2. A Quadratic Extension

By Takasi NAGAHARA
Department of Mathematics, Okayama University

(Comm. by Kenjiro SHODA, M. J. A., Jan. 12, 1971)

Throughout this paper A will be a commutative ring with an identity element 1, and B a subring of A containing the identity element 1 of A.

In [2], K. Kishimoto proved a theorem concerning quadratic extensions of commutative rings which is as follows: Assume that B contains a field of characteristic $\neq 2$ (containing 1). Let $A=B+Bd$ and $d^2 \in B$. Let A be B-projective and $\{1\otimes 1, 1\otimes d\}$ a free B_M-basis of A_M for every maximal ideal M of B where B_M is a localization of B at M and $A_M=B_M \otimes_B A$. Then, A/B is a Galois extension with a Galois group of order 2 if and only if d^2 is inversible in B.

The purpose of this note is to prove the following theorem which contains the above Kishimoto's result.[1)]

Theorem. *Let $A=B+Bd \supsetneqq B$ and $d^2 \in B$. Then, A/B is a Galois extension if and only if $\{1, d\}$ is a free B-basis of A and $2\cdot 1$, d^2 are inversible in B.*

First we shall prove the following

Lemma 1. *Let $A=B+Ba \supsetneqq B$, and let A/B be a Galois extension with a Galois group $\mathfrak{G}$. Then*

(1) *$\mathfrak{G}$ is of order 2.*

(2) *For $\sigma \neq 1 \in \mathfrak{G}$, $a-\sigma(a)$ is inversible in A.*

(3) *$\{1, a\}$ is a free B-basis of A.*

(4) *If $a^2=b_0+b_1a$ $(b_0, b_1 \in B)$ then $2a-b_1$ is inversible in A.*

Proof. Let $\sigma \neq 1 \in \mathfrak{G}$. We suppose that $a-\sigma(a)$ is not inversible in A. Then there exists a maximal ideal M_0 of A such that $M_0 \ni a-\sigma(a)$. For an arbitrary element $u+va$ of A $(u, v \in B)$, we have $u+va-\sigma(u+va)=v(a-\sigma(a)) \in M_0$. This contradicts to the result of [1, Theorem 1.3 (f)]. Hence $a-\sigma(a)$ is inversible in A. If $r+sa=0$ $(r, s \in B)$ then $r+s\sigma(a)=0$; whence $s(a-\sigma(a))=0$ which implies $s=0$ and $r=0$. This shows that $\{1, a\}$ is a free B-basis of A. Let n be the order of $\mathfrak{G}$. Then by [1, Theorem 1.3 (e)], $A\otimes_B A$ is a free $(A\otimes 1)$-module of rank n. Since $A\otimes A=(A\otimes 1)(1\otimes 1)+(A\otimes 1)(1\otimes a)$, it follows that $n=2$. Then $a+\sigma(a)$, $a\sigma(a) \in B$, and $a^2=(a+\sigma(a))a-a\sigma(a)$. Hence if $a^2=b_1a+b_0$

1) Let $A=B+Bd$. Then, it is proved easily that $\{1, d\}$ is a free B-basis of A if and only if $\{1\otimes 1, 1\otimes d\}$ is a free B_M-basis of A_M for every maximal ideal M of B.

$(b_1, b_0 \in B)$ then $b_1 = a + \sigma(a)$, and thus we have $2a - b_1 = a - \sigma(a)$ which is inversible in A.

Next, we shall prove the following

Lemma 2. *Let $A = B + Ba \supsetneqq B$. Then, A/B is a Galois extension if and only if there holds that*

(1) *$\{1, a\}$ is a free B-basis of A, and*

(2) *if $a^2 = b_0 + b_1 a$ $(b_0, b_1 \in B)$ then $2a - b_1$ is inversible in A.*

Proof. If A/B is a Galois extension then there hold (1) and (2) by Lemma 1. We assume (1) and (2). Let X be an indeterminate and $f(X) = X^2 - b_1 X - b_0$. Then the B-algebra $B[X]/(f(X))$ is isomorphic to A under the mapping $u + v\bar{X} \to u + va$ $(u, v \in B)$ where $\bar{X} = X + (f(X))$. Let $f'(X)$ be the derivative of $f(X)$. Then $f'(a) = 2a - b_1$ is inversible in A. Hence $f'(\bar{X})$ is inversible in $B[\bar{X}]$. Therefore it follows from [3, Theorem 2] that A/B is a Galois extension.[2)]

Now, we shall prove our theorem.

Proof of Theorem. We assume that A/B is a Galois extension. Then by Lemma 2, $\{1, d\}$ is a free B-basis of A and $2d$ is inversible in A; whence $2 \cdot 1$ and d^2 is inversible in B. Conversely, if $\{1, d\}$ is a free B-basis of A and $2 \cdot 1$, d^2 are inversible in B, then $2d$ is inversible in A; and hence by Lemma 2, A/B is a Galois extension.

References

[1] S. U. Chase, D. K. Harrison, and A. Rosenberg: Galois theory and Galois cohomology of commutative rings. Mem. Amer. Math. Soc., No. 52, 15–33 (1965).

[2] K. Kishimoto: Note on quadratic extensions of rings. J. Fac. Sci. Shinshu Univ., Matsumoto, Japan, **5**, 25–28 (1970).

[3] T. Nagahara: Characterization of separable polynomials over a commutative ring. Proc. Japan Acad., **46**, 1011–1015 (1970).

2) Let $\mathfrak{G}_1$ be a Galois group of A/B. Then $\sigma(a) = b_1 - a$ for $\sigma \neq 1 \in \mathfrak{G}_1$. Hence if $\mathfrak{G}_2$ is a Galois group of A/B then $\mathfrak{G}_2 = \mathfrak{G}_1$. For $2a - b_1$, we have three casis: (i) $2 \cdot 1 \neq 0$ and is not inversible in A (and so in B); (ii) $2 \cdot 1$ is inversible in A; (iii) $2 \cdot 1 = 0$. In case (ii), set $u = (2a - b_1)^2$, then $u \in B$ and A is B-algebra isomorphic to $B[X]/(X^2 - u)$. In case (iii), set $v = (b_1^{-1}a)^2 - b_1^{-1}a$, then $v \in B$ and A is B-algebra isomorphic to $B[X]/(X^2 - X - v)$.