

Mathematical Journal of Okayama University

Volume 10, Issue 1

1960

Article 2

OCTOBER 1960

On generating elements of Galois extensions of division rings V

Takasi Nagahara*

*Okayama University

Copyright ©1960 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 V

TAKASI NAGAHARA

1°. Let a division ring K be Galois over a division subring L . In case L is infinite over the center of L , we have proved, in a previous paper [8]¹⁾, that if D is an arbitrary intermediate subring of K/L which is left finite over L then D is simple over L . In this paper, for an arbitrary L - L -submodule X of K which is left finite over L , we shall prove that X has a single generating element over L , that is, $X = LaL$ for some a (Theorem 1).

In 3°, our interest will be directed to Kurosch's problem for algebraic Galois extensions of division rings. And, we shall prove the following: Every (left) algebraic Galois extension K of L is locally finite over L if either L is infinite over the center of L or the centralizer of L in K is finite over the center of K (Theorem 2 and Theorem 3). Moreover, if K is Galois, left algebraic and of bounded degree over L , then K is finite over L (Theorem 4).

Finally, as to notations and terminologies used in this paper, we follow the previous ones [6], [7] and [8].

2°. Generating elements of L - L -submodules of K .

Throughout this paper, K will be a division ring and L a division subring of K . C and Z will be the centers of K and L respectively, and V will mean $V_K(L)$. Moreover, in this section, we shall use the following conventions: X be a L - L -submodule of K and \mathfrak{X} the L_r - K_r -module consisting of all the (module) homomorphisms of X into K . And, we set $\mathfrak{Y} = \{\alpha \in \mathfrak{X} \mid \alpha l_r = l_r \alpha \text{ for all } l_r \in L_r\}$.

The following lemma contains [7, Lemma 1] and [8, Lemma 1] as special cases. However, as the proof proceeds just as in the proof of [8, Lemma 1], the proof may be omitted.

Lemma 1. *For any subset \mathfrak{S} of \mathfrak{Y} , \mathfrak{S} is linearly independent over V_r if and only if it is linearly independent over K_r .*

Often the next corollary will be very convenient.

Corollary 1. *Let K be Galois over L , and \mathfrak{G} a Galois group of K/L , that is, the fixing of \mathfrak{G} is L . If \mathfrak{G}_X means the restriction of \mathfrak{G} on X then:*

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

- (1) $[\mathbb{G}_X V_r : V_r]_r = [\mathbb{G}_X K_r : K_r]_r \approx [X : L]_l^{(2)}$ and $\mathbb{G}_X K_r \cap \mathfrak{V} = \mathbb{G}_X V_r$.
 (2) If $X = LaL^{(3)}$ for some $a \in X$, then $[a\mathbb{G}_X V_r : V_r]_r \approx [X : L]_l$.

Proof. The first part of our corollary will be proved by making use of the same method as in the proof of [8, Corollary 2]. Thus, we shall prove here the second part only. Noting that $\alpha \in \mathbb{G}_X V_r$ annihilates a when and only when $X\alpha = L(a\alpha)L = 0$, we obtain $[a\mathbb{G}_X V_r : V_r]_r = [\mathbb{G}_X V_r : V_r]_r$. Hence, (2) is an easy consequence of (1).

In the rest of this note, we denote by \mathbb{G} a Galois group of K/L when K is Galois over L .

Remark 1. Let K be Galois and finite over L . If $V \subset L$ then there exists some a such that $K = a\mathbb{G}L_r$ ([3, Satz 9]). And then, we have $[K : L]_r = [a\mathbb{G}L_r : L]_r \leq [a\mathbb{G}V_r : V_r]_r = [LaL : L]_l$ by Corollary 1(2). It follows that $K = LaL = \sum_{i=1}^n \oplus Ll_i al_i^{-1} = \sum_{i=1}^n \oplus l_i' al_i'^{-1} L^{(4)}$ with l_i 's and l_i' 's of L .

In order to prove Theorem 1 which has been cited in 1°, one more lemma will be required.

Lemma 2. Let K be Galois over L , M a (commutative) subfield of L which is algebraic and infinite over Z , N a right V -submodule of K which is (right) finite over V , and d an element of K . If $d\mathbb{G}V_r = \sum_{u=1}^r \oplus d_u V$ and $\sum_{u=1}^r d_u M_0 = \sum_{u=1}^s \oplus d_u M_0$, where $M_0 = M[V] = M \times_Z V (\subset L \times_Z V)$, then there exist an element $m \in M$ and a division subring M^* of M_0 containing V such that $[M^* : V]_r < \infty$, $N + \sum_{u=1}^s d_u m M^* = N \oplus \sum_{u=1}^s d_u m M^* = N \oplus (\sum_{u=1}^s d_u M^*)m$ and that $d\mathbb{G}V_r \subset \sum_{u=1}^s d_u M^*$.

Proof. We set $d_i = \sum_{u=1}^s d_u m_{iu}$ with m_{iu} 's of $M_0 (i = s+1, \dots, r)$ and denote by R the intersection of N and $\sum_{u=1}^s d_u M_0$. Clearly, R is a right V -submodule of K which is finite over V .

Now we shall distinguish two cases: Firstly in case $R = 0$, we set $M^* = V[\{m_{iu}\}]$. Since $M_0 = M \times_Z V$, we can choose a finite subset F of M such that $M^{*'} = V[F] \supset M^*$. Then, noting that M is a commutative field which is algebraic over Z , we have $[M^* : V]_r \leq [M^{*'} : V]_r < \infty$. Further, we obtain $N + \sum_{u=1}^s d_u M^* = N \oplus \sum_{u=1}^s d_u M^*$ since $R = \{0\}$. It is clear that $d\mathbb{G}V_r \subset \sum_{u=1}^s d_u M^*$.

Secondly, we consider the case $R \neq \{0\}$. As R is a right V -module which is finite over V , we denote by $\{x_1, \dots, x_n\}$ a right V -basis of R . Then

- (1) $x_h = \sum_{u=1}^s d_u y_{hu} (h = 1, 2, \dots, n)$

where y_{hu} 's are all in M_0 . We set here $M^* = V[\{m_{iu}\}, \{y_{hu}\}]$. Noting that $M_0 = M \times_Z V$, we can take some finite subset F of M such that $V[F] \supset M^*$. Since M is algebraic over Z , we have $[V[F] : V] < \infty$, which means that

2) $[:]_l$ and $[:]_r$ denote the left and right dimensions respectively. And in case $[X : L]_l = [X : L]_r$, they are denoted as $[X : L]$. If either $[\mathbb{G}_X V_r : V_r]_r = [X : L]_l$ or $[\mathbb{G}_X V_r : V_r]_r = \infty$ and $[X : L]_l = \infty$, then we write $[\mathbb{G}_X V_r : V_r]_r \approx [X : L]_l$.

3) LaL is the two-sided L -module generated by a over L .

4) Given a collection $\{A_i\}$ of modules, $\sum \oplus A_i$ denote the direct sum of the A_i .

$[M^*: V] < \infty$. Then, from $[M: Z] = [M_0: V] = \infty$, we obtain $M^* \subseteq M_0$, and so $M \not\subseteq M^*$. Hence, there exists an element $m \in M \setminus M^*$. Suppose that $N \cap \sum_{u=1}^s d_u m M^* \neq \{0\}$. Let

$$(2) \quad \sum_{h=1}^n x_h v_h = \sum_{u=1}^s d_u m y_u'$$

be a non-zero element of $N \cap \sum_{u=1}^s d_u m M^* \subset R$, where v_h 's are all in V and y_u 's are all in M^* . Then, from (1) and (2), we obtain

$\sum_{u=1}^s d_u (m y_u' - \sum_{h=1}^n y_{hu} v_h) = 0$, whence $m y_u' - \sum_{h=1}^n y_{hu} v_h = 0$ ($u = 1, 2, \dots, s$). This leads to the contradiction $m \in M^*$. Hence we have $N + \sum_{u=1}^s d_u m M^* = N \oplus \sum_{u=1}^s d_u m M^*$ and $d \otimes V_r \subset \sum_{u=1}^s d_u m M^*$.

Now we are at the position to prove the following which contains [8, Theorem 1*].

Theorem 1. *Let K be Galois over L , and let $[L: Z] = \infty$. If X is a L - L -submodule of K which is left finite over L , then $X = LaL$ for some $a \in X$.*

Proof. Let $[X: L]_i = n$. Then, from Corollary 1(2), we have $[a \otimes V_r: V]_r = [LaL: L]_i \leq [X: L]_i = n$ for any element a in X . Hence, it suffices to prove that there exists an element $a \in X$ such that $[a \otimes V_r: V]_r = [X: L]_i = n$.

We set $X = \sum_{i=1}^n L d^{(i)}$ and $\otimes_x V_r = \sum_{i=1}^n \oplus \sigma_{ix} V_r$ (Corollary 1(1)). Then, by Corollary 1(2), we have $[d^{(i)} \otimes V_r: V]_r < \infty$. We shall distinguish two cases:

Case I. L is not algebraic over Z . Let $x \in L$ be transcendental over Z . If we set $M' = \sum_{i=1}^n d^{(i)} \otimes V_r$, then, by [8, Lemma 3], there exists some positive integer k such that $\sum_{i=0}^{\infty} M' y^i = \sum_{i=0}^{\infty} \oplus M' y^i$ for $y = x^k$. If $\alpha = \sum_{i=1}^n \sigma_{ix} v_{ir}$ is a non-zero element of $\otimes_x V_r$, then $0 \neq X\alpha = \sum_{i=1}^n L(d^{(i)}\alpha)$, so that, there exists an element $d^{(i)}$ such that $d^{(i)}\alpha \neq 0$. We set here $a = \sum_{i=1}^n d^{(i)} y^i$. Noting that $d^{(i)}\alpha \in M'$ and $\sum_{i=1}^n M' y^i = \sum_{i=1}^n \oplus M' y^i$, we obtain $a\alpha = \sum_{i=1}^n (d^{(i)}\alpha) y^i \neq 0$. Hence, $\{a\sigma_1, \dots, a\sigma_n\}$ is right V -independent. There holds therefore $[a \otimes V_r: V]_r = [\otimes_x V_r: V_r]_r = n$.

Case II. L is algebraic over Z . Let M be a maximal subfield of L . Then it is clear that $[M: Z] = \infty$. As to notations used in the rest of our proof, we shall follow Lemma 2. In case $n = 1$, our assertion is trivial, and so we may restrict our proof to the case $n > 1$. We set $d^{(i)} \otimes V_r = \sum_{u=1}^{r_i} d_{iu} V$ ($i = 2, \dots, n$), and $\sum_{u=1}^{r_i} d_{iu} M_0 = \sum_{u=1}^{r_i} \oplus d_{iu} M_0$. Applying Lemma 2 to $N = d^{(i)} \otimes V_r$ and $d = d^{(2)}$, we obtain an element $m_1 \in M$ and a division ring M_1 of M_0 containing V such that $[M_1: V]_r < \infty$, $d^{(i)} \otimes V_r + \sum_{u=1}^{s_2} d_{2u} m_1 M_1 = d^{(i)} \otimes V_r \oplus \sum_{u=1}^{s_2} d_{2u} m_1 M_1$, and that $d^{(2)} \otimes V_r \subset \sum_{u=1}^{s_2} d_{2u} M_1$. Repeating the same procedure to $N = d^{(i)} \otimes V_r \oplus \sum_{u=1}^{s_2} d_{2u} m_1 M_1$ and $d = d^{(3)}$, and so on, we have eventually $n-1$ elements m_i 's of M and $n-1$ subfields M_i of M_0 containing V such that $d^{(i)} \otimes V_r + \sum_{i=1}^{n-1} (\sum_{u=1}^{s_{i+1}} d_{i+1u} m_i M_i) = d^{(i)} \otimes V_r \oplus \sum_{i=1}^{n-1} (\sum_{u=1}^{s_{i+1}} d_{i+1u} m_i M_i)$

$d_{i+1u}m_i M_i) = d^{(1)} \otimes V_r \oplus \sum_{i=1}^{n-1} \oplus (\sum_{u=1}^{s_{i+1}} d_{i+1u} M_i) m_i$ and that $d^{(t+1)} \otimes V_r \subset \sum_{u=1}^{s_{i+1}} d_{i+1u} M_i (i = 1, \dots, n-1)$. Setting here $a = d^{(1)} + \sum_{i=1}^{n-1} d^{(i+1)} m_i$, the same argument as in the latter part of case I will show that $[a \otimes V_r : V]_r = n$.

Corollary 2. *Under the same assumption as in Theorem 1, for each subring D of K which is left finite over L , $D = \sum_{i=1}^n \oplus L l_i a l_i^{-1}$ with some $a \in D$.*

3°. Algebraic Galois extensions.

In [1, VII, §6], N. Jacobson gave the following definition :

Definition. An element a of a division ring K is called left algebraic over a division subring L if and only if $[L[a] : L]_l < \infty$. K is left algebraic over L if and only if every $a \in K$ is left algebraic over L .

We denote by N the set of all elements of K such that $[LaL : L]_l < \infty$. Let a_1, a_2 be elements of N . Then, noting that $L(a_1 + a_2)L \subset La_1L + La_2L$ and $La_1a_2L \subset La_1La_2L$, we obtain $[L(a_1 + a_2)L : L]_l \leq [La_1L : L]_l + [La_2L : L]_l < \infty$ and $[La_1a_2L : L]_l \leq [La_1La_2L : L]_l \leq [La_1L : L]_l [La_2L : L]_l < \infty$. Hence, both $a_1 + a_2$ and a_1a_2 are contained in N ; this shows that N is a subring of K . Moreover, one will easily see that N contains all the elements which are left algebraic over L . Under this convention, there holds the next lemma.

Lemma 3. *Let K be Galois over L , and let $[L : Z] = \infty$. If $\{a_1, \dots, a_n\}$ is a finite subset of N , then $\sum_{i=1}^n La_iL = LaL$ for some $a \in N$, and so, $L[a_1, \dots, a_n] = L[a]$.*

Proof. Since $[La_iL : L]_l$ is finite for each a_i , $\sum_{i=1}^n La_iL$ is left finite over L . Hence, our assertion is a consequence of Theorem 1.

Noting that if K is left algebraic over L then $K = N$, Lemma 3 yields at once the following.

Theorem 2. *Let K be Galois and left algebraic over L . If $[L : Z] = \infty$, then K is left locally finite over L ⁵⁾.*

Corollary 3. *Let K be Galois over L . If K is left algebraic over L , then K is right algebraic over L .*

Proof. In case $[L : Z] = \infty$, K is left locally finite over L . Hence, by [5, Corollary 1], K is right locally finite over L , accordingly, K is right algebraic over L . Let $[L : Z] < \infty$, and a an element of K . Then, by [1, Theorem 7.9.1], we have $[L[a] : L]_r \leq [L[a] : Z]_r = [L[a] : Z]_l < \infty$.

Remark 2. We set $H = V_K(V)$. If K is Galois and left algebraic over

5) If K is Galois and left locally finite over L , then K is right locally finite too ([5, Theorem 2]).

L , then one will easily see that K is left algebraic over H (Cf. [9, Lemma 2]). Further, we can prove that if K is Galois over L and left algebraic over H then, for each intermediate subring D of K/L which is left finite over L , $[D : L]_l = [D : L]_r$. In fact, in case $[L : Z] < \infty$, the same argument as in the proof of Corollary 3 will give our assertion. On the other hand, in case $[L : Z] = \infty$, $L[V] = L \times_z V \supset (L \times_z V) \cap H \supset L \times_z V_H(H)$ implies $[H : V_H(H)] = \infty$. Accordingly, our assertion is a consequence of Theorem 2 and [5, Theorem 2].

Our next theorem will enable us to restate [4, § 3] in a similar form as in [1, VII, § 6]⁶⁾.

Theorem 3. *Let K be Galois, and left algebraic over L . If $[V : C] < \infty$, then K is left locally finite over L .*

Proof. By the light of Theorem 2, we may, and shall, restrict our proof to the case $[L : Z] < \infty$. Since $L[V] = L \times_z V$, we have $[L[V] : C] = [L[V] : V][V : C] < \infty$, whence K is inner Galois over $L[V]$. Then, noting that $V_K(L[V]) \subset V_K(L) = V$, we obtain $H = V_K(V) \subset V_K(V_K(L[V])) = L[V]$, and so $[K : L[V]] \leq [K : H] = [V : C] < \infty$. Thus, we get $[K : C] = [K : L[V]][L[V] : C] < \infty$.

On the other hand, noting that $L[V]$ is left algebraic over L , we see that V is algebraic over Z , so that, the subfield $Z[C]$ is (\mathfrak{G} -normal⁷⁾ and) locally finite over Z . And then, for any finite subset F of C , a similar argument as in the proof of [6, Lemma 3 (3)] enables us to prove that $Z[F\mathfrak{G}] = Z \times_{Z \cap C} (Z \cap C)[F\mathfrak{G}]$, and so we have $Z[C] = Z \times_{Z \cap C} C$. Hence, there holds that $L[C] = L \times_z Z[C] = L \times_z (Z \times_{Z \cap C} C) = L \times_{Z \cap C} C$, whence we obtain $[L : (Z \cap C)] = [L[C] : C]$. It follows therefore that for any $k \in K$, $[(Z \cap C)[k] : (Z \cap C)] \leq [L[k] : (Z \cap C)] = [L[k] : L][L : (Z \cap C)] = [L[k] : L][L[C] : C] \leq [L[k] : L][K : C]$. Thus, recalling that $[K : C] < \infty$, we see that K is algebraic over $Z \cap C$. Then, by [1, Proposition 10.12.3], K is locally finite over $Z \cap C$. Consequently, from $[L : (Z \cap C)] (= [L[C] : C]) \leq [K : C] < \infty$, our assertion is immediate.

Lemma 4. *Let L be a subfield of K containing the center C of K . If K/L is left algebraic and of bounded degree then $[K : L] < \infty$.*

Proof. Suppose that $x \in L$ is transcendental over C . Then, $\{1, x_r, x_r^2, \dots\} (\subset \text{Hom}_{L_r}(K, K)^{(8)})$ is linearly independent over $L_l (\subset \text{Hom}_{L_l}(K, K))$. Now, let X be an arbitrary L - L -submodule of K with $[X : L]_l < \infty$, and

6) See [8, Remark 2] and the remarks of [9, Theorem 2'].

7) For any subring D of K , we say that D is \mathfrak{G} -normal when $D^\sigma = D$ for all $\sigma \in \mathfrak{G}$.

8) $\text{Hom}_{L_l}(K, K)$ denotes the module consisting of all the left L -homomorphisms of K into K .

$\mu_x(\cdot)$ a minimal polynomial of $(x_r)_x$ (which may be considered as an element of $\text{Hom}_{L_1}(X, X)$) over $L_1(\subset \text{Hom}_{L_1}(X, X))$ with the degree $n(X)$. We can find here an element $k \in K$ such that $k\mu_x(x_r) \neq 0$, and then $X_1 = X + LkL$ is an L - L -submodule with $[X_1 : L]_i < \infty$. Since $X_1\mu_x(x_r) \neq 0$, we readily see that $n(X_1) > n(X)$. And, this enables us to choose an L - L -submodule Y with $[Y : L]_i < \infty$ such that $n(Y) > m$, where m is an integer such that $[L[a] : L]_i \leq m$ for all $a \in K$. Then, by [2, p. 69, Theorem 1], there exists some $y \in Y$ such that $\{y, yx_r, \dots, yx_r^{n(Y)}\}$ is linearly left independent over L . But, recalling that $x \in L$, this gives a contradiction $n(Y) \leq [LyL : L]_i \leq [L[y] : L]_i \leq m$. Thus, we see that L is algebraic over C .

Secondly, we shall prove $[L : C] < \infty$. If, otherwise, $[L : C] = \infty$, then there exists a subfield L_1 of L with $m < [L_1 : C] = s < \infty$. Evidently, K is finite and Galois over $V_K(L_1)$ and $L_1 \subset V_K(L_1)$. Hence, by [3, Satz 9], there exists an element $u \in K$ such that $K = \sum_{i=1}^s \oplus V_K(L_1)u\tilde{l}_i$, where \tilde{l}_i 's are suitable elements of $L_1^{(9)}$. Accordingly, $\sum_{i=1}^s Lu\tilde{l}_i = \sum_{i=1}^s \oplus Lu\tilde{l}_i = \sum_{i=1}^s \oplus Lu\tilde{l}_i^{-1}$, which gives a contradiction $s \leq [LuL : L]_i \leq m$. Hence, $[L : C] < \infty$. Accordingly $V_K(V_K(L)) \cap V_K(L) = L \cap V_K(L) = L$, whence $V_K(L)$ is algebraic and of bounded degree over its center L . [1, Theorem 7.11.1] proves therefore $[V_K(L) : L] < \infty$. And we have eventually $[K : L] = [K : V_K(L)] [V_K(L) : L] < \infty$.

Now, we can prove a theorem which contains [1, Theorem 7.11.1] as a special case.

Theorem 4. *If K is Galois, left algebraic and of bounded degree over L , then $[K : L] < \infty$.*

Proof. In case $[L : Z] = \infty$, our assertion is contained in Lemma 3. Thus, in what follows, we shall restrict our proof to the case $[L : Z] = q < \infty$. Since $L[V] = L \times_Z V$, V is algebraic and of bounded degree over Z , accordingly so is the center C_0 of V . Moreover, C_0 is \mathfrak{G} -normal and \mathfrak{G}_{C_0} is the Galois group of C_0/Z . Hence, C_0 being normal and separable over Z , we readily obtain $[C_0 : Z] = \text{order of } \mathfrak{G}_{C_0} < \infty$. Then, noting that the center C of K is a \mathfrak{G} -normal subfield of C_0 , we obtain $s = [C : L \cap C] = \text{order of } \mathfrak{G}_C \leq \text{order of } \mathfrak{G}_{C_0} < \infty$. Now, let k be an arbitrary element of K . Then, one will easily see that $L[k][C] = \sum_{i=1}^s L[k]c_i$ for a $(L \cap C)$ -basis $\{c_1, \dots, c_s\}$ of C , whence we obtain $[Z[C][k] : Z[C]]_i \leq [L[C][k] : Z[C]]_i \leq [L[C][k] : Z]_i = [L[k][C] : L[k]]_i [L[k] : L]_i [L : Z] \leq smq$, where m is an integer such that $[L[a] : L]_i \leq m$ for all $a \in K$. We have proved therefore that K is left algebraic and of bounded degree over the field $Z[C](\supset C)$. Consequently, by Lemma 4, we obtain $[K : Z[C]]_i < \infty$. And so, we

9) \tilde{l} means the inner automorphism determined by $l : \tilde{l} = l_l l_r^{-1}$.

obtain our assertion $[K:L]_t \leq [K:Z]_t \leq [K:Z[C]]_t [Z[C]:Z] < \infty$ since $[Z[C]:Z] \leq [C:Z \cap C] = [C:L \cap C] = s < \infty$.

REFERENCES

- [1] N. JACOBSON : Structure of rings, Amer. Math. Soc. Colloq. Publ., 37 (1956).
- [2] _____ : Lecture in abstract algebra II. (1951).
- [3] F. KASCH : Über den endomorphismenring eines Vektorraumes und den Satz von der Normalbasis, Math. Ann., 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] _____ : Some remarks on Galois extensions of division rings, Math. J. Okayama Univ., 9 (1959), 5—8.
- [6] T. NAGAHARA : On generating elements of Galois extensions of division rings, Math. J. Okayama Univ., 6 (1957), 181—190.
- [7] _____ : On generating elements of Galois extensions of division rings III, Math. J. Okayama Univ., 7 (1957), 173—178.
- [8] _____ : On generating elements of Galois extensions of division rings IV, Math. J. Okayama Univ., 8 (1958), 181—188.
- [9] N. NOBUSAWA : A note on Galois extensions of division rings, Math. J. Okayama Univ., 7 (1957), 179—183.

DEPARTMENT OF MATHEMATICS,
OKAYAMA UNIVERSITY

(Received June 20, 1960)