ON NORMAL BASIS THEOREM AND STRICTLY GALOIS EXTENSIONS

TAKASI NAGAHARA, TAKESI ONODERA
and HISAO TOMINAGA

Let K be a Galois extension field of finite degree over the ground field L. Then, as is well-known, K possesses a linearly independent L-basis of the form $\{k\sigma\}$, where σ runs over the Galois group $\mathfrak{G}^*$ of K/L (normal basis theorem). Evidently this proposition may be interpreted in the following way: K is $\mathfrak{G}^*L_r$-isomorphic to $\mathfrak{G}^*L_r$, where L_r means the right multiplication by L. After several extensions of the normal basis theorem to division rings and other rings with outer Galois groups, F. Kasch put forward his consideration along the line of the above interpretion, and obtained some interesting results for rings with not necessarily outer Galois groups [3][1]. One of the purposes of this paper is to present supplementary remarks to Kasch's work (§1). In §§2—4, we shall deal mainly with strictly Galois extensions, for which a sort of normal basis elements can be found, more precisely, for some finite subgroup of the Galois group we can find a normal basis element. Almost every result stated in §2 has been given in [2] and [9], however §2 will play a preparatory rôle for §§3—4. In §3, we shall consider the structure of simple rings treated in §2. Further §4 contains a remark on quaternion algebras, and we shall conclude our study with an appendix containing several results on group rings over simple rings (§5).

1. Throughout the present paper except §5, R will denote a simple ring (with an identity element and minimum condition for one-sided ideals), and $\mathfrak{G}$ a group of autmorphisms of R.

Definition 1. R is said to be *w-Galois with respect to* $\mathfrak{G}$ when the subring S of all $\mathfrak{G}$-invariants ($S = J(\mathfrak{G}, R)$) is simple. Or, for a simple subring S of R, we say that R/S is *w-Galois* if there exists some $\mathfrak{G}$ such that $S = J(\mathfrak{G}, R)$. In case R/S is w-Galois with respect to $\mathfrak{G}$, $\mathfrak{G}$ will be called *a Galois group* of R/S, and the group of all S-automorphisms of R *the Galois group* of R/S. Further, if R/S is w-Galois and $V_R(S)$[2] is a simple subring then R/S is said to be *Galois* (or R is *Galois* over S).[3]

Definition 2. Let R be Galois and finite over a simple subring S. If

[1] Number in brackets refer to the references cited at the end of this paper.

[2] For any non-empty subset X of a ring U, $V_U(X)$ means the centralizer of X in U.

[3] One readily sees that R is Galois and finite over S if and only if $S = J(\mathfrak{G}, R)$ for some regular group $\mathfrak{G}$ (in Nakayama's sense [6]).

R is $\mathfrak{G}^*S_r$-isomorphic to $\mathfrak{G}^*S_r$[4] (as a right-module) then we say that *normal basis theorem holds for R/S,* where $\mathfrak{G}^*$ is the Galois group of R/S.

Definition 3. Let R be Galois over S. R is said to be *commutatively extended from S* if $R=S\otimes_{V_S(S)} C$ for some field C (cf. [1]).

Our first result is the next theorem.

Theorem 1. *Let R be Galois and finite over S. Then, for any $\mathfrak{G}$ with $S=J(\mathfrak{G}, R)$, the S_l-endomorphism ring of R coincides with $\mathfrak{G}R_r$: $\mathrm{Hom}_{S_l}(R, R)=\mathfrak{G}R_r$ if and only if $V(\mathfrak{G})$ is two-simple, where $V(\mathfrak{G})$ means the subring generated by all regular elements $v\in R$ with $\tilde{v}=v_l v_r^{-1}\in\mathfrak{G}$.*

Proof. Let $\mathfrak{G}^*$ be the Galois group of R/S, and $\mathfrak{J}^*=\widetilde{V_R(S)}$[5]. Then, as is well-known, $(\mathfrak{G}^*:\mathfrak{J}^*)\cdot[V_R(S):V_R(R)]=[R:S]<\infty$[6] and $\mathrm{Hom}_{S_l}(R, R)=\mathfrak{G}^*R_r=\sum_{\sigma^*}\oplus\sigma^*V_R(S)_l\otimes R_r$, where $\otimes$ means the tensor product over $V_R(R)_r(=V_R(R)_l)$ and σ^* runs over some fixed complete representative system of $\mathfrak{G}^*/\mathfrak{J}^*$ (cf. [6]). Similarly, $\mathfrak{G}R_r=\sum_{\sigma}\oplus\sigma V(\mathfrak{G})_l\otimes R_r$, where σ runs over some fixed complete representative system of $\mathfrak{G}/\mathfrak{G}\cap\mathfrak{J}^*$. Noting that $\mathfrak{G}/\mathfrak{G}\cap\mathfrak{J}^*\cong\mathfrak{G}\mathfrak{J}^*/\mathfrak{J}^*$ and $V(\mathfrak{G})\subseteq V_R(S)$, we readily see that $\mathfrak{G}^*R_r=\mathfrak{G}R_r$ if and only if $V_R(S)=V(\mathfrak{G})$ and $\mathfrak{G}^*=\mathfrak{G}\mathfrak{J}^*$. However, if $V(\mathfrak{G})$ is (two-sided) simple then a similar argument as in the proof of $\mathrm{Hom}_{S_l}(R, R)=\mathfrak{G}^*R_r$ shows that $\mathfrak{G}R_r$ is simple (cf. [6]), and so $\mathfrak{G}R_r=\mathrm{Hom}_{S_l}(R, R)$, completing the proof.

Now, replacing U and R in [8, Theorem] by R and $V_R(S)$ respectively, we readily obtain the following

Lemma 1. *Let R be Galois over S. If the Galois group of R/S is finite then either $V_R(S)=V_R(R)$ or $V_R(S)$ is finite.*

Theorem 2. *Let R be Galois (and finite) over S. If the order n of the Galois group $\mathfrak{G}^*=\mathfrak{G}(R/S)$ of R/S coincides with $[R:S]$: ord. $\mathfrak{G}^*=[R:S]$, then $V_R(S)=V_R(R)$.*

Proof. As ord. $(\mathfrak{G}^*/\widetilde{V_R(S)})=[V_R(V_R(S)):S]$,[7] we obtain ord. $\widetilde{V_R(S)}=[R:V_R(V_R(S))]$. Thus, it suffices to prove that if R is inner

[4] v_l and v_r means the left and the right multiplications by v respectively. Similarly, for any subset X, $X_r=\{x_r \mid x\in X\}$.

[5] For any subset X, $\tilde{X}$ denotes the totality of inner automorphisms induced by regular elements contained in X. And so, $\widetilde{V_R(S)}$ is the subgroup of $\mathfrak{G}^*$ consisting of all inner automorphisms.

[6] $[\ :\ ]_l$ and $[\ :\ ]_r$ denote the left and the right dimenions respectively. And in case $[\ :\ ]_l=[\ :\ ]_r$, they are denoted as $[\ :\ ]$.

[7] Recall here that $V_R(V_R(S))$ is outer Galos Over S.

Galois over S and $n = [R : S]$ then $n = 1$. By Lemma 1, either $V_R(S) = V_R(R)$ or $V_R(S) = \sum_{h,k=1}^{m} De_{hk}$ where e_{hk}'s are matric units and $D = V_{V_R(S)}(\{e_{hk}\})$ is a finite field, say $GF(q^s)$ with $\{d_1, \cdots, d_s\}$ as an independent basis over $C = V_R(R)$. Then we may, and shall, restrict our attention to the latter case. At first we shall prove $m = 1$. Suppose, on the contrary, $m > 1$, then the following set $U(\subseteq V_R(S))$ defines $s(m^2 + 1)$ $(> n)$ different inner automorphisms: $U = \{d_i(i = 1, \cdots, s),\ d_i(1 + e_{hk})\ (i = 1, \cdots, s;\ h \neq k),\ d_i(1 + e_{h1})(1 + e_{1h})\ (i = 1, \cdots, s;\ h \neq 1),\ d_i \sum_{t=1}^{m} e_{t,m-t+1}\ (i = 1, \cdots, s)\}$. This contradiction shows $m = 1$, that is, $n = s$. Now let D^* and C^* be the multiplicative groups consisting of all non-zero elements of D and C respectively. If $n > 1$, then the index of C^* in $D^*(= \text{ord.}\,\mathfrak{G})$ is $(q^n - 1)/(q - 1) > n$, which is a contradiction.

In his paper [3], F. Kasch proved that, in case R is a division ring, in order that normal basis theorem holds for R/S it is necessary and sufficient that either $V_R(S) = V_R(R)$ or $V_R(S) \subseteq S$. Moreover, for simple rings too, he verified the sufficiency of the above condition, We shall prove here that the condition is necessary as well for our Galois extensions.[8]

Theorem 3. *Let R be Galois and finite over S, and let $\mathfrak{G}^*$ be the Galois group of R/S. Then the following conditions are equivalent to each other :*

(1) *Normal basis theorem holds for R/S.*

(2) $[\mathfrak{G}^* S_r : S_r]_r = [R : S]$.

(3) *Either $V_R(S) = V_R(R)$ or $V_R(S) \subseteq S$.*

Proof. (3) ⇒ (1) is contained in [3, Satz 7], and (1) ⇒ (2) is trivial. Now we shall prove (2) ⇒ (3). Throughout the proof, we shall set $V_R(S) = \sum_{i,j=1}^{n} De_{ij}$ where e_{ij}'s are matric units and $D = V_{V_R(S)}(\{e_{ij}\})$ is a division ring. To our end, it suffices to show that if $V_R(S) \neq V_R(R)$ and $V_R(S) \not\subseteq S$, then there exist a regular element $v \in V_R(S)$ and a finite set $\{v_i\}$ consisting of regular elements of $V_R(S)$ which are linearly independent over $V_R(R)$ such that $\tilde{v} = v_l v_r^{-1}$ is a linear combination of $\tilde{v}_i$'s with coefficients $(\in R_r)$ not all in S_r. Since in case $n = 1$ the proof proceeds just as in that of [3, Satz 10], in what follows, we shall restrict our attention to the case $n > 1$.

Evidently the regular elements 1 and all $f_{ij} = 1 + e_{ij}$ $(i, j = 1, \cdots, n;\ i \neq j)$ are linearly independent over $V_R(R)$, and similarly in case n is

[8] Kasch's definition of Galois extensions is rather general than ours (cf. [3, p. 455]).

even so are the regular ones $f_i = e_{ii} + \sum_{j=1}^{n} e_{j,n-j+1} (i = 1, \cdots, n)$. Noting that $V_R(S) \cap S = V_S(S)$ is a field contained in the center of $V_R(S)$, it is clear that no nondiagonal elements of $V_R(S)$ are contained in S. Now we are going to prove our assertion by distinguishing two cases:

Case I. S is not of characteristic 2. Evidently, in this case, $1 + f_{ij}$ $(i \neq j)$ are all regular and not contained in S. And so, the following is our desired relation : $(\widetilde{1+f_{ij}}) = \tilde{1}(1+f_{ij})_r^{-1} + \tilde{f}_{ij}(f_{ij}(1+f_{ij})^{-1})_r$.

Case II. S is of characteristic 2. We shall distinguish further two cases : (1) *n is odd*. In this case, one readily sees that $u = 1 + \sum_{i=2}^{n} f_{i-1i}$ is a regular element not contained in S. Accordingly we have $\tilde{u} = \tilde{1}(u^{-1})_r + \sum_{i=2}^{n} \tilde{f}_{i-1i}(f_{i-1i}u^{-1})_r$. (2) *$n$ is even*. There holds $1 = \sum_{i=1}^{n} f_i$ obviously, and so $\tilde{1} = \sum_{i=1}^{n} \tilde{f}_i(f_i)_r$ is a required relation. We have completed therefore our proof.

Remark 1. Of course in case R is a division ring, the notion of w-Galois coincides with that of Galois, and the simplicity of $V(\mathfrak{G})$ in Theorem 1 is superfluous, whence $\mathrm{Hom}_{S_l}(R, R) = \mathfrak{G}R_r$ for any $\mathfrak{G}$ with $S = J(\mathfrak{G}, R)$.

2. In case R/S is outer Galois, as is well-known, there exists a normal basis, (or what is the same, normal basis theorem holds in our sense). In [2] and [9], this fact is extended to some wider class of Galois extensions. We shall summarize here principal results cited there together with several supplementary remarks.

Definition 4. Let R be w-Galois with respect to a *finite* group $\mathfrak{G}$. For any $r \in R$, $T_{\mathfrak{G}}(r) = \sum_{\sigma \in \mathfrak{G}} r\sigma$ that is contained in $S = J(\mathfrak{G}, R)$ is called the *$\mathfrak{G}$-trace* of r. If $\{r\sigma \mid \sigma \in \mathfrak{G}\}$ forms an independent (right) S-basis of R then r is a *$\mathfrak{G}$-normal basis element* (abr. *$\mathfrak{G}$-n. b. e.*) of R over S.

The next definition is, in case R is a division ring, nothing but to say that $\mathfrak{G}$ is of finite order.

Definition 5. $\mathfrak{G}$ is called an *F-group* if it is of finite order and $V(\mathfrak{G})$ (cf. Theorem 1) is two-sided simple, that is, $V(\mathfrak{G})$ contains no proper two-sided ideals other than the zero-ideal. Particularly, if $V(\mathfrak{G})$ is a two-sided simple integral domain, then the F-group is said to be a *DF-group*.

Lemma 2. *Let $\mathfrak{G}$ be an F-group, and set $S = J(\mathfrak{G}, R)$. Then R is Galois over S, $[R : S] \leqq$* ord. $\mathfrak{G}$, *and $V(\mathfrak{G}) = V_R(S)$ which is finite over $V_R(R)$. And of course there holds* $\mathrm{Hom}_{S_l}(R, R) = \mathfrak{G}R_r$. *In particular, if $\mathfrak{G}$ is a DF-group then $V_R(S)$ is a division ring.*

Lemma 3. *Let $\mathfrak{G}$ be a DF-group, and set $S = J(\mathfrak{G}, R)$. Then any* *subgroup* $\mathfrak{H}$ *of* $\mathfrak{G}$ *is a DF-group too, and* $V_T(S)$ *is a division ring where* $T=J(\mathfrak{H}, R)$.

Proof. By Lemma 2, $V(\mathfrak{G}) = V_R(S)$ is a division ring finite over $V_R(R)$, accordingly $V(\mathfrak{H})$ is so as a subring of $V_R(S)$ containing $V_R(R)$.

Now, by the light of Lemma 2, we may set the following definition.

Definition 6. Let $\mathfrak{G}$ be an F-group, and set $S = J(\mathfrak{G}, R)$. If ord. $\mathfrak{G} = [R : S]$ then we say that R is *strictly Galois* over S with respect to $\mathfrak{G}$ (or simply R/S is strictly Galois).

The next is [2, Theorem 2][9] (or a corollary of [9, Theorem 1]).

Theorem 4. *If* R *is strictly Galois over* $S = J(\mathfrak{G}, R)$ *with respect to* $\mathfrak{G}$ *then* R *possesses a* $\mathfrak{G}$*-n. b. e. over* S, *and* R *is* $\mathfrak{G}^*S_r$*-homomorphic to* $\mathfrak{G}^*S_r$ *where* $\mathfrak{G}^* = \mathfrak{G}(R/S)$.

Further, the next is also a corollary of [9, Theorem 2].

Theorem 5. *Let* R *be strictly Galois over* S *with respect to* $\mathfrak{G}$, $\mathfrak{H}$ *an* F*-group of order* $n > 1$ *which is a normal subgroup of* $\mathfrak{G}$, *and let* $T = J(\mathfrak{H}, R)$. *Then the following conditions are equivalent to each other :*

(I) $r \in R$ *is a* $\mathfrak{G}$*-n. b. e. over* S *if and only if the* $\mathfrak{H}$*-trace of* r *is a* $\overline{\mathfrak{G}}$*-n. b. e. over* S, *where* $\overline{\mathfrak{G}} = \mathfrak{G}/\mathfrak{H}$ *and* $\overline{\mathfrak{G}}$ *may be considered as an automorphism group of* T.

(II) S *is of characteristic* $p \neq 0$ *and* n *is a power of* p.

Corollary 1. *Let* R *be a simple ring,* $\mathfrak{G}$ *an* F*-group of order* n, *and* R *be strictly Galois with respect to* $\mathfrak{G}$. *If* R *is of characteristic* $p \neq 0$ *and* n *is a power of* p *then* $r \in R$ *is a* $\mathfrak{G}$*-n. b. e. over* $J(\mathfrak{G}, R)$ *whenever the* $\mathfrak{G}$*-trace is regular. And the converse is true when* $n > 1$.

As a consequence of Corollary 1, we obtain the next which contains [1, Lemma 1] and [1, Corollary to Lemma 12].

Corollary 2. *Let* R *be of characteristic* $p \neq 0$ *and strictly Galois over* S *with respect to* $\mathfrak{G}$ *of order* p^e. *Then a necessary and sufficient condition that* R *is commutatively extended from* S *is the existence of an element* c *of* $V_R(R)$ *with non-zero* $\mathfrak{G}$*-trace. Further, when it is the case, any normal intermediate simple subring of* R/S *is also commutatively extended from* S.

Proof. If $T_{\mathfrak{G}}(c) \neq 0$ $(c \in V_R(R))$ then $\{c\sigma \mid \sigma \in \mathfrak{G}\}$ is an independent S-basis of R contained in $V_R(R)$ by Corollary 1. Accordingly $R = S[V_R(R)] = S \otimes_{V_S(S)} V_R(R)$. The converse is also clear.

Finally we shall prove the following

[9] Cf. also the errata for [2] to appear in the Notices of Amer. Math. Soc.

Corollary 3. *Let a division ring R of characteristic $p \neq 0$ be strictly Galois over S with respect to $\mathfrak{G}$ of order p^e. If normal basis theorem holds for R/S, then each element with non-zero $\mathfrak{G}$-trace is a generating element of R over S.* (Cf. also Corollary 4.)

Proof. By Theorem 3, either $V_R(S) = V_R(R)$ or $V_R(S) \subseteq S$. Since in the first case there is nothing to prove (because of Corollary 1), we assume hereafter $V_R(S) \subseteq S$, and let $T_{\mathfrak{G}}(r) \neq 0$. Recalling that $\mathfrak{G}(R/S) \subseteq \mathfrak{G}V_R(S)_r \subseteq \mathfrak{G}S_r$, any $\tau \in \mathfrak{G}(R/S[r])$ is represented uniquely in the form $\tau = \sum_{\sigma \in \mathfrak{G}} \sigma s_{\sigma r}$ with $s_\sigma \in S$. Hence we have $r = r\tau = \sum_{\sigma \in \mathfrak{G}} (r\sigma)s_\sigma$, whence, $\{r\sigma \mid \sigma \in \mathfrak{G}\}$ being an independent S-basis of R, we obtain $s_\sigma = 0$ for all $\sigma \neq 1$ and $s_1 = 1$, that is, $\tau = 1$. Thus we have proved the corollary.

3. In this section, we shall use the following conventions, unless otherwise specified : R is a simple ring with the center C of characteristic $p \neq 0$, $\mathfrak{G}$ a DF-group of order p^e, and $S = J(\mathfrak{G}, R)$.

If $\mathfrak{J}$ is the subgroup consisting of all inner automorphisms contained in $\mathfrak{G}$ then $J(\mathfrak{J}, R) = V_R(V_R(S))$ evidently. Our first lemma is the next

Lemma 4. *$[R : S]$ divides p^e.*

Proof. In case $e = 1$, R/S is either outer or inner Galois. If R/S is outer Galois then, as is well-known, $[R : S] = p$. Thus we assume R/S is inner Galois, and set $\mathfrak{G} = \widetilde{\{1, \tilde{v}, \cdots, \tilde{v}^{p-1}\}}$. Then $v^p = c$ for some $c \in C$, whence one can readily see that the polynomial $x^p - c \in C[x]$ is irreducible. And so, $V_R(S) = C[v]$ yields $[V_R(S) : C] = p$, that is, $[R : S] = p$. Now we proceed with induction for e, and assume $e > 1$. Take a normal subgroup $\mathfrak{P}$ of order p. Then, by Lemma 3, $P = J(\mathfrak{P}, R)$ is a simple ring over which R is of dimension p and $V_P(S)$ is a division ring (of finite dimension over $V_P(P)$). Thus $\mathfrak{G}_P$ (the restriction of $\mathfrak{G}$ onto P) is also a DF-group. Noting that ord. $\mathfrak{G}_P$ is a proper divisor of ord. $\mathfrak{G} = p^e$, our induction hypothesis yields at once that $[R : S] = [R : P] \cdot [P : S]$ is a divisor of p^e.

Lemma 5. *If the order of $\mathfrak{G}$ is greater than $1 : p^e > 1$, then $S \neq C$.*

Proof.[10] If, on the contrary, $S = C$ then (R is a division ring and), the center of $\mathfrak{G}$ being different from the identity group, the center of $\mathfrak{G}$ contains a subgroup $\mathfrak{P} = \widetilde{\{1, \tilde{v}, \cdots, \tilde{v}^{p-1}\}}$ of order p. Now let $\sigma = \tilde{u}$ be an arbitrary element of $\mathfrak{G}$. Then $\widetilde{u^{-1}vu} = \tilde{u}\,\tilde{v}\,\tilde{u}^{-1} = \tilde{v}$ implies $v\sigma = vc$ with some $c \in C$. Further, as $\widetilde{v^p} = \tilde{v}^p = \tilde{1}$, there exists some

[10] As is readily seen from the proof, Lemma 5 can be generalized as follows : *Let $\mathfrak{G}$ be a DF-group of order p^e (p a prime and $e > 0$) of a simple ring R. If the center C of R contains no primitive pth roots of 1, then $J(\mathfrak{G}, R) \neq C$.*

$c_0 \in C$ such that $v^p = c_0$. Then one can easily see that $c_0 = u^{-1}v^p u = (v\sigma)^p = v^p c^p = c_0 c^p$, that is, $c^p = 1$, whence we have $c = 1$. Hence there holds that $v\sigma = v$ for each $\sigma \in \mathfrak{G}$ and so v must be contained in C, that is, $v = 1$. But this is a contradiction.

Theorem 6. *Let R be a simple ring of characteristic $p \neq 0$, and $\mathfrak{G}$ a DF-group of order p^e. Then $V_R(S) = C[V_S(S)]$, where $S = J(\mathfrak{G}, R)$.*

Proof. At first, let $e = 1$. Since in case $\mathfrak{G}$ is outer our assertion is clear, we assume $\mathfrak{G}$ is inner and set $\mathfrak{G} = \{\widetilde{1}, \tilde{v}, \cdots, \tilde{v}^{p-1}\}$. Then $V_R(S) = C[v]$, and so $V_R(S) = V_S(S)$ as desired. Now we shall proceed with induction for e. Assume $e > 1$, and denote by C_0 the center of $V_R(S)$. Then the group of all the inner automorphisms contained in $\mathfrak{G}$ induces a Galois group $\mathfrak{J}_0$ of $V_R(S)/C_0$. Since the order of $\mathfrak{J}_0$ divides p^e, Lemma 5 shows that ord. $\mathfrak{J}_0 = 1$, that is, $V_R(S) = C_0$. Finally, suppose $V_R(S) \supsetneqq C[V_S(S)]$. Since $V_R(S) = V(\mathfrak{G})$, $\mathfrak{G}$ contains an inner automorphism defined by an element v not contained in $C[V_S(S)]$. Then evidently $v^{p^d} \in C$ for some $d > 0$, whence v is inseparable over $C[V_S(S)]$. However, this contradicts the fact that $V_R(S)$ is (Galois and so) separable over $C[V_S(S)]$. Hence $V_R(S)$ has to coincides with $C[V_S(S)]$.

Now, by [4, Theorem 1], the next is a direct consequence of the preceding theorem.

Corollary 4. *Let R be a division ring of characteristic $p \neq 0$, and $\mathfrak{G}$ a p-group. Then $V_R(S)$ is a field, and therefore, for any intermediate subring T of R/S, $T = S[t]$ with some t.*

In the last corollary, R can be obtained by successive cyclic extensions (of degree p). And so, we may apply the proof of [1, Corollary 2 to Theorem 9] to see the next

Corollary 5. *Under the same assumption as in Corollary 4, if S is a perfect field then R is commutative.*

Remark 2. In case $\mathfrak{G}$ is inner, $V_R(S) \subseteq S$ by Theorem 6, and so it is clear that, for any intermediate simple subring T of R/S, T/S is also inner Galois. In connection with this fact, we may remark here the following general fact: *Let R be a simple ring which is inner Galois and finite over a simple subring S, and let T be an intermediate simple subring of R/S. Then S is the fixring of some inner automorphism group of T, or what is the same, T is inner Galois over S if and only if the center of T is contained in S.*

Proof. As the only if part is almost clear, we shall prove here the if part only. Our assumption $V_T(T) \subseteq S$ implies $V_R(S)$ is an algebra over $V_T(T)$. On the other hand, $V_T(S)$ is a central simple algebra (of finite rank over $V_T(T)$). These facts enable us to apply Wedderburn's theorem to prove $V_R(S) = V_R(T) \otimes_{V_T(T)} V_{V_R(S)}(V_R(T)) = V_R(T) \otimes_{V_T(T)} V_T(S)$. From the last relation, we see that $V_T(S)$ is simple, and so we have $S \subseteq J(\widetilde{V_T(S)}, T) = V_T(V_T(S)) = V_T(V_T(S) \otimes_{V_T(T)} V_R(T)) \subseteq V_R(V_R(S)) = S$, proving our assertion.

4. Evidently, in case R/S is strictly Galois with respect to *cyclic* $\mathfrak{G}$, $V_R(S)$ is a field. However, the converse part of the following theorem shows that this is not always true for general case.

Theorem 7. *Let R be a simple ring with the center C, and let $[R : C] = 4$. If R/C is strictly Galois with respect to $\mathfrak{G}$, then C is not of characteristic 2, and R is a quaternion algebra, and convesely.*

Proof. As $[R : C] = 4$, R is either a central division algebra or the complete 2×2 matrix ring C_2 over C. In case R is a division ring, C is not of characteristic 2 by Lemma 5. Thus, in what follows, we restrict our attention to the case $R = C_2$. Supposing, on the contrary, that C is of characteristic 2, one readily sees that, for $r \ni R$, $r^4 \in C$ if and only if r is of the form $\begin{pmatrix} c & b \\ d & c \end{pmatrix}$. And so, $\mathfrak{G} = \left\{ \tilde{1}, \widetilde{\begin{pmatrix} c_1 & b_1 \\ d_1 & c_1 \end{pmatrix}}, \widetilde{\begin{pmatrix} c_2 & b_2 \\ d_2 & c_2 \end{pmatrix}}, \widetilde{\begin{pmatrix} c_3 & b_3 \\ d_3 & c_3 \end{pmatrix}} \right\}$ with some b_i, c_i, $d_i \in C$. Noting that $V(\mathfrak{G}) = R$, we see that 1, and the matrices $\begin{pmatrix} c_i & b_i \\ d_i & c_i \end{pmatrix}$'s are linearly independent over C. But this is a contradiction, because $\begin{pmatrix} 0 & b_i \\ d_i & 0 \end{pmatrix}$'s are linearly dependent clearly. Hence C is not of characteristic 2 in either cases, accordingly, as is well-known, R is a quaternion algebra over C.[11] The converse part will be almost evident.

5. In [9], the notion of group rings over primary rings played an important rôle. Taking consideration of this situation, we may state here several results on group rings over simple rings.

Throughout this section, $\mathfrak{G}$ be a finite group of order n, and S a simple ring with the center Z. Then, as is shown in [5, Corollary to Theorem 14], the group ring $\mathfrak{G}S$ is a Frobenius ring. Moreover, noting that $\mathfrak{G}S = \mathfrak{G}Z \otimes_Z S$, we readily see that $\mathfrak{G}S$ is semi-simple if and only if S is either of characteristic zero or of characteristic $p \neq 0$ not dividing n. In what follows, our attention will be mainly directed towards non-semi-simple $\mathfrak{G}S$. We set here the following lemma.

Lemma 6. *Let A be an algebra of finite rank over Z with an identity.*

[11] Cf. [3, p. 460].

(1) *$A\otimes_Z S$ is primary decomposable if and only if A is so.*

(2) *$A\otimes_Z S$ is uni-serial if and only if A is so.*

Proof. Noting that $\mathfrak{a}\rightarrow\mathfrak{a}\otimes_Z S$ and $\mathfrak{A}\rightarrow\mathfrak{A}\cap A$ are mutually inverse 1-1 correspondences between (two-sided) ideals $\mathfrak{a}$ of A and ideals $\mathfrak{A}$ of $A\otimes_Z S$, the first proposition is almost clear. Thus we shall prove (2) only. At first, suppose that A is uni-serial. Then [5, Theorem 16] yields that $A/\mathfrak{a}$ is Frobenius for any ideal $\mathfrak{a}$. As $(A\otimes_Z S)/\mathfrak{A}\cong(A/\mathfrak{A}\cap A)\otimes_Z S$ for any ideal $\mathfrak{A}$ of $A\otimes_Z S$, $(A\otimes_Z S)/\mathfrak{A}$ is Frobenius by [5, Theorem 14]. Hence $A\otimes_Z S$ is uni-serial by [5, Theorem 16]. The converse part also will be shown in the similar way.

Now, combining Lemma 6 with Theorems 1 and 6 of [7], we obtain the following theorem at once.

Theorem 8. *Let S be of characteristic $p\neq 0$, and $n=p^e n'$ with $(p, n')=1$.*

(1) *$\mathfrak{G}S$ is primary decomposable if and only if $\mathfrak{G}$ contains a normal subgroup of index p^e.*

(2) *$\mathfrak{G}S$ is uni-serial if and only if $\mathfrak{G}$ contains a normal subgroup of index p^e and a p-Sylow group of $\mathfrak{G}$ is cyclic.*

The following theorem is contained essentially in [9, Corollary 2].

Theorem 9. *Let $\mathfrak{G}$ be of order $n>1$. Then the following conditions are equivalent to each other :*

(1) *$\sum_{\sigma\in\mathfrak{G}}\sigma x_\sigma\in\mathfrak{G}S$ is regular if and only if $\sum_{\sigma\in\mathfrak{G}}x_\sigma\in S$ is regular.*

(2) *S is of characteristic $p\neq 0$, and n is a power of p.*

(3) *$\mathfrak{G}S$ is primary.*

Proof. The equivalence of (1) and (2) is a special case of [9, Corollary 2]. $\mathfrak{G}S$ is primary if and only if $\mathfrak{G}Z$ is (primary and so) completely primary. Thus the equivalence of (2) and (3) is also clear by [9, Lemma 3].

Corollary 6. *Under the assumption of Theorem 9, the following conditions are equivalent to each other :*

(1) *$\sum_{\sigma\in\mathfrak{G}}\sigma x_\sigma\in\mathfrak{G}S$ is regular if and only if $\sum_{\sigma\in\mathfrak{G}}x_\sigma\in S$ is non-zero.*

(2) *S is a division ring of characteristic $p\neq 0$ and n is a power of p.*

(3) *$\mathfrak{G}S$ is completely primary.*

REFERENCES

[1] A. S. AMITSUR, Non-commutative cyclic fields, Duke Math. J., 21 (1954) 87—106.

[2] C.C. FAITH, Galois extensions in which every element with regular trace is a normal basis element, Proc. Amer. Math. Soc., 9 (1958) 222—229.

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

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

[5] T. NAKAYAMA, On Frobeniusean algebras II, Ann. Math., 42 (1941) 1—21.

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

[7] M. OSIMA, On primary decomposable group rings, Proc. Phys.-Math. Soc. Japan, 24 (1942) 1—9.

[8] H. TOMINAGA, A note on conjugates, Math. J. Okayama Univ., 7 (1957) 75—76.

[9] H. TOMINAGA, A note on Galois theory of primary rings, Math. J. Okayama Univ., 8 (1958) 117—123

DEPARTMENTS OF MATHEMATICS,
OKAYAMA UNIVERSITY
HOKKAIDŌ GAKUGEI UNIVERSITY
OKAYAMA UNIVERSITY

(Received August 26, 1958)