51. On Generating Elements of Simple Rings

By Hisao TOMINAGA and Friedrich KASCH

Mathematical Institutes, Okayama University and Heidelberg University

(Comm. by Z. SUETUNA, M.J.A., April 12, 1957)

1. Introduction. Some years ago, one of the present authors investigated in what range the classical theorem for the existence of a primitive element is carried over to Galois extensions of division rings, and proved the following: Any Galois extension K of a division subring H of finite rank possesses two generating elements over H [4, Satz 14]. In particular, if the center of the centralizer of H in K is separable over the center of K then there exist two generating elements of K/H which are conjugate (with respect to an inner automorphism) [2, Satz 5].

Regarding the corresponding question in ring extensions the author also sharpened Albert's result in [1] as follows: In any separable algebra A/F, where F is an infinite field, there exist two generating elements over F which are conjugate [3].

Recently these problems are reexamined: T. Nagahara succeeded first in excluding the separability hypothesis assumed in [2, Satz 5] [5, Theorem 4], and by the light of this fact, another of the present authors showed that any simple ring which is Galois and finite over a simple subring S is generated over S by three regular elements [7, Theorem 2].

In what follows, we shall prove that Nagahara's result is still valid for simple rings (Theorem 1), and that the result in [3] restricted to simple algebras is true without the infiniteness hypothesis for the ground field (Theorem 2).

2. Fundamental lemma. By a *simple ring* we shall mean, throughout this note, a two-sided simple ring with an identity satisfying minimum condition for one-sided ideals. And we say a simple ring R is *Galois* over a simple subring S if S is the fixed subring of an automorphism group in R and $V_R(S)$ (the centralizer of S in R) is simple. At last, for any subring U and any subset X in a ring T, $U(X)$ will mean the subring of T generated by X over U.

Let a ring T with an identity be finite over a simple subring $U=\sum_1^m Kc_{ij}$ containing the identity of T as a U-left module, where c_{ij}'s are matric units and $K=V_U(\{c_{ij}\})$ is a division ring. As evidently T is finite over K, we can easily see that, *for any regular element $t\in T$, t^{-1} is contained in $K(t)$, so that in $U(t)$.* This fact will be used very often in the sequel.

Now let a simple ring $R=\sum_1^n De_{ij}$ be finite over a simple subring S (containing the identity of R) as an S-left module, where e_{ij}'s are matric units and $D=V_R(\{e_{ij}\})$ is a division ring. Then we set $S_1=S(\{e_{ij}\})=\sum_1^n D_1e_{ij}$, where $D_1=V_{S_1}(\{e_{ij}\})$ is a division ring by the last remark. And evidently D is finite over D_1. Under this situation, there holds the next which is essential in the present investigation.

Lemma. *If $D=D_1(x,y)$ with some conjugate $x,y\in D$ then $R=S(u,v)$ with some conjugate, regular $u,v\in R$.*

Proof. Clearly it suffices to prove our assertion for $n>1$. Throughout the proof, we set $t=\sum_1^n e_{in-i+1}\,(=t^{-1})$, $u^*=\sum_2^n e_{i-1i}$, $v^*=\sum_2^n e_{ii-1}=tu^*t^{-1}$ and $y=dxd^{-1}$ with $d\in D$. Then by a brief computation, we obtain

$$e_{ij}=v^{*i-1}u^{*n-1}v^{*n-1}u^{*j-1}\quad (i,j=1,\cdots,n).$$

Now in case $S=S(x,y)$, we have $S(1-u^*,\ 1-v^*)=S(u^*,v^*)=S(\{e_{ij}\})=R$ by the above remark, whence the regular elements $1-u^*$, $1-v^*$ are our desired u,v. Hence in the rest of the proof, we shall assume $S\neq S(x,y)$. Moreover, without loss of generality, we may assume $S\neq S(x)$. Then we shall show that for our desired u,v one can adopt those ones which are not too different from u^*, v^* respectively. We distinguish here two cases: (I) $xy\neq 1$. We set

$$u=u^*+xe_{n1},$$
$$v=v^*+ye_{1n}=(dt)u(dt)^{-1}.$$

Then $u^{-1}=v^*+x^{-1}e_{1n}$ is contained in $S(u)$, and so $(x^{-1}-y)e_{1n}=u^{-1}-v\in S(u,v)$. We obtain therefore $(1-xy)e_{nn}=u(x^{-1}-y)e_{1n}\in S(u,v)$. And we can easily verify

$$\left.\begin{array}{l}(1-xy)e_{in}=u^{n-i}(1-xy)e_{nn}\\(1-xy)e_{nj}=(1-xy)e_{nn}v^{n-j}\end{array}\right\}\in S(u,v)\quad (i,j=1,\cdots,n).$$

Hence all $(1-xy)^2e_{ij}$'s, and so $(1-xy)^2\in S(u,v)$. Noting that $(1-xy)^2$ is a regular element, we obtain $(1-xy)^{-2}\in S(u,v)$, accordingly all e_{ij}'s are contained in $S(u,v)$. Furthermore $x=\sum_1^n e_{in}ue_{1i}$ and $y=\sum_1^n e_{i1}ve_{ni}$ are in $S(u,v)$, and we have eventually $S(u,v)=S_1(x,y)=R$. (II) $xy=1$. In this case, $D=D_1(x,y)=D_1(x)$ obviously. And our assumption $S\neq S(x)$ implies $x\neq\pm 1$, that is, $x^2\neq 1$. Accordingly we can apply the argument in (I) for x,x instead of x,y.

3. Consequences

Theorem 1. *If a simple ring R is Galois and finite over a simple subring S, then $R=S(u,v)$ with some conjugate, regular $u,v\in R$.*

Proof. Under the notations mentioned in § 2, R is Galois over S_1 by [6, Theorem 2], and so D is Galois and finite over D_1. Hence $D=D_1(x,dxd^{-1})$ with some $x,d\in D$ by [5, Theorem 4], and our assertion is a direct consequence of our lemma.

Theorem 2. *Any separable simple algebra over a field is generated over the ground field by two conjugate regular elements.*

Proof. Let R be a separable simple algebra over a field S. Then again under the notations mentioned in § 2, we have $D=V_D(D)(x, dxd^{-1})$ with some $d, x \in D$ by [2, Satz 5]. Moreover, as is readily seen from the proof of [2, Satz 5], we can choose as x a generating element over S of any maximal commutative subfield of D which is separable over $V_D(D)$. Hence we may set $D=S(x, dxd^{-1})$, and so our assertion is clear from our lemma.

References

[1] A. A. Albert: Two elements generation of a separable algebra, Bull. Amer. Math. Soc., **50**, 786–788 (1944).

[2] F. Kasch: Über den Satz vom primitiven Element bei Schiefkörper, J. f. reine u. angew. Math., **180**, 150–159 (1951).

[3] F. Kasch: Zur Erzeugung separabler Algebren, Norsk Mat. Tidsskr., **34**, 97–99 (1952).

[4] F. Kasch: Über den Endomorphismenring eines Vektorraumes und den Satz von der Normalbasis, Math. Ann., **126**, 447–463 (1953).

[5] T. Nagahara: On generating elements of Galois extensions of division rings, Math. J. Okayama Univ. (to appear).

[6] H. Tominaga: Galois theory of simple rings, Math. J. Okayama Univ., **6**, 29–48 (1956).

[7] H. Tominaga: Galois theory of simple rings II, Math. J. Okayama Univ. (to appear).