134. On Generating Elements of Galois Extensions of Simple Rings

By Takasi NAGAHARA
Department of Mathematics, Okayama University, Okayama
(Comm. by Z. SUETUNA, M.J.A., Nov. 12, 1962)

If a simple ring R is Galois and finite over a simple subring S then $R=S[u, v]$ with some conjugate u, v [6, Theorem 1]. In case R is a division ring we have seen that $R=S[r]$ with some r if and only if R is commutative or S is not contained in the center C of R [2, Theorem 3]. The purpose of this paper is to prove that this fact is still valid for simple rings.

Throughout the present paper, R be always a simple ring (with minimum condition), and S a simple subring of R containing the identity element of R. And we shall use the following conventions: $R=\sum_1^n De_{ij}$, where e_{ij}'s are matrix units and $D=V_R(\{e_{ij}\text{'s}\})$ a division ring. And, C, Z and V are the center of R, the center of S and the centralizer $V_R(S)$ of S in R respectively. When R is Galois over S, we denote by $\mathfrak{G}$ the Galois group of R/S. Finally, as to notations and terminologies used in this paper, we follow [4].

In what follows, we shall prove several preliminary lemmas, which will be needed exclusively for the proof of our principal result.

Lemma 1. *Let R be Galois and finite over S. If R' is an intermediate ring of R/S such that R is R'-R-irreducible then R' is a simple ring.*

Proof. By [3, Lemma 2], $(\sigma|R')R_r$ is R'_r-R_r-irreducible and canonically R_r-isomorphic to R_r for each $\sigma\in\mathfrak{G}$. Next, let $(\tau|R')R_r$ be R'_r-R_r-isomorphic to $(\sigma|R')R_r$ $(\sigma, \tau\in\mathfrak{G})$. If $\sigma|R'\leftrightarrow\tau v_r|R'$ under the isomorphism, then one will easily see that $v\in V$. Moreove, $(\tau v_r|R')R_r=(\tau|R')R_r$ yields at once $vR=R$. Hence, v is a regular element of R. Now, it will be easy to see that $\tau|R'=\sigma\tilde{v}|R'$. And, the converse is true as well. Finally, one may remark that $V_R(R')$ is a division ring. By the light of these facts, patterning after the proof of [4, Lemma 1.4], we can prove that R' is a simple ring. The details may be left to readers.

Lemma 2. *If $e_{ii}R\cap S\neq 0$ $(i=1,\cdots, n)$ then $S\supseteqq\{e_{11},\cdots, e_{nn}\}$.*

Proof. Each $\mathfrak{r}_i=e_{ii}R\cap S$ is a non-zero right-ideal of S, and $\mathfrak{r}_1+\cdots+\mathfrak{r}_n=\mathfrak{r}_1\oplus\cdots\oplus\mathfrak{r}_n$. As the capacity of S never exceeds that of R, we obtain $\mathfrak{r}_1+\cdots+\mathfrak{r}_n=S$. Hence, $e_{11}+\cdots+e_{nn}=1=a_1+\cdots+a_n$ for some $a_i\in\mathfrak{r}_i$. Recalling here that $\mathfrak{r}_i\subseteqq e_{ii}R$, it follows that $e_{ii}=a_i\in S$ $(i=1,\cdots, n)$.

Lemma 3. *Let* $=\sum_1^n e_{ij}c_{ij}$ *be an element of* R *with* $c_{1n}\neq 0$.

(i) *Let* $n>2$. *If* $h\in D$ $k\neq 0\in D$ *are given, then there exists a regular element* $r\in R$ *such that* $rbr^{-1}=\sum_1^n e_{ij}d_{ij}$, $d_{1n-1}=h$, $d_{1n}=k$ *and* $d_{in}=0$ $(i=2,\cdots,n)$.

(ii) *If* $n=2$ *and* b *is a regular element, then there exists a regular element* $r\in R$ *such that* $rbr^{-1}=\sum_1^2 e_{ij}d_{ij}$, $d_{12}\neq 0$, $d_{21}=1$ *and* $d_{22}=0$.

Proof. (i) Set $h'=c_{1n}^{-1}(h-c_{1n-1})$, $k'=c_{1n}^{-1}k$. And consider the following product r of elementary matrices:

$$r=(\textstyle\sum_1^{n-1}e_{ii}+e_{nn}k'^{-1})(1-e_{nn-1}h')\cdot$$
$$(1-e_{n1}c_{nn}c_{1n}^{-1})(1-e_{n-11}c_{n-1n}c_{1n}^{-1})\cdots(1-e_{21}c_{2n}c_{1n}^{-1}).$$

Then, we see that

$$r^{-1}=(1+e_{21}c_{2n}c_{1n}^{-1})\cdots(1+e_{n-11}c_{n-1n}c_{1n}^{-1})(1+e_{n1}c_{nn}c_{1n}^{-1})\cdot$$
$$(1+e_{nn-1}h')(\textstyle\sum_1^{n-1}e_{ii}+e_{nn}k').$$

(ii) $b^*=(1-e_{21}c_{22}c_{12}^{-1})b(1-e_{21}c_{22}c_{12}^{-1})^{-1}=(1-e_{21}c_{22}c_{12}^{-1})b(1+e_{21}c_{22}c_{12}^{-1})=e_{11}c_1^*+e_{21}c_2^*+e_{12}c_{12}$ $(c_1^*, c_2^*\in D)$. Here, b^* being a regular element, c_2^* can not be zero. And so, $(e_{11}c_2^*+e_{22})b^*(e_{11}c_2^*+e_{22})^{-1}=(e_{11}c_2^*+e_{22})b^*(e_{11}c_2^{*-1}+e_{22})=e_{11}d^*+e_{12}c_2^*c_{12}+e_{21}$ $(d^*\in D)$. Hence, it will be clear that $r=(e_{11}c_2^*+e_{22})(1-e_{21}c_{22}c_{12}^{-1})$ is our desired one.

In the rest of our preliminaries, we shall assume that R is Galois and finite over S and $[S:Z]<\infty$. Then, to be easily seen, R is Galois and finite over $C'=C\cap S$ (cf. [5, Lemma]). And so, R is Galois and finite over $\sum_1^n e_{ij}C'$; this means that $V_R(\sum_1^n e_{ij}C')=D$ is Galois and finite over C'. Hence, by [1, Theorem 4] or [6, Theorem 1], $D=C'[x,y]$ for some non-zero elements $x, y\in D$.[1)]

Lemma 4. *Let* R *be Galois and finite over* S, $[S:Z]<\infty$, V *a division ring, and* $n=2$. *If* S *contains an element* $a=\sum_1^2 e_{ij}d_{ij}$ *such that* $d_{12}\neq 0$, $d_{21}=1$ *and* $d_{22}=0$, *then* $R=S[u']$ *for* $u'=e_{21}x+e_{22}y$.

Proof. Set $R'=S[u']$, that is a simple ring by [4, Lemma 1.4]. Then, $au'=e_{11}d_{12}x+e_{12}d_{12}y$ and $u'a=e_{21}(xd_{11}+y)+e_{22}xd_{12}$ are non-zero elements of $R'\cap e_{11}R$ and $R'\cap e_{22}R$ respectively. And so, Lemma 2 yields $R'\supseteqq\{e_{11}, e_{22}\}$. Hence, $e_{21}=e_{22}ae_{11}$ and $e_{12}d_{12}=e_{11}ae_{22}$ are contained in R', whence $d_{12}=(e_{21}+e_{12}d_{12})^2\in R'$. Accordingly, $e_{12}=e_{12}d_{12}\cdot d_{12}^{-1}\in R'$. Moreover,

$$\left.\begin{array}{l} x=(e_{21}+e_{12}x)^2=(e_{21}+e_{12}u'e_{12})^2 \\ y=(e_{21}+e_{12}y)^2=(e_{21}+e_{12}u'e_{22})^2 \end{array}\right\}\in R'.$$

We obtain therefore $R'=S[u']=S[\{e_{ij}\text{'s}\}, x, y]=R$.

Lemma 5. *Let* R *be Galois and finite over* S, $[S:Z]<\infty$, *and* $n\geqq 2$. *If* S *contains an element* $a=\sum_1^n e_{ij}d_{ij}$ *such that* $d_{1n-1}=x$, $d_{1n}=y$ *and* $d_{in}=0$ $(i=2,\cdots,n)$, *then* $R=S[u]$ *for* $u=\sum_2^n e_{ii-1}$.

Proof. Set $R'=S[u]$. Then, by [3, Lemma 6 (i)], we see that

1) D is evidently a separable division algebra over C', and $D=C'[x,y]$ can be regarded as a consequence of this fact too.

R is R'-R-irreducible. Hence, R' is simple by Lemma 1. Moreover, as $u^{n-1}=e_{n1}$, we see that $u^{k-1}au^{n-1}=e_{k1}y$ is a non-zero element of $R'\cap e_{kk}R$ ($k=1, \cdots, n$ and $u^0=1$). And so, Lemma 2 yields $R'\supseteqq\{e_{11}, \cdots, e_{nn}\}$. Hence, $e_{1n}y=e_{11}ae_{nn}\in R'$, whence $y=(u+e_{1n}y)^n$ and y^{-1} are contained in R'. Accordingly, $e_{1n}=e_{1n}yy^{-1}\in R'$ and $e_{ij}=(u+e_{1n})^{i-1}e_{1n}(u+e_{1n})^{n-j}\in R'$ ($i, j=1, \cdots, n$). And finally, $x=(u+e_{1n}x)^n\in R'$. We obtain therefore $R'=S[u]=S[\{e_{ij}\text{'s}\}, x, y]=R$.

Now we are at the position to prove the following:

Principal Theorem. *Let R be Galois and finite over S. Then $R=S[r]$ for some r if and only if R is commutative or $S\nsubseteq C$.*

Proof. The only if part will be almost trivial. And so, we shall prove here the if part. For the case where $[S:Z]=\infty$ our assertion is contained in [4, Corollary 2.1], and for the case where R is commutative our assertion is well-known. Thus, in what follows, we shall prove that if $[S:Z]<\infty$ and $S\nsubseteq C$ then $R=S[r]$ for some r. To this end, we shall distinguish two cases:

Case I: *S contains merely diagonal elements.* In this case, V contains $\{e_{11}, \cdots, e_{nn}\}$, whence we see that the capacity of V coincides with that of R. And so, without loss of generality, we may assume that e_{ij}'s are all contained in V, whence $S\subseteqq D$. Now, our assertion is a direct consequence of [4, Lemma 2.3].

Case II: *S contains a non-diagonal element $b=\sum_1^n e_{ij}c_{ij}$.* Here, without loss of generality, we may assume that $d_{1n}\neq 0$ (cf. [3, pp. 62–63]). We shall distinguish here further two cases:

1. $n>2$. By Lemma 3 (i), there exists a regular element r such that $a=rbr^{-1}=\sum_1^n e_{ij}d_{ij}$, $d_{1n-1}=x$, $d_{1n}=y$ and $d_{in}=0$ ($i\geqq 2$). As we can easily see that $R(=rRr^{-1})$ is Galois and finite over rSr^{-1} and $C\cap rSr^{-1}=C\cap S$, Lemma 5 yields $R=rSr^{-1}[u]$ where $u=\sum_2^n e_{ii-1}$. Hence, we have $R=r^{-1}Rr=S[r^{-1}ur]$.

2. $n=2$. Since S is generated by regular elements, we may assume that b is a regular element. And then, by Lemma 3 (ii), there exists a regular element r such that $a=rbr^{-1}=\sum_1^2 e_{ij}d_{ij}$, $d_{12}\neq 0$, $d_{21}=1$ and $d_{22}=0$. If V is not a division ring, then the capacity of V is equal to 2 (the capacity of R) and our assertion is contained in Case I. Thus, we may assume that V is a division ring. Now, noting that R is Galois and finite over rSr^{-1}, $C\cap S=C\cap rSr^{-1}$, and that $V_R(rSr^{-1})=rVr^{-1}$ is a division ring, we obtain $R=rSr^{-1}[u']$ for $u'=e_{21}x+e_{22}y$ by Lemma 4. It follows therefore $R=r^{-1}Rr=S[r^{-1}u'r]$.

References

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

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

[3] T. Nagahara: On algebraic Galois extensions of simple rings, Math. J. Okayama Univ., **11**, 59–65 (1962).

[4] T. Nagahara and H. Tominaga: On Galois and locally Galois extensions of simple rings, Math J. Okayama Univ., **10**, 143–166 (1961).

[5] H. Tominaga: On a theorem of N. Jacobson, Proc. Japan Acad., **31**, 653–654 (1955).

[6] H. Tominaga and F. Kasch: On generating elements of simple rings, Proc. Japan Acad., **33**, 187–189 (1957).