A NOTE ON NON-COMMUTATIVE KUMMER EXTENSIONS

By

Masayuki ÔHORI 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 $\mathfrak{H}|N\cong\mathfrak{H}/\mathfrak{N}$.

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 $\sigma\to x_\sigma$ is an anti-homomorphism of $\mathfrak{H}$ into $B^\cdot$ (the multiplicative group of units of B) then there exists an element $x\in A^\cdot$ such that $x\sigma=xx_\sigma$.

4°. Let $\mathfrak{H}$ be cyclic with a generator σ 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 $a\in A^\cdot$ such that $a\sigma=a\zeta$, there holds $A=\oplus_{i=0}^{m-1}Ba^i=\oplus_{i=0}^{m-1}a^iB$.

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 $A=\oplus_{i=1}^m a_iB=\oplus_{i=1}^m Ba_i$ with some $a_i\in A^\cdot$ such that every $\zeta_{ij}=a_i^{-1}\cdot a_i\eta_j$ 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_0 of $\mathfrak{H}$ coincides with the least common multiple $\{m_1,\cdots,m_e\}$. Now, let ζ be a primitive m_0-th root of 1 contained in $B\cap C$, and let $\zeta_i=\zeta^{m_0/m_i}$, that is evidently a primitive m_i-th root of 1. Then, $\eta=\prod_{j=1}^{e}\sigma_j^{t_j}\to\zeta_i^{t_i}$ defines a homomorphism of $\mathfrak{H}$ into $(B\cap C)^{\cdot}$ $(i=1,\cdots,e)$. Thus, by 3°, there exists an element $x_i\in A^{\cdot}$ such that $x_i\sigma_i=x_i\zeta_i$ and $x_i\sigma_j=x_i$ for all $j\neq i$. Noting that $J(\mathfrak{H}_2\times\cdots\times\mathfrak{H}_e, A)$ contains x_1 and is strictly Galois with respect to $\mathfrak{H}_1$ by 1°, 4° yields at once $J(\mathfrak{H}_2\times\cdots\times\mathfrak{H}_e, A)=\oplus_{t=0}^{m_1-1}x_1^tB$. Repeating similar arguments, we obtain $J(\mathfrak{H}_{j+1}\times\cdots\times\mathfrak{H}_e, A)=\oplus_{t=0}^{m_j-1}x_j^tJ(\mathfrak{H}_j\times\cdots\times\mathfrak{H}_e, A)=\oplus_{0\leqslant t_i<m_i}x_j^{t_j}\cdots x_1^{t_1}B$, in particular, $A=\oplus_{0\leqslant t_i<m_i}x_e^{t_e}\cdots x_1^{t_1}B$. If $\eta=\prod_{i=1}^{e}\sigma_i^{s_i}$ $(0\leqslant s_i<m_i)$ is an arbitrary element of $\mathfrak{H}$ and $a=x_e^{t_e}\cdots x_1^{t_1}$ then it is easy to see $a\eta=a\zeta_e^{t_es_e}\cdots\zeta_1^{t_1s_1}$, so that $a^{-1}\cdot a\eta=\zeta_e^{t_es_e}\cdots\zeta_1^{t_1s_1}$ is contained in $B\cap C$, as desired. Conversely, assume that $A=\oplus_{i=1}^{m}a_iB$ $(a_i\in A^{\cdot})$ and every $\zeta_{ij}=a_i^{-1}\cdot a_i\eta_j$ is contained in $B\cap C$. As ζ_{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 $k=0,1,\cdots$. We see therefore that if η_j is of order k then $a_i\eta_j^k=a_i$ and $\zeta_{ij}^k=1$, whence it follows that some one among ζ_{ij} $(i=1,\cdots,m)$ is a primitive k-th root of 1. We see accordingly $B\cap C$ contains a primitive m_0-th root of 1. Next, if $a=\sum_{i=1}^{m}a_ib_i$ $(b_i\in B)$ is an arbitrary element of A then $a\eta_s\eta_t=\sum_{i=1}^{m}a_i\eta_s\eta_t\cdot b_i=\sum_{i=1}^{m}a_ib_i\zeta_{it}\zeta_{is}=a\eta_t\eta_s$, 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 $A=B_1B_2=B_2B_1$ and every $\mathfrak{H}_2$-n.b.e. of B_1/B is an $\mathfrak{H}_2$-n.b.e. of A/B_2.*

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

Proof. By assumption, $a\eta_j=\sum_{i=1}^{m}a_i\eta_j\cdot b_i=\sum_{i=1}^{m}a_ib_i\zeta_{ij}$. Accordingly, a is an $\mathfrak{H}$-n.b.e. if and only if the matrix $(b_i\zeta_{ij})=\begin{pmatrix}b_1 & & 0\\ & \ddots & \\ 0 & & b_m\end{pmatrix}(\zeta_{ij})$ is regular. In any rate, A contains an $\mathfrak{H}$-n.b.e. by 2°, so that the matrix $(b_i\zeta_{ij})$ is regular for some choice of b_i, whence it follows the matrix (ζ_{ij}) is regular. Thus, a is an $\mathfrak{H}$-n.b.e. if and only if $\begin{pmatrix}b_1 & & 0\\ & \ddots & \\ 0 & & b_m\end{pmatrix}$ is regular, that is, every b_i is in $B^{\cdot}$.

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 $A/J(\mathfrak{H}_0, A)$.*

Proof. Let $B_i=J(\mathfrak{H}_i, A)$ $(i=0,1,2)$, and $\mathfrak{H}_1^*=\mathfrak{H}_0\cap\mathfrak{H}_1=[\sigma_1^s]$ with a positive divisor s of m_1. 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 $a_1=1$, $a_2, \cdots, a_n\in B_1$ and $a\in B_2$ such that $A=\oplus_{0\leqslant j<m_1}^{1\leqslant i\leqslant n} a_i a^j B$, $a_i^{-1}\cdot a_i\eta\in B\cap C$ for each $\eta\in\mathfrak{H}_2$, and $a\sigma_1=a\zeta_1$ where ζ_1 is a primitive m_1-th root of 1 contained in $B\cap C$. If $n_1=m_1/s$ then $a^{n_1}\sigma_1^s=a^{n_1}$, so that $\{a^{n_1\lambda};\ 0\leqslant\lambda<s\}$ forms a right B-basis of B_0 by 1°. It follows therefore $\{a_i a^\mu;\ 1\leqslant i\leqslant n,\ 0\leqslant\mu<n_1\}$ is a right B_0-basis of A and $(a_i a^\mu)^{-1}\cdot(a_i a^\mu)\eta\in B\cap C$ for each $\eta\in\mathfrak{H}_0$. Now, if $u=\sum_{i,\mu,\lambda} a_i a^\mu a^{n_1\lambda} b_{i\mu\lambda}$ $(b_{i\mu\lambda}\in B)$ is an $\mathfrak{H}$-n.b.e. of A/B then every $b_{i\mu\lambda}$ is non-zero by Corollary 2, whence we see that every $\sum_\lambda a^{n_1\lambda} b_{i\mu\lambda}$ 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 $G=[g_1]\times\cdots\times[g_t]$ such that $H=[g_1^{\alpha_1}]\times\cdots\times[g_t^{\alpha_t}]$ with some α_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, $\mathfrak{H}=\mathfrak{H}_1\times\cdots\times\mathfrak{H}_t$ with the p_i-primary components $\mathfrak{H}_i$. If $\mathfrak{H}_0$ is a subgroup of $\mathfrak{H}$ with prime index p_1, then $\mathfrak{H}_0=\mathfrak{H}_1^*\times\mathfrak{H}_2^*$ with a subgroup $\mathfrak{H}_1^*$ of $\mathfrak{H}_1$ and $\mathfrak{H}_2^*=\mathfrak{H}_2\times\cdots\times\mathfrak{H}_t$. As $(\mathfrak{H}_1:\mathfrak{H}_1^*)=p_1$ implies $\mathfrak{H}_1^*\supseteq\mathfrak{H}_1^p$, $\mathfrak{H}_1^*$ 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 $\mathfrak{H}_0$-n.b.e. of $A/J(\mathfrak{H}_0, A)$. Now, the proof of our theorem will be completed by the induction with respect to the order of $\mathfrak{H}$.

References

[1] C. C. FAITH: Extensions of normal bases and completely basic fields, Trans. Amer. Math. Soc., 85 (1957), 406–427.

[2] T. NAGAHARA, T. ONODERA and H. TOMINAGA: On normal basis theorem and strictly Galois extensions, Math. J. Okayama Univ., 8 (1958), 133–142.

[3] N. NOBUSAWA and H. TOMINAGA: Some remarks on strictly Galois extensions of simple rings, Math. J. Okayama Univ., 9 (1959), 13–17.

Department of Mathematics,
Hokkaido University

(Received April 10, 1964)