Mathematical Journal of Okayama University

Volume 12, *Issue* 1 1963 *Article* 2

DECEMBER 1963

Automorphisms of algebras and a theorem concerning norms

Katsuhiko Masuda[*]

[*] Okayama University

AUTOMORPHISMS OF ALGEBRAS AND A THEOREM CONCERNING NORMS

KATSUHIKO MASUDA

When a new theorem is obtained in the theory of non-commutative algebras as a generalization of a well-known theorem in the theory of fields, the following question arises rather naturally: What a thing new does the generalization introduce into the proper theory of fields? Sometimes one can find an answer to it readily in a proof to the generalization. This paper will be devoted to obtaining such a proof to the following theorem:

Theorem 1. *Let K be a field, A a normal simple algebra over K of finite rank, σ a ring-automorphism of A, B the set of elements that σ keeps unchanged, and k the intersection $B\cap K$ of B and K. Suppose that the rank $[K:k]$ of K over k is finite and BK is simple. Then, there exists, for each simple subring H of A containing B, a ring-automorphism τ of A, such that H coincides with the set of elements of A that τ keeps unchanged. Conversely, let μ be an arbitrary ring-automorphism of A that keeps each element of B unchanged, then the set M of elements of A that μ keeps unchanged is a simple ring.*

The new point of this theorem lies in that it does not exclude the case when k is a Galoisfeld, which was open hitherto. When k contains infinitely many number of elements, it coincides with the known generalizations[1] of Bortfeld's theorem[2], due to Nagahara, Tominaga, and Inatomi, up to formulation of the condition. Our proof is self-contained, and we do not need the Galois theory of rings as its prerequisite.

Chapter I, consisting of four sections, is devoted to reducing the proof of Theorem 1 into a proof of a theorem (Theorem 3) belonging to the proper scope of the theory of fields. Chapter II, consisting of three sections, is devoted to proving Theorem 3. These two chapters are independent to each other except the point that combining them furnishes the proof to Theorem 1, our main theorem. In §§1–2, we shall give a lemma (Lemma 1) and a theorem (Theorem 2). In §3, we shall prove the last part of Theorem 1, and reduce the proof of the rest part to a proof to a certain special case (stated in Lemma 4). In §4, we shall complete the desired reduction.

In §5, we shall study polynomials and simple extension of fields. In §6, we shall study the form that gives the norm mapping. After preparations in

[1] Cf. [2] and [3]. We consider only the case that $[A:K]<\infty$, though the case that $[A:K]=\infty$ is disscussed in these papers.

[2] Cf. [1].

§§ 5–6, we shall prove Theorem 3, in § 7, and complete the proof of Theorem 1.

Chapter 1. Ring-Automorphisms of Algebras.

1 Lemma.

Lemma 1. *Let k be a field, K a finite algebraic extension field of k, separable and Galois over k, A a ring that contains K in its center and is of finite rank over K, and B a subring of A having k as its intersection $B\cap K$ with K. Suppose that BK is simple. Then, for an arbitrary subring H of BK containing B there holds that H is simple, BK is isomorphic with the tensor product $H\otimes_L K$ of H and K over the intersection L of H and K, $H=BL$, and, moreover, H is isomorphic with the tensor product $B\otimes_k L$ of B and L over k.*

Proof. Let H be as stated in the lemma. As, from the supposition, BK is simple and K is contained by the center of A, H can not have the radical, and the center W of BK is a field. As W coincides with the centralizer of B considered in BK, the center V of H is the intersection $H\cap W$ of H and W, so $W\supset V\supset K$. As W is an extension field of K of finite rank over K, V is a field. Then H is simple.

Obviously, $V\cap K=H\cap K=L$. As K/L is separable and Galois, VK is isomorphic with the tensor product $V\otimes_L K$ of V and K over L. On the other hand, as K/L is separable, the tensor product $H\otimes_L K$ of H and K over L is semisimple, and so, the center of HK coincides with the natural image of the center of $H\otimes_L K$. The center of $H\otimes_L K$ coincides with $V\otimes_L K\cong VK\subset W$. Therefore, the kernel of the natural mapping of $H\otimes_L K$ onto $HK=BK\subset A$ consists only of 0, so $BK\cong H\otimes_L K$, and $W=VK$.

Let F denote BL. As F is a subring of BK containing B, from the above proof it follows that F is simple. Obviously, $H\supset F$, and $F\cap K=L$. Applying the above proof to F in place of H, we obtain that $BK=FK$ is isomorphic with the tensor product $F\otimes_L K$ of F and K over L. Then we obtain $[H:L]\cdot[K:L]=[BK:L]=[F:L]\ [K:L]$. Hence $[H:L]=[F:L]$, so $H=F\cong B\otimes_k L$, q. e. d..

2. The subring charactrized by σ^n. Let K be a field, A a normal simple algebra over K of finite rank, σ a ringautomorphism of A, B the subring of A consisting of elements of A that σ keeps unchanged, and k the intersection of B and K. Suppose that the rank of K over k is finite. Then it holds

Theorem 2. *The set of all elements of A that σ^n keeps unchanged coincides with BK, where we denote the rank $[K:k]$ of K over k by n.*

Proof. Let $\overline{K}$ be an extension field of k equivalent witn K/k, and let $\overline{A}$

denote the tensor product of A and $\bar{K}$ over k. As, from the supposition, K/k is separable, $\bar{A}$ is semisimple, having $K\otimes_k\bar{K}$[3] as its center. There exists a set of n mutually orthogonal idempotent $e_1, e_2, \cdots, e_n$ belonging to the center of $\bar{A}$, such that $1=e_1+e_2+\cdots+e_n$. We denote $\bar{A}e_i(i=1, 2, \cdots, n)$ by $\bar{A}_i$. Each $\bar{A}_i$ is isomorphic with A. As σ keeps each element of k invariant, there exists a ringautomorphism $\bar{\sigma}$ of $\bar{A}$ satisfying

$$(1) \qquad (a\otimes\alpha)^{\bar{\sigma}}=a^{\sigma}\otimes\alpha \qquad\qquad (a\otimes\alpha\in\bar{A};\ a\in A,\ \alpha\in\bar{K}).$$

Applying a suitable permutation to the suffices, if necessary, we can, as is well known, suppose that

$$e_1^{\bar{\sigma}}=e_2,\ e_2^{\bar{\sigma}}=e_3,\ \cdots,\ e_n^{\bar{\sigma}}=e_1.$$

From now on, we suppose it, without any loss of the generality of our proof. Obviously, the set of all elements of $\bar{A}$ that $\bar{\sigma}$ keeps unchanged coincides with $B\otimes_k\bar{K}$. $\bar{\sigma}^n$ keeps each e_i with $i=1, 2, \cdots, n$ unchanged, induces a ring-automorphism of $\bar{A}^i$. Then an arbitrary element $\bar{a}$ of $\bar{A}$ is kept by $\bar{\sigma}$ unchanged, if and only if $\bar{a}$ can be written as $\bar{a}=\bar{a}e_1+(\bar{a}e_1)^{\bar{\sigma}}\cdots+(\bar{a}e_1)^{\bar{\sigma}^{n-1}}$ and $\bar{a}e_1$ is kept by $\bar{\sigma}^n$ unchanged. Then the projection of $B\otimes_k\bar{K}$ into $\bar{A}_i$ coincides with the set of the elements of $\bar{A}_i$ that $\bar{\sigma}$ keeps unchanged, and so we obtain that the direct sum

$$(B\otimes_k\bar{K})\mathrm{e}_1+(B\ \otimes_k\bar{K})\mathrm{e}_2+\cdots+(B\otimes_k\bar{K})\mathrm{e}_n$$

of $(B\otimes_k\bar{K})e_i\subset\bar{A}$ with $i=1, 2, \cdots, n$ coincides with the set M of the elements of $\bar{A}$ that $\bar{\sigma}^n$ keeps unchanged. Therefore,

$$M=B(K\otimes_k\bar{K})=(BK)\otimes_k\bar{K}\subset\bar{A}=A\otimes_k\bar{K}.$$

As BK coincides with the intersection of A and $(BK)\otimes_k\bar{K}$, we obtain $A\cap M=BK$, which certifies the theorem, q. e. d..

3. **Reduction 1.** Let K be a field, A a normal simple algebra of finite rank over K. Let σ be a ring-automorphism of A, B the subring of A consisting of the elements of A that σ keeps unchanged, and k the intersection $B\cap K$ of B and K. Suppose that the rank $n=[K:k]$ of K over k is finite. Then σ^n is an inner automorphism of A, and there exists a regular element s of A such that

$$(2) \qquad a^{\sigma^n}=sas^{-1} \qquad\qquad (a\in A).$$

Obviously, $sss^{-1}=s$, and so, from Theorem 2, it follows

$$(3) \qquad s\in BK.$$

The subring $K[s]$ of A generated dy s over K is contained by the center U of BK, and BK coincides with the centralizer of $K[s]$ considered in A. From now on, throughout Chapter I, we suppose that BK is simple. Then

[3] Cf. [4].

U is a finite algebraic extension field of K, and $K[s]$ is a field: $K[s]=K(s)$. Then as is easily seen, $K(s)$ coincides with U, which we state as

Lemma 2. *Let s be a regular element of A satisfying* (2), *and suppose that BK is simple. Then $K[s]$ is a field and coinsides with the center U of BK.*

Let a be an,arbitrary element of A. Obviously,

$$s^{\sigma}a^{\sigma}(s^{\sigma})^{-1}=(sas^{-1})^{\sigma}=(a)^{\sigma^{n+1}}=(a^{\sigma})^{\sigma n}=sa^{\sigma}s^{-1}, \tag{4}$$

and thus s and s^{σ} determine the same inner automorphism of A, so, we obtain

$$\zeta=s^{\sigma}s^{-1}\in K.$$

Then, $N_{K/k}\zeta=1$, and, as K/k is cyclic, there exists a regular element η of K such that

$$\zeta^{-1}=\eta^{-1}\eta^{\sigma}.$$

Let s_0 denote $s\eta$. As easily seen, s_0 belongs to the intersection of B and $K(s)$, and satisfies (2). From Lemma 2 follows $K(s_0)=U$. Let U_0 denote the intersection $U\frown B$ of U and B. Obviously, U_0 coincides with the center of B, and there holds $U_0\frown K=k$. As K/k is separable and Galois,

$$[U:U_0]\,[U_0:k]=[K:k]\,[U_0:k]=[K(s_0):k]=[K:k]\,[k(s_0):k],$$

hence, $[U_0:k]=[k(s_0):k]$, and $U_0=k(s_0)$, which we state as

Lemma 3. *Under the supposition of Lemma* 2, *there exists a regular element s_0 of the center U_0 of B such that s_0 satisfies* (2) *and generates U_0 over k.*

Lemma 4. *Let τ be a ring-automorphism of A keeping every element of B unchanged. Let B_τ be the set of the elements of A that τ keeps unchanged, then B_τ is simple.*

Proof. Let k_τ denote the intersection $B_\tau\frown K$ of B_τ and K. The rank m of K over k is a divisor of n. From Theorem 2 it follows that $B_\tau K$ is the set of the elements of A that τ^m keeps unchanged. Obviously, τ^m is an inner automorphis m of A, and there exists a regular element t of A such that

$$a^{\tau^m}=tat^{-1} \qquad (a\in A).$$

As, from the supposition, τ keeps each element of B unchanged, t belongs to the center of $U=K(s_0)$, so, t generates a field over K. Obviously, $B_\tau K$ is the centralizer of $K(t)$. Hence $B_\tau K$ is simple and has $K(t)$ as its center. Applying Lemma 1 to K/k_τ and $B_\tau K$, we obtain that B_τ is simple, q. e. d..

Let H be an arbitrary simple subring of A containing B. Let B' denote the intersection $H\frown BK$ of H and BK, k' the intersection $B'\frown K$ of B' and K, and m' the rank $[k':k]$ of k' over k. Then it follows readily from Lemma 1, that B' is simple and coincides with the set of the elements of A that $\sigma'=\sigma^{m'}$ keeps unchanged. Considering B', k', and σ', in place of B, k, and σ, we obtain the following

Lemma 5. *For the proof of the existence of* τ *for* H *as stated in Theorem* 1, *it is sufficient that we give a proof to it under the supposition of* $H\cap BK=B$.

4. Reduction II. Let H be a simple subring of A which contains B and whose intersection $H\cap BK$ with BK coincides with B. Then, obviously, $H\cap K=B\cap K=k$. The centralizer V of H considered in A is contained by $K(s_0)$, is algebraic simple extension field of k, and coincides with the center W of HK; $V=W$. The center Z of H coincides with the intersection $H\cap W$. Obiously, $H\cap W=H\cap BK\cap W=B\cap W=B\cap K(s_0)\cap W=k(s_0)\cap W$. So, Z is an algebraic simple extension field of k: there exists a non-zero element t_0 of Z such that $Z=k(t_0)$. From Lemma 1 it follows $W=K(t_0)$, and HK is isomorphic with the tensor product $H\otimes_k K$ of H and K over k. Therefore, there exists a ringautomorphism σ^* of HK such that

$$(5)\qquad h^{\sigma^*}=h,\ \alpha^{\sigma^*}={}^{\alpha K}_{\sigma}\qquad (h\in H, \alpha\in K),$$

where we denote the restriction of σ into K by σ_K. Let f be an arbitrary regular element of A. We denote the inner automorphism of A given by the mapping $a\rightarrow faf^{-1}(a\in A)$ by f^*. Obviously, $\sigma^*\sigma^{-1}$ induces an inner automorphism of HK. Hence there exists a regular element u of HK such that the restriction of u^* into HK coincides with $\sigma^*\sigma^{-1}$. We denote the ringautomorphism $u^*\sigma$ of A by μ. So, the restriction of μ into HK coincides with σ^*. Therefore, μ keeps every element of H and u belongs to the center W of HK. Let H_1 be the set of the elements of A that μ keeps unchanged. From Lemma 4 follows that H_1 is simple. Let v denote $s_0N_{U/U_0}u$. Obviously,

$$(6)\qquad v^*=\mu^n.$$

Then, from Lemma 3, we obtain that there exists a non-zero element v_0 of the center Z_1 of H_1 such that $v_0{}^*=v^*$ and $k(v_0)$ coincides with Z_1. Now, we suppose that there exists a regular element w in the center W of HK such that $v_1=v_0N_{U/U_0}w$ generates Z over k; $k(v_1)=Z$. Under this supposition, we can prove that there exsts a ring-automorphism τ of A such that H coincides with the set of the elements of A that τ keeps unchanged, as follows; let $\tau=\mu w^*$, and let F be the set of the elements of A that τ keeps unchanged. As is easily seen, FK is the centralizer of $K(v_1)$ in A. As, from the supposition, $K(v_1)=ZK=W$, we obtain $FK=HK$. $F\cap K=k$, and $HK\supset F\supset H$. Then it follows readily from Lemma 1 that $F=H$. Thus, the proof of Theorem 1 is reduced to the proof of the following

Theorem 3. *Let L be a field, M, K be subfields, and k the intersection of M and K, respectively. Suppose that L is equal to MK and is of finite rank over k, Kk/k is separable and Galois, and, moreover, M/k is simple extension. Then there exists for each non-zero element c of M a non-zero element d of M such that $cN_{L/M}d$ generates M over k; $M=k(cN_{L/M}d)$.*

The proof of this theorem will be obtained in §7 in the next chapter.

Chapter II. Norms and simple extensions.

5. Polynomials and simple extensions. We state the following lemma without proof.

Lemma 6. *Let L be a field, M a subfield. Let $F(X_1, X_2, \cdots X_r)$ be a polynomial of r independent indeterminates X_i with $i=1, 2, \cdots, r$ with coefficients in L. Let $m_i (i=1, 2, \cdots, r)$ be natural numbers such that each m_i is properly greater than the degree of F with reference to X_i, respectively. Suppose that there exists a set of m elements a_{i_j} of M with suffices $i=1, 2, \cdots, r$ and $j=1, 2, \cdots, m_i$ such that $F(a_{1_{j1}}, a_{2_{j2}}, \cdots, a_{r_{jr}}) \in M$ for each pair of J_i's with $1 \leqq j_i \leqq m_i$ and $a_{ij} \neq a_{ij'}$ for $j \neq j'$, where we denote $\prod_{i=1}^{r} m_i$ by m. Then $F(X_1, \cdots, X_r)$ is a polynomial of X_i's with coefficents in M.*

One obtains its proof by the mathematical induction with reference to r without any difficulty, and we omit it.

Lemma 7. *Let L be a field, and M a subfield. Suppose L/M is an algebraic simple extension. Let $F(X_1, X_2, \cdots, X_r)$ be a polynomial of r in dependent indeterminates with coefficients in L such that L is generated by the coefficients of $F(X_1, \cdots, X_r)$ over M, and suppose that M contains infinitely many elements. Then there exists a set $\mathfrak{A}$ of sufficiently many points p of the r-space over M such that, for each p of $\mathfrak{A}$, $F(p)=F(p_1, p_2, \cdots, p_r)$ generates L over M, and it holds $p_i \neq q_i$ for each pair of distinct two points p, q of $\mathfrak{A}$, where we denote the i-th coordinates of p and q by p_i and q_i, respectively.*

Proof. .Let Ω be an algebraic closure of L, and s denote the rank $[L_s : M]$ of the maximum separable extension L_s of M contained by L. Let $\sigma_i (i=1, 2, \cdots, s)$ be this distinct isomorphisms of L/M into Ω/M. Let $D(X_1, X_2, \cdots, X_r)=\prod_{i<j} (F^{\sigma_i}-F^{\sigma_j})$. Then, from the supposition, $D \neq O$, and there exist point sets $\mathfrak{A}$ of points $p, q, \cdots$ of the r-space over M such that $D(p)=D(p_1, \cdots, p_r) \neq 0$, and $p_i \neq q_i (i=1, 2, \cdots, r)$ for each pair of points p, q $(p \neq q)$ in $\mathfrak{A}$. As, from the supposition, L/M is simple extension of finite rank, the

intermediate fields between L and L_s are linearly ordered (in a finite length) by inclusions. Suppose that this lemma is false. Then, for each $\mathfrak{A}$, we can not generate L over M by $F(p)$ with $p\in\mathfrak{A}$. On the other hand, we can take $\mathfrak{A}$ with sufficiently many $\mathrm{p}\in\mathfrak{A}$ satisfying $M(F(p))\supseteqq L_s$. We can readily obtain a contradiction, considering both Lemma 6 and the supposition that the coefficicents of F generate L over M. The rest is trivial, q. e. d..

6. The generic form of norms. Let G be a finite group of order n, Q the rational number field, X_g and Y_k $2n$ independent indeterminate with elements g, h of G as suffices. Let $F(XY)$ be the polynomial of X's and Y's with coefficients of rational integers given as

$$(7) \qquad F(XY)=\prod_{h\in G}(\sum_{g\in G} X_{gh}Y_g)\in Q[X, \cdots, Y, \cdots].$$

We call it the generic form of norms with reference to G. Let y denote a monomial $Y_{g_1}^{i_1}\ Y_{g_2}^{i_2}\cdots Y_{g_n}^{i_n}$ of Y's of degree n:

$$n=i_1+i_2+\cdots+i_n.$$

Let $P_y(X)$ denote the coefficient of y in $F(XY)$ arranged as polynomial of Y's with coefficients in $Q[X_{g_1}, \cdots, X_{g_n}]$. We fix a linear order of elements of G, denote $X_{g_i}(Y_{g_i})$ by X_i (Y_i), respectively, so as to obtain the lexicographic order of monomials of X's. Let r_y denote the rational integer that appears as the coefficient of the highest term of $P_y(X)$. As is easily seen, $P_y(X)\neq 0$ and $r_y=1$, for every finite group G and every y as stated above. For example, let G be a cyclic group of order 4. Then

$$\begin{aligned} F(XY)=&(X_1Y_1+X_2Y_2+X_3Y_3+X_4Y_4)\ (X_1Y_2+X_2Y_3+X_3Y_4+X_4Y_1)\\ &\cdot(X_1Y_3+X_2Y_4+X_3Y_1+X_1Y_2)\ (X_1Y_4+X_2Y_1+X_3Y_2+X_4Y_3). \end{aligned}$$

Let y be, for exampl, $Y_1^2Y_3Y_4$. Then the highest term of $P_y(X)$ is $X_1^3X^4$.

Applying the natural mapping of the ring of rational integers onto the prime field of characteristic $p\neq 0$, if necessary, we obtain

Lemma 8. *Let k be an arbitrary field and let $F(XY)$ be the generic form of norms with reference to a finite group G of order n, considered as polynomial of X's and Y's with coefficients in k. Then every monomial of Y's of degree n appears in* F(XY), *having a polynomial of* X's *(with coefficients in k) or positive degree as its coefficient.*

7. Proof of Theorem 3. Let L be a field, M and K subfields of L, and let k be the intersection $M\cap K$ of M and K. Suppose that $L=MK$, L is of finite rank over k, M/k is an algebraic simple extension, and, moreover, K/k is separable and Galois. Let c be an arbitrary non-zero element of M. Now, we distinguish the following two cases: *Case* 1. Suppose that k is a Galoisfeld. Then, from the supposition, L is a Galoisfeld, and, as is well known, every

3). Cf. [4].

element of M is a norm of an element of L[3]. Let m be a non-zero element of M such that $M=k(m)$. There exists an element d of L such that

$$c^{-1}m=N_{L/M}d. \tag{8}$$

Then the theorem is obvious[4].

Case 2. Suppose that k contains infinitely many elements. If $M=k$, the theorem is trivial. Hence we suppose that the rank m of M over k is properly greater than 1. Let $F(XY)$ be the generic form of norms with reference to the Galois group G of L/M. We determine a linear order of the elements of G, fix it throughout the rest of this paper, and use it as in the proof of Lemma 8. Let $n=[K:k]$, and $\{w^{g_i};\ g_i\in G,\ i=1, 2, \cdots, n\}$ be a normal basis of K/k. We denote w^{g_i} by w_i. Let $U_i(i=1, 2, \cdots, n)$ be n independent indeterminates, and let

$$u_j=\sum_{i=1}^{n} w_i^{g_j}U_i \qquad (j=1, 2, \cdots, n). \tag{9}$$

As the determinant of the coefficients of (15) is not equal to 0, from Lemma 8 follows that every monomial y's of Y's of degree n appears in $F(uY)=F(u_1, \cdots, u_n, Y_1, \cdots, Y_n)$, where we denote Y_{g_i} by Y_i, as before. As, from the supposition, k contains infinitely many elements, we can find n elements p_i $(i=1, 2, \cdots, n)$ of K such that every monomial y of Y's of degree n appears in $F(\bar{p}Y)$, having non-zero coeffieient $P_y(\bar{p})$, where $P_y(\bar{p})$ denotes the element of L obtained from $P_y(X)$ through the substitution (specialization) $X_i\rightarrow\bar{p}_i$ with

$$\bar{p}_i=w_1^{g_i}p_1+w_2^{g_i}p_2+\cdots+w_n^{g_i}p_n \qquad (i=1, 2, \cdots, n). \tag{10}$$

$\bar{p}_i$'s belong to K and as is easily seen, $P_y(\bar{p})$ belong to k. Let $v_j(j=1, 2, \cdots m)$ be a basis of M/k, and $W_{ij}(i=1, 2, \cdots, n$ and $j=1, 2, \cdots, m)$ be nm independent indeterminates, and $\bar{w}_i$ be such linear form given as

$$\bar{w}_i=W_{i1}v_1+W_{i2}v_2+\cdots+W_{im}v_m. \qquad (i=1, 2, \cdots, n). \tag{11}$$

If y and y_1 are two monomials of Y's of degree n different to each other, then, obviously, a same monomial of W's does not appear in both $y(\bar{w})$ and $y_1(\bar{w})$ at the same time. Therefore, considering the expansion of the polynomial of W's obtained from $y_0=Y_1Y_2\cdots Y_n$ through substitution $Y_i\rightarrow\bar{w}_i$ we obtain that the coefficients of $F(\bar{p}, \bar{w})$ considered as a polynomial of W contain (as subset) a linear basis of M over k. Then, obviously, the coefficients of $cF(\bar{p}, \bar{w})$ generate M over k. From Lemma 8 follows that there exists a point $b=(b_{ij})$ of mn-space over k such that the element $F(\bar{p}, \bar{w}(b))$ of M obtained from $F(\bar{p}, \bar{w})$ through the specialization $W_{ij}\rightarrow b_{ij}$ generates M over k. Let

$$d=\bar{p}_1\cdot w_1(\mathrm{b}_1)+\bar{p}_2\cdot w_2(b_2)+\cdots+\bar{p}_n\cdot w_n(b_n), \tag{12}$$

[4] When k is a Galoisfeld, we can find an element d' such that $k(cN_{L/M}d')$ coincides with arbitrarily given intermediate field M' between M and L.

where we denote $\bar{p}_i\cdot(b_{i1}v_1+b_{i2}v_2+\cdots+b_{im}v_m)\in L$ by $\bar{p}_i\cdot\bar{w}_i(b_i)$ $(i=1,2,\cdots,n)$. As is easily seen, $N_{L/M}d=F(\bar{p},\bar{w}(b))$, and we obtain $M=k(cN_{L/M}d)$, q. e. d..

As is stated in §4, it completes the proof of Theorem 1, which is the aim of this paper.

REFERENCES

[1] R. BORTFELD; Ein Satz zur Galoistheorie in Shiefkörpern, J. reine u. angew. Math. 201 (1959), 196—206.

[2] A. INATOMI; Remark on Galois theory of simple rings, Kōdai Math. Sem. Rep., 14 (1962), 160—161.

[3] T. NAGAHARA, H. TOMINAGA; On Galois and locally Galois extensions of simple rings, Math. J. Okayama Univ. 10 (1961), 143—166.

[4] O. F. G. SHILLING; The Theory of Valuations, Math. Surveys no. IV, the A. M. S., New York City.

DEPARTMENT OF MATHEMATICS,
OKAYAMA UNIVERSITY

(*Received April 18, 1963*)