ON GENERATING ELEMENTS OF SIMPLE ALGEBRAS

By Akira Inatomi

§ 1. Introduction.

Let K be a division ring which is a finite Galois extension of division subring L of K. Some years ago, Nagahara [10] proved the following theorem: K is a simple extension of L, if and only if L is not contained in the center of K or K is commutative.

Recently, by Nagahara-Tominaga [12], the theorem is extended to simple ring, in case the dimensionality of L over its center is infinite.

In this note, at first, we shall prove the following theorem: Let A be a finite-dimensional simple algebra over the center C and let B be a subring of A. If $B \frown C = P$ is a field and C is finite separable extension of P, then A is simple extension of B, if and only if B is not contained in C or A is commutative. In case A is division ring, this theorem has been proved by Nagahara. From the recent result of Nagahara-Tominaga and this theorem, we can see easily that the Nagahara's theorem is still valid for simple ring.

Finally we shall be concerned with generating elements of some intermediate simple ring between B and A.

These results correspond to some part of results of Nagahara in division ring.

§ 2. Preliminaries.

In this section, we make preparations for the theorem which will be proved in the next section. Here, we shall prove the following theorem:

Theorem 1. *Let A be a finite-dimensional simple algebra over the center C which is not a division algebra. We suppose that C is an infinite field. Let R be a proper subring of A which is not contained in C. If $R \frown C = P$ is a field and C is a separable and finite extension of P then there exists a nilpotent element b of A such that $(1+bx)r(1+bx)^{-1}$ (or $(1+bx)^{-1}r(1+bx)) \notin R$ for some element r of R, and for an infinite number of elements, x's of P.*

Lemma 1. *Let A be an algebra with a unit element over an infinite field P (dimensionality over P is finite or infinite). Let R be a P-submodule of A. If there exists a nilpotent element b ($b^s = 0$) such that brb^{s-1} (or $b^{s-1}rb) \notin R$ for some element r in A then there exist at most s elements x's of P with $(1+bx)r(1+bx)^{-1}$ (or $(1+bx)^{-1}r(1+bx)) \in R$.*

Received May 20, 1962.

Proof. Let us take b as above, then

$$(1+b)r(1+b)^{-1}=(1+b)r(1-b+b^2-\cdots+(-1)^{s-1}b^{s-1})$$

and hence this can be represented in the form

$$u_0+u_1+\cdots+u_s,$$

where $u_0=r$, $u_s=(-1)^{s-1}brb^{s-1}$ and $u_i=(-1)^i(rb^i-brb^{i-1})$ for $1\leqq i\leqq s-1$. Therefore

$$(1+bx)r(1+bx)^{-1}=u_0+u_1x+\cdots+u_sx^s$$

for every $x\in P$. Let $x_0,x_1,\cdots,x_s$, be different elements of P. Suppose that $(1+bx_i)r(1+bx_i)^{-1}=t_i\in R$ for $i=0,\cdots,s$. Since, in the system of linear equations

$$u_0+u_1x_i+\cdots+u_sx_i^s=t_i$$

for $i=0,\cdots,s$, $|1,x_i,x_i^2,\cdots,x_i^s|\neq 0$,[1] u_s is represented in the linear form

$$\alpha_0t_0+\alpha_1t_2+\cdots+\alpha_st_s,$$

where $\alpha_i\in P$ for $i=0,\cdots,s$. This shows that brb^{s-1} belongs to R. Similarly for $b^{s-1}rb$.

In the rest of this section, A will denote a finite-dimensional simple algebra over a field P which is not a division algebra. Hence A is represented in the form $\sum_{i,j=1}^n De_{i,j}$ $(n>1)$ with matric units $e_{i,j}$'s and a division algebra $D=V_A(\{e_{i,j}\})$.[2] Let C be the center of A. Then we may suppose that $C\supseteq P$.

LEMMA 2. *We suppose that D is non-commutative. Let $r=\sum_{i,j=1}^n r_{i,j}e_{i,j}$, where $r_{i,j}\in D$, $r_{1,2}\neq 0$ and $r_{2,1}=1$, and let R be the subring of A which is generated, over P, by the element r and the set of all elements in the forms brb^{s-1} and $b^{s-1}rb$, where b is a nilpotent element of A and $b^s=0$. Then $R=A$.*

Proof. We obtain $R\ni\delta^2e_{1,2}$ for every $\delta\in D$, because $(\delta e_{1,2})^2=0$ and $\delta^2e_{1,2}=(\delta e_{1,2})r(\delta e_{1,2})$. Similarly, $R\ni r_{1,2}e_{2,1}$ and $r_{1,2}^{-1}e_{2,1}$. Now $\delta^2e_{1,1}=(\delta^2e_{1,2})\,(r_{1,2}e_{2,1})e_{1,2}\cdot(r_{1,2}^{-1}e_{2,1})$. Hence $\delta^2e_{1,1}\in R$. Since D is a non-commutative division algebra over P, it is generated, over P, by the set of all elements in the form δ^2, where $\delta\in D$.[3] Hence $R\ni d_{1,1}e_{1,1}$, for every $d_{1,1}\in D$. Next let

$$b=e_{1,2}+e_{2,3}+\cdots+e_{k-1,k},$$

where $2\leqq k\leqq n$, then $b^k=0$, $b^{k-1}=e_{1,k}$ and hence $bre_{1,k}=brb^{k-1}\in R$. We have $e_{1,k}=e_{1,2}re_{1,k}=e_{1,1}brb^{k-1}$ and therefore $e_{1,k}\in R$. Let

$$b'=e_{2,1}+e_{3,2}+\cdots+e_{k,k-1},$$

[1] $|1,x_i,x_i^2,\cdots,x_i^s|$ denotes the Vandermonde's determinant. Since $x_0,x_1,\cdots,x_s$ are different, we can see easily that this is not zero.

[2] Let B be a subset of a ring A, then $V_A(B)$ denote the commutator of B in A.

[3] $(D:P)<\infty$, so an intermediate ring between P and D is a division ring. See Hua [4] and Kaplansky [6].

where $2 \leqq k \leqq n$, then $b'^{k} = 0$, $b'^{k-1} = e_{k,1}$ and hence $b'^{k-1} r b' (r_{1,2}^{-1} e_{1,1}) = e_{k,1} r e_{2,1} r_{1,2}^{-1} = e_{k,1} \in R$. Then $d_{i,j} e_{i,j} = e_{i,1} (d_{i,j} e_{1,1}) e_{1,j}$ for every $d_{i,j} \in D$, and therefore $d_{i,j} e_{i,j} \in R$. Thus $R = A$.

Lemma 2′. *We suppose that C is separable over P. Let us take R such as in the lemma 2. Then $R = A$, even if D is commutative.*

Proof. If z^2 belongs to P for every element z of C, the irreducible equation of y over P, where $y \notin P$, is $f(x) = x^2 - \alpha = 0$, where $\alpha \in P$. From the assumption for C, $f(x)$ has the other root y' which is different from y and $y' = -y$. And $(1+y)^2$ is mapped to $(1-y)^2$ by a suitable isomorphism leaving P elementwise fixed. Since $(1+y)^2 \in P$, $(1+y)^2 = (1-y)^2$. Therefore $y = y'$. From this contradiction, it must hold that $P(\delta^2) \nsubseteq P$ for some $\delta \in C$. Since $(C : P) < \infty$, it follows that C is generated, over P, by the set of all δ^2's, where $\delta \in C$.[4] Noting the above fact, we can prove this lemma by the same way as in lemma 2.

Lemma 3. *We suppose that a field P is infinite. Let R be a proper subring of A which contains P and an element, $r = \sum_{i,j=1}^{n} r_{i,j} e_{i,j}$, where $r_{2,1} = 1$ and $r_{1,2} \neq 0$. If D is non-commutative, or C is separable over P then there exists a nilpotent element b of A such that $(bx+1) r (bx+1)^{-1}$ (or $(bx+1)^{-1} r (bx+1)) \notin R$ for an infinite number of elements x's of P.*

Proof. Since R is a proper subring of A, from lemma 2 and lemma 2′, brb^{s-1} (or $b^{s-1} r b) \notin R$ for some nilpotent element b ($b^s = 0$). On the other hand, R is a P-submodule of A, so, from lemma 1, $(bx+1) r (bx+1)^{-1}$ (or $(bx+1)^{-1} r \cdot (bx+1)) \notin R$ for an infinite number of elements x's of P.

Remark. In lemma 2 and 2′, we supposed that $(A : P) < \infty$ and either D or C has some condition. But, in case $n > 2$, these assumptions are superfluous. Indeed, if we choose an element, $b = e_{1,2} + \delta e_{2,3}$, where $\delta \in D$, then $b^2 = \delta e_{1,3}$, $b^3 = 0$ and hence $\delta e_{1,3} = e_{1,2} r (\delta e_{1,3}) = e_{1,1} b r b^2$. Hence $\delta e_{1,3}$ belongs to R. Similarly, using an element $b' = e_{2,1} + r_{1,2}^{-1} e_{3,2}$, $e_{3,1} \in R$. We have $\delta e_{1,1} = (\delta e_{1,3}) e_{3,1}$ and hence $\delta e_{1,1} \in R$. The rest of the proof is analogous to that of lemma 2.

Therefore, if $n > 2$ and P is an infinite field, the same assumptions as above are superfluous in lemma 3, too.

Again, we suppose that a field P is infinite. Let $a = \sum_{i,j=1}^{n} a_{i,j} e_{i,j}$ be a regular element of A.

If $a_{i_0, j_0} \neq 0$, where $i_0 \neq j_0$, then let

$$d = \Big(\sum_{\substack{i=1 \\ i \neq 2}}^{n} e_{i,i} + a_{i_0,j_0}^{-1} e_{2,2} \Big) \Big(\sum_{\substack{i=1 \\ i \neq 2, i_0}}^{n} e_{i,i} + e_{2,i_0} + e_{i_0,2} \Big) \Big(\sum_{\substack{i=2 \\ i \neq j_0}}^{n} e_{i,i} + e_{1,j_0} + e_{j_0,1} \Big),$$

and we have $a_1 = dad^{-1} = \sum_{i,j=1}^{n} a_{1,i,j} e_{i,j}$, where $a_{1,2,1} = 1$. If $a_{1,1,2} = 0$, then let $d_1 = 1 + \alpha e_{1,2}$, where $P \ni \alpha \neq 0$, and $a_{1,1,1} - a_{1,2,2} \neq \alpha$, and we have $a_2 = d_1^{-1} a_1 d$

[4] Cf. lemma in Kaplansky [6].

$=\sum_{i,j=1}^{n} a_{2,i,j}e_{i,j}$, where $a_{2,2,1}=1$ and $a_{2,1,2}\neq 0$.

Next, we consider the case $a_{i,j}=0$ for all $i\neq j$; that is, $a=\sum_{i=1}^{n} a_{i,i}e_{i,i}$. If $a_{1,1}\neq a_{2,2}$, then let $f=1+e_{2,1}$ and we have $faf^{-1}=\sum_{i,j=1}^{n} a'_{i,j}e_{i,j}$, where $a'_{2,1}\neq 0$. If $a_{i,i}=\delta$ for all $i=1,\cdots,n$ and $\delta\notin C$, then let $g=\sum_{i=1,i\neq 2}^{n} e_{i,i}+\rho e_{2,2}$, where $\rho\in D$ and $\rho\delta\neq\delta\rho$, and we have $gag^{-1}=\sum_{i,j=1}^{n} a''_{i,j}e_{i,j}$, where $a''_{1,1}\neq a''_{2,2}$.

In short, if a is a regular element of A which is not contained in C, we can transform it to the form $r=\sum_{i,j=1}^{n} r_{i,j}e_{i,j}$, where $r_{2,1}=1$ and $r_{1,2}\neq 0$, by a suitable inner automorphism of A.

Generally, we say that two elements (or two sets) of a ring are conjugate with each other, if the one is transformed to the other by a suitable inner automorphism.

Proof of theorem 1. Since P is an infinite field and $(R:P)<\infty$, R is gererated by regular elements of R.[5] We can choose a regular element r which is not contained in C, for R is not contained in C. Hence, from lemma 3 and the above remark, we can see easily that this theorem holds for the suitable conjugate ring R' to R. Thus the theorem holds for R.

REMARK. This theorem is a specialization of a theorem of Kasch.[6]

§ 3. Generating element of a simple algebra.

Throughout this section, let A be a simple algebra which has finite dimensionality over the center C. We shall use the same notation as in § 2. Let $l^2=(D:C)$ and let $t=ln$, where $(A:D)=n^2$.

The main theorem of this section is the following:

THEOREM 2. *Let B be a subring of A such that $B\frown C=P$ is a field, and C is a seperable and finite extension of P. Then A is generated by some regular element* $\mathfrak{b}$ *of A over B, if and only if B is not contained in C or A is commutative.*

Nagahara has proved this theorem in case A is a division algebra,[7] so we may suppose that $n>1$.

1. In case C is an infinite field.

Let $m=(C:P)$ and let K be a maximal subfield of D which is separable over C. Since C is separable and finite over P, $K=P(\theta)$ with some θ of K. Now, let

$$\omega=e_{1,1}\theta+e_{2,2}(\theta+c_2)+\cdots+e_{n,n}(\theta+c_n),$$

where c_i is such an element of P that is decided as $f_j(\theta+c_i)\neq 0$ for $1\leqq j<i$, if $f_1(x)=0$ and $f_i(x)=0$, for $i=2,\cdots,n$, are the irreducible equations of θ and

[5] See Bialynicki-Birula [1] and Shôda [14].

[6] See "Satz 3" in Kasch [7].

[7] See proposition 1 in Nagahara [11].

$\theta + c_i$, over P, respectively. Let

$$W = e_{1,1}K \oplus \cdots \oplus e_{n,n}K,$$

then clearly $P(\omega) \subseteq W$. On the other hand, we have

$$f_1(\omega)f_2(\omega)\cdots f_l(\omega) = e_{l+1,l+1}\alpha_{l,l+1,l+1} + \cdots + e_{n,n}\alpha_{l,n,n},$$

where $\alpha_{l,j,j} \neq 0$ and $\in K$ for all $j = l+1, \cdots, n$, in particular, $f_1(\omega)\cdots f_{n-1}(\omega) = e_{n,n}\alpha_{n-1,n,n}$. Therefore $P(\omega) \supseteq Ke_{i,i}$. Then we have $P(\omega) = W$.

Since P is an infinite field, B has a regular element r which is not contained in C. Let S be the set whose elements are conjugate to r. Then we can choose such an element $r' = drd^{-1}$ from S that $(W(r'):P)$ is as great as possible. If $W(r') = R \neq A$, then, from theorem 1, there exists a nilpotent element b such that $r'_x = (1+xb)r'(1+xb)^{-1}$ (or $(1+xb)^{-1}r'(1+xb)) \notin R$ for an infinite number of elements, x's of P.

Let Ω be a splitting field of A over P which contains a Galois extension of $P(\theta)$, then we have

$$A \underset{P}{\times} \Omega \simeq f_1\Omega_t \oplus \cdots \oplus f_m\Omega_t,$$

where Ω_t is $t \times t$ full matrix ring over Ω and

$$f_i f_j = \begin{cases} f_i & (i = j), \\ 0 & (i \neq j). \end{cases}$$

Let $e^k_{i,j}$ be a matric unit of $f_k\Omega_t$, where $1 \leqq k \leqq m$ and $1 \leqq i, j \leqq t$. In this representation, we have $W \times_P \Omega = \sum_{i=1}^{t}\sum_{j=1}^{m} \oplus g_{i,j}\Omega$, where $g_{i,j} \in f_j\Omega$ and

$$g_{i,j}g_{i',j'} = \begin{cases} 0, & i \neq i' \text{ or } j \neq j', \\ g_{i,j}, & i = i' \text{ and } j = j', \end{cases}$$

therefore, if A' is the suitable ring conjugate to A in $A \times_P \Omega$, then $W' \times_P \Omega = \sum_{i=1}^{t}\sum_{k=1}^{m} \oplus e^k_{i,i}\Omega$. Hence, we may suppose that $W \times_P \Omega = \sum_{i=1}^{t}\sum_{k=1}^{m} \oplus e^k_{i,i}\Omega$.

When we use the same notation as lemma 1, we have

$$r'_x = u_0 + u_1x + \cdots + u_sx^s,$$

where $b^s = 0$. Let $r'^k_{x,i,j}$ be a matric component of r'_x in $A \times_P \Omega$, then

$$r'^k_{x,i,j} = u^k_{0,i,j} + u^k_{x,i,j}x + \cdots + u^k_{s,i,j}x^s.$$

When $u^k_{0,i,j} \neq 0$, there exists at most a finite number of elements x's in P such that $r'^k_{x,i,j} = 0$. Therefore we can choose such an element x_0 in P that $r'^k_{x_0,i,j} \neq 0$, if $u^k_{0,i,j} \neq 0$, and that $r'_{x_0} \notin R \times_P \Omega$. We can see easily that $W(r'_{x_0}) \times_P \Omega$ contains r', so

$$(W(r'_{x_0}) \times \Omega : \Omega) > (W(r') \times_P \Omega : \Omega).$$

Hence

$$(W(r'_{x_0}) : P) > (W(r') : P).$$

Since $r'_{x_0} \in S$, being contrary to the maximality of $(W(r'):P)$, $W(r') = A$; that is, $A = P(\omega, drd^{-1})$ and hence we have $A = d^{-1}Ad = d^{-1}P(\omega, drd^{-1})d = P(d^{-1}\omega d, r)$. Let $\mathfrak{d} = d^{-1}\omega d$, then we have $P(r, \mathfrak{d}) = P(r)(\mathfrak{d}) \subseteq B(\mathfrak{d}) \subseteq A = P(r, \mathfrak{d})$. Thus $B(\mathfrak{d}) = A$.

REMARK. If C has an infinite field and a separable finite extension of P, A is generated by two conjugate regular elements over P. For, if we set $B=W$, $A=P(\omega, d^{-1}\omega d)$.[8]

2. In case C is a finite field.[9]

Since C is a finite field, $A=C_n$. We may consider only the case where $n>1$.

First, we suppose that B has a nilpotent element, so B has a nilpotent element b such that $b^2=0$. Let $\mathfrak{M}$ be a left representation module of A with respect to C and let $\mathfrak{M}_2=\{x \mid bx=0 : x\in\mathfrak{M}\}$, then $\mathfrak{M}=\mathfrak{M}_1+\mathfrak{M}_2$. Since $b\mathfrak{M}=b\mathfrak{M}_1 \subseteq \mathfrak{M}_2$, $\mathfrak{M}=\mathfrak{M}_1+\mathfrak{M}_2'+b\mathfrak{M}_1$, where $\mathfrak{M}_2'+b\mathfrak{M}_1=\mathfrak{M}_2$. Hence, relative to a suitable basis, we obtain the following representation of b:

$$b=e_{s,1}+e_{s+1,2}+\cdots+e_{n,n+1-s},$$

where $n\geqq s>[n+1/2]$.

Let F be a subring of A represented in the form $C(e_{1,1}+\cdots+e_{i,i})\oplus C(e_{i+1,i+1}+\cdots+e_{k,k})\oplus\cdots\oplus C(e_{l,l}+\cdots+e_{n,n})$, where $1\leqq i\leqq n-1$. Let

$$\omega=e_{2,1}+e_{3,2}+\cdots+e_{n,n-1}+\alpha e_{1,n},$$

where $0\neq\alpha\in C$. Then $A=F(\omega)$, because, $F\supseteq C$ and $F(\omega)\ni\alpha e_{1,n}=(e_{1,1}+\cdots+e_{i,i})\omega(e_{l,l}+\cdots+e_{n,n})$, so $F(\omega)\ni u=e_{1,2}+e_{2,3}+\cdots+e_{n-1,n}$, $v=e_{2,1}+e_{3,2}+\cdots+e_{n,n-1}$.[10] Now, since C is a separable finite extension of P, let us put a primitive element of C over P in α. Then $P(\omega)\supseteq C$. Let $R=P(b,\omega)$, then $R\ni e_{1,1}+e_{2,2}+\cdots+e_{n-s+1,n-s+1}=\alpha^{-1}\omega^{n-s+1}b$, where $1\leqq n-s+1<n$, and hence $R\supset F$. Therefore, $R=A$. Thus $A=B(\omega)$.

If BC has a nilpotent element, choosing the same element ω as above, $B(\omega)\supset BC$. Hence $B(\omega)=A$.

If BC has no nilpotent element, BC is a direct sum of commutative fields. Moreover, if BC is not a field, we may suppose that $BC=F$. On the other hand, we have $B(\omega)\supset BC$. Hence $B(\omega)=A$.

If BC is a field, let us take a element r of B which is not contained in C. Let $k=(C(r):C)$ and let $q=n/k$. Then r is represented by a suitable basis in the following form:[11]

$$M\times E_q, \text{ where } M=\begin{bmatrix} 0 & & \alpha_1 \\ 1 & & \alpha_2 \\ & \ddots & \vdots \\ & 1 & \alpha_k \end{bmatrix} \quad (\alpha_i\in C).$$

When $q=1$, let $\omega'=1+\alpha e_{1,n}$, where $C=P(\alpha)$, and let $R=P(r,\omega')$. Then $R\ni e_{s+1,n}=r^s\alpha e_{1,n}$ for $1\leqq s\leqq n-1$, so $R\ni\delta e_{n,n}$, where $\delta\in C$, and hence $R\ni\omega$, where ω is the same element as above. Hence $R\supset C$ and $R\ni u,v$. Therefore

[8] This fact holds, even if C is a finite field. These are proved by Kasch-Tominaga [8].

[9] Here, we shall identify B with B' which is conjugate to B.

[10] We see in Kasch-Tominaga [8] that $e_{i,j}=v^{i-1}u^{n-1}v^{n-1}u^{j-1}$.

[11] See Jacobson [5].

$R=A$. Thus $B(\omega')=A$. When $q>1$, we choose the following element:[12]

$$\omega' = \begin{bmatrix} NE & & 0 \\ & \ddots & \\ 0 & & E \\ E & & \end{bmatrix}, \text{ where } N = \left.\begin{bmatrix} & \alpha \\ 0 & \end{bmatrix}\right\} k.$$

Then $P(r,\omega)=A$.

Clearly, ω and ω' used above are regular elements.

The converse part of this theorem is trivial. Thus, theorem 2 is proved completely.

REMARK. In 2, it is not essential that C is a finite field; that is, if $A=C_n$, we can take a generating element such as in 2.

COROLLARY. *Let B be a subring of A such that $B \frown C=P$ is a field and $(C:P)<\infty$, and let T be an intermediate simple subring between B and A. If the characteristic of C is zero, then $T=B(\mathfrak{b})$ with some regular element $\mathfrak{b}$, if and anly if $B \not\subseteq V_T(T)$ or T is commutative*; *cf. Nagahara* [11].

Proof. Clearly, $V_T(T) \supseteq P$ and $(V_T(T):P)<\infty$. Since the characteristic of C is zero, $V_T(T)$ is a separable extension over P, and hence, if $B \not\subseteq V_T(T)$, $T=B(\mathfrak{b})$ with some regular element $\mathfrak{b}$, from theorem 2. The converse part will be trivial.

§ 4. Application to Galois extension.

Throughout this section, by a simple ring we shall mean a two-sided simple ring with a unit element which satisfy minimum condition for left ideals.

A simple ring A is called a finite Galois extension of a simple subring B, if $(A:B)_l<\infty$, B is a ring fixed by a group of automorphisms of A and $V_A(B)$ is a simple ring. Then the group $\mathfrak{G}$ of all the automorphisms which leave all the elements of B fixed is called a Galois group of A with respect to B. Let $\mathfrak{J}$ be the group which consists of all the inner automorphisms contained in $\mathfrak{G}$ and let $R(\mathfrak{G})$ be a ring which is generated by all the regular elements inducing $\mathfrak{J}$. Then $R(\mathfrak{G})=V_A(B)$. Conversely, $\mathfrak{J}$ has the inner automorphism of A which is induced by a regular element in $V_A(B)$; that is, $\mathfrak{G}$ is complete. And $(A:B)=(\mathfrak{G}:\mathfrak{J})(R(\mathfrak{G}):C)$, where C is the center of A; so $\mathfrak{G}/\mathfrak{J}$ is a finite group. Let $P=B \frown C$. Then P is elementwise fixed by $\mathfrak{G}/\mathfrak{J}$ in C, so $(V_A(B):P)<\infty$.[13]

If A is a finite dimensional algebra over C which is a finite Galois extension over B, we have

$$B \underset{P}{\times} C \simeq BC = V_A(V_A(B)) \text{ and the center of } BC = ZC \simeq Z \underset{P}{\times} C,$$[14]

[12] The suggestion of this generating element is due to M. Okuzumi.

[13] See Nakayama [13] and Tominaga [16].

[14] See Hochschild [3].

where Z is a center of B. Clearly, $(A:P)<\infty$, C and ZC are finite Galois extensions over P and Z, respectively.

In this section, we are concerned with a finite Galois extension, so a simple ring A will be a finite Galois extension over a simple subring B, and the other notations will be used as in the explanation above.

By Kasch and Tominaga [8], it is proved that A is generated by two conjugate regular elements over B. Moreover, the following theorem is proved in the recent paper of Nagahara and Tominaga [12]:

THEOREM (*Nagahara and Tominaga*). *Let T be a intermediate subring between B and A. If $(B:Z)=\infty$, then $T=B(\mathfrak{d})$ with some element $\mathfrak{d}$ of T, in particular, $A=B(\mathfrak{d})$.*

If $(B:Z)<\infty$, A is a finite dimensional algebra over C.[15] Hence the following two theorems hold, from theorem 2, corollary and the above theorem.

THEOREM 3. *$A=B(\mathfrak{d})$ with some element $\mathfrak{d}$ in A, if and only if $B\nsubseteq C$ or A is commutative.*

THEOREM 4. *Let T be a intermediate simple subring between B and A. If the characteristic of C is zero, $T=B(\mathfrak{d})$ with some element $\mathfrak{d}$ of T, if and only of $B\nsubseteq V_T(T)$ or T is commutative*; *cf. Nagahara* [11].

Let U be ring and let $\mathfrak{h}$ be a group of automorphisms of U. A subring T of U is called $\mathfrak{h}$-normal, if T is fixed setwise by $\mathfrak{h}$.

We shall prove the following lemma:

LEMMA 4. *Let U be a ring with a unit element, and let both B and S be simple ring whose unit elements are the unit element of U. Let $S=\sum_{i,j=1}^{n} De_{i,j}$. We suppose that D is neither a prime field P_2 with characteristic 2 nor $n=2$. If B is fixed setwise by all the inner automorphisms induced by regular elements of S, then either $B\subseteq V_U(S)$ or $B\supseteq S$.*[16]

Proof. In case $n=1$; that is, $S=D$, the above is proved by Nagahara-Tominaga [12], so we are concerned with only the case $n\geqq 2$. Then, clearly, either $B\subseteq V_U(D)$ or $B\supseteq D$.

In case $B\subseteq V_U(D)$. Let $\theta_1=1+\sum_{i=1}^{n-1} e_{i,i+1}$ and $\theta_2=1+\sum_{i=1}^{n-1} e_{i+1,i}$, then clearly $\theta_i\,(i=1,2)$ is a regular element. When $D\neq P_2$, we can take an element k of D such that θ_i+k, for $i=1,2$, is a regular element. Hence, for every a of B, $a\theta_i=\theta_i a_{i,1}$, and $a(\theta_i+k)=(\theta_i+k)a_{i,2}$, where $B\ni a_{i,1}$, $a_{i,2}$, and hence $k(a-a_{i,2})=\theta_i(a_{i,2}-a_{i,1})$. If $a_{i,1}=a_{i,2}$, then θ_i is commutative with a. On the other hand, if $a_{i,2}-a_{i,1}\neq 0$, the two sided ideal $B(a_{i,2}-a_{i,1})B$ coincides with B

[15] See lemma in Tominaga [15].

[16] Cf. theorem 5 in Bialynicki-Birula [1].

and hence $1=\sum_j x_j(a_{i,2}-a_{i,1})y_j$, where $B\ni x_j, y_j$. Hence we have $\sum_j(k^{-1}\theta_i)\cdot x_j(k^{-1}\theta_i)^{-1}(a-a_{i,2})y_j=\sum_j(k^{-1}\theta_i)x_j(a_{i,2}-a_{i,1})y_j=k^{-1}\theta_i$.17) In this relation, the left side is contained in B and so $k^{-1}\theta_i\in B$. Since $k^{-1}\theta_i$ is not contained in the center of $S, B\frown S$ has an element which which is not contained in the center of S and hence $B\supseteq S$.18) If both θ_i's are commutative with every a in B, then $B\subseteq V_U(D(\theta_1,\theta_2))=V_U(S)$. When $D=P_2$ and $n>2$, then we take the two regular elements $\theta=\sum_{i=1}^{n-1}e_{i,i+1}+e_{n,1}+e_{n,2}$, $\theta'=\sum_{i=1}^{n-1}e_{i,i+1}+e_{n,1}$, then $\theta+1=\omega$ and $\theta'+\omega$ are regular elements and $D(\theta,\theta')=S$. By the same way as above, either $\theta\in B$ or θ is commutative with B. If $\theta\in B$, $B\supseteq S$. If θ is commutative with B, then ω is so also. Then we take θ' and ω, respectively, instead of θ_i and k. If $\omega^{-1}\theta'\in B$ then $B\supseteq S$, and if θ' is commutative with B, then $B\subseteq V_U(D(\theta,\theta'))=V_U(S)$.

In case $B\supseteq D$. First, we suppose that the characteristic p of D is not 2. Then, since θ_i+1 is a regular element, so $B\supseteq S$ or both θ_i's are commutative with B. In the latter, we take an element d of D which is not contained in the center of B, then θ_i+d is a regular element, so, for som element d of B, $a\theta_i=\theta_i a$ and $a(\theta_i+d)=(\theta_i+d)a_i$, where $a_i\in B$ and $a\neq a_i$. Hence $ad-da_i=\theta_i(a_i-a)$. Since the left sided element belongs to B, $\theta_i\in B$ and hence $B\supseteq S$. Finally, we shall consider the case $D\neq P_2$ and $p=2$. If $n>3$, we can see easily that $B\supseteq S$ or both θ and θ' are commutative with B. Since $P_2(\theta,\theta')\ni\theta_i\,(i=1,2)$, also $B\supseteq S$. If $n=2$, we set $\theta=e_{2,1}+e_{1,2}+ke_{2,2}$, where $k\in D$ and $\neq 1$, $\theta'=e_{2,1}+e_{1,2}$ and the same proof as above holds.

Remark. If $D=P_2$ and $n=2$, generally this lemma is not true from the Kasch's example [7]; that is, the subring of S which is generated by the element $e_{1,2}+e_{2,1}+e_{2,2}$ is not contained in the center of S, but it is S-invariant.

In the following theorems, we may suppose that A is finite dimensional algebra over the center C and C is an infinite field. Indeed, if $(A:C)=\infty$ then from the result of Nagahara and Tominaga, these hold, even if T is arbitrary ring. If $(A:C)<\infty$ and C is a finite field, then A is a finite ring. Hence these hold, from the same reason such as corollary in §3 or from the result of Kasch and Tominaga [8], even if A is neither a Galois extension of B nor T is $\mathfrak{Z}$-normal.

Theorem 5. *Let T be an $\mathfrak{Z}$-normal simple subring of A containing B, then $T=B(\mathfrak{d},d^{-1}\mathfrak{d}d)$ with some elements $\mathfrak{d}$ and d of T.*

Proof. From lemma 4[19] either $T\subseteq V_A(V_A(B))=BC$ or $T\supseteq V_A(B)$. If $T\subseteq BC$, the center Z' of T contains Z and is contained in ZC. Since ZC is separable over Z, Z' is so over Z. Hence, from theorem 2, $T=B(\mathfrak{d})$ with some

17) Cf. proof of theorem in Brauer [2].

18) See "Satz 3" in Kasch [7].

19) Lemma 4 is generalization of a theorem of Birula, but we can use Birula's result for the proof of this theorem.

regular element $\mathfrak{d}$ of T. In the latter case, we represent T in the form $\sum_{i,j=1}^{n} D_2 e_{ij}$. Let $A' = V_A(\{e_{i,j}\})$ and we set $B' = B(\{e_{i,j}\}) = \sum_{i,j=1}^{n} D_1 e_{i,j}$, where $D_1 = V_{B'}(\{e_{i,j}\})$ is a division ring and, clearly, $D_2 \supseteq D_1$. We can see easily that A' is a finite Galois extension of D_1 and $D_2 \supseteq V_{A'}(D_1)$. Hence $D_2 = D_1(x, y)$ with some conjugate regular element x, y[20] and therefore $T = B(\mathfrak{d}, d^{-1}\mathfrak{d}d)$, where $\mathfrak{d}$ is a regular element.[21]

THEOREM 6. *Let T be an $\mathfrak{J}$-normal simple subring of A containing B. If B is not a division ring then $T = B(\mathfrak{d})$.*

Proof. We may suppose that $T \supseteq V_A(B)$. Clearly, the center Z' of T is contained in $V_A(B) \frown BC = ZC$. Let $K = BC$ and $B = \sum_{i,j} D' f_{i,j}$, We set $K' = V_K(\{f_{i,j}\})$ and $T' = V_T(\{f_{i,j}\})$, then both K' and T' are simple rings and $T' \supseteq K' \supseteq D'$. Clearly $K' = D'(x)$ and $T' = K'(y)$, so $T' = D'(x, y)$, where x and y are regular elements. Let $\mathfrak{d} = x + f_{1,2}y$, then $\mathfrak{d}$ is a regular element and $T = B(\mathfrak{d})$.

REMARK. In case A is a division ring. If B is non-commutative and T is $\mathfrak{J}$-normal division ring which contain B, $T = B(\mathfrak{d})$; see Nagahara [10].

REFERENCES

[1] BIALYNICKI-BIRULA, A., On automorphisms and derivations of simple rings with minimum condition. Trans. Amer. Math. Soc. 98 (1961), 468–484.

[2] BRAUER, R., On a theorem of H. Cartan. Bull. Amer. Math. Soc. 55 (1949), 619–620.

[3] HOCHSCHILD, G. P., Automorphisms of simple algebras. Trans. Amer. Math. Soc. 69 (1950), 292–301.

[4] HUA, L. K., Some properties of a sfield. Proc. Nat. Acad. USA. 35 (1949), 533–537.

[5] JACOBSON, N., Lectures in abstract algebra, II. New York (1953).

[6] KAPLANSKY, I., A theorem on division rings. Canad. J. Math. 3 (1951), 290–292.

[7] KASCH, F., Invariante Untermoduln des Endomorphismenrings eines Vektorraums. Arch. Math. 4 (1953), 182–190.

[8] KASCH, F., AND H. TOMINAGA, On generating elements of simple rings. Proc. Japan Acad. 33 (1957), 187–189.

[9] NAGAHARA, T., On generating elements of Galois extensions of division rings. Math. J. Okayama Univ. 6 (1957), 181–190.

[10] NAGAHARA, T., On generating elements of Galois extensions of division rings, III. Math. J. Okayama Univ. 7 (1957), 173–178.

[11] NAGAHARA, T., On generating elements of Galois extension of division rings, IV. Math. J. Okayama Univ. 8 (1958), 181–188.

[12] NAGAHARA, T., AND H. TOMINAGA. On Galois and locally Galois extensions of simple rings. Math. J. Okayama Univ. 10 (1961), 143–166.

[20] We can prove by the same way as in lemma 8 in Nagahara [9].

[21] See the fundamental theorem in Kasch-Tominaga [8].

[13] NAKAYAMA, T. Galois theory of simple rings. Trans. Amer. Math. Soc. **73** (1953), 276-292.

[14] SHÔDA, K., Über die Galoissche Theorie der halbeinfachen hyperkomplexen Systeme. Math. Ann. **107** (1933), 252-258.

[15] TOMINAGA, H., On a theorem of N. Jacobson. Proc. Japan Acad. **31** (1955), 653-654.

[16] TOMINAGA, H., Galois theory of simple rings. Math. J. Okayama Univ. (1956), 29-48.

DEPARTMENT OF MATHEMATICS,
TOKYO INSTITUTE OF TECHNOLOGY.