ON GENERATING ELEMENTS OF SIMPLE RING EXTENSIONS

HISAO TOMINAGA

Throughout the present note, A will be a simple (artinian) ring with the identity element 1 which is represented as $\sum_1^n De_{ij}$ with a system of matrix units $E=\{e_{ij}\}$ such that the centralizer $V_A(E)$ of E in A is the division ring D. In subsequent use, a subring of A will mean one containing the identity element 1 of A. Further, we use the following conventions: B will mean a simple subring of A, and $\mathfrak{G}$ the group of all ring automorphisms in A which leave every element of B invariant. The centers of A and B will be denoted by C and Z respectively, and we use the notations $V=V_A(B)$, $H=V_A(V)$ and $C_0=V\cap H(=$center of $V)$. If the fixring of $\mathfrak{G}$ coincides with B and V is simple, A/B is said to be Galois (cf. [6]).

Concerning generating elements of a finite Galois extension A/B, we have obtained a number of interesting results ([2], [3] and [9]), and seen that the tools used in the respective cases $[B:Z]=\infty$ and $[B:Z]<\infty$ are strikingly distinct. In this note, we shall sharpen slightly the key propositions for these respective cases which were given in [2] and [3], and give as easy consequence of these sharpenings several results obtained previously in [2], [3], [4] and [9] with some refinement.

1.

In this section, the preliminary results will be stated without proof as lemmas.

Lemma 1 ([8; Lemma]). *If $[A:C]<\infty$ then $[B:Z]<\infty$. The converse is true, provided A is left (or right) finite over B.*

Lemma 2 ([1; Theorem VII. 11. 3] or [7]). *Let A be a division ring, and $[A:C]<\infty$. If M is a maximal subfield of A and $M=C[m]$ then there exists an element a such that $A=\sum_{i,j=0}^t m^i am^j C$.*

Lemma 3 ([6] and [2; Lemma 1.4]). *Assume that A is finite Galois over B.*

(a) *If B' is a simple intermediate ring of A/B and $V_A(B')$ is simple then A is Galois over B'.*

(b) *If V is a division ring then every intermediate ring of A/B is simple, and conversely.*

Lemma 4 ([2; Corollary 2.1]). *Assume that A is finite Galois over B and $[B:Z]=\infty$. If X is a B-B-submodule of A then $X=BxB$ with some x. In particular, every intermediate ring of A/B is singly generated over B.*

Lemma 5 ([3; Lemma 7]). *Let $n\geqslant 2$, and let x be a non-zero element of D. If a is an element of A not contained in C then there exists a unit r of A such that $a^{\tilde{r}}=rar^{-1}=\sum x_{ij}e_{ij}$ where $x_{1n}=x$ and $x_{in}=0$ for every $i>1$.*

Lemma 6 ([5; Lemma 1]). *Let $n\geqslant 2$, and let T be a left artinian subring of A. If T contains $a=\sum x_{ij}e_{ij}$ $(x_{ij}\in D)$ such as $x_{1n}=1$ and $x_{in}=0$ for every $i>1$ and $u(E,d)=de_{21}+\sum_3^n e_{ii-1}$ with non-zero $d\in D$, then T is a simple ring containing E, d and x_{ij}'s.*

2.

We shall prove first the key proposition for the case $[B:Z]=\infty$.

Proposition 1. *Assume that A is finite Galois over B and $[B:Z]=\infty$.*

(a) *If A' is an intermediate ring of $A/B\cdot V$ then $A'=B[a']$ with some unit a'. In particular, $A=B[a]$ with some unit a.*

(b) *If V is a division ring, then for every intermediate ring A' of A/B there exists a unit a' of A' such that $A'=B[a']$.*

Proof. (a) As $B\cdot V=B\otimes_Z V$ is simple and $V_A(B\cdot V)=C_0$, A' is a simple ring by Lemma 3. Accordingly, we have $A'=\sum_1^{n'}D'e'_{ij}$ where $E'=\{e'_{ij}\}$ is a system of matrix units such that $V_{A'}(E')$ is the division ring D'. Obviously, by Lemma 4, it suffices to prove the case $n'>1$. Moreover, in virtue of Lemma 5, we may assume that B contains an element $b=\sum x'_{ij}e'_{ij}$ $(x'_{ij}\in D')$ such as $x'_{1n}=1$ and $x'_{in}=0$ for every $i>1$. We consider here the simple ring $B_1=B[E']=\sum_1^{n'}D_1e'_{ij}$, where $D_1=V_{B_1}(E')$ is a division subring of D'. If we set $V=\sum_1^{r}Ug_{pq}$ with a system of matrix units $\Gamma=\{g_{pq}\}$ such that $U=V_V(\Gamma)$ is a division ring, then we may assume further that E' contains Γ. It follows then $V_A(B_1)=V_V(E')=V_U(E')$ is a division ring, and therefore $V_A(E')$ is finite Galois over D_1 by Lemma 3 (a). Since D_1 is infinite over its center (Lemma 1), we can find a non-zero element d' such that $D'=D_1[d']$ (Lemma 4). Setting $a'=1-u(E',$

$d')$, a' is a unit of A' and Lemma 6 proves $A'=B[b, u(E', d')]=B[a']$.

(b) As V is a division ring, A' is simple by Lemma 3 (b) and the proof proceeds in the same way as in (a).

3.

The next is stated in [9]. However, for the sake of completeness, we shall give here the proof.

Theorem 1. *If A is a separable simple algebra of finite rank over a field Φ then $A=\Phi[u, u\tilde{r}]$ with some units u and r.*

Proof. Case I. $n=1$: As is well known, A contains a maximal subfield M which is separable over Φ. Since $M=\Phi[u]$ with some u, by Lemma 2 there exists a unit r such that $A=\sum_{i,j}u^i r u^j C=\sum u^i(u\tilde{r})^j C=\Phi[u, u\tilde{r}]$.

Case II. $n>1$: As D is a separable division algebra over Φ, by Case I there exist non-zero elements x, $d\in D$ such that $D=\Phi[x, x\tilde{d}]$. We set $t=\sum_1^n e_{i\,n-i+1}(=t^{-1})$, $u^*=u(E, 1)$ and $v^*=u^*\tilde{t}=\sum_2^n e_{i-1\,i}$. Then, one will easily see that $e_{ij}=u^{*i-1}v^{*n-1}u^{*n-1}v^{*j-1}$ $(i, j=1, 2, \cdots, n)$. In case $D=\Phi$, $1-u^*$ is a unit and $\Phi[1-u^*, (1-u^*)\tilde{t}]=\Phi[u^*, v^*]=\Phi[E]=A$. Thus, in what follows, we may restrict our attention to the case $D\neq\Phi$. Under this situation, if $x\tilde{d}\cdot x=1$ then $\Phi[x, x\tilde{d}]=\Phi[x, x\tilde{1}]$ and $x\cdot x\neq 1$. Accordingly, we may assume further that $x\tilde{d}\cdot x\neq 1$. If $u=u^*+xe_{1n}$ and $v=u\widetilde{dt}=v^*+x\tilde{d}\cdot e_{n1}$ then $u^{-1}=v^*+x^{-1}e_{n1}\in\Phi[u]$ yields $(x^{-1}-x\tilde{d})e_{n1}=u^{-1}-v\in\Phi[u, v]$, whence it follows $(1-x\tilde{d}\cdot x)e_{nn}=(u^{-1}-v)u\in\Phi[u, v]$. Noting that $x=u^n$ and $x\tilde{d}=v^n$ are contained in $\Phi[u, v]$, we obtain $e_{nn}\in\Phi[u, v]$, which forces $e_{ij}=v^{n-i}e_{nn}u^{n-j}\in\Phi[u, v]$. Consequently, we have $\Phi[u, v]=\Phi[x, x\tilde{d}, E]=A$, completing the proof.

Corollary 1. *If A is finite Galois over B and $[B:Z]<\infty$ then $A=(B\cap C)[u, u\tilde{r}]$ with some units u and r.*

Proof. Since $[A:C]<\infty$ by Lemma 1 and C is finite Galois over $B\cap C$, A is a separable simple algebra of finite rank over $B\cap C$.

4.

The next is the key result for the case $[B:Z]<\infty$ (cf. [3; Proposition 1]).

Proposition 2. *Assume that A is finite Galois over B and $[B:Z]$*

$<\infty$. *Let* A^* *be a simple intermediate ring of* A/B *such that the center* C^* *of* A^* *is contained in* C_0.

(a) *If* A^* *is commutative then* $A^*=Z[c_0]$ *with some* c_0.

(b) *If* a *is an arbitrary element of* A^* *not contained in* C^* *then there exists a unit* a' *of* A^* *such that* $A^*=Z[a, a']$.

Proof. Let $\Phi=B\cap C$ and $A^*=\sum_1^{n^*}D^*e_{ij}^*$ where $E^*=\{e_{ij}^*\}$ is a system of matrix units such that $V_{A^*}(E^*)$ is the division ring D^*. In the proof of [3; Proposition], we must complete only the case that $D^*\neq C^*$ and $n^*=2$. In any rate, we have known that $A^*=Z[a, a'']$ with some a''. Noting that Φ is infinite, one will easily see that there exists an element $\alpha\in\Phi$ such that $a'=a''-\alpha$ is a unit of A^*. Then, we obtain $A^*=Z[a, a'']=Z[a, a']$.

5.

As the first consequence of Proposition 2, we obtain the following [4; Theorem 1] with an extremely short proof (cf. also [3; Theorem 1]).

Theorem 2. *Let* A *be a separable simple algebra of finite rank over a field* Φ. *If* a *in an arbitrary element of* A *not contained in* C *then* $A=\Phi[a, a']$ *with some unit* a'.

Proof. As is well known, the centeral simple algebra A over C has a finite Galois extension C^* of C as a splitting field, where we may assume further C^* is Galois over Φ. Then, $A^*=A\otimes_C C^*=(C^*)_m$ is finite Galois over Φ, and so we can apply Proposition 2 to A^*/Φ and A to see that there exists a unit a' such that $A=\Phi[a, a']$.

Next, combining Proposition 1 with Proposition 2 and Corollary 1, one will obtain at once the following sharpening of [3; Theorem 5] and [3; Corollary 2] itself.

Theorem 3. *Assume that* A *is finite Galois over* B.

(a) *If* a *is an arbitrary element of* A *not contained in* C *then there exists a unit* a' *such that* $A=B[a, a']$. *Accordingly,* A/B *is singly generated if and only if either* $A=C$ *or* $B\not\subset C$.

(b) $A=B[u, u\tilde{r}]$ *with some units* u *and* r.

Moreover, the validity of Proposition 1 enables us to see the following (cf. [3; Theorem 2]):

Theorem 4. *Assume that* A *is finite Galois over* B. *If* V *is commutative then for every intermediate ring* A' *of* A/B *there exists a unit* a' *such that* $A'=B[a']$.

REFERENCES

[1] N. JACOBSON: Structure of rings, Amer. Math. Soc. Colloq. Publ. 37, 1956.
[2] T. NAGAHARA and H. TOMINAGA: On Galois and locally Galois extensions of simple rings, Math. J. Okayama Univ. 10, 143—166 (1961).
[3] T. NAGAHARA and H. TOMINAGA: Corrections and supplements to the previous paper "On Galois and locally Galois extensions of simple rings", Math. J. Okayama Univ. 11, 67—77 (1963).
[4] T. NAGAHARA, K. KISHIMOTO and H. TOMINAGA: Supplementary remarks to the previous papers, Math. J. Okayama Univ. 11, 159—163 (1963).
[5] T. NAGAHARA, A. NAKAJIMA and H. TOMINAGA: Algebraic extensions of simple rings I, Math. J. Okayama Univ. 13, 15—22 (1967).
[6] T. NAKAYAMA: Galois theory of simple rings, Trans. Amer. Math. Soc. 73, 276—292 (1952).
[7] T. ONODERA: On semilinear normal basis, J. Fac. Sci. Hokkaido Univ., Ser. I. 18, 23—33 (1964).
[8] H. TOMINAGA: On a theorem of N. Jacobson, Proc. Japan Acad. 31, 653—654 (1955).
[9] H. TOMINAGA and F. KASCH: On generating elements of simple rings, Proc. Japan Acad. 33, 187—189 (1957).

DEPARTMENT OF MATHEMATICS,
OKAYAMA UNIVERSITY

(Received February 20, 1969)