ON PRIMITIVE ELEMENTS OF GALOIS EXTENSIONS OF DIVISION RINGS*

TAKASI NAGAHARA

It is a result of F. Kasch [3][1] that if a division ring K is Galois and finite over a division subring L and the center of $V_K(L)$, the *centralizer* of L in K, is separable over the center of K then $K=L(d, udu^{-1})$ with some d, u in K. In this note, under the same assumptions as above, we shall prove the following:

Principal Theorem. *Let D be an intermediate division subring of K/L and $\mathfrak{J}$ be the group of all L-inner automorphisms of K/L. If, for each element x of D, $\{x\}^{\mathfrak{J}}\backslash D$ is a finite set, then $D=L(d, udu^{-1})$ with some d, u in D where $\{x\}^{\mathfrak{J}}$ means the set of all images of x by $\mathfrak{J}$ and $\{x\}^{\mathfrak{J}}\backslash D$ the complement of $\{x\}^{\mathfrak{J}}$ in D.*

Clearly this theorem contains the result of F. Kasch as a special case. Further, our proof is completed without aid of Lagrange's interpolation formula used in the proof of F. Kasch.

§ 1. **Preliminaries.** Throughout this note, L will be a division ring, K be a division ring which is Galois and finite over L, and C be the center of K. If L is a finite ring then so is K, and hence, by the well-known Theorem of Wedderburn, our Principal Theorem is always true without special assumptions. Therefore, we shall assume in the sequel that L is an infinite division ring. For any division subring T of K, we denote by $\mathfrak{G}(K/T)$ the *total group* of K/T, that is, $\mathfrak{G}(K/T)$ is the group of all automorphisms of K which leave T element-wise invariant. Let now $V_K(L)$ be the *centralizer* of L in K. Then $V_K(V_K(L))=H$ is *normal* over L, the total group $\mathfrak{G}(H/L)$ of H/L is outer and the *total group* $\mathfrak{G}(K/H)$ of K/H is $\mathfrak{J}$, the group of all inner automorphisms of K/L. For any subset S of K, we consider the subring $L(S)$ of K, the minimal subring of K containing S and L. Clearly, $L(S)$ is a division subring of K.

---

*) The author wishes to express his best thanks to Prof. M. Moriya for his kind encouragement and advice.

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

Lemma 1. *Let S be an infinite subset of L and let a, b be elements of K. If, for $\mathfrak{H} = \bigcup_{x \in S} \mathfrak{G}(K/L(a+xb))$, $\{a\}^{\mathfrak{H}}$ and $\{b\}^{\mathfrak{H}}$ are finite, then there exists an element s in S such that $L(a, b) = L(a+sb)$.*

Proof. We denote by $\{a_1 = a, a_2, \ldots, a_r\}$ and $\{b_1 = b, b_2, \ldots, b_t\}$ all different elements of $\{a\}^{\mathfrak{H}}$ and $\{b\}^{\mathfrak{H}}$ respectively. Since S is infinite there exists an element $s \in S$ such that $a + sb \neq a_i + sb_j$ for all pairs $(i, j) \neq (1, 1)$. For each automorphism $\sigma \in \mathfrak{G}(K/L(a+sb))$, we have $a^\sigma + sb^\sigma = (a+sb)^\sigma = a + sb$, which means that $a^\sigma = a$ and $b^\sigma = b$. Since, by Galois theory (see [2], [3] or [5]), $L(a+sb)$ is the fixed subring of $\mathfrak{G}(K/L(a+sb))$ in K, both a and b must be contained in $L(a+sb)$, whence $L(a, b) = L(a+sb)$.

By induction, one will readily prove the next:

Corollary 1. *If $\{a_1, a_2, \ldots, a_n\}$ is a finite subset of K such that $\{a_i\}^{\mathfrak{G}(K/L)}$ $(i = 1, 2, \ldots, n)$ are finite, then there exists a finite subset $\{x_1, x_2, \ldots, x_n\}$ of L such that $L(a_1, a_2, \ldots, a_n) = L(\sum_{i=1}^{n} x_i a_i)$.*

The next result of N. Nobusawa ([6]) follows readily from the above corollary.

Corollary 2. *If $\mathfrak{G}(K/L)$ is locally finite*[1] *then any intermediate subring D possesses a single primitive element over L: $D = L(d)$ for some d in D.*

Since the *total group* $\mathfrak{G}(H/L)$ of $H = V_K(V_K(L))$ is outer, $\mathfrak{G}(H/L)$ is *locally finite*[2]. Hence we obtain by Corollary 2 the next:

Corollary 3. *Any intermediate division subring T of H possesses a single primitive element over L.*

Lemma 2. *Let R be a proper division subring of K containing C and $\{c_1, c_2, \ldots, c_n\}$ be a subset of C consisting of n different elements. If a is an element in R such that $ab \neq ba$ for some b in $K \backslash R$ then $\{(b+c_i)a(b+c_i)^{-1};\ i = 1, 2, \ldots; n\}$ is a subset of K consisting of n different elements and there exists at most one element c in C such that $(b+c)a(b+c)^{-1}$ is contained in R.*

Proof. If c_1, c_2 are different elements in C then $(b+c_1)a(b+c_1)^{-1} \neq (b+c_2)a(b+c_2)^{-1}$. For, if not, $(b+b_1)a(b+c_1)^{-1} = (b+c_2)a(b+c_2)^{-1}$

1) See [4, § 1].
2) See [4, Theorem 1].

$=a'$ imply that $(c_1-c_2)a=a'(c_1-c_2)$, whence $a=a'$. But $(b+c_1)a(b+c_1)^{-1}=a$ leads to a contradiction $ba=ab$. Now we suppose that $(b+c_1)a(b+c_1)^{-1}=a_1\in R$ and $(b+c_2)a(b+c_2)^{-1}=a_2\in R$. Then $ba-a_1b=a_1c_1-c_1a$, $ba-a_2b=a_2c_2-c_2a$, whence $(a_2-a_1)b=(a_1c_1-c_1a)-(a_2c_2-c_2a)$. Since $a_1\neq a_2$, we obtain the contradiction that $b=(a_2-a_1)^{-1}\{(a_1c_1-c_1a)-(a_2c_2-c_2a)\}\in R$.

§ 2. **Primitive elements of Galois extensions.** At first we shall state the following generalization of H. Cartan's theorem[1].

Lemma 3. *Let R, S be division subrings of a division ring K. If all inner automorphisms induced by non-zero elements of S leave R set-wise invariant, then $R\supset S$ or $R\subset V_K(S)$.*

Lemma 4. *Let $\mathfrak{G}(K/L)$ be not locally finite and D be an intermediate subring of K/L such that $D^{\mathfrak{J}}=D$. If the center Z of $V_K(L)$ is separable over C then $D=L(d, udu^{-1})$ with some d, u in D.*

Proof. By Galois theory, there holds that $[K:L]=[\mathfrak{G}(K/L):\mathfrak{J}][V_K(L):C]$. Clearly, each automorphism in $\mathfrak{J}$ is induced by some non-zero element of $V_K(L)$. Since $\mathfrak{G}(K/L)$ is not locally finite $\mathfrak{J}$ must be an infinite group, whence C is infinite by the relation $[V_K(L):C]\leqq[K:L]$. Further, K is non-commutative because $\mathfrak{J}$ is not the identity group.

By Lemma 3, either $D\subset V_K(V_K(L))=H$ or $D\supset V_K(L)$. In the first case, D has a single primitive element over L by Corollary 2 because H is Galois, finite over L, and $\mathfrak{G}(H/L)$ is locally finite. Hence we may, and shall, assume $D\not\subset H$ so that $D\supset V_K(L)$ $(=V_D(L))$ and D is non-commutative. Now we set $V_D(V_K(L))=V_D(V_D(L))=H_0$, $V_D(D)=C_0$, and denote by W a separable, maximal subfield of $V_K(L)$ over Z. Noting that $V_K(D)\subset V_K(L)\cap V_K(V_K(L))=V_{V_K(L)}(V_K(L))=Z$, we have $C\subset C_0\subset Z$. As Z is separable over C, so is W over C, whence $W=C(b)=C_0(b)$ with some b in W. Clearly $L\subset H_0\subset H$, and so, by Corollary 3, $H_0=L(a)$ for some $a\in H_0$. As is easily verified, $V_D(V_D(H_0))=H_0$, which means that D is Galois over H_0 and $\mathfrak{G}(D/H_0)$ is inner. We set here $M=L(a, b)=H_0(b)$. As $H_0\subset M\subset D$ and $W\subset V_D(M)\subset$

1) See [4, Lemma 2].

$V_D(L)\cap V_D(W)\subset V_K(L)\cap V_D(W)=V_{V_K(L)}(W)=W$, D is Galois, finite over M and $\mathfrak{G}(D/M)=\widetilde{W}$ by Galois theory, where $\widetilde{W}$ denote the group of inner automorphisms determined by all non-zero elements in W.

We shall prove next that $M=L(a, b)=L(a+lb)$ wifh some l in L. To show this, in virtue of Lemma 1, it suffices to show that $\{a\}^{\mathfrak{H}}$ and $\{b\}^{\mathfrak{H}}$ are finite, where $\mathfrak{H}=\bigcup_{x\in L/(0)}\mathfrak{G}(K/L(a+xb))$ $(\subset\mathfrak{G}(K/L))$. Since $a\in H$, $\{a\}^{\mathfrak{G}(K/L)}=\{a\}^{\mathfrak{G}(H/L)}$ is finite. If y is in $V_K(L(a+xb))$ then $y\in V_K(L)$ and $y(a+xb)=(a+xb)y$, whence $yb=by$, and so y belongs to the centralizer of W in $V_K(L)$, that is, $y\in W$. On the other hand, one can easily see that $W\subset V_K(L(a+xb))$, that is, $V_K(L(a+xb))=W$. For each $\sigma\in\mathfrak{G}(K/L(a+xb))$, and for any $y\in V_K(L(a+xb))=W$, we have $y(a^\sigma+xb^\sigma)=y(a+xb)^\sigma=y(a+xb)=(a+xb)y=(a^\sigma+xb^\sigma)y$. Since $a^\sigma\in H^\sigma=H$ and $y\in V_K(L(a+xb))=W\subset V_K(L)$, it follows that $yb^\sigma=b^\sigma y$ from the above equations, that is, $b^\sigma\in V_K(W)$. As σ leaves $V_K(L)$ setwise invariant, $b^\sigma\in W^\sigma\subset V_K(L)$ which shows $b^\sigma\in V_K(W)\cap V_K(L)=V_{V_K(L)}(W)=W$. Hence, $\{b\}^{\mathfrak{H}}\subset W$. Obviously, $\mathfrak{G}^*(K/L)$, the restriction of $\mathfrak{G}(K/L)$ on $V_K(L)$, has $V_L(L)$ as the fixed subring and $[V_K(L):V_L(L)]<\infty$[1].

Since $V_L(L)\subset Z\subset W$, b satisfies some equation $f(x)=0$ in $V_L(L)$. Therefore, for any $\sigma\in\mathfrak{H}$, we have $f(b^\sigma)=0$; this means that $\{b\}^{\mathfrak{H}}(\subset W)$ is a finite subset of K. Hence, there exists some $l\in L$ such that $M=L(d)$ for $d=a+lb$.

If $L\subset C_0$ then $d\notin C_0$, for $M=L(d)\subset C_0$ implies $W=V_D(M)\supset V_D(C_0)=D$ but this gives a contradiction because D is non-commutative. On the other hand, if $L\not\subset C_0$ and $d\in C_0$ then, for any $l'\in L\backslash C_0$, $l'd$ is also a primitive element of M/L. Therefore, without loss of generality, we may assume that $M=L(d)$ for some $d\notin C_0$.

Since W is finite and separable over C_0, there exists only a finite number of subfields $\{W_1, W_2, \dots, W_n\}$ of W which properly contains C_0. Then, as $W=V_D(M)$, all proper division subrings of D containing M are exhausted by $\{M_i=V_D(W_i);\ i=1, 2, \dots, n\}$. Let $\{t_1, t_2, \dots, t_n\}$ be chosen such as $t_i\in W_i\setminus C_0$. Then there exists a subset $\{f_i;\ i=0, 1, \dots, n\}$ of D such that $df_0d^{-1}\neq f_0$, and $t_if_it_i^{-1}\neq f_i$ $(i=1, 2, \dots, n)$ by Hilfsatz 1 of [3], there exists an element $f\in D$ so that $dfd^{-1}\neq f$ and $t_ift_i^{-1}\neq f$ $(i=1, 2, \dots, n)$. It is clear that $f\in D\backslash M_i$, $d\in M\subset M_i$ and $M_i\supset C_0$. Since C is infinite, by using Lemma 2 repeatedly, we can select an element $c\in C_0$ such that $d'=(f+c)d(f+c)^{-1}\notin M_i$ $(i=1, 2,$

1) See [4, Lemma 4].

$\dots, n$) Suppose that $L(d, d') \subsetneqq D$. Then $W = V_D(M) \supset V_D(M(d')) = V_D(L(d, d')) \supsetneqq C_0$, and so $V_D(L(d, d'))$ must coincide with some W_i $(1 \leqq i \leqq n)$. However, this shows that $M_i = V_D(W_i) \supset L(d, d') \ni d'$, being contrary to the property of d'. Therefore, $L(d, d') = D$, q. e. d.

§ 3. **Proof of Principal Theorem.** Combining Corollary 2 with Lemma 4, we can now prove our principal theorem. In case $\mathfrak{G}(K/L)$ is *locally finite*, by Corollary 2, $D = L(d)$ with some element $d \in D$, and all the restrictions in our theorem is superfluous. On the other hand, in case $\mathfrak{G}(K/L)$ is not locally finite, C is infinite. Suppose that $D^{\mathfrak{J}} \neq D$, then there exists an element $g \in D$ such that, for some $v \in V_K(L)$, $vgv^{-1} \notin D$. Since C is infinite, accordingly $C \cap D$ is infinite, by making use of the same method as in the proof of Lemma 2, we see that the set $\{(v + x)g(v + x)^{-1};\ x \in C \cap D\} \setminus D$ is infinite, which means that $\{g\}^{\mathfrak{J}} \setminus D$ is infinite. Therefore, there must hold $D^{\mathfrak{J}} = D$ and hence, $D = L(d, d')$ by Lemma 4, where $d' = udu^{-1}$ for some $u \in D$.

As an easy consequence of the principal theorem, we obtain the following:

Corollary 4. *Let K/L be Galois, $\mathfrak{G}(K/L)$ be locally finite-dimensional and locally compact*[1] *and the center of $V_K(L)$ be separable over C. If D is an intermediate subring of K finite over L such that, for each $x \in D$, the set $\{x\}^{\mathfrak{J}} \setminus D$ is finite, then $D = L(d, udu^{-1})$ with some d, u in D.*

Proof. In case $\mathfrak{G}(K/L)$ is *locally finite*, our assertion follows from Corollary 2. On the other hand, if $\mathfrak{G}(K/L)$ is *not locally finite*, then, by assumption, $[V_K(L) : V_L(L)] < \infty$ [4, Theorem 6]. Since $\mathfrak{G}(K/L)$ is locally finite-dimensional, there exists a subring K' of K which is normal, finite over L and contains $D(V_K(L))$. Clearly the center of K' contains C and $V_K(L) = V_{K'}(L)$, and so our assertion is a direct consequence of the principal theorem.

References

[1] R. Brauer: On a theorem of H. Cartan, Bull. Amer. Math. Soc., 55 (1949), 619—620.

[2] H. Cartan: Théorie de Galois pour les corps non commutatifs, Ann. Ecole Norm. Sup., 64 (1947), 59—77.

1) See [4, Theorem 6].

[3] F. KASCH: Über den Satz vom primitiven Element bei Schiefkörper, J. reine und angew. Math., 180 (1951), 150—159.
[4] T. NAGAHARA and H. TOMINAGA: On Galois theory of division rings, Math. J. Okayama Univ., 6 (1956) 1—22.
[5] N. NOBUSAWA: An extension of Krull's Galois theory to division rings, Osaka Math. J., 7 (1955), 1—6.
[6] N. NOBUSAWA: On compact Galois groups of division rings, Osaka Math. J., 8 (1956), 43—50.

DEPARTMENT OF MATHEMATICS,
OKAYAMA UNIVERSITY

(Received July 24, 1956)