<table>
<thead>
<tr>
<th>Type</th>
<th>Instructions for use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>A NOTE ON NON-COMMUTATIVE KUMMER EXTENSIONS</td>
</tr>
<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>File Information</td>
<td>JFSHIU_18_N1-2_078-080.pdf</td>
</tr>
</tbody>
</table>

Hokkaido University Collection of Scholarly and Academic Papers : HUSCAP
A NOTE ON NON-COMMUTATIVE KUMMER EXTENSIONS

By

Masayuki ŌHORI and Hisao TOMINAGA

Let a simple ring $A$ (with 1 and minimum condition) be strictly Galois with respect to (an $F$-group) $\mathfrak{G}$ in the sense of [2]. Then $B=J(\mathfrak{G}, A)$ is a simple ring with $[A:B]=\# \mathfrak{G}$, 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 $\mathfrak{R}$ be an $F$-subgroup of $\mathfrak{G}$. If $N=J(\mathfrak{R}, A)$, then $A/N$ is strictly Galois with respect to $\mathfrak{R}$, $[N:B]=(\mathfrak{G}:\mathfrak{R})$ and $\mathfrak{G}(N)=\mathfrak{R}$. In particular, if $\mathfrak{R}$ is an invariant subgroup of $\mathfrak{G}$ then $\mathfrak{G}|N\equiv \mathfrak{G}/\mathfrak{R}$.

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

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

4°. Let $\mathfrak{G}$ 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 $a \in A^{*}$ such that $a_{\sigma}=a_{\sigma \zeta}$, there holds $A=\bigoplus_{i=0}^{m^{-1}} Ba^{i}=\bigoplus_{i=0}^{m^{-1}} a^{i}B$.

Further, $A/B$ was called an $\mathfrak{G}$-Kummer extension if $\mathfrak{G}$ 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 $\mathfrak{G}$-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 $1^{o}-4^{o}$, a slight modification of Faith's proof will accomplish our attempt. Firstly, we exhibit the following characterization of an $\mathfrak{G}$-Kummer extension.

**Theorem 1.** Let $\mathfrak{G}=\{\eta_{1}, \cdots, \eta_{m}\}$ be a $DF$-group of $A$ whose exponent is $m_{0}$. If $A/B$ is an $\mathfrak{G}$-Kummer extension then $A=\bigoplus_{i=1}^{m_{0}} a_{i}B=\bigoplus_{i=1}^{m_{0}} Ba_{i}$ with some $a_{i} \in A^{*}$ such that every $\zeta_{ij}=a_{i}^{-1} \cdot a_{0} \eta_{j}$ is contained in $B \cap C$, and conversely.
Proof. Let $\mathfrak{S} = \mathfrak{S}_1 \times \cdots \times \mathfrak{S}_e$ with cyclic $\mathfrak{S}_i = [\sigma_i]$ of order $m_i$. Then, the exponent $m_0$ of $\mathfrak{S}$ coincides with the least common multiple $\{m_1, \ldots, m_e\}$. Now, let $\zeta$ be a primitive $m_0$-th root of 1 contained in $B \cap C$, and let $\zeta_i = \zeta^{m_i/m_0}$, that is evidently a primitive $m_i$-th root of 1. Then, $\eta = \prod_{j=1}^{e} \sigma_i^{j-i} \rightarrow \zeta_i$ defines a homomorphism of $\mathfrak{S}$ into $(B \cap C)^e$ (i.e., $e$, $\eta$). Thus, by $3^e$, there exists an element $x_\epsilon \in A$ such that $x_\epsilon \sigma_i = x_\epsilon \zeta_i$ and $x_\epsilon \sigma_j = x_\epsilon$ for all $j \neq i$. Noting that $J(\mathfrak{S}_2 \times \cdots \times \mathfrak{S}_e, A)$ contains $x_\epsilon$ and is strictly Galois with respect to $\mathfrak{S}$, by 1$^e$, 4$^e$ yields at once $J(\mathfrak{S}_2 \times \cdots \times \mathfrak{S}_e, A) = \oplus_{i=0}^{m_i-1} x_i^i B$. Repeating similar arguments, we obtain $J(\mathfrak{S}_1 \times \cdots \times \mathfrak{S}_e, A) = \oplus_{i=0}^{m_i-1} x_i^i B(\mathfrak{S}_1 \times \cdots \times \mathfrak{S}_e, A) = \oplus_{0 \leq t_i \leq m_i} x_i^i B$, in particular, $A = \oplus_{0 \leq t_i \leq m_i} x_i^i B$. If $\eta = \prod_{i=1}^{e} \sigma_i^{t_i}$ (0$\leq t_i < m_i$) is an arbitrary element of $\mathfrak{S}$ and $a = x_\epsilon \cdots x_i^i$, then it is easy to see $a\eta = a\zeta^{\epsilon e} \cdots \zeta_i^{t_i}$, so that $a^{-1} \cdot a\eta = \zeta^{t_1} \cdots \zeta_i^{t_i}$ is contained in $B \cap C$, as desired. Conversely, assume that $A = \oplus_{i=0}^{m_i-1} a_i B$ (a$\in A$) and every $\zeta_{ij} = a_i^{-1} \cdot a_i \eta_j$ is contained in $B \cap C$. As $\zeta_{ij}$ is contained in $B$, it will be easy to see that $\zeta_{ij}^k = a_i^{-1} \cdot a_i \eta_j^k$ for $k = 0, 1, \ldots$. We see therefore that if $\eta_j$ is of order $k$ then $a_i \eta_j^k = a_i$ and $\zeta_{ij} = 1$, whence it follows that some one among $\zeta_{ij}$ (i.e., $0, \cdots, m$) 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 $a = \sum_{i=1}^{m_i} a_i b_i$ (b$\in B$) is an arbitrary element of $A$ then $a\eta_i = \sum_{i=1}^{m_i} a_i b_i \eta_i = \sum_{i=1}^{m_i} a_i b_i \zeta_{ij} = a_i \eta_i \zeta_{ij}$, which asserts $\mathfrak{S}$ is abelian.

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

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

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

Proof. By assumption, $a\eta_i = \sum_{i=1}^{m} a_i \eta_i \cdot b_i = \sum_{i=1}^{m} a_i b_i \zeta_{ij}$. Accordingly, $a$ is an $\mathfrak{S}$-n.b.e. if and only if the matrix $(b_i \zeta_{ij}) = \left( \begin{array}{c} b_1 \\ 0 \\ b_m \end{array} \right)$ is regular. In any case, $A$ contains an $\mathfrak{S}$-n.b.e. by $2^e$, so that the matrix $(b_i \zeta_{ij})$ is regular for some choice of $b_i$, whence it follows the matrix $(\zeta_{ij})$ is regular. Thus, $a$ is an $\mathfrak{S}$-n.b.e. if and only if $(\begin{array}{c} b_1 \\ 0 \\ b_m \end{array})$ is regular, that is, every $b_i$ is in $B$.

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

Proof. Let $B_i = J(\mathfrak{S}_i, A)$ (i=0, 1, 2), and $\mathfrak{S}^* = \mathfrak{S}_0 \cap \mathfrak{S}_1 = [\sigma_i]$ 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 $a_i = 1$, $a_2$, $\cdots$, $a_n \in B_1$ and $a \in B_2$ such that $A = \bigoplus_{0 \leq j < m_i} a_j a^j B$, $a_i^{-1} \cdot a \eta \in B \cap C$ for each $\eta \in \mathfrak{H}_0$, and $a \sigma_i = a \sigma_i$, where $\sigma_i$ is a primitive $m_i$-th root of 1 contained in $B \cap C$. If $n_i = m_i/s$ then $a^{n_i} \sigma_i = a^{n_i}$, so that $\{a^{n_i} ; 0 \leq \lambda < s\}$ forms a right $B$-basis of $B_0$ by 1°. It follows therefore $(a_i a^\mu ; 1 \leq i \leq n, 0 \leq \mu < n_1)$ is a right $B_0$-basis of $A$ and $(a_i a^\mu)^{-1}$. $(a_i a^\mu) \eta \in B \cap C$ for each $\eta \in \mathfrak{H}_0$. Now, if $u = \sum_{i, \mu, \lambda} a_i a^\mu a^{n_1 \lambda} b_{ip \lambda} \in B_{1\mu \lambda}$ is an n.b.e. of $A/B$ then every $b_{ip \lambda}$ is non-zero by Corollary 2, whence we see that every $\sum_1 a^{n_1} b_{ip \lambda}$ is a non-zero element of $B_0$. Hence, again by Corollary 2, $u$ is an $\mathfrak{H}_0$-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 $G = [g_1] \times \cdots \times [g_r]$ such that $H = [g_1^*] \times \cdots \times [g_r^*]$ with some $\alpha_i$'s 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, $\mathfrak{H} = \mathfrak{H}_1 \times \cdots \times \mathfrak{H}_t$ 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 $\mathfrak{H}_i = \mathfrak{H}_i^* \times \mathfrak{H}_2^*$ with a subgroup $\mathfrak{H}_1^*$ of $\mathfrak{H}_1$ and $\mathfrak{H}_2^* = \mathfrak{H}_2 \times \cdots \times \mathfrak{H}_t$. As $(\mathfrak{H}_1 : \mathfrak{H}_1^*) = p_i$ implies $\mathfrak{H}_1^* \supseteq \mathfrak{H}_1^*$, $\mathfrak{H}_1^*$ is a regular subgroup of $\mathfrak{H}_1$ by [1, Lemma 2.4]. And so, by Lemma 1, we see that any $\mathfrak{H}$-n.b.e. of $A/B$ is an $\mathfrak{H}$-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)