1 = \Gamma_2$ .

Proof. We have for all  $z$  in  $\Gamma_1$

$$\sum_{i=1}^n x_i t_G(y_i z) = \sum_{i=1}^n \sum_{\sigma \in G} x_i \sigma(y_i) \sigma(z) = z.$$

Since  $t_G(y_i z)$  is in  $\Lambda$  for  $i=1, 2, \dots, n$ ,  $\Gamma_1$  is generated by  $x_1, x_2, \dots, x_n$  over  $\Lambda$ , hence  $\Gamma_1 = \Gamma_2$ .

**Theorem 2.** *Let  $\Gamma$  be a ring such that its center  $C$  has no idempotent other than 0 or 1 and  $R$  a subring of  $C$ . Then  $\Gamma$  is a Galois extension of  $R$  relative to a group  $G$  if and only if  $\Gamma$  is a Galois extension of  $C$  relative to  $H$  where  $H = \{\sigma \mid \sigma \in G, \sigma(x) = x \text{ for all } x \in C\}$  and  $C$  is a Galois extension of  $R$  relative to the factor group  $G/H$ .*

Proof. Necessity. Assume that  $\Gamma$  is a Galois extension of  $R$  relative to a group  $G$ . Then  $\Gamma$  is separable over  $R$ , so that its center  $C$  is

separable over  $R$  and  $C$  is a direct summand of  $\Gamma$  as a  $R$ -module. Since  $\Gamma$  is  $R$ -projective,  $C$  is  $R$ -projective. By Lemma 5,  $C$  is a Galois extension of  $R$  relative to  $G/H$ . Since we have  $(\Gamma^H)^{G/H} = R = C^{G/H}$ , we get  $C = \Gamma^H$  by Lemma 6, so that  $\Gamma$  is a Galois extension of  $C$  relative to  $H$ .

Sufficiency. Assume that  $\Gamma$  is a Galois extension of  $C$  relative to  $H$  and  $C$  is a Galois extension of  $R$  relative to  $G/H$ . Then we have  $t_G(\Gamma) = t_{G/H}(t_H(\Gamma)) = t_{G/H}(C) = R$ . Let  $x_1, x_2, \dots, x_m$  and  $y_1, y_2, \dots, y_m$  be Galois generators of  $(\Gamma, C, H)$  and  $v_1, v_2, \dots, v_n$  and  $w_1, w_2, \dots, w_n$  Galois generators of  $(C, R, G/H)$ . Then we have for all  $\tau$  in  $H$

$$\begin{aligned} \sum_{j=1}^n \sum_{i=1}^m x_i v_j \tau(w_j y_i) &= \sum_{j=1}^n \sum_{i=1}^m x_i v_j w_j \tau(y_i) = \sum_{i=1}^m x_i \tau(y_i) \\ &= \begin{cases} 1 & \text{if } \tau = 1 \\ 0 & \text{if } \tau \neq 1 \end{cases} \end{aligned}$$

and for all  $\sigma$  in  $G$ ,  $\sigma \notin H$

$$\sum_{j=1}^n \sum_{i=1}^m x_i v_j \sigma(w_j y_i) = \sum_{i=1}^m \sum_{j=1}^n x_i v_j \sigma(w_j) \sigma(y_i) = 0$$

If we set  $x_{i,j} = x_i v_j$  and  $y_{i,j} = w_j y_i$ , then we obtain for all  $\sigma$  in  $G$

$$\sum_{i=1}^m \sum_{j=1}^n x_{i,j} \sigma(y_{i,j}) = \begin{cases} 1 & \text{if } \sigma = 1 \\ 0 & \text{if } \sigma \neq 1. \end{cases}$$

Therefore  $\Gamma$  is a Galois extension of  $R$  relative to  $G$ .

**Lemma 6.** *Let a ring  $\Gamma$  be a Galois extension of its center  $C$  relative to a group  $G$ . Then if  $|G| = n$ , we have  $n \cdot C = C$ .*

Proof. By Lemma 2 and Theorem 2, 1 in [2],  $\Gamma \otimes_{\mathcal{C}} \Gamma^0$  is isomorphic to  $\text{Hom}_C(\Gamma, \Gamma)$ . By Remark,  $\Gamma \otimes_{\mathcal{C}} \Gamma^0$  is isomorphic to  $\Delta(\Gamma, G)$ . Since  $\Gamma \otimes_{\mathcal{C}} \Gamma^0$  is a Galois extension of  $\Gamma \otimes_{\mathcal{C}} 1$ ,  $\Delta(\Gamma, G)$  is a Galois extension of  $\Gamma$ . If we write  $\Delta$  for  $\Delta(\Gamma, G)$ ,  $\Delta \otimes_{\Gamma} \Delta$  is a two sided  $\Delta$ -module by setting  $z(x \otimes y) = zx \otimes y$  and  $(x \otimes y)z = x \otimes yz$  for  $x \otimes y \in \Delta \otimes_{\Gamma} \Delta$ ,  $z \in \Delta$ . Let  $x_1, x_2, \dots, x_n$  and  $y_1, y_2, \dots, y_n$  be Galois generators of  $\Delta(\Gamma, G)$ . Then we have for all  $z$  in  $\Delta$

$$\begin{aligned} z \left( \sum_{i=1}^n x_i \otimes y_i \right) &= \sum_{i=1}^n z x_i \otimes y_i = \sum_{i,j=1}^n x_j h(y_j z x_i) \otimes y_i \\ &= \sum_{i,j=1}^n x_j \otimes h(y_j z x_i) y_i = \left( \sum_{j=1}^n x_j \otimes y_j \right) z \end{aligned}$$

where  $\sum_{i=1}^n x_i \otimes y_i$  is the element of  $\Delta \otimes_{\Gamma} \Delta$  and  $h$  is a Frobenius homomorphism of  $\Delta/\Gamma$ . If we set  $\sum_{i=1}^n x_i \otimes y_i = \sum_{\sigma, \tau \in G} z_{\sigma, \tau} \sigma \otimes \tau$  ( $z_{\sigma, \tau} \in \Gamma$ ), then we get



for all  $z$  in  $\Gamma$

$$\sum_{\sigma, \tau \in G} z z_{\sigma, \tau} \sigma \otimes \tau = \sum_{\sigma, \tau \in G} z_{\sigma, \tau} \sigma \otimes \tau z = \sum_{\sigma, \tau \in G} z_{\sigma, \tau} \sigma \tau(z) \sigma \otimes \tau$$

so that  $z z_{\sigma, \tau} = z_{\sigma, \tau} \sigma \tau(z)$  for all  $\sigma, \tau$  in  $G$  and all  $z$  in  $\Gamma$ . Therefore  $z_{1,1}$  is contained in  $C$ . Since we have for all  $\rho$  in  $G$

$$\rho \sum_{\sigma, \tau \in G} z_{\sigma, \tau} \sigma \otimes \tau = \sum_{\sigma, \tau \in G} \rho(z_{\sigma, \tau}) \rho \sigma \otimes \tau = \sum_{\tau, \rho \in G} \rho(z_{\rho^{-1} \delta, \tau}) \delta \otimes \tau$$

and on the other hand,

$$\rho \sum_{\sigma, \tau \in G} z_{\sigma, \tau} \sigma \otimes \tau = \sum_{\sigma, \tau \in G} z_{\sigma, \tau} \sigma \otimes \tau \rho = \sum_{\sigma, \mu \in G} z_{\sigma, \mu \rho^{-1}} \sigma \otimes \mu,$$

we have  $\rho(z_{\rho^{-1} \sigma, \tau}) = z_{\sigma, \tau \rho^{-1}}$  for all  $\sigma, \tau, \rho$  in  $G$ . Hence  $z_{1,1} = z_{\sigma, \sigma^{-1}}$  for all  $\sigma$  in  $G$ . It follows from the equation  $\sum_{i=1}^n x_i y_i = 1$  that  $\sum_{\sigma, \tau \in G} z_{\sigma, \tau} \sigma \tau$  is the unit element, so that  $1 = \sum_{\sigma \in G} z_{\sigma, \sigma^{-1}} = n z_{1,1}$ , which completes the proof.

**Theorem 3.** *Let  $\Gamma$  be a Galois extension of its center  $C$  relative to a group  $G$ . If all element of  $G$  are inner automorphisms of  $\Gamma$ , then  $\Gamma$  is generated by units of  $\Gamma$  over  $C$ .*

*Proof.* Let  $u_\sigma$  ( $\sigma \in G$ ) be a unit in  $\Gamma$  which induces  $\sigma$ . If we set  $u_{\sigma\tau}^{-1} u_\sigma u_\tau = c_{\sigma, \tau}$ , then  $\{c_{\sigma, \tau}\}$  ( $\sigma, \tau \in G$ ) is a factor set of units in  $C$ . If we denote by  $\Gamma'$  a subring of  $\Gamma$  which is generated by all  $u_\sigma$  with  $\sigma$  in  $G$  over  $C$ , then  $\Gamma$  is a homomorphic image of a generalized group ring of  $G$  over  $C$  with the factor set  $\{c_{\sigma, \tau}\}$ .  $\Gamma'$  is a central separable  $C$ -algebra whence this generalized group ring is a separable  $C$ -algebra by Lemma 4 in [6]. Then, by Theorem 3 in [2], we have  $V_\Gamma(V_\Gamma(\Gamma')) = \Gamma'$  where  $V_\Gamma(\Lambda)$  is the commutor ring of a ring  $\Lambda$  in  $\Gamma$ . On the other hand, we get  $V_\Gamma(V_\Gamma(\Gamma)) = \Gamma$  whence  $V_\Gamma(\Gamma) = C$ . Therefore  $\Gamma$  is generated by the units  $u_\sigma$  ( $\sigma \in G$ ) in  $\Gamma$  over  $C$ .

**EXAMPLE.** We shall give here an example of Galois extension satisfying the assumptions in Theorem 3. Let  $R$  be the ring of quotients of the ring of rational integers with respect to the prime ideal (3) and  $D$  a quaternion algebra over  $R$  with basis  $1, i, j$  and  $k$ . We denote  $1, i, j$  and  $k$  by  $x_1, x_2, x_3$  and  $x_4$ .

Now if  $G$  is the group of inner automorphisms  $\sigma_i$  of  $D$  which is induced by  $x_i$  ( $i=1, 2, 3, 4$ ), then  $D$  is a Galois extension of  $R$  relative to  $G$ . For we have for all  $j$

$$\sum_{i=1}^4 x_i \sigma_j(x_i^{-1}) = \begin{cases} 4x_1 & (j=1) \\ 0 & (j \neq 1). \end{cases}$$

## References

- [1] M. Auslander and O. Goldman: *Maximal orders*, Trans. Amer. Math. Soc. **97** (1960), 1-24.
- [2] —————: *The Brauer group of a commutative ring*, Trans. Amer. Math. Soc. **97** (1960), 367-409.
- [3] N. Bourbaki: *Algèbre commutative* chap. I-II, Paris, 1962.
- [4] H. Cartan and S. Eilenberg: *Homological algebra*, Princeton University Press, 1956.
- [5] S. U. Chase, D. K. Harrison and A. Resenberg: *Galois theory and Galois cohomology of commutative rings*, Mem. Amer. Math. Soc. No. 52 (1964).
- [6] M. Harada: *Some criteria for heredity of crossed products*, Osaka J. Math. **1** (1964), 69-80.
- [7] T. Kanzaki: *On commutator ring and Galois theory of separable algebras*, Osaka J. Math. **1** (1964), 103-115.
- [8] —————: *On Galois extension of rings* (to appear).
- [9] T. Onodera: *Some studies on projective Frobenius extensions*, J. Fac. Sci. Hokkaidō Univ. **18** (1964), 89-107.

*Added in proof.* After submitting this paper I learned that Theorem 3 has been obtained independently by Frank R. DeMeyer in his paper which will appear in this Journal.

