ON THE NORMAL BASIS THEOREMS AND THE EXTENSION DIMENSION

By

Kazuo KISHIMOTO, Takesi ONODERA
and Hisao TOMINAGA

Recently, in his paper [7] one of the authors has presented several generalized normal basis theorems for a division ring extension, which contain as special cases the normal basis theorems given in [1] by Kasch (provided for division ring extensions). One of the purposes of this paper is to extend his results to simple rings. In §1, we shall prove those extensions, and add a decision condition for a normal basis element in a strictly Galois extension of a division ring, which is well-known in commutative case. Next, in §2, we shall treat exclusively an F-group of order p^e in a simple ring, and consider the relations between the extension dimension over the fixed subring and the order of the F-group. The principal theorem of §2 is an improvement of the result stated in [8] for a DF-group. As to notations and terminologies used in this paper, we follow [3] and [5].

§1. The following lemma has been given in [7][1], and will play a fundamental role in our present study.

Lemma 1. *Let $T\ni 1$ be a ring with minimum condition for right ideals, and let M, N be unital right T-modules.*

(i) *M is T-projective if and only if it is T-isomorphic to a direct sum of submodules each of which is T-isomorphic to a directly indecomposable direct summand of T.*

(ii) *If $M^{(m)}\simeq T^{(\omega)}$ for a positive integer m and an infinite cardinal number ω, then $M\simeq T^{(\omega)}$.*

(iii) *If $M^{(m)}\simeq T^{(t)}$ for positive integers m, t and $t=mq+r$ $(0\leq r<m)$, then $M\simeq T^{(q)}\oplus M_0$, where M_0 is a T-homomorphic image of T such that $M_0^{(m)}\simeq T^{(r)}$. In particular, if $m=t$ then $M\simeq T$.*

(iv) *If M is T-projective and $M^{(m)}\sim N^{(n)}$ with $m\leq n$ then $M\sim N$.*

Theorem 1. *Let $\mathfrak{H}$ be an N-group with $B=J(\mathfrak{H}, A)$, and $N\ni 1$ an $\mathfrak{H}$-invariant subring of A with minimum condition for right ideals such that A possesses a finite (linearly independent) right N-basis $\{x_1, \cdots, x_t\}$. If*

1) Numbers in brackets refer to the references cited at the end of this paper.

$t\leq[A:B]$ then A is $\mathfrak{H}N_r$-homomorphic to $\mathfrak{H}N_r$, in particular, A is always $\mathfrak{H}B_r$-homomorphic to $\mathfrak{H}B_r$.

Proof. Since $V_{\mathrm{Hom}\,(A,A)}(B_l)=\mathfrak{H}A_r$ by [3, Theorem 1], $[A:B]=m$ implies $A^{(m)}\overset{\mathfrak{H}A_r}{\simeq}\mathfrak{H}A_r$ and $\mathfrak{H}A_r=\oplus_{i=1}^m\sigma_iA_r=\oplus_{i,j}\sigma_ix_{jr}N_r$ with some $\sigma_i\in\mathfrak{H}$. Then, to be easily verified, $\mathfrak{H}N_r$ satisfies the minimum condition for right ideals and $\mathfrak{H}A_r=A_r\mathfrak{H}=\sum x_{i_r}N_r\mathfrak{H}=\sum x_{ir}(\mathfrak{H}N_r)$, so that $\mathfrak{H}A_r$ is $\mathfrak{H}N_r$-homomorphic to $(\mathfrak{H}N_r)^{(t)}$, whence it follows that $A^{(m)}$ is $\mathfrak{H}N_r$-homomorphic to $(\mathfrak{H}N_r)^{(t)}$. Hence, by Lemma 1 (iv), A is $\mathfrak{H}N_r$-homomorphic to $\mathfrak{H}N_r$.

Lemma 2. *Let $\mathfrak{H}$ be an N-group with $B=J(\mathfrak{H},A)$ and $N\ni 1$ an $\mathfrak{H}$-invariant subring of A with minimum condition for right ideals such that A possesses a right N-basis $\{x_\lambda;\ \lambda\in\Lambda\}$.*

(i) *If $V=C$ or $V\subseteq N$, then $\mathfrak{H}N_r$ possesses a right N_r-basis containing $[A:B]$ elements and $\{x_{\lambda r};\ \lambda\in\Lambda\}$ forms a right $\mathfrak{H}N_r$-basis of $\mathfrak{H}A_r$.*

(ii) *If A/B is strictly Galois with respect to $\mathfrak{H}=\{\sigma_1,\cdots,\sigma_m\}$, then $\mathfrak{H}N_r=\oplus_1^m\sigma_iN_r$ and $\{x_{\lambda r};\ \lambda\in\Lambda\}$ forms a right $\mathfrak{H}N_r$-basis of $\mathfrak{H}A_r$.*

Proof. (i) As in the proof of Theorem 1, $A^{(m)}\overset{\mathfrak{H}A_r}{\simeq}\mathfrak{H}A_r$ $(m=[A:B])$ and $\mathfrak{H}A_r=\oplus_1^m\sigma_iA_r=\oplus_1^m A_r\sigma_i$ with some $\sigma_i\in\mathfrak{H}$. If $V=C$ then $\mathfrak{H}$ coincides with $\{\sigma_1,\cdots,\sigma_m\}$ by [6, Theorem 1]. On the other hand, if $V\subseteq N$ then $\mathfrak{H}V_r=\oplus_1^m\sigma_iV_r\subseteq\oplus_1^m\sigma_iN_r$ by [5, Lemma 1.3 (iii)]. Thus, in either cases, $\mathfrak{H}N_r=\oplus_1^m\sigma_iN_r$ and $\mathfrak{H}A_r=\oplus_{i,\lambda}x_{\lambda r}N_r\sigma_i=\oplus_\lambda x_{\lambda r}(\mathfrak{H}N_r)$, so that $\{x_{\lambda r};\ \lambda\in\Lambda\}$ is a right $\mathfrak{H}N_r$-basis of $\mathfrak{H}A_r$.

(ii) As $\mathfrak{H}A_r=\oplus_1^m\sigma_iA_r$, $\mathfrak{H}N_r=\oplus_1^m\sigma_iN_r$ of course. So that, the rest of the proof is the same with the last part of (i).

Lemma 3. *Let A be Galois and finite over B, and $N\ni 1$ a $\mathfrak{G}$-invariant simple subring of A. If V is different from $(GF(2))_2$ and $[\mathfrak{G}N_r:N_r]_r=[A:B]$ then $V=C$ or $V\subseteq N$.*

Proof. The proof will proceed except only one point in the same way as [3, Theorem 3] did. However, for the sake of completeness, we shall give it here. Suppose on the contrary that V is neither C nor contained in N. Every element of V is a finite sum of elements contained in $V^\cdot$ (the group of units in V) and $[\mathfrak{G}A_r:A_r]_r=[A:B]=[\mathfrak{G}N_r:N_r]_r$. In what follows, we shall prove that there exist some $v,v_1,\cdots,v_k\in V^\cdot$ such that $\{v_1,\cdots,v_k\}$ is linearly independent over C and $\tilde{v}=\sum_1^k\tilde{v}_ia_{ir}$ with some $a_i\in A$ not all contained in N. (But, by [4, Lemma 1.3 and Lemma 1.4], the last fact yields at once a contradiction.) To this end, we set $V=\sum_1^tUg_{pq}$ where $\{g_{pq}\}$ is a system of matrix units and $U=V_V(\{g_{pq}\})$ a division ring, and distinguish between two cases:

Case I. $l=1$: Let $\{v_1, \cdots, v_m\}$ be a C-basis of V. Then, $V\neq C$ yields $m>1$. We shall distinguish further between three cases:

(i) $C\not\subseteq N$: As is readily verified, $\widetilde{v_1+v_2}=\tilde{v}_1(v_1(v_1+v_2)^{-1})_r+\tilde{v}_2(v_2(v_1+v_2)^{-1})_r$. If $v_1(v_1+v_2)^{-1}\notin N$ then v_1+v_2, v_1 and v_2 are elements desired. On the other hand, if $d_1=v_1(v_1+v_2)^{-1}$ is in N then $v_2=(d_1^{-1}-1)v_1$ and d_1 is different from 1. For an arbitrary $c\in C\setminus N$, we have $\widetilde{v_1+cv_2}=\tilde{v}_1(v_1(v_1+cv_2)^{-1})_r+\tilde{v}_2(v_2c(v_1+cv_2)^{-1})_r$. Then, $d_2=v_1(v_1+cv_2)^{-1}$ is not contained in N. In fact, if $d_2\in N$ then $(d_1^{-1}-1)v_1=v_2=c^{-1}(d_2^{-1}-1)v_1$ yields a contradiction $c=(d_2^{-1}-1)\cdot(d_1^{-1}-1)^{-1}\in N$.

(ii) $C\subseteq N$ and $\{v_1, \cdots, v_m\}\frown N=\emptyset$: $1=v_1c_1+\cdots+v_mc_m$ with $c_i\in C$, so that $\tilde{1}=\tilde{v}_1(v_1c_1)_r+\cdots+\tilde{v}_m(v_mc_m)_r$. Recalling that $c_j\neq 0$ for some j and hence $v_jc_j\notin N$, 1, $v_1, \cdots, v_m$ are evidently desired ones.

(iii) $C\subseteq N$ and $\{v_1, \cdots, v_m\}\frown N\neq\emptyset$: As $C\subseteq N$ and $V\not\subseteq N$, without loss of generality, we may assume that $v_1\in N$ and $v_2\notin N$. Then, $\widetilde{v_1+v_2}=\tilde{v}_1(v_1(v_1+v_2)^{-1})_r+\tilde{v}_2(v_2(v_1+v_2)^{-1})_r$ and $v_1(v_1+v_2)^{-1}\notin N$, so that v_1+v_2, v_1 and v_2 are desired ones.

Case II. $l>1$: Evidently, $\{1, f_{pq}=1-g_{pq}\ (p, q=1, \cdots, l\,; p\neq q)\}$ $(\subseteq V^{\cdot})$ is linearly independent over C, and similarly in case l is even so is $\{f_q=g_{qq}+\sum_1^l g_{pl-p+1}\ (q=1, \cdots, l)\}$ $(\subseteq V^{\cdot})$. By [2, Theorem 2], $V\subseteq N$ or $N\subseteq H$, so that $N\subseteq H$ in reality[2]. Noting that $V\frown N$ is then a field contained in the center of V, it is clear that no non-diagonal elements of V are contained in N. Now, we shall complete our proof by distinguishing between two cases:

(i) V is not of characteristic 2: In this case, every $1+f_{pq}$ is in $V^{\cdot}$ and $\widetilde{1+f_{pq}}=\tilde{1}(1+f_{pq})_r^{-1}+\tilde{f}_{pq}(f_{pq}(1+f_{pq})^{-1})_r$ with $(1+f_{pq})^{-1}\notin N$.

(ii) V is of characteristic 2: If l is odd, then $u=1+\sum_2^l f_{p-1p}\in V^{\cdot}$ and $\tilde{u}=\tilde{1}u_r^{-1}+\sum_2^l\tilde{f}_{p-1p}(f_{p-1p}u^{-1})_r$ with $u^{-1}\notin N$. On the other hand, if l is even then $1=\sum_1^l f_p$, so that $\tilde{1}=\sum_1^l\tilde{f}_p f_{pr}$ with $f_p\notin N$.

The following example will show that the assumption $V\neq(GF(2))_2$ is indispensable in Lemma 3.

Example 1. Let $A=(GF(2))_2$, $B=GF(2)$. Then, $1=\begin{pmatrix}1&0\\0&1\end{pmatrix}$, $\alpha=\begin{pmatrix}1&0\\1&1\end{pmatrix}$, $\beta=\begin{pmatrix}1&1\\0&1\end{pmatrix}$, $\gamma=\begin{pmatrix}0&1\\1&0\end{pmatrix}$, $\delta=\begin{pmatrix}1&1\\1&0\end{pmatrix}$, $\varepsilon=\begin{pmatrix}0&1\\1&1\end{pmatrix}$ induce the Galois group $\mathfrak{G}=\{\tilde{1}, \tilde{\alpha}, \tilde{\beta}, \tilde{\gamma}, \tilde{\delta}, \tilde{\varepsilon}\}$ of A/B, $V=A$ and $N=\{0, 1, \delta, \varepsilon\}$ is a $\mathfrak{G}$-invariant subfield of A. Since $\tilde{\gamma}=\tilde{\alpha}\varepsilon_r+\tilde{\beta}\delta_r$ and $\tilde{\varepsilon}=\tilde{1}\delta_r+\tilde{\delta}\varepsilon_r$, we obtain $\mathfrak{G}N_r=\tilde{1}N_r\oplus\tilde{\alpha}N_r\oplus\tilde{\beta}N_r\oplus\tilde{\delta}N_r$, so that $[\mathfrak{G}N_r : N_r]_r=4=[A:B]$. However, to be easily verified, $V\neq C$ and $\not\subseteq N$.

2) The assumption $V\neq(GF(2))_2$ is needed only to secure $N\subseteq H$ (provided $V\not\subseteq N$). Accordingly, our lemma is evidently valid for $N=B$ even in case $V=(GF(2))_2$. (Cf. [2, Theorem 3]).

Theorem 2. *Let A/B be Galois, $[A:B]=m$, V different from $(GF(2))_2$, and let N be a $\mathfrak{G}$-invariant simple subring of A.*

(i) *The following conditions are equivalent to each other:*

(1) $V=C$ *or* $V\subseteq N$.

(2) $[\mathfrak{G}N_r:N_r]_r=[A:B]$.

(ii) *If $[A:N]_r$ is an infinite cardinal number ω, then A is $\mathfrak{G}N_r$-isomorphic to $(\mathfrak{G}N_r)^{(\omega)}$.*

(iii) *If $[A:N]_r=t$ and $t=mq+r$ $(0\leq r<m)$, then each of the conditions* (1), (2) *cited in* (i) *is equivalent to the next:*

(3) *A is $\mathfrak{G}N_r$-isomorphic to $(\mathfrak{G}N_r)^{(q)}\oplus\mathfrak{M}$, where $\mathfrak{M}$ is a $\mathfrak{G}N_r$-homomorphic image of $\mathfrak{G}N_r$ such that $M^{(m)}\simeq(\mathfrak{G}N_r)^{(r)}$.*

Proof. (i) The equivalence is a direct consequence of Lemma 2 (i) and Lemma 3. (ii) $A^{(m)}\overset{\mathfrak{G}A_r}{\simeq}\mathfrak{G}A_r\overset{\mathfrak{G}N_r}{\simeq}(\mathfrak{G}N_r)^{(\omega)}$ by Lemma 2 (i). Hence, Lemma 1 (ii) yields at once our assertion. (iii) By (i) and Lemma 1 (iii), one will easily see the equivalence relations.

Now, by the light of Lemma 2 (ii), Lemma 1 (ii) and (iii) will yield the following, too. The proof may be left to readers.

Theorem 3. *Let A/B be strictly Galois with respect to $\mathfrak{H}$ of order m, and $N\ni 1$ an $\mathfrak{H}$-invariant subring of A with minimum condition for right ideals such that A possesses a right N-basis $\{x_\lambda;\ \lambda\in\Lambda\}$.*

(i) *If Λ is infinite then there exists a subset $\{u_\lambda;\ \lambda\in\Lambda\}$ of A such that $\{u_\lambda\sigma;\ \lambda\in\Lambda$ and $\sigma\in\mathfrak{H}\}$ is a right N-basis of A.*

(ii) *If $\sharp\Lambda=t<\infty$ and $t=mq+r$ $(0\leq r<m)$ then A contains q elements $u_1,\cdots,u_q$ and an $\mathfrak{H}N_r$-homomorphic image M with $M^{(m)}\simeq(\mathfrak{H}N_r)^{(r)}$ such that $\{u_i\sigma;\ i=1,\cdots,q$ and $\sigma\in\mathfrak{H}\}$ is right linearly independent over N and $A=(\oplus_{i,\sigma}(x_i\sigma)N)\oplus M$.*

As a special case of Theorem 3 (ii), we see that if A/B is strictly Galois with respect to $\mathfrak{H}$ then there exists a right (and similarly a left) $\mathfrak{H}$-n.b.e. (cf. [3, Theorem 4]). In case A is a division ring, we can prove the following theorem, that is well-known for the commutative case.

Theorem 4. *Let A be a division ring, and $\mathfrak{H}=\{\sigma_1,\cdots,\sigma_m\}$ an automorphism group of A with $B=J(\mathfrak{H},A)$. In order that $[A:B]$ coincides with m, it is necessary and sufficient that there exists an element $a\in A$ such that the matrix $(a\sigma_i\sigma_j)$ is regular. Moreover, $a\in A$ is a left $\mathfrak{H}$-n.b.e. (right $\mathfrak{H}$-n.b.e.) if and only if the matrix $(a\sigma_i\sigma_j)$ (the matrix ${}^t(a\sigma_i\sigma_j)$ transposed) is regular.*

Proof. If $[A:B]=m$, that is, A/B is strictly Galois with respect to $\mathfrak{H}$, then there exists a left $\mathfrak{H}$-n.b.e. $a\in A$ by Theorem 3, for which we have

$T_{\mathfrak{H}}(a)=\sum a\sigma_i\neq 0$. Suppose $(a\sigma_i\sigma_j)$ is non-regular. Then, the matrix is a zero-divisor, so that there hold non-trivial relations $\sum a_i\cdot a\sigma_i\sigma_j=0$ $(j=1,\cdots,m)$ with some $a_1,\cdots,a_m\in A$, where we assume $a_k\neq 0$. Since $\sum aa_k^{-1}a_i\cdot a\sigma_i\sigma_j=0$ $(j=1,\cdots,m)$ and $T_{\mathfrak{H}}(aa_k^{-1}a_k)=T_{\mathfrak{H}}(a)\neq 0$, we may assume further $T_{\mathfrak{H}}(a_k)\neq 0$. We obtain then $0=\sum_{i,j}a_i\sigma_j^{-1}\cdot a\sigma_i=\sum_i T_{\mathfrak{H}}(a_i)\cdot a\sigma_i$. Now, $T_{\mathfrak{H}}(a_i)\in B$ and $T_{\mathfrak{H}}(a_k)\neq 0$ contradict our assumption that a is a left $\mathfrak{H}$-n.b.e. Conversely, if $(a\sigma_i\sigma_j)$ is regular then $\{a\sigma_1,\cdots,a\sigma_m\}$ is linearly left independent over B, so that $[A:B]=m$ by [3, Lemma 2]. The latter assertion will be evident by the above proof.

Corollary 1. *Let a division ring A be strictly Galois with respect $\mathfrak{H}$ of order m. A left $\mathfrak{H}$-n.b.e. is a right $\mathfrak{H}$-n.b.e. as well, provided either $\mathfrak{H}$ is abelian or A is of characteristic p and $m=p^e$.*

Proof. If $\mathfrak{H}$ is abelian, our assertion is evident by Theorem 4. On the other hand, in case A is of characteristic p and $m=p^e$, our assertion is a direct consequence of [3, Corollary 1].

§2. In [8][3], the results obtained in [3, §3] have been generalized as follows: Let $A(\ni 1)$ be a simple ring (satisfying the minimum condition for right ideals) with the center C, $\mathfrak{H}$ a *DF*-group of order p^e (p a prime), and $B=J(\mathfrak{H},A)$. If the center Z of B contains no primitive p-th roots of 1, then $V=V_A(B)$ coincides with $C[Z]$ and $[A:B]$ divides p^e. If moreover A is not of characteristic p, then $[A:B]$ coincides with p^e. In below, we shall present an improvement of the above theorem (Theorem 5) together with several additional remarks. Our improvement is essentially due to the following brief lemma.

Lemma 4. *Let A be a central simple algebra of finite rank over C, $\mathfrak{H}$ an automorphism group of A such that $J(\mathfrak{H},A)=C$ and $\sharp\mathfrak{H}=p^e$ (p a prime). If C contains no primitive p-th roots of 1 then A coincides with C.*

Proof. Suppose on the contrary $e>0$. As $\mathfrak{G}(A/C)=\tilde{A}$, the center of $\mathfrak{H}$ contains a subgroup $\mathfrak{P}=\{\tilde{1},\tilde{v},\cdots,\tilde{v}^{p-1}\}$ of order p. Then, for each $\sigma=\tilde{u}\in\mathfrak{H}$, $\tilde{v}\sigma=\sigma\tilde{v}$ implies $v\sigma=vc_\sigma$ with some $c_\sigma\in C$. And, $v^p=uv^pu^{-1}=(v\sigma)^p=v^pc_\sigma^p$ yields $c_\sigma^p=1$, i.e. $c_\sigma=1$, which means evidently $v\sigma=v$, so that $v\in J(\mathfrak{H},A)=C$. But, this is a contradiction.

In the rest of this paper, we use the following conventions: A is a simple ring with the center C, and $\mathfrak{H}$ an *F*-group of A of order p^e (p a prime). We set $B=J(\mathfrak{H},A)$, that is a simple ring by [3, Lemma 2]. And,

3) By the way, we should like to note here a typographical error in the proof of [8, Theorem 2]: $\mathfrak{Z}=\tilde{V}\frown\mathfrak{G}$ should replace $\mathfrak{Z}=\tilde{V}$.

Z, V and H represent the center of B, $V_A(B)$ and $V_A(V)$, respectively. $\mathfrak{H}_0=\mathfrak{H}_\frown\tilde{V}$ is evidently an invariant subgroup of $\mathfrak{H}$ consisting of all the inner automorphisms contained in $\mathfrak{H}$. One may remark here that $V=V(\mathfrak{H})=V(\mathfrak{H}_0)$ by [3, Lemma 2]. Finally, by p^ε we denote the exponent of $\mathfrak{H}_0$, and set $p^f=(\mathfrak{H}:\mathfrak{H}_0)\cdot p^\varepsilon$.

Theorem 5. *If Z contains no primitive p-th roots of* 1, *then V is the composite $C[Z]$ of C and Z (accordingly $\mathfrak{H}$ is a DF-group*[4]*), and $[A:B]$ is a multiple of p^f and a divisor of p^e. In particular, if moreover, A is not of characteristic p then $[A:B]$ coincides with p^e.*

Proof. Let C_0 be the center of V. Then, $\mathfrak{H}|C_0$ is evidently the Galois group of C_0/Z, so that $[C_0:Z]=\#(\mathfrak{H}|C_0)$ divides p^e. Hence, C_0 contains no primitive p-th roots of 1. Next, $\mathfrak{H}_0|V$ is an automorphism group of V and its order divides p^e. As $J(\mathfrak{H}_0|V, V)=C_0$ and $[V:C_0]<\infty$, Lemma 4 yields then $V=C_0$. Suppose $V\supsetneqq C[Z]$. Then, noting that $V=V(\mathfrak{H}_0)$, we can find an element $v\in V\setminus C[Z]$ with $\tilde{v}\in\mathfrak{H}_0$. Since the field V is normal and separable over $C[Z]$ and $v^{p^e}=c\in C$, there exists an element $u\in V$ different from v with $u^{p^e}=v^{p^e}$, that is, $(vu^{-1})^{p^e}=1$. Recalling here that $C_0=V$ contains no primitive p-th roots of 1, we obtain $vu^{-1}=1$. Hence, we have a contradiction $v=u$, which proves our first assertion $V=C[Z]$. It follows then, $[A:B]$ is a divisor of p^e by [4, Theorem 1] and in case A is not of characteristic p it coincides with p^e by [8, Theorem 3]. And so, in what follows, we shall prove that if A is of characteristic p then p^f divides $[A:B]$. By [6], we obtain $\mathfrak{H}(H)=\mathfrak{H}_0$ and $[H:B]=(\mathfrak{H}:\mathfrak{H}_0)$. Since the field V coincides with $V(\mathfrak{H}_0)$ and the order of $\mathfrak{H}_0$ is a power of p, V is a finite dimensional purely inseparable extension of C and one will easily see that the exponent of V/C coincides with ε. Hence, p^ε divides $[V:C]=[A:H]$, so that $p^f=p^\varepsilon\cdot(\mathfrak{H}:\mathfrak{H}_0)$ does $[A:H][H:B]$ $=[A:B]$.

Now, combining the first assertion of Theorem 5 with [4, Corollary 1. 3], we readily obtain the next:

Corollary 2. *Let A be of characteristic p, and $\mathfrak{H}$ a fundamental abelian group: $\mathfrak{H}=\mathfrak{H}_1\times\cdots\times\mathfrak{H}_e$, where $\mathfrak{H}_i=[\sigma_i]$ is cyclic with a generator σ_i of order p. If A/B is strictly Galois with respect to $\mathfrak{H}$ then there exist some $x_1,\cdots,x_e\in A$ such that* (1) $x_i^p-x_i\in B$, (2) $A=B[x_1,\cdots,x_e]$, (3) $B=B[x_i]_\frown B[x_1,\cdots,\check{x}_i,\cdots,x_e]$ *and* (4) *$B[x_i]/B$ is strictly Galois with respect to $\mathfrak{H}_i$.*

Theorem 6. *Let A be of characteristic p. In order that $[A:B]$ coincides with p^f, it is necessary and sufficient that V/C is primitive.*

Proof. As was noted in the proof of Theorem 5, $[H:B]=(\mathfrak{H}:\mathfrak{H}_0)$ and

4) However, in case Z contains a primitive p-th root, $\mathfrak{H}$ is not always a DF-group.

the exponent of V/C coincides with ε. So that, by [9, p. 140], V/C is primitive if and only if $p^{\varepsilon}=[V:C]=[A:H]$, i.e. $p^{f}=[A:B]$.

Corollary 3. *Let Z contain no primitive p-th roots of* 1. *If $\mathfrak{H}_0$ is cyclic then $[A:B]=p^e$, in particular, if C is a Galoisfeld then $[A:B]=p^e$*[5].

Proof. In virtue of Theorem 5, we may assume that A is of characteristic p. Since the exponent of cyclic $\mathfrak{H}_0$ coincides with $\#\mathfrak{H}_0$, our assertion is a direct consequence of Theorem 6.

Finally, let A be of characteristic p. As $\mathfrak{H}_0$ is abelian by Theorem 5, we may set $\mathfrak{H}_0=\mathfrak{H}_1\times\cdots\times\mathfrak{H}_t$ with cyclic $\mathfrak{H}_i$. If we set $V_i=V(\mathfrak{H}_i)$ (a field), then $V=V_1\cdots V_t$ and $[V_i:C]=\#\mathfrak{H}_i$ by Corollary 3. Now, one will easily see the following:

Theorem 7. *Let A be of characteristic p. In order that $[A:B]$ coincides with p^e, it is necessary and sufficient that $V_1\cdots V_t=V_1\otimes_C\cdots\otimes_C V_t$.*

Example 2. Let $\Phi=GF(p)$, and $C=\Phi(x_1,\cdots,x_e)$ with e indeterminates $x_1,\cdots,x_e$. $B=C(x_1^{\frac{1}{p}},\cdots,x_e^{\frac{1}{p}})$ is evidently a p^e-dimensional purely inseparable extension over C with exponent 1. Let A be the ring of $p^e\times p^e$ matrices with entries in C. Then, C is the center of A, B is a maximal subfield of A and $[A:B]=p^e$. We consider here inner automorphisms σ_i induced by $x_i^{\frac{1}{p}}$ $(i=1,\cdots,e)$. To be easily verified, $\mathfrak{H}_1=[\sigma_1,\cdots,\sigma_e]=[\sigma_1]\times\cdots\times[\sigma_e]$ is a DF-group of order p^e with $J(\mathfrak{H}_1,A)=B$. If $e>1$, we consider further the inner automorphism σ_0 induced by $\sum_1^e x_i^{\frac{1}{p}}$. $\mathfrak{H}_2=[\sigma_0,\sigma_1,\cdots,\sigma_e]=[\sigma_0]\times[\sigma_1]\times\cdots\times[\sigma_e]$ is then a DF-group of order p^{e+1} with $J(\mathfrak{H}_2,A)=B$.

References

[1] F. KASCH: Über den Endomorphismenring eines Vektorraums und den Satz von der Normalbasis, Math. Ann., 126, (1953), 447–463.

[2] K. KISHIMOTO, T. NAGAHARA and H. TOMINAGA: Supplementary remarks to the previous papers, Math. J. Okayama Univ., 11 (1963), 159–163.

[3] T. NAGAHARA, T. ONODERA and H. TOMINAGA: On normal basis theorem and strictly Galois extension of simple rings, Math. J. Okayama Univ., 8 (1958), 133–148.

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

[5] T. NAGAHARA and H. TOMINAGA: On Galois theory of simple rings, Math. J. Okayama Univ., 11 (1963), 79–117.

5) If C is a Galoisfeld of characteristic p, $\mathfrak{H}$ is outer in reality. Moreover, we can prove that if A is of characteristic p and $\mathfrak{H}$ is not outer then every element of $V\setminus C$ is transcendental over its prime field (cf. Example 2).

[6] T. NAKAYAMA: Galois theory of simple rings, Trans. Amer. Math. Soc., 73 (1952), 276–292.
[7] T. ONODERA: On semi-linear normal basis, J. Fac. Sci. Hokkaido Univ., Ser. I, 18 (1964), 23–33.
[8] T. TAKAZAWA and H. TOMINAGA: On a simple ring with a Galois group of order p^e, J. Fac. Sci. Hokkaido Univ., Ser. I, 15 (1961) 198–201.
[9] B. L. van der WAERDEN: Moderne Algebra, Bd. I, Berlin (1950).

Hokkaido Gakugei University
Hokkaido University
Hokkaido University

(Received April 14, 1964)