

Mathematical Journal of Okayama University

Volume 6, Issue 2

1956

Article 7

MARCH 1957

On generating elements of Galois extensions of division rings

Takesi Nagahara*

*Okayama University

Copyright ©1956 by the authors. *Mathematical Journal of Okayama University* is produced by
The Berkeley Electronic Press (bepress). <http://escholarship.lib.okayama-u.ac.jp/mjou>

ON GENERATING ELEMENTS OF GALOIS EXTENSIONS OF DIVISION RINGS ¹⁾

TAKASI NAGAHARA

In his paper [2], F. Kasch proved the next theorem: If a division ring K is Galois and finite over a division subring L and the center of $V_K(L)$ is separable over the center of K then $K = L[k, uku^{-1}]$ ²⁾ with some $k, u \in K$.

Afterwards he obtained also the following theorem [3, Satz 14]: If a division ring K is Galois and finite over a division subring L , then $K = L[k, h]$ with some $k, h \in K$. Moreover, if either $V_K(L) = C$ or $V_K(L) \subset L$, then $K = L[k]$ with some $k \in K$, where C is the center of K .

The purpose of this note is to give an ultimate sharpening of the above theorems: Let K be a division ring which is Galois and finite over a division subring L , D be an intermediate subring of K/L , and \mathfrak{S} be the totality of L -inner automorphisms in K . If $\{x\}\mathfrak{S} \setminus D$ is finite for each $x \in D$, then $D = L[k, uku^{-1}]$ with some $k, u \in D$. In particular, $K = L[k, uku^{-1}]$ with some $k, u \in K$ (§3). And in this connection, we shall prove also that a division ring K has a single generating element over a division subring L of K under somewhat weaker assumption than those in the latter half of [3, Satz 14] (§2).

In this note, we wish to make use of the same notations and terminologies as in [4]³⁾.

1. Preliminaries.

Throughout this note, K will be a division ring, L be a division subring of K , and D be an intermediate division subring of K/L . Moreover, C will be the center of K , Z be that of L , and H will mean $V_K(V_K(L))$. If K is finite over L , then the total group of K/H is the totality of L -inner automorphisms of K . And clearly $Z = L \cap V_K(L)$, $V_H(H) = V_{V_K(L)}(V_K(L))$.

1) The author wishes to express his best thanks to Prof. M. Moriya and Mr. H. Tominaga for their kind encouragements and advices.

2) In general, for any subset S in K , $L[S]$ signify the subring of K generated by S over L , which was denoted by $L(S)$ in the previous papers [4], [5].

3) See [4, § 1].

Lemma 1. *Let R be a proper division subring of K , and a be an element in K such that $ab \neq ba$ for some b in $K \setminus R$.*

- (1) *There exist at most two c 's in $C \cap R$ with $(b+c)a(b+c)^{-1} \in R$.*
- (2) *If a is in R then there exists at most one c in $V_R(a)$ with $(b+c)a(b+c)^{-1} \in R$.*

Proof. At first we remark that if c', c'' are different elements in $V_R(a)$ then $(b+c')a(b+c')^{-1} \neq (b+c'')a(b+c'')^{-1}$. For, if not, $(b+c')a(b+c')^{-1} = (b+c'')a(b+c'')^{-1} = a'$ imply that $(c'+c'')a = a'(c'+c'')$, whence $a = a'$. But $(b+c')a(b+c')^{-1} = a$ leads to a contradiction $ba = ab$.

(1) Now we suppose $(b+c_i)a(b+c_i)^{-1} = a_i \in R$ with different c_i 's in $C \cap R$ ($i = 1, 2, 3$). Then $ba + c_1a = a_1b + a_1c_1$, $ba + c_2a = a_2b + a_2c_2$ and $ba + c_3a = a_3b + a_3c_3$, whence $(c_1 - c_2)a = (a_1 - a_2)b + (a_1c_1 - a_2c_2)$ and $(c_1 - c_3)a = (a_1 - a_3)b + (a_1c_1 - a_3c_3)$. Hence we have $a = (c_1 - c_2)^{-1}(a_1 - a_2)b + (c_1 - c_2)^{-1}(a_1c_1 - a_2c_2)$, $a = (c_1 - c_3)^{-1}(a_1 - a_3)b + (c_1 - c_3)^{-1}(a_1c_1 - a_3c_3)$, and so $0 = \{(c_1 - c_2)^{-1}(a_1 - a_2) - (c_1 - c_3)^{-1}(a_1 - a_3)\}b - \{(c_1 - c_2)^{-1}(a_1c_1 - a_2c_2) - (c_1 - c_3)^{-1}(a_1c_1 - a_3c_3)\}$. Since b is not in R , we must have:

- (i) $(c_1 - c_2)^{-1}(a_1 - a_2) - (c_1 - c_3)^{-1}(a_1 - a_3) = 0$,
- (ii) $(c_1 - c_2)^{-1}(a_1c_1 - a_2c_2) - (c_1 - c_3)^{-1}(a_1c_1 - a_3c_3) = 0$.

From (i) $\times c_1 -$ (ii), we obtain

$$(c_1 - c_2)^{-1}(c_1 - c_2)a_2 = (c_1 - c_3)^{-1}(c_1 - c_3)a_3,$$

whence $a_2 = a_3$. But this is a contradiction by the remark at the beginning.

(2) Suppose that $(b+c_1)a(b+c_1)^{-1} = a_1 \in R$ and $(b+c_2)a(b+c_2)^{-1} = a_2 \in R$ with some different c_1, c_2 in $V_R(a)$. Then $ba - a_1b = a_1c_1 - c_1a$, $ba - a_2b = a_2c_2 - c_2a$, whence we obtain $b = (a_2 - a_1)^{-1}\{(a_1c_1 - c_1a) - (a_2c_2 - c_2a)\} \in R$, being contradictory.

Lemma 2. *If $[K : L] < \infty$ and there exists only a finite number of intermediate subrings of $K/L[k']$ for some k' then $K = L[h', k']$ with some h' . If moreover K is really non-commutative then $K = L[k, uku^{-1}]$ with some $k, u \in K$.*

Proof. We may, and shall, consider only the case where $L[k'] \neq K$ and $L[k']$ is infinite. Choose such an element h' that $[L[h', k'] : L[k']]$ is as great as possible. Then we have $L[h', k'] = K$. For, if not, there exists some $x \in K \setminus L[h', k']$. And the infiniteness of $L[k']$ and our assumption that there exists only a finite number of intermediate subrings of $K/L[k']$ imply that there holds $L[h' + y_1x, k'] = L[h' + y_2x, k']$ for some different $y_1, y_2 \in L[k']$. Then we readily see $L[h' + y_1x, k'] = L[h', k', x]$, being contrary to the maximality of $[L[h', k'] : L[k']]$.

Now we shall prove the second part (under the assumption that $L[k']$

is a proper infinite subring of K .) At first we shall show that there exist some h, k such that $K=L[h, k]$, $L[k]=L[k']$ and $hk \neq kh$. Obviously it suffices to consider the case where $h'k' = k'h'$. We distinguish here three cases: (I) $L \not\subset V_K(k')$. For any $l \in L \setminus V_K(k')$, set $h = h' + l$, $k = k'$. (II) $L \not\subset V_K(h')$. For any $l' \in L \setminus V_K(h')$, set $h = h'$, $k = k' + l'$. (III) $L \subset V_K(h', k')$. There exist some $l_1, l_2 \in L$ such that $l_1 l_2 \neq l_2 l_1$. Set $h = h' + l_1$, $k = k' + l_2$.

Next we note that $V_{L(k)}(k)$ is infinite. For, if it is finite, so is $V_{L(k)}(L[k])[k]$. And so $[L[k] : V_{L(k)}(k)] = [V_{L(k)}(L[k])[k] : V_{L(k)}(L[k])] < \infty$, whence $L[k]$ ($= L[k']$) is finite, being contradictory. We can find therefore such $v \in V_{L(k)}(k)$ that $(h+v)k(h+v)^{-1}$ is not contained in any proper subring of K over $L[k]$, by using repeatedly Lemma 1 (2). This completes our proof.

In the rest of this note, K will be Galois and finite over L . and \mathfrak{G} , \mathfrak{F} will mean the total group of K/L , the totality of all L -inner automorphisms contained in \mathfrak{G} respectively. Then K is Galois over H and the total group of K/H coincides with \mathfrak{F} .

- Lemma 3.** (1) $L[V_K(L)] = L \times_Z V_K(L)$.
 (2) $V_H(H) = C$ implies $K = H \times_C V_K(L)$.
 (3) $D \cap C[Z] = Z \times_{Z \cap C} (D \cap C)$, $[V_K(L) : Z \cap C] < \infty$.

Proof. (1) is true without any assumption, and (2) is a direct consequence of [1, Theorem 7.3F]. Now we shall prove (3). As $\mathfrak{G}_{C[Z]}$ (the restriction of \mathfrak{G} on $C[Z]$) is the Galois group of $C[Z]/Z$ and \mathfrak{G}_C is the Galois group of $C/Z \cap C$, σ_C is identity if and only if $\sigma_{C[Z]}$ is the identity, where σ is an arbitrary automorphism in \mathfrak{G} . We obtain therefore $[C : C \cap Z] = \text{order of } \mathfrak{G}_C = \text{order of } \mathfrak{G}_{C[Z]} = [C[Z] : Z]$, whence $C[Z] = Z \times_{Z \cap C} C$. Let $\{z_1, z_2, \dots, z_n\}$ be a $Z \cap C$ -basis of Z and $d = \sum_{i=1}^n z_i c_i$ an arbitrary element of $D \cap C[Z]$ where c_i 's are in C , then $\sum_{i=1}^n z_i c_i = d = \sum_{i=1}^n z_i c_i^\sigma$ for each $\sigma \in \mathfrak{G}(K/D)$. Since C is normal, we obtain $c_i = c_i^\sigma$, that is, c_i 's are contained in D , and so $D \cap C[Z] = Z \times_{Z \cap C} (D \cap C)$. The latter part is easy.

Lemma 4. If $K \supset D_1 \supset D_2 \supset L$, then $[D_1 : V_{D_1}(Z)] \geq [D_2 : V_{D_2}(Z)]$.

Proof. Clearly there holds $[D_1 : V_{D_1}(Z)] = [V_{D_1}(D_1)[Z] : V_{D_1}(D_1)]$ and $[D_2 : V_{D_2}(Z)] = [V_{D_2}(D_2)[Z] : V_{D_2}(D_2)]$. Now we shall prove $[V_{D_1}(D_1)[Z] : V_{D_1}(D_1)] \geq [V_{D_2}(D_2)[Z] : V_{D_2}(D_2)]$. Let S be a (finite

independent) $V_{D_2}(D_2)$ -basis of $V_{D_2}(D_2)[Z]$ contained in Z . Then, if S is not linearly independent over $V_K(D_2)$ there exists a minimal subset $T = \{z_1, \dots, z_t\}$ of S which is not linearly independent over $V_K(D_2)$. Hence there holds that $a = z_1 + \sum_{i=2}^n z_i d_i = 0$, where $d_i \in V_K(D_2)$ ($i = 2, \dots, t$). Clearly, there is some d_j ($2 \leq j \leq t$) which does not belong to $V_{D_2}(D_2)$ and so, there exists some automorphism σ in $\mathfrak{G}(K/D_2)$ such that $d_j^\sigma \neq d_j$ (if $d_j^\tau = d_j$ for all τ in $\mathfrak{G}(K/D_2)$ then $d_j \in V_K(D_2) \cap D_2 = V_{D_2}(D_2)$). We can easily see that $d_i^\sigma \in V_K(D_2)$ ($i = 2, \dots, t$). From $a^\sigma - a = 0$, it follows that $\{z_1, \dots, z_t\}$ is a proper subset of T which is not linearly independent over $V_K(D_2)$ but this contradicts the choice of the subset T . Therefore, S is linearly independent over $V_K(D_2)$. Since $V_{D_1}(D_1) \subset V_K(D_1) \subset V_K(D_2)$, S is linearly independent over $V_{D_1}(D_1)$. As $S \subset V_{D_1}(D_1)[Z]$, we obtain $[V_{D_1}(D_1)[Z] : V_{D_1}(D_1)] \cong [V_{D_2}(D_2)[Z] : V_{D_2}(D_2)]$.

2. Generating elements of K over L .

Lemma 5. *If $V_H(H) = C$ and $L \cong Z$, then $K = L[k]$ with some $k \in K$.*

Proof. We may, and shall, assume that Z is infinite (For, in case Z is finite, \mathfrak{G} is outer and so, our assertion is true without any restriction ([5], [7])). As $V_K(L)$ is Galois and finite over Z , we obtain $V_K(L) = Z[v_1, v_2]$ with some v_i 's in $V_K(L)$ by [3, Satz 14]. Further, noting that H is outer Galois over $L[C]$, there exists a normal basis $\{h^\tau; \tau \in \mathfrak{G}(H/L[C])\}$ of H over $L[C]$, and so $H = L[C, h]$. As $\sum_{\tau \in \mathfrak{G}(H/L[C])} h^\tau$ is contained in $L[C]$, we may assume that $\sum_{\tau \in \mathfrak{G}(H/L[C])} h^\tau = 1$. Since $L \cong Z$, there exist some d_1, d_2 in L such that $d_1 d_2 \neq d_2 d_1$. Then, $1, d_1, d_2$ are $V_K(L)$ -independent. Now we set $\mathfrak{F} = \bigcup_{0 \neq x \in Z} \mathfrak{G}_x$, where $\mathfrak{G}_x = \mathfrak{G}(K/L[d_1 v_1 + d_2 v_2 + xw + h])$ and w is a primitive element of C over $C \cap Z$. Let σ be an arbitrary automorphism in \mathfrak{F} . As σ is contained in some \mathfrak{G}_x ($x \in Z$), $d_1 v_1 + d_2 v_2 + xw + h = d_1 v_1^\sigma + d_2 v_2^\sigma + xw^\sigma + h^\sigma$. Then if $h^\sigma = h$, we have $d_1 (v_1^\sigma - v_1) + d_2 (v_2^\sigma - v_2) + (xw^\sigma - xw) = 0$. Noting that $\{v_1^\sigma - v_1, v_2^\sigma - v_2, xw^\sigma - xw\} \subset V_K(L)$ and $1, d_1, d_2$ are $V_K(L)$ -independent, we can readily see $w^\sigma = w$. Conversely if $w^\sigma = w$, σ is contained in $\mathfrak{G}(K/L[C])$. As $d_1 v_1 + d_2 v_2 + xw + h = d_1 v_1^\sigma - d_2 v_2^\sigma - xw - h^\sigma$, we have $d_1 (v_1 - v_1^\sigma) + d_2 (v_2 - v_2^\sigma) = -h + h^\sigma = l \in L \cap V_K(L) \cap H = L[C]$. Recalling $\sigma \in \mathfrak{G}(K/L[C])$,

$h^\sigma = h^{\tau_0}$ for some $\tau_0 \in \mathfrak{G}(H/L[C]) = \mathfrak{G}(K/L[C])_H$. As $\sum_{\tau \in \mathfrak{G}(H/L[C])} h^\tau = 1$, we have $-h + h^\sigma = \sum h^{\tau_l}$. If $h \neq h^\sigma$ then $l = -1$, which contradicts the fact that $1, d_1, d_2$ are $V_K(L)$ -independent. Thus we have proved that, for any $\sigma \in \mathfrak{G}$, $h^\sigma = h$ is equivalent with $w^\sigma = w$.

Next we shall prove that there exists some \mathfrak{G}_{x_0} ($x_0 \in Z$) such that $h^\sigma = h$ for each σ in \mathfrak{G}_{x_0} . In case $h^\sigma = h$ for all σ in \mathfrak{G} , we have nothing to prove. Therefore, we shall assume that there exist σ 's in \mathfrak{G} such that $h^\sigma \neq h$ (accordingly $w^\sigma \neq w$ by the last remark). Now we set $\{h\}^\mathfrak{G} = \{h^{\sigma_1} = h, h^{\sigma_2}, \dots, h^{\sigma_m}\} (\subset H)$ and $\{w\}^\mathfrak{G} = \{w_1 = w, w_2, \dots, w_n\} (\subset C)$, where σ_i is in \mathfrak{G}_{x_i} . (Note that $m, n > 1$.) As Z is infinite, we can choose a non-zero element x_0 in Z such that $x_j(w - w_i) \neq x_0(w - w_i)$ ($i, l = 2, \dots, n; j = 1, 2, \dots, m$). Then $h^\sigma = h$ for all σ in \mathfrak{G}_{x_0} . For, if not, there exists some σ in \mathfrak{G}_{x_0} such that $d_1 v_1 + d_2 v_2 + x_0 w + h = d_1 v_1^\sigma + d_2 v_2^\sigma + x_0 w + h^\sigma$ with some $i \neq 1, j \neq 1$. On the other hand, $d_1 v_1 + d_2 v_2 + x_j w + h = d_1 v_1^{\sigma_j} + d_2 v_2^{\sigma_j} + x_j w + h^{\sigma_j}$ for some $l \neq 1$. Hence we have $x_0(w - w_i) - x_j(w - w_i) = d_1(v_1^\sigma - v_1^{\sigma_j}) + d_2(v_2^\sigma - v_2^{\sigma_j})$, which shows $x_0(w - w_i) - x_j(w - w_i) = 0$, for $1, d_1$ and d_2 are $V_K(L)$ -independent. But this is a contradiction. Thus $h^\sigma = h$ and so $w^\sigma = w$ for all σ in \mathfrak{G}_{x_0} by the above remark, which implies $v_1^\sigma = v_1, v_2^\sigma = v_2$ for all σ in \mathfrak{G}_{x_0} . Hence, by Galois theory, v_1, v_2, w, h are contained in $L[d_1 v_1 + d_2 v_2 + x_0 w + h]$, whence we have $L[d_1 v_1 + d_2 v_2 + x_0 w + h] \supset L[V_K(L), h] = H[V_K(L)] = K$ by Lemma 3 (2).

Corollary 1. *If $V_H(H) = C, L \supseteq Z$ and D is a subring of K which is normal over L , then $D = L[d]$ with some d in D .*

Proof. Since D is normal over L, D is Galois and finite over L . As $D^\mathfrak{G} = D$, either $D \subset H$ or $D \supset V_K(L)$ by [4, Lemma 2]. In case $D \subset H, D = L[d]$ by [5, Corollary 3]. On the other hand, if $D \supset V_K(L)$, we can readily see all the assumptions in Lemma 5 are fulfilled with respect to K/L . And so our proof is a direct consequence of Lemma 5.

Corollary 2. *If $L \supseteq Z$ then $V_K(V_H(H)) = L[k]$ with some $k \in V_K(V_H(H))$.*

Proof. If we set $V_K(V_H(H)) = T$ then T is clearly normal over L , whence T is Galois and finite over L . Since $[V_H(H) : C] < \infty$, we have $V_K(T) = V_K(V_K(V_H(H))) = V_H(H)$. As $T \supset V_K(H) = V_K(L) = V_T(L), T \supset V_K(L) \supset V_K(T)$ and $V_T(T) = V_K(T) = V_H(H)$, we can apply Lemma 5 to T/L instead of K/L .

Lemma 6. *If v is a non-zero element of $V_D(Z)$, there exist some element d in D and some finite subset $\{z_1, \dots, z_n\}$ of Z such that $D = \sum_{i=1}^n \oplus d^{\tilde{z}_i} V_D(Z)$ and that $d^{\tilde{z}_1} v + d^{\tilde{z}_2} v_2 + \dots + d^{\tilde{z}_n} v_n = 1$ with some v_i 's in $V_D(Z)$, where \tilde{z}_i are inner automorphisms generated by z_i ($i=1, \dots, n$).*

Proof. By Lemma 3 (3), $Z \cap C \subset D \cap C \subset V_D(D)$ and $[V_K(L) : Z \cap C] < \infty$. Since $V_K(L) \supset V_D(D)$ and $V_K(L) \supset Z$, we have $[V_D(D)[Z] : V_D(D)] \leq [V_K(L) : Z \cap C] < \infty$. As $V_D(V_D(D)[Z]) = V_D(Z)$ and $[V_D(D)[Z] : V_D(D)] < \infty$, it follows that $V_D(V_D(Z)) = V_D(D)[Z]$ and so $V_D(V_D(V_D(Z))) = V_D(Z)$, that is, D is finite and Galois over $V_D(Z)$ and the total group of $D/V_D(Z)$ is inner. Furthermore, since $V_D(V_D(Z)) = V_D(D)[Z] \subset V_D(Z)$, the ring \mathfrak{D} of endomorphisms of D generated by $\mathfrak{G}(D/V_D(Z))$ and $V_D(Z)$ ¹⁾ is \mathfrak{D} -isomorphic with D by [3, Satz 9]. Now we can choose a $V_D(D)$ -basis $\{z_1, \dots, z_n\}$ of $V_D(D)[Z]$ from $Z : V_D(D)[Z] = \sum_{i=1}^n \oplus z_i V_D(D)$. Clearly there holds $\sum_{i=1}^n \tilde{z}_i D_r = \sum_{i=1}^n \oplus \tilde{z}_i D_r$, and so $\sum_{i=1}^n \tilde{z}_i (V_D(Z))_r = \sum_{i=1}^n \oplus \tilde{z}_i (V_D(Z))_r$. Since $[D : V_D(Z)] = [V_D(D)[Z] : V_D(D)]$, $\mathfrak{D} = \sum_{i=1}^n \tilde{z}_i (V_D(Z))_r$ by [3, Satz 10]. As \mathfrak{D} is \mathfrak{D} -isomorphic to D , there exists an element d' in D which corresponds to 1 of $\sum_{i=1}^n \tilde{z}_i (V_D(Z))_r = \mathfrak{D}$ under this isomorphism. Then $D = \sum_{i=1}^n \oplus d'^{\tilde{z}_i} V_D(Z) = V_D(Z)[d']$ and we have $\sum_{i=1}^n d'^{\tilde{z}_i} v_i = 1$ with some v_i 's in $V_D(Z)$. Here without loss of generality, we may assume that v_1 is non-zero, then $d = d' v_1' v^{-1}$ is clearly a required one.

Theorem 1. (1) *If v is a non-zero element of $V_D(Z)$, then there exists some element d in D such that $L[d] \ni v$ and $D = V_D(Z)[d]$.*

(2) *If $V_D(Z) \subset H$, then $D = L[d]$ with some d in D .*

Proof. (1) By Lemma 6, there exists an element $d \in D$ and elements $\{z_1, \dots, z_n\}$ in Z such that $D = \sum_{i=1}^n \oplus d^{\tilde{z}_i} V_D(Z) = V_D(Z)[d]$ and that $d^{\tilde{z}_1} v + d^{\tilde{z}_2} v_2 + \dots + d^{\tilde{z}_n} v_n = 1$ with some v_i 's in $V_D(Z)$. Clearly $D \supset L[d]$, and so, by Lemma 4, $[D : V_D(Z)] \geq [L[d] : V_{\mathcal{K}(d)}(Z)]$ and $L[d] \supset \{d^{\tilde{z}_1}, \dots, d^{\tilde{z}_n}\}$. As $\{d^{\tilde{z}_1}, \dots, d^{\tilde{z}_n}\}$ is $V_D(Z)$ -independent, it is *a fortiori* $V_{\mathcal{K}(d)}(Z)$ -independent. Accordingly $\{d^{\tilde{z}_1}, \dots, d^{\tilde{z}_n}\}$ is a $V_{\mathcal{K}(d)}(Z)$ -basis of

1) $V_D(Z)_r$ denotes the totality of right multiplications determined by elements of $V_D(Z)$.

$L[d]$. Noting that $L[d] \ni 1$, $d^{\tilde{z}_1} v + \sum_{i=2}^n d^{\tilde{z}_i} v_i = 1 = \sum_{i=1}^n d^{\tilde{z}_i} v_i'$ for some v_i' 's in $V_{K(a)}(Z)$. As $d^{\tilde{z}_i}$'s are $V_D(Z)$ -independent, we have $v = v_1' \in V_{K(a)}(Z) \subset L[d]$, that is, $L[d] \ni v$. (2) In this case, $V_D(Z) = L[d']$ with some d' in $V_D(Z)$ by [5, Corollary 3]. Accordingly $D = V_D(Z)[d]$ for some d in D with $L[d] \ni d'$ by (1). Since $L[d] \supset L[d', d] = V_D(Z)[d] = D$ and trivially $L[d] \subset D$, we have $D = L[d]$.

Corollary 3. *If $V_H(H) = C[Z]$, $L \cong Z$ and $V_D(Z)$ is a subring of K which is normal over L , then $D = L[d]$ with some d in D .*

Proof. We shall denote $V_D(Z) = T$. Since T is normal over L , either $T \subset H$ or $T \supset V_K(L)$ by [4, Lemma 2]. If $T \subset H$, then $D = L[d]$ for some $d \in D$ by Theorem 1 (2). If $T \supset V_K(L)$ then $V_T(L) = T \cap V_K(L) = V_K(L)$, that is, the center of $V_T(L)$ is $C[Z] = V_H(H)$ (= center of $V_K(L)$). Since $C[Z] \subset V_K(L) \subset T = V_D(Z)$, we may easily see that $C[Z] \subset V_T(T) \subset V_{V_T(L)}(V_T(L)) = C[Z]$, whence $C[Z] = V_T(T)$. Applying Lemma 5 to T/L , we have $V_D(Z) = L[d']$ for some $d' \in V_D(Z)$ and hence, $D = L[d]$ for some $d \in D$ by Theorem 1 (1).

Corollary 4. *If $V_K(L) = C[Z]$ and D is an intermediate subring of K/L , then $D = L[d]$ with some $d \in D$.*

Proof. Clearly $V_D(Z) \subset H = V_K(C[Z])$, and so $D = L[d]$ with some $d \in D$ by Theorem 1 (2). In particular, if $V_K(L) \subset L$, that is, $V_K(L) = Z$, then $D = L[d]$ with some $d \in D$.

Corollary 5. *Let L be finite over Z . Then we have the following:*

- (1) *If $V_K(L)$ is commutative, then $D = L[d]$ with some $d \in D$.*
- (2) *If $L \cong Z$ and D is a subring of K which is normal over L , then $D = L[d]$ with some $d \in D$.*

Proof. As $[L : Z] < \infty$, we have $[K : C] < \infty$ (Cf. 4, p. 10), whence K is inner Galois over C . We obtain therefore $V_K(V_K(L)) = V_K(V_K(L[C])) = L[C] \subset L \times_Z V_K(L)$, and so $V_H(H) = C[Z]$. (1) If $V_K(L)$ is commutative, then $D = L[d]$ with some d in D by Corollary 4. (2) If D is normal over L , then so is $V_D(Z)$, and hence $D = L[d]$ with some d in D by Corollary 3.

Lemma 7. *If L is a field and $L \not\subset C$, then $K = L[d]$ for some $d \in K$.*

Proof. We set $L \cap C = C_0$. Then, $[K : C] < \infty$ and $[C : C_0] < \infty$, whence $[K : C_0] = [K : C][C : C_0] < \infty$. Let \tilde{K} be the group of

all inner automorphisms generated by non-zero elements of K and let \mathfrak{G} be the total group of K/L . Then, C_0 is the fixed subring of $[\widetilde{K}, \mathfrak{G}]$ in K where $[\widetilde{K}, \mathfrak{G}]$ is the group of automorphisms generated by \widetilde{K} and \mathfrak{G} , that is, K is finite and Galois over C_0 . If C_0 is finite then K is a finite field and so, $K = C$ which contradicts $L \not\subseteq C$. Therefore, C_0 is an infinite field. We consider a maximal subfield M of K which is separable over C . Since C is separable over C_0 , M is separable over C_0 . Therefore, there is an element $d_1 \in M$ such that $M = C_0[d_1]$. Further, there exists only a finite number of subfields $\{W_1, W_2, \dots, W_n\}$ of M which properly contain C . As $V_K(M) = M$, there exists an element d_2 such that $K = M[d_2] = C_0[d_1, d_2]$. Now, let a be an element of $L \setminus C$. Then, we may assume without loss of generality that $ad_2 \neq d_2a$. For, if not, we can use $d_1 + d_2$ in place of d_2 . As $K_i = V_K(W_i) \supset M$ and $W_i \cong C$ for $i = 1, 2, \dots, n$, d_2 is contained in none of K_i 's. Since C_0 is infinite, we can choose by Lemma 1 an element $c \in C_0$ such that $(d_2 + c)a(d_2 + c)^{-1} \notin K_i$ ($i = 1, 2, \dots, n$). Hence we have $K = C_0[d_1, (d_2 + c)a(d_2 + c)^{-1}]$. Clearly, $K = (d_2 + c)^{-1}K(d_2 + c) = C_0[(d_2 + c)^{-1}d_1(d_2 + c), a] = C_0[a] [(d_2 + c)^{-1}d_1(d_2 + c)] = L[(d_2 + c)^{-1}d_1(d_2 + c)] = K$, whence $K = L[d]$ for $d = (d_2 + c)^{-1}d_1(d_2 + c)$.

Remark. In case $L = Z$, $H = L[C]$ and so $V_H(H) = C[Z]$.

Combining Lemma 7 with Corollaries 3, 4, we can easily obtain the following :

Theorem 2. *Under the assumption that K is non-commutative and $V_H(H) = C[Z]$, $K = L[d]$ with some d if and only if $L \not\subseteq C$.*

Corollary 6. *Under the assumption that K is non-commutative and K is inner Galois over L , $K = L[d]$ with some d if and only if $L \cong C$.*

Proof. Clearly, $H = V_K(V_K(L)) = L$, and so, we obtain $C \subset V_H(H) = V_L(L) = Z$. Hence, our assertion is an immediate consequence of Theorem 2.

Combining Lemma 7 with Corollary 5, we can easily obtain the following :

Corollary 7. *Let L be finite over Z and K be non-commutative, then $D = L[d]$ with some $d \in K$ if and only if $L \not\subseteq C$.*

3. Two conjugate generating elements of K over L .

Theorem 3. *If $V_K(L)$ is commutative, then $D = L[k, uku^{-1}]$ with some $k, u \in D$.*

Proof. If $V_K(L)$ is finite, then $D = L[d]$ with some d in D by [5, Corollary 2]. If $V_D(Z) \subset H$, then $D = L[d]$ with some d in D by Theorem 1 (2). In both cases, the theorem holds clearly true. Hence we shall assume that $V_K(L)$ is infinite and $V_D(Z)$ is not contained in H . Then clearly $L \cap C$ is infinite, D is non-commutative and $V_K(L) \cong V_K(V_D(Z))$. Since $V_K(L) \supset V_K(V_D(Z)) \supset Z$ and $V_K(L)$ is separable over Z , so it is over $V_K(V_D(Z))$. Then there exists only a finite number of subfields $\{W_1, \dots, W_n\}$ of $V_K(L)$ which properly contain $V_K(V_D(Z))$. Let $\{t_1, \dots, t_n\}$ be chosen such as $t_i \in W_i \setminus V_K(V_D(Z))$. Since L is infinite, we can select from $V_D(Z)$ an element d such that $d^{\bar{t}_i} \neq d (i = 1, 2, \dots, n)$, by making use of the same method as in the proof of [2, Hilfssatz 1]. Then $V_{V_K(L)}(d) = V_K(V_D(Z))$. Moreover, by Theorem (1), there exists some $f \in D$ such that $D = V_D(Z)[f]$ and $L[f] \ni d$. And so, $V_K(L[f]) = V_K(L[f, d]) = V_{V_K(L)}(f, d) = V_{V_K(L)}(f) \cap V_{V_K(L)}(d) = V_{V_K(L)}(f) \cap V_K(V_D(Z)) = V_K(V_D(Z)[f]) = V_K(D)$. Thus, we have $V_K(V_K(L[f])) \supset D \supset L[f]$. Clearly, $V_K(V_K(L[f]))$ is outer Galois over $L[f]$ so that there exists only a finite number of intermediate subrings of $D/L[f]$. Hence, by Lemma 2, $D = L[k, uku^{-1}]$ for some k, u in D .

Lemma 8. *If D is left set-wise invariant by \mathfrak{S} , then $D = L[k, uku^{-1}]$ with some $k, u \in D$.*

Proof. By [4, Lemma 2], either $D \subset H$ or $D \supset V_K(L)$. In the first case, D has a single generating element over L by [5, Corollary 3]. Now, we shall assume that $D \not\subset H$, so that $D \supset V_K(L) (= V_D(L))$ and D is non-commutative. We set $D_1 = V_D(V_D(L))$, then D is inner Galois over D_1 . If $D_1 \cong V_D(D)$, then $D = D_1[d]$ by Corollary 6. Since $V_D(L) = V_K(L)$, it follows that $L \subset D_1 \subset H$, whence $V_K(L[d]) = V_{V_K(L)}(d) = V_{V_K(D_1)}(d) = V_K(D_1[d]) = V_K(D)$. Hence $V_K(V_K(L[d])) \supset D \supset L[d]$. Clearly, $V_K(V_K(L[d]))$ is outer Galois over $L[d]$. So that, all the assumptions in Lemma 2 are satisfied with respect to $D/L[d]$. Hence $D = L[k, uku^{-1}]$ for some $k, u \in D$ by Lemma 2.

On the other hand, if $D_1 = V_D(D)$, then $L \subset D_1 = V_D(D)$, and so $Z = V_L(L) = L$, $V_K(L) \subset D \subset V_K(V_D(D)) \subset V_K(L)$. Hence $D = V_K(L)$. As is easily seen, $V_K(L)$ is Galois over Z . Moreover, $V_D(D) = C[Z]$ is

separable over Z . We have therefore $D = V_x(L) = Z[k, uku^{-1}]$ with some $k, u \in D$ by [5, Lemma 4].

Theorem 4. *If, for any $x \in D$, $\{x\}^{\mathfrak{S}} \setminus D$ is finite, then $D = L[k, uku^{-1}]$ for some $k, u \in D$. In particular, $K = L[k, uku^{-1}]$ for some $k, u \in K$.*

Proof. In case $\mathfrak{G}(K/L)$ is almost outer, all the restrictions in this theorem are superfluous and $D = L[d]$ for some $d \in D$ by [5, Corollary]. On the other hand, in case $\mathfrak{G}(K/L)$ is not almost outer, by making use of the same method as in the proof of [5, Principal Theorem], we obtain that D is left set-wise invariant by \mathfrak{S} . Hence $D = L[k, uku^{-1}]$ for some $k, u \in D$ by Lemma 8.

And we can readily see.

Corollary 8. *Let K/L be Galois, $\mathfrak{G}(K/L)$ be locally finite-dimensional. If D is an intermediate subring of K finite over L such that, for any $x \in D$, $\{x\}^{\mathfrak{G}} \setminus D$ is finite, then $D = L[k, uku^{-1}]$ with some $k, u \in D$.*

REFERENCES

- [1] E. ARTIN, C. NESBITT and R. THRALL: Rings with minimum condition, Ann Arbor (1944).
- [2] F. KASCH: Über den Satz vom primitiven Element bei Schiefkörper, J. reine und angew. Math., 180 (1951), 150—159.
- [3] ———: Über den Endomorphismenring eines Vektorraumes und den Satz von der Normalbasis, Math. Annalen., 129 (1953), 447—463.
- [4] T. NAGAHARA and H. TOMINAGA: On Galois theory of division rings, Math. J. Okayama Univ., 6 (1956) 1—21.
- [5] NAGAHARA: On primitive elements of Galois extensions of division rings, Math. J. Okayama Univ., 6 (1956) 23—28.
- [6] N. NOBUSAWA: An Extension of Krull's Galois theory to division rings, Osaka Math. J., 7 (1955), 1—6.
- [7] ———: On compact Galois groups of division rings, Osaka Math. J., 8 (1956), 43—50.

DEPARTMENT OF MATHEMATICS,
OKAYAMA UNIVERSITY

(Received March 3, 1957)