ON GALOIS AND LOCALLY GALOIS EXTENSIONS OF SIMPLE RINGS

TAKASI NAGAHARA and HISAO TOMINAGA

Let K be a division ring which is Galois and finite over L. On generating elements of K (and of an intermediate ring of K/L), one of the present authors continued his considerations in [6; 7; 8; 9][1], and obtained a number of important results. Although one of those results has been extended to simple rings by F. Kasch and another of the present authors [21], it has been unsolved whether other of those can be extended to simple rings or not. One of the purposes of this paper is to present the extensions of several results cited in [6; 7; 8] to simple rings (§§ 2 and 3). More precisely; if a simple ring R is Galois[2] and finite over a simple subring S, we can prove the following: (1) If either S is infinite over its center or $V_R(S)$ is commutative, then for any intermediate ring T of R/S there exists an element t such that $T = S[t]$ (Theorem 2.1 and Theorem 3.1). (2) If S is not a division ring, then $R=S[r]$ with some regular element r (Theorem 2.2). (3) If S is not commutative and $V_R(S)$ is a division ring, then $R = S[r]$ with some r (Theorem 3.2).

On the other hand, since 1956, Galois theory of simple rings of infinite dimension has been undertaken under some finiteness assumptions [10; 19; 20], and then the Galois extensions considered there became necessarily locally Galois. In §§ 1 and 4, we shall deal mainly with locally Galois extensions. The principal theorem of § 1 is the next: Let R be a simple ring which is locally Galois over a simple subring S. In order that every intermediate ring of R/S is a simple ring, it is necessary and sufficient that $V_R(S)$ is a division ring (Theorem 1.1). And in § 4, we shall see that if R/S is locally Galois and $V_R(S)$ is finite over the center of R then R/S is Galois (Theorem 4.1). Moreover, in case $V_R(S)$ is a division ring, we shall obtain a generalization of this fact which corresponds to the conditions adopted in [20]. In § 5, our interest will be directed towards Galois extensions of central simple algebras of finite rank. And for those extensions, several results obtained in [9] will be generalized in part. In the last section § 6, as appendices, we shall present an extension of [1, Satz] to simple rings and another proof of [9, Theorem 1] in which [9, Lemma 2] is not needed.

1) Numbers in brackets refer to the references cited at the end of this paper.

2) If there exists an automorphism group $\mathfrak{G}$ of R such that S is the fixring of $\mathfrak{G}$ and the centeralizer $V_R(S)$ is a simple ring, then we say that R is Galois over S, and $\mathfrak{G}$ is called *a Galois group* of R/S.

Throughout the present paper, we use the following conventions:

R: a simple ring (with minimum condition), which is represented as $\sum_{i,j=1}^{n} De_{ij}$ with matric units e_{ij}'s and a division ring $D = V_R(\{e_{ij}\text{'s}\})$.

S: a simple subring of R containing the identity element of R.

V: the centralizer $V_R(S)$ of S in R.

H: $V_R(V)$.

C: the center of R.

Z: the center of S.

$\mathfrak{G}$: the group of all (ring) automorphisms of R which leave invariant every element of S.

$\mathfrak{I}$: the group of all inner automorphisms of R which leave invariant every element of S.

$\sigma|M$: the restriction of the map σ onto the subset M, where σ is defined on a set containing M. Similarly, for a set $\mathfrak{S}$ of maps defined on a fixed set containing M, $\mathfrak{S}|M = \{\sigma|M\,;\ \sigma \in \mathfrak{S}\}$.

Finally, as to other notations and terminologies used in this paper, we follow [10; 20].

§ 1. To obtain our principal theorem of this section cited in the introduction, several preliminary lemmas will be needed. They are related with Galois extensions of finite dimension, and the first of them is the next:

Lemma 1. 1. *Let R be Galois and finite over S. Then R is homogeneously completely reducible as an S-R-module, and the length of its composition series coincides with the capacity of the simple ring V. In particular, R is S-R-irreducible if and only if V is a division ring.*

Proof. Since $\mathrm{Hom}_{S_l}(R, R) = \mathfrak{G}R_r$, the S-R-module R is completely reducible by [13, Lemma 1. 1]. Recalling here that $\mathrm{Hom}_{S_l \cdot R_r}(R, R) = V_l$ and that V is simple, our assertion will be readily seen.

The next is well-known as the normality theorem, however we shall prove it as a corollary of Lemma 1. 1.

Corollary 1. 1. *Let R be outer Galois and finite over S. An intermediate simple ring N of R/S is $\mathfrak{G}$-normal ($\mathfrak{G}$-invariant) if (and only if) N/S is Galois.*

Proof. Let σ be an S-(ring) isomorphism of N into R. Since R_r is S_r-R_r-irreducible by Lemma 1. 1, so is σR_r, whence σR_r is N_r-R_r-irreducible of course. Now, noting that $\mathrm{Hom}_{S_l}(N, R) = \mathfrak{G}(N/S)R_r$, there exists some $\tau \in \mathfrak{G}(N/S)$ such that σR_r is N_r-R_r-isomorphic to τR_r. If $\sigma a_r \leftrightarrow \tau(a \neq 0)$ under this isomorphism, then, for each $x \in N$, $\sigma(x\sigma)_r a_r = x_r \sigma a_r \leftrightarrow x_r \tau$. On the other hand, $\sigma a_r (x\tau)_r \leftrightarrow \tau(x\tau)_r = x_r \tau$. Hence, we have $(x\sigma)a = a(x\tau)$. Since in particular $sa = as$ for each $s \in S$, we see that a is contained in $V = C$. Conse-

quently, it follows $\sigma = \tau a_t a_r^{-1} = \tau \in \mathfrak{G}(N/S)$.

Lemma 1. 2. *Let R be Galois and finite over S, and M an S-S-submodule of R which possesses a linearly independent S-left basis.*

(i) *$(\mathfrak{G}|M)V_r$ possesses a linearly independent V_r-right basis which is at the same time a linearly independent R_r-basis of $(\mathfrak{G}|M)R_r$.*

(ii) $[M:S]_l = [(\mathfrak{G}|M)R_r : R_r]_r = [(\mathfrak{G}|M)V_r : V_r]_r$.

Proof. It suffices to prove (i) only. Let $V = \sum_{i=1}^{u} \oplus e_i V$, where e_i's are primitive idempotents which are orthogonal to each other. Then, as $R = \sum_{i=1}^{u} \oplus e_i R$, we obtain $(\mathfrak{G}|M)R_r = \sum_{\sigma \in \mathfrak{G}} (\sigma|M)(e_i R)_r$. Since $(\sigma|M)(e_i R)_r$ is S_r-R_r-homomorphic to $(e_i R)_r$ which is isomorphic to each other $(e_k R)_r$ and S_r-R_r-irreducible by Lemma 1. 1, $(\mathfrak{G}|M)R_r$ is homogeneously completely reducible. Now, we set $(\mathfrak{G}|M)R_r = \sum_{j=1}^{s} \oplus (\sigma_j|M)(e_{\alpha_j} R)_r$ and $t = [M:S]_l = [(\mathfrak{G}|M)R_r : R_r]_r$. Then $R = \sum_{i=1}^{u} \oplus e_i R$ will show that $s = tu$. Consequently, $\mathfrak{V} = \sum_{j=1}^{s} (\sigma_j|M)(e_{\alpha_j} V)_r$ possesses a linearly independent V_r-right basis $\{\varepsilon_1, \cdots, \varepsilon_t\}$: $\mathfrak{V} = \sum_{i=1}^{t} \oplus \varepsilon_i V_r$. Since $(\mathfrak{G}|M)R_r = \mathfrak{V}R_r = \sum_{i=1}^{t} \varepsilon_i R_r$ and $[(\mathfrak{G}|M)R_r : R_r]_r = t$, it is clear that $\{\varepsilon_1, \cdots, \varepsilon_t\}$ is also a linearly independent R_r-right basis of $(\mathfrak{G}|M)R_r$. Finally, we shall prove $\mathfrak{V} = (\mathfrak{G}|M)V_r$. If σ is in $\mathfrak{G}$, then $\sigma|M = \sum_{i=1}^{t} \varepsilon_i a_{ir} (a_i \in R)$. Since, for each $s \in S$ we have $\sum_{i=1}^{t} \varepsilon_i s_r a_{ir} = s_r \sigma|M = (\sigma|M)s_r = \sum_{i=1}^{t} \varepsilon_i a_{ir} s_r$, it follows that each a_i is contained in V, whence $\mathfrak{G}|M \subseteq \mathfrak{V}$. We obtain therefore our assertion $(\mathfrak{G}|M)V_r = \mathfrak{V}$, which completes the proof of our lemma.

Lemma 1. 3. *Let R be Galois and finite over S, and T an intermediate ring of R/S. If V is a division ring, then there hold the following*:

(i) *$\{v_1, \cdots, v_m\} \subseteq V$ $(v_i \neq 0)$ is linearly right-independent over $V_R(T)$ if and only if $\{\tilde{v}_1|T, \cdots, \tilde{v}_m|T\}$ is linearly right-independent over R_r, where $\tilde{v} = v_l v_r^{-1}$.*

(ii) *If σ_1, σ_2 are in $\mathfrak{G}$, then $(\sigma_l|T)R_r$ is T_r-R_r-irreducible. And, $(\sigma_1|T)R_r$ is T_r-R_r-isomorphic to $(\sigma_2|T)R_r$ if and only if $\sigma_1|T = \sigma_2 \tilde{v}|T$ for some non-zero $v \in V$.*

(iii) *If $V = \sum_{i=1}^{t} \oplus v_i V_R(T)$, then $(\sigma \widetilde{V}|T)R_r = (\widetilde{V\sigma}|T)R_r = \sum_{i=1}^{t} \oplus (\tilde{v}_i \sigma|T)R_r$ for each $\sigma \in \mathfrak{G}$. In particular, $[(\widetilde{V\sigma}|T)R_r : R_r]_r = t$.*

Proof. (i) Suppose $\{\tilde{v}_1|T, \cdots, \tilde{v}_m|T\}$ is linearly dependent. By Lemma 1. 1, it will be easy to see that each $(v_{il}|T)R_r$ is S_r-R_r-irreducible. And so, we may assume that $\sum_{i=1}^{m} (v_{il}|T)R_r = \sum_{i=s}^{m} \oplus (v_{il}|T)R_r$ with some $s > 1$. We set here $v_{il}|T = \sum_{i=s}^{m} (v_{il}|T)a_{ir}$ $(a_i \in R)$. Then, for each $t \in T$, there holds $\sum_{i=s}^{m} (v_{il}|T)(a_i t)_r = \sum_{i=s}^{m} (v_{il}|T)(t a_i)_r$, whence we have $a_i \in V_R(T)$. This proves evidently that $\{v_1, \cdots, v_m\}$ is linearly dependent over $V_R(T)$. Conversely, suppose that $\{\tilde{v}_1|T, \cdots, \tilde{v}_m|T\}$ is linearly independent. If $\{v_1, \cdots, v_m\}$ is linearly dependent over $V_R(T)$: $\sum_{i=1}^{m} v_i a_i = 0$ (a_i's are contained in $V_R(T)$ and not all zero), then $\sum_{i=1}^{m} (\tilde{v}_i|T)(v_i a_i)_r = 0$, which is a contradiction.

(ii) The T_r-R_r-irreducibility is a consequence of Lemma 1. 1, and the rest of the proof will be completed by making use of the same method as in the proof of Corollary 1. 1.

(iii) $(\widetilde{V}\sigma|T)\mathrm{R}_r = (\widetilde{V}|T)R_r\sigma = (\sum_{i=1}^{t}\oplus(\tilde{v}_i|T)R_r)\sigma = \sum_{i=1}^{t}\oplus(\tilde{v}_i\sigma|T)R_r$ by (i).

Lemma 1. 4. *Let R be Galois and finite over S. If V is a division ring, then each intermediate ring T of R/S is a simple ring.*

Proof. As is cited in Lemma 1. 3, the T_r-R_r-module $(\mathfrak{G}|T)R_r$ is completely reducible and its homogeneous component is of the form $(\widetilde{V}\sigma|T)R_r$:

$$(\mathfrak{G}|T)R_r = \sum_{i=1}^{g}\oplus(\widetilde{V}\sigma_i|T)R_r \qquad \text{with some } \sigma_i\in\mathfrak{G}.$$

Since $\mathfrak{G}(T)$ is evidently a regular group in Nakayama's sense [13], $T'=J(\mathfrak{G}(T), R)$ is a simple ring by [13, Theorem 1]. In what follows, we shall prove that $T'=T$. Since, by Lemma 1. 3 (ii), for any $\tau\in\mathfrak{G}$ there exists some σ_j and $v\in V$ such that $\tau|T=\sigma_j\tilde{v}|T$, that is, $\tau=\tau'\sigma_j\tilde{v}$ for some $\tau'\in\mathfrak{G}(T)$, we have $\tau|T'=\sigma_j\tilde{v}|T'\in(\widetilde{V}\sigma_j|T')R_r$. On the other hand, it is clear that $V_R(T)=V_R(T')$, and so there holds $[(\widetilde{V}\sigma|T)R_r: R_r]_r=[(\widetilde{V}\sigma|T')R_r: R_r]_r$ by Lemma 1. 3 (iii). Accordingly, it will be easy to see that $[T': S]_l = [(\mathfrak{G}|T')R_r: R_r]_r \leqq [(\mathfrak{G}|T)R_r: R_r]_r = [T: S]_l$. As $T'\supseteq T$ of course, it follows eventually $T'=T$.

Corollary 1. 2. *Let R be Galois and finite over S. If either $V=C$ or $V\subseteq S$, then $R=S[r]$ for some $r\in R$.*

Proof. By [5, Satz 9], R is $\mathfrak{G}S_r$-isomorphic to $\mathfrak{G}S_r=\sum_{i=1}^{g}\oplus\sigma_iS_r(\sigma_i\in\mathfrak{G})$. If r is the element of R corresponding to $1\in\mathfrak{G}S_r$ under the above isomorphism, then $\{r\sigma_1, \cdots, r\sigma_g\}$ is a linearly independent S-right basis of R. Now, if $\tau=\sum_{i=1}^{g}\sigma_is_{ir}\in\mathfrak{G}(S[r])$, then $r\cdot 1=r\tau=\sum_{i=1}^{g}(r\sigma_i)s_i$ will yield at once $\tau=1$. Since V is a field in either case, $S[r]$ is simple by Lemma 1. 4. Hence, our assertion is clear by the Galois correspondence established in [13] (or in [19]).

The proof of the next will proceed just as in that of [16, Theorem 4], and the details may be left to readers.

Corollary 1. 3. *Let R/S be abelian with respect to $\mathfrak{H}$.*[3] *If R is of characteristic $p\neq 0$, and $\mathfrak{H}=\mathfrak{H}_1\times\mathfrak{H}_2\times\cdots\times\mathfrak{H}_e$ where each $\mathfrak{H}_i$ is of order p, then there exist some $x_1, \cdots, x_e$ such that*: (1) $x_i^p-x_i\in S$, (2) $R=S[x_1, \cdots, x_e]$, (3) $S[x_i]\cap S[x_1, \cdots, \overset{\vee}{x_i}, \cdots, x_e]=S$, *and* (4) $S[x_i]/S$ *is abelian with respect to* $\mathfrak{H}_i$.

Now we shall prove our principal theorem of this section, which contains the first half of [20, Theorem 3].

3) Cf. [16, p. 16].

Theorem 1. 1. *Let R be locally Galois over S. Then the following conditions are equivalent to each other*:

(1) *Every intermediate ring of R/S is a simple ring.*

(2) *V is a division ring.*

Proof. (1)⇒(2).[4] Let v be an arbitrary non-zero element of V. Then there exists a simple subring N such that $N \supseteq S[v]$, N/S is Galois, and $[N: S] < \infty$. Recalling here $S[V_N(S)] = S \times_Z V_N(S)$, we see that $[V_N(S): Z] < \infty$. Accordingly, if $V_N(S)$ ($\subseteq V$) is not a division ring, then $V_N(S)$ contains a zero-divisor $z \neq 0$. It follows therefore that the center of the simple ring $S[z]$ contains a non-unit z, which is evidently a contradiction. Hence, $V_N(S)$ is a division ring, and so v possesses an inverse in V.

(2)⇒(1). Let T be an arbitrary subring containing S. Since R/S is locally Galois by our assumption, each subring finitely generated over S is simple by Lemma 1. 4. Then, in virtue of this fact, we have $T = \bigcup_{\alpha} S_\alpha$ where S_α runs over all the (simple) subrings of T finitely generated over S. Now, it will be easy to see that T is two-sided simple, so that T is primitive. Moreover, one will penetrate the fact that each non-zero right ideal of T contains a non-zero idempotent element. Combining these with the fact that T is of bounded index (of nilpotency) as a subring of the simple ring R, we have eventually, by [14, (39. 5)], that T is a simple ring.

As an easy consequence of Theorem 1. 1, the following will be readily seen. (Cf. [10; 19; 20].)

Corollary 1. 4. *If R/S is Galois and $\mathfrak{G}$ is l. f. d., then the conditions cited in Theorem 1. 1 are equivalent to each other. In particular, if R/S is locally finite and outer Galois, then there exists a 1—1 dual correspondence between closed subgroups of $\mathfrak{G}$ and intermediate rings of R/S, in the usual sense of Galois theory.*

§ 2. Throughout this section, we assume that *R is Galois and finite over S.*

Lemma 2. 1. *Let K be an intermediate field of S/Z, $N = \sum_{i=1}^{n'} \oplus x_i Z$ a Z-right submodule of R, and $\{a_1, \cdots, a_t\} \subseteq R$ be linearly right indepndent over Z. If K is algebraic and infinite over Z, and $\sum_{u=1}^{s} a_u K = \sum_{u=1}^{s} \oplus a_u K$, then there exist an intermediate field K^* of K/Z and an element $k \in K$ such that $k \notin K^*$, $[K^*: Z] < \infty$, $N + \sum_{u=1}^{s} a_u k K^* = N \oplus \sum_{u=1}^{s} a_u k K^*$, and $\{a_1, \cdots, a_t\}$ is contained in $\sum_{u=1}^{s} a_u K^*$.*

4) Let $S = J(\mathfrak{H}, R)$ with some automorphism group $\mathfrak{H}$, and $[R: S]_l < \infty$. Under this situation, to be easily seen, the proof of (1) ⇒ (2) is still valid. And so, by Lemma 1. 4, we see that the conditions cited in Theorem 1. 1 are equivalent to each other.

Proof. We set $a_i=\sum_{u=1}^{s} a_u k_{iu}$ with $k_{iu}\in K$ $(i=s+1, \cdots, t)$. In case $N\cap\sum_{u=1}^{s} a_u K=\{0\}$, it will be easy to see that $K^*=Z[\{k_{iu}\text{'s}\}]$ and an arbitrary $k\in K\setminus K^*$ are our desired ones. In what follows, we shall consider intently the case where $N\cap\sum_{u=1}^{s} a_u K\neq\{0\}$. Now let $\mathfrak{S}=\{S_1, \cdots, S_q\}$ be the collection of all the (non-empty) subsets $S_h=\{x_h^{(1)}, \cdots, x_h^{(n_h)}\}$ of $\{x_1, \cdots, x_{n'}\}$ such that $\sum_{j=1}^{n_h} x_h^{(j)} Z\cap\sum_{u=1}^{s} a_u K\neq\{0\}$. Then we have

(1) $\sum_{j=1}^{n_h} x_h^{(j)} z_{hj}=\sum_{u=1}^{s} a_u y_{hu}$ with not all zero $z_{hj}\in Z$ and $y_{hu}\in K$ $(h=1, \cdots, q)$. We set here $K^*=Z[\{k_{iu}\text{'s}\}, \{y_{hu}\text{'s}\}]$, and choose an element $k\in K\setminus K^*$. Suppose $N\cap\sum_{u=1}^{s} a_u k K^*\neq\{0\}$. Then, there exists some $S_p\in\mathfrak{S}$ such that $\sum_{j=1}^{n_p} x_p^{(j)} Z\cap\sum_{u=1}^{s} a_u k K^*\neq\{0\}$, that is,

(2) $\sum_{j=1}^{n_p} x_p^{(j)} z'_{pj}=\sum_{u=1}^{s} a_u k y^*_{pu}$ with not all zero $z'_{pj}\in Z$ and $y^*_{pu}\in K^*$.

If $z_{pj_0}\neq 0$, there exists some $z\in Z$ such that $z'_{pj_0}=zz_{pj_0}$. Now, subtracting (1) (for $h=p$) multiplied by z from (2), we obtain

(3) $\sum_{j=1}^{n_p} x_p^{(j)} z''_{pj}=\sum_{u=1}^{s} a_u (k y^*_{pu}-w_u)$, where $z''_{pj}\in Z$ and $w_u\in K^*$.

Since k is not contained in K^*, we may remark here that the coefficients $k y^*_{pu}-w_u$ are not all zero, that is, $S_p\setminus\{x_p^{(j_0)}\}$ is some $S_{p'}$. Secondly, we repeat the same procedure with (3) and (1) (for $h=p'$), and so on. Then we arrive to a contradiction $0=\sum_{u=1}^{s} a_u k_u$ with not all zero $k_u\in K$. Hence, we have $N+\sum_{u=1}^{s} a_u k K^*=N\oplus\sum_{u=1}^{s} a_u k K^*$. The rest of the proof will be almost evident.

Lemma 2. 2. *Let R be Galois and finite over a division ring S, M an S-S-submodule of R, and a an element of M. Then there hold:*

(i) *$a\mathfrak{G}V_r$ possesses a linearly independent (finite) V-right basis.*

(ii) *If $[M: S]_l=[a\mathfrak{G}V_r: V]_r$, then $M=SaS$.*

Proof. (i) Let α be an element of $\mathfrak{G}V_r$. If $a\alpha=0$ then $(SaS)\alpha=S(a\alpha)S=0$, and conversely. And so, by Lemma 1. 2, we have $[SaS: S]_l=[(\mathfrak{G}\,|\,SaS)V_r: V_r]_r=[a\mathfrak{G}V_r: V]_r$.

(ii) Since $[M: S]_l=[a\mathfrak{G}V_r: V]_r=[(\mathfrak{G}\,|\,SaS)\,V_r: V_r]_r=[SaS: S]_l$ by our assumption and the fact cited at the end of the proof of (i), $M=SaS$ is evident.

Theorem 2. 1. *Let M be an S-S-submodule of R. If $[S: Z]=\infty$, then $M=SaS$ for some $a\in M$.*

Proof. Let $S=\sum_{h,k=1}^{m} Ef_{hk}$, where f_{hk}'s are matric units and $E=V_S(\{f_{hk}\text{'s}\})$ is a division ring. Then, $V_R(E)=\sum_{h,k=1}^{m} Vf_{hk}$ is simple, and R is Galois and finite over E. If it has been shown that $M=EaE$ for some $a\in M$, then $M=SaS$ of course. So that, to our end, it suffices to prove our theorem for the case where S is a division ring.

Now, let $M=\sum_{i=1}^{n'}\oplus Sa^{(i)}$, and $\{\varepsilon_1, \cdots, \varepsilon_{n'}\}$ is a linearly independent V_r-

basis of $(\mathfrak{G}|M)V_r : (\mathfrak{G}|M)V_r = \sum_{i=1}^{n'} \oplus \varepsilon_i V_r$ (cf. Lemma 1. 2). As our assertion is clear for $n'=1$, in what follows, we shall prove the case $n'>1$. By Lemma 2. 2, it suffices to show that M contains an element a such that $[a\mathfrak{G}V_r : V]_r = [M : S]_l$. We distinguish here two cases:

Case I: *S contains an element x that is transcendental over Z.* Set $M' = \sum_{i=1}^{n'} a^{(i)}\mathfrak{G}V_r$. Then, $[V : Z] < \infty$ implies $[M' : Z]_r < \infty$. And then the same argument as in the proof of [8, Lemma 3] applies to see that there exists a positive integer k such that $\sum_{i=0}^{\infty} M'y^i = \sum_{i=0}^{\infty} \oplus M'y^i$ for $y = x^k$. If $\alpha = \sum_{i=1}^{n'} \varepsilon_i v_{ir}$ is a non-zero element of $(\mathfrak{G}|M)V_r$, then $0 \neq M\alpha = \sum_{i=1}^{n'} S(a^{(i)}\alpha)$, whence we have $a^{(i_0)}\alpha \neq 0$ for some i_0. We set here $a = \sum_{i=1}^{n'} a^{(i)}y^i$. Then, recalling that $a^{(i)}\alpha \in M'$ and $\sum_{i=0}^{\infty} M'y^i = \sum_{i=0}^{\infty} \oplus M'y^i$, we obtain $a\alpha = \sum_{i=1}^{n'} (a^{(i)}\alpha)y^i \neq 0$. From this, we see that $\{a\varepsilon_1, \cdots, a\varepsilon_{n'}\}$ is a linearly independent V-right basis of $a\mathfrak{G}V_r$, that is, $[a\mathfrak{G}V_r : V]_r = [(\mathfrak{G}|M)V_r : V_r]_r = [M : S]_l$.

Case II: *S is algebraic over Z.* Let K be a maximal subfield of S. Then, $[K : Z] = \infty$ evidently. We set here $a^{(i)}\mathfrak{G}V_r = \sum_{u=1}^{t_i} \oplus a_{iu}Z$, and $\sum_{u=1}^{t_i} a_{iu}K = \sum_{u=1}^{s_i} \oplus a_{iu}K$ $(i=2, \cdots, n')$. Applying Lemma 2. 1 for $N = a^{(1)}\mathfrak{G}V_r$ and $\{a_1, \cdots, a_t\} = \{a_{21}, \cdots, a_{2t_2}\}$, we obtain an intermediate field K_1^* of K/Z and an element $k_1 \in K \setminus K_1^*$ such that $[K_1^* : Z] < \infty$, $a^{(1)}\mathfrak{G}V_r + \sum_{u=1}^{s_2} a_{2u}k_1K_1^* = a^{(1)}\mathfrak{G}V_r \oplus \sum_{u=1}^{s_2} a_{2u}k_1K_1^*$, and $a^{(2)}\mathfrak{G}V_r \subseteq \sum_{u=1}^{s_2} a_{2u}K_1^*$. Repeating the same procedures for the module $a^{(1)}\mathfrak{G}V_r \oplus \sum_{u=1}^{s_2} a_{2u}k_1K_1^*$ and $\{a_{31}, \cdots, a_{3t_3}\}$, and so on, one will obtain eventually $k_1, \cdots, k_{n'-1} \in K$ and intermediate fields $K_1^*, \cdots, K_{n'-1}^*$ of K/Z such that $k_i \in K \setminus K_i^*$, $[K_i^* : Z] < \infty$ and that

$$a^{(1)}\mathfrak{G}V_r + \sum_{i=1}^{n'-1} \sum_{u=1}^{s_{i+1}} a_{i+1u}k_iK_i^* = a^{(1)}\mathfrak{G}V_r \oplus \sum_{i=1}^{n'-1} \oplus \sum_{u=1}^{s_{i+1}} a_{i+1u}k_iK_i^*,$$
$$a^{(i+1)}\mathfrak{G}V_r \subseteq \sum_{u=1}^{s_{i+1}} a_{i+1u}K_i^* (\rightarrow i = 1, \cdots, n'-1).$$

Setting here $a = a^{(1)} + \sum_{i=1}^{n'-1} a^{(i+1)}k_i$, by the same way as in Case I, it will readily follow $[a\mathfrak{G}V_r : V]_r = n'$.

Corollary 2. 1. *If $[S : Z] = \infty$, then for each intermediate ring T of R/S there exists an element $t \in T$ such that $T = S[t]$.*

In [21], it has been shown that $R = S[r, r']$ with some conjugate, regular elements r, r'. As an easy consequence of this fact, we obtain

Theorem 2. 2. *If S is not a division ring, then $R = S[r]$ with some regular element r.*

Proof. Let $S = \sum_{h,k=1}^{m} Ef_{hk}$ $(m>1)$, where f_{hk}'s are matric units and $E = V_S(\{f_{hk}\text{'s}\})$ is a division ring. Then, as is well-known, $R' = V_R(\{f_{hk}\text{'s}\})$ is a simple ring and $R = \sum_{h,k=1}^{m} R'f_{hk}$. Noting that R' is Galois and finite over E, by [21, Theorem 1], we obtain $R' = E[x, y]$ with some regular elements x, y. And then, to be easily verified, $x + f_{12}y$ is a regular element

and $R=S[x+f_{12}y]$.

Lemma 2. 3. *If S is not contained in C but in D, then $R=S[r]$ with some regular element r.*[5]

Proof. By [7, Theorem 3], it suffices to prove the case where $n>1$. Since R is Galois and finite over $\sum_{i,j=1}^{n} Se_{ij}$, so is D over S. Hence, by [7, Theorem 3], $S \subsetneq C = V_n(D)$ yields $D=S[x]$ with some regular element $x \in D$. Here, without loss of generality, we may assume that there exists an element $y \in S$ such that $xy \neq yx$. Now, we set $r=\sum_{i=2}^{n} e_{i-1,i} + xe_{n1}$.[6] Then, we readily see that $r^{-1}=\sum_{i=2}^{n} e_{i,i-1} + x^{-1}e_{1n} \in S[r]$. Moreover, by a brief computation, the next will be verified:

$$S[r] \ni r^{n-i}(r-yry^{-1})(r^{-1}-yr^{-1}y^{-1})r^{-(n-j)}$$
$$=(x-yxy^{-1})(x^{-1}-yx^{-1}y^{-1})e_{ij}, \qquad (i, j=1, \cdots, n).$$

And so, $(x-yxy^{-1})(x^{-1}-yx^{-1}y^{-1})=a$ is contained in $S[r]$. Since $xy \neq yx$, a is a non-zero element of D, whence every e_{ij} is contained in $S[r]$.

Theorem 2. 3. *If $S \cap D$ is not contained in C, then $R=S[r]$. If moreover $[S:Z]<\infty$ then $R=S[r]$ with some regular element r.*

Proof. By Corollary 2. 1, it suffices to prove the latter assertion. Evidently, $V_R(S \cap D)=\sum_{i,j=1}^{n} V_D(S \cap D)e_{ij}$ and $S \cap D = J(\mathfrak{H}, R)$, where $\mathfrak{H}$ is the automorphism group generated by $\mathfrak{G}$ and all inner automorphisms determined by regular elements of $\sum_{i,j=1}^{n} Ce_{ij}$. On the other hand, by [18, Lemma], $[S:Z]<\infty$ and $[R:S]<\infty$ yield $[R:C]<\infty$. It follows therefore that $U=V_R(S \cap D)$ is a simple ring which is finite over C. Moreover, noting that $(\mathfrak{H} \cdot \widetilde{U} : \widetilde{U}) \leqq (\mathfrak{G} : \widetilde{V}) < \infty$, we see that $\mathfrak{H} \cdot \widetilde{U}$ is a regular group of R in Nakayama's sense [13]. Hence, R is Galois and finite over $J(\mathfrak{H} \cdot \widetilde{U}, R) = S \cap D$. Accordingly, by Lemma 2. 3, $R=(S \cap D)[r]=S[r]$ with some regular element r.

Remark. As is shown in [7, Theorem 3], in case R is a division ring, $R=S[r]$ with some r when either $S \subsetneq C$ or R is commutative (and conversely). However, for a simple ring with $[S:Z]<\infty$, it will be considerably difficult to extend the theorem to simple rings. (For the case $[S:Z]=\infty$, by Theorem 2. 1, there is nothing to prove. Cf. also § 3 and [6, Lemma 7].)

---

5) In particular, the complete $t \times t$ matrix ring $(K)_t$ over a non-commutative division ring K can be written as $K[r]$ with some regular element r.

6) As is noted in the proof of [21, Lemma], for $u^*=\sum_{i=2}^{n} e_{i-1,i}$ and $v^*=\sum_{i=2}^{n} e_{i,i-1}$ there holds $e_{ij}=v^{*i-1}u^{*n-1}v^{*n-1}u^{*j-1}$ $(i, j=1, \cdots, n)$. By making use of these equations, one will readily see the following: Let A be a central division algebra of degree (or index) n over a field K. If an algebraic extension field L of K is infinite over K and splits A, then L contains a splitting field L_0 that can be obtained by adjoining at most $2n^2$ elements to K.

§ 3. Throughout the present section, we assume that *R is Galois and finite over S*. And we shall deal exclusively with the case where V is a division ring. At first we shall prove the next:

Lemma 3. 1. *If V is a division ring, and T_1, T_2 are subrings such that $R \supseteq T_1 \supseteq T_2 \supseteq S$, then $[T_1 : V_{T_1}(Z)] \geqq [T_2 : V_{T_2}(Z)]$.*

Proof. Since $[V : V_S(R)] < \infty$ and T_i is simple by Lemma 1. 4, it will be clear that $\infty > [V_{T_i}(T_i)[Z] : V_{T_1}(T_1)] = [T_i : V_{T_i}(Z)]$. Thus, to our end, it suffices to prove that $[V_{T_1}(T_1)[Z] : V_{T_1}(T_1)] \geqq [V_{T_2}(T_2)[Z] : V_{T_2}(T_2)]$. Now we can find a linearly independent $V_{T_2}(T_2)$-basis $\{z_1, \cdots, z_t\}$ of $V_{T_2}(T_2)[Z]$ from Z. If $\{z_1, \cdots, z_t\}$ is not linearly independent over $V_R(T_2)$ then, without loss of generality, we may assume that $\{z_s, \cdots, z_t\}$ $(s > 1)$ is linearly independent over $V_R(T_2)$ and $z_1 = \sum_{i=s}^{t} z_i v_i$ $(v_i \in V_R(T_2))$. Since for each T_2-(ring) automorphism σ of R we have $v_i\sigma \in V_R(T_2)$ and $z_1 = \sum_{i=s}^{t} z_i(v_i\sigma)$, it follows $0 = \sum_{i=s}^{t} z_i(v_i\sigma - v_i)$, that is, $v_i\sigma = v_i$. Recalllng here that R/T_2 is Galois by [13], we see that each v_i is contained in T_2, and hence, in $V_{T_2}(T_2)$. But this is a contradiction. Hence, $\{z_1, \cdots, z_t\}$ is still linearly independent over $V_R(T_2)$. Now, noting that $V_{T_1}(T_1) \subseteq V_R(T_2)$, one will readily obtain our assertion.

Moreover, by the validity of Lemma 1. 4, the proof of the next can be completed just as in that of [6, Lemma 6].

Lemma 3. 2. *Let V be a division ring, and T a subring of R containing S. If v is a regular element of $V_T(Z)$, then there exist some element $t \in T$ and some finite subset $\{z_1, \cdots, z_p\}$ of Z such that $T = \sum_{i=1}^{p} \oplus (t\tilde{z}_i) V_T(Z)$ and that $(t\tilde{z}_1)v + (t\tilde{z}_2)v_2 + \cdots + (t\tilde{z}_p)v_p = 1$ with some v_i's in $V_T(Z)$.*

By the light of these lemmas, we can obtain the following, whose proof proceeds just as in that of [6, Theorem 1], and may be left to readers.

Lemma 3. 3. *Let V be a division ring, and T an intermediate ring of R/S.*

(i) *If v is a regular element of $V_T(Z)$, then there exists some $t \in T$ such that $S[t] \ni v$ and $T = V_T(Z)[t]$.*

(ii) *If $V_T(Z) = S[v]$ with some regular element v, then $T = S[t]$ for some t.*

Now, we can prove the next theorem that contains Corollary 1. 2 as a special case.

Theorem 3. 1. *Let T be an arbitrary intermediate ring of R/S. If V is commutative, then $T = S[t]$ with some t.*

Proof. By Theorem 2. 1, it suffices to prove our theorem for the case where $[S : Z] < \infty$. Since $[R : C] < \infty$ by [18, Lemma] and $S[C]$ is

simple by Theorem 1. 1, $R/S[C]$ is inner Galois, whence we have $V_R(V) = V_R(V_R(S[C])) = S[C]$. And then, noting that $V \subseteq V_R(V) = S[C] = S \times_Z Z[C]$, it follows $V = Z[C]$. Hence, we have $V_R(Z) = V_R(V) = S \times_Z Z[C]$. Accordingly, there holds $V_T(Z) = S \times_Z Z'$ with some intermediate field Z' of $Z[C]/Z$. Since, as in the proof of [6, Lemma 3], we can easily see that $\mathfrak{G}|Z[C] = \mathfrak{G}(Z[C]/Z)$ and $\mathfrak{G}|C = \mathfrak{G}(C/Z \cap C)$ possess the same order, it will be readily seen that $Z[C] = Z \times_{Z \cap C} C$, and that $Z' = Z \times_{Z \cap C} C'$ with some intermediate field C' of $C/Z \cap C$. Hence, it follows $V_T(Z) = S \times_Z (Z \times_{Z \cap C} C') = S \times_{Z \cap C} C'$. Recalling here that C is Galois and finite over $Z \cap C$, we have $C' = (Z \cap C)[v]$ for some non-zero (regular) element v. Since $V_T(Z) = S[v]$ of course, our assertion is a direct consequence of Lemma 3. 3 (ii).

The next is clear by Theorem 3. 1 and [11, Theorem 6].

Corollary 3. 1. *If R is of characteristic $p \neq 0$, and R/S possesses a DF-group*[7] *of order p^e as a Galois group, then for any intermediate ring T of R/S, there exists an element t such that $T = S[t]$.*

In general, if R/S is strictly Galois[8] with sespect to $\mathfrak{H}$ (in particular, if outer Galois), then R contains a $\mathfrak{H}$-normal basis element r, that is, $\{r\sigma; \sigma \in \mathfrak{H}\}$ is a linearly independent S-right basis of R [11, Theorem 4], and $T_{\mathfrak{H}}(r) = \sum_{\sigma \in \mathfrak{H}} r\sigma$ is evidently a regular element of S. Taking this fact into our consideration, we can apply the argument in the proof of [6, Lemma 5] to see the next:

Lemma 3. 4. *Let V be a division ring. If $V_H(H) = C$ and $S \supsetneq Z$, then $R = S[r]$ for some r.*

Proof. As evidently V is Galois and finite over Z, $V = Z[v_1, v_2]$ with some v_i's in V by [5, Satz 14] (or [21, Theorem 1]. Further, noting that H is outer Galois over $S[C]$ (Lemma 1. 4), there exists a $\mathfrak{G}(H/S[C])$-normal basis element h by [11, Theorem 4]), and there holds $H = S[C, h]$ by the proof of Corollary 1. 2. Moreover, as is noted before our lemma, $\sum_{\tau \in \mathfrak{G}(H/S[C])} h^\tau$ is a regular element of $S[C]$. And so, from the beginning, we may assume $\sum_{\tau \in \mathfrak{G}(H/S[C])} h^\tau = 1$. In case Z, and so V is finite, by Theorem 3. 1 (or Corollary 2. 1), our assertion is true without any restriction. Thus, we may restrict our proof to the case where Z is infinite. And then, the rest of the proof proceeds just as in that of [6, Lemma 5].

We insert here the following lemma which may be regarded as a slight generalization of [4, Theorem 7. 13. 1 (1)] and [12, Lemma 2].

Lemma 3. 5. *Let U be a ring with 1, and $B \ni 1$ a two-sided simple subring of U. If $A \ni 1$ is a division subring of U such that B is invariant relative to all inner automorphisms determined by non-zero elements of A,*

7) Cf. [11, Definition 5].
8) Cf. [11, Definition 6].

then either $A\subseteq B$ *or* $A\subseteq V_U(B)$.

Proof. At first, we shall prove $A=(A\cap B)\cup V_A(B)$. Let a be an arbitrary element of A. If a and 1 are linearly left-independent over B, then $(1-a)b'=b^*(1-a)$ $(b\in B)$ implies that $b-b^{**}a=b^*-b^*a$ where $ab=b^{**}a$, and then $b=b^*=b^{**}$, that is, $a\in V_A(B)$. On the other hand, if a and 1 are linearly dependent: $b_1a-b_2=0$ with non-zero $b_1\in B$, then, recalling that B is two-sided simple, we can easily see that a is contained in B.

In case $A\cap B\subseteq V_A(B)$, $A=(A\cap B)\cup V_A(B)$ yields at once $A\subseteq V_U(B)$. Thus, it remains only to show that if $A\cap B\not\subseteq V_A(B)$ then $A\subseteq B$. Now, we can find an element $a_0\in A\cap B$ not contained in $V_A(B)$. Suppose, on the contrary, A is not contained in B. Then there exists an element $a'\in A$ not contained in $A\cap B$, which is in $V_A(B)$ by the remark stated at the beginning of the proof. Since, at the same time, $a'+a_0$ is not contained in $A\cap B$, $a'+a_0$ is also in $V_A(B)$. Hence, a_0 is in $V_A(B)$, which is a contradiction.

By the validity of Lemma 3. 4 and Lemma 3. 5, one will readily see that [6, Corollary 1] and [6, Corollary 2] are still valid in our present stage:

Corollary 3. 2. *Let* V *be a division ring, and* T *a* $\mathfrak{G}$*-normal* ($\mathfrak{G}$*-invariant*) *intermediate ring of* R/S. *If* $V_H(H)=C$ *and* $S\supsetneqq Z$ *then* $T=S[t]$ *with some* t.

Corollary 3. 3. *If* V *is a division ring and* $S\supsetneqq Z$, *then* $V_R(V_H(H))=S[r]$ *with some* r.

Lemma 3. 6. *Let* T *be an intermediate ring of* R/S, Z *be infinite, and* $[S:Z]<\infty$. *If* $T=S[t]$, then $T=S[u]$ *with some regular element* u.

Proof. By [18, Lemma], it follows $[R:C]<\infty$. Combining this with $[C:C\cap S]<\infty$, we obtain $[R:V_S(R)]<\infty$. Hence, $A=V_S(R)[t]$ is a finite dimensional commutative algebra over the field $K=V_S(R)$. If we denote by N the radical of A, then $\bar{A}=A/N=K[\bar{t}]=\bar{A}_1\oplus\cdots\oplus\bar{A}_s$, where $\bar{A}_i$'s are fields over K and $\bar{t}$ is the residue class of t modulo N. We set here $\bar{t}=\bar{a}_1+\cdots+\bar{a}_s$ $(\bar{a}_i\in\bar{A}_i)$. Recalling that Z, and so K is infinite, we can find some $k\in K$ such that each $\bar{A}_i$-component of $\overline{t-k}$ is non-zero. And then, it will be clear that $t-k$ is a regular element and $T=S[t-k]$.

Now, in virtue of Corollary 2. 1, Theorem 3. 1 and Lemma 3. 6, the proof of [6, Corollary 3] is still efficient in proving the next

Corollary 3. 4. *Let* V *be a division ring and* T *an intermediate ring of* R/S. *If* $V_H(H)(=V_V(V))=C[Z]$, $S\supsetneqq Z$, *and* $V_T(Z)$ *is* $\mathfrak{F}$*-normal, then* $T=S[t]$ *for some* $t\in T$.

Proof. If either $[S:Z]=\infty$ or Z is finite, our assertion is clear by

Corollary 2. 1 and Theorem 3. 1. Thus, in what follows, we may restrict our attention to the case where $[S:Z]<\infty$ and Z is infinite. Since $N=V_T(Z)$ is $\mathfrak{F}$-normal, $N\subseteq H$ or $N\supseteq V$ by Lemma 3. 5. If $N\subseteq H$, then $N=S[u]$ for some regular element u by Theorem 3. 1 and Lemma 3. 6. On the other hand, if $N\supseteq V$ then $V_N(S)=V$, whence the center of $V_N(S)$ is $C[Z]$. Since $C[Z]\subseteq V\subseteq N=V_T(Z)$, we may easily see that $C[Z]\subseteq V_N(N)\subseteq$ the center of $V_N(S)=C[Z]$, whence $C[Z]=V_N(N)$. Moreover, recalling that $[R:C]<\infty$ by [18, Lemma], we have $V_R(Z)=V_R(C[Z])=S[V]\subseteq T$ by $V_R(S[V])=C[Z]$ and Theorem 1. 1, whence it follows that $V_T(Z)=V_R(Z)$. And this implies that N is $\mathfrak{G}$-normal, and so N/S is Galois.[9] Hence, by Lemma 3. 4 and Lemma 3. 6, there holds $N=S[u]$ for some regular element u. Since, in either case, $V_T(Z)=S[u]$ with some regular element u, the rest of the proof is clear by Lemma 3. 3 (ii).

And now, we shall prove the following theorem.

Theorem 3. 2. *Let V be a division ring. If $S\supsetneq Z$, and T a $\mathfrak{F}$-normal intermediate ring of R/S, then $T=S[t]$ with some t.*

Proof. If $[S:Z]=\infty$, then our assertion is true without any restriction by Corollary 2. 1. On the other hand, if $[S:Z]<\infty$ then $[R:C]<\infty$ by [18, Lemma], whence it follows $H=V_R(V_R(S[C]))=S[C]\subseteq S\times_Z V$ by Theorem 1. 1. And so, there holds $V_H(H)=C[Z]$. Since $V_T(Z)$ is $\mathfrak{F}$-normal evidently, our assertion is a direct consequence of Corollary 3. 4.

Corollary 3. 5. *If V is a division ring, then $R=S[r, vrv^{-1}]$ for some $r\in R$ and $v\in V$.*

Proof. If $S\supsetneq Z$, by Theorem 3. 2, there is nothing to prove. Thus, it remains only to prove the case $S=Z$. Since the division ring $V=V_R(Z)$ is Galois and finite over S, by [21, Theorem 1], we obtain $V=S[x, vxv^{-1}]$ with some regular elements x, $v\in V$. And then, by Lemma 3. 3 (i), there exists an element $r\in R$ such that $S[r]\ni x$ and $R=V[r]$. Recalling here that $vxv^{-1}\in vS[r]v^{-1}=S[vrv^{-1}]$, it will be clear that $S[r, vrv^{-1}]=V[r]=R$.

§ 4. In this section we shall deal exclusively with locally Galois extensions, and show that in some important cases if R/S is locally Galois then it becomes Galois.

Lemma 4. 1. *Let R/S be locally Galois, N a simple subring of R such that $V_R(N)$ is a division ring, N/S is Galois, and $[N:S]<\infty$. If a is in $N\cap H$ and σ in $\mathfrak{G}(N/S)$, then $a\sigma$ is contained in H.*

Proof. If $a\sigma$ is not contained in H, there exists some $v\in V$ such that $v^{-1}(a\sigma)v\neq a\sigma$. Now, choose a simple subring N' containing $N[v]$ such that

9) Of course, $V_N(S)$ is a division ring.

N'/S is Galois and $[N':S]<\infty$. Then, as is well-known, σ can be extended to an automorphism $\sigma' \in \mathfrak{G}(N'/S)$. As evidently $v\sigma'^{-1} \in V$, we have $(v\sigma'^{-1})^{-1}a(v\sigma'^{-1}) = a$, whence $v^{-1}(a\sigma)v = a\sigma$. But this is a contradiction.

Lemma 4. 2. *If R/S is locally Galois and $V=C$, then R/S is Galois.*

Proof. Let N_α be an intermediate (simple) ring of R/S such that N_α/S is Galois and $[N_\alpha:S]<\infty$, and put $\mathfrak{G}_\alpha = \mathfrak{G}(N_\alpha/S)$. By Corollary 1. 1, if $N_\alpha \supseteq N_\beta$, then there holds $\mathfrak{G}_\alpha | N_\beta = \mathfrak{G}_\beta$. Now let $\mathfrak{G}^*$ be the inverse limit of the system $\{\mathfrak{G}_\alpha; N_\alpha$ runs over all the subrings of R such that N_α/S is Galois and $[N_\alpha:S]<\infty\}$. Then, $\mathfrak{G}^*(\ni 1)$ may be regarded as an automorphism group of R. Since each $\mathfrak{G}_\alpha$ is finite and there holds $\mathfrak{G}_\alpha | N_\beta = \mathfrak{G}_\beta$ for $N_\alpha \supseteq N_\beta$, [2, Corollary 3. 9] yields at once $\mathfrak{G}^* | N_\alpha = \mathfrak{G}_\alpha$, whence our assertion follows directly.

Lemma 4. 3. *If R/S is locally Galois, then V is a simple ring.*

Proof. Let v be an arbitrary non-zero element of V. Now, let N be a simple subring containing $S[v]$ such that N/S is Galois and $[N:S]<\infty$. Since $V_N(S)$ is a simple subring of V containing v, there holds $V_N(S)vV_N(S) = V_N(S) \ni 1$, whence we see that V is two-sided simple, and that each non-zero right ideal of V contains a non-zero idempotent element. Since V is of bounded index, our assertion is a consequence of [14, (39. 5)].

Lemma 4. 4. *If R/S is locally Galois and V is finite over the center Z_0 of V, then there hold the following*:

(i) *H is a simple ring and $\mathfrak{G}(R/H)$ is l. f. d.*

(ii) *H/S is Galois.*

Proof. (i) Let $\{w_1, \cdots, w_t\}$ be a linearly independent Z_0-basis of V, and set $S''=S[\{e_{ij}$'s$\}, \{w_u$'s$\}]$, $H''=V_R(V_R(S''))$. Then, S'' is evidently a simple ring. Moreover, $[S'':S]_l<\infty$ yields $[V: V_R(S'')]_r<\infty$ [10, Corollary 1]. Combining this with $[V:Z_0]<\infty$, we obtain $[V_R(S''):Z'']<\infty$ by [18, Lemma], where Z'' is the center of $V_R(S'')$. Next, recalling that $V_{H''}(H) = V$, we readily see that $[V_{H''}(H): V_{H''}(H'')] = [V:Z''] = [V: V_R(S'')]_r \cdot [V_R(S''):Z''] < \infty$. Thus, V being simple by Lemma 4. 3, $H = V_{H''}(V)$ is simple and $[H'':H]_l = [H'': V_{H''}(V_{H''}(H))]_l < \infty$. Since R/S'' is locally finite, by [15, Theorem 1], one will readily see that R/H'' is locally finite too. Hence, so is R/H. And then, $\mathfrak{G}(R/H)$ is l. f. d. by $[V_R(H): V_H(H)] = [V:Z_0] < \infty$ [20].

(ii) Since H is simple, we can set $H = \sum_{p,q=1}^{n} Fg_{pq}$ with matric units g_{pq}'s and a division ring $F = V_H(\{g_{pq}$'s$\})$. Then, $S^* = S[\{e_{ij}$'s$\}, \{g_{pq}$'s$\}]$ and $H^* = S^* \cap H$ are simple, and $V_R(S^*)$ is a division ring. Let F be an arbitrary finite subset of H. Then we can choose a simple subring N containing $S^*[F]$ such that N/S is Galois and $[N:S]<\infty$. Now, by Lemma 4. 1, it will be easy to see that $N \cap H (\supseteq S[F])$ is a simple subring of H which is

Galois and finite over S. Hence, H/S is locally Galois, whence it is Galois by Lemma 4. 2.

Theorem 4. 1. *If R is locally Galois and V is finite over the center of R, then R/S and $R/S[\{e_{ij}$'s$\}]$ are Galois.*

Proof. Since $R/S[\{e_{ij}$'s$\}]$ is locally Galois necessarily, it suffices to show that R/S is Galois (cf. also [18, Lemma]). Let $\{r_1, \cdots, r_t\}$ be a linearly independent H-left basis of R. We choose here a simple subring M containing $S[\{e_{ij}$'s$\}, \{r_u$'s$\}]$ such that M/S is Galois and $[M:S]<\infty$. Then, to be easily verified, R/M is outer Galois by Lemma 4. 2. And so, to our end, it suffices to prove that $\mathfrak{G}(M/S) \subseteq \mathfrak{G}|M$. Let ρ be an arbitrary automorphism in $\mathfrak{G}(M/S)$. For any intermediate simple ring M_α of R/M such that M_α/S is Galois and $[M_\alpha : M]<\infty$, ρ can be extended to an automorphism in $\mathfrak{G}(M_\alpha/S)$. Now, we denote by $\mathfrak{F}_\alpha$ the totality of these extended automorphisms of ρ, and by $\mathfrak{F}$ the inverse limit of the syetem $\{\mathfrak{F}_\alpha ; M_\alpha$ runs over all the intermediate simple rings of R/M such that M_α/S is Galois and $[M_\alpha : M]<\infty\}$, which may be regarded as a set of isomorphisms of R into R. Since $\mathfrak{G}(M_\alpha/M)$ is a finite group, each $\mathfrak{F}_\alpha$ is finite too. Hence, $\mathfrak{F}$ is non-empty by [2, Theorem 3. 6]. If σ is an arbitrary element of $\mathfrak{F}$, and x an arbitrary element of H which is contained, say, in M_α, then $x\sigma = x(\sigma|M_\alpha) \in H$ by Lemma 4. 1. Thus, we see that $H\sigma \subseteq H$. Further, recalling that H/S is outer Galois by Lemma 4. 4 (ii), we have $H\sigma = H$ [19]. Combining this with $R = H[M]$, we readily see that σ is in fact an automorphism of R.

As a direct consequence of Theorem 4. 1, one will see that the conditions (1)—(4) introduced in [20] (or those assumed in [10, Theorem 1]) are equivalent to the condition that R/S is locally Galois and $[V: C]<\infty$. For the sake of completeness, we shall state this fact as a theorem.

Theorem 4. 2. *Let R/S be locally Galois and $[V: C]<\infty$.*

(i) *For each intermediate regular subrings R_1, R_2 of R/S, every S-(ring) isomorphism of R_1 onto R_2 can be extended to an automorphism of R.*

(ii) *For each intermediate regular subring R' of R/S, R is Galois and locally Galois over R'.*

Moreover, in case V is a division ring, Theorem 4. 1 is still true under a somewhat weakened assumption. To see this, we shall prove more several preliminary lemmas.

Lemma 4. 5. *Let R/S be locally finite, and T an arbitrary intermediate ring of H/S. If $\mathfrak{G}'(F_1/S)|F_2 = \mathfrak{G}'(F_2/S)$ for any subrings F_1, F_2 of R such that $F_1 \supseteq F_2 \supseteq S$ and $[F_1 : S]_l<\infty$, then there holds $T\mathfrak{G}'(T/S) \subseteq H$, where $\mathfrak{G}'(T/S)$ signifies the set of all S-(ring) isomorphisms of T into R.*

Proof. It suffices to prove our lemma for the case where $[T:S]_l<\infty$. Let σ be in $\mathfrak{G}'(T/S)$. If $T\sigma\not\subseteq H$, then there exist some $0\neq v\in V$ and $t\in T$ such that $(t\sigma)v\neq v(t\sigma)$. Since $\sigma^{-1}\in\mathfrak{G}'(T\sigma/S)=\mathfrak{G}'((T\sigma)[v]/S)\,|\,T\sigma$ by our assumption, there holds $\sigma^{-1}=\tau\,|\,T\sigma$ for some $\tau\in\mathfrak{G}'((T\sigma)[v]/S)$. Then, $v\tau$ being evidently in V, $t(v\tau)=(v\tau)t$, whence $(t\tau^{-1})v=v(t\tau^{-1})$, that is, $(t\sigma)v=v(t\sigma)$. But this is a contradiction.

By Theorem 1. 1 and [13, Theorem 6], the next will be almost clear.

Corollary 4. 1. *Let R/S be locally Galois, and T an intermediate ring of H/S. If V is a division ring, then $T\mathfrak{G}'(T/S)\subseteq H$.*

Remark. In fact, Corollary 4. 1 is an easy consequence of Lemma 4. 1. However, we believe Lemma 4. 5 may be of use in investigating local theory of division ring extensions. (Cf., for instance, [17].)

Lemma 4. 6. *If R/S is locally Galois, and V a division ring which is finite over its center Z_0, then, for any finite subset F of R, there exists a (simple) subring H^* such that $H^*\supseteq H[\{e_{ij}'s\}, F]$, $[H^*:H]_l<\infty$, H^*/S and $H^*/S[\{e_{ij}'s\}]$ are Galois, and $[V_{H*}(S):V_{H*}(H^*)]<\infty$.*

Proof. Let S^* be a subring such that $S^*\supseteq S''[F]$, $[S^*:S]_l<\infty$, and S^*/S is Galois, where S'' is the subring considered in the proof of Lemma 4. 4 (i). Setting here $H^*=V_R(V_R(S^*))$ (which is simple by Theorem 1. 1), the same argument as in the proof of Lemma 4. 4 will yield $[V_{H*}(H):V_{H*}(H^*)]<\infty$, $V_{H*}(V_{H*}(H))=H$ and $V_{H*}(H[S^*])=V_{H*}(H)^*$. Hence, by the fundamental theorem of simple rings, we see that $H^*=H[S^*]$. Since, again as in the proof of Lemma 4. 4, one readily sees that $V_R(S^*)$ is finite over its center, H^*/S^* is outer Galois by Lemma 4. 4 (ii). Now let ρ be an arbitrary automorphism in $\mathfrak{G}(S^*/S)$. For any $\mathfrak{G}(H^*/S^*)$-normal intermediate ring M_α^* of H^*/S^* such that $[M_\alpha^*:S]_l<\infty$, ρ can be extended to an element of $\mathfrak{G}'(M_\alpha^*/S)$ by our assumption. Here, we denote by $\mathfrak{F}_\alpha^*$ the totality of these extended isomorphisms of ρ, and by $\mathfrak{F}^*$ the inverse limit of the system $\{\mathfrak{F}_\alpha^*;\ M_\alpha^*$ runs over all the intermediate rings of H^*/S^* such that $[M_\alpha^*:S_l]<\infty\}$, which may be regarded as a set of isomorphisms of H^* into R.[10] If σ and τ are in $\mathfrak{F}_\alpha^*$, then $\tau^{-1}=\gamma\,|\,M_\alpha^*\tau$ with some $\gamma\in\mathfrak{G}'((M_\alpha^*\tau)[M_\alpha^*\sigma]/S)$ by our assumption. Hence, we have $\sigma\gamma=\varepsilon$ with some $\varepsilon\in\mathfrak{G}'(M_\alpha^*/S^*)$. Since $\mathfrak{G}'(M_\alpha^*/S^*)$ coincides with the finite group $\mathfrak{G}(M_\alpha^*/S^*)$ by Corollary 4. 1, we readily see that $\sigma=\varepsilon\tau$ and that $\mathfrak{F}_\alpha^*$ is finite. Consequently, $\mathfrak{F}^*$ is non-empty by [2, Theorem 3. 6]. If ρ^* is an arbitrary element of $\mathfrak{F}^*$, then, recalling that $H^*=H[S^*]$, Corollary 4. 1 will show that ρ^* is an automorphism of H^*. Hence, it will be easy to see that H^*/S and $H^*/S[\{e_{ij}'s\}]$ are Galois. The rest of the proof will be almost evident.

10) By [20], there holds $H^*=\bigcup_\alpha M^*{}_\alpha$.

Theorem 4. 3. *If R/S is locally Galois, V a division ring which is finite over its center Z_0, and $[R:H]_l<\aleph_0$, then R/S is Galois.*

Proof. In virtue of Lemma 4. 6, we can apply the same method as in the proof of [10, Lemma 5] to see that $\mathfrak{G}(H/S)\subseteq\mathfrak{G}|H$. Our assertion is an easy consequence of this fact.

The next is an easy consequence of [18, Lemma] and Theorem 4. 2.

Corollary 4. 2. *If R/S is locally Galois, V finite over its center Z_0, and $[R:H]_l<\aleph_0$, then $R/S[\{e_{ij}'s\}]$ is Galois.*

As an easy consequence of Corollary 4. 2, we see that the conditions (1)—(4) introduced in [10] are equivalent to the condition that R/S is Galois and locally Galois, V is finite over its center Z_0, and $[R:H]_l<\aleph_0$. Consequently, we obtain

Theorem 4. 4. *Let R/S be Galois and locally Galois, $[V:Z_0]<\infty$ and $[R:H]_l<\aleph_0$. And let R' be an intermediate regular subring of R/S with $[V:V_R(R')]_r<\infty$.*

(i) *If ρ is an S-(ring) isomorphism of R' into R and $R'\rho$ is a regular subring with $[V:V_R(R'\rho)]_r<\infty$, then ρ is contained in $\mathfrak{G}|R'$.*

(ii) *R is Galois and locally Galois over R'.*

§ 5. R is called *left algebraic* over S if for each $a\in R$ the ring $S[a]$ is left finite over S. If morever $[S]a[:S]_l\leqq m$ for all $a\in R$ with some fixed integer m, then we shall say that R is *left algebraic and of bounded degree* over S. In this section, we shall restrict our attention to left algebraic Galois extensions of a central simple algebra S of finite rank. At first we shall prove the next:

Theorem 5. 1. *Let S be a central simple algebra of finite rank. If $[V:C]<\infty$, and R is Galois and left algebraic over S, then R is left locally finite over S.*

Proof. It is well-known that $S[V]=S\times_Z V$ is a simple ring. Since $[S[V]:C]=[S[V]:V]\cdot[V:C]=[S:Z]\cdot[V:C]<\infty$, a fundamental theorem of simple rings yields $S[V]=V_R(V_R(S[V]))\supseteq V_R(V)=H$. Accordingly, $[R:S[V]]_l\leqq[R:H]=[V:C]<\infty$, whence it follows $[R:C]=[R:S[V]]_l\cdot[S[V]:C]<\infty$. On the other hand, noting that $S[V]$ is left algebraic over S and $Z[C]$ is contained in the center of V, one will readily see that the field $Z[C]$ is $\mathfrak{G}$-normal (whence $Z[C]/Z$ is Galois) and locally finite over Z. And then, for any finite subset F of C, a similar argument as in the proof of Theorem 3. 1 enables us to see that $Z[F\mathfrak{G}]=Z\times_{Z\cap C}(Z\cap C)[F\mathfrak{G}]$, whence it follows $Z[C]=Z\times_{Z\cap C}C$. There holds therefore $S[C]=S\times_Z Z[C]=S\times_Z(Z\times_{Z\cap C}C)=S\times_{Z\cap C}C$, whence we have

$[S: Z\cap C]=[S[C]: C]\leqslant[R: C]<\infty$. Now, one will easily see that R is algebraic over $Z\cap C$. Combining this with $[R: C]<\infty$, [4, Proposition 10. 12. 3] proves that R is locally finite over $Z\cap C$. Hence, our assertion is clear by $[S: Z\cap C]<\infty$.

The next is an extension of [9, Lemma 4] to simple rings. Although the proof proceeds just as in that of [9, Lemma 4], for the sake of completeness, we shall repeat it here.

Lemma 5. 1. *Let S be a subfield of R containing the center C. If R is left algebraic and of bounded degree over S, then $[R: C]<\infty$.*

Proof. At first we shall prove that S is algebraic over C. If, on the contrary, there exists an element $x\in S$ that is transcendental over C, then, as is well-known, $\{1, x_r, \cdots, x_r^i, \cdots\}$ ($\subseteq \mathrm{Hom}_{S_l}(R, R)$) is linearly independent over R_l, whence so it is over S_l. Now, let X be an arbitrary S-S-submodule of R with $[X: S]_l<\infty$,[11] and ${}_l\mu_X(*)$ a minimal polynomial of $x_r \mid X\in \mathrm{Hom}_{S_l}(X, X)$ over S_l[12] with the degree $n(X)$. And then, choose an element $u\in R$ such that ${}_l\mu_X(x_r)u\neq 0$, and set $X_1=X+SuS$, which is evidently left finite over S. Since $X_1{}_l\mu_X(x_r)\neq 0$, it follows that the degree $n(X_1)$ of a minimal polynomial of $x_r \mid X_1$ over S_l is greater than $n(X)$. Continuing the same procedures, we can find an S-S-submodule Y with $[Y: S]_l<\infty$ such that the degree $n(Y)$ of a minimal polynomial of $x_r \mid Y$ over S_l exceeds m, where m is an integer with $[S[a]: S]_l\leqslant m$ for all $a\in R$. Then, by [3, p. 69, Theorem 1], there exists an element $y\in Y$ such that $\{y, yx_r, \cdots, yx_r^{n(Y)-1}\}$ is linearly left-independent over S. But, recalling that x is contained in S, this yields a contradiction $n(Y)\leqslant[SyS: S]_l\leqslant[S[y]: S]_l\leqslant m$. We have proved therefore S is algebraic over C, as desired.

Secondly, we shall show that $[S: C]<\infty$. Now, suppose $[S: C]=\infty$, and take an intermediate field S^* of S/C with $\infty>p=[S^*: C]>m$, where m is the integer cited just above. Since R is inner Galois and finite over the simple ring $V_R(S^*)$, by [5, Satz 9], $V_R(V_R(S^*))=S^*\subseteq V_R(S^*)$ secures the existence of an element $r\in R$ such that $R=\sum_{i=1}^{p}\oplus V_R(S^*)(r\bar{s}_i)$, where s_i's are regular elements of S^*. Accordingly, we see that $\{rs_1^{-1}, \cdots, rs_p^{-1}\}$ is a linearly independent S-left basis of $\sum_{i=1}^{p}S(r\bar{s}_i)=\sum_{i=1}^{p}\oplus Srs_i^{-1}$. But this yields a contradiction $p\leqslant[S[r]: S]_l\leqslant m$. Hence, we have proved $[S: C]<\infty$. Now, since R is evidently algebraic and of bounded degree over C, $[R: C]<\infty$ follows by [4, Theorem 7. 11. 1].

As a consequence of Lemma 5. 1, we obtain the following which corresponds to [9, Theorem 4].

Theorem 5. 2. *Let S be a central simple algebra of finite rank. If R*

11) For instance, arbitrary $S[a](a\in R)$ may be taken as our X.

12) Here, S_l may be regaded naturally as a subset of $\mathrm{Hom}_{S_l}(X, X)$.

is Galois, left algebraic and of bounded degree over S, *then* $[R:C]<\infty$ *and* $[R:S]<\infty$.

Proof. R is naturally left algebraic and of bounded degree over Z. In particular, the center Z_0 of V being Galois over Z, we see that $[Z_0:Z]<\infty$. Accordingly, it follows $[Z[C]:Z]<\infty$. We set here $Z[C]=\sum_{i=1}^{p}Zc_i$ with some c_i's in C. Now, let x be an arbitrary element of R. Then, there holds $Z[x]=\sum_{j=1}^{q}Zx_j$ with some x_j's, where q is bounded with a fixed integer m. And then, it will be easily seen that $(Z[C])[x]=\sum_{i=1}^{p}\sum_{j=1}^{q}Zc_ix_j$, which proves that R is left algebraic and of bounded degree over the field $Z[C]$ (containing the center C). Hence, our first assertion is a direct consequence of Lemma 5. 1. Next, combining $[R:C]<\infty$ with the fact $[Z_0:Z]<\infty$, it follows that $[R:S]_l\leqq[R:Z]_l=[R:Z_0]_l\cdot[Z_0:Z]\leqq[R:C]\cdot[Z_0:Z]<\infty$, which is the second assertion.

§ 6. Appendices.

(a) As an application of Lemma 1. 4 (or Theorem 1. 1), we can prove the following theorem.

Theorem 6. 1. *Let* V *be a division ring containing infinitely many elements, and* R *(left) finite over* S. *If* $S=J(\sigma, R)$ *with some automorphism* σ, *then for each intermediate ring* T *there exists an automorphism* ρ *such that* $T=J(\rho, R)$.

For the case where R is a division ring, this theorem has been obtained by Bortfeld [1]. And Lemma 1. 4 enables us to apply his method to complete the proof of our theorem. In the sequel, we assume always that V is a division ring and $S=J(\sigma, R)$.

At first, $H=V_R(V)$ is a simple ring. If $[H:S]=a$ then a is the order of $\sigma|H$, and so $\sigma^a=\tilde{v}$. Moreover, $\sigma\tilde{v}\sigma=\tilde{v}\sigma=\sigma\tilde{v}$ implies $v\sigma=cv$ with some $c\in C$. Hence, one will readily see that V is the *field* $C[v]$.

Next, if b is the order of $\sigma|V$, then it will be almost evident that b divides a. Recalling that C is Galois and finite (consequently, separable and finite) over $V_S(R)$ and $V=C[v]$, it will be easy to see that V is primitive over $V_S(R)$. Hence, as is well-known, there exists only a finite number of intermediate fields of $V/V_S(R)$.

Now, by Lemma 1. 4, each intermediate ring T of H/S is $J(\sigma^t|H, H)$ with some positive divisor t of a. Recalling here that $(\sigma^t)^{\frac{a}{t}}=\tilde{v}$, we obtain $J(\sigma^t|H, H)=J(\sigma^t, R)$. In general, for each positive divisor t of a, we denote by $\mathfrak{R}_{\sigma^t}$ the set of all intermediate (simple) rings T of R/S such that $T\cap H=J(\sigma^t, R)$. Since $J(\sigma^\nu|H, H)=J(\sigma^{(\nu,a)}|H, H)\in\mathfrak{R}_{\sigma^{(\nu,a)}}$, it will be clear that each intermediate ring T of R/S is contained in some $\mathfrak{R}_{\sigma^t}$. And then, if we set $\sigma^*=\sigma^t$ and $S^*=J(\sigma^*, R)$, $V_R(V_R(S^*))=H$ shows at once $T\in\mathfrak{R}_{\sigma^{*1}}$. Thus,

to prove our theorem, it suffices to do the following proposition.

Proposition. *If V contains infinitely many elements, then for each $T \in \mathfrak{R}_{\sigma^1}$ there exists an automorphism ρ such that $T = J(\rho, R)$.*

Although the proof of our proposition proceeds just as in that of the corresponding fact for division rings, for the sake of self-containedness, we shall sketch it here.

If a ring M is maximal in $\mathfrak{R}_{\sigma^1}$, then $M = J(\tilde{u}\sigma, R)$ with some $u \in V$. For, recalling that R/M is Galois and $M \cap H = S$, we see that $\mathfrak{G}(R/M)$ contains some $\tilde{u}\sigma$ and $M \subseteq J(\tilde{u}\sigma, R) \in \mathfrak{R}_{\sigma^1}$. We shall prove here the following lemma.

Lemma 6. 1. *Let u be a non-zero element of V, and T an intermediate ring of $J(\tilde{u}\sigma, R)/S$, then $J(\tilde{u}\sigma, R)/T$ is inner Galois and $V_{J(\tilde{u}\sigma, R)}(T) = V_S(T)$.*

Proof. Since $(\prod_{\nu=0}^{a-1} u\sigma^\nu) = \prod_{\nu=0}^{a-1} u\sigma^\nu$, $u_0 = \prod_{\nu=0}^{a-1} u\sigma^\nu$ is contained in S. On the other hand, for each $x \in J(\tilde{u}\sigma, R)$, $x = x(\tilde{u}\sigma)^a = x\tilde{v}\tilde{u}_0$, i. e. $x\tilde{v} = x\tilde{u}_0^{-1}$. Hence, $S = J(\tilde{u}\sigma \mid H, H) = J(\tilde{u}\sigma, R) \cap V_R(v) = V_{J(\tilde{u}\sigma, R)}(u_0) = J(\tilde{u}_0, J(\tilde{u}\sigma, R))$, which contains $V_{J(\tilde{u}\sigma, R)}(S)$. Consequently, $J(\tilde{u}\sigma, R)/S$ is inner Galois, whence so is $J(\tilde{u}\sigma, R)/T$. Moreover, we obtain $V_S(T) \subseteq V_{J(\tilde{u}\sigma, R)}(T) = V_{J(\tilde{u}\sigma, R)}(S) \cap V_R(T) \subseteq S \cap V_R(T) = V_S(T)$, whence $V_{J(\tilde{u}\sigma, R)}(T) = V_S(T)$.

In what follows, we shall use the following additional conventions: T is an arbitrary ring contained in $\mathfrak{R}_{\sigma^1}$. Let $\{M_\alpha\}$ be the set consisting of all the subrings which contain T and are maximal in $\mathfrak{R}_{\sigma^1}$. Since $V_S(R) \subseteq V_R(M_\alpha) \subseteq V$, as is noted above, $\{V_R(M_\alpha)\}$ contains only a finite number of different rings. We shall denote them as $\{V_R(M_1), \cdots, V_R(M_r)\}$. In particular, we set $M = M_1 = J(\tilde{w}\sigma, R)$ and $w_0 = \prod_{\nu=0}^{a-1} w\sigma^\nu$, which is contained in S (cf. the proof cf Lemma 6. 1). And finally, we set $V_R(T) = V_S(R)[d]$.

Lemma 6. 2. *$V_R(T)$ is σ-invariant and $[V_R(T) : V_S(T)] = b$.*

Proof. Since $(\tilde{w}\sigma)^a = \widetilde{w_0 v}$, we have $V_R(M) = C[w_0 v]$. Recalling here that $w_0 \in S$ and $v\sigma = cv (c \in C)$, it is evident that $V_R(M) = C[w_0 v]$ is σ-invariant. Moreover, $\sigma^i \mid V_R(M) = 1 \Leftrightarrow \sigma^i \mid C[v] = 1 \Leftrightarrow \sigma^i \mid V = 1$ proves that the order of $\sigma \mid V_R(M)$ is b. By [13], each automorphism of M/T can be extended to an automorphism of R/T. Now, we denote by $\mathfrak{H}$ the group consisting of all these extended automorphisms. Then, recalling that M/T is Galois, we obtain $J(\mathfrak{H}, R) = T$. Since for each $\tilde{u} \in \mathfrak{H}$ there exists an element $s \in V_S(T)$ such that $\tilde{u} \mid M = \tilde{s} \mid M$ (Lemma 6. 1), we see that $u \in sV_R(M)$. Hence, $V(\mathfrak{H})$ (= the ring generated by all regular elements of R effecting inner automorphisms belonging to $\mathfrak{H}$) is the field $V_R(M)[V_S(T)]$, whence it follows $V_R(T) = V_R(M)[V_S(T)]$, which is evidently σ-invariant. Moreover, noting that $\sigma^i \mid V_R(T) = 1 \Leftrightarrow \sigma^i \mid V_R(M) = 1$, it is clear that the order of $\sigma \mid V_R(T)$ is b, whence we have $[V_R(T) : V_S(T)] = b$.

Lemma 6. 3. *If $g(x) = \prod_{\nu=0}^{a-1}(x - d\sigma^\nu) = \sum_{i=0}^{a} g_i x^i (g_a = 1)$, then $V_S(T) =$*

$V_S(M)[g_0, \cdots, g_{a-1}]$.

Proof. Let $f(x)=\prod_{\nu=0}^{b-1}(x-d\sigma^\nu)=\sum_{i=0}^{b} f_i x^i$. Since $V_R(T)$ is σ-invariant by Lemma 6. 2, $f(x)\in V_S(T)[x]$, and $g(x)=(f(x))^{\frac{a}{b}}$. At first we shall prove that $V_S(T)=V_S(M)[f_0, \cdots, f_{b-1}]$. It is clear that $V_S(T)\supseteq V_S(M)[f_0, \cdots, f_{b-1}]$. On the other hand, noting that $V_R(T)=V_S(M)[d]$ and $f(d)=0$, we have $[V_R(T): V_S(T)]=b\geqq[V_R(T): V_S(M)[f_0, \cdots, f_{b-1}]]$ by Lemma 6. 2. We have proved therefore $V_S(T)=V_S(M)[f_0, \cdots, f_{b-1}]$. We shall distinguish here two cases:

Case I: *the characteristic of R does not divide a/b.* $U=V_S(M)[g_0, \cdots, g_{a-1}]$ is contained in $V_S(T)$. Since $g_{a-1}=(a/b)f_{b-1}$, we see that $f_{b-1}\in U$. Furthermore, $g_{a-\mu}=(a/b)f_{b-\mu}+P(f_{b-\mu+1}, \cdots, f_{b-1})$ (P is a polynomial with integeral coefficients) shows inductively that $f_{b-\mu}\in U$. Hence we have $V_S(T)=V_S(M)[f_0, \cdots, f_{b-1}]\subseteq U$.

Case II: *the chacteristic p of R divides a/b.* Since $V_R(M)=C[w_0 v]$, we see $V=V_R(M)[w_0]$. Recalling that $\sigma^b|V=1$, it is easy to see that $w_0=(w_*)^{\frac{a}{b}}$, where $w_*=\prod_{\nu=0}^{b-1} w\sigma^\nu$. If w_* is inseparable over $V_R(M)$, $V_R(M)[w_*{}^p]\subsetneqq V_R(M)[w_*]=V$. On the other hand, $V_R(M)[w_*{}^p]\supseteq V_R(M)[(w_*{}^p)^{\frac{a}{pb}}]=V_R(M)[w_0]=V$, which is a contradiction. Hence, $V_R(T)/V_R(M)$ has to be separable. Moreover, recalling that $V_R(M)/V_S(M)$ is Galois by Lemma 6. 2, $V_R(T)/V_S(M)$ is separable. Accordingly, to be easily verified, for each $h_1, \cdots, h_m\in V_R(T)$ and an arbitrary positive integer s there holds $V_S(M)[h_1^{p^s}, \cdots, h_m^{p^s}]=V_S(M)[h_1, \cdots, h_m]$. In particular, if p^s divides a/b exactly then $V_S(M)[f_0^{p^s}, \cdots, f_{b-1}^{p^s}]=V_S(M)[f_0, \cdots, f_{b-1}]=V_S(T)$. Since $g(x)=(f_0^{p^s}+f_1^{p^s}x^{p^s}+\cdots+x^{bp^s})^{\frac{a}{bp^s}}=g_0+g_1x+\cdots+g_{a-1}x^{a-1}+x^a$ and p does not divide a/bp^s, the same argument as in Case I enables us to obtain $V_S(M)[g_0, \cdots, g_{a-1}]=V_S(T)$.

Remark. One may remark here that Lemma 6. 3 is true for all maximal M_j.

Lemma 6. 4. *Let $\mathfrak{M}$ be an infinite subset of $V_S(R)$, and $k_0, \cdots, k_q$ elements of $V_S(T)$ such that $V_S(T)=V_S(M_j)[k_0, \cdots, k_q]$ for all $j=1, \cdots, r$. Then, there exists an infinite subset $\overline{\mathfrak{M}}$ of $\mathfrak{M}\setminus\{d\}$ such that $V_S(M_j)[k(m)]=V_S(T)$ for all $m\in\overline{\mathfrak{M}}$ and all j, where $k(x)=\sum_{i=0}^{q} k_i x^i$.*

Proof. Since there exists only a finite number of intermediate fields of $V_S(T)/V_S(M)$, there exists an intermediate field W such that $\mathfrak{M}_1=\{m\in\mathfrak{M}; m\neq d$ and $V_S(M)[k(m)]=W\}$ is infinite. Now, for different $m_1, \cdots, m_{q+1}\in\mathfrak{M}_1$ the simultaneous equations with Vandermond determinant

$$k_0+k_1m_i+\cdots+k_qm_i^q=v_i\in W \qquad (i=1, \cdots, q+1)$$

possess a unique solution, which is necessarily contained in W. Hence, it follows $V_S(T)=V_S(M)[k_0, \cdots, k_q]\subseteq W$, that is, $V_S(T)=W=V_S(M)[k(m)]$

for all $m \in \mathfrak{M}_1$. Repeating the same procedures for $\mathfrak{M}_1$ and M_2 and so on, one will eventually obtain the desired $\widetilde{\mathfrak{M}}$.

Lemma 6.5. *Let V contain infinitely many elements. Then, for an arbitrary positive integer n, there exist n elements $m_1, \cdots, m_n \in V_S(R)\setminus\{d\}$ such that $V_S(M_j)[\prod_{i=s}^{t} g(m_i)] = V_S(T)$ for all j and all integers s, t with $1 \leqq s \leqq t \leqq n$, where $g(x) = \prod_{\nu=0}^{a-1}(x - d\sigma^\nu)$.*

Proof. We shall proceed with induction for n. If $n=1$, by Lemma 6.3, $V_S(M_j)[g_0, \cdots, g_{a-1}] = V_S(T)$ for all j. And then, by Lemma 6.4, there exists an infinite set $\mathfrak{M}_0$ contained in $V_S(R)\setminus\{d\}$ such that $V_S(M_j)[g(m_1)] = V_S(T)$ for all $m_1 \in \mathfrak{M}_0$ and all j. Now, we assume that $m_1, \cdots, m_n$ have been so chosen as desired:

$$V_S(M_j)[\prod_{i=s}^{t} g(m_i)] = V_S(T) \qquad \text{for all } j \text{ and all } 1 \leqq s \leqq t \leqq n.$$

We set here $\prod_{i=s}^{n} g(m_i) = u_s (s = 1, \cdots, n)$. Since $V_S(M_j)[u_s g_0, \cdots, u_s g_{a-1}, u_s] = V_S(M_j)[u_s] = V_S(T)$, noting that $u_s g(x) = u_s g_0 + u_s g_1 x + \cdots + u_s g_{a-1} x^{a-1} + u_s x^a$, Lemma 6.4 secures the existence of such an infinite subset $\mathfrak{M}_1$ of $V_S(R)\setminus\{d\}$ that $V_S(M_j)[u_1 g(m_{n+1,1})] = V_S(T)$ for all $m_{n+1,1} \in \mathfrak{M}_1$ and all j. Next, again by Lemma 6.4, there exists an infinite subset $\mathfrak{M}_2$ of $\mathfrak{M}_1$ such that $V_S(M_j)[u_2 g(m_{n+1,2})] = V_S(T)$ for all $m_{n+1,2} \in \mathfrak{M}_2$ and all j. Repeating the same procedures, we obtain eventually an infinite subset $\mathfrak{M}_n$ of $\mathfrak{M}_{n-1}$ such that $V_S(M_j)[u_n g(m_{n+1,n})] = V_S(T)$ for all $m_{n+1,n} \in \mathfrak{M}_n$ and all j. Finally, as in the case $n=1$, we can find an element $m_{n+1} \in \mathfrak{M}_n$ such that $V_S(M_j)[g(m_{n+1})] = V_S(T)$ for all j. Now, it will be easy to see that $V_S(M_j)[\prod_{i=s}^{t} g(m_i)] = V_S(T)$ for all j and all $1 \leqq s \leqq t \leqq n+1$.

Now, we are at the position to prove our proposition.

Proof of Proposition. Let q be the number of all intermediate fields of $V_R(T)/C$. By Lemma 6.5, we can find $q+1$ elements $m_1, \cdots, m_{q+1} \in V_S(R)\setminus\{d\}$ such that

$$(1) \qquad V_S(M_j)[\prod_{i=s}^{t} g(m_i)] = V_S(T) \text{ for all } j \text{ and all } 1 \leqq s \leqq t \leqq q+1.$$

If we set $w_n = \prod_{k=1}^{n}(m_k - d)(n = 1, \cdots, q+1)$, then $T_n = J(\widetilde{w_n w\sigma}, R)$ is contained in $\mathfrak{N}_\sigma^1$, and $\widetilde{w_n w\sigma} \mid T = \widetilde{w}\sigma \mid T = 1$ shows $T \subseteq T_n$. Since $(\widetilde{w_n w\sigma})^a = \widetilde{w}_n^*$ where $w_n^* = v\prod_{\nu=0}^{a-1} w\sigma^\nu \prod_{k=1}^{n} g(m_k)$, there holds $V_R(T_n) = C[v\prod_{\nu=0}^{a-1} w\sigma^\nu \prod_{k=1}^{n} g(m_k)]$ $(n = 1, \cdots, q+1)$. Noting that $V_R(T) \supseteq V_R(T_n) \supseteq C$, there exists some e, f $(1 \leqq e < f \leqq q+1)$ such that $V_R(T_e) = V_R(T_f)$, that is;

$$(2) \qquad C[v\prod_{\nu=0}^{a-1} w\sigma^\nu \prod_{k=1}^{e} g(m_k)] = C[v\prod_{\nu=0}^{a-1} w\sigma^\nu \prod_{k=1}^{f} g(m_k)].$$

Recalling here that $m_k - d \neq 0$, one will readily see that $v\prod_{\nu=0}^{a-1} w\sigma^\nu \prod_{k=1}^{e} g(m_k) \neq 0$. Accordingly, from (2), we obtain $V_S(T_f)[\prod_{k=e+1}^{f} g(m_k)] \subseteq V_S(T_f)$. Since $V_S(T) \supseteq V_S(T_f)) \supseteq V_S(M_{j_0})$ for some j_0, by (1), there holds $V_S(T) = V_S(T_f)[\prod_{k=e+1}^{f} g(m_k)]$, whence it follows $V_S(T) = V_S(T_f)$. And then, $V_R(T)$

$\supseteq V_R(T_f)$ and $[V_R(T): V_S(T)]=b=[V_R(T_f): V_S(T_f)]$ (Lemma 6. 2) yield at once $V_R(T)=V_R(T_f)$. Consequently, we have $V_{T_f}(T)=V_{T_f}(T_f)$. Now, since T_f/T is inner Galois by Lemma 6. 1, $T_f=T$, which is our assertion.

(**b**) In what follows, R be always a division ring (accordingly, so is S). And we shall present here another proof of [9, Theorem 1] that we believe is fairly simpler than that given in [9]. To this end, at first we shall prove the next.

Lemma 6. 6. *Let N be a right V-submodule of R that is finite over V. If $[S: Z]=\infty$ then for each positive integer n there exist n non-zero elements $s_1, \cdots, s_n \in S$ such that $\sum_{i=1}^{n} Ns_i=\sum_{i=1}^{n} \oplus Ns_i$.*

Proof. In case S/Z is not algebraic, our assertion is contained in [8, Lemma 3]. Thus, it remains only to prove the lemma for the case where S/Z is algebraic.

Let M be a maximal subfield of S. Then it will be clear that M is infinite and locally finite over Z. Accordingly, $M[V](=M\times_Z V\subseteq S\times_Z V)$ is a division ring that is infinite and locally finite over V. If $N=\sum_{u=1}^{w} \oplus d_u V$, then we may assume $\sum_{u=1}^{w} d_u M[V]=\sum_{u=1}^{w} \oplus d_u M[V]$, and we can find such a finite subset F of $M[V]$ that $\sum_{u=1}^{w} d_u V[F]\supseteq N$. Since $[V]F]: V]_r<\infty$ and $[M[V]: V]_r=\infty$, it follows $M\not\subseteq V[F]$. And so, we can choose an element $s_1\in M\setminus V[F]$. If $\sum_{u=1}^{t} d_u y_u=\sum_{u=1}^{t} d_u s_1 y'_u$, that is, $\sum_{u=1}^{t} d_u(y_u-s_1 y'_u)=0$ with $y_u, y'_u\in V[F]$, then, noting that $y_u-s_1 y'_u\in M[V]$, we see that y_u's and y'_u's are all zero, which means $\{0\}=\sum_{u=1}^{t} d_u V[F]\cap \sum_{u=1}^{t} d_u s_1 V[F]\supseteq N\cap Ns_1$. Hence, we have $N+Ns_1=N\oplus Ns_1$.

Next, if we have found such non-zero $s_1, \cdots, s_n\in S$ that $\sum_{i=1}^{n} Ns_i=\sum_{i=1}^{n} \oplus Ns_i$, we can apply the above argument for $N'=\sum_{i=1}^{n} Ns_i$ in place of N to obtain a non-zero element $s'_{n+1}\in S$ such that $N'+N's'_{n+1}=N'\oplus N's'_{n+1}$. Then, setting $s_{n+1}=s_1 s'_{n+1}$, one will readily see that $\sum_{i=1}^{n+1} Ns_i=\sum_{i=1}^{n+1} \oplus Ns_i$.

Now the proof of the next [9, Theorem 1] can be completed without distinguishing two cases.

Theorem 6. 2. *Let a division ring R be Galois over S, and $[S: Z]=\infty$. If X is an S-S-submodule of R which is left finite over S, then $X=SaS$ for some $a\in X$.*

Proof. Let $[X: S]_l=n$. Then, by [9, Corollary 1 (2)], we have $[x\mathfrak{G}V_r: V]_r=[SxS: S_l]\leqq[X: S]_l=n$ for each $x\in X$. Hence, to our end, it suffices to show that there exists an element $a\in X$ such that $[a\mathfrak{G}V_r: V]_r=[X: S]_l=n$.

We set here $X=\sum_{i=1}^{n} \oplus Sd_i$ and $(\mathfrak{G}|X)V_r=\sum_{i=1}^{n} \oplus (\sigma_i|X)V_r$, where $\sigma_i\in\mathfrak{G}$ (cf. [Corollary 1 (1)]). Then, by [9, Corollary 1 (2)], we have $[d_i\mathfrak{G}V_r: V]_r<\infty$. And so, $N=\sum_{i=1}^{n} d_i\mathfrak{G}V_r$ is right-finite over V. Hence,

by Lemma 6. 6, there exist n *non-zero elements* $s_1, \cdots s_n, \in S$ such that $\sum_{i=1}^{n} Ns_i = \sum_{i=1}^{n} \oplus Ns_i$. We set here $a = \sum_{i=1}^{n} d_i s_i$. If $\alpha = \sum_{i=1}^{n} (\sigma_i | X) v_{i_r}$ is a non-zero element of $(\mathfrak{G} | X) V_r$, then $0 \neq X\alpha = \sum_{i=1}^{n} S(d_i\alpha)$, whence it follows that $d_{i_0}\alpha \neq 0$ for some i_0. Noting that $d_i\alpha \in N$ and $\sum_{i=1}^{n} Ns_i = \sum_{i=1}^{n} \oplus Ns_i$, we obtain $a\alpha = \sum_{i=1}^{n} (d_i\alpha)s_i \neq 0$. Hence, $\{a\sigma_1, \cdots, a\sigma_n\}$ is linearly right-independent over V. There holds therefore $[a\mathfrak{G}V_r : V]_r = [(\mathfrak{G} | X) V_r : V_r]_r = n$.

REFERENCES

[1] R. BORTFELD : Ein Satz zur Galoistheorie in Schiefkörpern, J. f. d. r. u. angew. Math., 201 (1959), 196—206.

[2] S. EILENBERG and N. STEENROD : Foundations of algebraic topology, Princeton (1952).

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

[4] _____ : Structure of rings, Providence (1956).

[5] F. KASCH : Über den Endomorphismenring eines Vektorraumes und den Satz von der Normalbasis, Math. Ann., 126 (1953), 447—463.

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

[7] _____ : On generating elements of Galois extensions of division rings III, Math. J. Okayama Univ., 7 (1957), 173—178.

[8] _____ : On generating elements of Galois extensions of division rings IV, Math. J. Okayama Uuiv., 8 (1958), 181—188.

[9] _____ : On generating elements of Galois extensions of division rings V, Math. J. Okayama Univ., 10 (1960), 11—17.

[10] T. NAGAHARA, N. NOBUSAWA and H. TOMINAGA : Galois theory of simple rings IV, Math. J. Okayama Univ., 8 (1958), 189—194.

[11] T. NAGAHARA, T. ONODERA and H. TOMINAGA : On normal basis theorem and strictly Galois extensions, Math. J. Okayama Univ, 8 (1958), 133—142.

[12] T. NAGAHARA and H. TOMINAGA : On Galois theory of division rings, Math. J. Okayama Univ., 6 (1956), 1—21.

[13] T. NAKAYAMA : Galois theory of simple rings, Trans. Amer. Math. Soc., 73 (1952), 276—292.

[14] T. NAKAYAMA and G. AZUMAYA : Algebra II (Theory of rings), Tokyo (1954), in Japanese.

[15] N. NOBUSAWA : A note on Galois extensions of division rings, Math. J. Okayama Univ., 7 (1957), 179—183.

[16] N. NOBUSAWA and H. TOMINAGA : Some remarks on strictly Galois extensions of simple rings, Math. J. Okayama Univ., 9 (1959), 13—17.

[17] N. NOBUSAWA and H. TOMINAGA : On Galois theory of division rings III, Math. J. Okayama Univ., 10 (1960), 67—73.

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

[19] _____ : Galois theory of simple rings, Math. J. Okayama Univ., 6 (1956), 29—48.

[20] _____ : Galois theory of simple rings II, Math. J. Okayama Univ., 6 (1957), 153—170.

[21] 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 January 13, 1961*)

Added in proof. In the proof of Corollary 3.4, $N=S[u]$ was obtained as a consequence of Lemma 3.4 and Lemma 3.6. However, by making use of Theorem 3.1 and Lemma 3.6, one will easily see that the assertion $N=S[u]$ is a direct consequence of the fact that $V_N(S)$ is the field $C[Z]$. Thus, Lemma 3.4 is unessential in our present study.