ON GALOIS EXTENSIONS OVER A FIELD AND ABELIAN GALOIS GROUPS

Dedicated to Professor Mikao Moriya on his 60th birth day

HISAO TOMINAGA

Throughout the present paper, we use the following conventions: $A \supseteq 1$ is always a simple ring (with minimum condition), B a unital simple subring of A, and $\mathfrak{G}$ means the group of all B-(ring) automorphisms of A. We set $C=V_A(A)$, $Z=V_B(B)$, $V=V_A(B)$ and $H=V_A^2(B)=V_A(V)$. Finally, as to other notations and terminologies used in this paper, we follow [5] and [9].

In [8], we have proved the following proposition that plays often important roles in Galois theory of simple rings (cf. [2], [5] and [6]).

Proposition 1. *If* $[A:C]<\infty$ then $[B:Z]<\infty$. *Conversely, if* $[A:B]_l<\infty$ *and* $[B:Z]<\infty$ *then* $[A:C]<\infty$.

One of the purposes of this paper is to present several results concerning Galois extensions over a field and Galois extensions with abelian Galois groups (§ 1). Prop. 1 will be used often to prove most of those results. Whereas, Prop. 1 was requested originally to prove that if $[A:B]_l=2$ and A is not of characteristic 2 then A/B is Galois [8]. In § 2, we shall present a new proof of the last fact without making use of Prop. 1.

§ 1. At first, we shall prove the following proposition that was cited in [2, § 1].

Proposition 2. *If A is outer Galois and finite over B and* $[B:Z]<\infty$ *then* $A=B\otimes_Z C$.

Proof. Since $[A:C]<\infty$ (Prop. 1), $V_A(B\cdot C)=V=C$ and $B\cdot C=B\otimes_Z C$ is simple, the principal theorem of simple rings yields at once $A=B\otimes_Z C$.

Corollary 1. *If A is outer Galois and left algebraic over a field B then A is a field.*

Proof. By [6, Lemma 4], A/B is locally finite. Hence, A/B is locally Galois by [5, Lemma 2.2], and our assertion is obvious by Prop. 2.

By the way, we shall show that [2, Cor. 2.2] can be extended as follows:

Proposition 3. *Let A/B be $\mathfrak{H}$-regular (or strictly Galois with respect to $\mathfrak{H}$). If Z is a perfect field of prime characteristic p and $\mathfrak{H}$ is of order p^e, then A/B is outer Galois. If moreover $[B:Z]<\infty$, then $A=B\otimes_Z C$.*

Proof. Since any derivation of the perfect field Z into B is 0, the case $e=1$ is obvious by [2, Th. 2.1 (c)]. Now, we shall proceed by the induction with respect to e. Assume $e>1$. If $\mathfrak{H}$ contains an inner automorphism different from 1, then $\mathfrak{H}_0=\mathfrak{H}\cap\tilde{V}$ is an invariant DF-subgroup of $\mathfrak{H}$ by [3, Th. 5], and $B_0=J(\mathfrak{H}_0, A)$ is $(\mathfrak{H}|B_0)$-regular over B by [9, Cor. 3]. Noting that B_0/B is outer Galois by the induction hypothesis, we see that the center of B_0 is still perfect. As is well known, $\mathfrak{H}_0$ contains an invariant subgroup $\mathfrak{P}$ of order p. Then, $J(\mathfrak{P}, A)/B_0$ is $(\mathfrak{H}_0|J(\mathfrak{P}, A))$-regular and the center of $J(\mathfrak{P}, A)$ is perfect. Hence, by the case $e=1$, $A/J(\mathfrak{P}, A)$ is outer Galois, which is a contradiction. The second assertion is now a direct consequence of the former and Prop. 2.

In [3, Th. 1], we have seen that if $\mathfrak{H}$ is an N-group of A with $B=J(\mathfrak{H}, A)$ then A is always $\mathfrak{H}B_r$-homomorphic to $\mathfrak{H}B_r$. If $\mathfrak{H}$ is abelian, we can prove the following:

Theorem 1. *If $\mathfrak{H}$ is an abelian N-group of A with $B=J(\mathfrak{H}, A)$, then A is $\mathfrak{H}B_r$-isomorphic to $\mathfrak{H}B_r$.*

Proof. If we set $A=\bigoplus_1^m x_iB$ $(m=[A:B])$ then $\mathrm{Hom}_{B_r}(A, A)=\mathfrak{H}A_r=\bigoplus_1^m\sigma_iA_r=\bigoplus_{i,j}\sigma_ix_{jr}B_r$ with some $\sigma_i\in\mathfrak{H}$([7, Th. 1]), and so the subring $\mathfrak{H}B_r$ of $\mathfrak{H}A_r$ satisfies the minimum condition for right ideals. If $\sigma=\sum_i\sigma_iy_{ir}$ $(y_i\in A)$ is an arbitrary element of $\mathfrak{H}$, then for each $\tau\in\mathfrak{H}$ there holds $\sum_i\tau\sigma_iy_{ir}=\tau\sigma=\sigma\tau=\sum_i\tau\sigma_i(y_i\tau)_r$, whence it follows $y_i=y_i\tau$ Hence, each y_i is contained in B, namely, $\mathfrak{H}B_r=\bigoplus_1^m\sigma_iB_r$. Accordingly, it follows $\mathfrak{H}A_r=A_r\mathfrak{H}=\bigoplus_{i,j}x_{jr}B_r\sigma_i=\bigoplus_1^m x_{jr}(\mathfrak{H}B_r)$. Noting that $A^{(m)}$(the direct sum of m copies of the $\mathfrak{H}A_r$-module A) is $\mathfrak{H}A_r$-isomorphic to $\mathfrak{H}A_r$, it is obvious that $A^{(m)}$ is $\mathfrak{H}B_r$-isomorphic to $(\mathfrak{H}B_r)^{(m)}$, and so Krull-Schmidt theorem yields the $\mathfrak{H}B_r$-isomorphism between A and $\mathfrak{H}B_r$.

Concerning a Galois extension with the abelian Galois group, there is a striking result that is essentially due to Faith [1, Th. 1].

Theorem 2. *Let A be Galois and finite over B, and $[B:Z]<\infty$. If $\mathfrak{G}$ is abelian then $V=C$ or $V\subseteq B$, and so A/B is either outer Galois or inner Galois. If moreover B is a field then either A is a field or B coincides with V.*

Proof. Assume that $\mathfrak{G}$ is not outer, namely, the field V does not coincides with C([1, prop. 1]). If x is in $V\setminus C$ then $x+c\in V$ (the multiplicative group of the regular elements in V) and $c=(x+c)-x$ for every

$c \in C$. We see therefore that V is generated by $V \setminus C$. Now, for arbitrary $x \in V \setminus C$ and $\sigma \in \mathfrak{G}$ there holds $\sigma\tilde{x}\sigma = \tilde{x}\sigma = \sigma\tilde{x}$, whence it follows $x\sigma = xc$ with some $c \in C$. Similarly, $(x-1)\sigma = (x-1)c'$ with some $c' \in C$. Accordingly, we obtain $x(c-c') = 1-c'$, so that $c = c' = 1$, which proves evidently $x\sigma = x$. Hence, it follows $C \subseteq V \subseteq B$. Noting that $[A : C] < \infty$ by Prop. 1, we readily obtain $V_A^2(B) = B$. The latter assertion is a consequence of Cor. 1.

In the rest of this section, we assume always that A is $\mathfrak{G}$-locally Galois over a field B and $\mathfrak{G}$ is abelian. Under this situation, the latter part of Th. 2 is still valid.

Corollary 3. *If A is $\mathfrak{G}$-locally Galois over a field B and $\mathfrak{G}$ is abelian, then either A is a field or B coincides with V, and so every intermediate ring of A/B is simple.*

Proof. By [5, Th. 2. 3], A/B is Galois. In case $\mathfrak{G}$ is outer, the commutativity of A has been shown in Cor. 1. Therefore, in what follows, we may restrict our attention to the case $V \neq C$. Let v be an arbitrary element in $V \setminus C$. Then, there exists $a \in A$ such that $va \neq av$. Now, for each $w \in V$, we can find a $\mathfrak{G}$-shade A' of $B[a, v, w]$. Since $\mathfrak{G}(A'/B)$ $(\subseteq \mathfrak{G}|A')$ is abelian and $V_{A'}(B)$ does not coincide with the center of A', $V_{A'}(B)$ coincides with B (Th. 2), which proves evidently $V = B$. The simplicity of every intermediate ring is then a consequence of [11, Cor. 2].

In what follows, we assume further that A is non-commutative, namely, A is inner Galois over the maximal subfield B (Cor. 3). We shall introduce here the following conditions:

(i) If C' is an intermediate field of B/C with $[B : C'] < \infty$, and T an intermediate ring of A/B with $V_T(T) \subseteq C'$, then there exists an intermediate ring B' of T/B with $V_{B'}(B') \subseteq C'$ and $[B' : B] < \infty$.

(ii) If C' is an intermediate field of B/C then there exists a family $\{C'_\alpha$'s$\}$ of intermediate fields C_α' of B/C such that $[B : C'_\alpha] < \infty$ and $\bigcap C'_\alpha = C'$.

(iii) If C' is an intermediate field of B/C with $[B' : C'] < \infty$ then $[C'' : C' \cap C''] < \infty$ for each intermediate field C'' of B/C.

If T and T' are arbitrary (simple) intermediate rings of A/B then $V_A(T) = V_{T'}(T) = V_B(T)$, and $J(\tilde{B}|T, T) = B$, so that T/B is always inner Galois. In particular, if $[T : B] < \infty$ then $[T : V_T(T)] = [B : V_T(T)]^2 = [T : B]^2 < \infty$.

Lemma 1. *Let $A \neq C$ be $\mathfrak{G}$-locally Galois over a field B, and let $\mathfrak{G}$ be abelian. Let C' be an intermediate field of B/C with $[B : C'] < \infty$, and T an intermediate ring of A/B with $V_T(T) \subseteq C'$. Assume the condi-*

tion (i). *If T' is an arbitrary intermediate ring of A/T then $V_{T'}(C')$ is a central simple algebra of finite rank over C'.*

Proof. By the condition (i), there exists an intermediate ring B' of T/B such that $V_{B'}(B') \subseteq C'$ and $[B' : B] < \infty$. Then, $[B' : V_{B'}(B')] < \infty$ by the above remark, and so we have $V^2_{B'}(C') = C'$. Hence, the center of $B'' = V_{B'}(C')$ coincides with C'. If $B^* = V_{T'}(C')$ $(\supseteq B'')$ then $C' \subseteq V_{B^*}(B^*) \subseteq V_{B^*}(B'') = V_{B'}(B'') = C'$, namely, $V_{B^*}(B'') = V_{B^*}(B^*) = C'$. We obtain therefore $\infty > [B'' : C'] = [B'' : V_{B^*}(B'')] = [B^* : C']$.

Now, we shall prove the following theorem that contains [4, Th. 2]. (Cf. [4, Lemma 2].)

Theorem 3. *Let $A \neq C$ be $\mathfrak{G}$-locally Galois over a field B, and let $\mathfrak{G}$ be abelian. If the conditions* (i), (ii) *and* (iii) *are satisfied, then there exists a* $1-1$ *dual correspondence between closed regular subgroups of $\mathfrak{G}$ and intermediate rings of A/B, in the usual sense of Galois theory.*

Proof. Let T be an arbitrary intermediate ring of A/B, and x an arbitrary element of $T' = V^2_A(T)$. If $T_1 = B[x]$ and $C_1 = V_{T_1}(T_1)$, then $\infty > [T_1 : B] = [B : C_1]$. Noting that $C_1 = V_{T'}(T_1) \supseteq V_{T'}(T') = V_T(T') = V_T(T)$, we see that $V_{T'}(C_1)$ and $V_T(C_1)$ are central simple algebras of finite rank over C_1 (Lemma 1). Hence, $[B : C_1]$ coincides with $[V_{T'}(C_1) : B]$ as well as with $[V_T(C_1) : B]$, and so x is contained in $V_{T'}(C_1) = V_T(C_1) \subseteq T$. We have proved thus $V^2_A(T) = T$. Next, we shall prove that $V^2_A(C') = C'$ for each intermediate field C' of B/C. By the condition (i), there exists a family $\{C_\alpha'\text{s}\}$ of intermediate fields C'_α of B/C such that $[B : C_\alpha'] < \infty$ and $\bigcap C_\alpha' = C'$. Since each $V_A(C'_\alpha)$ is a central simple algebra (of finite rank) over C_α' (Lemma 1), $C'_\alpha = V^2_A(C_\alpha') \cap V_A(C'_\alpha) = V^2_A(C_\alpha')$. It follows therefore $C' \subseteq V^2_A(C') \subseteq \bigcap V^2_A(C'_\alpha) = \bigcap C'_\alpha = C'$, nemely, $V^2_A(C') = C'$. Finally, we shall prove that A/T is left locally finite. Let F be an arbitrary finite subset of A. If we set $T^* = B[F]$ and $C^* = V_{T^*}(T^*)$, then $[B : C^*] = [T^* : B] < \infty$. Accordingly, if $C'' = V_T(T) = V_A(T)$ then $[C'' : C^* \cap C''] < \infty$ by the condition (iii). Since the center of $T_1 = V_A(C^* \cap C'')$ coincides with $V^2_A(C^* \cap C'') = C^* \cap C''$ by the second assertion cited above, we obtain $[T_1 : V_{T_1}(C'')] = [C'' : C^* \cap C''] < \infty$. Recalling here that $T_1 \supseteq V_A(C'') = V^2_A(T) = T$ by the first assertion cited above, it is evident that $T = V_A(C'') = V_{T_1}(C'')$. We obtain therefore $[T_1 : T] = [C'' : C^* \cap C'']$. Since T_1 contains obviously T^* as well as T, it follows then $[T[F] : T]_l \leqq [T_1 : T] < \infty$, which proves the left local finiteness of A/T. Since A is B-A-irreducible by [10, Th. 1], A is T-A-irreducible much more. Accordingly, A/T is h-Galois by [10, Prop. 4], and so $\mathfrak{G}(T) = \mathrm{Cl}\ \widetilde{V_A(T)}$ by [10, Th. 11 (a)].

§ 2. At first, we shall prove the following proposition.

Proposition 4. *Let A be left locally finite over B. If $\tilde{V}A_r$ is dense in $\mathrm{Hom}_{B_l}(A, A)$ then A/T is inner Galois for any simple intermediate ring T of A/B with $[T:B]_l<\infty$.*

Proof. In the proof of [10, Th. 1], we have $\mathfrak{G}(T^*, A/B)=\tilde{V}|T^*$ by [11, Cor. 1], so that $\mathfrak{M}_j=\sigma_j u_{j1}A_r=(v_{j1}|T^*)A_r$ for some $v_j\in V$. Recalling here that $v_{j1}|T^*$ is contained in $\mathrm{Hom}_{T_l}(T^*, A)$, we see that v_j is contained in $V_A(T)$. It follows therefore $M_j=(Te)\mathfrak{M}_j=v_j(TeA)=v_jM$ is a T-A-homomorphic image of M, which proves that A is homogeneously T-A-completely reducible. Hence, $V_A(T)$ is a simple ring. The rest of the proof is obvious by [11, Cor. 1].

Corollary 4. *If $[A:B]_l=2$ and $J(\mathfrak{G}, A)=B$ then A/B is Galois.*

Proof. Since $2=[A:B]_l=[\mathrm{Hom}_{B_l}(A, A):A_r]_r\geqq[\mathfrak{G}A_r:A_r]_r=(\mathfrak{G}:\tilde{V})\cdot[I(\mathfrak{G}):C]$ by [5, Lemmas 1. 3 (i), (iv) and 1. 4 (ii)] (those are valid without the assumption that B is regular), $\mathfrak{G}\neq 1$ yields at once $\mathrm{Hom}_{B_l}(A, A)=\mathfrak{G}A_r$. If $[I(\mathfrak{G}):C]=1$, then $\mathfrak{G}$ is an outer group of order 2, and then A/B is outer Galois. On the other hand, if $(\mathfrak{G}:\tilde{V})=1$ then $\mathrm{Hom}_{B_l}(A, A)=\tilde{V}A_r$, and so A/B is inner Galois by Prop. 4.

In the proof of Prop. 1 given in [8], the standard identity played an essential role. We shall remark finally that the following theorem [8, Th.] can be proved without making use of the standard identity.

Theorem 4. *If $[A:B]_l=2$, $[B:Z]<\infty$ and Z is not of characteristic 2, then A/B is Galois.*

Proof. Obviously, there exist no intermediate rings of A/B except A and B If $B=C$, there is nothing to prove. Next, if $B\supsetneqq C$ then $\mathfrak{G}\neq 1$, and then A/B is Galois by Cor. 4. Finally, we shall consider the case $B\not\supseteq C$. Let c be an arbitrary element of $C\backslash B$. Then, as we readily obtain $B\cap Bc=0$, there holds $A=B\oplus Bc$. Consequently, it follows $V=V_A(B\cdot C)=C$ and $Z=C\cap B$. We set here $c^2=b_1c+b_2$ $(b_i\in B)$. Then, for each $b\in B$ we have $(bb_1)c+bb_2=(b_1b)c+b_2b$, which implies $b_1, b_2\in Z=C\cap B$. Hence, $u=c-\frac{1}{2}b_1$ is an element of $C\backslash B$ (and so $A=B\oplus Bu$) and u^2 is contained in Z. Now, one will easily verify that the mapping $\sigma: x+yu\longrightarrow x-yu$ $(x, y\in B)$ is an automorphism of A with $J(\sigma, A)=B$.

REFERENCES

[1] C. C. FAITH: Abelian Galois groups, Proc. Amer. Math. Soc., 10 (1959), 767—774.
[2] K. KISHIMOTO: On cyclic extensions of simple rings, J. Fac. Sci. Hokkaido Univ.,

Ser. I, 19 (1966), 74—85.
[3] K. KISHIMOTO, T. ONODERA and H. TOMINAGA: On the normal basis theorems and the extension dimension, J. Fac. Sci. Hokkaido Univ., Ser. I, 18 (1964), 81—88.
[4] M. MORIYA, T. NAGAHARA and H, TOMINAGA: A note on Galois theory of division rings, Math. J. Okayama Univ., 7 (1957), 83—88.
[5] T. NAGAHARA and H. TOMINAGA: On Galois theory of simple rings, Math. J. Okayama Univ, 11 (1963), 79—117.
[6] T. NAGAHARA and H. TOMINAGA: Some theorems on Galois theory of simple rings, J. Fac. Sci. Hokkaido Univ., Ser. I, 17 (1963), 1—13.
[7] T, NAGAHARA, T. ONODERA and H. TOMINAGA: On the normal basis theorem and strictly Galois extensions, Math. J. Okayama Univ., 8 (1958), 133—142.
[8] H. TOMINAGA: On a theorem of N. Jacobson, Proc. Japan Acad., 31 (1955), 653—654.
[9] H. TOMINAGA: A note on Galois theory of primary rings, Math. J. Okayama Univ., 8 (1958), 117—123.
[10] H. TOMINAGA: On q-Galois extensions of simple rings, Nagoya Math. J., Nakayama Memorial Number (1966), 485—507.
[11] H. TOMINAGA: Note on q-Galois extensions of simple rings, J. Fac. Sci. Hokkaido Univ., Ser. I, 19 (1966), 66—70.

DEPARTMENT of MATHEMATICS,
HOKKAIDO UNIVERSITY

(Received April 1, 1966)