ON GENERATING ELEMENTS OF GALOIS EXTENSIONS OF DIVISION RINGS III

TAKASI NAGAHARA

In his previous papers [4], [5] and [3][1], the author has investigated mainly finding two conjugate generating elements of Galois extensions, while in the present paper he will consider simple extensions[2], and prove that a division ring K which is Galois and finite over L is simple over L if and only if either L is not contained in the center of K or K is commutative. (Further Theorem 2 is proved for certain intermediate subrings.) Moreover we may remark here in passing that the results in [3] are of no use for the present purpose.

Finally, as to notations and terminologies used in this paper we follow the previous ones [4], [5] and [3].

1. Preliminaries.

Throughout this note, K will be a division ring and L a division subring of K. We set here $V=V_K(L)$ and $\mathfrak{V}=V_{\mathfrak{A}}(L_r)$, where $\mathfrak{A}$ is the absolute endomorphism ring of K. Then we obtain the following:

Lemma 1. *For a subset $\mathfrak{S}$ of $\mathfrak{V}$, $\mathfrak{S}$ is linearly independent over V_r if and only if it is linealry independent over K_r.*

Proof. Let $\mathfrak{S}$ be linearly independent over V_r. If $\mathfrak{S}$ is not linearly independent over K_r, then there exists a minimal (finite) subset $\mathfrak{T}=\{\alpha_1, \cdots, \alpha_n\}$ of $\mathfrak{S}$ which is linearly dependent over K_r. Hence there holds $\alpha_1=\sum_{i=2}^{n}\alpha_i a_{ir}$ with some $a_i\in K$ $(i=2, \cdots, n)$. Clearly there exists some a_j $(j\geq 2)$ which does not belong to V, that is, there exists an element $b\in L$ such that $a_jb\neq ba_j$. Since $\alpha_i(i=1, 2, \cdots, n)$ are in $\mathfrak{V}$, we have $0=\alpha_1-b_r\alpha_1b_r^{-1}=\sum_{i=2}^{n}\alpha_i(a_{ir}-b_ra_{ir}b_r^{-1})=\sum_{i=2}^{n}\alpha_i(a_i-ba_ib^{-1})_r$. But, as $(a_j-ba_jb^{-1})_r\neq 0$, this contradicts the minimality of $\mathfrak{T}$, whence $\mathfrak{S}$ is linearly independent over K_r. The converse is trivial.

Corollary 1. *Let $\mathfrak{M}, \mathfrak{N}$ be arbitrary K_r-, V_r-submodules of $\mathfrak{A}$ and $\mathfrak{V}$ respectively. Then there hold the following facts:*

---

1) Numbers in brackets refer to references cited at the end of this paper.

2) K is said to be simple over L if $K=L[k]$ with some k ([3, p. 89]).

(1) $[V_{\mathfrak{M}}(L_r): V_r] \leq [\mathfrak{M}: K_r]$.

(2) $[\mathfrak{N}: V_r] = [\mathfrak{N}K_r: K_r]$ *and* $V_{\mathfrak{N}K_r}(L_r) = \mathfrak{N}$[3].

Proof. (1) and the first part of (2) are easy consequences of Lemma 1. Thus, it suffices to prove the latter part of (2). Let $\mathfrak{N} = \sum \oplus \alpha_\iota V_r$. If there exists some $\beta = \sum_{\iota=1}^{n} \alpha_\iota a_{\iota r} \in V_{\mathfrak{N}K_r}(L_r) \setminus \mathfrak{N}$, then some of a_ι's, say a_1, is not in V. Hence there exists an elment b in L such that $a_1 b \neq b a_1$. And so $0 = b_r\beta - \beta b_r = \sum_{\iota=1}^{n} \alpha_\iota (ba_\iota - a_\iota b)_r$, which contradicts Lemma 1. As evidently $V_{\mathfrak{N}K_r}(L_r) \supset \mathfrak{N}$, our proof is complete.

Corollary 2. *Let K be Galois over L, and $\mathfrak{G}$ a group of automorphism with L as its fixring. Then there hold the following facts:*

(1) $[\mathfrak{G}V_r: V_r] = [\mathfrak{G}K_r: K_r]$ *and* $\mathfrak{G}V_r = V_{\mathfrak{G}K_r}(L_r)$.

(2) *In particular, if* $[K: L] < \infty$ *then* $[\mathfrak{G}V_r: V_r] = [K: L]$.

Proof. (1) is an easy consequence of Corollary 1 (2). In case $[K: L] < \infty$, $\mathfrak{G}K_r = V_{\mathfrak{G}}(L_\iota)$ and $[V_{\mathfrak{G}}(L_\iota): K_r] = [K: L]$ by [1, Proposition 7. 2. 1]. Hence (2) is also a consequence of the above corollary.

2. Simple Galois extensions.

We shall use the following conventions throughout this section: K will be Galois and finite over L, and $\mathfrak{G}$, $\mathfrak{F}$ mean the Galois group of K/L, and the totality of L-inner automorphisms of K respectively. C, Z will be the centers of K, L respectively, and we shall set $V = V_K(L)$ and $H = V_K(V)$. Further, D will be an arbitrary intermediate subring of K/L, and for any set $\mathfrak{H}$ of automorphisms of K we say that D is $\mathfrak{H}$-*normal* when $D^\sigma = D$ for all $\sigma \in \mathfrak{H}$.

Lemma 2. *Let X be a subset of L which is linearly independent over Z (and so over V*[4]*), and $X = \bigcup_\lambda X_\lambda$ be an arbitrary partition of X into non-empty finite subsets. Then, given $k_1, k_2 \in K$, the number of X_λ's such that $k_1(k_2\mathfrak{G}V_r) \cap X_\lambda V \neq \{0\}$*[5] *never exceeds $[K: L]$ (and so finite).*

Proof. If, on the contrary, there holds $k_1(k_2\mathfrak{G}V_r) \cap X_i V \neq \{0\}$ for $i = 1, \cdots, m > [K: L]$, then there exist $\varepsilon_i \in \mathfrak{G}V_r$ and $y_i \in X_i V$ such that $k_1(k_2\varepsilon_i) = y_i \neq 0$ $(i = 1, \cdots, m)$. Noting that $\{\varepsilon_1, \cdots, \varepsilon_m\}$ is linearly dependent

3) We always consider right-modules and right-dimensions, where the dimension $[\mathfrak{M}: K_r]$ is to be defined as the cardinal number of a right-basis of $\mathfrak{M}$ over K_r.

4) Recall that $L[V] = L \times_Z V$ ([5, p. 183]).

5) $X_\lambda V$ is the V-module generated by X_λ over V.

over V_r by Corollary 2 (2), there holds $\sum_{i=1}^{m} \varepsilon_i v_{ir} = 0$ with not all zero $v_i \in V$. Thus we have $0 = \sum_{i=1}^{m} (k_1(k_2\varepsilon_i) - y_i)v_i = -\sum_{i=1}^{m} y_i v_i$, but this is a contradiction, because $y_1, \cdots, y_m$ are linearly independent over V by our assumption.

Corollary 3. *Let* $[L : Z] = \infty$. *Then there hold the following facts:*

(1) *If* $L_0 = L[v_1, \cdots, v_n, k]$ *with some* v_i*'s* $\in V$ *and* $k \in K$ *then* L_0/L *is simple.*

(2) *If* $L_0 = L[h, k]$ *with some* $h \in H$ *and* $k \in K$ *then* L_0/L *is simple.*

Proof. Choose a countably infinite subset $\{x_i\}$ of L which is linearly independent over Z. (1) We set $L[\sum_{i=1}^{n} x_{jn+i}v_i + k] = L_j$ $(j = 1, 2, \cdots)$. Now suppose that the assertion of (1) is not true. Then for each j, one of v_i's, say $v_{j'}$, is not contained in L_j and there exists an automorphism $\sigma_j \in \mathfrak{G}(K/L_j)$ such that $v_{j'}^{\sigma_j} \neq v_{j'}$. As $x_{jn+i}v_i + k$ is contained in L_j, we have $(\sum_{i=1}^{n} x_{jn+i}v_i + k)^{\sigma_j} = \sum_{i=1}^{n} x_{jn+i}v_j^{\sigma_j} + k^{\sigma_j} = \sum_{i=1}^{n} x_{jn+i}v_i + k$, whence $\sum_{i=1}^{n} x_{jn+i}(v_i^{\sigma_j} - v_i) = k(1_r - \sigma_j) \neq 0$ for each j. But this contradicts Lemma 2. Hence L_0 is simple over L. (2) We set here $L_i = L[hx_i + k]$ and $\mathfrak{G}_i = \mathfrak{G}(K/L_i)$. If an infinite number of L_i's does not contain h then $\{h\}^{\mathfrak{G}_i} \neq \{h\}$ for infinitely many i's. As $\{h\}^{\mathfrak{G}}$ is a finite set, there exists an infinite subset $\{x_{i_1}, x_{i_2}, \cdots\}$ of $\{x_i\}$ such that all $\{h\}^{\mathfrak{G}_{i_j}}$'s are the same. Thus, without loss of generality, we may assume from the beginning that all $\{h\}^{\mathfrak{G}_i}$'s are the same. We choose some $h' \neq h$ from $\{h\}^{\mathfrak{G}_i}$, then $h' = h^{\sigma_i}$ with some $\sigma_i \in \mathfrak{G}_i$. Now $(hx_i + k)^{\sigma_i} = hx_i + k$ implies $(h' - h)x_i = k(1_r - \sigma_i)$, that is, $0 \neq x_i = (h' - h)^{-1}\{k(1_r - \sigma_i)\}$ for all i. But this contradicts Lemma 2. Hence, for almost all i, L_i contains h, consequently coincides with L_0.

Corollary 4. *Let* $[L : Z] = \infty$. *If* $V_K(V_K(L[f])) \supset D \supset L[f]$ *for some* f *then* D/L *is simple.*

Proof. Set $H' = V_K(V_K(L[f]))$, then we readily see that $H' = H[f]$, because $V_K(L[f]) = V_K(H[f])$ and K/H is inner Galois. And so, for any $\sigma \in \mathfrak{G}(H'/L[f])$, σ_H is the identity when and only when σ is so. Then recalling that $H'/L[f]$ and H/L are outer Galois and that any $\sigma \in \mathfrak{G}(H'/L[f])$ is in $\mathfrak{G}(K/L[f])_{H'}$, we obtain $[H' : L[f]]$ = order of $\mathfrak{G}(H'/L[f])$ = order of $\mathfrak{G}(H/H \cap L[f]) = [H : H \cap L[f]]$. Now, as

is well-known, $H\cap D = L[h]$ for some h ([4, Corollary 3]), and then we shall prove $D = L[f, h]$, from which our corollary is clear by Corollary 3 (2). Noting that $H' \supset D \supset L[f, h] \supset L[f]$, the above method proves that $[H' : D]$ = order of $\mathfrak{G}(H'/D)$ = order of $\mathfrak{G}(H/H\cap D) = [H : H\cap D]$, and $[H' : L[f, h]]$ = order of $\mathfrak{G}(H'/L[f, h])$ = order of $\mathfrak{G}(H/H\cap L[f, h]) = [H : H\cap L[f, h]]$. Accordingly, it suffices to show that $H\cap D$ $(=L[h]) = H\cap L[f, h]$, however it is evident.

Theorem 1. *If V is commutative then D is simple over L.*

Proof. Since V is commutative, from the proof of [5, Theorem 3], we can select in any rate an element $f\in D$ such that $V_K(V_K(L[f])) \supset D\supset L[f]$. If $[L : Z] = \infty$ then D is simple over L by Corollary 3. On the other hand, if $[L : Z] < \infty$ then D is also simple by [5, Corollary 5 (1)].

Lemma 3. *Let $L \supsetneqq Z$, and D be $\mathfrak{F}$-normal. Then D is simple over L.*

Proof. By [4, Lemma 3], either $D\subset H$ or $D\supset V$. In case $D\subset H$, our assertion is clear by [4, Corollary 3]. Thus we may, and shall, assume $D\supset V$. Now we consider a subring $L_1 = L[V] = L\times_Z V$ of D. Noting that $V_K(L_1)\subset V\subset L_1$, we have $V_K(L_1) = V_{L_1}(L_1)$, whence, by [5, Corollary 4], we obtain $D = L_1[k] = L[v_1, \cdots, v_n, k]$ for some k, where $\{v_1, \cdots, v_n\}$ is a basis of V/Z. Hence, in case $[L : Z] = \infty$, D/L is simple by Lemma 3 (1). Accordingly, it remains only to prove our assertion for the case $[L : Z] < \infty$. Let $[L : Z] < \infty$ hereafter. Then K is finite over C by [1, Theorem 7.9.1], and so K/C is inner Galois. Since $V_K(L_1) = V_K(L[V]) = C[Z]$ (see the proof of [5, Corollary 5]), we obtain $V_K(Z) = V_K(C[Z]) = L_1\subset D$, and so $V_D(Z) = V_K(Z)$. Hence $V_D(Z)$ is Galois over L, whence we have $V_D(Z) = L[k]$ for some k by [5, Corollary 5 (2)]. Then [5, Theorem 1] implies that there exists some element d in D such that $L[d]\ni k$ and $V_D(Z)[d] = D$. Hence we have $L[d] = L[d, k] = V_D(Z)[d] = D$.

Lemma 4. *Let $L = Z$, and D be $\mathfrak{F}$-normal. If $L \not\subset V_D(D)$ then D is simple over L.*

Proof. By the remark in [5, p. 188], $C[Z] = H$. If $D\subset H$ then $L\subset D = V_D(D)$, being contradictory to $L \not\subset V_D(D)$. Thus $D \not\subset H$, whence the $\mathfrak{F}$-normal D contains V by [4, Lemma 2]. And then there holds $V_D(D) \subset D\cap H\subset C[Z]$. Recalling $[K : Z\cap C] < \infty$ in the present case, we see that D is Galois and finite over E, where $E = J(\mathfrak{S}, D)$ and $\mathfrak{S}$

is the group of $C \cap Z$-automorphisms of D. Of course, we have then $D \supset V_D(D) \supset E$ from $V_D(D) \supset C \cap Z$. Now, as $Z \not\subset V_D(D)$, there exists some $z \in Z \setminus V_D(D)$. Noting that the field $E[z]$ is not contained in $V_D(D)$ and $D/E[z]$ is Galois, $D = E[z][d] = E[z, d]$ with some $d \in D$ by [5, Lemma 7], and evidently $D = E[z, d] = H[d]$. Now, set $\mathfrak{G}' = \mathfrak{G}(K/Z[d])$. Then, as $D = H[d]$ is $\mathfrak{G}'$-normal, $J(\mathfrak{G}'_D, D) = Z[d]$. And so, $Z[d] \supset Z \cap C$ implies $Z[d] \supset E$, whence $Z[d] \supset E[z, d] = D$. We have proved therefore $D = Z[d]$.

Now we are at the position to prove our principal theorem.

Theorem 2. *Let D be an intermediate division subring of K/L such that for each $x \in D$, $\{x\}^{\mathfrak{F}} \setminus D$ is a finite set. Then D is simple over L if and only if either $L \not\subset V_D(D)$ or D is commutative.*

Proof. In case $\mathfrak{G}$ is almost outer, our assertion is clear by [4, Corollary 2]. On the other hand, in case $\mathfrak{G}$ is not almost outer, by making use of the same method as in the proof [4, Principal Theorem], we readily see that D is $\mathfrak{F}$-normal. Then, if $L \not\subset V_D(D)$, then D is simple over L by Lemmas 3 and 4. While, if D is commutative then we have $D \subset V_K(D) \subset V$. Since D is $\mathfrak{F}$-normal, either $D \subset H$ or $D \supset V$. Hence, in either cases, $D \subset H$, whence D is simple over L. The converse part will be trivial.

Theorem 3. *K is simple over L when and only when either $L \not\subset C$ or K is commutative.*

Proof. Our theorem is only an easy corollary of Theorem 2, however we shall present here another proof.

It suffices to show that if $L \not\subset C$ then K/L is simple. By [2, Satz 14], $K = L[v, k]$ for some $v \in V$ and $k \in K$. Hence, in case $[L : Z] = \infty$, K is simple over L by Corollary 3 (1). On the other hand, in case $[L : Z] < \infty$, K is Galois and finite over $L \cap C$[6]. And so, for any $a \in L \setminus L \cap C$, $(L \cap C)[a]$ is a field and $(L \cap C)[a] \not\subset C$. And then K/L is simple by [5, Lemma 7].

Remark. Let K_1, K_2 be central non-commutative division algebras over the rational number field C with degrees prime to each other. (The existence of such algebras is well-known.) Now we set $K = K_1 \times_C K_2$. Then, as is well-known, K is a central division algebra over C too. Given $a \in K_1 \setminus C$, $C[a]$ is a field and $K/C[a]$ is inner Galois. Hence

6) $[K : C] < \infty$ by [1, Theorem 7.9.1], and $[C : L \cap C] < \infty$ by $J(\mathfrak{G}_0, C) = L \cap C$.

$K/C[a]$ is simple by [5, Corollary 7]. On the other hand, as the center of the non-commutative algebra $D=V_K(C[a])=V_{K_1}(C[a])\times_C K_2$ coincides with $C[a]$, D is not simple over $C[a]$ evidently.

REFERENCES

[1] N. JACOBSON, Structure of rings, Amer. Math. Soc. Colloq. Publ., Vol. 37 (1956).
[2] F. KASCH, Über den Endomorphismenring eines Vektorraumes und den Satz von der Normalbasis, Math. Ann., 129 (1953) 447—463.
[3] M. MORIYA and T. NAGAHARA. On generating elements of Galois extensions of division rings II, Math. J. Okayama Univ., 7 (1957) 89—94.
[4] T. NAGAHARA, On primitive elements of Galois extensions of division rings, Math. J. Okayama Univ., 6 (1956) 23—28.
[5] ———, On generating elements of Galois extensions of division rings, Math. J. Okayama Univ., 6 (1957) 181—190.

DEPARTMENT OF MATHEMATICS,
OKAYAMA UNIVERSITY

(*Received November 25, 1957*)