CORRECTIONS AND SUPPLEMENTS TO THE PREVIOUS PAPER "ON GALOIS AND LOCALLY GALOIS EXTENSIONS OF SIMPLE RINGS"

TAKASI NAGAHARA and HISAO TOMINAGA

It has recently been found that §3 of our previous paper [5] contained in its tool lemmas Lemmas 3.2 and 3.3 some errors. Nevertheless we have been able to prove a notably efficient proposition which enables us to prove all the theorems cited in [5, §3]. This will be given in §2 of the present paper. And in §3, we shall see that Theorems 3.1 and 3.2 of [5] are still valid and that further several interesting facts can be shown as corollaries to our proposition.

Throughout the present paper, $R=\sum_1^n De_{ij}$ be a simple ring, where e_{ij}'s are matrix units and $D=V_R(\{e_{ij}\text{'s}\})$ is a division ring. And S be always a simple subring of R (containing the identiy element 1 of R). Further, we set $C=V_R(R)$, $Z=V_S(S)$, $V=V_R(S)$, $H=V_R(V)$, $C_0=V_V(V)$ and $K=Z\cap C=V_S(R)$. As to general notations and terminologies used here, we folow [5].

1. Preliminary lemmas.

Lemma 1. *Let R be a separable division algebra over a field $\Phi\subseteq C$ (of finite rank). If an intermediate ring S of R/Φ is not contained in C then $R=S[x]$ with some x.*

Proof. Let M be a maximal subfield of R such that M/C is separable. Then, as is well-known, $M=\Phi[v]$ with some v. And, by [1, Theorem VII. 12. 3], we can find such an element u of R that $R=C[u,v]=\Phi[u,v]$. Since M/C is separable, there exists only a finite number of intermediate fields of M/C. Accordingly, $T_1,\cdots,T_q$ be all the intermediate rings of R/M different from R. Here, choose arbitrarily an element $a\in S\setminus C$. Then, without loss of generality, we may assume that $au\neq ua$. As $u\notin T_i (i=1,\cdots,q)$, in virtue of [2, Lemma 1 (i)], there exist at most two elements $c\in\Phi$ such that $(u+c)a(u+c)^{-1}\in T_i$. As $R\neq C$ implies evidently that Φ is infinite, there exists some $c_0\in\Phi$ such that $a'=(u+c_0)a(u+c_0)^{-1}\notin T_i$ for all i. Hence, $R=M[a']=\Phi[a',v]=\Phi[a,(u+c_0)^{-1}v(u+c_0)]=S[u+c_0)^{-1}v(u+c_0)]$.

Lemma 2. *Let R be Galois and finite over S, and $[S:Z]<\infty$. And let $R^*=\sum_1^{n^*} D^*e^*_{ij}$ be an intermediate simple ring of R/S with matrix units e^*_{ij}'s and a division ring $D^*=V_{R^*}(\{e^*_{ij}\text{'s}\})$ such that the center C^* of R^* is contained in C_0.*

(i) $Z[C^*]=Z[\alpha]$ *for some non-zero* α *in* $V_{R^*}(R)$.

(ii) *For each* $x\in D^*\setminus C^*$, *there exists a non-zero element* $y\in D^*$ *such that* $D^*=C^*[x, y]$ *and* $K[y]\ni\alpha$.

Proof. As $S[C]=S\times_Z Z[C]$ $(\subseteq S\times_Z V)$, $S[C]$ is a simple ring. And so, $V_R(H)=V=V_R(S[C])$ and $[R: C]<\infty$ ([6, Lemma]) yield at once $H=S[C]$. Hence, $C_0=H\cap V=V_{S\times_Z Z[C]}(S)=Z[C]$. As C_0/Z and C/K are finite dimensional Galois extensions and $\mathfrak{G}(C_0/Z)$ is isomorphic to $\mathfrak{G}(C/K)$ by the restriction map, one will readily see that $Z[C]=Z\times_K C$. Accordingly, as an intermediate field of C_0/Z, $Z[C^*]=Z\times_K C'$ with some intermediate field C' of C/K. As $C'=K[\alpha]$ for some $\alpha\neq 0$, we obtain $Z[C^*]=Z[\alpha]$, where, needless to say, α is contained in $V_{R^*}(R)$. Next, we have $D^*=C^*[x, y']$ with some y' by Lemma 1. Recalling here that $K[\alpha, y']$ is a field finite over K and α is separable over K, Abel's theorem proves that $K[\alpha, y']=K[y]$ with some $y\neq 0$. We have proved therefore that $K[y]\ni\alpha$ and $C^*[x, y]=C^*[x, y', \alpha]=D^*$.

The next two lemmas may be more or less known, however, for the same of completeness, we shall give here the proofs.

Lemma 3. *Let R be Galois and finite over S, and T an intermediate ring of R/S. If R is T-R-irreducible then T is a regular subring of R.*

Proof. As $V_R(T)$ is a division ring, $\mathfrak{G}(T)$ $(\mathfrak{G}=\mathfrak{G}(R/S))$ is a regular group in Nakayama's sense. And so, $T'=J(\mathfrak{G}(T), R)$ is a regular subring of R and $V_R(T)=V_R(T')$ by finite dimensional Galois theory (cf. [1, VI]). In what follows, we shall prove that T coincides with T'. By [3, Lemma 2], $(\sigma|T)R_r$ is T_r-R_r-irreducible and canonically R_r-isomprphic to R_r for each $\sigma\in\mathfrak{G}$. Next, let $(\tau|T)R_r$ be T_r-R_r-isomorphic to $(\sigma|T)R_r(\sigma, \tau\in\mathfrak{G})$. If $\sigma|T\leftrightarrow\tau v_r|T$ under the isomorphism, then one will easily see that $v\in V$. Moreover, v is a regular element of R. Now, it will be easy to see that $\tau|T=\sigma\tilde{v}|T$. And, the converse is true as well. We have seen therefore that $(\mathfrak{G}|T)R_r$ is completely reducible and its homogeneous component is of the form $(\widetilde{V}\sigma|T)R_r$. And moreover, patterning after the proof of [5, Lemma 1.3], we can prove that $[(\widetilde{V}\sigma|T)R_r: R_r]_r=[V: V_R(T)]_r$. Now, we may set $\mathrm{Hom}_{S_l}(T, R)=(\mathfrak{G}|T)R_r=\sum_1^s\oplus(\widetilde{V}\sigma_i|T)R_r$ with some σ_i's in $\mathfrak{G}$. If $T\subsetneqq T'$ then $[(\mathfrak{G}|T)R_r: R_r]_r=[T: S]_l<[T': S]_l=[(\mathfrak{G}|T')R_r: R_r]_r$, recalling that $\sum_1^s(\widetilde{V}\sigma_i|T')R_r=\sum_1^s\oplus(\widetilde{V}\sigma_i|T')R_r$ naturally, we see that there exists some $\tau\in\mathfrak{G}$ such that $\tau|T'\notin\sum_1^s\oplus(\widetilde{V}\sigma_i|T')R_r$. But, $\tau|T\in\sum_1^s\oplus(\widetilde{V}\sigma_i|T)R_r$ yields $\tau|T=\sigma_j\tilde{v}|T$ for some j and $v\in V$. And so, $\tau(\sigma_j\tilde{v})^{-1}=\tau'\in\mathfrak{G}(T)$, whence we have a contradiction $\tau|T'=\tau'\sigma_j\tilde{v}|T'=\sigma_j\tilde{v}|T'$.

Lemma 4. *Let R be Galois and finite over S, and T an intermediate simple ring of R/S.*

(i) *R is T-R-completely reducible.*

(ii) *If T is a regular subring then R is T-R-homogeneously completely reducible and the length of its composition series coincides with the capacity of $V_R(T)$. In particular, R is T-R-irreducible if and only if $V_R(T)$ is a division ring.*

Proof. At first we shall remark that each R_r-R_r-irreducible submodule $\mathfrak{M}$ of $\mathrm{Hom}_{S_l}(R, R) = \mathfrak{G}R_r$ is of the form $\sigma u_i R_r$ with some $\sigma \in \mathfrak{G}$ and $u \in R$. In fact, if $\mathfrak{M}$ is R_r-R_r-isomorphic to σR_r and $\mathfrak{M} \ni \alpha \leftrightarrow \sigma$ then $x_r\alpha = \alpha(x\sigma)_r$ for each $x \in R$, whence $(1\alpha)(x\sigma) = x\alpha$. As $\mathfrak{T} = \mathrm{Hom}_{T_l}(R, R)$ (contains R_r and so) is an R_r-R_r-submodule of $\mathrm{Hom}_{S_l}(R, R) = \mathfrak{G}R_r$, $\mathfrak{T} = \sum \oplus \sigma_i u_{ii} R_r$ with some σ_i's in $\mathfrak{G} = \mathfrak{G}(R/S)$. Now, let N be an arbitrary T-R-irreducible submodule of R. Then $N\mathfrak{T}$ is T-$\mathfrak{T}$-admissible, whence we have $R = N\mathfrak{T}$. On the other hand, $N\mathfrak{T} = \sum N\sigma_i u_{ii} R_r = \sum N\sigma_i u_{ii} (\sigma_i u_{ii} \in \mathrm{Hom}_{T_l}(R, R))$. As one can readily see that every $N\sigma_i u_{ii}$ is 0 or T-R-irreducible, R is T-R-completely reducible. And the second assertion is an easy consequence of the fact that $V_{\mathrm{Hom}(R,R)}(T_l \cdot R_r) = V_R(T)_l$.

Remark. For a subring $T \ni 1$ of R, R is T-R-irreducible if and only if R is $T[C]$-R-irredncible. This fact will be needed in the proof of Lemma 10.

Lemma 5. *If $e_{ii}R \cap S \neq 0 (i = 1, \cdots, n)$ then $e_{11}, \cdots, e_{nn} \in S$.*

Proof. Each $S_i = e_{ii}R \cap S$ is a non-zero right ideal of S, and $S_1 + \cdots + S_n = S_1 \oplus \cdots \oplus S_n$. As the capacity of S never exceeds that of R, we obtain $S_1 + \cdots + S_n = S$. Hence, $e_{11} + \cdots + e_{nn} = 1 = a_1 + \cdots + a_n$ with some $a_i \in S_i$. Recalling here that $S_i \subseteq e_{ii}R$, it follows that $e_{ii} = a_i \in S (i = 1, \cdots, n)$.

Lemma 6. *Let $[R:S] < \infty$, and T be an intermediate simple ring of R/S.*

(i) *If $n \geqq 2$, and T contains $a = \sum_1^n d_{ij} e_{ij}$ with $d_{1n} \neq 0$, $d_{in} = 0 (i \geqq 2)$ and $u = \sum_2^n e_{ii-1}$ then T contains all the e_{ij}'s and d_{ij}'s.*

(ii) *Let $n = 2$, and $x \neq 0$ and y given elements of D. If T contains $a = de_{11} + d'e_{21} + e_{12}$ and $v = xe_{21} + ye_{22}$ then T contains all the e_{ij}'s, d, d', x, and y.*

Proof. (i) As $u^{k-1} a\, u^{n-1} = d_{1n} e_{k1}$ is a non-zero element of $T \cap e_{kk}R (k = 1, \cdots, n)$, $T \ni e_{11}, \cdots, e_{nn}$ by Lemma 5. And so, $d_{1n}e_{1n} = e_{11}\, ae_{nn} \in T$, whence it follows $d_{1n} = (u + d_{1n}e_{1n})^n \in T$ and $d_{1n}^{-1} \in T$. Hence, $e_{1n} \in T$. Now, to be easily verified, $e_{ij} = (u + e_{1n})^{i-1} e_{1n} (u + e_{1n})^{n-j} \in T$ and $d_{ij} = \sum_1^n e_{ki}\, ae_{jk} \in T$.

(ii) $av = xe_{11} + ye_{12}$ and v are non-zero elements of $T \cap e_{11}R$ and $T \cap e_{22}R$ respectively. And so, $T \ni e_{11}, e_{22}$ by Lemma 5. Accordingly, both $e_{12} = e_{11}ae_{22}$ and $xe_{21} = e_{22}ve_{11}$ are contained in T, whence $x = (e_{12} + xe_{21})^2 \in T$. Hence, $e_{21} \in T$ and $y = (e_{12} + ve_{21})^2 = (e_{11} + ye_{21})^2 \in T$. And, it will be easy to see that d, d' are in T, too.

Lemma 7. *Let $n\geqq 2$, $y\neq 0$ and x given elements of D, and $a=\sum_1^n c_{ij}e_{ij}(c_{ij}\in D)$ in $R\backslash C$.*

(i) *There exists a regular element $r\in R$ such that $a^{\tilde{r}}=\sum_1^n d_{ij}e_{ij}$ with $d_{1n}=y$ and $d_{in}=0$ $(i\geqq 2)$.*

(ii) *If $n>2$, then there exists a regular element $r\in R$ such that $a^{\tilde{r}}=\sum_1^n d_{ij}e_{ij}$ with $d_{1n-1}=x$, $d_{1n}=y$ and $d_{in}=0$ $(i\geqq 2)$.*

Proof. At first, suppose a is diagonal: $a=\sum_1^n c_ie_{ii}$. If $c_h\neq c_k$ for some $h\neq k$, then $a^{\tilde{b}}=\sum_1^n c_ie_{ii}+(c_k-c_h)e_{hk}$ for $b=1+e_{hk}$. If on the other hand $a=d\in D\backslash C$, then there exists some $d'\in D$ such that $dd'-d'd\neq 0$, and $a^{\tilde{b}}=d+(d'd-dd')e_{12}$ *for* $b=1+d'e_{12}$. Thus, we may assume, from the beginning, that a is non-diagonal. In general, if $\begin{pmatrix}1\cdots n\\ p_1\cdots p_n\end{pmatrix}$ is an arbitrary permutation of $1,\cdots,n$ then, to be easily verified, $\sum_1^n x_{ij}e_{p_ip_j}\to\sum_1^n x_{ij}e_{ij}(x_{ij}\in D)$ is a D-(ring) automorphism of R, which is an inner automorphism effected by some regular element of $\sum_1^n Ce_{ij}$. Accordingly, without loss of generality, we may assume further that $c_{1n}\neq 0$. Now, under this situation, if $t=(\sum_1^{n-1}e_{ii}+c_{1n}e_{nn})(1-c_{nn}c_{1n}^{-1}e_{n1})\cdots(1-c_{2n}c_{1n}^{-1}e_{21})$ then $a^*=a^{\tilde{t}}=\sum_1^n c^*_{ij}e_{ij}$ with $c^*_{1n}=1$, $c^*_{in}=0$ $(i\geqq 2)$.

(i) For $s=\sum_1^{n-1}e_{ii}+y^{-1}e_{nn}$, we obtain $a^{*\tilde{s}}=\sum_1^n d_{ij}e_{ij}$ with $d_{1n}=y$ and $d_{in}=0$ $(i\geqq 2)$.

(ii) Choose such an element $x'\in D$ that $c^*_{1n-1}+x'=x$. Then, for $s=(\sum_1^{n-1}e_{ii}+y^{-1}e_{nn})(1-x'e_{nn-1})$ we obtain $a^{*\tilde{s}}=\sum_1^n d_{ij}e_{ij}$ with $d_{1n-1}=x$, $d_{1n}=y$ and $d_{in}=0$ $(i\geqq 2)$.

Lemma 8. *Let $n\geqq 2$, and $T\ni 1$ a subring of R. If T contains $a=\sum_1^n c_{ij}e_{ij}$ with $c_{1n}\neq 0$ and $u=\sum_2^n x_ie_{ii-1}$ with non-zero x_i's in D then R is T-R-irreducible.*

Proof. Let M be an arbitrary non-zero T-R-submodule of R. Then, M contains an element $b=\sum_p^n d_ie_{in}$ with $d_p\neq 0$ for some p. Since $M\ni u^{n-p}b=x_n\cdots x_{p+1}d_pe_{nn}$ (if $p=n$, $M\ni b=d_ne_{nn}$), e_{nn} is contained in M, whence it follows $M\ni ae_{nn}=\sum_1^n c_{in}e_{in}$. Hence, there holds $M\ni u^{n-k}\sum_1^n c_{in}e_{in}=\sum_2^k x_{n-k+i}\cdots x_{i+1}c_{in}e_{n-k+i\,n}+x_{n-k+1}\cdots x_2c_{1n}e_{n-k+1n}(k=1,\cdots,n)$. Recalling here that $c_{1n}\neq 0$, one can see inductively that $e_{nn}, e_{n-1n},\cdots,e_{1n}\in M$, whence eventually every $e_{ij}\in M$. Now, it will be easy to see that $M=R$.

Lemma 9. *Let R be a simple algebra over a field $\Phi\subseteq C$ (of finite rank) with $n=2$, and $f(\lambda)=\lambda^2-d\lambda-d'$ a polynomial of $C[\lambda]$. If x, y are non-zero elements of D such that $f(y^{-1}x)\neq 0$ then $\Phi[de_{11}+d'e_{21}+e_{12}, xe_{21}+ye_{22}]\cap De_{21}\neq 0$.*

Proof. We set $a=de_{11}+d'e_{21}+e_{12}$, $v=xe_{21}+ye_{22}$. Then, it will be easy to see that $va=(xd+yd')e_{21}+xe_{22}$ and $(va)^2=(x^2d+xyd')e_{21}+x^2e_{22}$. Now, let $g(\lambda)=\sum_0^m c_i\lambda^i\in\Phi[\lambda]$ be a minimal polynomial of $y(c_0=1, c_m\neq 0)$. As $v^i=y^{i-1}v=y^{i-1}xe_{21}+y^ie_{22}(i\geqq 1)$, we obtain $\Phi[a,v]\ni g(v)=e_{11}+$

$\sum_1^m c_i y^{i-1} x e_{21} + \sum_0^m c_i y^i e_{22} = e_{11} - y^{-1} x e_{21}$. And one will easily verify that $\Phi[a, v] \ni (va)^2 g(v) = \{(x^2 d + xyd')e_{21} + x^2 e_{22}\}(e_{11} - y^{-1} x e_{21}) = -xy\{(y^{-1}x)^2 - d(y^{-1}x) - d'\}e_{21} \neq 0$.

Lemma 10. *Let R be Galois and finite over S, and $[S:Z] < \infty$. And let $R^* = \sum_1^{n^*} D^* e^*_{ij}$ be an intermediate simple ring of R/S with matrix units e^*_{ij}'s and a division ring $D^* = V_{R^*}(\{e^*_{ij}\text{'s}\})$ such that $V_R(R^*)$ is a division ring and $Z[C^*] = Z[\alpha]$ with some $\alpha \in V_{R^*}(R)$, where C^* is the center of R^*.*

(i) *Let $n^* \geqq 2$, and $a = \sum_1^{n^*} d_{ij} e^*_{ij} (d_{ij} \in D^*)$ be an element of R^*. If $d_{1n^*} \neq 0$, $d_{in^*} = 0$ $(i \geqq 2)$, $K[d_{1n^*}] \ni \alpha$ and $D^* = C^*[\{d_{ij}\text{'s}\}]$ then there exists some $b \in R^*$ such that $R^* = Z[a, b]$.*

(ii) *Let $n^* = 2$, and $a = de^*_{11} + d'e^*_{21} + e^*_{12}$ be an element of R^*. If $D^* = C^*[y, d, d']$ and $K[y] \ni \alpha$* for some non-zero *$y \in D^*$ then $R^* = Z[a, ye^*_{21}]$.*

(iii) *Let $n^* = 2$, and $a = de^*_{11} + d'e^*_{21} + e^*_{12}$ be an element of R^* with $d, d' \in C^*$. If x, y are non-zero elements of D^* such that $K[y] \ni \alpha$, $D^* = C^*[x, y]$ and $(y^{-1}x)^2 - d(y^{-1}x) - d' \neq 0$, then $R^* = Z[a, xe^*_{21} + ye^*_{22}]$.*

Proof. (i) We set $u^* = \sum_2^{n^*} e^*_{ii-1}$ and $T = Z[a, u^*]$. Then, by Lemma 8, R^* is T-R^*-irreducible, whence $T[\alpha]$-R^*-irreducible. Since $R^* \supseteq T[\alpha] \supseteq Z[\alpha] \supseteq C^*$, R^*/C^* is Galois and $[R^*: C^*] < \infty$ by our assumption and [6, Lemma], $T[\alpha]$ is a simple ring by Lemma 3. And so, in virtue of Lemma 6 (i), $T[\alpha] \supseteq Z[\{e^*_{ij}\text{'s}\}, \{d_{ij}\text{'s}\}, \alpha] = Z[C^*][\{e^*_{ij}\text{'s}\}, \{d_{ij}\text{'s}\}] = R^*$, that is, $T[\alpha] = R^*$. As $V_R(R^*)$ is a division ring, R is $T[\alpha]$-R-irreducible by Lemma 4. Accordingly, as is noted in Remark, R is T-R-irreducible. Further, to be easily verified, $V_R(Z) = V_R(Z[C])$ is a simple ring, whence R is Galois and finite over Z. And so, T is a simple ring again by Lemma 3. Hence, Lemma 6 (i) yields $T \supseteq Z[\{e^*_{ij}\text{'s}\}, \{d_{ij}\text{'s}\}] = Z[\{e^*_{ij}\text{'s}\}, \{d_{ij}\text{'s}\}, \alpha] = R^*$, that is, $T = R^*$.

(ii) We set $T = Z[a, ye^*_{21}]$. By Lemma 8, R^* is T-R^*-irreducible, whence $T[\alpha]$-R^*-irreducible. And so, at in the proof of (i), we see that $T[\alpha]$ is simple. Accordingly, in virtue of Lemma 6 (ii), we have $T[\alpha] \supseteq Z[\{e^*_{ij}\text{'s}\}, d, d', y, \alpha] = R^*$, that is, $T[\alpha] = R^*$. And, again as in the proof of (i), we see that T is simple. Hence, in virtue of Lemma 6 (ii), it follows that $T \supseteq Z[\{e^*_{ij}\text{'s}\}, d, d', y] = Z[\{e^*_{ij}\text{'s}\}, d, d', y, \alpha] = R^*$, that is, $T = R^*$.

(iii) We set $T = Z[a, xe^*_{21} + ye^*_{22}]$. Then, noting that $[R: K] = [R: C] \cdot [C: K] < \infty$ by [6, Lemma], we obtain $T \cap D^* e^*_{21} \neq 0$ by Lemma 9, whence R^* is T-R^*irreducible by Lemma 8. And the rest of the proof will proceed just as in that of (ii).

2. Fundamental proposition.

Now, we can prove the following fundamental proposition.

Proposition. *Let R be Galois and finite over S, and $[S:Z]<\infty$. And let $R^*=\sum_1^{n^*}D^*e^*_{ij}$ be an intermediate simple ring of R/S with matrix units e^*_{ij}'s and a division ring $D^*=V_{R^*}(\{e^*_{ij}\text{'s}\})$ such that $V_R(R^*)$ is a division ring and the center C^* of R^* is contained in C_0.*

(i) *If* $R^*=C^*$ then $R^*=Z[\alpha]$ *for some* α.

(ii) *If a is in $R^*\backslash C^*$ then $R^*=Z[a, b]$ for some b.*

Proof. (i) $R^*=C^*=Z[C^*]=Z[\alpha]$ for some α by Lemma 2 (i).

(ii) At first, by Lemma 2 (i), we can find some non-zero element $\alpha\in V_{R^*}(R)(\subseteq C)$ such that $Z[C^*]=Z[\alpha]$. In case $n^*=1$, Lemma 2 (ii) enables us to see that there exists some $b\in D^*(=R^*)$ such that $D^*=C^*[a, b]$ and $K[b]\ni\alpha$, whence $Z[a, b]=Z[a, b, \alpha]=Z[C^*][a, b]=D^*$. And so, in what follows, we may, and shall, restrict our attention to the case $n^*\geqq 2$. We may remark here the following which will be refered sometimes in the sequel: Let r be a regular element of R^*. Then, $Z\tilde{r}$ and $C_0\tilde{r}$ coincide with the center of $S\tilde{r}$ and the center of $V_R(S\tilde{r})$ respectively, $Z\tilde{r}\cap C=K$ and $Z\tilde{r}[C^*]=Z\tilde{r}[\alpha]$, whence we shall see that R, R^*, and $S\tilde{r}$ yet satisfy the assumptions in our proposition. Now the rest of the proof will be completed by distinguishing three cases:

Case I. $D^*=C^*$. By Lemma 7 (i), there exists a regular element $r\in R^*$ such that $a\tilde{r}=\sum_1^{n^*}d_{ij}e^*_{ij}$ with $d_{1n^*}=\alpha$ and $d_{in^*}=0\ (i\geqq 2)$. And so, by the remark mentioned above and Lemma 10 (i), there exists some b' such that $R^*=Z\tilde{r}[a\tilde{r}, b']=(Z\tilde{r}[a\tilde{r}, b'])\tilde{r}^{-1}=Z[a, b'\tilde{r}^{-1}]$.

Case II. $D^*\supsetneqq C^*$ *and* $n^*>2$. By Lemma 2 (ii), we can find some non-zero $x, y\in D^*$ such that $D^*=C^*[x, y]$ and $K[y]\ni\alpha$. And, by Lemma 7 (ii), there exists some regular element $r\in R^*$ such that $a\tilde{r}=\sum_1^{n^*}d_{ij}e^*_{ij}$ with $d_{1,n^*-1}=x$, $d_{1n^*}=y$, $d_{in^*}=y$, $d_{in^*}=0\ (i\geqq 2)$. And so, again by the remark mentioned above and Lemma 10 (i), there exists some $b'\in R^*$ such that $R^*=Z\tilde{r}[a\tilde{r}, b']=Z[a, b'\tilde{r}^{-1}]$.

Case III. $D^*\supsetneqq C^*$ *and* $n^*=2$. By Lemma 7 (i), there exists a regular element $r\in R^*$ such that $a\tilde{r}=de^*_{11}+d'e^*_{21}+e^*_{12}$. If one of d and d' is not contained in C^*, then we can find a non-zero element $y\in D^*$ such that $D^*=C^*[y, d, d']$ and $K[y]\ni\alpha$ by Lemma 2 (ii). And so, by the remark mentioned above and Lemma 10 (ii), we see that $R^*=Z\tilde{r}[a\tilde{r}, ye^*_{21}]=Z[a, (ye^*_{21})\tilde{r}^{-1}]$. On the other hand, if both d and d' are contained in C^*, then in any rate we can find some $x\in D^*\backslash C^*$ and some non-zero $y\in D^*$ such that $D^*=C^*[x, y]$ and $K[y]\ni\alpha$ by Lemma 2 (ii). We set here $f(\lambda)=\lambda^2-d\lambda-d'$, $z=y^{-1}x$. If $f(y^{-1}x)=f(z)=0$ and $f(y^{-1}(x+1))=f(z+y^{-1})=0$, then by a brief computation we see that $f(y^{-1}(x+\beta))=f(z+\beta y^{-1})=f(z+y^{-1})+(\beta-1)\{f(z+y^{-1})-f(z)\}-\beta(1-\beta)y^{-2}=-\beta(1-\beta)y^{-2}$

for arbitrary $\beta \in K$. Recalling here again $D^* \supsetneqq C^*$, it will be clear that K is infinite. And so, we can find some $\beta \in K$ such that $f(y^{-1}(x+\beta)) \neq 0$. Thus, we may assume, from the beginning, that $f(y^{-1}x) \neq 0$. Consequently, again by the remark cited above and Lemma 10 (iii), it follows $R^* = Z\tilde{r}[a\tilde{r}, xe^*_{21} + ye^*_{22}] = Z[a, (xe^*_{21} + ye^*_{22})\tilde{r}^{-1}]$.

3. Consequences.

Lemma 11. *Let $T \ni 1$ be a subring of R with minimum condition for left ideals. If $R = T \cdot C$ then T is a simple ring.*

Proof. For an arbitrary non-zero ideal N of T, $N \cdot C$ is evidently a non-zero ideal of $R = T \cdot C$, whence $N \cdot C = R$. Now, let N_1, N_2 be ideals of T with $N_1 \cdot N_2 = 0$. Then, $0 = (N_1 \cdot C) \cdot (N_2 \cdot C)$, whence it follows $N_1 = 0$ or $N_2 = 0$. We have proved therefore that 0 is a prime ideal of T, that is, T is simple.

Now, as a first application of Proposition, we can prove the following theorem which contains evidently Lemma 1.

Theorem 1. *Let R be a separable simple algebra over a field $\Phi \subseteq C$ (of finite rank). If a is an element of $R \backslash C$ then $R = \Phi[a, b]$ for some b.*

Proof. Our poof will be completed by distinguishing four cases:

Case I. $n = 1$. In this case, our theorem is Lemma 1 itself.

Case II. $n > 2$. As D is a separable division algebra over Φ, $D = \Phi[x, y]$ with some non-zero elements $x, y \in D$ by Lemma 1. In virtue of Lemma 7 (ii), there exists a regular element $r \in R$ such that $a\tilde{r} = \sum_1^n d_{ij}e_{ij}$ with $d_{1n-1} = x$, $d_{1n} = y$ and $d_{in} = 0$ $(i \geqq 2)$. Now, let $u = \sum_2^n e_{ii-1}$, and set $T = \Phi[a\tilde{r}, u]$, $T^* = T \cdot C$. Then, by Lemma 8, R is T-R-irreducible, whence T^*-R-irreducible. Accordingly, noting that R is inner Galois and finite over C, we see that T^* is simple by Lemma 3. Hence, by Lemma 6 (i), $T^* \supseteq \Phi[\{e_{ij}\text{'s}\}, \{d_{ij}\text{'s}\}] \supseteq \Phi[\{e_{ij}\text{'s}\}, x, y] = R$, that is, $T^* = R$. As evidently T is a ring with minimum condition for left ideals, Lemma 11 enables us to see that T is simple. It follows therefore, again by Lemma 6 (i), $T \supseteq \Phi[\{e_{ij}\text{'s}\}, \{d_{ij}\text{'s}\}] \supseteq \Phi[\{e_{ij}\text{'s}\}, x, y] = R$, whence we obtain $R = T = T\tilde{r}^{-1} = \Phi[a, u\tilde{r}^{-1}]$.

Case III. $D = C$. Let $\bar{C}$ be an extension field of C such that $\bar{C}$ is Galois and finite over Φ. Then, the complete $n \times n$ matrix ring $\bar{R}$ over $\bar{C}$ may be assumed to be $\sum_1^n \bar{C}e_{ij}$. As evidently, C is contained in the center $\bar{C}$ of $\bar{R}$, $V_{\bar{R}}(R)$ is the field $\bar{C}$, and $\bar{R}$ is Galois and finite over Φ, $\bar{R}$, R and Φ satisfy the assumptions of Proposition. Accordingly, our assertion is a direct consequence of Proposition.

Case IV. $n = 2$ *and* $D \neq C$. As $D \neq C$, it will be evident that Φ is infinite. In virtue of Lemma 7 (i), there exists a regular element $r \in R$ such that $a\tilde{r} = de_{11} + d'e_{21} + e_{12}$. If one of d and d' is not contained in C, then we can find some non-zero element $y \in D$ such that $D = \Phi[d, d', y]$ by Lemma 1. We set here $T = \Phi[a\tilde{r}, ye_{21}]$, $T^* = T \cdot C$. Then, by Lemma 8, R is T-R-irreducible, whence T^*-R-irreducible. Accordingly, as R/C is Galois, T^* is simple by Lemma 3. And so, Lemma 6 (ii) implies $T^* \supseteq \Phi[\{e_{ij}\text{'s}\}, d, d', y] = R$, that is, $T^* = R$, whence T is simple by Lemma 11. Hence, again by Lemma 6 (ii), $T \supseteq \Phi[\{e_{ij}\text{'s}\}, d, d', y] = R$. We obtain therefore $R = T = T\tilde{r}^{-1} = \Phi[a, (ye_{21})\tilde{r}^{-1}]$. On the other hand, if both d and d' are contained in C, then by making use of the same argument as in Case III of the proof of Proposition we can find some non-zero elements $x, y \in D$ such that $D = \Phi[x, y]$ and $(y^{-1}x)^2 - d(y^{-1}x) - d' \neq 0$. We set here $T = \Phi[a\tilde{r}, xe_{21} + ye_{22}]$, $T^* = T \cdot C$. As $T \cap De_{21} \neq 0$ by Lemma 9, R is T-R-irreducible by Lemma 8. And so, as in the previous case, Lemma 3 and Lemma 6 (ii) enables us to see that $T^* = R$, whence T is simple by Lemma 11. Hence, again by Lemma 6 (ii), $T \supseteq \Phi[\{e_{ij}\text{'s}\}, x, y] = R$, and eventually $T = T\tilde{r}^{-1} = \Phi[a, (xe_{21} + ye_{22})\tilde{r}^{-1}]$.

In general, for a ring $A \ni 1$ which is left-finite over a simple subring $B \ni 1$, if $A = B[a_1, \cdots, a_k]$ for some $a_1, \cdots, a_k \in A (k > 0)$ and if $A = B[a'_1, \cdots, a'_s]$ $(s > 0)$ always implies $k \leqq s$ then (the uniquely determined) k will be denoted as $n(A/B)$. Needless to say, $n(A/B) = 1$ means that A can be generated over B by only one element. In case R is Galois and finite over S, recalling that V is finite over Z, $n_0 = \text{Max } n(W/Z)$ is finite, where W runs over all the intermediate rings of V/Z. Now, we shall prove that [5, Theorem 3.1] is certainly true.

Theorem 2. *Let R be Galois and finite over S, and V commutative. If T is an arbitrary intermediate ring of R/S, then $n(T/S) = 1$.*

Proof. At first, T is a simple ring by [5, Lemma 1.4]. As our assertion for the case $[S:Z] = \infty$ is given in [5, Corollary 2.1], it suffices to prove our theorem for the case $[S:Z] < \infty$. If $S \subseteq V_T(T)$, then $S \subseteq T = V_T(S) \subseteq V$. And so, recalling that V/S is (Galois and so) separable, we have $T = S[t]$ for some t. As $V_T(T) \subseteq V = C_0$, R, T and S satisfy the assumptions of Proposition. And so, if $S \not\subseteq V_T(T)$ then for each $a \in S \backslash V_T(T)$ Proposition enables us to see that there exists some $t \in T$ such that $T = Z[a, t] = S[t]$.

Next, we shall prove the following:

Theorem 3. *Let R be Galois and finite over S, $S \supsetneqq Z$, and T an intermediate ring of R/S. Then, $n(T/S) = 1$ provided $T \subseteq H$ or $T \supseteq V$.*

Proof. For the case $T \subseteq H$, our assertion is clear by Theorem 2. If $T \supseteq V$, then $V_R(T) \subseteq V_R(S[V]) = V \cap H = C_0$. Hence, $V_R(T)$ is a field. Moreover, to be easily seen, $R/S[V]$ is Galois and $V_R(S[V]) = C_0$ is a field. And so, by [5, Lemma 1.4], T is a simple ring. Again by [5, Corollary

2.1], it suffices to prove our assertion for the case $[S:Z]<\infty$. Noting here that $V_T(T)\subseteq V_R(T)\subseteq C_0$, it will be clear that R, T and S satisfy the assumptions of Proposition. Now, let a be an arbitrary element of $S\backslash Z$. Then, a being in $T\backslash V_T(T)$ of course, there exists some t such that $T=Z[a,t]=S[t]$ by Proposition.

As an easy consequence of Theorem 3, we obtain [5, Theorem 3.2]:

Corollary 1. *Let R be Galois and finite over S, $S\supsetneqq Z$, and V a division ring. If T is a $\tilde{V}$-normal intermediate ring of R/S then $n(T/S)=1$.*

Proof. By [5, Lemma 3.5], there holds $T\subseteq H$ or $T\supseteq V$. And so, our assertion is a direct consequence of Theorem 3.

Moreover, we can prove the following theorem.

Theorem 4. *Let R be Galois and finite over S, V a division ring, and T a $\tilde{V}$-normal intermediate ring of R/S. Then, $n(T/S)=1$ if and only if $T=V_T(T)$ or $S\not\subseteq V_T(T)$.*

Proof. As the only if part is trivial, we shall prove the if part only. For the case where $S\supsetneqq Z$, our theorem is Corollary 1 itself. While, if T is commutative then we have $T\subseteq V_R(T)\subseteq V$. Noting here that $T\subseteq H$ or $V\subseteq T$ by [5, Lemma 3.5], we readily see that $T\subseteq H$ in either cases. Hence, $n(T/S)=1$ by Theorem 2. Thus, it remains only to prove that if $S=Z$ and $S\not\subseteq V_T(T)$ then $n(T/S)=1$. As $V_R(S[C])=V=V_R(H)$ and $[R:C]<\infty$ by [6, Lemma], H coincides with the field $S[C]$. And so, $T\subseteq H$ implies a contradiction $S\subseteq T=V_T(T)$, whence we have $V\subseteq T$ by [5, Lemma 3.5]. Accordingly, there holds $V_T(T)\subseteq V_T(V)\subseteq H=C_0$. Hence, R, T and S satisfy the assumptions of Proposition. If s is an arbitrary element of $S\backslash V_T(T)$, then there exists some t such that $T=Z[s,t]=S[t]$ by Proposition.

As another easy consequence of our proposition, we obtain the next, which is however of enough interest for itself.

Theorem 5. *Let R be Galois and finite over S. If a is in $R\backslash C$ then $R=S[a,b]$ with some b.*

Proof. Again by [5, Corollary 2.1], it suffices to prove our theorem for the case $[S:Z]<\infty$. Applying Proposition for $R^*=R$, we obtain at once our assertion.

And, Theorem 5 yields at once the following, which ia an affirmative answer to the question stated in [5, p. 150].

Corollary 2. *Let R be Galois and finite over S. $n(R/S)=1$ if and only if $R=C$ or $S\not\subseteq C$.*

If R is Galois and finite over S, $R=S[a,b]$ with snme conjugate (with respect to an inner automorphism) a, b by [7, Theorem 1]. And so, combining this fact with Corollary 2, we readily see that [5, Corollary

3.5] holds good. Moreover, it will be easy to see that all the results cited in [5, §3] except [5, Lemmas 3.2 and 3.3] are yet true.

Next, as a partial correction of [5, Lemma 3.3], we shall prove the following:

Lemma 12. *Let R be Galois and finite over S, V a division ring, and T an intermediate ring of R/S. If v is an arbitrary element of $V_T(S)$, then there exists some $t\in T$ such that $S[t]\ni v$ and $T=V_T(Z)[t]$.*

Proof. At first, any intermediate ring of R/S is a simple ring by [5, Lemma 1.4]. By [5, Corollary 2.1], it suffices to prove our lemma for the case where $[S:Z]<\infty$. And so, let $\{x_1, \cdots, x_p\}$ be a linearly independent Z-basis of S. In virtue of [6, Lemma], T is inner Galois and finite over the center C' of T. Accordingly, $V_T(V_T(S))=V_T(V_T(C'[S]))=C'[S]=S\times_Z Z[C'](\subseteq S\times_Z V)$, whence $V_T(S[V_T(S)])=V_T(S)\cap V_T(V_T(S))=V_{S\times_Z Z[C']}(S)=Z[C']$. Hence, we see that $V_T(Z)=V_T(Z[C'])=S[V_T(S)]=S\times_Z V_T(S)$. As T is Galois and finite over $V_T(Z)$ and $V_T(V_T(Z))=Z[C']\subseteq V_T(Z)$, T is $\mathfrak{T}$-isomorphic to $\mathfrak{T}$ by [4, Theorem 3], where $\mathfrak{T}=\mathfrak{G}(T/V_T(Z))\cdot V_T(Z)_r=\widetilde{Z[C']}\cdot V_T(Z)_r$. Now, we can choose a linearly independent C'-basis $\{z_1, \cdots, z_q\}$ of $Z[C']$ from Z. Then, again by [4, Theorem 3], we have $\mathfrak{T}=\sum_1^q\oplus\tilde{z}_i V_R(Z)_r$. If $T\ni t'\leftrightarrow 1\in\mathfrak{T}$ under the isomorphism mentioned above, then $\{t'\tilde{z}_1, \cdots, t'\tilde{z}_q\}$ is evidently a linearly independent $V_T(Z)$-right basis of T and $T=V_T(Z)[t']$. In what follows, we may assume that $v\neq 0$. There holds $1=\sum_1^q(t'\tilde{z}_i)u'_i$ with $u'_i\in V_T(Z)=S\times_Z V_T(S)$. Here, in the representations $u'_i=\sum_1^p v'_{ij}x_j$ with $v'_{ij}\in V_T(S)$ $(i=1, \cdots, q)$, without loss of generality, we may assume that $v'_{11}\neq 0$. Setting here $t=t'v'_{11}v^{-1}$, it will be easy to see that $\{t\tilde{z}_1, \cdots, t\tilde{z}_q\}$ is still a linearly independent $V_T(Z)$-right basis of T (whence $T=V_T(Z)[t]$) and $1=\sum_1^q(t\tilde{z}_i)u_i$ $(u_i\in V_T(Z))$ with $u_1=vx_1+v_2x_2+\cdots+v_px_p$ $(v_j\in V_T(S))$. As $[T:V_T(Z)]\geq[S[t]:V_{S[t]}(Z)]$ by [5, Lemma 3.1], $\{t\tilde{z}_1, \cdots, t\tilde{z}_q\}(\subseteq S[t])$ is also a linearly independent $V_{S[t]}(Z)$-right basis of $S[t]$, which proves that every u_i is contained in $S[t]$. Now, let σ be an arbitrary element of $\mathfrak{G}(R/S[u_1])$. Then, $u_1=u_1\sigma=v\sigma\cdot x_1+v_2\sigma\cdot x_2+\cdots+v_p\sigma\cdot x_p$. And so, recalling that $v\sigma$, $v_i\sigma\in V$ and $S[V]=S\times_Z V$, it follows at once $v=v\sigma$, that is, $v\in S[u_1]$. We have proved therefore $v\in S[u_1]\subseteq S[t]$.

As an application of Lemma 12, we shall prove the following theorem.

Theorem 6. *Let R be Galois and finite over S, and V a division ring. For any intermediate ring T of R/S, $n(T/S)\leqq n_0=\mathrm{Max}\, n(W/Z)$, where W runs over all the intermediate rings of V/Z.*

Proof. If $[S:Z]=\infty$, there is nothing to prove by [5, Corollary 2.1]. And so, we may restrict our proof to the case $[S:Z]<\infty$. And, in this case, as was shown in the proof of Lemma 12, $V_T(Z)=S\times_Z V_T(S)$. Now, let $V_T(S)=Z[v_1, \cdots, v_s]$, where $s=n(V_T(S)/Z)$. Then, $s \leqq n_0$ of course and $V_T(Z)=S[v_1, \cdots, v_s]$. As there exists some t such that $T=V_T(Z)[t]$ and $S[t] \ni v_1$ by Lemma 12, we obtain $T=S[t, v_2, \cdots, v_s]$, which proves our assertion $n(T/S) \leqq s \leqq n_0$.

To be easily seen Theorem 2, that is, [5, Theorem 3.1], is a direct consequence of Theorem 6, too.

Finally, in the proof of [5, Theorem 4.1], we should remark that $\mathfrak{G}_\alpha | M_\beta \subseteq \mathfrak{G}_\beta$ if $M_\alpha \supseteq M_\beta$, which will be easily seen by [5, Corollary 1.1]. And, by the way, we may remark here that the last part of the proof can be omitted. In fact, it is cleat that σ is an automorphism of R.

REFERENCES

[1] N. JACOBSON: Structure of rings, Providence (1956).

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

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

[4] T. NAGAHARA, T. ONODERA and H. TOMINAGA: On normal basis theorem and strictly Galois extensions, Math. J. Okayama Univ', 8 (1958), 133—142.

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

[6] H. TOMINAGA: On a theorem of N. Jacobson, Proc. Japan Acad., 31 (1955), 653—654.

[7] H. TOMINAGA and F. KASCH: On generating elements of simple rings, Proc. Japan Acad., 33 (1957), 187—189.

DEPARTMENT of MATHEMATICS,
OKAYAMA UNIVERSITY
and
DEPARTMENT of MATHEMATICS,
HOKKAIDO UNIVERSITY.

(Received at 18. Juue 1962)