ON GENERATING ELEMENTS OF GALOIS EXTENSIONS OF DIVISION RINGS II

MIKAO MORIYA and TAKASI NAGAHARA

1. In his previous paper [4], the latter of the present authors proved that if K is a division ring which is Galois and finite over a division subring L then $K = L[k, uku^{-1}]$ with some k, $u \in K$. In this note, we shall present several precisions of this fact. Our principal results are stated as follows: 1) If a division ring K is Galois and finite over L, then $K = L[k, vkv^{-1}]$ for some $k \in K$, $v \in V_K(L)$ (Theorem 1). 2) Moreover, if $V_K(L)$ is commutative then $K = L[k]$ for some $k \in K$ (Theorem 3).

All the results in this note have been obtained originally by the latter and the appendix is added by the former of the present authors.

Finally as to notations and terminologies, we follow [4].

2. Throughout this note, K be a division ring which is Galois and finite over a division subring L, and C, Z and C_0 be the centers of K, L and $H = V_K(V_K(L))$ respectively. As we have already proved, $V_K(H) = V_K(L)$ and the center of $V_K(L)$ coincides with C_0. Moreover, H is outer Galois over L, further, $C_0 \supset C \cup Z$ and C is finite and Galois over $C \cap Z$. In the following we shall say that K/L is *simple* if $K = L[k]$ for some k.

Theorem 1. $K = L[k, vkv^{-1}]$ *for some* $k \in K$, $v \in V_K(L)$. *Particularly, in case* K/L *is not simple,* $K = L[k, vkv^{-1}]$ *for some* $k \in K$, $v \in C_0$ *if and only if* $L \not\subset C$.

Proof. In case $L \subset C$, $V_K(L) = V_K(C) = K$. As $K = L[k, uku^{-1}]$ for some k, $u \in K$ by [4, Theorem 4], our assertion is clear. If K/L is simple then trivially $K = L[k, vkv^{-1}]$ for a primitive element k of K/L and for $v \in V_K(L)$. We shall assume therefore that K/L is not simple and $L \not\subset C$. In this case, $C_0 \supsetneqq Z[C]$ by [4, Theorem 2]. And $C \cap Z$ is an infinite set, for, if not, C is finite and so $V_K(L)$ is also finite, that is, the totall Galois group of K/L is almost outer so that K/L is simple [3, Corollary 2]. Now set $L_1 = L[C_0]$. Then, $L_1 = L \times_Z C_0$. Therefore $V_{L_1}(L_1) = C_0[Z] = C_0$, and $L \subset L_1 \subset H$ implies $V_K(H) \subset V_K(L_1) \subset V_K(L)$ whence $V_K(L_1) = V_K(L)$. Since $L_1 \not\subset C$ and $V_{L_1}(L_1) = C_0 = V_{V_K(L_1)}(V_K(L_1))$ we obtain $K = L_1[k]$ $(= H[k])$ by [4, Theorem 2]. Further, we have $C = V_K(H[k]) = V_K(H) \cap V_K(\{k\}) = V_K(L) \cap V_K(\{k\}) =$

$V_K(L[k])$. This shows that the total Galois group of $K/L[k]$ is outer. Hence, there exists only a finite number of intermediate division subrings of $K/L[k]$ different from K: $K_1, \dots, K_n$ $(n > 0)$. As C_0/Z is Galois so that separable, we have $C_0 = Z[v]$ for some v. Hence, $K = L_1[k] = L[v, k]$. If $vk = kv$ then $v \in C_0 \cap V_K(\{k\}) \subset V_K(H) \cap V_K(\{k\}) = V_K(H[k]) = V_K(K) = C$ and hence, $Z[C] = C_0$ which is contrary to our assumption $C_0 \supsetneqq Z[C]$. Since $v \notin K_i$ $(i = 1, 2, \dots, n)$, we obtain from [4, Lemma 1]: $K = L[k, (v+c)k(v+c)^{-1}]$ with some $c \in C \cap Z$. (Note here that $C \cap Z$ is an infinite set.) Finally, in case $L \subset C$, C_0 coincides with C. Accordingly our second assertion is clear from the above proof.

Lemma 1. *For any $a \in K \setminus H$, there exists some k with $K = L[a, k]$.*

Proof. Obviously, it suffices to prove the Lemma in case K/L is not simple. If $L \subset C$ then $L[a]$ is commutative, but not contained in C. For, if $L[a] \subset C$, then $a \in C \subset C_0 = V_H(H) \subset H$. Therefore, by [4, Lemma 7], $K = L[a][k] = L[a, k]$ for some k. Accordingly, we should consider only the case $L \not\subset C$. Then, Theorem 1 proves $K = L[k, vkv^{-1}] = L[k, v]$ for some $k \in K$, $v \in C_0$. We note here that $C \cap Z$ is infinite. Evidently $C \subset V_K(L[k]) = V_K(L) \cap V_K(\{k\}) \subset V_K(L[k, v]) = V_K(K)$, that is, the total Galois group of $K/L[k]$ is outer. Therefore, there exists only a finite number of intermediate division subrings $K_1, K_2, \dots, K_n$ $(n > 0)$ of $K/L[k]$ different from K.

Since $V_K(L)/Z$ is finite and Galois and C_0/Z is separable, we can readily see from the proof of [1, Satz 5] that, for some $x, y \in V_K(L)$, $V_K(L) = Z[x, yxy^{-1}] \supset Z[x] \supset C_0$. Noting that $Z[yxy^{-1}] = yZ[x]y^{-1} \supset C_0$ and $H = V_K(V_K(L)) = V_K(Z[x, yxy^{-1}])$, we may assume without loss of generality that $ax \neq xa$[1]. Now, $L[k, x] \supset Z[x] \supset C_0 \ni v$ so that $K = L[k, v] = L[k, x]$, whence $x \notin K_i$ $(i = 1, 2, \dots, n)$. Therefore, we can choose by [4, Lemma 1] some $c \in C \cap Z$ such that $(x+c)a(x+c)^{-1} \notin K_i$ $(i = 1, 2, \dots, n)$. Hence $K = L[k, (x+c)a(x+c)^{-1}] = L[(x+c)^{-1}k(x+c), a]$.

Theorem 2. *If $L \supsetneqq Z$ and some $l \in L \setminus Z$ is algebraic over Z then K/L is simple.*

Proof. We shall denote by $\mathfrak{J}_0$ the group of inner automorphisms of K which are generated by all non-zero elements in $Z[l]$. Clearly, the fixed subring of $\mathfrak{J}_0$ in L is $V_L(Z[l]) = V_L(\{l\})$ which will be denoted by L_0. Then, we have $L_0 \subset J(\mathfrak{G}(L_0), K) \subset J(\{\mathfrak{G}(K/L) \cup \mathfrak{J}_0\}, K) =$

1) If $a \in V_K(\{x, yxy^{-1}\})$ then $a \notin V_K(Z)$, and so $az \neq za$ for some $z \in Z$. We can take here $x + z$ instead of x.

$J(\mathfrak{G}(K/L), K) \cap J(\mathfrak{J}_0, K) = L \cap J(\mathfrak{J}_0, K) = J(\mathfrak{J}_0, L) = L_0$. As $1 < [Z[l] : Z] < \infty$, we have $1 < [L : L_0] < \infty$. Hence K is Galois and finite over L_0. Let t be any element in L belonging to $V_K(V_K(L_0))$. Then $t \in L \cap V_K(V_K(L_0)) \subset L \cap V_K(V_L(L_0)) = V_L(V_L(L_0)) = L_0$. Therefore, if $l' \in L \setminus L_0$, $K = L_0[l', k] = L[k]$ for some k by Lemma 1.

Lemma 2. *If $V_K(L)$ is commutative, then there exists an element k in K such that k and $k^{\tilde{v}}$ are linearly independent over H for all $v \in V_K(L) \setminus C$ where $\tilde{v}$ is the inner automorphism of K generated by v.*

Proof. We shall denote by H_r the ring of all right multiplications generated by H, and by $\widetilde{V_K(L)}$ the group of inner automorphisms of K generated by all non-zero elements of $V_K(L)$. Consider the ring $\mathfrak{K}$ of endomorphisms of K generated by $\widetilde{V_K(L)}$ and H_r. Then, $\mathfrak{K} = \widetilde{V_K(L)} \cdot H_r$ because $V_K(L) = V_K(H)$. Since $V_K(L)$ is commutative, $H = V_K(V_K(L)) \supset V_K(L)$ and $\mathfrak{K}$ is $\mathfrak{K}$-isomorphic to K as a right $\mathfrak{K}$-module[2)]. We denote this isomorphism by φ, and let k be the image of the identity 1 of $\mathfrak{K}$ by φ. Now we can choose an C-basis of $V_K(L)$ $\{v_1, v_2, \dots, v_n\}$ such that $v_1 = 1$, $v_2 = v$. Then, as is well-known, $\{\tilde{v}_1, \tilde{v}_2, \dots, \tilde{v}_n\}$ are H_r-independent. Since $[K : H] = [V_K(L) : C]$, $\{\tilde{v}_1, \tilde{v}_2, \dots, \tilde{v}_n\}$ is an H_r-basis of $\mathfrak{K}$ by [2, Satz 10]. Therefore, $\{\varphi(\tilde{v}_i) = \varphi(1 \cdot \tilde{v}_i) = k^{\tilde{v}_i}\,;\ i = 1, 2, \dots, n\}$ forms an H-basis of K.

Theorem 3. *If $V_K(L)$ is commutative, then K is simple over L.*

Proof. If $V_K(L) = C[Z]$, then K is simple over L by [4, Corollary 4]. We may therefore consider only the case where $V_K(L) \supsetneqq C[Z]$. Accordingly L is infinite and $K \supsetneqq H \supsetneqq L$. By [3, Corollary 3], $H = L[h]$ with some $h \in H$. On the other hand, by Lemma 2, there exists an element $k \in K$ such that k and $k^{\tilde{v}}$ are linearly independent over H (and so $k \neq k^{\tilde{v}}$) for sll $v \in V_K(L) \setminus C$. This fact means evidently $K = H[k]$. Now we set $\mathfrak{H} = \bigcup_{x \in L} \mathfrak{G}_x$ where $\mathfrak{G}_x = \mathfrak{G}(K/L[k(h+x)])$. Noting that $V_K(L[k(h+x)]) = V_{V_K(L)}(\{k(h+x)\}) = V_{V_K(H)}(\{k(h+x)\}) = V_K(H[k(h+x)]) = V_K(K) = C$, it follows that K is outer Galois over $L[k(h+x)]$, whence each $\mathfrak{G}_x$ is a finite outer subgroup of $\mathfrak{G}(K/L)$. Accordingly we have: order of $\mathfrak{G}_x$ = order of $\overline{\mathfrak{G}}_x$ where $\overline{\mathfrak{G}}_x$ is the restriction of $\mathfrak{G}_x$ to H. If x_1, x_2 are different in L then $L[k(h+x_1), k(h+x_2)] = K$, consequently $\mathfrak{G}_{x_1} \cap \mathfrak{G}_{x_2}$ is the identity group.

Now we shall prove that $\mathfrak{H}$ is finite. Suppose, on the contrary, that

2) See [2, Satz 9].

$\mathfrak{H}$ is infinite. Then, from the preceding remarks, we can find such different x_1, x_2 in L that $\mathfrak{G}_{x_1}$, $\mathfrak{G}_{x_2}$ are both different from the identity group and $\bar{\mathfrak{G}}_{x_1} = \bar{\mathfrak{G}}_{x_2}$ since the total Galois group of H/L has only a finite number of subgroups. If $\mathfrak{G}_{x_1} = \{\sigma_1, \dots, \sigma_m\}$ then $\mathfrak{G}_{x_2} = \{\sigma_1\tilde{v}_1, \dots, \sigma_m \tilde{v}_m\}$ with v_j's in $V_K(L)$, where some of v_j's, say v_1, is not in C. Since $k(h + x_1) = k^{\sigma_1}(h + x_1)^{\sigma_1}$ and $k(h + x_2) = k^{\sigma_1\tilde{v}_1}(h + x_2)^{\sigma_1\tilde{v}_1}$ (that is, $k^{\tilde{v}_1^{-1}} (h + x_2) = k^{\sigma_1}(h + x_2)^{\sigma_1})$, we obtain $k(h + x_1) ((h + x_1)^{\sigma_1})^{-1} = k^{\sigma_1}$ and $k^{\tilde{v}_1^{-1}} (h + x_2) ((h + x_2)^{\sigma_1})^{-1} = k^{\sigma_1}$. Hence we have $k(h + x_1) (h + x_1)^{\sigma_1})^{-1} - k^{\tilde{v}_1^{-1}} (h + x_2) ((h + x_2)^{\sigma_1})^{-1} = 0$. Recalling that H is normal over L, $(h + x_1) ((h + x_1)^{\sigma_1})^{-1}$ and $(h + x_2) ((h + x_2)^{\sigma_1})^{-1}$ are both in H. Accordingly the last equation contradicts the fact that k and $k^{\tilde{v}_1^{-1}}$ are linearly independent over H. Hence $\mathfrak{H}$ is a finite set. Since L is infinite and $\mathfrak{G}_x \cap \mathfrak{G}_y$ is the identity group for any different x, y in L, there exists some $x_0 \in L$ such that $\mathfrak{G}_{x_0}$ itself is the identity group. Then evidently $K = L[k(h + x_0)]$.

3. Appendix

In the sequel, we wish to present an alternative proof of Theorem 3.

Proposition 1. *The group $\mathfrak{J}$ of all the L-inner automorphisms of K is commutative if and only if $V_K(L)$ is commutative.*

Proof. If $V_K(L)$ is commutative then so is $\mathfrak{J}$ evidently. Conversely suppose $\mathfrak{J}$ is commutative. If there exist some a, $b \in V_K(L)$ such that $ab \neq ba$ then, as $\tilde{a}\,\tilde{b} = \tilde{b}\,\tilde{a}$, $ab = bac$ for some c $(\neq 1)$ in C, that is, $aba^{-1} = bc$. Further, for any non-zero $c* \in C$, there holds $a(b + c*)a^{-1} = (b + c*)c'$ with some $c' \in C$. As $a(b + c*)a^{-1} = aba^{-1} + c* = bc + c*$ and $a(b + c*)a^{-1} = bc' + c*c'$, we obtain $b(c - c') = c*(c' - 1)$. Noting that $b \notin C$, we have $c = c' = 1$. But this is a contradiction, and consequently $V_K(L)$ must be commutative.

Proposition 2. *Let ι_1, ι_2, ι_3 be inner automorphisms of K and c_1, c_2, c_3 be non-zero elements in C. If $\iota_1 c_{1r} + \iota_2 c_{2r} + \iota_3 c_{3r} = 0$ then ι_i's are not all different.*

Proof. Let x_i be elements in K such that $\iota_i = \tilde{x}_i (i = 1, 2, 3)$. Then, from the assumption, we have $x_{1l} + x_{2l}\, y_{2r} + x_{3l}\, y_{3r} = 0$,[3] where $y_i = x_i^{-1} c_i x_1 c_1^{-1}$ $(i = 2, 3)$. Further, there holds $x_{2l}\,(y_{2r} k_r - k_r y_{2r}) + x_{3l}(y_{3r} k_r$

3) For $x \in K$, x_r and x_l mean the right- and left-multiplications by x respectively.

$- k_r y_{3r}) = 0$ for all $k \in K$. If x_{2l} and x_{3l} are K_r-independent then $y_2 k - ky_2 = 0 = y_3 k - ky_3$. Hence, in this case, both y_2 and y_3 are in C. As $y_i = x_i^{-1} c_i x_1 c_1^{-1}$ $(i = 2, 3)$, we have $x_i^{-1} x_1 \in C$, whence $\iota_1 = \iota_2 = \iota_3$. On the other hand, if x_{2l} and x_{3l} are K_r-dependent then $x_{2l} + x_{3l} y_r = 0$ for some $y \in K$, from which we readily see $\iota_2 = \iota_3$.

Now we shall prove the following theorem which is equivalent to Theorem 3.

Theorem 3′. *Let K be Galois and finite over L. If the group $\mathfrak{J}$ of all the L-inner automorphisms in K is commutative then K/L is simple.*

Proof. Since $V_K(L)$ $(= V_K(H))$ is commutative by Proposition 1, H contains $V_K(H)$. And so [2, Satz 7] shows that K has a normal basis $\{k^{\rho_i}; i = 1, 2, \dots, n\}$ over H where $n = [V_K(L) : C]$ and $\rho_i \in \mathfrak{J}$. In case $\mathfrak{G}(K/L)$ is almost outer, our theorem is obviously true. We shall therefore, in the rest, restrict out attention to the case where $\mathfrak{G}(K/L)$ is not almost outer. Accordingly $C \cap Z$ is an infinite field. Since H/L is outer Galois, $H = L[h]$ for some h. Then we can prove that $K = L[xh + k]$ with some $x \in C \cap Z$. This fact is obviously involved in the following lemma.

Lemma 3. *Let $\mathfrak{J}$ be commutative, $H = L[h]$ and $\{k^{\rho_i}; i = 1, 2, \dots, n\}$ be an H-basis of K where ρ_i's in $\mathfrak{J}$. If $\{x_j; j = 1, 2, \dots\}$ is any infinite subset of $C \cap Z$ then almost all $L[x_j h + k]$ coincide with K.*

Proof. We shall denote by $\mathfrak{G}_j$ the total group $\mathfrak{G}(K/L[x_j h + k])$.

i) *$\mathfrak{G}_j$ is outer.* Let ι be in $\mathfrak{G}_j \cap \mathfrak{J}$. Then $x_j h + k^{\iota} = (x_j h + k)^{\iota} = x_j h + k$, whence $k^{\iota} = k$. Hence ι is contained in $\mathfrak{G}(K/H[k]) = \mathfrak{G}(K/K)$, that is, ι is the identity.

Now suppose that the assertion of the lemma is not true. Then there exists an infinite number of $\mathfrak{G}_j$'s different from the identity group. Accordingly, without loss of generality, we may assume that all $\mathfrak{G}_j$'s are different from the identity group.

ii) *There is an infinite subset S of $\{\mathfrak{G}_j; j = 1, 2, \dots\}$ such that the restriction of each member of S to H is the same subgroup of the total group $\mathfrak{H}$ of H/L.* Since H is normal over L, and each $\mathfrak{G}_j$ is outer by i), the restriction of $\mathfrak{G}_j$ to H is a subgroup of $\mathfrak{H}$ which is isomorphic to $\mathfrak{G}_j$. As $\mathfrak{H}$ is outer, it contains only a finite number of subgroups. Accordingly, there exists an infinite subset S of $\{\mathfrak{G}_j; j = 1, 2, \dots\}$ such that the restriction of each member of S to H is the same subgroup of $\mathfrak{H}$.

We may assume therefore, without loss of generality, further that the restriction of each $\mathfrak{G}_j$ to H is the same subgroup of $\mathfrak{H}$, which is evidently different from the identity group. Then there exist σ_j's in $\mathfrak{G}_j$'s such that $h^{\sigma_1} = h^{\sigma_j} \neq h$ $(j = 1, 2, \dots)$. Hence $(x_j h + k)^{\sigma_j} = x_j h + k$ implies $(x_1 - x_j)(h^{\sigma_1} - h) + k^{\sigma_1} - k^{\sigma_j} = 0$ $(j = 2, 3, 4)$. As $\sigma_j \sigma_1^{-1} = \iota_{j-1} \in \mathfrak{J}$, we obtain

$$(*) \qquad (x_1 - x_{j+1})(h - h^{\sigma_1^{-1}}) + k - k^{\iota_j} = 0 \qquad (j = 1, 2, 3).$$

Now, as is well-known, there exist non-zero $c_1, c_2, c_3 \in C \cap Z$ such that $c_1 + c_2 + c_3 = 0$ and $\sum_{j=1}^{3} (x_1 - x_{j+1}) c_j = 0$. Then from (*), we have $\sum_{j=1}^{3} k^{\iota_j} c_j = 0$, which means that $k \cdot (\sum_{j=1}^{3} \iota_j c_{j_r}) = 0$. Noting that $\mathfrak{J}$ is commutative, we can easily see $(\sum_{i=1}^{n} k^{\rho_i} h_i) \cdot (\sum_{j=1}^{3} \iota_j c_{j_r}) = k \cdot (\sum_{i=1}^{n} \rho_i h_{i_r}) (\sum_{j=1}^{3} \iota_j c_{j_r}) = (k \cdot \sum_{j=1}^{3} \iota_j c_{j_r}) (\sum_{i=1}^{n} \rho_i h_{i_r}) = 0$ for any h_i's in H. As each element of K is of the form $\sum_{i=1}^{n} k^{\rho_i} h_i$ with $h_i \in H$, we have proved that $\sum_{j=1}^{3} \iota_j c_{j_r}$ is the zero-endomorphism of K. Accordingly, by Proposition 2, at least two of ι_j's, say ι_1 and ι_2, must coincide. Then, again from (*), we obtain $(x_3 - x_2)(h - h^{\sigma_1^{-1}}) = 0$, which leads to a contradiction $x_2 = x_3$. This completes the proof.

REFERENCES

[1] F. KASCH, Über den Satz vom primitiven Element bei Schiefkörper, J. reine und angew. Math., 180 (1951) 150—159.

[2] ————, Über den Endomorphismenring eines Vektorraumes und den Satz von der Normalbasis, Math. Ann., 129 (1953) 447—463.

[3] T. NAGAHARA, On primitive elements of Galois extensions of division rings, Math. J. Okayama Univ., 6 (1956) 23—28.

[4] ————, On generating elements of Galois extensions of division rings, Math. J. Okayama Univ., 6 (1957) 181—190.

DEPARTMENT OF MATHEMATICS,
OKAYAMA UNIVERSITY

(*Received July 15, 1957*)