SOME REMARKS ON STRICTLY GALOIS EXTENSIONS OF SIMPLE RINGS

NOBUO NOBUSAWA and HISAO TOMINAGA

Let K be a finite dimensional Galois (normal and separable) extension field of L, and $\mathfrak{G}$ the Galois group of K/L. Then the following is well-known as a theorem of Noether-Speiser : The 1-dimensional cohomology group $H^1(K^*, \mathfrak{G})$ is trivial, where K^* is the multiplicative group consisting of all the regular (non-zero) elements of K. On the other hand, considering K as an additive group, $H^1(K, \mathfrak{G})$ is also trivial [4], and this fact is of use in studying Galois extensions of degree p^e over a field of characteristic p.

In this note, we shall try to extend these theorems mentioned above to simple rings. In fact, under the assumption that the extension considered is strictly Galois with respect to an F-group, these are still true (Theorem 1 and Theorem 2). And in the final section, as applications of these generalizations, several abelian extensions will be treated.

Finally, as to notations and terminologies used in this note, we follow [2] and [3].

1°. Let R be a simple ring (with an identity elemenet and minimum condition), and $\mathfrak{G}$ a finite group consisting of automorphisms of R. If the subring $V(\mathfrak{G})$ generated by all the regular elements of R which induce inner automorphisms contained in $\mathfrak{G}$ is a (two-sided) simple ring [division ring], then $\mathfrak{G}$ is called an *F-group* [*DF-group*]. Here, needless to say, if R is a division ring then every finite $\mathfrak{G}$ is a *DF-group* necessarily. For F-groups, the following fact will be most fundamental [2] : *Let $\mathfrak{G}$ be an F-group, and $S = J(\mathfrak{G}, R)$. Then R is Galois over the simple ring S, $[R : S] \leqq$ order of $\mathfrak{G}$, $V(\mathfrak{G}) = V_R(S)$ which is finite over $V_R(R)$, and* $\mathrm{Hom}_{S_l}(R, R) = \mathfrak{G}R_r$. By the light of this fact, we have introduced the following definition [2] : Let $\mathfrak{G}$ be an F-group, and $S = J(\mathfrak{G}, R)$. If $[R : S] =$ order of $\mathfrak{G}$, then we say that R(or R/S) is *strictly Galois* with respect to $\mathfrak{G}$. In what follows, we always assume that *R is a simple ring which is strictly Galois with respect to* $\mathfrak{G}$, and set $S = J(\mathfrak{G}, R)$.

Now, for the sake of the later use, we set here the following lemma whose second assertion is [2, Theorem 4].

Lemma 1. (1) $\mathfrak{G}R_r = \sum_{\sigma\in\mathfrak{G}} \oplus \sigma R_r$, *and they are simple rings.*

(2) *R possesses a $\mathfrak{G}$-noraml basis element, that is, there exists some $r \in R$ such that $R = \sum_{\sigma\in\mathfrak{G}} \oplus (r\sigma)S$.*

Lemma 2. *Let M be a unitary (right) R-module finite over R. If*

for each $\sigma \in \mathfrak{G}$ there correspond semi-linear automorphisms belonging to σ θ_σ, $\bar{\theta}_\sigma$, and there hold $\theta_\sigma\theta_\tau = \theta_{\sigma\tau}$ and $\bar{\theta}_\sigma\bar{\theta}_\tau = \bar{\theta}_{\sigma\tau}$ ($\sigma, \tau \in \mathfrak{G}$), then we can find an R-automorphism η of M such that $\bar{\theta}_\sigma = \eta^{-1}\theta_\sigma\eta$.

Proof. Evidently, $\mathfrak{R} = \sum_{\sigma\in\mathfrak{G}} \theta_\sigma R$ and $\bar{\mathfrak{R}} = \sum_{\sigma\in\mathfrak{G}} \bar{\theta}_\sigma R$ are subrings of $\mathfrak{A} = \mathrm{Hom}(M, M)$ which are homomorphic images of the simple ring $\mathfrak{G}R_r = \sum \oplus \sigma R_r$ (Lemma 1 (1)). Thus, $\mathfrak{R}$ and $\bar{\mathfrak{R}}$ are isomorphic simple rings (containing R), and then $\varphi : \sum \theta_\sigma r_\sigma \to \sum \bar{\theta}_\sigma r_\sigma$ is a (ring) isomorphism of $\mathfrak{R}$ onto $\bar{\mathfrak{R}}$. Then, by [1, Theorem 1 2)], there exists an automorphism $\eta \in \mathfrak{A}$ such that $\lambda\varphi = \eta^{-1}\lambda\eta$ for $\lambda \in \mathfrak{R}$. Noting that $r = r\varphi = \eta^{-1}r\eta$ for $r \in R$, we obtain $\eta \in V_{\mathfrak{A}}(R)$, as desired.

The next lemma may be more or less known, however, for the sake of completeness, we shall give here the proof.

Lemma 3. *Let D be a division ring, and K a subfield of D. Then the equation $f(x) = d_0x^m + d_1x^{m-1} + \ldots + d_m = 0$ ($d_i \in D$; $d_0 \neq 0$) possesses at most m different roots in K.*

Proof. Suppose $k_1, \ldots, k_{m+1} \in K$ be $m+1$ different roots of $f(x) = 0$. Then the simultaneous linear equations $\sum_{j=0}^{m} y_j k_i^{m-j} = 0$ ($i = 1, \ldots, m+1$) possess a non-trivial solution $(d_0, d_1, \ldots, d_m)$ in D. Since all the k_i^{m-j}'s are in K, the last equations possess a non-trivial solution $(c_0, c_1, \ldots, c_m)$ in K too. Thus, the (non-trivial) equation $g(x) = c_0x^m + c_1x^{m-1} + \ldots + c_m = 0$ of degree at most m possesses $m+1$ different roots k_i's in K, which is a contradiction.

Lemma 4. *Let $A \supseteq B$ be simple rings with the same identity element 1, and $\mathfrak{H} = \{\sigma^i\}$ a cyclic group of order n generated by a B-(ring) automorphism σ of A. If (the field) $V_B(A)$ contains a primitive n-th root ζ of 1, and a is a regular element of A such that $a\sigma = a\zeta$, then there holds $[B[a] : B]_l \geqq n$.*

Proof. It suffices to prove our lemma for the case where a is a root of a (non-zero) polynomial with left coefficients in B. We take here such a polynomial of the lowest degree : $f(x) = b_0x^m + b_1x^{m-1} + \ldots + b_m$ ($b_i \in B$; b_0, $b_m \neq 0$). Then,

$f(a)\sigma^i = b_0a^m\zeta^{im} + b_1a^{m-1}\zeta^{i(m-1)} + \ldots + b_m = 0$ ($i = 0, 1, \ldots, n-1$).

Now let $A = \sum_{h,k=1}^{l} De_{hk}$, where e_{hk}'s are matrix units and $D = V_A(\{e_{hk}\})$ is a division ring. Since $b_0a^m \neq 0$, one of the components of its representation in $\sum De_{hk}$, say, the (p, q)-component is non-zero. Noting that $D \supseteq V_B(A) \ni \zeta$, we obtain

$d_0\zeta^{im} + d_1\zeta^{i(m-1)} + \ldots + d_m = 0$ ($i = 0, 1, \ldots, n-1$),

where $d_0, d_1, \ldots, d_m \in D$ are the (p, q)-components of $b_0a^m, b_1a^{m-1}, \ldots, b_m$ respectively. Hence, d_0 being non-zero, Lemma 3 shows $m \geqq n$.

Consequently, we have $[B[a] : B]_l \geqq n$.

To be easily seen from the proof of Lemma 4, we obtain

Corollary 1. *Let $\mathfrak{G} = \{\sigma^i\}$ be cyclic and of order n. If $V_S(R)$ contains a primitive n-th root ζ of 1, and x is a regular element of R such that $x\sigma = x\zeta$, then $R = \sum_{i=0}^{n-1} \oplus Sx^i$.*

2°. Speiser's theorem can be generalized in the following way:

Theorem 1. *Let R be strictly Galois with respect to $\mathfrak{G}$, and $S = J(\mathfrak{G}, R)$. If for each $\sigma \in \mathfrak{G}$ there corresponds a regular matrix γ_σ of the $n \times n$ matrix ring $(R)_n$ over R, and there holds*

$$(*) \qquad \gamma_\tau(\gamma_\sigma{}^\tau) = \gamma_{\sigma\tau} \qquad (\sigma, \tau \in \mathfrak{G}),$$

then we can find a regular matrix $\alpha \in (R)_n$ such that $\gamma_\sigma = \alpha^{-1}(\alpha\sigma)$, and conversely.

Proof. Let $M = u_1R + \ldots + u_nR$ be an R-module with $u_1, \ldots, u_n$ as a linearly independent basis. Then θ_σ: $\sum u_i x_i \to \sum u_i \sum r_{ij}(\sigma)(x_j\sigma)$ where $(r_{ij}(\sigma)) = \gamma_\sigma$ is evidently a semi-linear automorphism of M belonging to σ, and by the light of (*) one readily see that $\theta_\sigma\theta_\tau = \theta_{\sigma\tau}(\sigma, \tau \in \mathfrak{G})$. Similarly, $\bar{\theta}_\sigma$: $\sum u_i x_i \to \sum u_i(x_i\sigma)$ is also a semi-linear automorphism belonging to σ, and there holds $\bar{\theta}_\sigma\bar{\theta}_\tau = \bar{\theta}_{\sigma\tau}(\sigma, \tau \in \mathfrak{G})$. Hence, by Lemma 2, there exists an R-automorphism η of M such that $\theta_\sigma\eta = \eta\bar{\theta}_\sigma$. Setting here $u_j\eta = \sum u_i a_{ij}$, one can easily verify that $\alpha = (a_{ij})$ is a desired one.

Corollary 2. *If $\sigma \to s_\sigma$ is an anti-homomorphism of $\mathfrak{G}$ into the multiplicative group of all the regular elements of S, then there exists a regular element $x \in R$ such that $x\sigma = xs_\sigma$.*

3°. Our generalization of the second is the next

Theorem 2. *Let R be strictly Galois with respect to $\mathfrak{G}$, and $S = J(\mathfrak{G}, R)$. If for each $\sigma \in \mathfrak{G}$ there corresponds an element $x_\sigma \in R$, and there holds*

$$(**) \qquad x_\sigma{}^\tau + x_\tau = x_{\sigma\tau} \qquad (\sigma, \tau \in \mathfrak{G}),$$

then we can find an element $x \in R$ such that $x_\sigma = x - x\sigma$, and conversely.

Proof. By Lemma 1 (2), R possesses a $\mathfrak{G}$-normal basis element r. Noting that $s = T_{\mathfrak{G}}(r) \in S$ is a regular element, we obtain $T_{\mathfrak{G}}(r') = 1$ where $r' = rs^{-1}$. Now we set $x = \sum_{\tau \in \mathfrak{G}} x_\tau(r'{}^\tau)$. Then, by (**), $x\sigma = \sum_\tau (x_\tau\sigma)(r'{}^\tau\sigma) = \sum_\tau (x_{\tau\sigma} - x_\sigma)(r'{}^\tau\sigma) = \sum_\tau x_{\tau\sigma}(r'{}^\tau\sigma) - x_\sigma \sum_\tau r'{}^\tau\sigma = x - x_\sigma$.

Corresponding to Corollary 2, we obtain

Corollary 3. *Let $\sigma \to s_\sigma$ be a homomorphism of $\mathfrak{G}$ into the additive group S. Then there exists an element $x \in R$ such that $s_\sigma = x - x\sigma$.*

Further, the following will be also easily seen.

Corollary 4. *Let* $\mathfrak{G}=\{\sigma^i\}$ *be cyclic. If* $T_{\mathfrak{G}}(r)=0$, *then there exists an element* $x\in R$ *such that* $r=x-x\sigma$.

4°. If R is strictly Galois with respect to an abelian DF-group $\mathfrak{G}$, then we may say that R is *abelian* with respect to $\mathfrak{G}$ (or R/S is *abelian* with respect to $\mathfrak{G}$ where $S=J(\mathfrak{G}, R)$). The following remarks will be readily seen from [2] and [3]: Let R be abelian with respect to $\mathfrak{G}$, and $\mathfrak{H}$ an arbitrary subgroup of $\mathfrak{G}$. Then R is abelian with respect to $\mathfrak{H}$, furthermore $T=J(\mathfrak{H}, R)$ is abelian with respect to $\mathfrak{G}/\mathfrak{H}$, where $\mathfrak{G}/\mathfrak{H}$ and $\mathfrak{G}_T$ may be identified.

Theorem 3. *Let* R *be abelian with respect to* $\mathfrak{G}$ *of exponent* n, *and* $V_S(R)$ *contain a primitive* n*-th root of* 1. *If* $\mathfrak{G}=\mathfrak{G}_1\times\ldots\times\mathfrak{G}_e$ *where* $\mathfrak{G}_i=\{\sigma_i^j\}$ *is cyclic and of order* n_i, *then there exist regular elements* $x_1, \ldots, x_e\in R$ *such that*: (1) $x_i^{n_i}\in S$, (2) $R=S[x_1, \ldots, x_e]$, (3) $S[x_i]\cap S[x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_e]=S$, (4) $S[x_i]/S$ *is abelian with respect to* $\mathfrak{G}_i$, *and* (5) *if* G *is the subgroup of* R^*(= *the multiplicative group consisting of all the regular elements of* R) *generated by* $x_1, \ldots, x_r$, *then* $G\cap S$ *is a normal subgroup of* G *and* $G/(G\cap S)$ *is isomorphic to* $\mathfrak{G}$.

Proof. Let ζ_i be a primitive n_i-th root of 1 contained in $V_S(R)$. Then $\mathfrak{G}\ni\sigma=\Pi\sigma_j^{t_j}\to\zeta_i^{t_i}$ defines a homomorphism of $\mathfrak{G}$ into the multiplicative group of $V_S(R)$. Thus, by Corollary 2, there exists a regular element $x_i\in R$ such that $x_i\sigma_i=x_i\zeta_i$ and $x_i\sigma_j=x_i$ for $j\neq i$. Evidently, $x_i^{n_i}=(x_i\sigma)^{n_i}=(x_i^{n_i})\sigma$ for all $\sigma\in\mathfrak{G}$, whence we have $x_i^{n_i}\in S$. Noting that $J(\mathfrak{G}_2\times\ldots\times\mathfrak{G}_e, R)$ is strictly Galois with respect to $\mathfrak{G}_1$ and contains x_1, Corollary 1 shows at once $J(\mathfrak{G}_2\times\ldots\times\mathfrak{G}_e, R)=S[x_1]$. Repeating the similar arguments, we obtain $J(\mathfrak{G}_{j+1}\times\ldots\times\mathfrak{G}_e, R)=S[x_1, \ldots, x_j]$, in particular, $R=S[x_1, \ldots, x_e]$. And so, (1)—(4) are proved. Further, recalling that every ζ_i is contained in $V_S(R)$, we have $(x_isx_i^{-1})\sigma=x_isx_i^{-1}$ for any $s\in S$ and $\sigma\in\mathfrak{G}$, whence $x_isx_i^{-1}\in S$. Hence $G\cap S$ is a normal subgroup of $\mathfrak{G}$. Similarly, it is easy to see that $(x_kx_jx_k^{-1}x_j^{-1})\sigma_i=x_kx_jx_k^{-1}x_j^{-1}$, or what is the same, that $x_kx_jx_k^{-1}x_j^{-1}\in S$, whence $G/(G\cap S)$ is abelian. (5) is therefore a direct consequence of (1)—(4) and Corollary 1.

Finally, as an application of Theorem 2, we shall present the following

Theorem 4. *Let a division ring* R *be abelian with respect to* $\mathfrak{G}$, *and of characteristic* p. *If* $\mathfrak{G}=\mathfrak{G}_1\times\ldots\times\mathfrak{G}_e$ *where* $\mathfrak{G}_i=\{\sigma_i^j\}$ *is of order* p, *then there exist elements* $x_1, \ldots, x_e\in R$ *such that*: (1) $x_i^p-x_i\in S$, (2) $R=S[x_1, \ldots, x_e]$, (3) $S[x_i]\cap S[x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_e]=S$, *and* (4) $S[x_i]/S$ *is abelian with respect to* $\mathfrak{G}_i$.

Proof. Evidently, $\mathfrak{G}\ni\sigma=\Pi\sigma_j^{t_j}\to t_i$ is a homomorphism of $\mathfrak{G}$ into the additive group S. Hence, by Corollary 3, there exists an element $x_i\in$

R such that $x_i\sigma_i = x_i - 1$ and $x_i\,\sigma_j = x_i$ for $j \neq i$. Since $(x_i^p)\,\sigma_i = (x_i - 1)^p = x_i^p - 1$, we have $(x_i^p - x_i)\,\sigma_i = x_i^p - x_i$, whence it follows $x_i^p - x_i \in S$. Now, the rest of the proof is easy.

Remark 1. Let a simple ring R be Galois over S. If the totality $\mathfrak{G}$ of all the S-inner automorphisms is abelian, then it is known that $V_R(S)$ is commutative. However, one may remark here that in case R is abelian with respect to $\mathfrak{G}$, $V_R(S)$ is not always commutative. In fact, a quaternion division algebra will provide a counter example.

Remark 2. The extension R/S considered in Theorem 3 may be regarded as a natural generalization of the notion of Kummer's extensions.

REFERENCES

[1] G. AZUMAYA, New foundation of the theory of simple rings, Proc. Japan Acad., 22 (1946) 325—332.

[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] H. TOMINAGA, A note on Galois theory of primary rings, Math. J. Okayama Univ., 8 (1958) 117—124.

[4] E. WITT, Der Existenzsatz für abelsche Funktionenkörper, J. f. d. r. u. angew. Math., 173 (1935) 43—51.

DEPARTMENTS OF MATHEMATICS,
OSAKA UNIVERSITY
HOKKAIDO UNIVERSITY

(Received August 6, 1959)