<table>
<thead>
<tr>
<th>Title</th>
<th>A NOTE ON NON-COMMUTATIVE KUMMER EXTENSIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Author(s)</td>
<td>Ôhori, Masayuki; Tominaga, Hisao</td>
</tr>
<tr>
<td>Citation</td>
<td>Journal of the Faculty of Science Hokkaido University. Ser. 1 Mathematics = 北海道大学理学部紀要 18(1-2): 078-080</td>
</tr>
<tr>
<td>Issue Date</td>
<td>1964</td>
</tr>
<tr>
<td>Doc URL</td>
<td><a href="http://hdl.handle.net/2115/56052">http://hdl.handle.net/2115/56052</a></td>
</tr>
<tr>
<td>Type</td>
<td>bulletin (article)</td>
</tr>
<tr>
<td>File Information</td>
<td>JFSHIU_18_N1-2_078-080.pdf</td>
</tr>
</tbody>
</table>
A NOTE ON NON-COMMUTATIVE KUMMER EXTENSIONS

By

Masayuki OHORI and Hisao Tominaga

Let a simple ring $A$ (with 1 and minimum condition) be strictly Galois with respect to (an $F$-group) $\mathfrak{H}$ in the sense of [2]. Then $B=J(\mathfrak{H}, A)$ is a simple ring with $[A : B]=\#\mathfrak{H}$, and the following facts have been given in [2] and [3]. (As to notations and terminologies used in this note, we follow [2].)

1°. Let $\mathfrak{N}$ be an $F$-subgroup of $\mathfrak{H}$. If $N=J(\mathfrak{N}, A)$, then $A/N$ is strictly Galois with respect to $\mathfrak{N}$, $[N : B]=(\mathfrak{H} : \mathfrak{N})$ and $\mathfrak{H}(N)=\mathfrak{N}$. In particular, if $\mathfrak{N}$ is an invariant subgroup of $\mathfrak{H}$ then $\mathfrak{H}|\mathfrak{N}=\mathfrak{H}/\mathfrak{N}$.

2°. $A$ contains an $\mathfrak{H}$-normal basis element ($\mathfrak{H}$-n.b.e.), that is, $A$ contains an element $a$ such that $\{a\sigma; \sigma\in \mathfrak{H}\}$ forms a (linearly independent) right $B$-basis of $A$.

3°. If $\sigma\rightarrow x_{\sigma}$ is an anti-homomorphism of $\mathfrak{H}$ into $B^\ast$ (the multiplicative group of units of $B$) then there exists an element $x\in A^\ast$ such that $x_{\sigma}=ax$. 

4°. Let $\mathfrak{H}$ be cyclic with a generator $\sigma$ of order $m$, and $B\cap C$ ($C$ the center of $A$) contains a primitive $m$-th root of 1. If there exists an element $a\in A^\ast$ such that $a\sigma=a\zeta$, there holds $A=\bigoplus_{i=0}^{m-1}Ba_{i}=\bigoplus_{i=0}^{m-1}a^{i}B$.

Further, $A/B$ was called an $\mathfrak{H}$-Kummer extension if $\mathfrak{H}$ is a commutative $DF$-group whose exponent is $m_{0}$ and $B\cap C$ contains a primitive $m_{0}$-th root of 1, and [3, Theorem 3] enabled us the notion of an $\mathfrak{H}$-Kummer extension to be naturally regarded as a generalization of the classical one for (commutative) fields. On the other hand, in his paper [1], C. C. Faith proved that any commutative Kummer extension $A/B$ is completely basic, more precisely, every normal basis element of $A/B$ is a normal basis element of $A/B'$ for any intermediate field $B'$ of $A/B$. The purpose of this note is to carry over the last proposition to division rings. In fact, by the validity of $1°-4°$, a slight modification of Faith's proof will accomplish our attempt. Firstly, we exhibit the following characterization of an $\mathfrak{H}$-Kummer extension.

**Theorem 1.** Let $\mathfrak{H}=\{\eta_{1}, \cdots, \eta_{m}\}$ be a $DF$-group of $A$ whose exponent is $m_{0}$. If $A/B$ is an $\mathfrak{H}$-Kummer extension then $A=\bigoplus_{i=1}^{m_{0}}a_{i}B=\bigoplus_{i=1}^{m_{0}}Ba_{i}$ with some $a_{i}\in A^\ast$ such that every $\zeta_{ij}=a_{i}^{-1}a_{j}$ is contained in $B\cap C$, and conversely.
Proof. Let $\mathfrak{H}=\mathfrak{H}_1 \times \cdots \times \mathfrak{H}_e$ with cyclic $\mathfrak{H}_i=[\sigma_i]$ of order $m_i$. Then, the exponent $m$ of $\mathfrak{H}$ coincides with the least common multiple $\{m_1, \cdots, m_e\}$. Now, let $\zeta$ be a primitive $m_i$-th root of 1 contained in $B \cap C$, and let $\zeta_i=\zeta^{m_i/m_i}$, that is evidently a primitive $m_i$-th root of 1. Then, $\eta=\prod_{j=1}^{e} \sigma_j^{s_j} \rightarrow \zeta_i^{s_j}$ defines a homomorphism of $\mathfrak{H}$ into $(B \cap C^*)$ $(i=1, \cdots, e)$. Thus, by $3^\circ$, there exists an element $x_i \in A_i$ such that $x_i \sigma_i=x_i \zeta_i$ and $x_i \sigma_j=x_i \zeta_i$ for all $j \neq i$. Noting that $J(\mathfrak{H}_2 \times \cdots \times \mathfrak{H}_e, A)$ contains $x_i$ and is strictly Galois with respect to $\mathfrak{H}$, by $1^\circ$, $4^\circ$ yields at once $J(\mathfrak{H}_2 \times \cdots \times \mathfrak{H}_e, A)=\oplus_{t=0}^{m_i-1}x_i^{t_i}$ and $\cdots,x_i^{t_1}B$, repeating similar arguments, we obtain $J(\mathfrak{H}_e,J(\mathfrak{H}_2 \times \cdots \times \mathfrak{H}_e, A))=\oplus_{t=1}^{m_i-1}x_i^{t_i}$ in particular, $A=\oplus_{0 \leq t_i \leq m_i}x_i^{t_i} \cdots x_i^{t_1}B$. If $\eta=\prod_{i=1}^{e} \sigma_j^{s_j}$ $(0 \leq s_i \leq m_i)$ is an arbitrary element of $\mathfrak{H}$ and $a=x_i^{s_i} \cdots x_i^{t_1}$, then it is easy to see $a\eta=a\zeta_1^{s_1} \cdots \zeta_i^{s_i}$, so that $a^{-1} \cdot a\eta=\zeta_1^{s_1} \cdots \zeta_i^{s_i}$ is contained in $B \cap C$, as desired. Conversely, assume that $A=\oplus_{t=0}^{m_i-1}a_iB$ $(a_i \in A \cap \mathfrak{H})$ and every $\zeta_j=a_i^{-1} \cdot a_i \eta_j$. As $\zeta_j$ is contained in $B$, it is easy to see that $\zeta_j^{m_i}=a_i^{-1} \cdot a_i \eta_j$ for $k=0,1, \cdots$. We see therefore that if $\eta_j$ is of order $k$ then $a_i \eta_j^{k}=a_i$ and $\zeta_j^{m_i}=1$, whence it follows that some one among $\zeta_j$ $(\sigma_j)$ is a primitive $k$-th root of 1. We see accordingly $B \cap C$ contains a primitive $m_i$-th root of 1. Next, if $a=\sum_{i=1}^{m}a_i b_i$ $(b_i \in B)$ is an arbitrary element of $A$, then $a\eta \eta_i=\sum_{i=1}^{m}a_i \eta_i \eta_i \cdot b_i=\sum_{i=1}^{m}a_i \zeta_i^{s_i}=a \eta \eta_i$, which asserts $\mathfrak{H}$ is abelian.

The next will be easily seen from the proof of Theorem 1.

Corollary 1. Let $A/B$ be an $\mathfrak{H}$-Kummer extension. If $\mathfrak{H}=\mathfrak{H}_1 \times \mathfrak{H}_2$ with $B_i=J(\mathfrak{H}_i, A)$, then $A=B,B_2=\mathfrak{H},$ and every $\mathfrak{H}$-n.b.e. of $B_i/B$ is an $\mathfrak{H}$-n.b.e. of $A/B_i$.

Corollary 2. Let $A/B$ be an $\mathfrak{H}$-Kummer extension with a basis $\{a_1, \cdots, a_m\}$ as in Theorem 1. Then, $a=\sum_{i=1}^{m}a_i b_i$ $(b_i \in B)$ is an $\mathfrak{H}$-n.b.e. if and only if every $b_i$ is in $B$.

Proof. By assumption, $\eta_j=\sum_{i=1}^{m}a_i \eta_j \cdot b_i=\sum_{i=1}^{m}a_i \zeta_i^{s_j}$. Accordingly, $a$ is an $\mathfrak{H}$-n.b.e. if and only if the matrix $(b_i \zeta_i^{s_j})$ is regular. In any rate, $A$ contains an $\mathfrak{H}$-n.b.e. by $2^\circ$, so that the matrix $(b_i \zeta_i^{s_j})$ is regular for some choice of $b_i$, whence it follows the matrix $(\zeta_i^{s_j})$ is regular. Thus, $a$ is an $\mathfrak{H}$-n.b.e. if and only if $(\begin{smallmatrix} b_i & 0 \\ 0 & b_m \end{smallmatrix})$ is regular, that is, every $b_i$ is in $B$.

Lemma 1. Let $A$ be a division ring, $A/B$ an $\mathfrak{H}$-Kummer extension, and $\mathfrak{H}=\mathfrak{H}_1 \times \mathfrak{H}_2$ with cyclic $\mathfrak{H}_1=[\sigma_1]$ of order $m_1$. If $\mathfrak{H}_0$ is a subgroup of $\mathfrak{H}$ containing $\mathfrak{H}_2$, then every $\mathfrak{H}$-n.b.e. of $A/B$ is an $\mathfrak{H}_0$-n.b.e. of $A/B_0$.

Proof. Let $B_i=J(\mathfrak{H}_i, A)$ $(i=0,1,2)$, and $\mathfrak{H}_i=\mathfrak{H} \cap \mathfrak{H}_0=[\sigma_i]^*$ with a posi-
tive divisor $s$ of $m_i$. Then, $\mathfrak{H}_0 = \mathfrak{H}_1^* \times \mathfrak{H}_2$. To be easily seen from the proof of Theorem 1, there exist (non-zero) elements $a_i = 1, a_2, \ldots, a_n \in B$, and $a \in B_2$ such that $A = \bigoplus_{0 \leq j < m_1} a \cdot a^j B, \ a_{i-1} \cdot a \eta \in B \cap C$ for each $\eta \in \mathfrak{H}_0$, and $a \sigma_i = a \zeta_i$, where $\zeta_i$ is a primitive $m_i$-th root of 1 contained in $B \cap C$. If $n_i/m_i$s then $a^{n_i} \sigma_i = a^{n_i}, n/s \leq \lambda < s$ forms a right $B$-basis of $B_0$ by (1º). It follows therefore $\{a_i a^n; 1 \leq i \leq n, 0 \leq \mu < n_1\}$ is a right $B_r$-basis of $A$ and $(a_i a^n)^{-1} (a_i a^n) \eta \in B \cap C$ for each $\eta \in \mathfrak{H}_0$. Now, if $u = \sum_{i \leq j, \mu} a_i a^n b_{i \mu} (b_{i \mu} \in B)$ is an $\mathfrak{H}$-n.b.e. of $A/B$ then every $b_{i \mu}$ is non-zero by Corollary 2, whence we see that every $\sum_i a^n b_{i \mu}$ is a non-zero element of $B_r$. Hence, again by Corollary 2, $u$ is an $\mathfrak{H}_r$-n.b.e. of $A/B_0$.

In [1], a subgroup $H$ of a $p$-primary abelian group $G$ of finite order was called a regular subgroup if $G$ has a factorization $G = [g_1] \times \cdots \times [g_s]$ such that $H = [g_1^\sharp] \times \cdots \times [g_s^\sharp]$ with some $\alpha_i$, and [1, Lemma 2.4] proved that if $H$ is a subgroup of a finite $p$-primary abelian group $G$ and contains $G^p = \{g^p ; g \in G\}$ then it is a regular subgroup. By the light of this fact, we can prove now our principal theorem.

**Theorem 2.** Let $A$ be a division ring. If $A/B$ is an $\mathfrak{H}$-Kummer extension then it is $\mathfrak{H}$-completely basic, that is, any $\mathfrak{H}$-n.b.e. of $A/B$ is always an $\mathfrak{H}^*$-n.b.e. of $A/J(\mathfrak{H}, A)$ for every subgroup $\mathfrak{H}^*$ of $\mathfrak{H}$.

**Proof.** As is well-known, $\mathfrak{H} = \mathfrak{H}_1 \times \cdots \times \mathfrak{H}_r$, with the $p_i$-primary components $\mathfrak{H}_i$. If $\mathfrak{H}_i$ is a subgroup of $\mathfrak{H}$ with prime index $p_i$, then $\mathfrak{H}_i = \mathfrak{H}_i^* \times \mathfrak{H}_i^*$ with a subgroup $\mathfrak{H}_i^*$ of $\mathfrak{H}_i$ and $\mathfrak{H}_i^* \times \cdots \times \mathfrak{H}_i^*$. As $(\mathfrak{H}_i : \mathfrak{H}_i^*) = p_i$ implies $\mathfrak{H}_i^* \supseteq \mathfrak{H}_i$, $\mathfrak{H}_i^*$ is a regular subgroup of $\mathfrak{H}_i$ by [1, Lemma 2.4]. And so, by Lemma 1, we see that any $\mathfrak{H}$-n.b.e. of $A/B$ is an $\mathfrak{H}_r$-n.b.e. of $A/J(\mathfrak{H}, A)$. Now, the proof of our theorem will be completed by the induction with respect to the order of $\mathfrak{H}$.

**References**


Department of Mathematics, Hokkaido University

(Received April 10, 1964)